



Avaya Solution & Interoperability Test Lab

Application Notes for the Witness Systems Compliance Package with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Witness Systems Compliance Package call recording server to successfully interoperate with Avaya Communication Manager and Avaya Application Enablement Services. During compliance testing, the Compliance Package successfully recorded calls placed to and from Avaya IP Telephones, Avaya Digital Telephones, Avaya IP Softphones (Telecommuter, Road Warrior), analog telephones, and agents, as well as calls placed to a Vector Directory Number (VDN) and queued to an agent hunt/skill group.

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

1. Introduction

These Application Notes describe the configuration steps required for the Witness Systems Compliance Package 7.3 call recording server to successfully interoperate with Avaya Communication Manager 3.0.1 and Avaya Application Enablement Services 3.1. During compliance testing, the Compliance Package successfully recorded calls placed to and from Avaya IP Telephones, Avaya Digital Telephones, Avaya IP Softphones (Telecommuter, Road Warrior), analog telephones, and agents, as well as calls placed to a Vector Directory Number (VDN) and queued to an agent hunt/skill group.

Figure 1 illustrates the network configuration used to verify the Witness Systems solution. The configuration details, provided in these Application Notes, focus on the interfaces between Avaya Communication Manager, Avaya AES server, and Witness Systems Compliance Package.

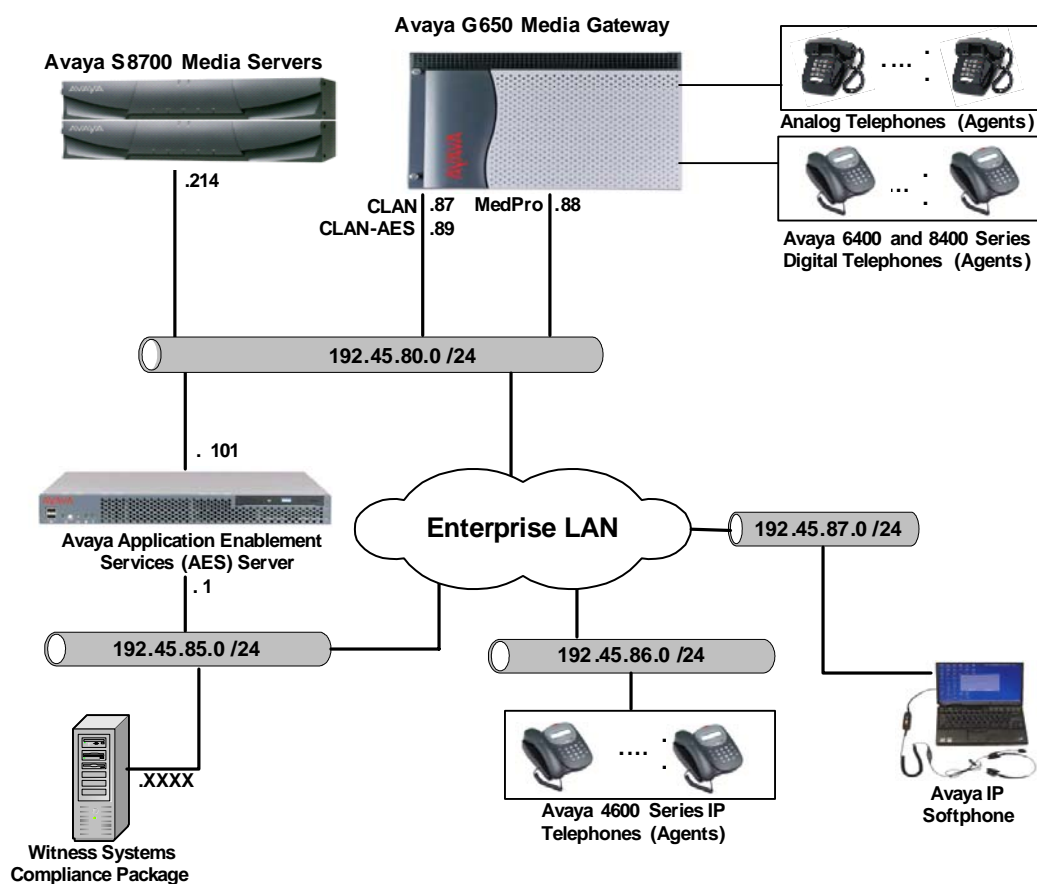


Figure 1: Test Configuration of Compliance Package with Avaya Communication Manager and Avaya Application Enablement Services

2. Equipment and Software Validated

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

Equipment		Software
Avaya S8700 Media Server		Communication Manager 3.0.1 (R013x.00.1.346.0)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface	FW 30
	TN799DP CLAN Interface	FW17
	TN2302AP IP Media Processor	FW108
	TN2602AP IP Media Resource 320	FW 07
Avaya Application Enablement Services (AES) Server		3.1 Bundled Offer Build 33.1
Avaya 4600 Series IP Telephones		
4620SW		2.3
4621SW		2.2.3
4625SW		2.5
Avaya IP Softphones		5.2.4.20
Avaya 6400 Series Digital Telephones		-
Analog Telephone		-
Witness Compliance Package		7.3.1

3. Configure Avaya Communication Manager

This section provides the procedures for configuring Computer Telephony Integration (CTI) links, hunt/skill groups, vectors, Vector Directory Numbers (VDN), agents, agent login/logoff codes, recording ports, and codecs on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the value used during the compliance test.

3.1. AES Link between Avaya Communication Manager and Avaya Application Enablement Services Server

The Avaya AES server forwards CTI requests, responses, and events between the Witness Systems Compliance Package Call Recording Server and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over an “AES” link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Compliance Package. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI links. See Section 4 for the details of configuring the AES side of the AES and CTI links.

Enter the **display system-parameters customer-options** command. On Page 3 of the “system-parameters customer-options” form, verify that the **ASAI Link Core Capabilities** field is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.

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	Backup Cluster Automatic Takeover? n
A/D Grp/Sys List Dialing Start at 01? n	CAS Branch? n
Answer Supervision by Call Classifier? n	CAS Main? n
ARS? y	Change COR by FAC? n
ARS/AAR Partitioning? y	Computer Telephony Adjunct Links? n
ARS/AAR Dialing without FAC? y	Cvg Of Calls Redirected Off-net? n
ASAI Link Core Capabilities? y	DCS (Basic)? n
ASAI Link Plus Capabilities? y	DCS Call Coverage? n
Async. Transfer Mode (ATM) PNC? n	DCS with Rerouting? n
Async. Transfer Mode (ATM) Trunking? n	
ATM WAN Spare Processor? n	Digital Loss Plan Modification? n
ATMS? n	DS1 MSP? y
Attendant Vectoring? n	DS1 Echo Cancellation? N

Enter the **add cti-link m** command, where **m** is a number between 1 and 16, inclusive. Enter a valid Extension under the provisioned dial plan in Avaya Communication Manager, set the **Type** field to **ADJ-IP**, and assign a descriptive **Name** to the CTI link.

add cti-link 5		Page 1 of 2
CTI LINK		
CTI Link: 5		
Extension: 20007		
Type: ADJ-IP		
		COR: 1
Name: AES-devcon223-tsapi-jtapi		

Enter the **change node-names ip** command. Note the node names and IP addresses of the C-LAN boards. In the compliance-tested configuration, one C-LAN board (**CLAN**) was dedicated for H.323 endpoint (Avaya IP Telephones and IP Softphones, and AES Device and Media Control API stations) registration, and the other C-LAN board (**CLAN-AES**) was enabled with Application Enablement Services to serve the AES link.

change node-names ip		Page 1 of 1
Name	IP Address	
CDR_buffer	192.45 .80 .250	
CLAN	192.45 .80 .87	
CLAN-AES	192.45 .80 .89	
G350	192.45 .82 .2	
MEDPRO	192.45 .80 .88	
MEDPRO2	192.45 .80 .161	
S8300	192.45 .81 .11	
default	0 .0 .0 .0	

Enter the **change ip-services** command. On Page 1 of the IP SERVICES form, configure entries for the C-LAN board that is dedicated for the AES link:

- Service Type – set to **AESVCS**
- Enabled – set to **y**.

- Local Node – **CLAN-AES** [Set to the node name of the C-LAN that serves the AES link]
- Local Port – set to **8765**.

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

On Page 4 of the IP SERVICES form, enter the hostname of the AES server (ssh into the AES server and run “uname -a” to get the hostname) for the AE Services Server field and an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in Section 4.2.

change ip-services				Page 4 of 4	
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	server1	xxxxxxxxxxxxxxxxxx	y	idle	
2:					
3:					
4:					
5:					

3.2. Agent Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the **display system-parameters customer-options** command. On Page 6 of the system-parameters customer-options form, verify that the ACD and Vectoring (Basic) fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.

display system-parameters customer-options

Page 6 of 11

CALL CENTER OPTIONAL FEATURES

Call Center Release: 3.0

ACD? y

Reason Codes? n

BCMS (Basic)? y

Service Level Maximizer? n

BCMS/VuStats Service Level? n

Service Observing (Basic)? y

BSR Local Treatment for IP & ISDN? n

Service Observing (Remote/By FAC)? y

Business Advocate? n

Service Observing (VDNs)? n

Call Work Codes? n

Timed ACW? N

DTMF Feedback Signals For VRU? n

Vectoring (Basic)? y

Dynamic Advocate? n

Vectoring (Prompting)? n

Expert Agent Selection (EAS)? n

Vectoring (G3V4 Enhanced)? n

EAS-PHD? n

Vectoring (3.0 Enhanced)? n

Forced ACD Calls? n

Vectoring (ANI/II-Digits Routing)? n

Least Occupied Agent? n

Vectoring (G3V4 Advanced Routing)? n

Lookahead Interflow (LAI)? n

Vectoring (CINFO)? n

Multiple Call Handling (On Request)? n

Vectoring (Best Service Routing)? n

Multiple Call Handling (Forced)? n

Vectoring (Holidays)? n

PASTE (Display PBX Data on Phone)? n

Vectoring (Variables)? n

(NOTE: You must logoff & login to effect the permission changes.)

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On Page 1 of the hunt group form, assign a descriptive **Group Name** and **Group Extension** valid in the provisioned dial plan and set the ACD, Queue, and Vector fields to **y**. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.

add hunt-group 1		Page 1 of 3	
HUNT GROUP			
Group Number: 1		ACD? y	
Group Name: Test Pool		Queue? y	
Group Extension: 50000		Vector? y	
Group Type: ucd-mia			
TN: 1			
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display:			
Queue Limit: unlimited			
Calls Warning Threshold:	Port:		
Time Warning Threshold:	Port:		

On Page 2, set the Skill field to **y**, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

add hunt-group 1		Page 2 of 3	
HUNT GROUP			
Skill? y			
AAS? n			
Measured: internal			
Supervisor Extension: 50001			
Controlling Adjunct: none			
VuStats Objective:			
Redirect on No Answer (rings): 3			
Redirect to VDN:			
Forced Entry of Stroke Counts or Call Work Codes? n			

Enter the **add agent-loginID p** command, where **p** is an extension valid in the provisioned dial plan. On Page 1 of the agent-loginID form, enter a descriptive **Name** and **Password**.

```

add agent-loginID 50050                                     Page 1 of 2

                                AGENT LOGINID

Login ID: 50050
Name: Agent-50050
TN: 1
COR: 1
Coverage Path:
Security Code:

AAS? n
AUDIX? n
LWC Reception: spe
LWC Log External Calls? n
AUDIX Name for Messaging:

LoginID for ISDN Display? n
Password: 1234
Password (enter again): 1234
Auto Answer: station
MIA Across Skills: system
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system

WARNING: Agent must log in again before changes take effect

```

On Page 2, set the Skill Number (SN) to the hunt group number previously created. The Skill Level (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.

```

add agent-loginID 50050                                     Page 2 of 2

                                AGENT LOGINID

Direct Agent Skill:
Call Handling Preference: skill-level
Local Call Preference? n

SN      SL      SN      SL      SN      SL      SN      SL
1: 1    1        16:      31:      46:
2:      17:      32:      47:
3:      18:      33:      48:
4:      19:      34:      49:
5:      20:      35:      50:
6:      21:      36:      51:
7:      22:      37:      52:
8:      23:      38:      53:
9:      24:      39:      54:
10:     25:      40:      55:
11:     26:      41:      56:
12:     27:      42:      57:
13:     28:      43:      58:
14:     29:      44:      59:
15:     30:      45:      60:

```

Enter the **add vector q** command, where **q** is an unused vector number. Enter a descriptive **Name**, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

add vector 1		Page 1 of 3	
CALL VECTOR			
Number: 1	Name: Queue to skill1		
Basic? y	EAS? y	G3V4 Enhanced? n	Meet-me Conf? n Lock? n
Prompting? n	LAI? n	G3V4 Adv Route? n	ANI/II-Digits? n ASAI Routing? y
Variables? n	3.0 Enhanced? n	CINFO? n	BSR? n Holidays? n
01 wait-time	2 secs	hearing ringback	
02 queue-to	skill 1	pri m	
03			
04			
05			
06			
07			
08			
09			
10			
11			
Press 'Esc f 6' for Vector Editing			

Enter the **add vdn r** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive **Name** for the VDN and the **Vector Number** configured in the previous step. In the example below, incoming calls to the extension 50060 will be routed to VDN 50060, which in turn will invoke the actions specified in vector 1.

