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.

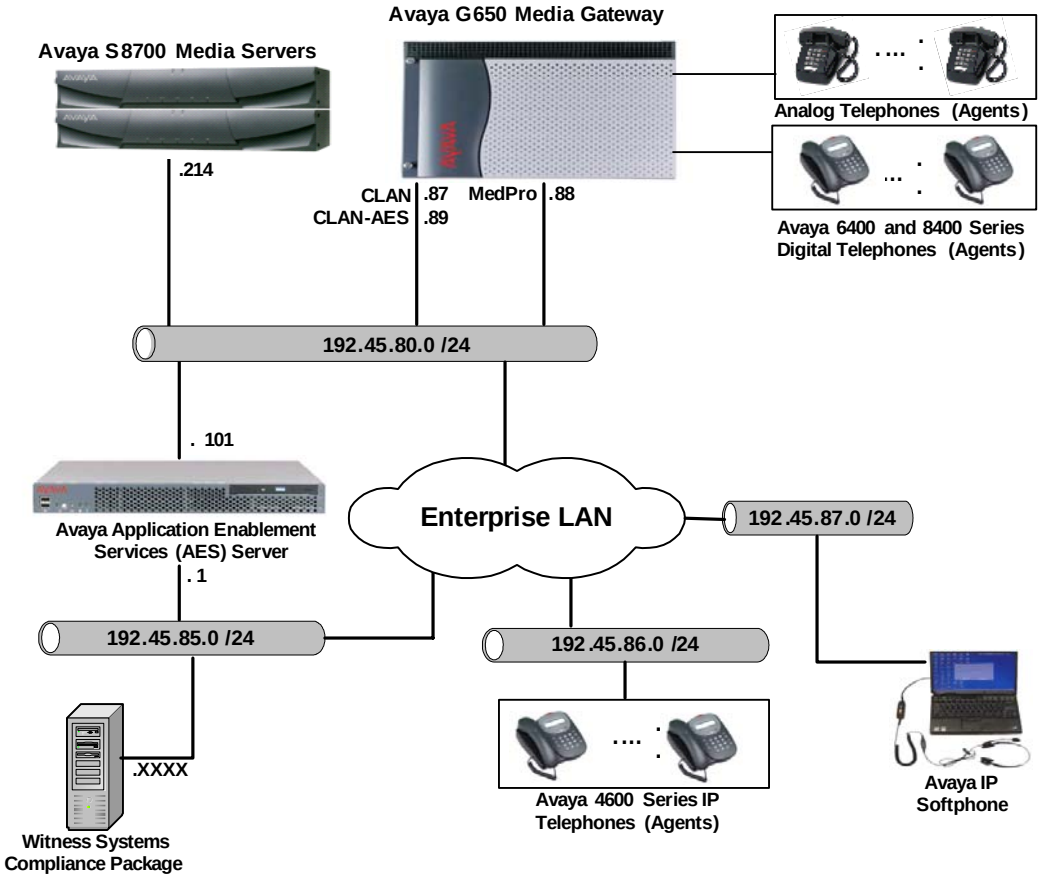


Figure 1: Test Configuration of Compliance Package with Avaya Communication Manager and Avaya Application Enablement Services

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 4621SW 4625SW		 2.3 2.2.3 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
                                   IP NODE NAMES
    Name              IP Address          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      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         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       Password          Enabled    Status
                   Server
      1:       server1           xxxxxxxxxxxxxxxx      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                                     AAS? n
                   Name: Agent-50050                             AUDIX? n
                     TN: 1                                LWC Reception: spe
                    COR: 1                          LWC Log External Calls? n
          Coverage Path:                          AUDIX Name for Messaging:
          Security Code:
                                                  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
                                           Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? y
 Prompting? n   LAI? n  G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
 Variables? n   3.0 Enhanced? 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
               : 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:
          Survivable COR: internal                  Media Complex Ext:
   Survivable Trunk Dest? y                              IP SoftPhone? 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.

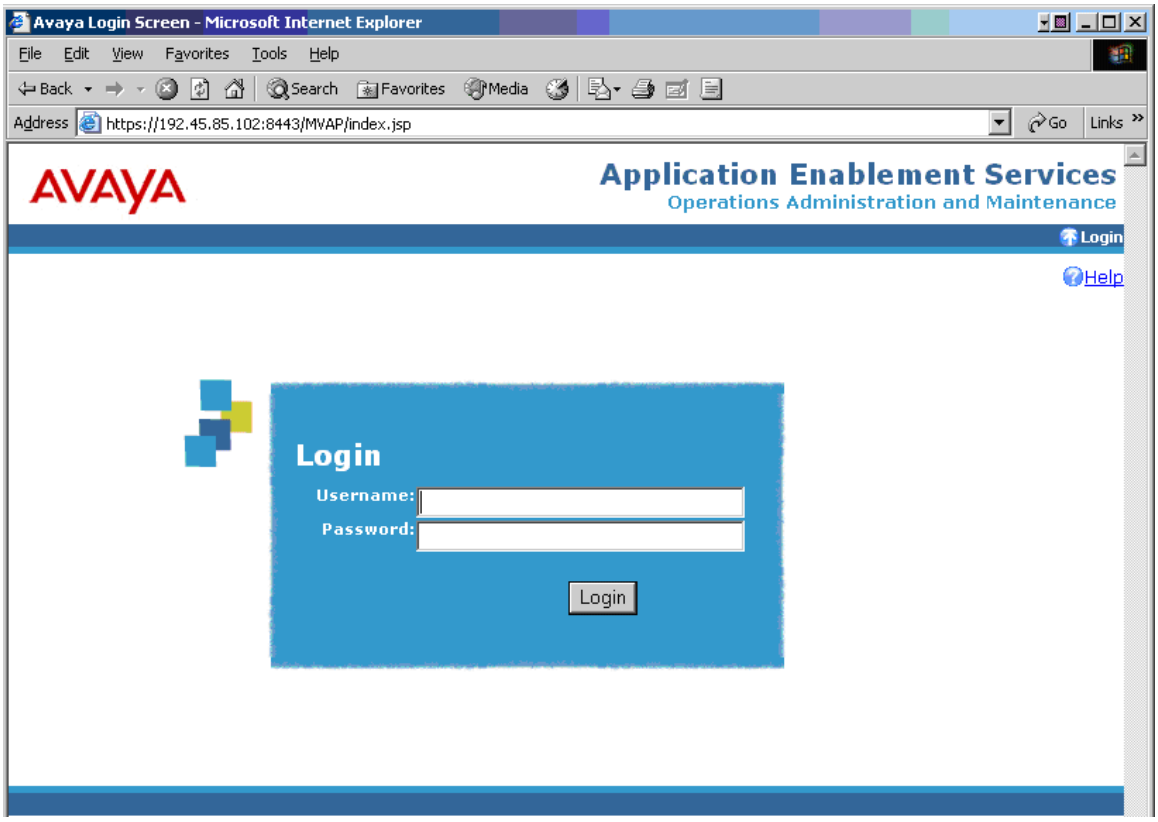
```
change ip-network-region 1                                      Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: No
      Codec Set: 1              Inter-region 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      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
```

4. Configure Avaya Application Enablement Services

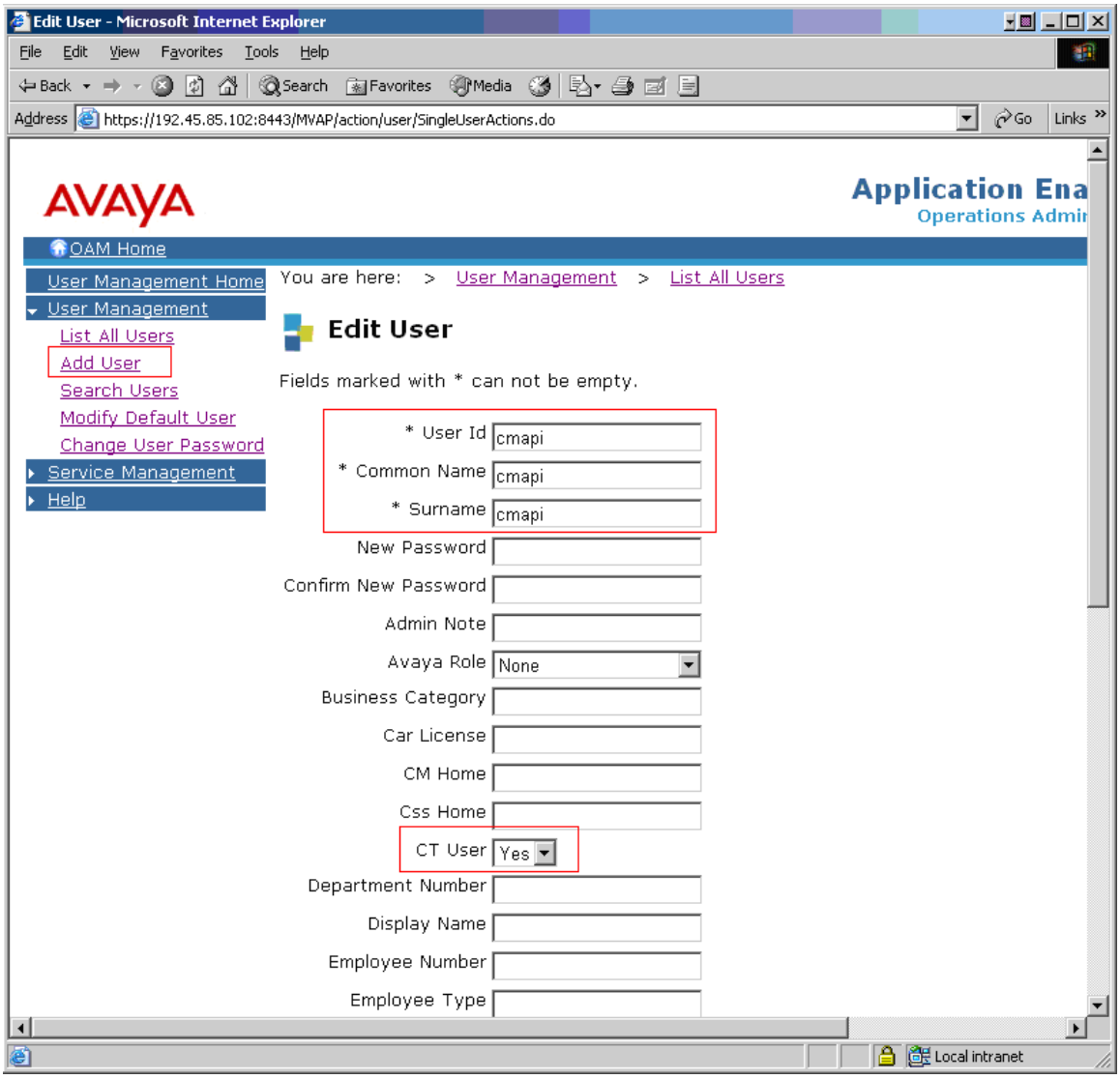
This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. Consult [2] for further guidance. The steps in this section describe the configuration of a TSAPI/JTAPI CTI user for the Compliance Package, a "Switch Connection" to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



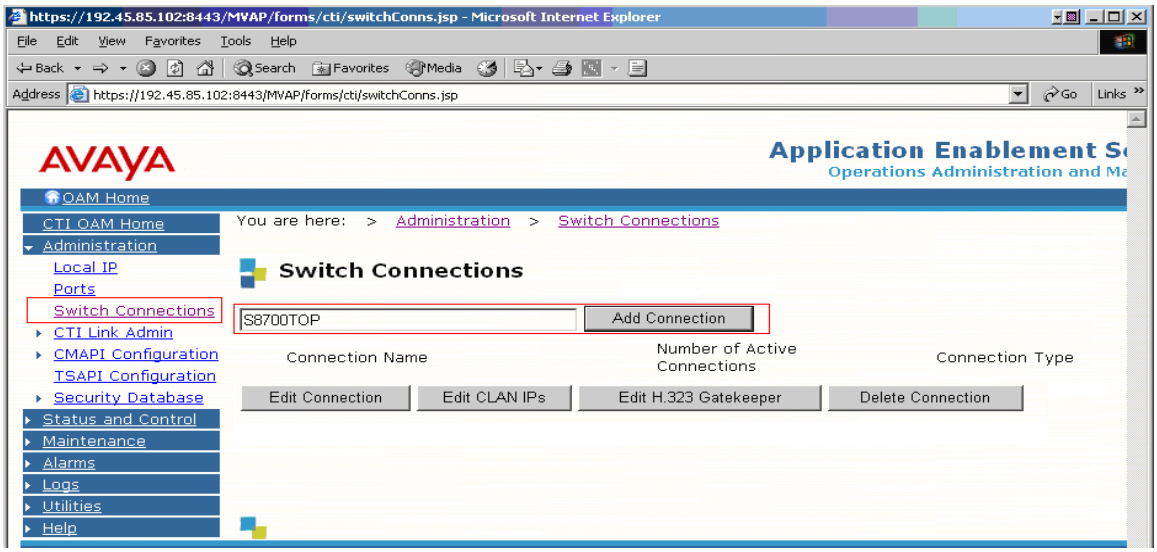
Click on **User Management**, then **User Management → Add User** in the left pane. Configure the required fields marked with asterisk, and set the CT User field to **Yes**. Compliance Package will use this **User Id** and **Password** to access the AES server. Scroll down to the bottom of the page and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



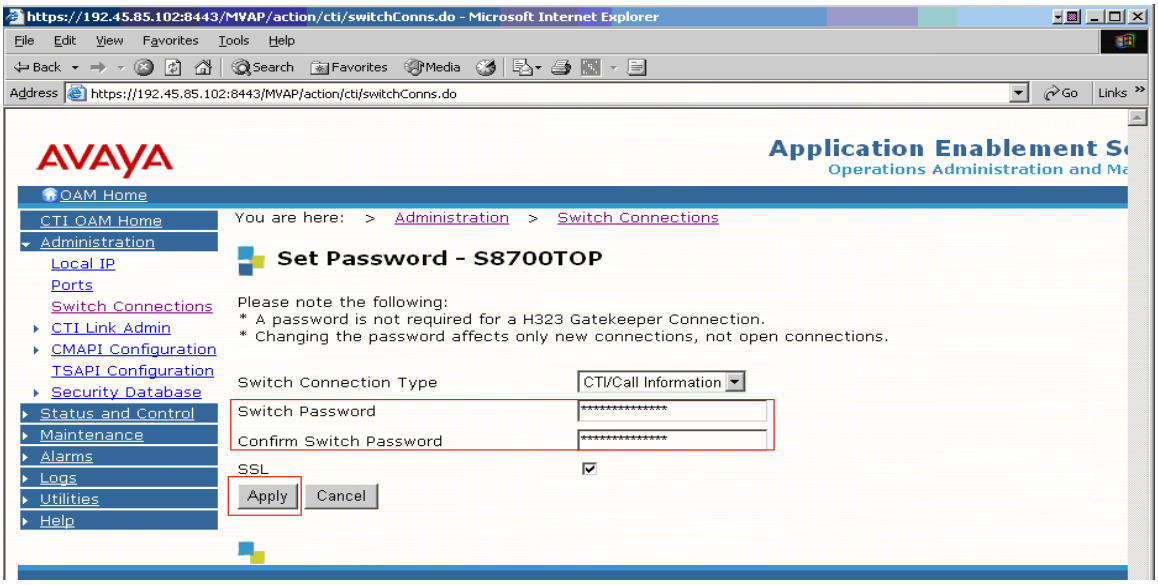
4.2. CTI OAM Admin

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.

