Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Newfound Communications IP Call Recorder with Avaya Aura™ SIP Enablement Services, Avaya Aura™ Application Enablement Services, and Avaya Aura™ Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Newfound Communications IP Call Recorder to interoperate with Avaya Aura™ SIP Enablement Services, Avaya Aura™ Application Enablement Services, and Avaya Aura™ Communication Manager.

The Newfound Communications IP Call Recorder is a SIP-based IP call recording solution that provides recording capabilities to VoiceXML applications running on a VoiceXML platform. The IP Call Recorder runs on the Newfound VoIP Media Gateway (VMG). A VoiceXML platform is provided as part of the VMG or a customer provided platform could be used. The function of the VoiceXML application is customer-specific but often provides an IVR menu for inbound calls to the enterprise. For the purposes of the compliance test, a demo VoiceXML IVR application provided by Newfound was used to exercise specific SIP call flows and recording capabilities. The IP Call Recorder can record any portion of an active call even after it is transferred to another party.

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

1. Introduction

These Application Notes describe the procedure for configuring the Newfound Communications IP Call Recorder to interoperate with Avaya Aura^{TM} SIP Enablement Services, Avaya Aura^{TM} Application Enablement Services, and Avaya Aura^{TM} Communication Manager.

The Newfound Communications IP Call Recorder is a SIP-based IP call recording solution that provides recording capabilities to VoiceXML applications running on a VoiceXML platform. The IP Call Recorder runs on the Newfound VoIP Media Gateway (VMG). A VoiceXML platform is provided as part of the VMG or a customer provided platform could be used. The function of the VoiceXML application is customer-specific but often provides an IVR menu for inbound calls to the enterprise.

The IP Call Recorder has two modes for recording calls. The first mode known as full call recording will record all calls all the time. It is enabled through configuration. The second mode is known as ad-hoc recording which allows the VoiceXML application to control the starting and stopping of the recording. Any portion of a call can be recorded and depending on the format used, one direction of the call can be recorded on the right stereo channel and the other direction can be recorded on the left stereo channel.

IP Call Record utilized Avaya Aura^{TM} Application Enablement Services JTAPI API to collect call events, such as DNIS, ANI, and call duration.

1.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance testing was primarily on verifying the interoperability between Newfound Communications IP Call Recorder, Avaya Aura^{TM} SIP Enablement Services, Avaya Aura^{TM} Application Enablement Services, and Avaya Aura^{TM} Communication Manager.

1.2. Support

Technical support for the Newfound Communications IP Call Recorder solution can be obtained by contacting Newfound Communications:

- URL – www.newfoundcomm.net
- Phone – 86newfound

2. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a SIP Enablement Services server and Communication Manager running on Avaya S8720 Servers with a G650 Media Gateway. The VMG contains software component including the IP Call Recorder, VoiceXML platform and VoiceXML application. Endpoints include Avaya 9600 Series SIP IP Telephones, Avaya 9600 Series H.323 IP Telephones, and an Avaya 6408D Digital Telephone. An Avaya S8300 Server with an Avaya G450 Media Gateway was included in the test to provide an inter-switch scenario.

The VMG does not register with SIP Enablement Services as an endpoint but instead is configured as a trusted host. Address Maps are configured on SIP Enablement Services to route calls between SIP Enablement Services and the VMG.

For interoperability, the IP Call Recorder requires the use of the G.711mu codec, and transmission of DTMF tones using RFC2833. In addition, the Direct IP-IP Audio feature (also know as media shuffling) must be disabled. This is due to an incompatibility in the way this feature is implemented between the Newfound and Avaya products.