add vdn 50060		Page 1 of 2	
VECTOR DIRECTORY NUMBER			
Extension: 50060			
Name: VDN-50060			
Vector Number: 1			
Meet-me Conferencing? n			
Allow VDN Override? n			
COR: 1			
TN: 1			
Measured: internal			
1st Skill:			
2nd Skill:			
3rd Skill:			

Enter the **change feature-access-codes** command. Define the **Auto-In Access Code**, **Login Access Code**, **Logout Access Code**, **Aux Work Access Code**, and **Service Observing Listen Only Access Code**.

```
change feature-access-codes                                     Page 5 of 6

                                FEATURE ACCESS CODE (FAC)

                                Automatic Call Distribution Features

                                After Call Work Access Code: 120
                                Assist Access Code: 121
                                Auto-In Access Code: 122
                                Aux Work Access Code: 123
                                Login Access Code: 124
                                Logout Access Code: 125
                                Manual-in Access Code: 126
                                Service Observing Listen Only Access Code: 127
                                Service Observing Listen/Talk Access Code: 128
                                Add Agent Skill Access Code: 130
                                Remove Agent Skill Access Code: 131
                                Remote Logout of Agent Access Code: 132
```

3.3. Recording Ports

The recording ports in this configuration are AES Device and Media Control API stations that essentially appear as IP softphones to Avaya Communication Manager. Each AES Device and Media Control API station requires an IP_API_A license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for AES Device and Media Control API stations. Enter the **display system-parameters customer-options** command and verify that there are sufficient **IP_API_A** licenses. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options                     Page 10 of 11

                                MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit      Used
IP_API_A   : 200         0
IP_API_B   : 0           0
IP_API_C   : 0           0
IP_Agent   : 50          0
IP_IR_A    : 0           0
IP_Phone   : 12000       3
IP_ROMax   : 12000       0
IP_Soft    : 2           0
IP_eCons   : 0           0
           : 0           0
           : 0           0
           : 0           0
           : 0           0
           : 0           0
           : 0           0