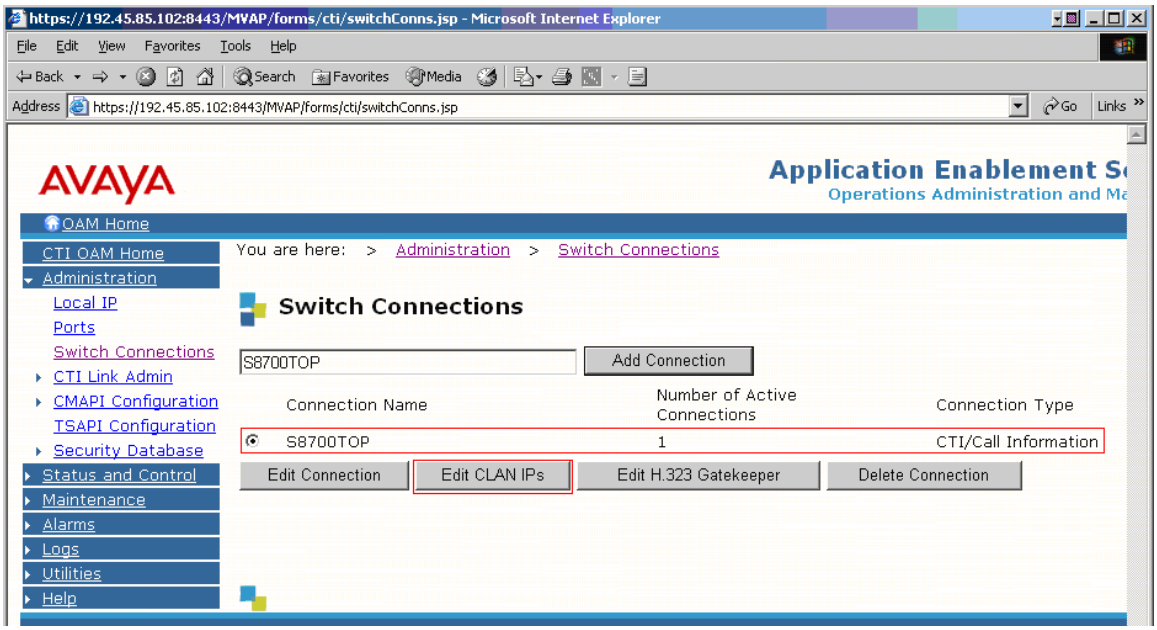
Click on **CTI OAM Home → Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the AES server and Avaya Communication Manager. Enter a descriptive name for the Switch Connection and click on **Add Connection**.



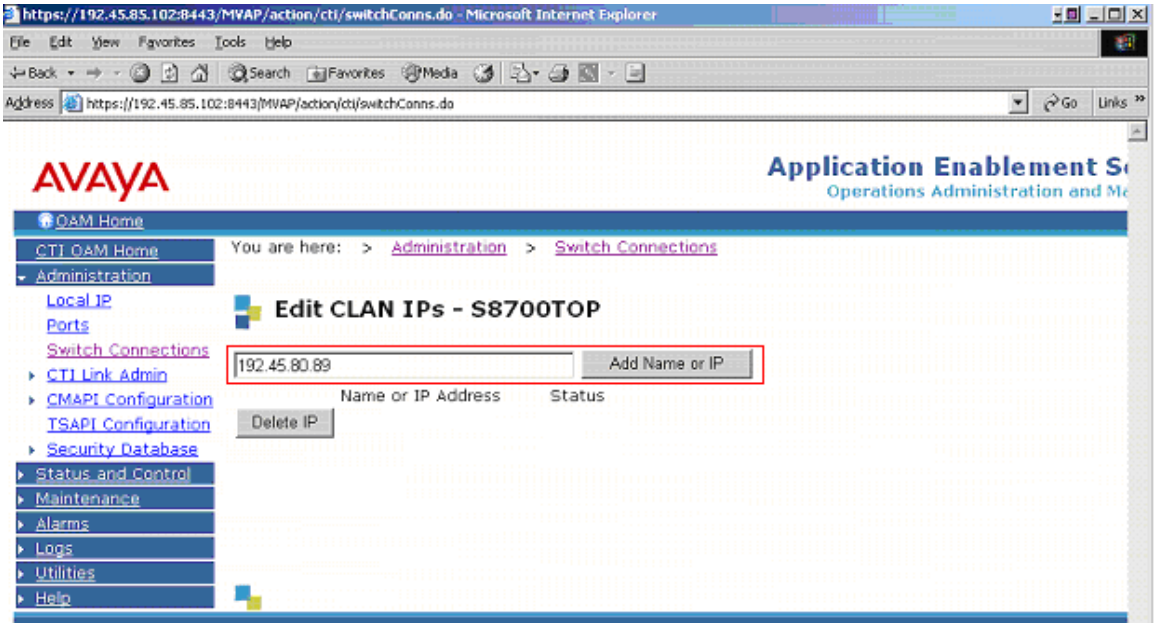
The next window that appears prompts for the Switch Connection password. Enter the same password that was administered on Avaya Communication Manager in Section 3.1. Click on **Apply**.



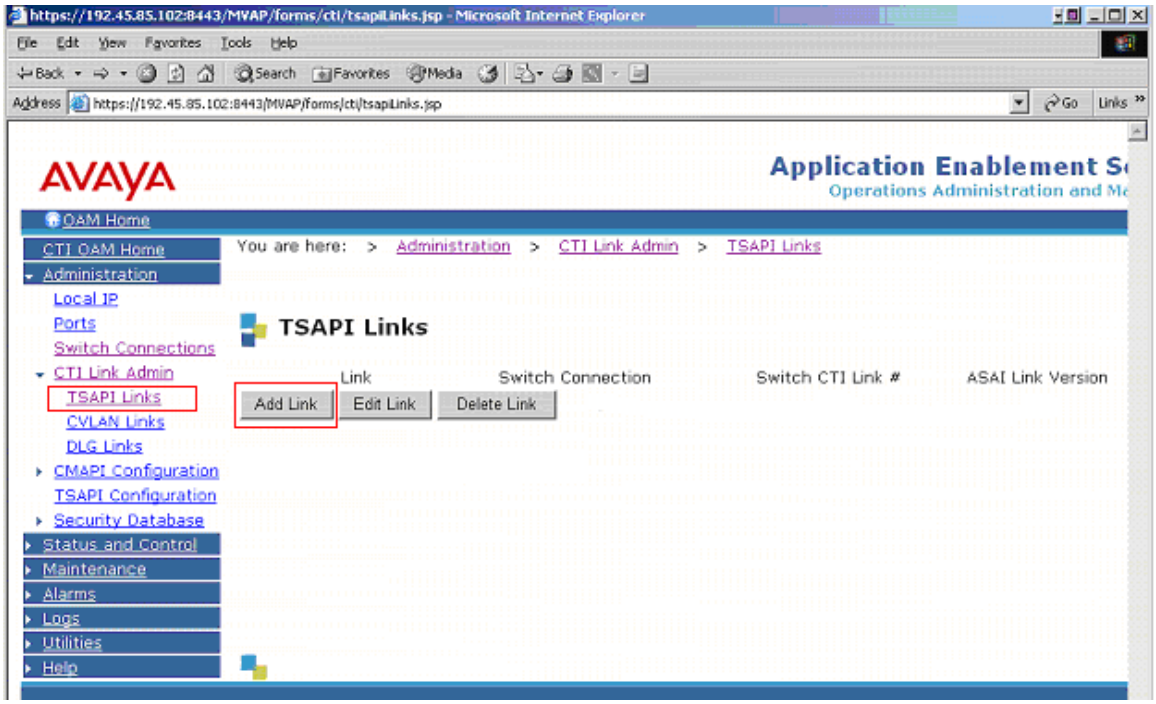
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.



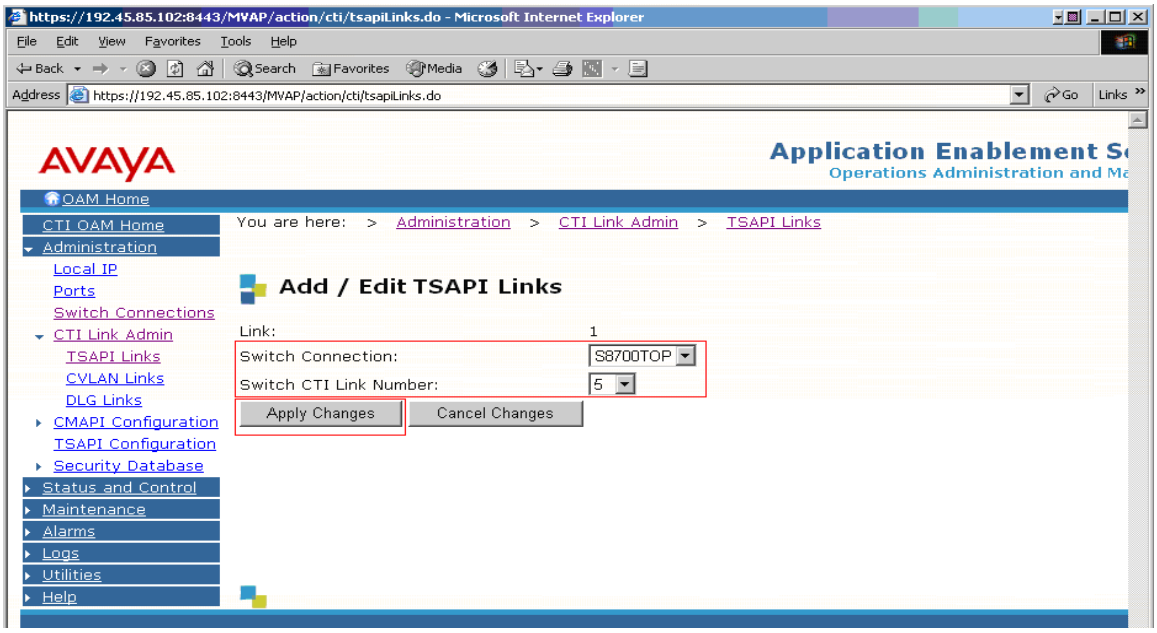
Enter the IP address of a C-LAN board enabled with Application Enablement Services (see Section 3.1) and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



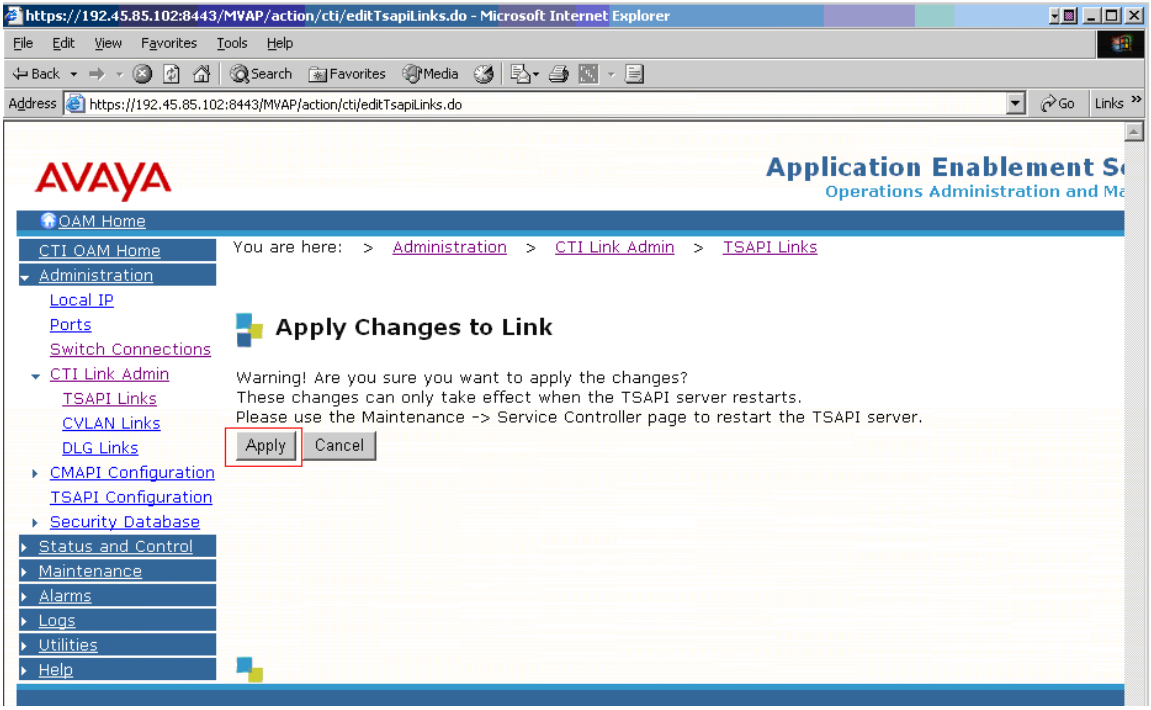
Under **Administration** in the left pane, click on **CTI Link Admin → TSAPI Links**. Click on **Add Link**.



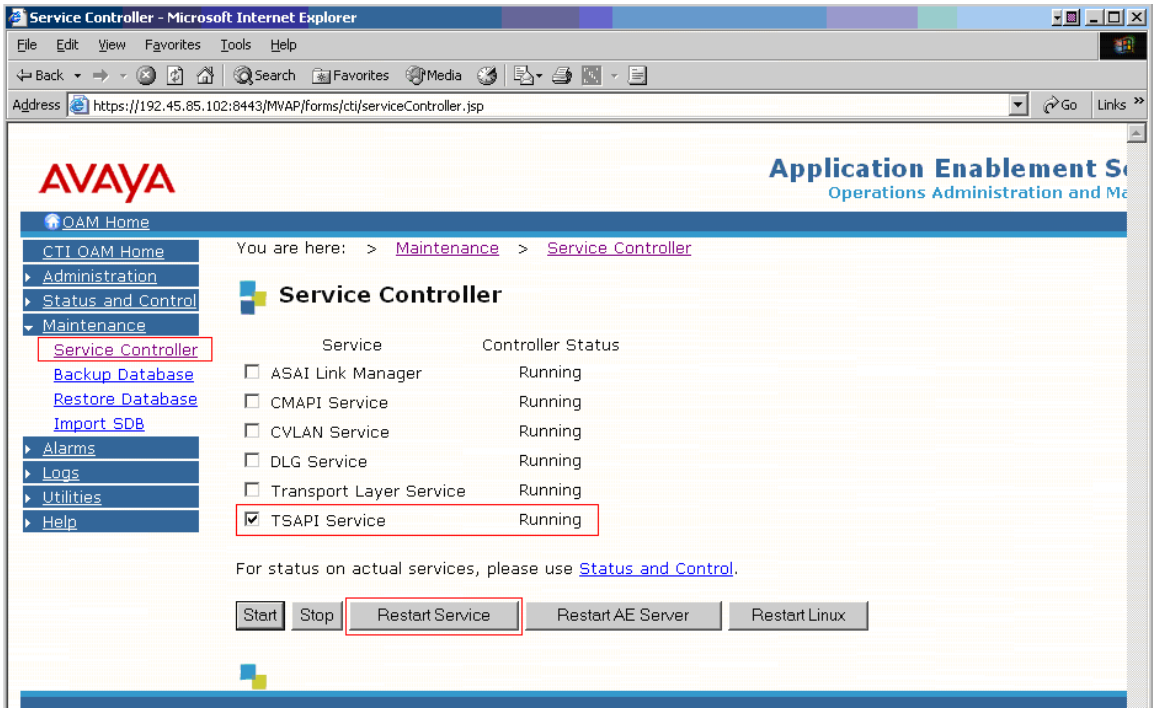
Set **Switch Connection** to the switch connection added previously and **Switch CTI Link Number** to the CTI link number configured on Avaya Communication Manager in Section 3.1. The **TSAPI Link** field is locally significant to this AES server only and may be set to any unused value. Click on **Apply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



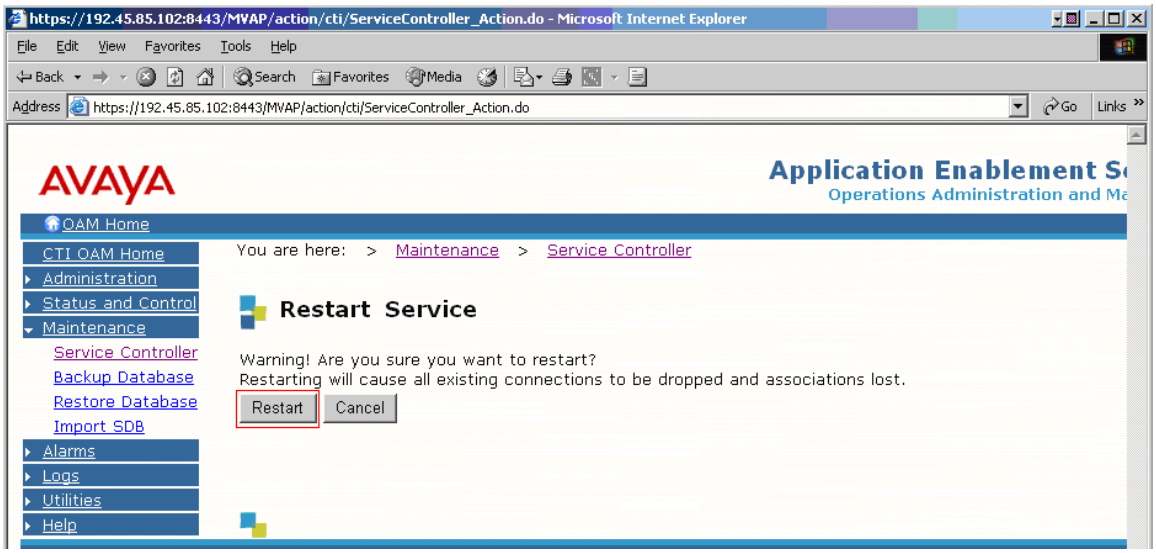
Click on **Apply** to confirm the changes.