(NOTE: You must logoff & login to effect the permission changes.)
```

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On Page 1 of the **STATION** form, set the Type field to an IP telephone set type, set the **Port** field to **ip**, enter a descriptive **Name**, specify the **Security Code**, and set the **IP Softphone** field to **y**. Repeat this as necessary, with the same **Security Code**, to configure additional AES Device and Media Control API stations.

add station 21001		Page 1 of 4	
STATION			
Extension: 21001	Lock Messages? n	BCC: 0	
Type: 4621	Security Code: 1234	TN: 1	
Port: ip	Coverage Path 1:	COR: 1	
Name: CMAPI-1	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 19	Personalized Ringing Pattern: 1		
	Message Lamp Ext: 21001		
Speakerphone: 2-way	Mute Button Enabled? y		
Display Language: english	Expansion Module? n		
Survivable GK Node Name:	Media Complex Ext:		
Survivable COR: internal	IP SoftPhone? y		
Survivable Trunk Dest? y			
	IP Video Softphone? n		

3.4. Recorded Stations

The stations that were recorded during the compliance testing include analog, digital, IP telephones and Avaya IP Softphones in both Road Warrior mode and Telecommuter mode. The extensions used were in the ranges 22001-22009.

3.5. Codec Configuration

Enter the **change ip-codec-set t** command, where **t** is a number between 1 and 7, inclusive. Compliance Package supports G.711MU and G.729A.

Note that the **Frames Per Pkt** field is set to **6** and the **Packet Size (ms)** field is set to **60**. This is required to work with Compliance Package.

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.711MU	n	6	60
2: G.729A	n	6	60
3:			
4:			
5:			
6:			

3.6. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. The Avaya IP Telephones and IP Softphones, as well as the AES Device and Media Control API stations used by Compliance Package, registered with the C-LAN boards and were thus also assigned to IP network region 1. One consequence of assigning the aforementioned IP telephones, IP Softphones, AES Device and Media Control API stations, and MedPro boards to a common IP network region is that the RTP traffic between them is governed by the same codec set. The second C-LAN board (CLAN-AES), which dedicated for AES server was assigned to the network region 2. The following screen shows only the network region 1.

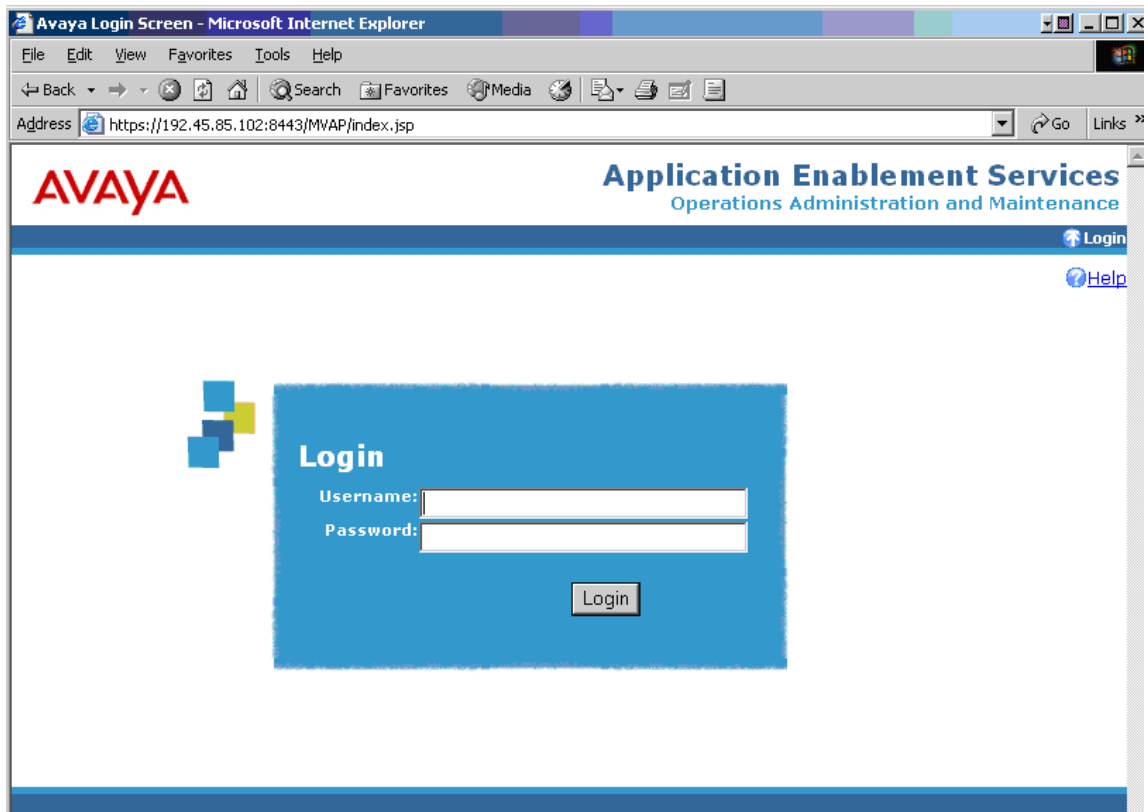
change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location:		Authoritative Domain:
Name:		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: No
Codec Set: 1		Inter-region IP-IP Direct Audio: No
UDP Port Min: 2048		IP Audio Hairpinning? No
UDP Port Max: 3028		
DIFFSERV/TOS PARAMETERS		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		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

4. Configure Avaya Application Enablement Services

This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. Consult [2] for further guidance. The steps in this section describe the configuration of a TSAPI/JTAPI CTI user for the Compliance Package, a “Switch Connection” to Avaya Communication Manager, and a JTAPI CTI link.

4.1. User Management

Enter <https://<IP address of AES server>:8443/MVAP> in the URL, and log in with the appropriate credentials for accessing the AES User Management pages.



Click on **User Management**, then **User Management → Add User** in the left pane. Configure the required fields marked with asterisk, and set the CT User field to **Yes**. Compliance Package will use this **User Id** and **Password** to access the AES server. Scroll down to the bottom of the page and click on **Apply**.

AVAYA Application Enabler Operations Admin

QAM Home

User Management Home You are here: > User Management > List All Users

User Management

- List All Users
- Add User**
- Search Users
- Modify Default User
- Change User Password

Service Management

Help

Edit User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

New Password

Confirm New Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Ciss Home

CT User

Department Number

Display Name

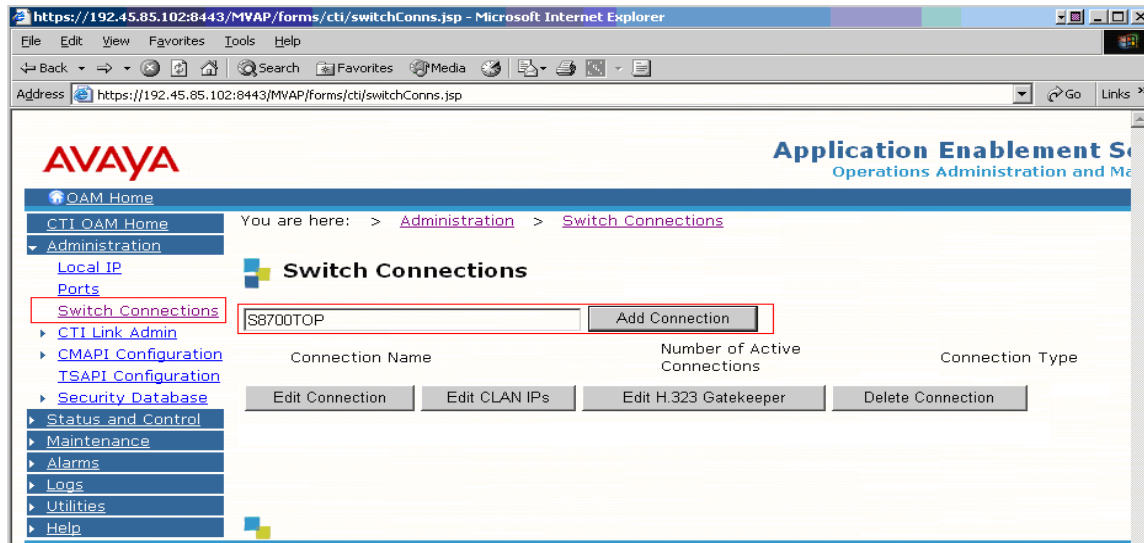
Employee Number

Employee Type

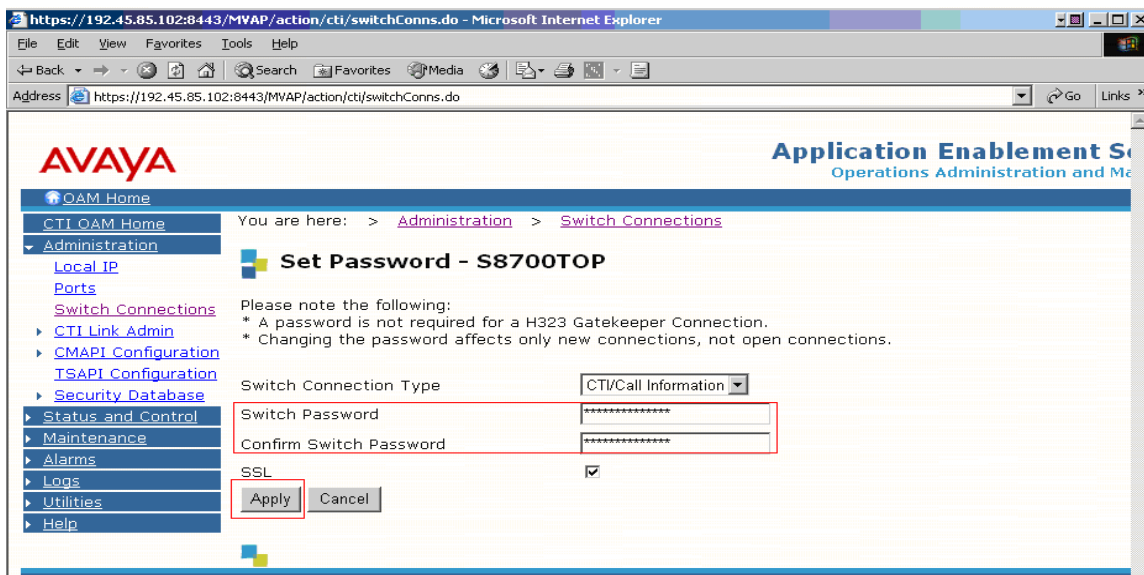
4.2. CTI OAM Admin

Launch a web browser, enter <https://<IP address of AES server>:8443/MVAP> in the URL, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

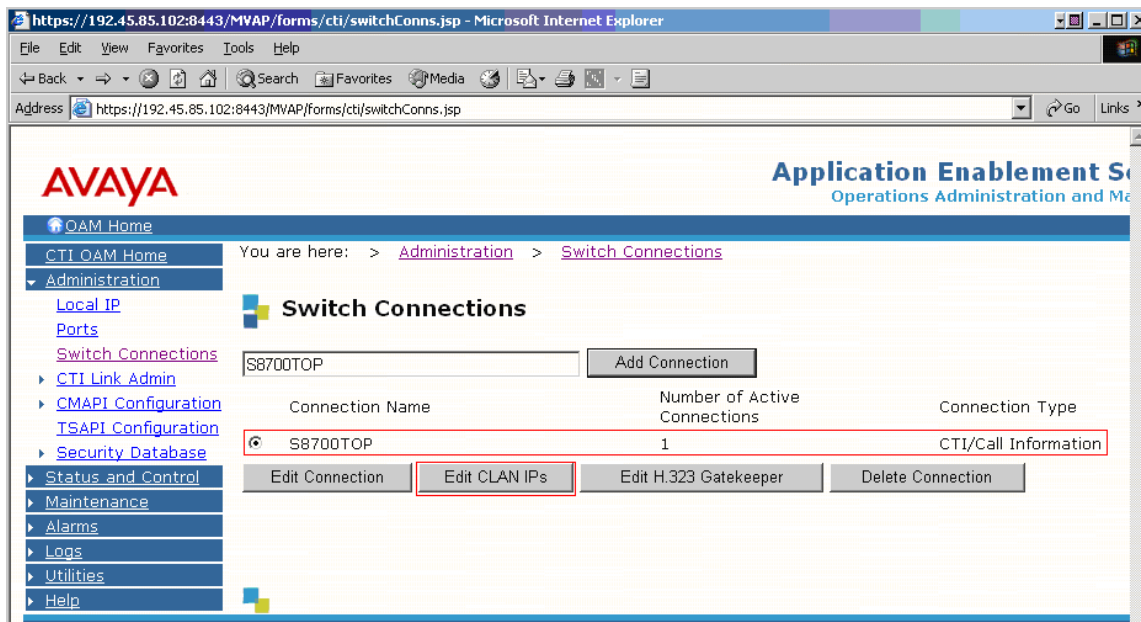
Click on **CTI OAM Home** → **Administration** → **Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the AES server and Avaya Communication Manager. Enter a descriptive name for the Switch Connection and click on **Add Connection**.



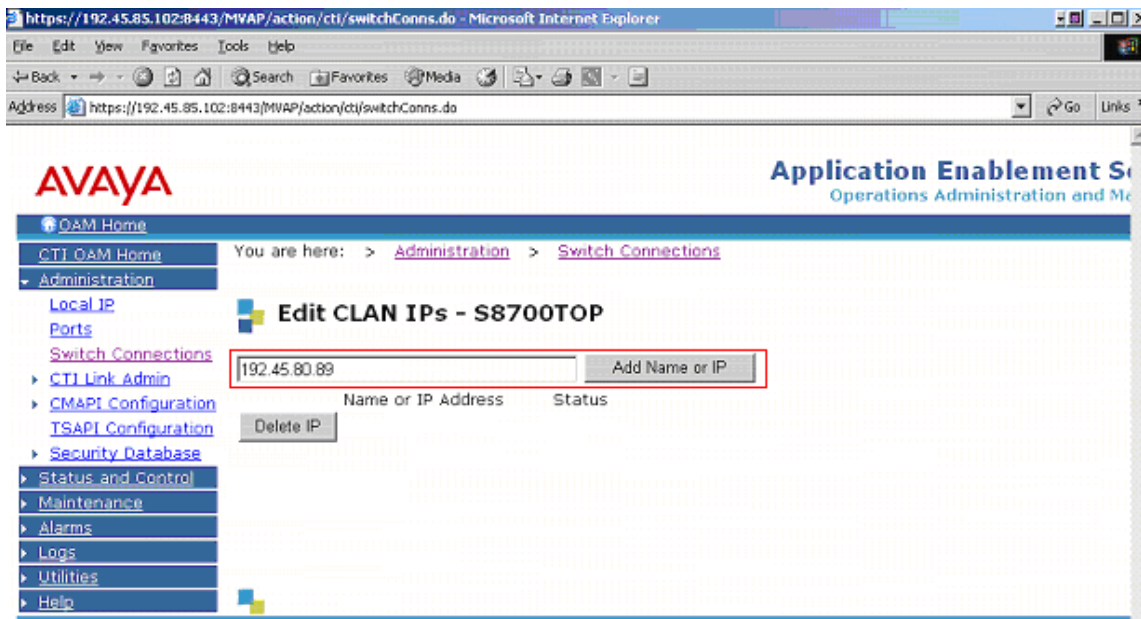
The next window that appears prompts for the Switch Connection password. Enter the same password that was administered on Avaya Communication Manager in Section 3.1. Click on **Apply**.



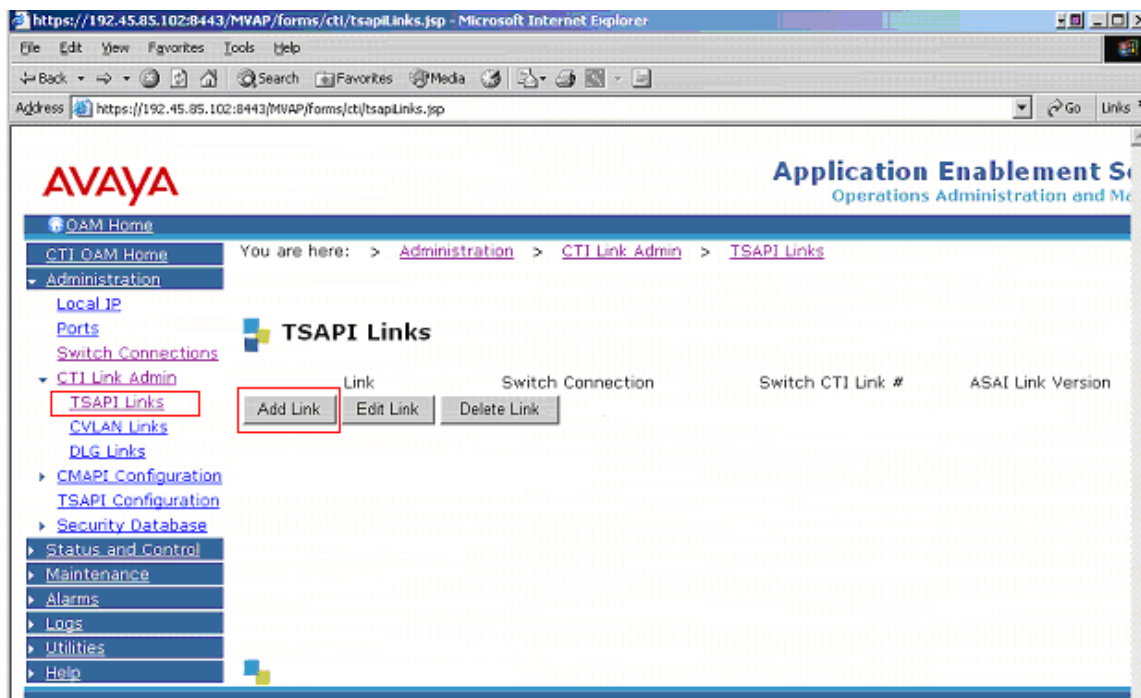
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.



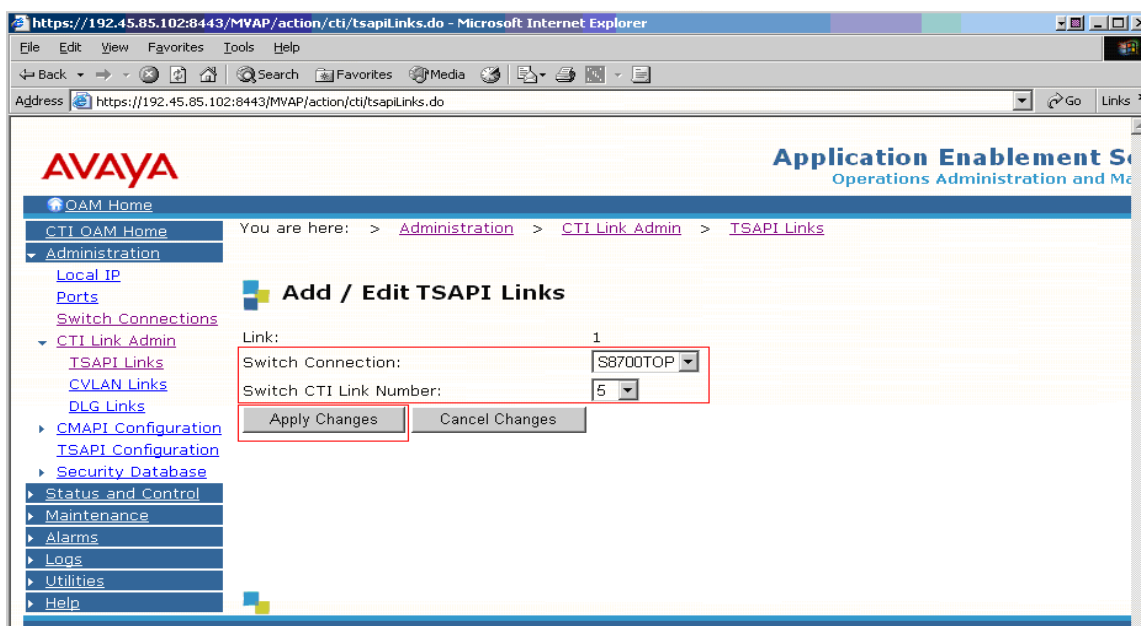
Enter the IP address of a C-LAN board enabled with Application Enablement Services (see Section 3.1) and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



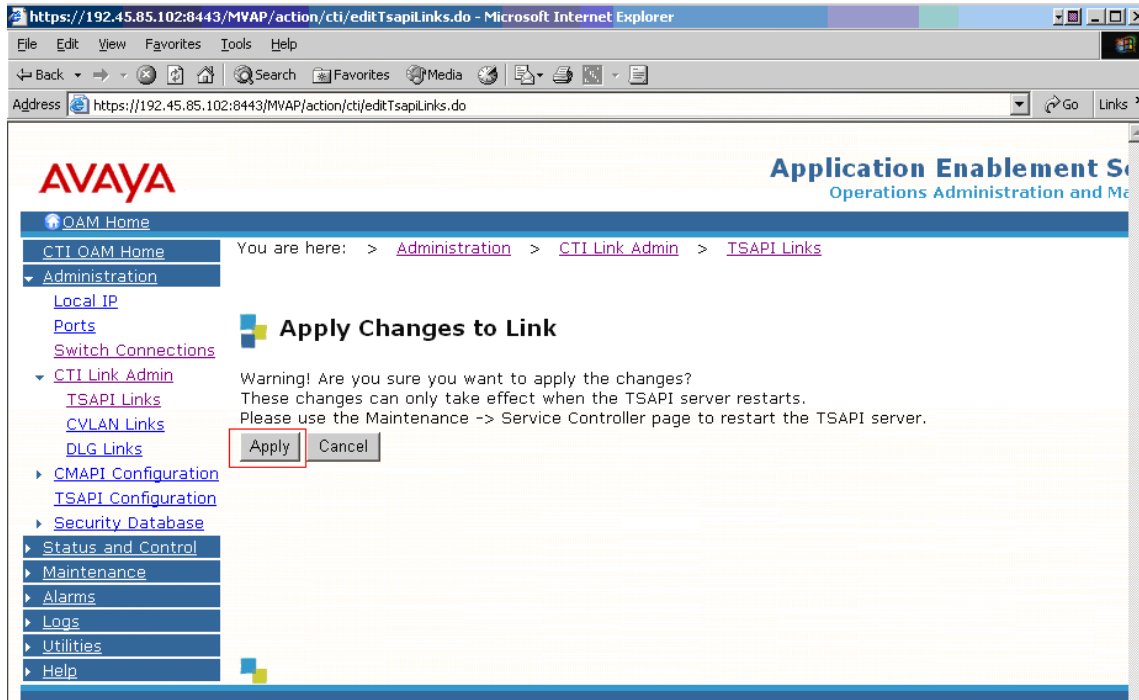
Under **Administration** in the left pane, click on **CTI Link Admin** → **TSAPI Links**. Click on **Add Link**.



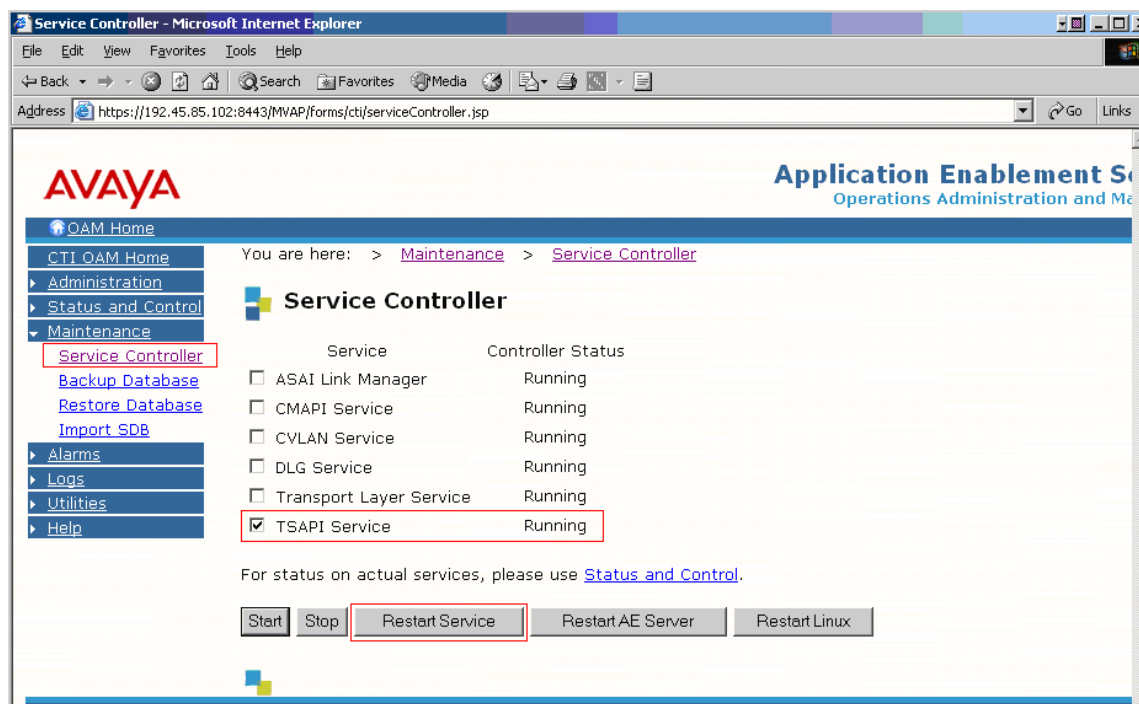
Set **Switch Connection** to the switch connection added previously and **Switch CTI Link Number** to the CTI link number configured on Avaya Communication Manager in Section 3.1. The **TSAPI Link** field is locally significant to this AES server only and may be set to any unused value. Click on **Apply Changes**.



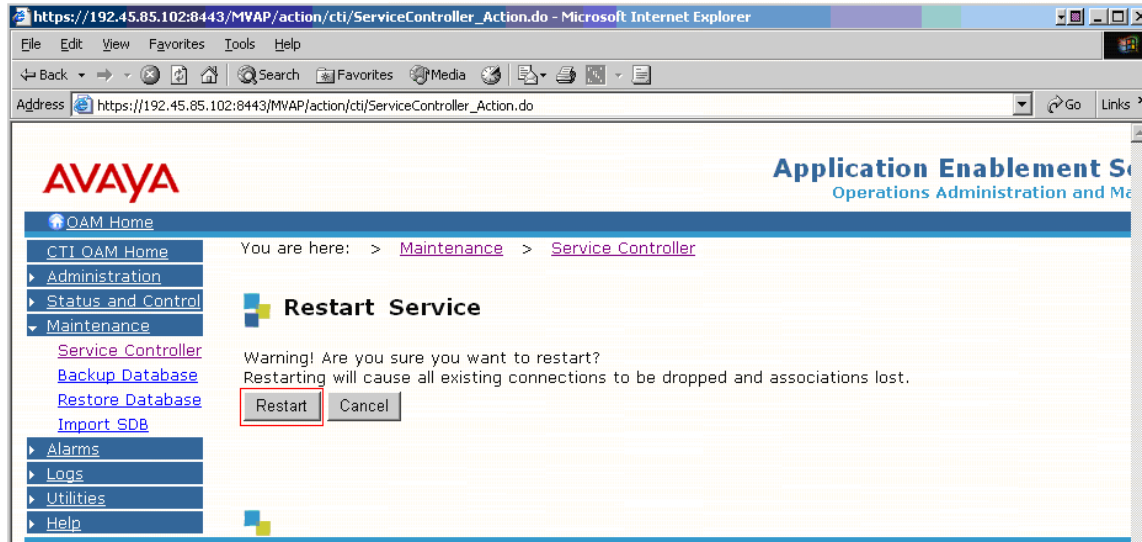
Click on **Apply** to confirm the changes.



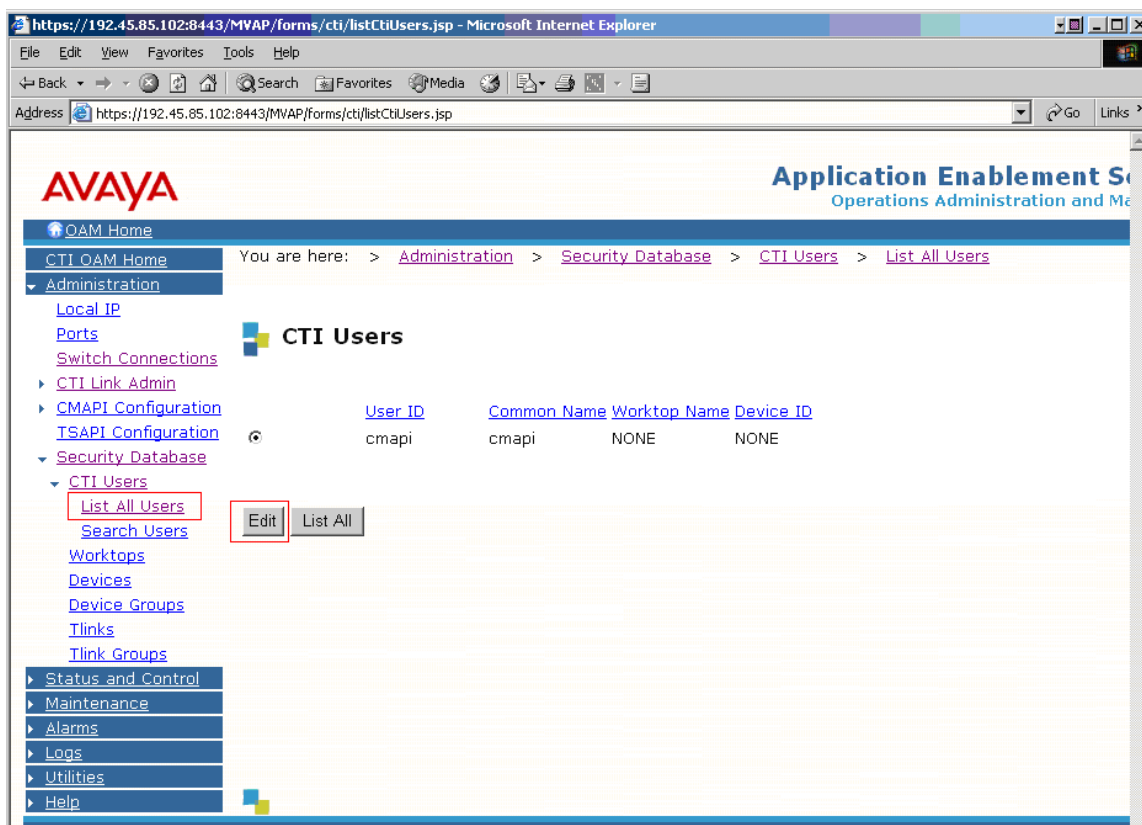
Under **Maintenance** in the left pane, click on **Service Controller**. Check the **TSAPI Service** checkbox and click on **Restart Service**.



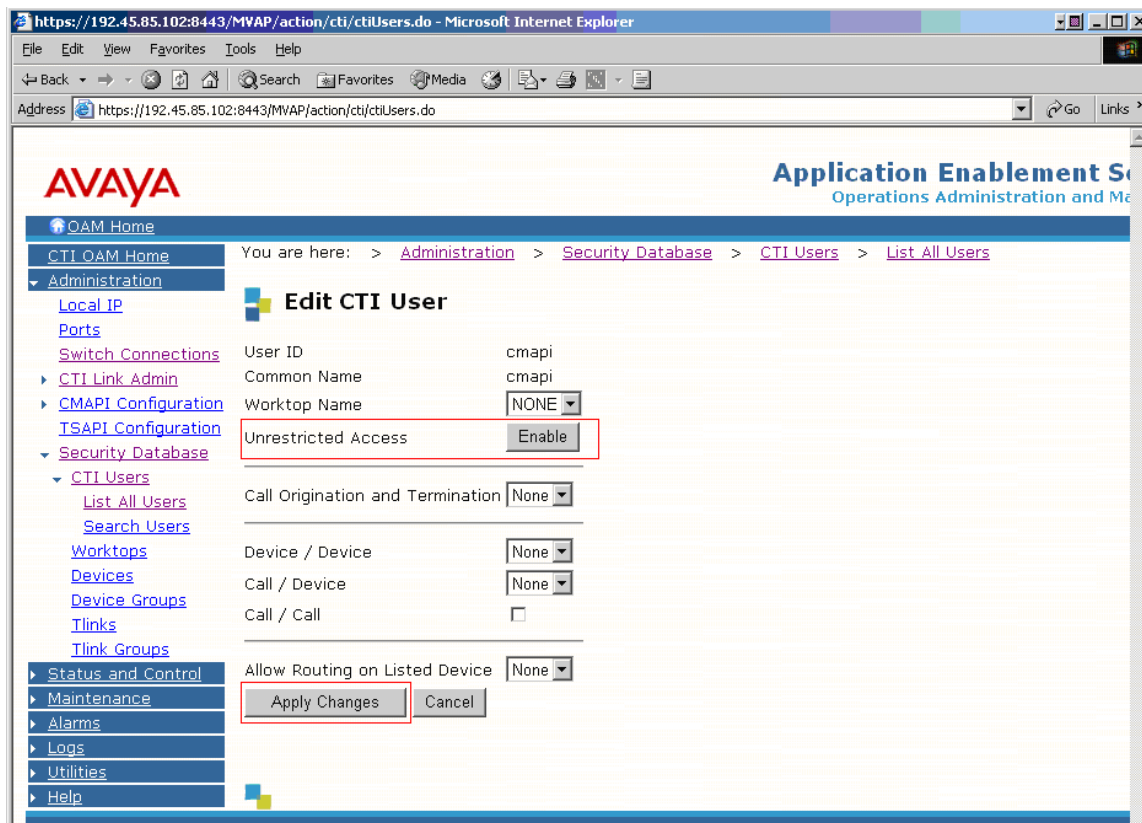
Click on **Restart** to confirm the restart.



Under **Administration** in the left pane, click on **Security Database** → **CTI Users** → **List All Users**. Select the **User ID** created in Section 4.1, and click on **Edit**.



Assign access rights and call/device privileges according to customer requirements. **Unrestricted Access** for the CTI user was enabled during compliance testing. Click on **Apply Changes**.

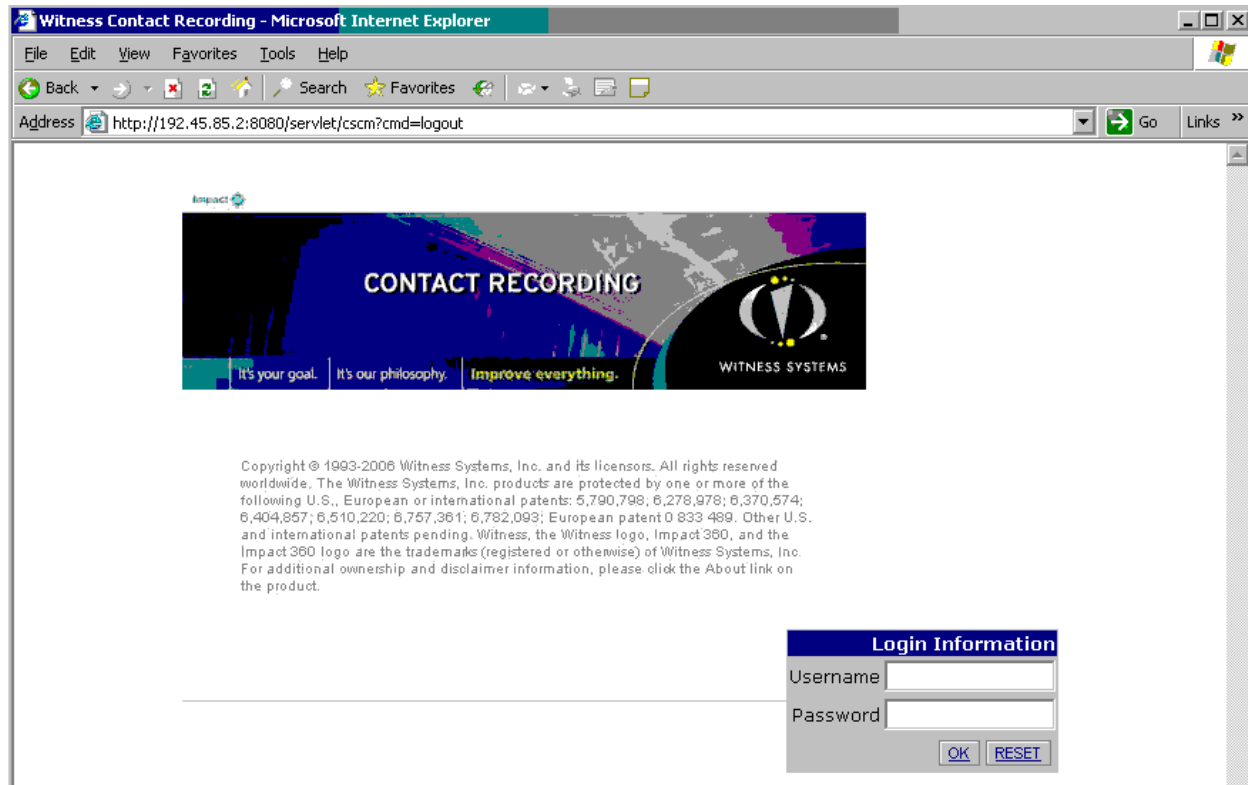


5. Configure Witness Systems Compliance Package

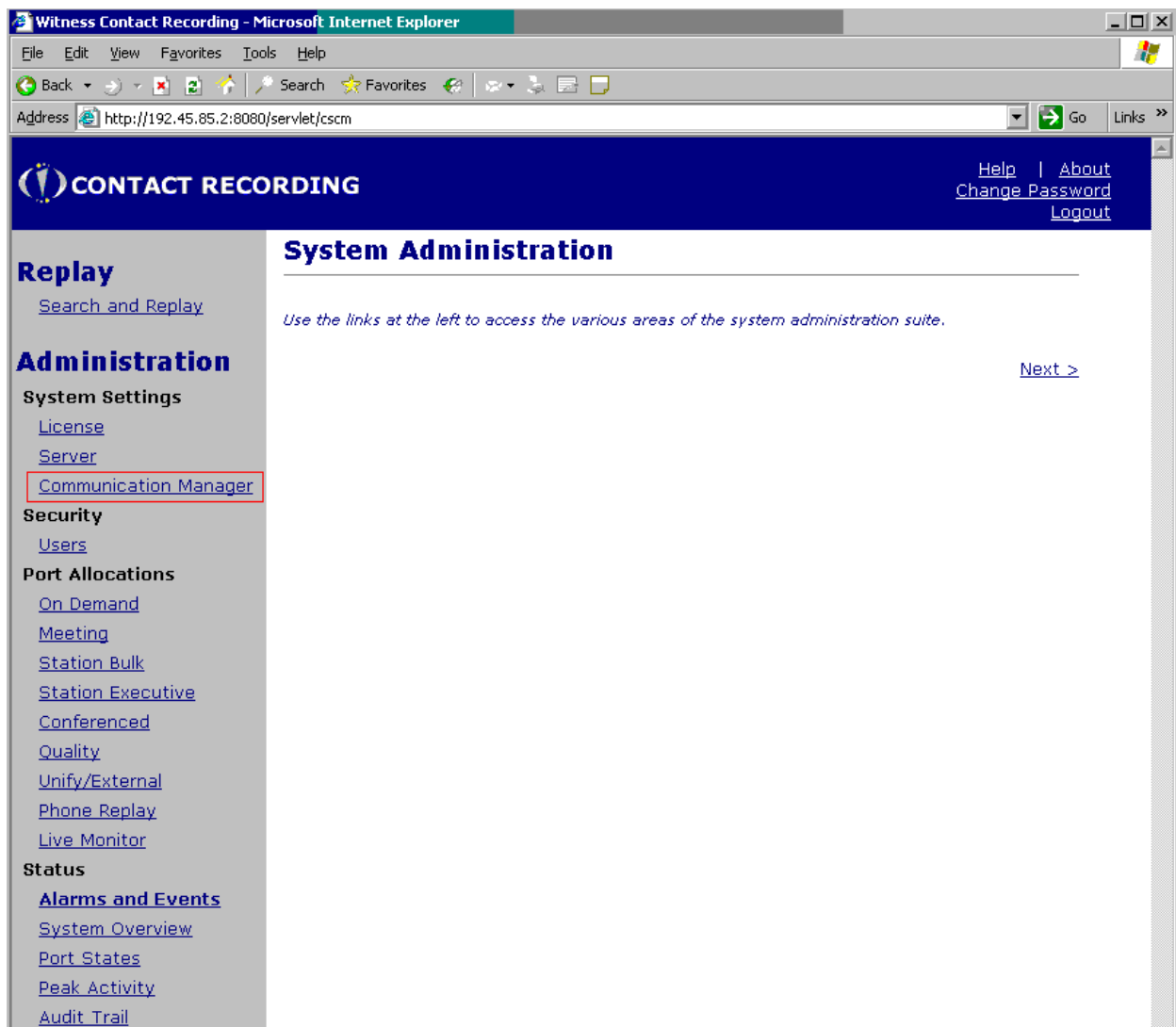
The steps in this section describe the configuration of CTI settings, stations/agents to be recorded full time, and recording stations on the Witness Systems Compliance Package. Consult Compliance Package documentation for instruction on installation. During the compliance test, the following recording modes were verified:

- On Demand
- Meeting
- Station Bulk
- Station Executive
- Conference
- Phone Replay
- Live Monitor

Enter http://<IP address of Compliance Package:8080> in the URL, and log in with the appropriate credentials for accessing the System Administration page.



From the left pane on the System Administration page, shown next screen, click on **Communication Manager** to configure Compliance Package to communicate with Avaya Communication Manager.



From the Communication Manager Settings page, configure the following:

- Default Avaya Communication Manager Name – **192.45.80.87** [CLAN IP Address]
- AE Server Address(es) – **192.45.85.102** [The IP address of the Avaya Application Enablement Services Server on which Avaya Communication Manager API is running]
- CMAPI Username – The user name that the recorder should use to log in to the Communication Manager API.
- CMAPI Password – The password that the recorder should use to log in to the Communication Manager API.
- IP Station Security Code – All stations that register with Avaya Communication Manager must provide a security code. The code you enter must match the code entered for all the stations created earlier on Communication Manager for the recorder to use. This field entry is masked for security purposes.

To configure each field, click on **Edit**.

Witness Contact Recording - Microsoft Internet Explorer

Address: <http://192.45.85.2:8080/servlet/cscm?cmd=cm>

CONTACT RECORDING [Help](#) | [About](#)
[Change Password](#)
[Logout](#)

Replay
[Search and Replay](#)

Administration
System Settings
[License](#)
[Server](#)
[Communication Manager](#)

Security
[Users](#)

Port Allocations
[On Demand](#)
[Meeting](#)
[Station Bulk](#)
[Station Executive](#)
[Conferenced](#)
[Quality](#)
[Unify/External](#)
[Phone Replay](#)
[Live Monitor](#)

Status
[Alarms and Events](#)
[System Overview](#)
[Port States](#)
[Peak Activity](#)
[Audit Trail](#)

Communication Manager Settings

These settings determine how the recorder contacts and interacts with your Avaya Communication Manager

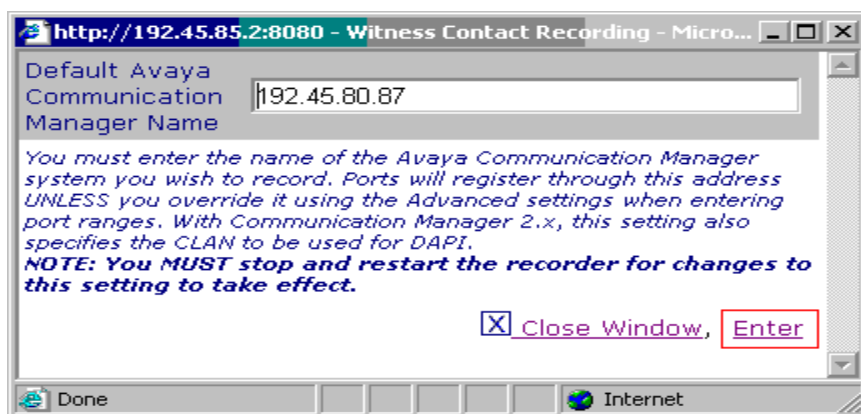
Item	Setting	
Default Avaya Communication Manager Name	192.45.80.87	Edit
AE Server Address(es)	192.45.85.102	Edit
CMAPI Username	chung	Edit
CMAPI Password	*****	Edit
IP Station Security Code	*****	Edit
Extensions assigned to recorder	120	
Unassigned Capacity	228	

The table below lists the range(s) of station numbers that the recorder will register its ports as. These must match the station numbers you have configured as softphones on your Avaya Communication Manager.

Select	Port(s)	No.	Detail
<input type="checkbox"/>	21001-21120	120	Edit

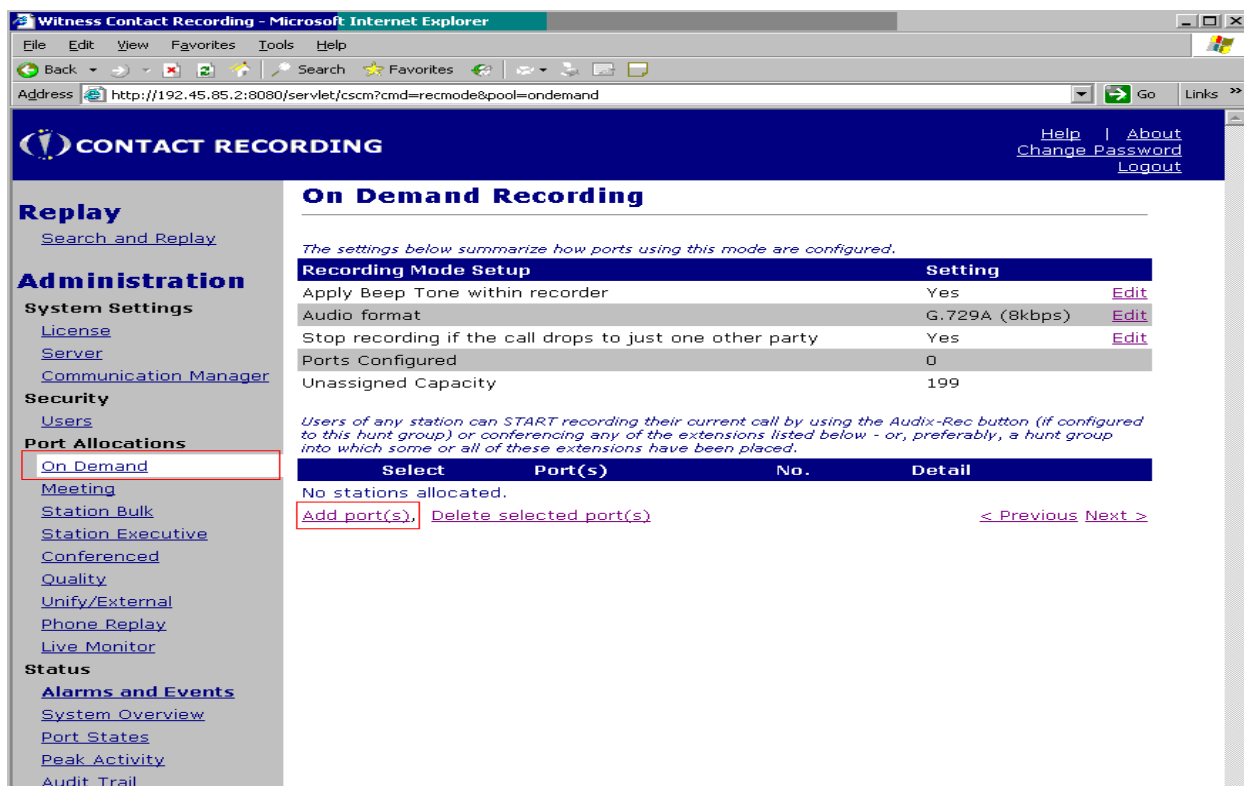
[Add port\(s\)](#), [Delete selected port\(s\)](#) [< Previous](#) [Next >](#)

The following screen shows the Edit window of the Default Avaya Communication Manager Name field. Click on **Enter** after the edit is completed. Repeat this step to configure the remaining fields.



5.1. Configure On Demand

On Demand Recording lets an authorized phone user on the system, conferences in a recording port (station) when the user wants to start recording a call. One or more "pools" of ports on the recorder can be assigned to this recording mode. The recorder automatically answers the incoming call on its port and starts recording. To access On Demand Recording, click on **On Demand** from the left pane. The following screen shows the On Demand Recording page. Allocate recording port(s) by clicking on **Add port(s)**.



Add a port (station) to record, and click on **Enter**.

Lowest Port Number

Highest Port Number (if more than 1)

Comment (optional e.g. hunt group number)

[Advanced](#)

☒ Close Window, Enter

The following screen shows the On Demand Recording page after the recording port is configured.

CONTACT RECORDING [Help](#) | [About](#) | [Change Password](#) | [Logout](#)

Replay
[Search and Replay](#)

Administration
System Settings
[License](#)
[Server](#)
[Communication Manager](#)
Security
[Users](#)
Port Allocations
[On Demand](#)
[Meeting](#)
[Station Bulk](#)
[Station Executive](#)
[Conferenced](#)
[Quality](#)
[Unify/External](#)
[Phone Replay](#)
[Live Monitor](#)
Status
[Alarms and Events](#)
[System Overview](#)
[Port States](#)
[Peak Activity](#)
[Audit Trail](#)

On Demand Recording

The settings below summarize how ports using this mode are configured.

Recording Mode Setup	Setting	
Apply Beep Tone within recorder	Yes	Edit
Audio format	G.729A (8kbps)	Edit
Stop recording if the call drops to just one other party	Yes	Edit
Ports Configured	1	
Unassigned Capacity	198	

Users of any station can START recording their current call by using the Audix-Rec button (if configured to this hunt group) or conferencing any of the extensions listed below - or, preferably, a hunt group into which some or all of these extensions have been placed.

Select	Port(s)	No.	Detail
<input type="checkbox"/>	21005	1	Edit

[Add port\(s\)](#), [Delete selected port\(s\)](#) [< Previous](#) [Next >](#)

5.2. Configure Meeting

Meeting Recording is normally utilized as a detailed log of a meeting, either as an audio recorder for those attending, or as a way to include non-attendees later. One or more "pools" of ports on the recorder can be assigned to this recording mode. To access Meeting Recording, click on **Meeting** from the left pane. The following screen shows the Meeting Recording page. Allocate recording port(s) by clicking on **Add Port(s)**.

The screenshot shows the 'Witness Contact Recording' web application in Microsoft Internet Explorer. The address bar displays 'http://192.45.85.2:8080/servlet/cscm?cmd=recmode&pool=meeting'. The page has a dark blue header with the 'CONTACT RECORDING' logo and navigation links: 'Help', 'About', 'Change Password', and 'Logout'. A left sidebar contains a 'Replay' section with a 'Search and Replay' link, and an 'Administration' section with links for 'System Settings' (License, Server, Communication Manager), 'Security' (Users), 'Port Allocations' (On Demand, Meeting, Station Bulk, Station Executive, Conferenced, Quality, Unify/External, Phone Replay, Live Monitor), and 'Status' (Alarms and Events, System Overview, Port States, Peak Activity, Audit Trail). The 'Meeting' link under 'Port Allocations' is highlighted with a red box. The main content area is titled 'Meeting Recording' and includes a summary of settings for the 'Recording Mode Setup'. Below this is a table with columns 'Select', 'Port(s)', 'No.', and 'Detail'. The table currently shows 'No stations allocated.' and has links for 'Add port(s)' (highlighted with a red box), 'Delete selected port(s)', '< Previous', and 'Next >'. The 'Add port(s)' link is also highlighted with a red box.

Recording Mode Setup		Setting
Apply Beep Tone within recorder	Yes	Edit
Stop recording if the call drops to just one other party	Yes	Edit
Ports Configured	0	
Unassigned Capacity	198	

Select	Port(s)	No.	Detail
No stations allocated.			
Add port(s) Delete selected port(s) < Previous Next >			

Add a port (station) to record, and click on **Enter and Close**.

The screenshot shows the 'Add port (station)' form in the 'Witness Contact Recording' application. The form has three input fields: 'Lowest Port Number' with the value '21004' (highlighted with a red box), 'Highest Port Number (if more than 1)', and 'Comment (optional e.g. hunt group number)'. Below the input fields is an 'Advanced' link. At the bottom of the form, there are three radio buttons: 'Close Window' (checked), 'Enter and Stay Open', and 'Enter and Close' (highlighted with a red box).

Lowest Port Number: 21004