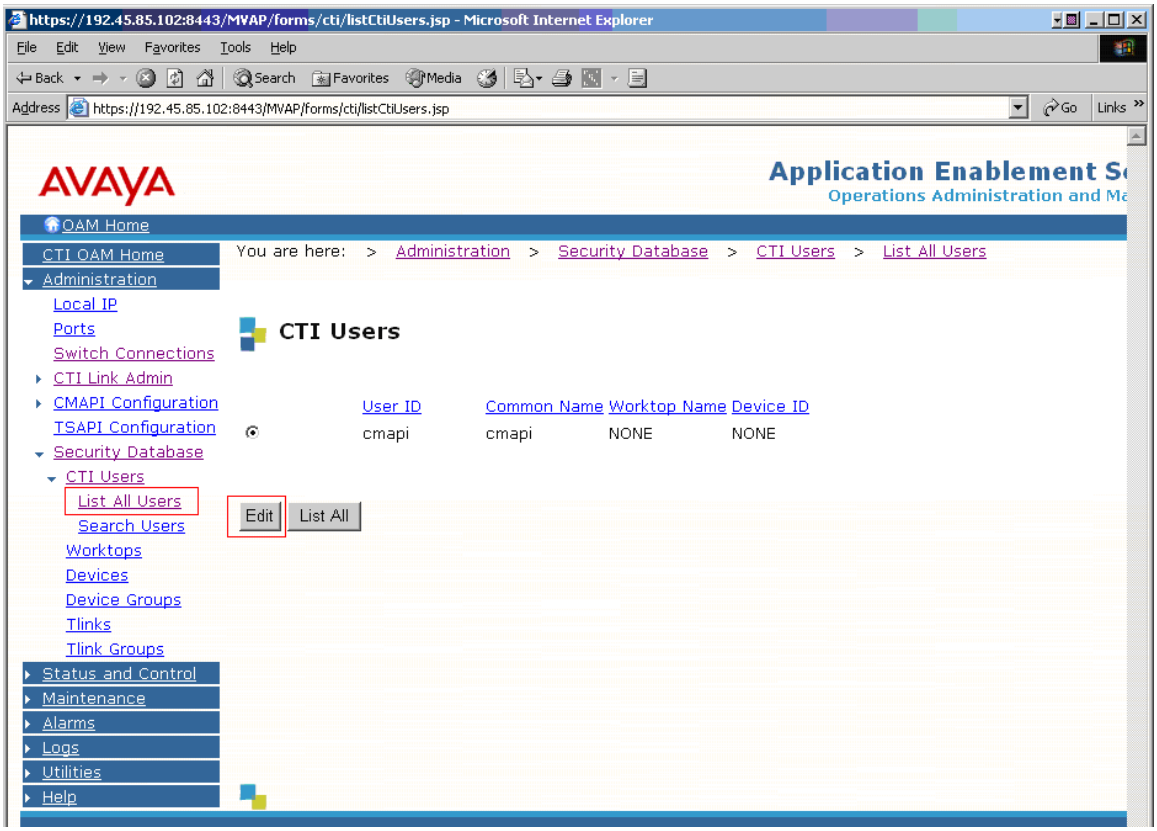
Under **Maintenance** in the left pane, click on **Service Controller**. Check the **TSAPI Service** checkbox and click on **Restart Service**.



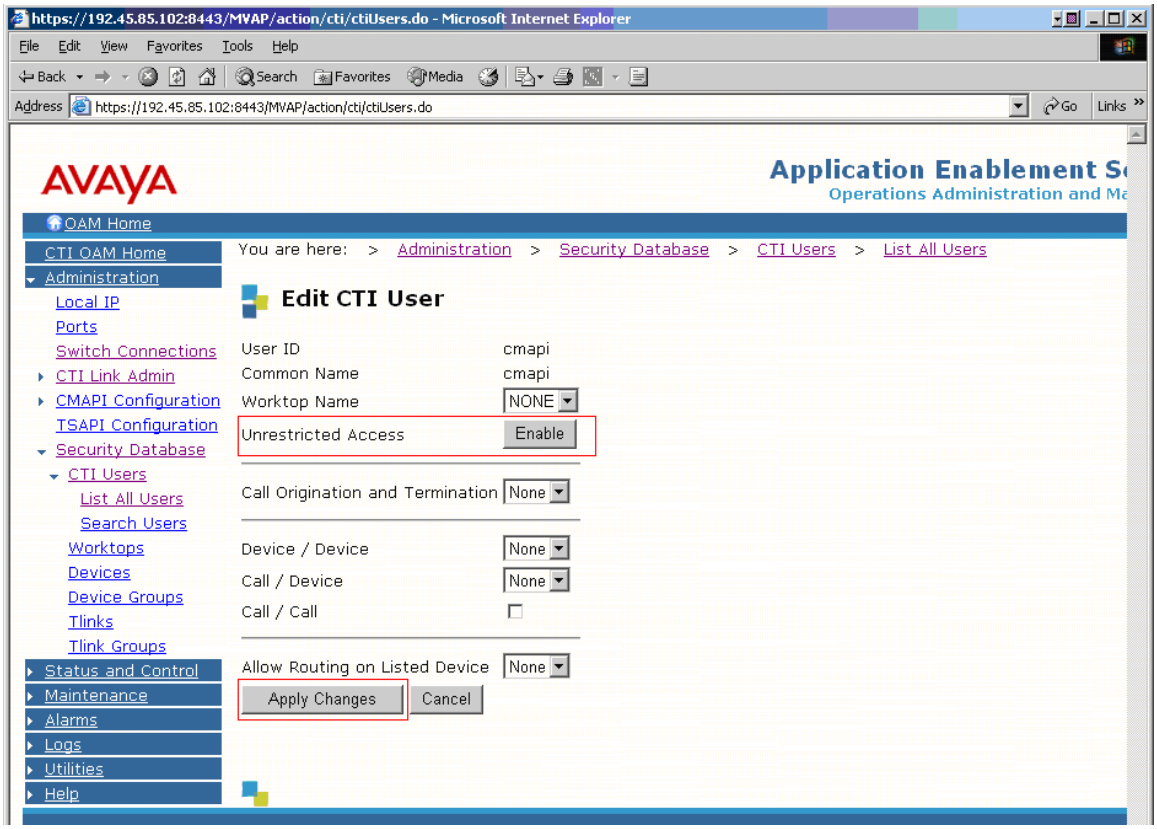
Click on **Restart** to confirm the restart.



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**.

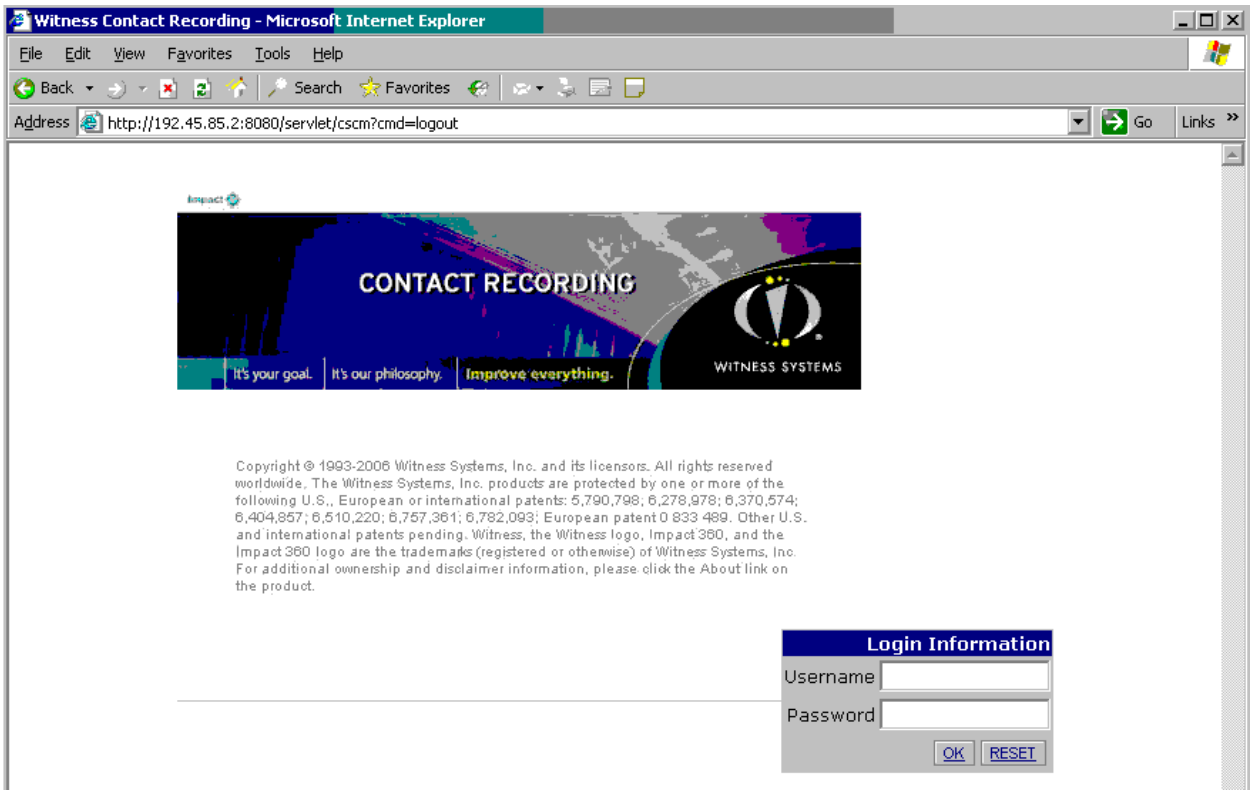


5. Configure Witness Systems Compliance Package

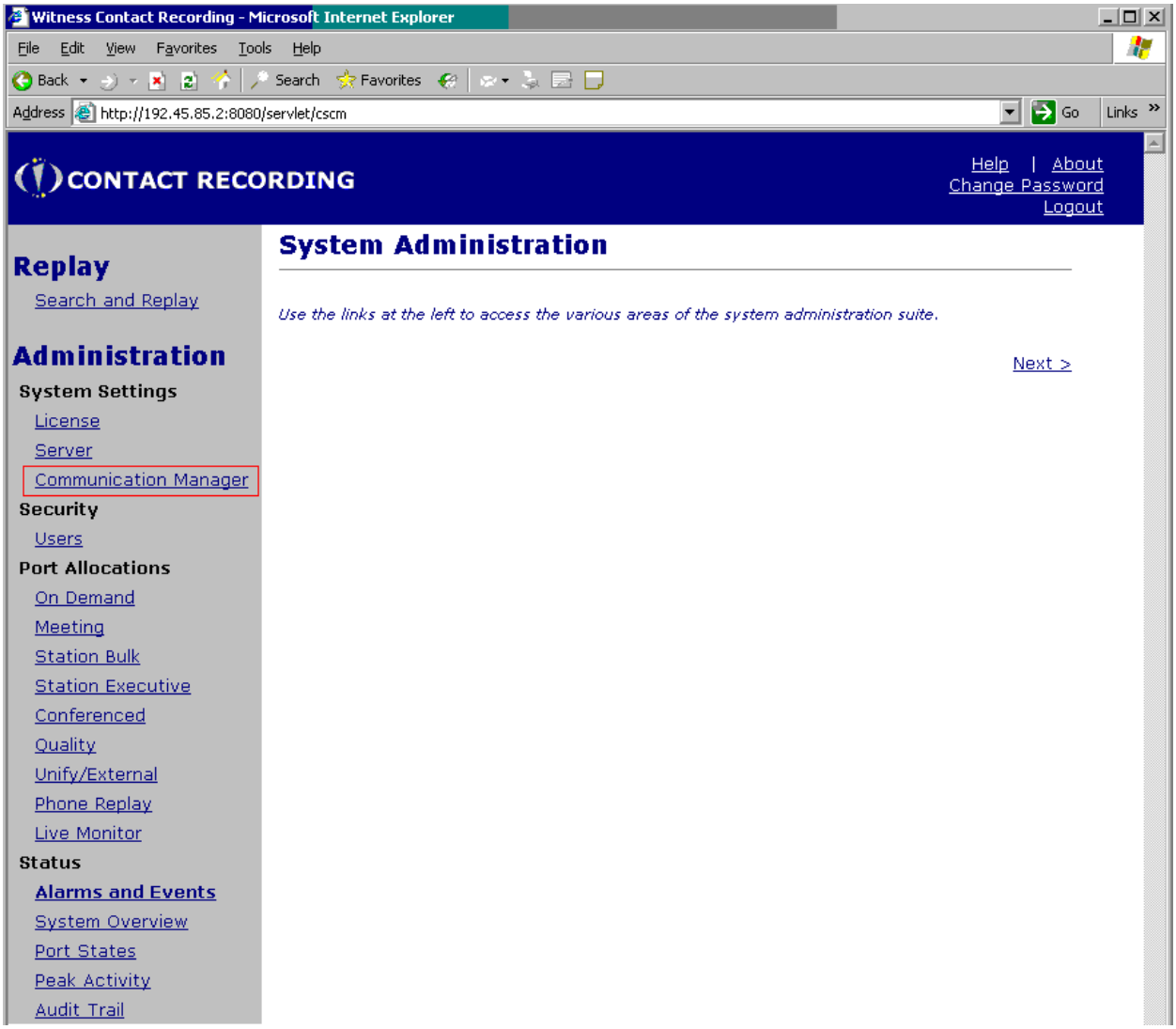
The steps in this section describe the configuration of CTI settings, stations/agents to be recorded full time, and recording stations on the Witness Systems Compliance Package. Consult Compliance Package documentation for instruction on installation. During the compliance test, the following recording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