Highest Port Number (if more than 1):
Comment (optional e.g. hunt group number):
[Advanced](#)
☒ Close Window, ☐ Enter and Stay Open, ☐ Enter and Close

The following screen shows the Meeting Recording page after the recording port is configured.

CONTACT RECORDING

[Help](#) | [About](#)
[Change Password](#)
[Logout](#)

Replay
[Search and Replay](#)

Administration
System Settings
[License](#)
[Server](#)
[Communication Manager](#)
Security
[Users](#)
Port Allocations
[On Demand](#)
[Meeting](#)
[Station Bulk](#)
[Station Executive](#)
[Conferenced](#)
[Quality](#)
[Unify/External](#)
[Phone Replay](#)
[Live Monitor](#)
Status
[Alarms and Events](#)
[System Overview](#)
[Port States](#)
[Peak Activity](#)
[Audit Trail](#)

Meeting Recording

The settings below summarize how ports using this mode are configured.

Recording Mode Setup		Setting
Apply Beep Tone within recorder	Yes	Edit
Stop recording if the call drops to just one other party	Yes	Edit
Ports Configured	1	
Unassigned Capacity	197	

Users of any station with speakerphone capability can record a meeting by calling any of the extensions listed below - or, preferably, a hunt group into which some or all of these extensions have been placed.

Select	Port(s)	No.	Detail
<input type="checkbox"/>	21004	1	Prompt users in English Edit

[Add port\(s\),](#) [Delete selected port\(s\)](#) [< Previous](#) [Next >](#)

5.3. Configure Station Bulk

This recording mode can be used to record all calls occurring at specific stations. This mode uses the switch's service observe feature and therefore requires a dedicated port per station that is recorded. To access Station Bulk Recording, click on **Station Bulk** from the left pane. The following screen shows the Station Bulk Recording page. Allocate station(s) by clicking on **Add station range**.

The screenshot shows the 'Witness Contact Recording' web application in Microsoft Internet Explorer. The browser's address bar displays the URL: `http://192.45.85.2:8080/servlet/cscm?pool=stnbulk&cmd=recmode&editmode=delete&token=0.24166153514232758&page=&col=&dir=&r`. The page has a dark blue header with the 'CONTACT RECORDING' logo and navigation links: [Help](#), [About](#), [Change Password](#), and [Logout](#).

The left sidebar contains a navigation menu with the following sections:

- Replay**
 - [Search and Replay](#)
- Administration**
 - System Settings**
 - [License](#)
 - [Server](#)
 - [Communication Manager](#)
 - Security**
 - [Users](#)
 - Port Allocations**
 - [On Demand](#)
 - [Meeting](#)
 - [Station Bulk](#)**
 - [Station Executive](#)
 - [Conferenced](#)
 - [Quality](#)
 - [Unify/External](#)
 - [Phone Replay](#)
 - [Live Monitor](#)
 - Status**
 - [Alarms and Events](#)
 - [System Overview](#)
 - [Port States](#)
 - [Peak Activity](#)
 - [Audit Trail](#)

The main content area is titled 'Station Bulk Recording'. It includes a sub-header: 'The settings below summarize how ports using this mode are configured.' Below this is a table with two columns: 'Recording Mode Setup' and 'Setting'.

Recording Mode Setup	Setting
Apply Beep Tone within recorder	No Edit
Audio format	G.729A (8kbps) Edit
Delete Recording by entering	123 Edit
Record calls that do NOT have a VDN number?	Yes Edit
Filter calls by VDN and/or Skill Hunt Group?	ALL Calls with a VDN Edit
Ports Configured	0
Unassigned Capacity	198

Below the table, a note states: 'The stations listed below will have their calls recorded automatically in accordance with the VDN/Skill rules set above. **DO NOT ENTER VDN, SKILL HUNT GROUP OR AGENT NUMBERS** only station numbers.'

A table with four columns is shown: 'Select', 'Station(s)', 'No.', and 'Detail'. The table is currently empty, displaying 'No stations allocated.' Below the table, there are two links: [Add station range](#) and [Delete selected station range\(s\)](#). At the bottom right of the table area are links: [< Previous](#) and [Next >](#).

Add recorded station(s), and click on **Enter and Close**.

The screenshot shows the 'Station Bulk' form in the 'Witness Contact Recording' application. The form is titled 'Station Bulk' and contains the following fields:

- Lowest (or only) Station Number to record (NOT VDN, Skill or Agent Number)**: A text input field containing the value '22002'.
- Highest Station Number (if more than 1)**: An empty text input field.
- Comment (optional)**: A large text area for entering a comment.

At the bottom right of the form is a link: [Advanced](#).

Below the form, there are three radio buttons with labels: ☒ [Close Window](#), ☐ [Enter and Stay Open](#), and ☐ [Enter and Close](#). The 'Enter and Close' option is highlighted with a red box.

The following screen shows the Station Bulk Recording page after the recorded station is configured.

Witness Contact Recording - Microsoft Internet Explorer

Address: <http://192.45.85.2:8080/servlet/cscm?pool=stnbulk&cmd=recmode&editmode=delete&token=0.24166153514232758&page=&col=&dir=&>

CONTACT RECORDING [Help](#) | [About](#) [Change Password](#) [Logout](#)

Replay
[Search and Replay](#)

Administration
System Settings
[License](#)
[Server](#)
[Communication Manager](#)
Security
[Users](#)
Port Allocations
[On Demand](#)
[Meeting](#)
[Station Bulk](#)
[Station Executive](#)
[Conferenced](#)
[Quality](#)
[Unify/External](#)
[Phone Replay](#)
[Live Monitor](#)
Status
[Alarms and Events](#)
[System Overview](#)
[Port States](#)
[Peak Activity](#)
[Audit Trail](#)

Station Bulk Recording

The settings below summarize how ports using this mode are configured.

Recording Mode Setup	Setting	
Apply Beep Tone within recorder	No	Edit
Audio format	G.729A (8kbps)	Edit
Delete Recording by entering	123	Edit
Record calls that do NOT have a VDN number?	Yes	Edit
Filter calls by VDN and/or Skill Hunt Group?	ALL Calls with a VDN	Edit
Ports Configured	1	
Unassigned Capacity	197	

*The stations listed below will have their calls recorded automatically in accordance with the VDN/Skill rules set above. **DO NOT ENTER VDN, SKILL HUNT GROUP OR AGENT NUMBERS** only station numbers.*

Select	Station(s)	No.	Detail
<input type="checkbox"/>	22002	1	Edit

[Add station range,](#) [Delete selected station range\(s\)](#) [< Previous](#) [Next >](#)

5.4. Configure Station Executive

This option lets users of specific phones choose which of the calls are recorded. Unless the user chooses to keep the recording, by pressing the “Retain Recording by entering” code, it is deleted as the call ends. This recording mode is particularly useful to users who occasionally need to record a call, and who might only recognize the need to record while the call is in progress. To access Station Executive Recording, click on **Station Executive** from the left pane. The following screen shows the Station Executive Recording page. Allocate station(s) by clicking on **Add station range**.

The screenshot shows a web browser window titled "Witness Contact Recording - Microsoft Internet Explorer". The address bar shows "http://192.45.85.2:8080/servlet/cscm?cmd=recmode&pool=stnexec". The page has a dark blue header with the "CONTACT RECORDING" logo and navigation links: "Help", "About", "Change Password", and "Logout".

The left sidebar contains a "Replay" section with a "Search and Replay" link, and an "Administration" section with links for "System Settings" (License, Server, Communication Manager), "Security" (Users), "Port Allocations" (On Demand, Meeting, Station Bulk, **Station Executive**), "Conferenced", "Quality", "Unify/External", "Phone Replay", and "Live Monitor". Under "Status", there are links for "Alarms and Events", "System Overview", "Port States", "Peak Activity", and "Audit Trail".

The main content area is titled "Station Executive Recording". It includes a note: "The settings below summarize how ports using this mode are configured." Below this is a table:

Recording Mode Setup	Setting	
Apply Beep Tone within recorder	After 'retain' command	Edit
Audio format	G.729A (8kbps)	Edit
Retain Recording by entering	**7	Edit
Ports Configured	0	
Unassigned Capacity	261	

Below the table is another note: "Users of the stations listed below can enter the retain code shown above to have their current call recorded. **DO NOT ENTER VDN, SKILL HUNT GROUP OR AGENT NUMBERS** only station numbers." Below this is a table with columns: "Select", "Station(s)", "No.", and "Detail". The table is currently empty, showing "No stations allocated." Below the table are links: "Add station range", "Delete selected station range(s)", and "< Previous Next >".

Add recorded station(s), and click on **Enter and Close**.

http://192.45.85.2:8080 - Witness Contact Recording - Microsoft Internet Explorer

Lowest (or only) **Station Number to record**
(NOT VDN, Skill or Agent Number)

Highest **Station Number** (if more than 1)

Comment (optional)

[Advanced](#)

☒ [Close Window](#), [Enter and Stay Open](#), [Enter and Close](#)

The following screen shows the Station Executive Recording page after the station is configured.

Witness Contact Recording - Microsoft Internet Explorer

Address: http://192.45.85.2:8080/servlet/cscm?cmd=recmode&pool=stnexec

CONTACT RECORDING [Help](#) | [About](#) [Change Password](#) [Logout](#)

Replay
[Search and Replay](#)

Administration
System Settings
[License](#)
[Server](#)
[Communication Manager](#)
Security
[Users](#)
Port Allocations
[On Demand](#)
[Meeting](#)
[Station Bulk](#)
[Station Executive](#)
[Conferenced](#)
[Quality](#)
[Unify/External](#)
[Phone Replay](#)
[Live Monitor](#)
Status
[Alarms and Events](#)
[System Overview](#)
[Port States](#)
[Peak Activity](#)
[Audit Trail](#)

Station Executive Recording

The settings below summarize how ports using this mode are configured.

Recording Mode Setup	Setting	
Apply Beep Tone within recorder	After 'retain' command	Edit
Audio format	G.729A (8kbps)	Edit
Retain Recording by entering	**7	Edit
Ports Configured	1	
Unassigned Capacity	260	

*Users of the stations listed below can enter the retain code shown above to have their current call recorded. **DO NOT ENTER VDN, SKILL HUNT GROUP OR AGENT NUMBERS** only station numbers.*

Select	Station(s)	No.	Detail
<input type="checkbox"/>	22001	1	Edit

[Add station range](#), [Delete selected station range\(s\)](#) [< Previous](#) [Next >](#)

5.5. Configure Conferenced

Rather than dedicating ports to specific stations, a pool of ports can be used in conjunction with an Avaya CT link to record calls on specific stations, agents, skill groups or VDNs. In this mode, the recorder uses single-step conferencing to connect into the calls to be recorded. To access Conferenced Recording, click on **Conferenced** from the left pane. The following screen shows the Conferenced Recording page. From the Conferenced Recording page, configure the following by clicking on **Edit**:

Maximum Concurrent Recordings (on this recorder)

- Avaya CT Server(s)
- Avaya CT Service Identifier(s)
- Avaya CT Service Login ID
- Avaya CT Service password

After the completion of the Conferenced Recording setup, click on **Add Address(es)**.

The screenshot shows the 'Witness Contact Recording' web application in an Internet Explorer browser. The address bar shows the URL: `http://192.45.85.2:8080/servlet/cscm?pool=conferenced&cmd=recmode&editmode=delete&token=0.5697395727795952&page=&col=&dir`. The page has a blue header with the 'CONTACT RECORDING' logo and navigation links: [Help](#), [About](#), [Change Password](#), and [Logout](#).

The left sidebar contains a 'Replay' section with a [Search and Replay](#) link, and an 'Administration' section with links for [System Settings](#), [License](#), [Server](#), [Communication Manager](#), [Security](#), [Users](#), [Port Allocations](#), [On Demand](#), [Meeting](#), [Station Bulk](#), [Station Executive](#), [Conferenced](#) (highlighted with a red box), [Quality](#), [Unify/External](#), [Phone Replay](#), [Live Monitor](#), [Status](#), [Alarms and Events](#), [System Overview](#), [Port States](#), [Peak Activity](#), and [Audit Trail](#).

The main content area is titled 'Conferenced Recording'. It includes a sub-header 'The settings below summarize how ports using this mode are configured.' and a table with two columns: 'Recording Mode Setup' and 'Setting'. The table lists various configuration items, each with an 'Edit' link. The following items are highlighted with red boxes:

Recording Mode Setup	Setting	Edit
Apply Beep Tone within recorder	Yes	Edit
Audio format	G.729A (8kbps)	Edit
Allow multiple recordings	No	Edit
Record calls that do NOT have a VDN number?	Yes	Edit
Filter calls by VDN and/or Skill Hunt Group?	ALL Calls with a VDN	Edit
Maximum Concurrent Recordings (on this recorder)	0	Edit
Warn when free port count falls BELOW	1	Edit
Agent Skill Group(s) to Observe	Not defined	Edit
VDN(s) to Observe	Not defined	Edit
Avaya CT Server(s)	192.45.85.102	Edit
Avaya CT Service Identifier(s)	AVAYA#S8700TOP#CSTA#SERVER1	Edit
Avaya CT Service Login ID	cmapi	Edit
Avaya CT Service password	*****	Edit
Ports Configured	0	
Unassigned Capacity	197	

Below the table, a note states: 'Calls involving the addresses (stations, agents, skill hunt groups and/or VDNs) below will be recorded via single-step conference (Requires Avaya CT interface)'. This is followed by a table with columns: 'Select', 'Address(es)', 'No.', and 'Detail'. The table currently shows 'No stations allocated.' and includes links for [Add address\(es\)](#) and [Delete selected address\(es\)](#). Navigation links [< Previous](#) and [Next >](#) are also present.

The following screen shows the Edit window of the Maximum Concurrent Recordings (on this recorder) field. Click on **Enter** after the edit is completed. Repeat this step to configure the remaining fields.

Add recording station(s), and click on **Enter**.

The following screen shows the Station Executive Recording page after the station is configured.

Conferenced Recording

The settings below summarize how ports using this mode are configured.

Recording Mode Setup	Setting	
Apply Beep Tone within recorder	Yes	Edit
Audio format	G.729A (8kbps)	Edit
Allow multiple recordings	No	Edit
Record calls that do NOT have a VDN number?	Yes	Edit
Filter calls by VDN and/or Skill Hunt Group?	ALL Calls with a VDN	Edit
Maximum Concurrent Recordings (on this recorder)	3	Edit
Warn when free port count falls BELOW	1	Edit
Agent Skill Group(s) to Observe	Not defined	Edit
VDN(s) to Observe	Not defined	Edit
Avaya CT Server(s)	192.45.85.102	Edit
Avaya CT Service Identifier(s)	AVAYA#S8700TOP#CSTA#SERVER1	Edit