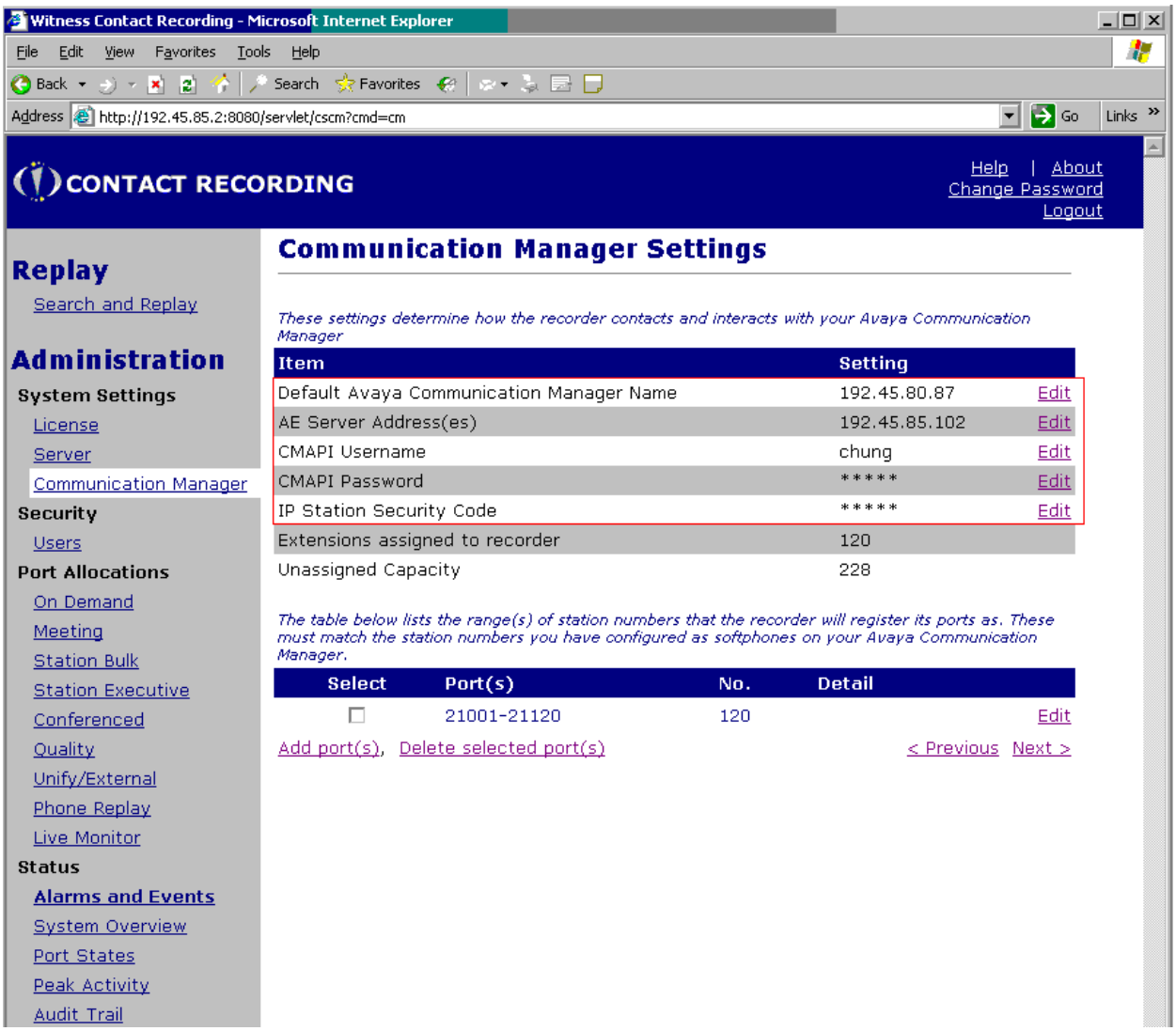
From the left pane on the System Administration page, shown next screen, click on **Communication Manager** to configure Compliance Package to communicate with Avaya Communication Manager.



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.

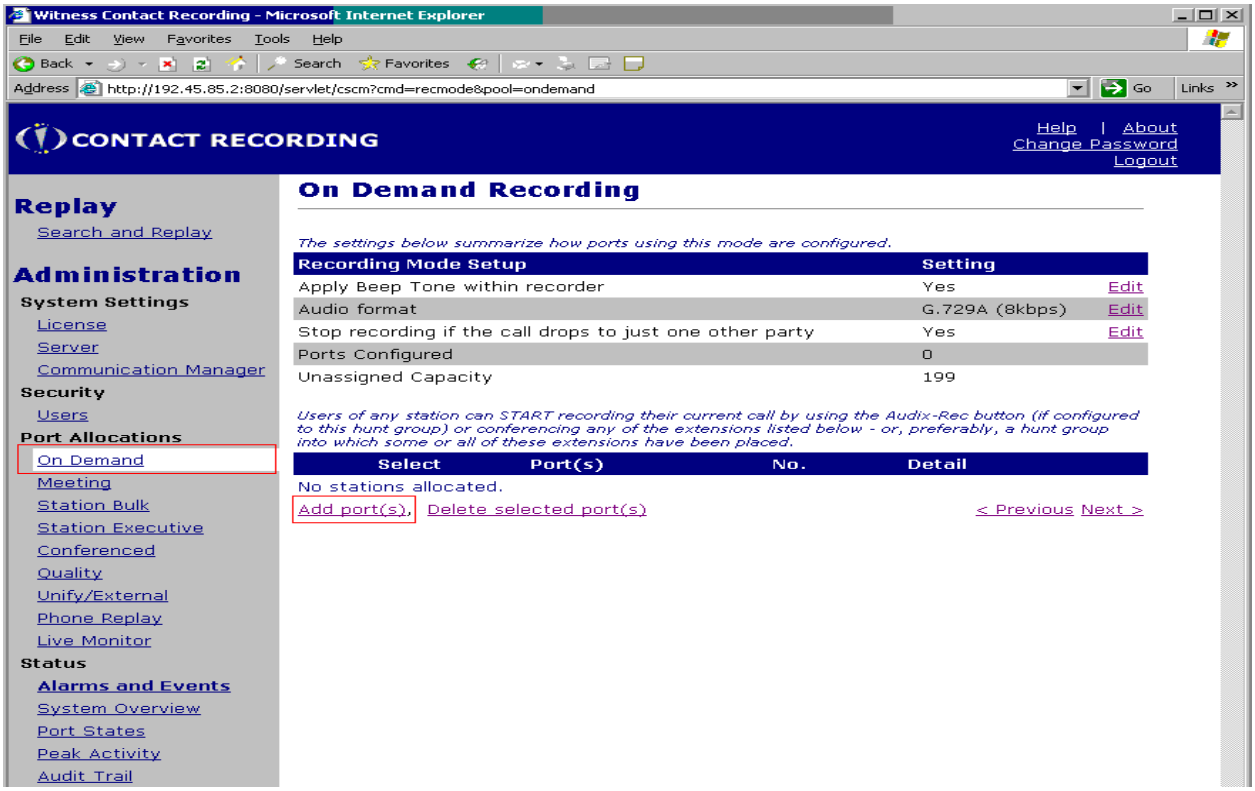
To configure each field, click on **Edit**.



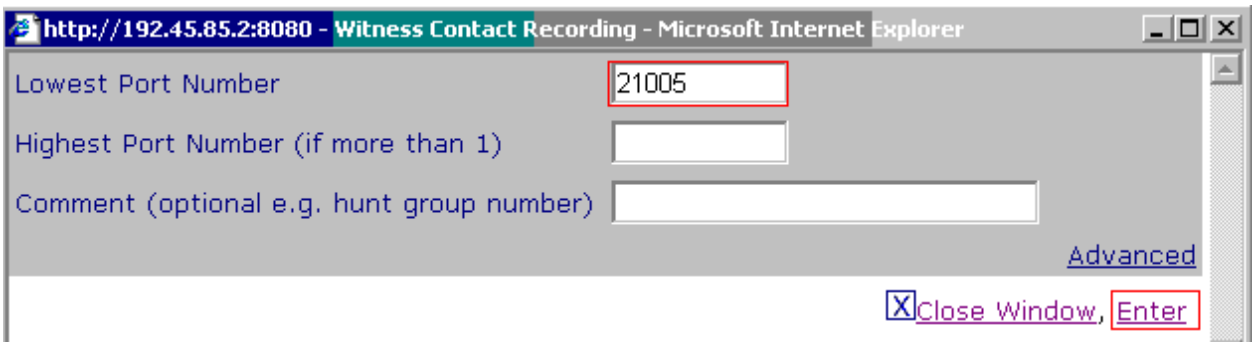
The following screen shows the Edit window of the Default Avaya Communication Manager Name field. Click on **Enter** after the edit is completed. Repeat this step to configure the remaining fields.

5.1. Configure On Demand

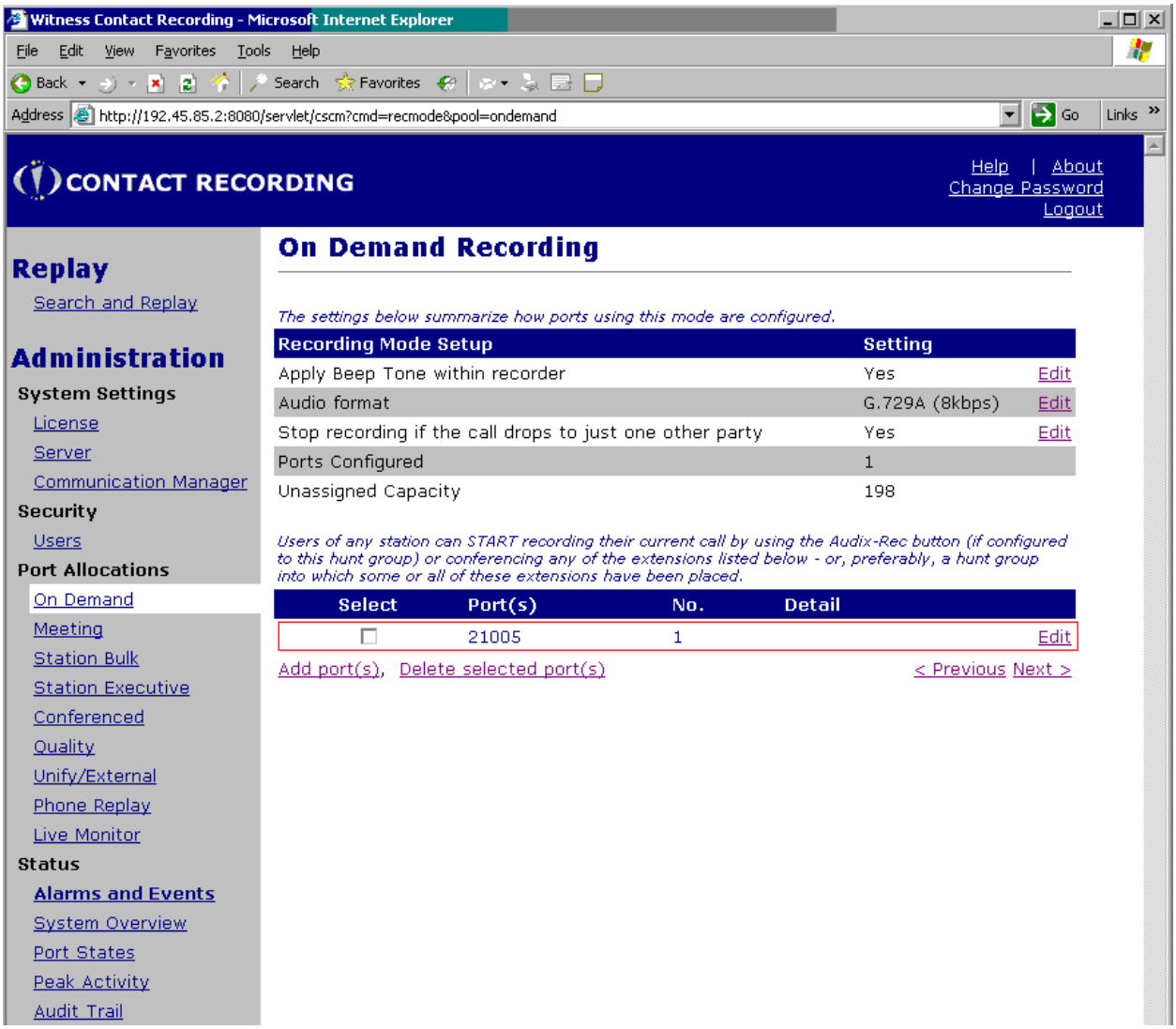
On Demand Recording lets an authorized phone user on the system, conferences in a recording port (station) when the user wants to start recording a call. One or more "pools" of ports on the recorder can be assigned to this recording mode. The recorder automatically answers the incoming call on its port 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**.

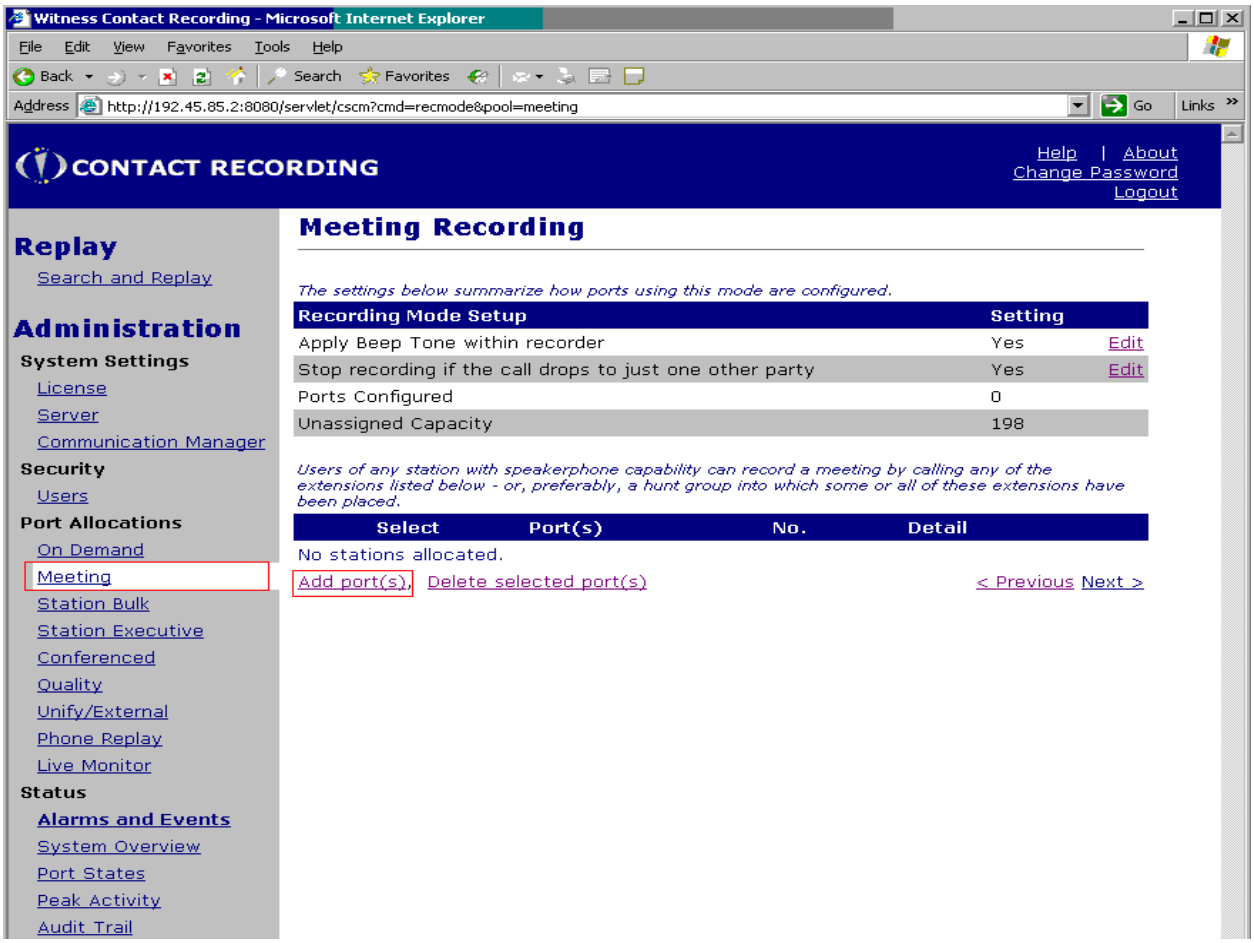


The following screen shows the On Demand Recording page after the recording port is configured.