Avaya CT Service Login ID	cmapi	Edit
Avaya CT Service password	*****	Edit
Ports Configured	3	
Unassigned Capacity	194	

Calls involving the addresses (stations, agents, skill hunt groups and/or VDNs) below will be recorded via single-step conference (Requires Avaya CT interface)

Select	Address(es)	No.	Detail
<input type="checkbox"/>	21001-21010	10	Edit

[Add address\(es\),](#) [Delete selected address\(es\)](#) [< Previous](#) [Next >](#)

5.6. Configure Phone Replay

The Phone Replay feature replays recorded messages via the user's telephone, and this does use a port. To access the Phone replay feature, click on **Phone Replay** from the left pane. The following screen shows the Phone Replay Ports page. Allocate station(s) by clicking on **Add port(s)**.

The screenshot shows a web browser window titled "Witness Contact Recording - Microsoft Internet Explorer". The address bar shows "http://192.45.85.2:8080/servlet/cscm?cmd=recmode&pool=replay". The page has a blue header with the "CONTACT RECORDING" logo and navigation links: "Help", "About", "Change Password", and "Logout".

On the left is a sidebar menu with the following sections:

- Replay**
 - [Search and Replay](#)
- Administration**
 - System Settings**
 - [License](#)
 - [Server](#)
 - [Communication Manager](#)
 - Security**
 - [Users](#)
 - Port Allocations**
 - [On Demand](#)
 - [Meeting](#)
 - [Station Bulk](#)
 - [Station Executive](#)
 - [Conferenced](#)
 - [Quality](#)
 - [Unify/External](#)
 - Phone Replay** (highlighted with a red box)
 - [Live Monitor](#)
 - Status**
 - [Alarms and Events](#)
 - [System Overview](#)
 - [Port States](#)
 - [Peak Activity](#)
 - [Audit Trail](#)

The main content area is titled "Phone Replay Ports". It contains the following text:

The settings below summarize how ports using this mode are configured.

Recording Mode Setup	Setting
Ports Configured	0
Unassigned Capacity	10

*The stations listed below will be used to replay recordings to users' phones. These are not needed if you are happy to replay via your PC's soundcard.
Please RESTART the recorder after changing the list of ports below.*

Select	Port(s)	No.	Detail
No stations allocated.			
Add port(s) (highlighted with a red box)	Delete selected port(s)		< Previous Next >

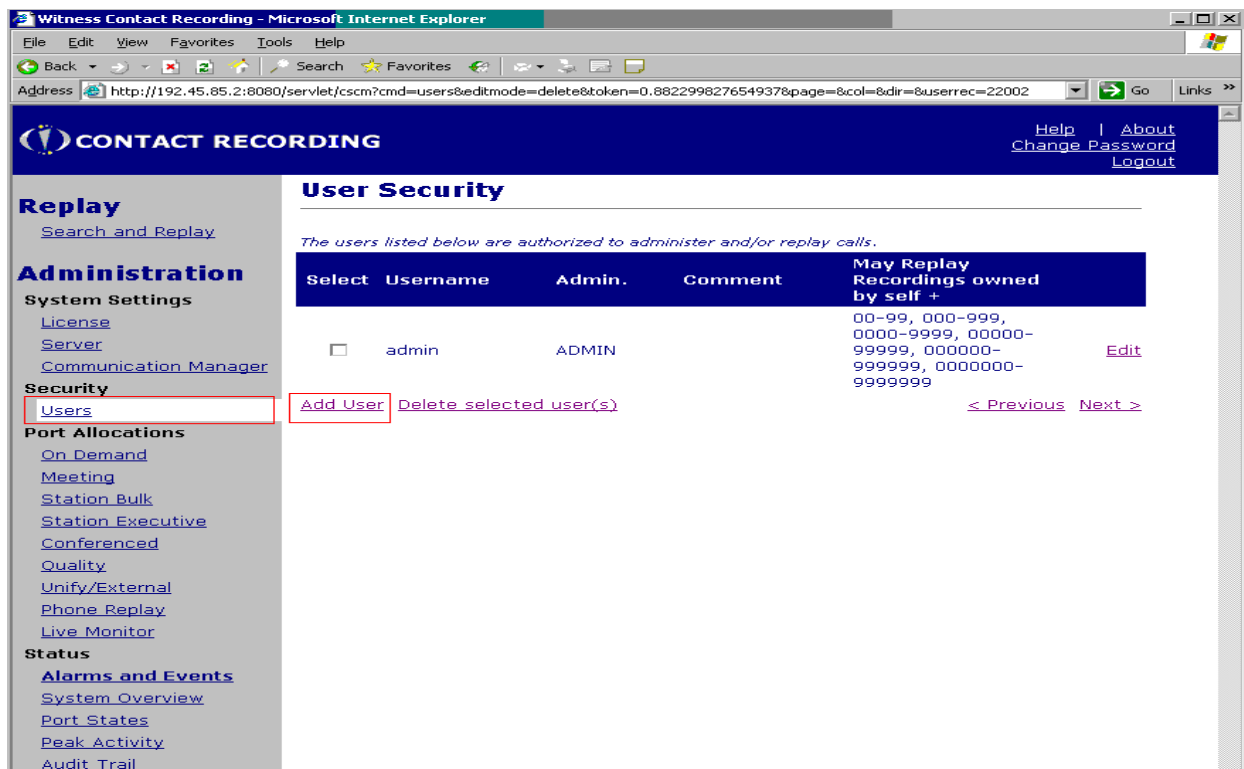
Add recording station(s), and click on **Enter**.

The screenshot shows the "Add port(s)" form. It has the following fields:

- Lowest Port Number: (highlighted with a red box)
- Highest Port Number (if more than 1):
- Comment (optional e.g. hunt group number):

At the bottom right, there is a checkbox labeled "Advanced" and a button labeled "Close Window, Enter" (highlighted with a red box).

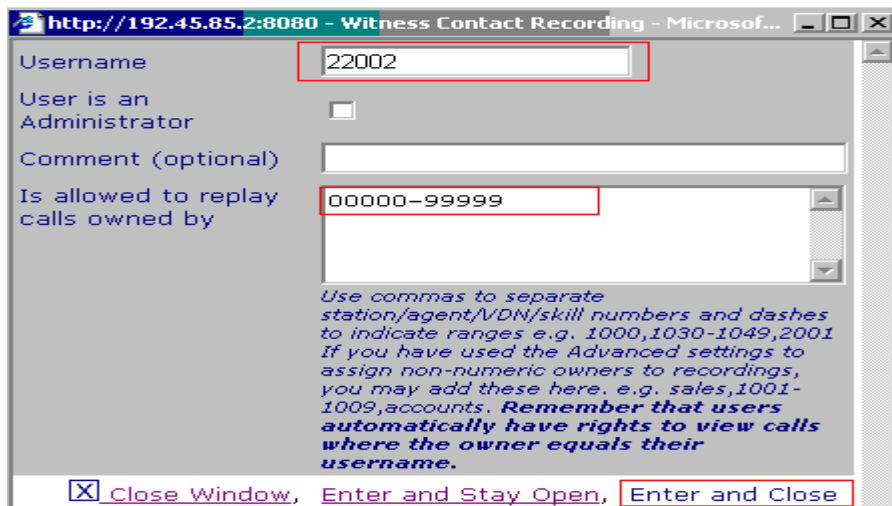
At this point, a user (a station to replay the recorded message) needs to be created. To create a user, click on **Users** from the left pane. The following screen shows the User Security page. Add a user by clicking on **Add User**



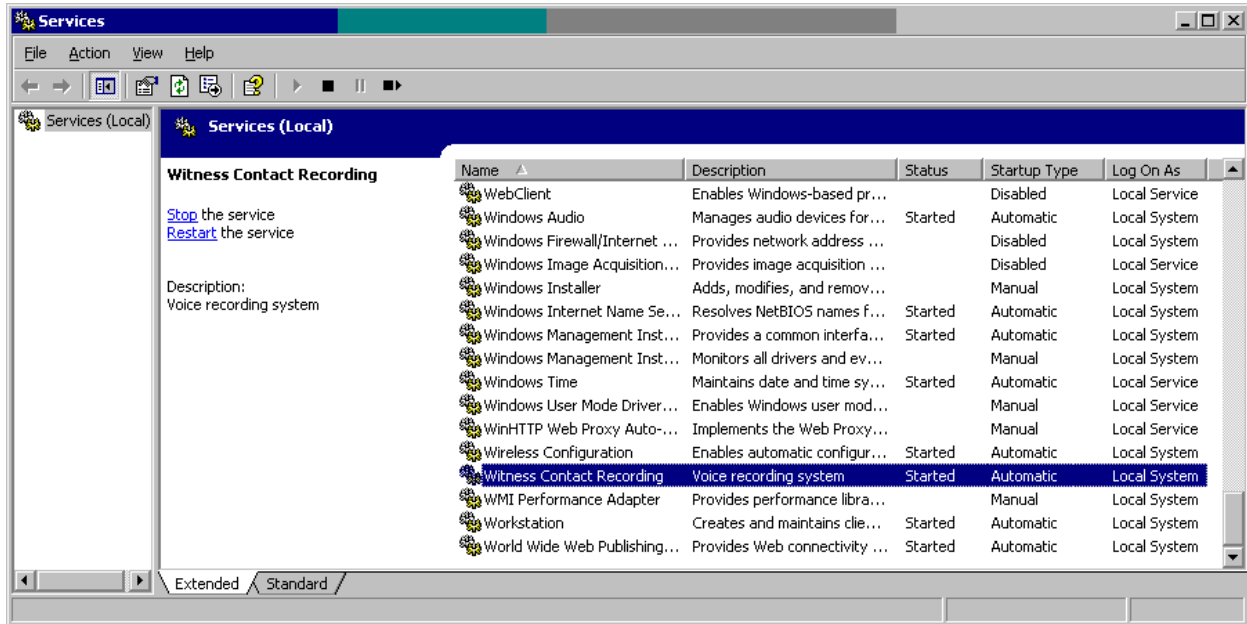
The following screen shows the User configuration window. Configure the following fields:

- Username
- Is allowed to replay calls owned by

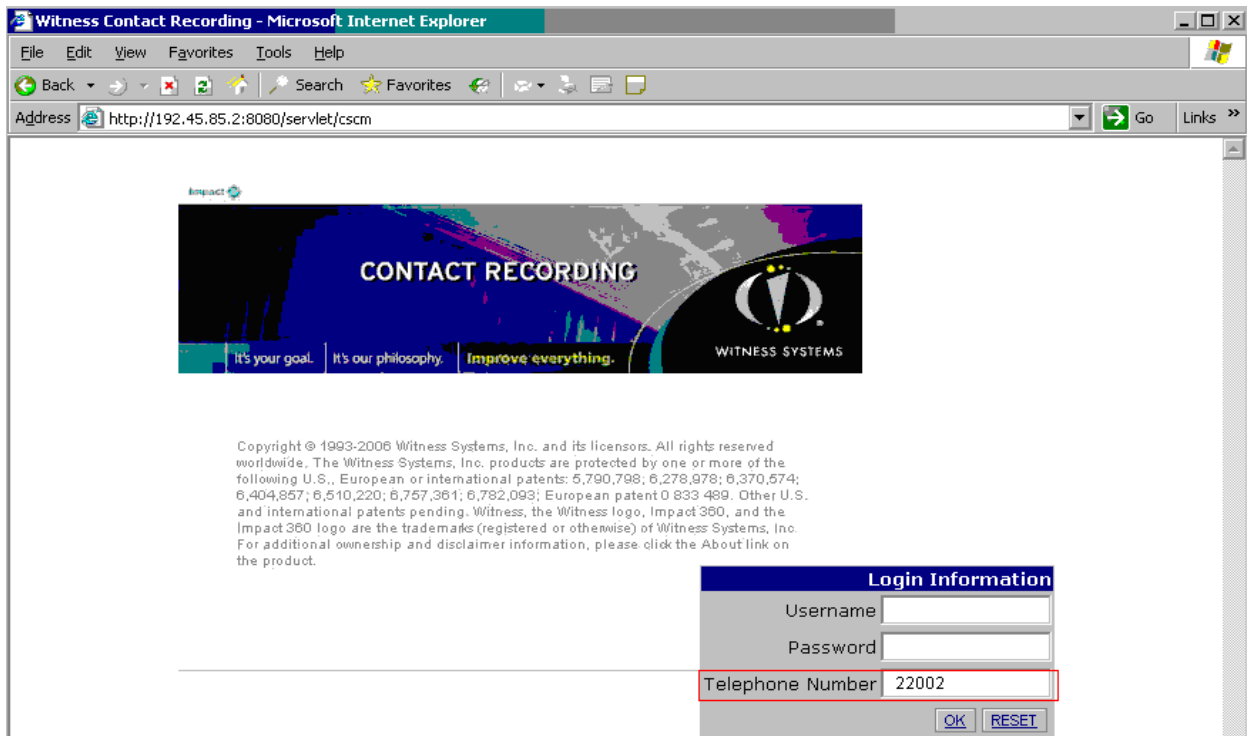
Click on **Enter and Close** after the user creation is completed.



Restart the service of Witness Compliance Package.



After the service is restarted, Enter `https://<IP address of Compliance Package>:8080` in the URL. Note that a new field called Telephone Number appears in the Login Information section. Provide the user (created from the previous step) on the Telephone Number field.



5.7. Configure Live Monitor

Live Monitor provides Users a way to listen in to calls in real-time using their telephone. This method uses one of the replay ports (recording station) within the recording pool. One or more ports on a Witness Contact Recorder can be assigned for Live Monitor use. Supervisors can ring these ports and dial the number of the station (recorded station) they wish to observe. The audio being recorded is relayed to them giving similar functionality to service observe. It is important that the audio format of Live Monitor Ports and recorded station should be matched. To access Live Monitor, click on **Live Monitor** from the left pane. The following screen shows the Live Monitor Ports page. Allocate recording station(s) by clicking on **Add port(s)**.

The screenshot shows a web browser window titled "Witness Contact Recording - Microsoft Internet Explorer". The address bar displays "http://192.45.85.2:8080/servlet/cscm?cmd=recmode&pool=monitor". The page has a blue header with the "CONTACT RECORDING" logo and navigation links: "Help", "About", "Change Password", and "Logout".

The left sidebar contains a "Replay" section with a link to "Search and Replay", and an "Administration" section with links for "System Settings", "License", "Server", "Communication Manager", "Security", "Users", "Port Allocations", "On Demand", "Meeting", "Station Bulk", "Station Executive", "Conferenced", "Quality", "Unify/External", "Phone Replay", and "Live Monitor" (which is highlighted with a red box).

The main content area is titled "Live Monitor Ports". It includes a summary of settings and a table of allocated stations.

The settings below summarize how ports using this mode are configured.

Recording Mode Setup	Setting	
Audio format	G.729A (8kbps)	Edit
Ports Configured	0	
Unassigned Capacity	10	

The stations listed below will be used to monitor phones being recorded using service observe.

Select	Port(s)	No.	Detail
No stations allocated.			
Add port(s) , Delete selected port(s)			

< Previous Next >

Add recording station(s), and click on **Enter**. This station will be utilized by a user (monitor station).

The following screen shows the Live Monitor Ports page after the station is configured. At this point, a user (a station to monitor the recorded station) needs to be created. To create a user, click on **Users** from the left pane.

Recording Mode Setup

Recording Mode Setup	Setting
Audio format	G.729A (8kbps) Edit
Ports Configured	1
Unassigned Capacity	9

The stations listed below will be used to monitor phones being recorded using service observe.

Select	Port(s)	No.	Detail
<input type="checkbox"/>	21006	1	Edit

[Add port\(s\),](#) [Delete selected port\(s\)](#) [< Previous](#) [Next >](#)

The following screen shows the User Security page. Add a user by clicking on **Add User**.

Witness Contact Recording - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address <http://192.45.85.2:8080/servlet/cscm?cmd=users&editmode=delete&token=0.22442972174053555&page=&col=&dir=&userrec=22002> Go Links »

CONTACT RECORDING [Help](#) | [About](#)
[Change Password](#)
[Logout](#)

Replay
[Search and Replay](#)

Administration
System Settings
[License](#)
[Server](#)
[Communication Manager](#)
Security
[Users](#)
Port Allocations
[On Demand](#)
[Meeting](#)
[Station Bulk](#)
[Station Executive](#)
[Conferenced](#)
[Quality](#)
[Unify/External](#)
[Phone Replay](#)
[Live Monitor](#)
Status
[Alarms and Events](#)
[System Overview](#)
[Port States](#)
[Peak Activity](#)
[Audit Trail](#)

User Security

The users listed below are authorized to administer and/or replay calls.

Select	Username▼▲	Admin.▼▲	Comment▼▲	May Replay Recordings owned by self ▼▲