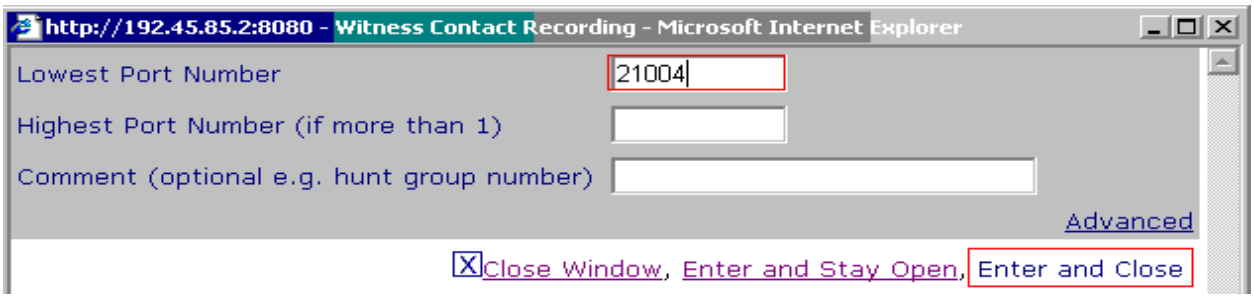


5.2. Configure Meeting

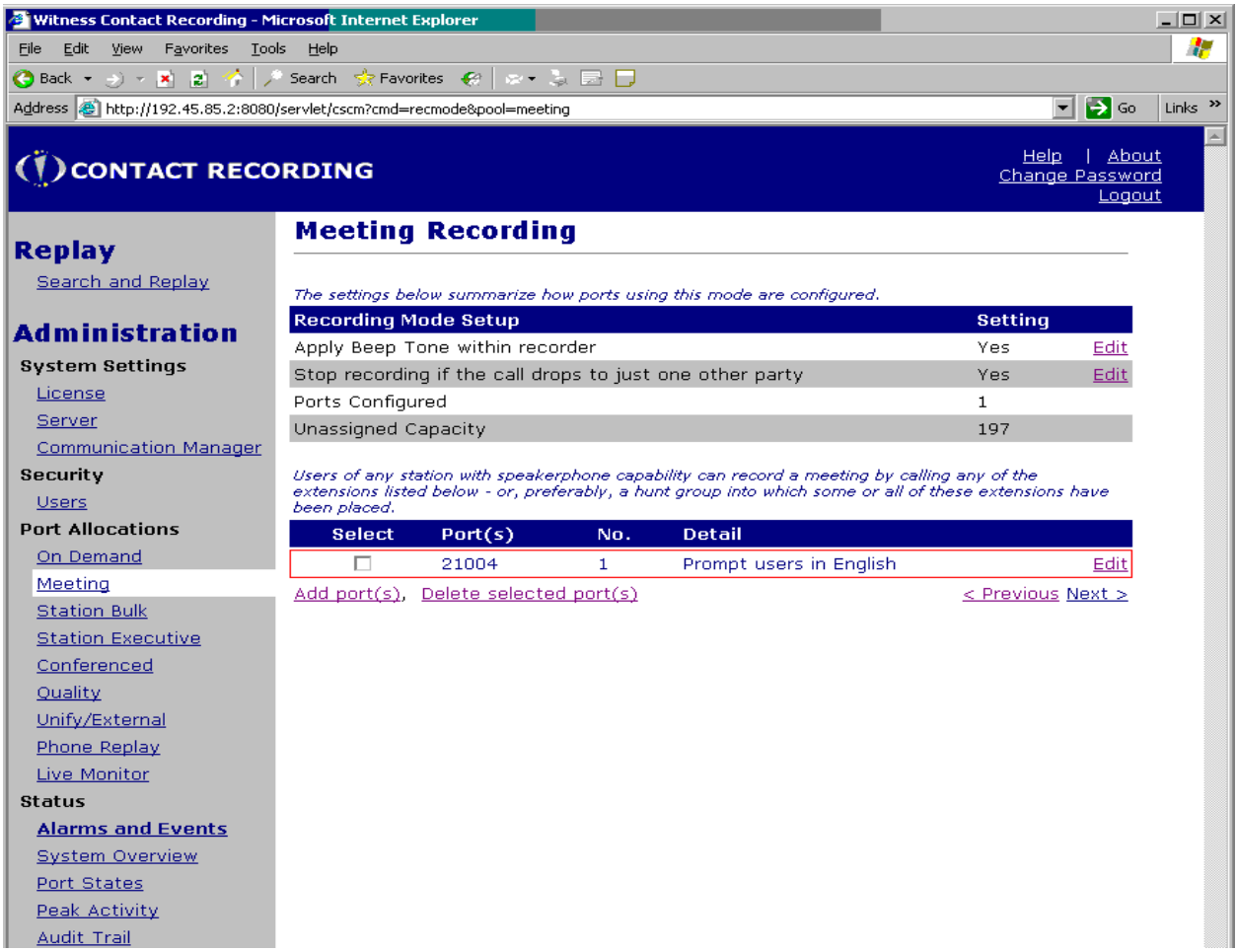
Meeting Recording is normally utilized as a detailed log of a meeting, either as an audio recorder for those attending, or as a way to include non-attendees later. One or more "pools" of ports on the recorder can be assigned to this recording mode. To access Meeting Recording, click on **Meeting** from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



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

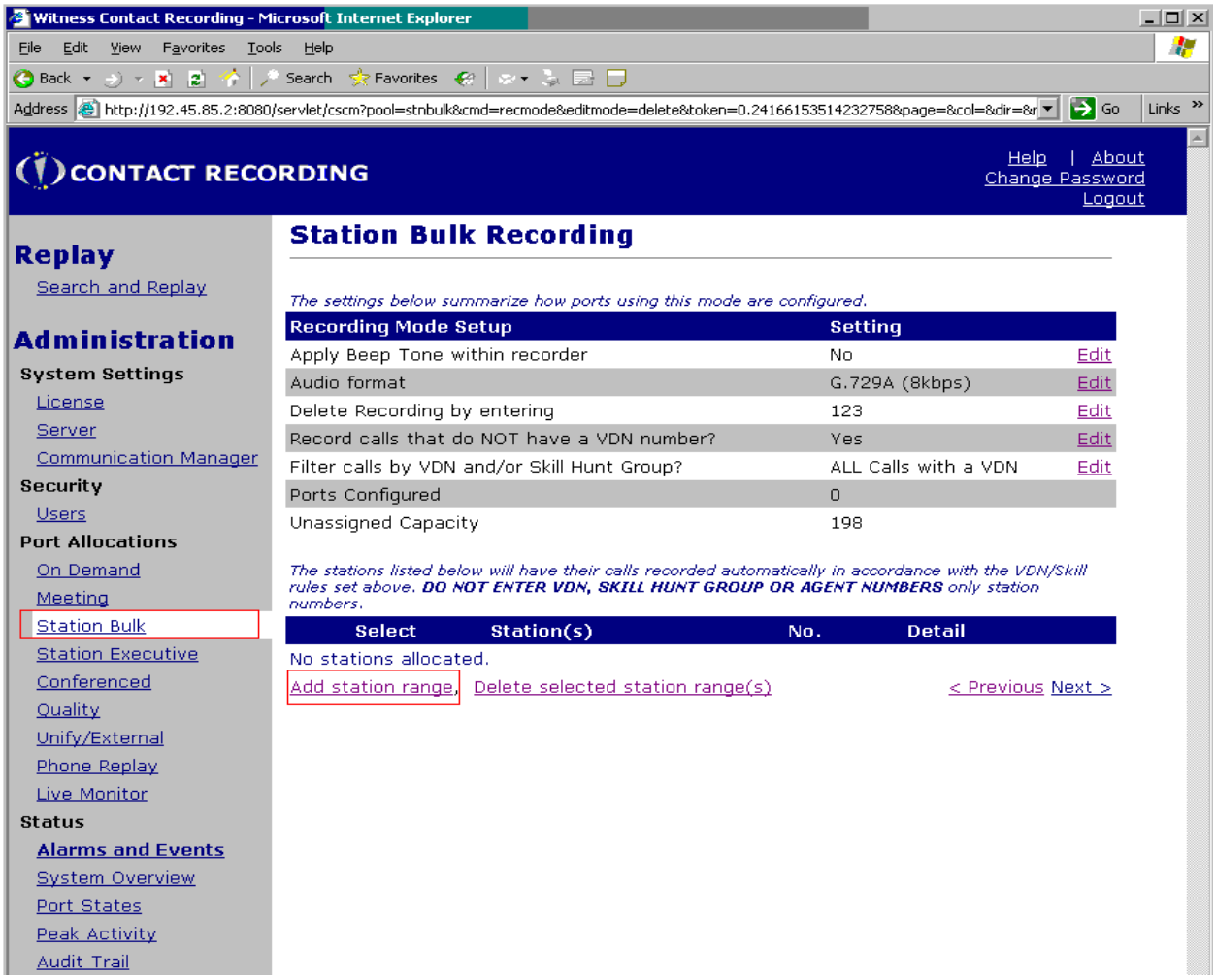


The following screen shows the Meeting Recording page after the recording port is configured.



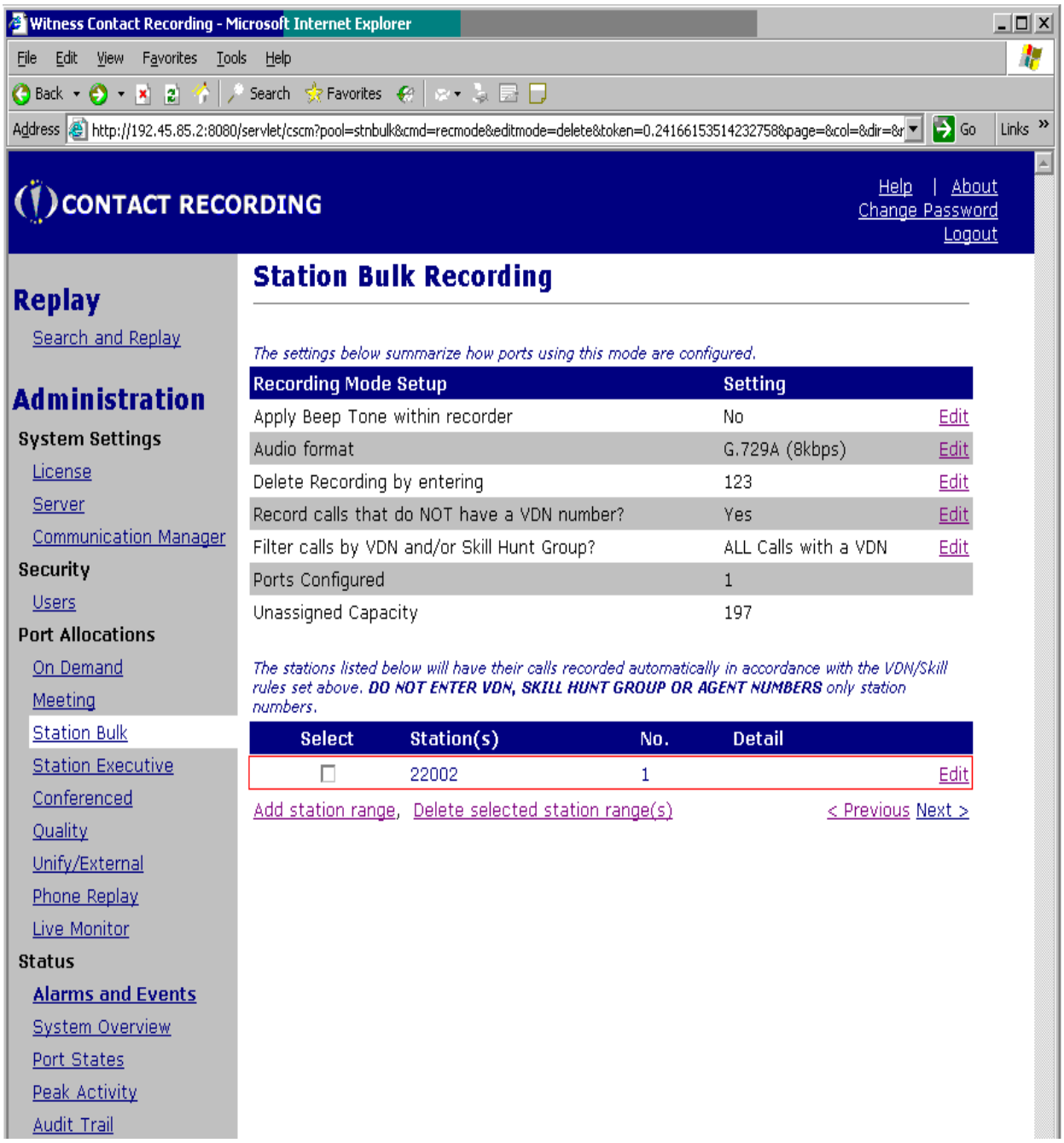
5.3. Configure Station Bulk

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**.



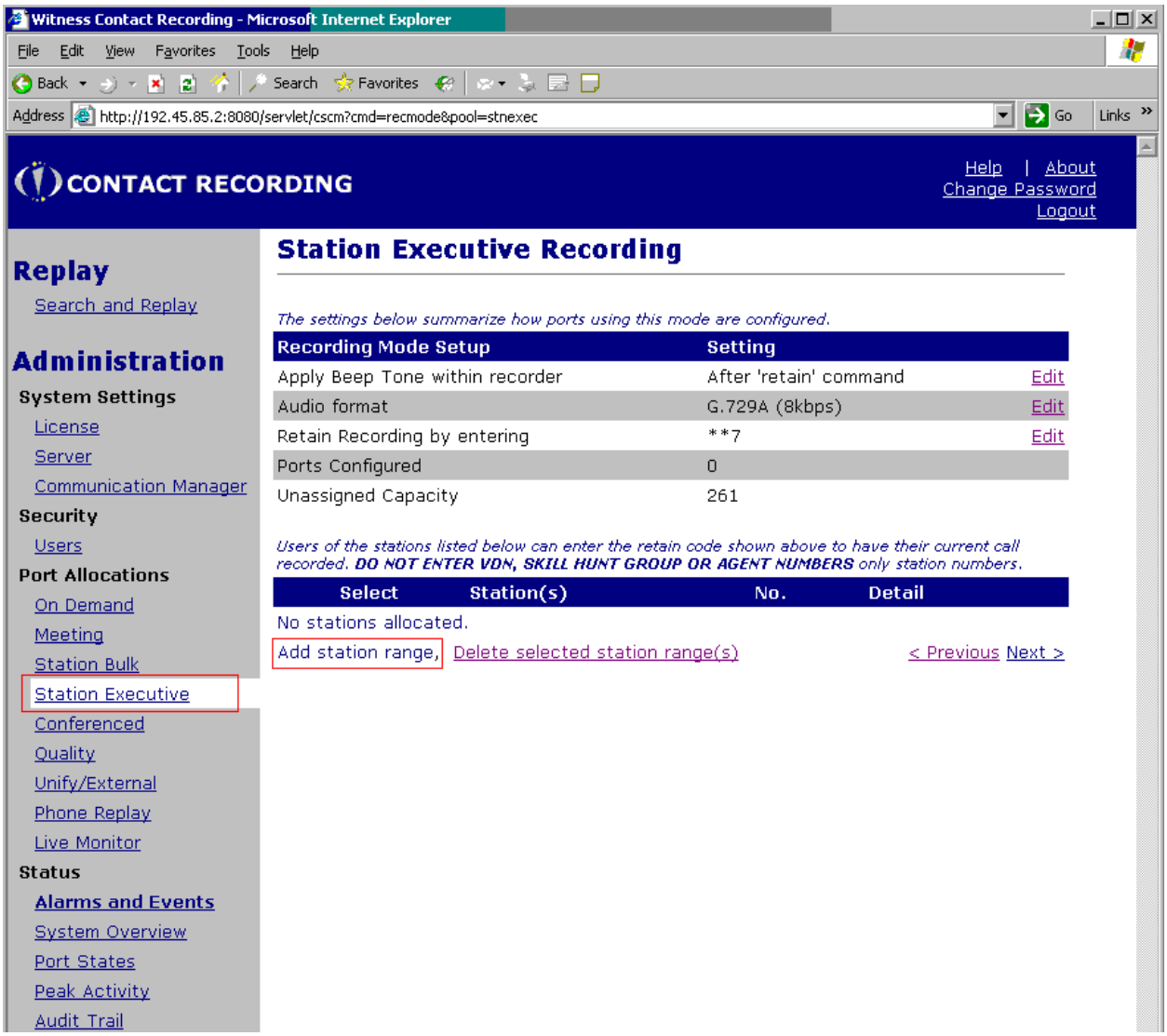
Add recorded station(s), and click on **Enter and Close**.

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



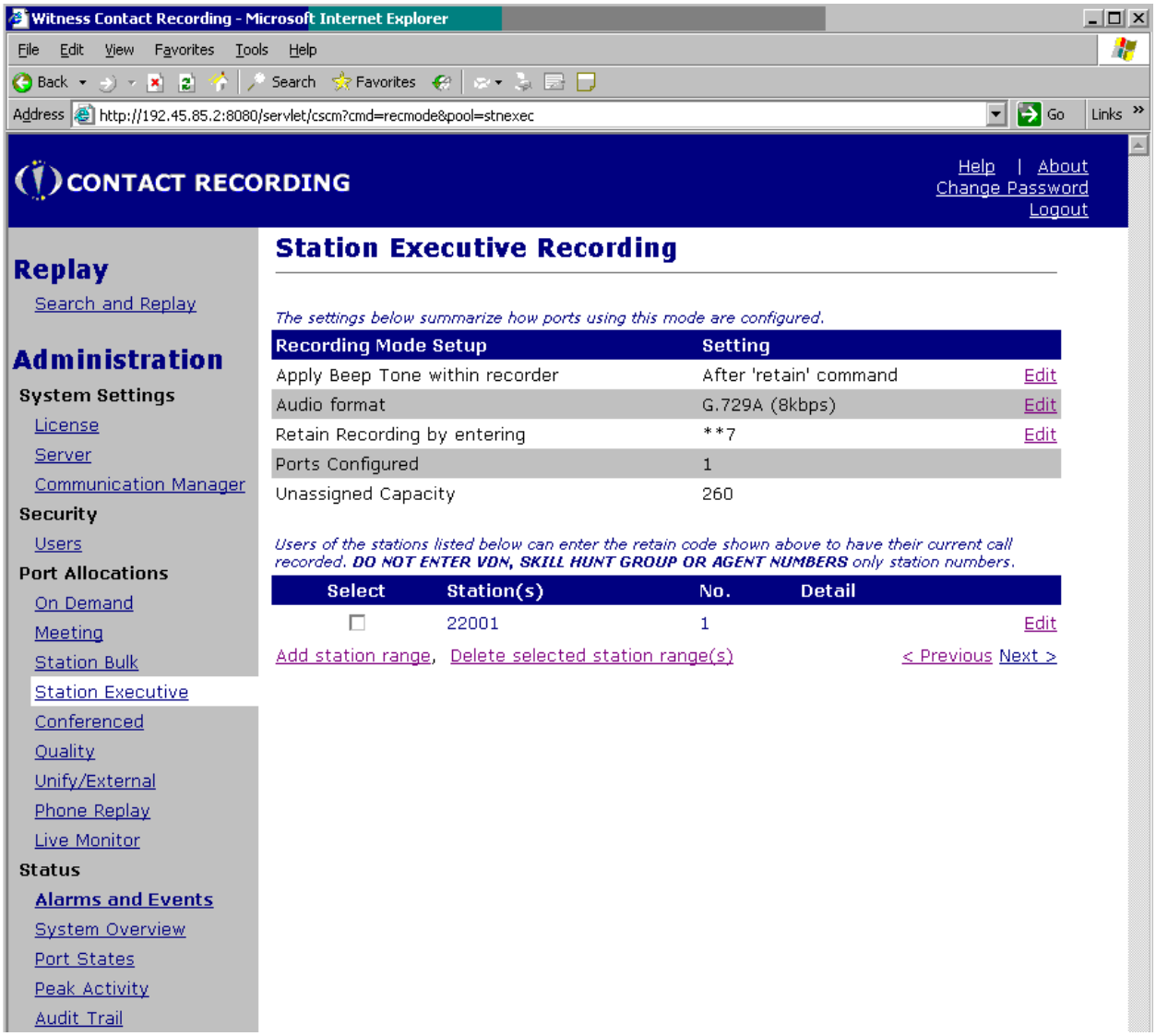
5.4. Configure Station Executive

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**.



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

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



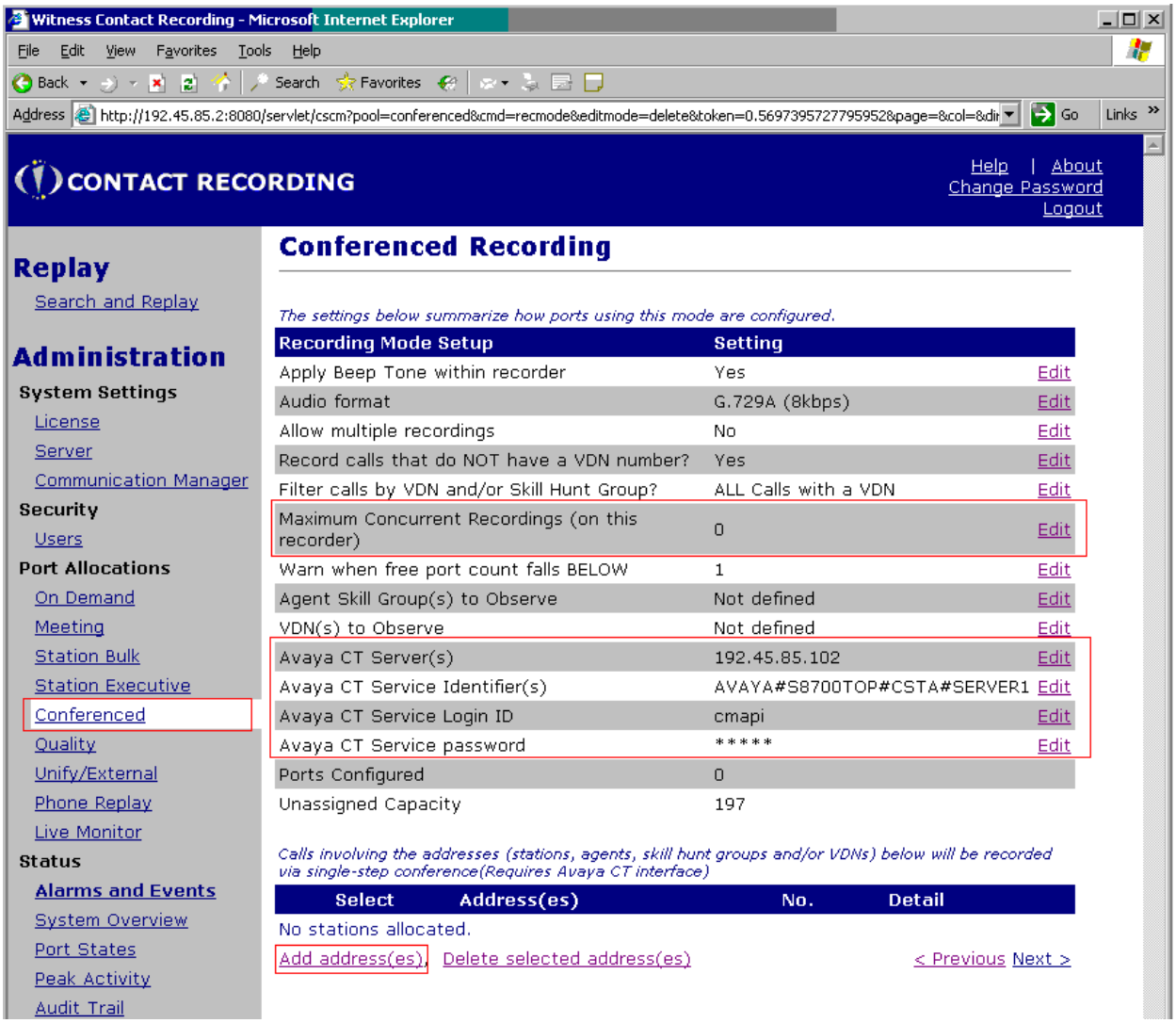
5.5. Configure Conferenced

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)

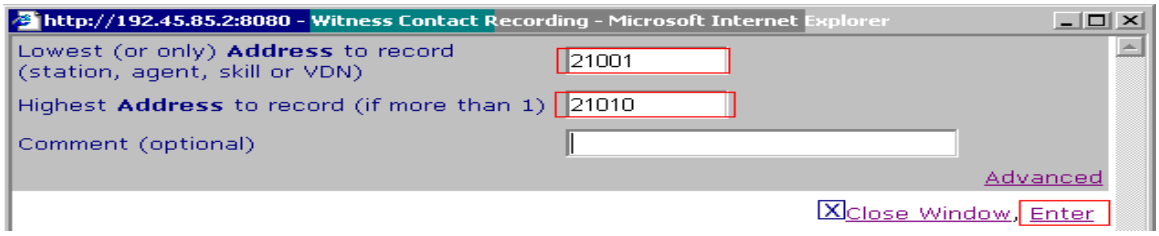
- Avaya CT Server(s)
- Avaya CT Service Identifier(s)
- Avaya CT Service Login ID
- Avaya CT Service password

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

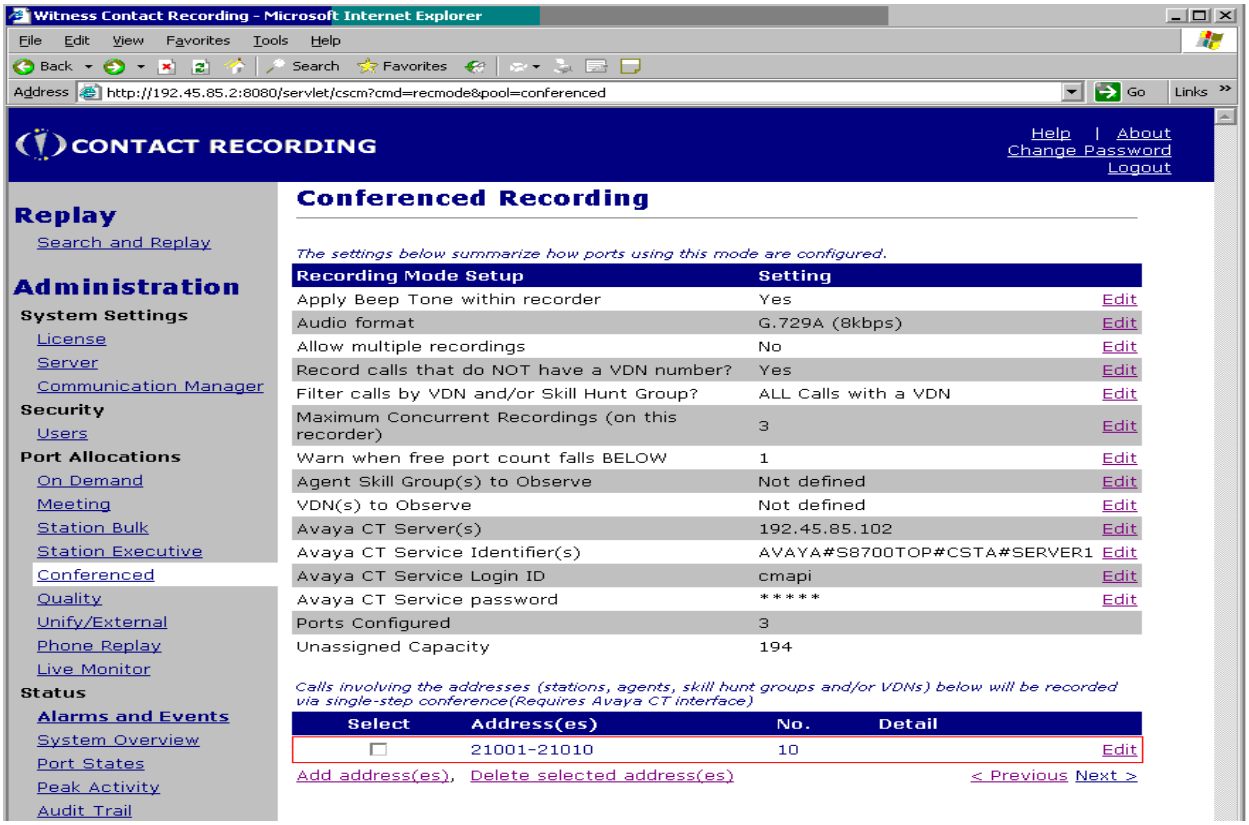


The following screen shows the Edit window of the Maximum Concurrent Recordings (on this recorder) field. Click on **Enter** after the edit is completed. Repeat this step to configure the remaining fields.

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

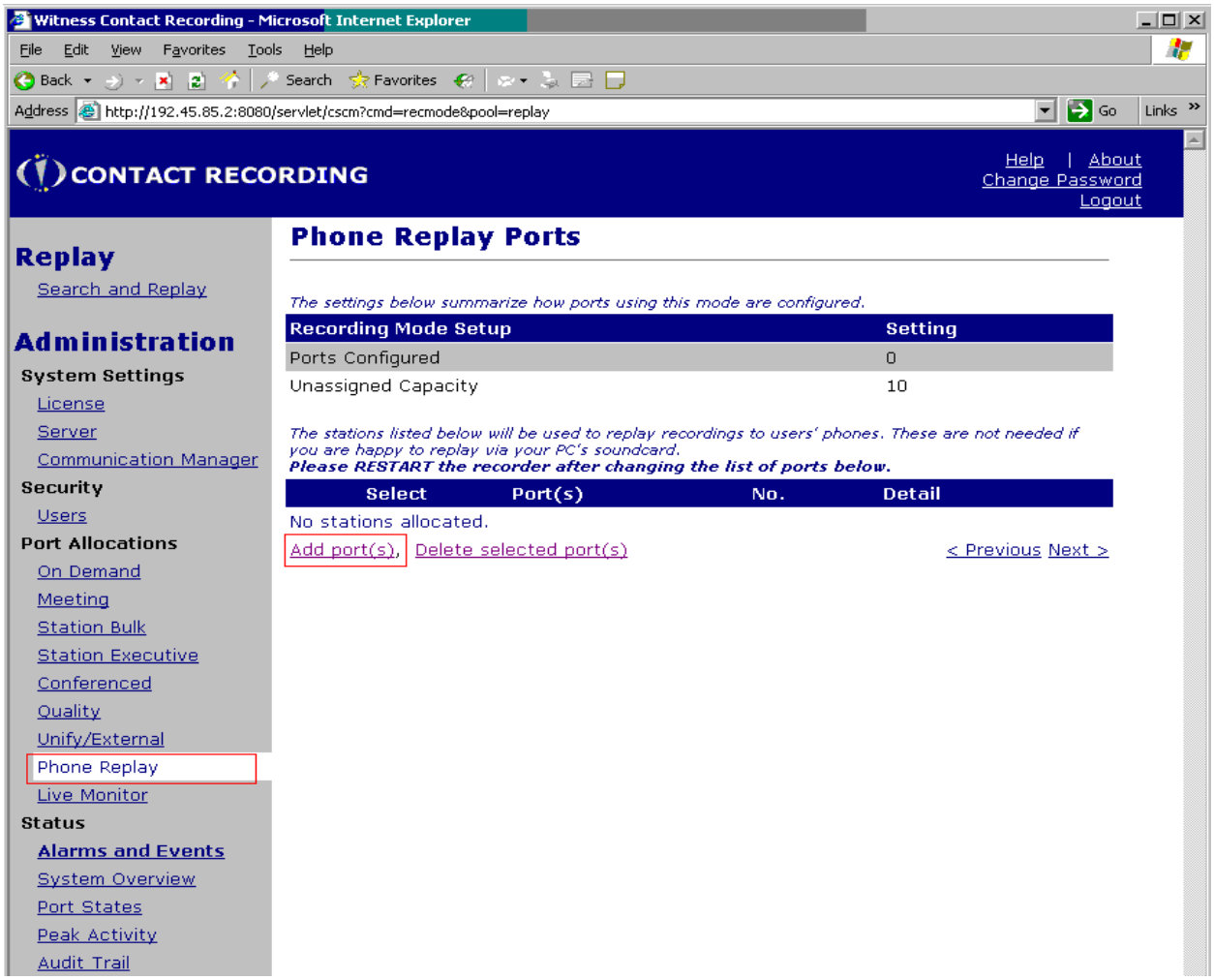


The following screen shows the Station Executive Recording page after the station is configured.