<input type="checkbox"/>	admin	ADMIN		00-99, 000-999, 0000-9999, 00000- 99999, 000000- 999999, 0000000- 9999999

[Add User](#) [Delete selected user\(s\)](#) [< Previous](#) [Next >](#)

The following screen shows the User configuration window. Configure the following fields:

- Username [monitoring station]
- Is allowed to replay calls owned by [a range of recorded stations that can be monitored by a monitoring station]

Click on **Enter and Close** after the user creation is completed.

http://192.45.85.2:8080 - Witness Contact Recording - Microsoft Internet Explorer

Username: 22005

User is an Administrator: ☐

Comment (optional):

Is allowed to replay calls owned by: 00000-99999

Use commas to separate station/agent/VDN/skill numbers and dashes to indicate ranges e.g. 1000,1030-1049,2001
If you have used the Advanced settings to assign non-numeric owners to recordings, you may add these here. e.g. sales,1001-1009,accounts. **Remember that users automatically have rights to view calls where the owner equals their username.**

☒ Close Window, Enter and Stay Open, Enter and Close

6. Interoperability Compliance Testing

Interoperability compliance testing included feature, serviceability and performance. The feature testing evaluated the ability of Compliance Package to record for various types of recording modes. The serviceability testing introduced failure scenarios to see if Compliance Package can resume call recordings after failure recovery. The performance test produced bulk call volumes to generate a substantial amount of call records.

6.1. General Test Approach

The general test approach was to manually place intra-switch calls, inter-switch calls, inbound and outbound PSTN trunk calls to and from telephones controlled by the Avaya Media Servers, and verify that Compliance Package successfully recorded calls. For serviceability testing, logical links were disabled/re-enabled, and media servers were reset. For performance testing, a call generator was used to place calls over an extended period of time.

6.2. Test Results

All executed test cases passed. The Compliance Package successfully recorded calls including intra-switch calls, inbound / outbound PSTN trunk calls, inbound/outbound inter-switch IP trunk calls, transferred calls, and conference calls. For serviceability testing, the Compliance Package

was able to resume recording calls after failure recovery. Performance tests verified that the Compliance Package could record calls during a sustained, high volume of calls.

7. Verification Steps

The following steps may be used to verify the configuration:

- Use the **ping** command to verify IP communication between Compliance Package, Avaya Communication Manager and Avaya AES server. Ping the CLAN IP Address, Avaya AES IP Address from Compliance Package. On the SAT of Avaya Media Server, enter the **status aesvcs cti-link** command and verify that the cti-link state is up.
- In Compliance Package, select **System Overview** from the left pane. Check the following fields:
 - Call Information Link to Communication Manager - **UP**
 - Avaya CT Link - **UP**

The screenshot shows the 'Witness Contact Recording - Microsoft Internet Explorer' window. The address bar displays 'http://localhost:8080/servlet/cscm'. The page has a blue header with the 'CONTACT RECORDING' logo and navigation links: 'Help', 'About', 'Change Password', and 'Logout'. The left sidebar contains a 'Replay' section with a 'Search and Replay' link, an 'Administration' section with links for 'System Settings' (License, Server, Communication Manager), 'Security' (Users), 'Port Allocations' (On Demand, Meeting, Station Bulk, Station Executive, Conferenced, Quality, Unify/External, Phone Replay, Live Monitor), and a 'Status' section with links for 'Alarms and Events', 'System Overview' (highlighted with a red box), 'Port States', 'Peak Activity', and 'Audit Trail'. The main content area is titled 'System Overview' and includes a refresh link. It contains two tables. The first table shows the current state of the server with two rows: 'Call Information Link to Communication Manager' and 'Avaya CT Link to AVAYA#S8700TOP#CSTA#SERVER1', both with a value of 'UP'. The second table shows port usage statistics for various recording modes, including Meeting, Station Bulk, and Conferenced, with a total of 46 (90%) ports active. A 'Refresh' link is located at the bottom right of the port usage table.

Item	Value
Call Information Link to Communication Manager	UP
Avaya CT Link to AVAYA#S8700TOP#CSTA#SERVER1	UP

Mode	Faulty	Starting	Idle	Setup	Connected	Active
Meeting	0	0	1 (100%)	0	0	0
Station Bulk	1 (2%)	0	0	0	46 (98%)	0
Conferenced	3 (100%)	0	0	0	0	0
Total	4 (8%)	0	1 (2%)	0	46 (90%)	0

- Place a call and verify that Compliance Package records the call by selecting **Search and Replay** from the left pane.

Administration
Administer System

Search Filters

Call Start Range
03/14/06 12:00:00 AM
03/14/06 11:59:59 PM

Parties
Agent
Length
Service
Universal Call ID
Call Set
SEARCH

Results
1 2 3 ... 7 Next Show All Select All Sele

Call Start	Len	Agent	Parties	Service	Univ. Call ID
03/14/06 03:16:26 PM	00:08	N/A	22001 (RECORD-1(4621)), 22002 (RECORD-2 (4625))	N/A	N/A
03/14/06 03:20:11 PM	00:02	N/A	22001 (RECORD-1(4621)), 22002 (RECORD-2 (4625))	N/A	100352 1142349556
03/14/06 03:55:05 PM	01:55	N/A	22001 (RECORD-1(4621)), 22002 (RECORD-2 (4625))	N/A	100358 1142351649
03/14/06 03:57:21 PM	00:06	N/A	22001 (RECORD-1(4621)), 22002 (RECORD-2 (4625))	N/A	100359 1142351786
03/14/06 03:59:03 PM	00:25	N/A	22001 (RECORD-1(4621)), 22002 (RECORD-2 (4625))	N/A	100363 1142351888
03/14/06 04:27:02 PM	00:50	N/A	22005 (RECORD-5)	N/A	100373 1142353562
03/14/06 04:28:44 PM	00:23	N/A	22005 (RECORD-5)	N/A	100374 1142353667
03/14/06 04:33:55 PM	00:05	N/A	22005 (RECORD-5)	N/A	100380 1142353970
03/14/06 04:42:50 PM	00:01	N/A	22005 (RECORD-5)	N/A	100382 1142354517
03/14/06 04:42:51 PM	00:14	N/A	22001 (RECORD-1(4621)), 22005 (RECORD-5)	N/A	100381 1142354462

8. Support

Technical support for the Compliance Package can be obtained by contacting Witness Systems' Customer Interaction Center (CIC) via the support link at <http://www.witness.com/support/> or by calling the support telephone number at 1-800-494-8637.

9. Conclusion

These Application Notes describe the procedures for configuring the Witness Systems Compliance Package 7.3 to interoperate with Avaya Communication Manager 3.0.1 and Avaya Application Enablement Services 3.1. Compliance Package 7.3 successfully passed all compliance testing.

10. References

This section references the Avaya and Witness Systems documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Feature Description and Implementation for Avaya Communication Manager*, Issue 4, February 2006, Document Number 555-245-205.

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 3.1, Issue 2, February 2006, Document Number 02-300357

The following Compliance Package documentation is provided by Witness Systems.

[3] *Planning, Installation and Administration Guide*, Release 7.3.1, March 2006

[4] *User Guide*, Release 7.3.1, March 2006

©2006 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 Developer*Connection* Program at devconnect@avaya.com.