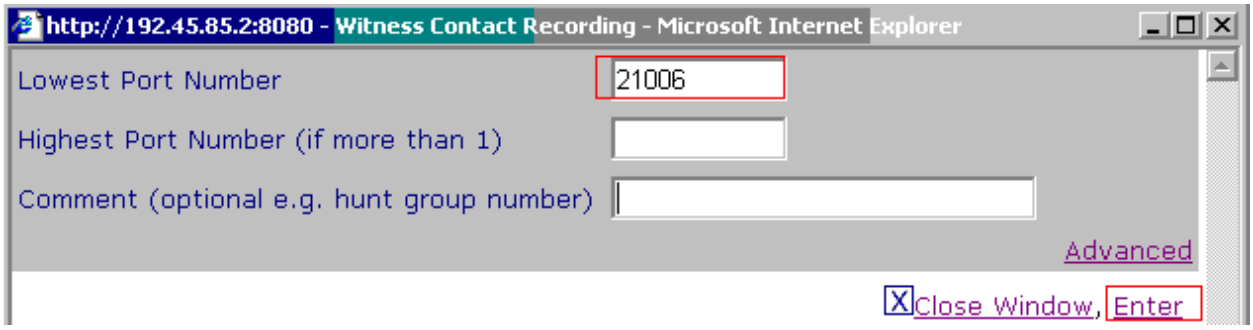


5.6. Configure Phone Replay

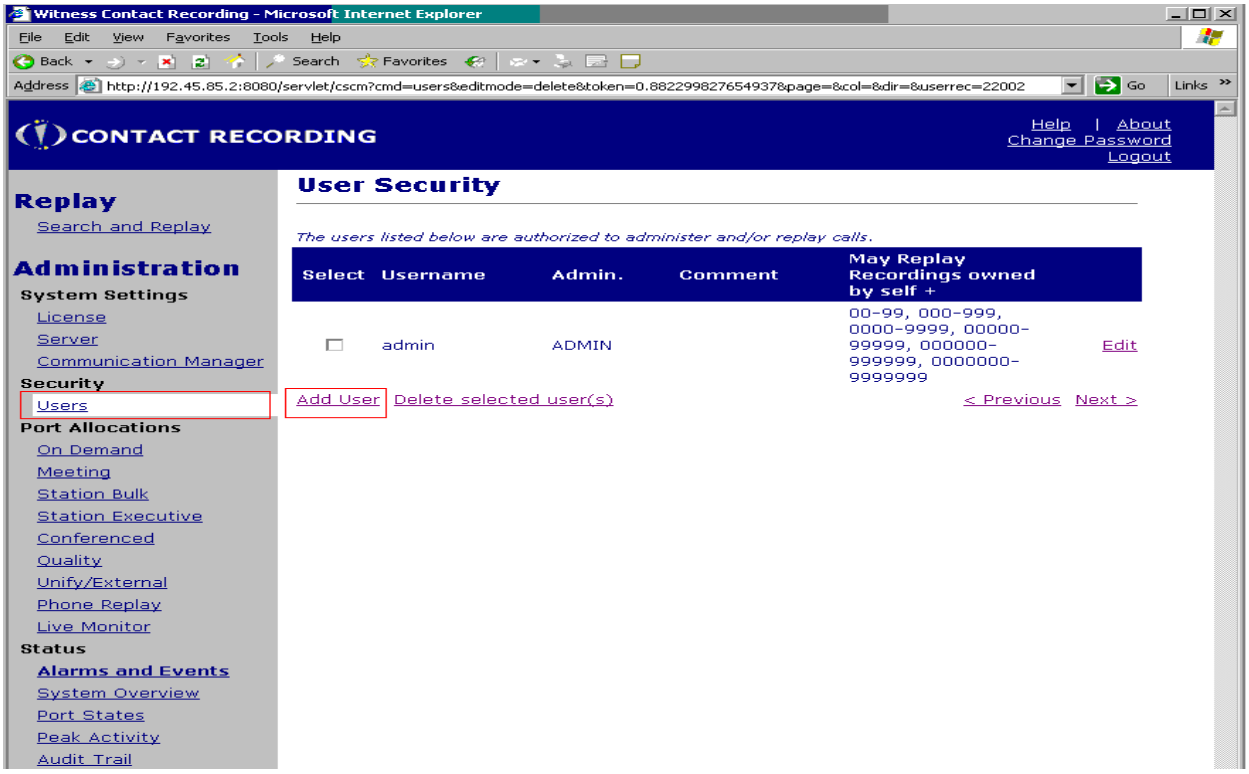
The Phone Replay feature replays recorded messages via the user's telephone, and this does use a port. To access the Phone replay feature, click on **Phone Replay** from the left pane. The following screen shows the Phone Replay Ports page. Allocate station(s) by clicking on **Add port(s)**.



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



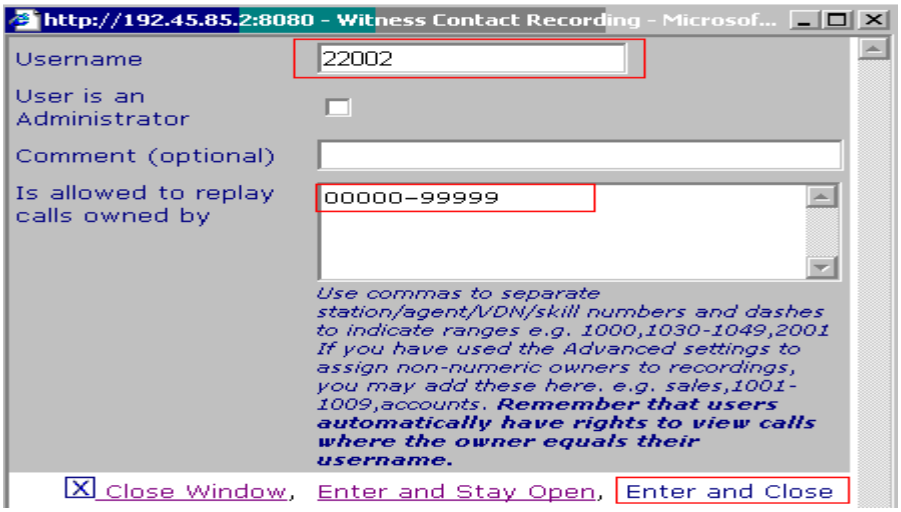
At this point, a user (a station to replay the recorded message) needs to be created. To create a user, click on **Users** from the left pane. The following screen shows the User Security page. Add a user by clicking on **Add User**



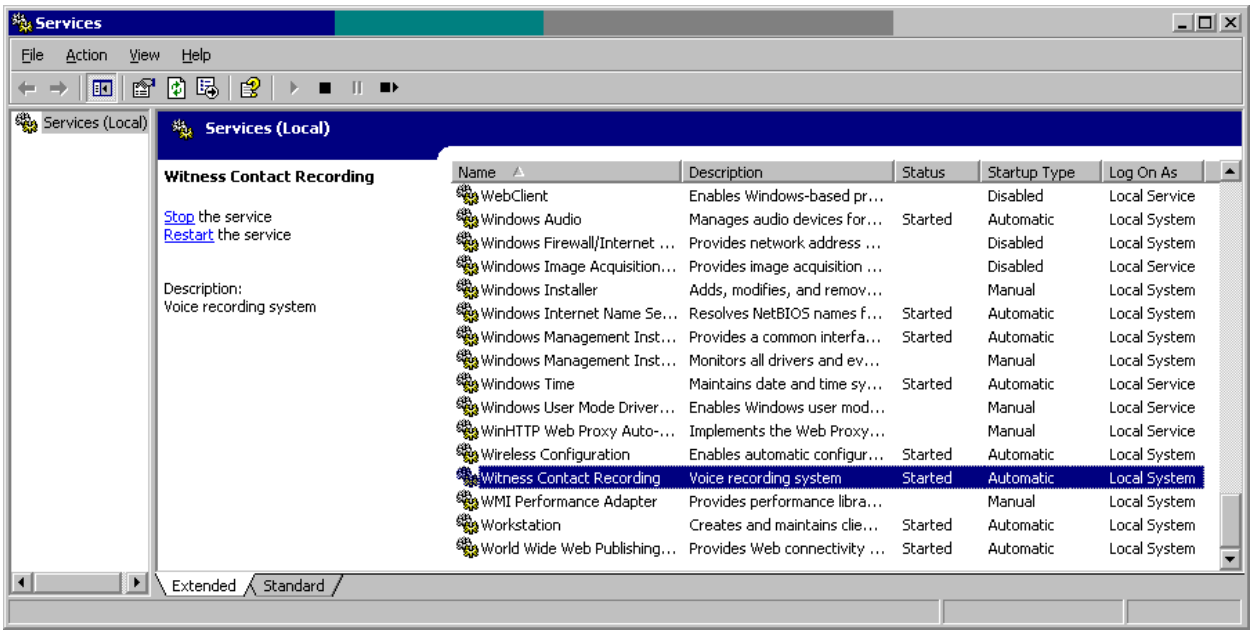
The following screen shows the User configuration window. Configure the following fields:

- Username
- Is allowed to replay calls owned by

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



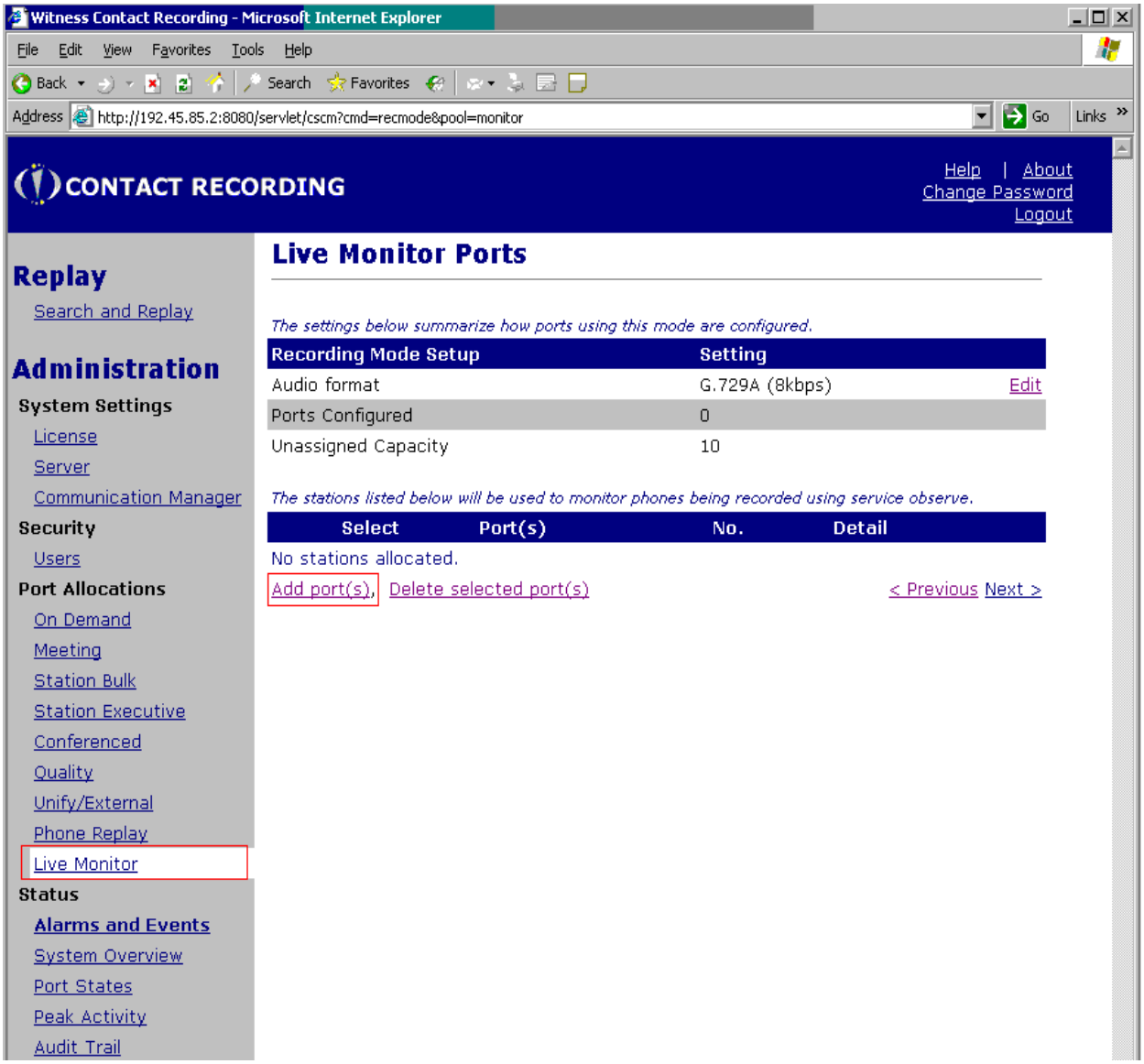
Restart the service of Witness Compliance Package.



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.

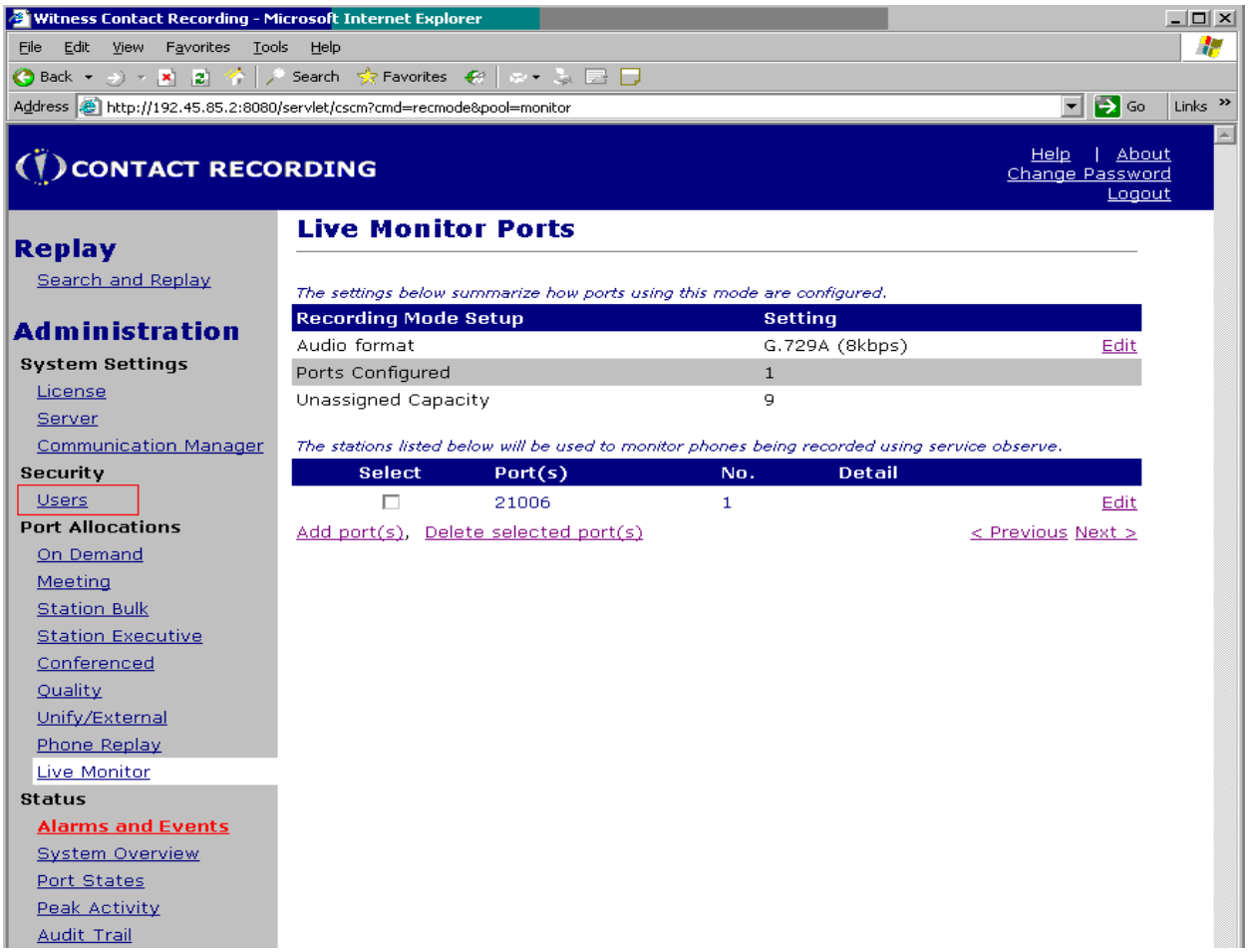
5.7. Configure Live Monitor

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)**.

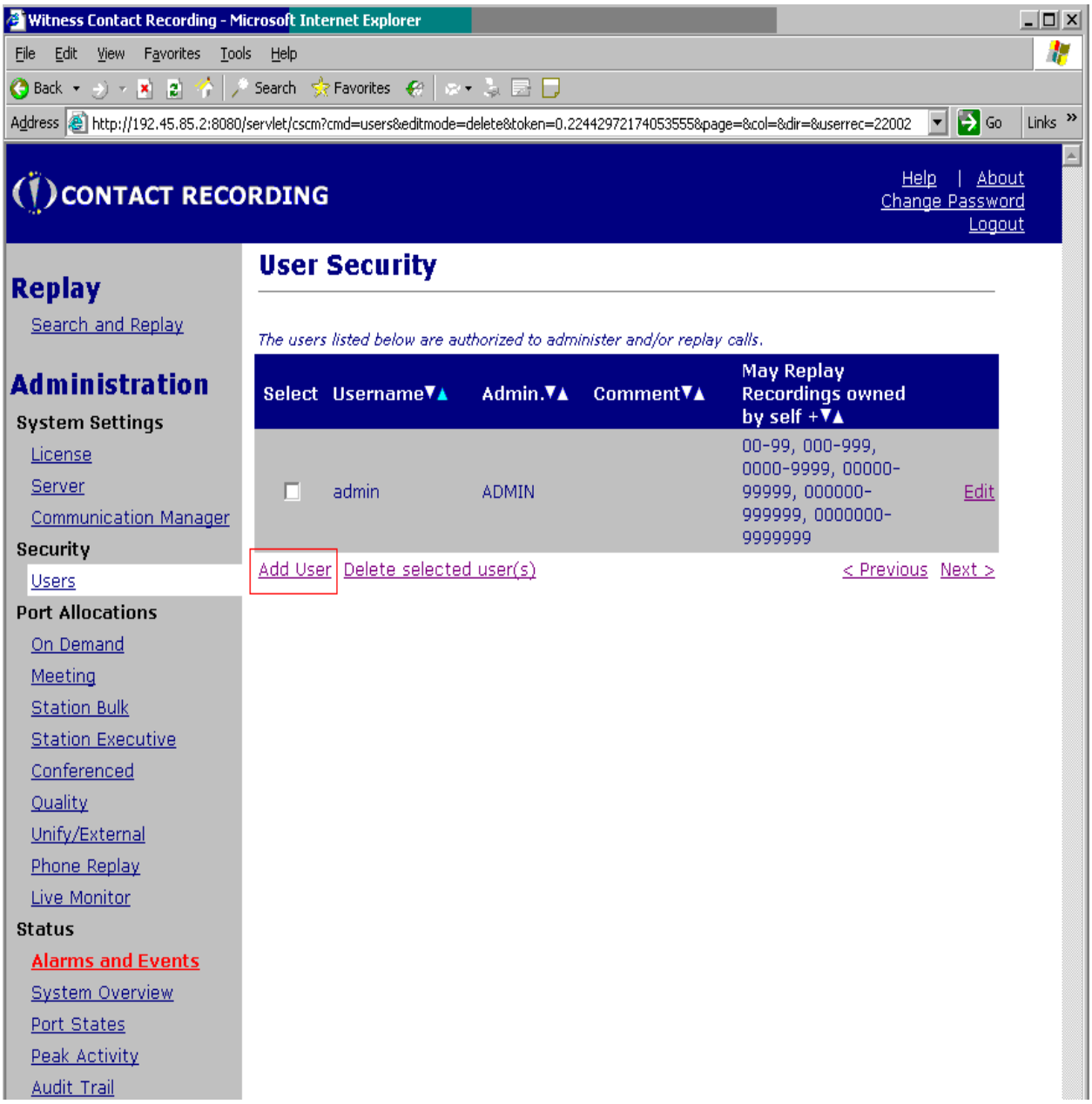


Add recording station(s), and click on **Enter**. This station will be utilized by a user (monitor station).

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.



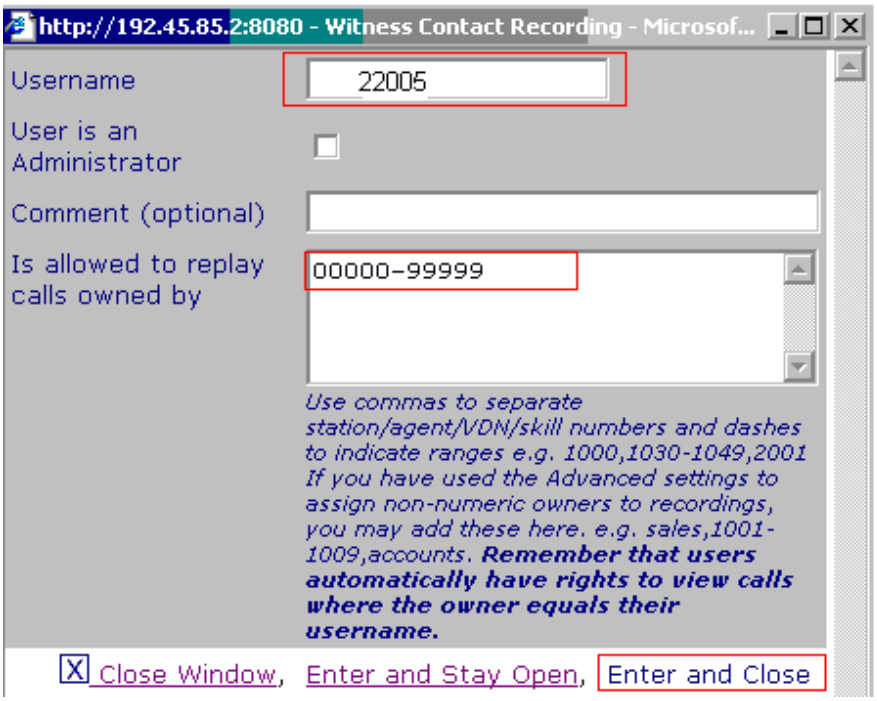
The following screen shows the User Security page. Add a user by clicking on **Add User.**



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

- Username [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.



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

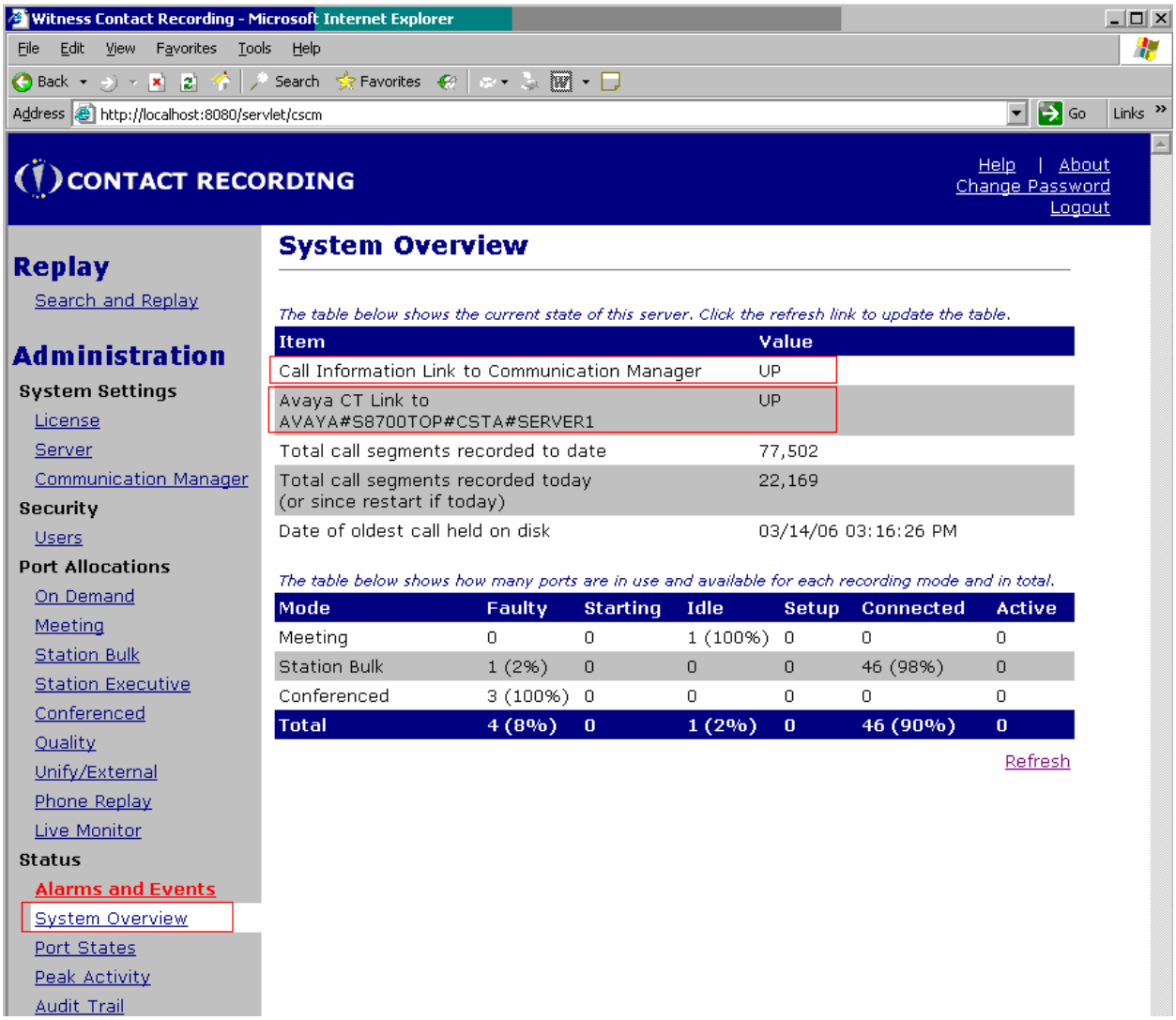
All executed test cases passed. The Compliance Package successfully recorded calls including intra-switch calls, inbound / outbound PSTN trunk calls, inbound/outbound inter-switch IP trunk calls, transferred calls, and conference calls. For serviceability testing, the Compliance Package

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.

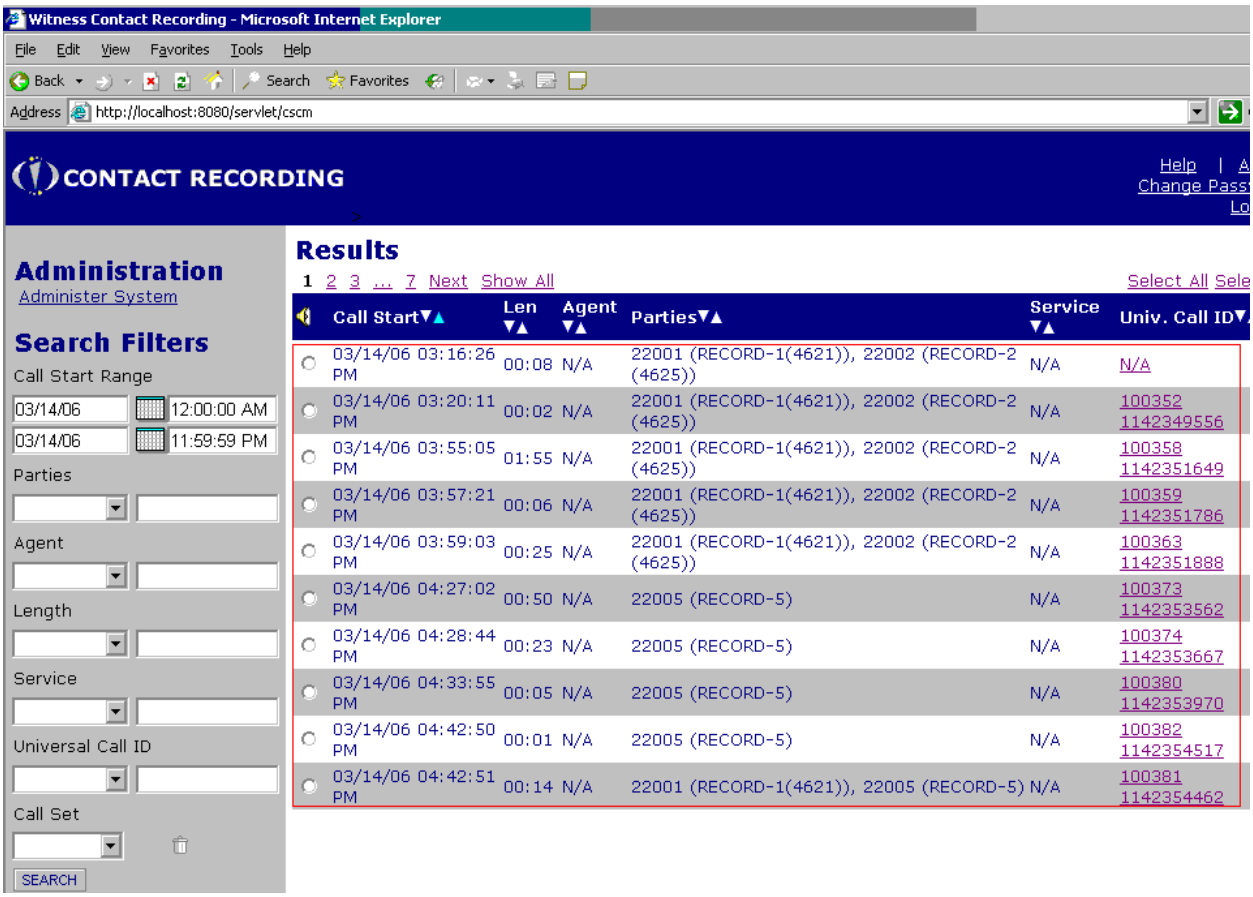
7. Verification Steps

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**



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



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

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.