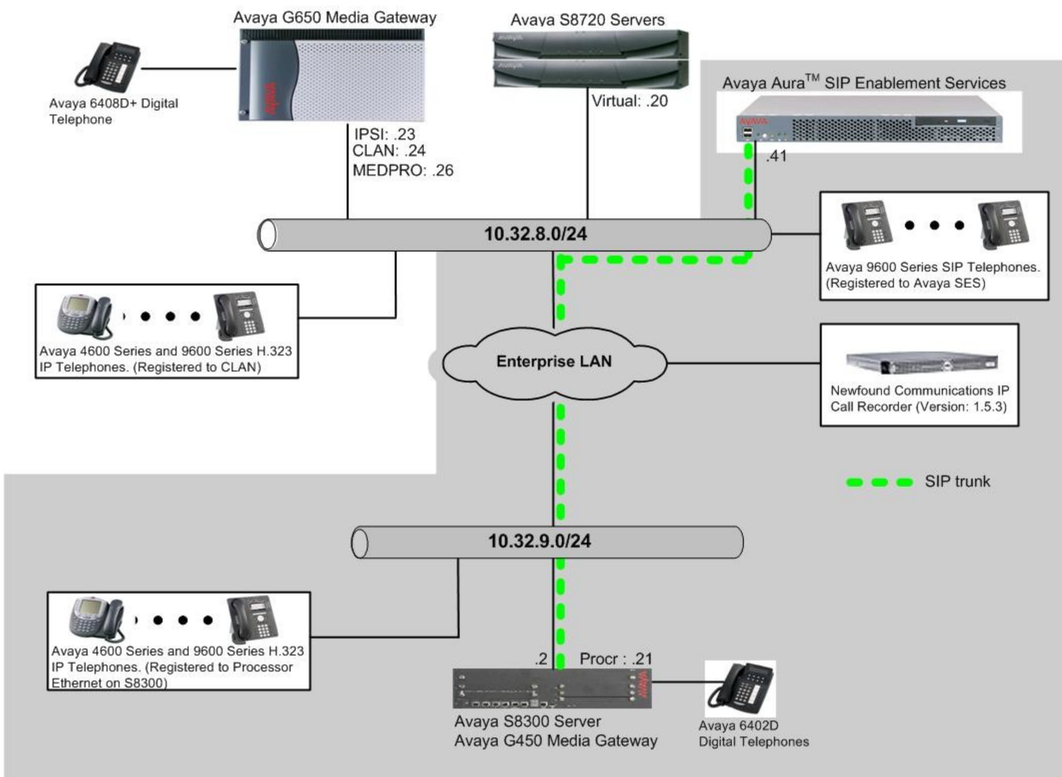


Figure 1: IP Call Recorder Test Configuration

3. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Servers		Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface TN799DP C-LAN Interface TN2302AP IP Media Processor	HW11 FW044 HW01 FW028 HW20 FW118
Avaya S8300 Server with Avaya G450 Media Gateway		Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya Aura™ SIP Enablement Services		5.2 (R015x.02.0.947.3) with Service Pack SES-02.0.947.3-SP2a
Avaya Aura™ Application Enablement Services		4.2
Avaya 4600 and 9600 Series SIP Telephones		
	9620 (SIP) 9630 (SIP) 9650 (SIP)	2.0.5 2.0.5 2.0.5
Avaya 4600 and 9600 Series IP Telephones		
	4625 (H.323) 9630 (H.323) 9650 (H.323)	2.9 3.002 3.002
Avaya 6408D+ Digital Telephone		-
Newfound IP Call Recorder		1.5.3

4. Configure Avaya Aura™ Communication Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and SES. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. The VMG and other SIP telephones are configured as off-PBX telephones in Communication Manager.

4.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses. If not, contact an authorized Avaya account representative to obtain additional licenses

```
display system-parameters customer-options                      Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V15                              Software Package: Standard
       Location: 1                             RFA System ID (SID): 1
       Platform: 6                             RFA Module ID (MID): 1

                                                                 USED
                                Platform Maximum Ports: 44000 254
                                      Maximum Stations: 36000 118
                              Maximum XMOBILE Stations: 0     0
                    Maximum Off-PBX Telephones - EC500: 50    1
                    Maximum Off-PBX Telephones -   OPS: 100   7
                    Maximum Off-PBX Telephones - PBFMC: 0     0
                    Maximum Off-PBX Telephones - PVFMC: 0     0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                               USED
                     Maximum Administered H.323 Trunks: 100   39
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 5     0
                  Maximum Video Capable H.323 Stations: 5     0
                   Maximum Video Capable IP Softphones: 5     0
                       Maximum Administered SIP Trunks: 100   40
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

4.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and SES. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 4.3** for configuring IP network region to specify which codec sets may be used within and between network regions.

```
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          2        20
```

4.3. Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and SES. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- Authoritative Domain –Set to the appropriate domain. During the compliance test, the authoritative domain is set to **testroom.avaya.com**. This should match the SIP Domain value on SES, in **Section 5.1**.
- Intra-region IP-IP Direct Audio – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or SES in the same IP network region. The default value for this field is **yes**.
- Codec Set – Set the codec set number as provisioned in **Section 4.2**.
- Inter-region IP-IP Direct Audio – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or SES in different IP network regions. The default value for this field is **yes**.

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

4.4. Configure IP Node Name

This section describes the steps for setting IP node name for SES in Communication Manager. Enter the **change node-names ip** command, and add a node name for SES along with its IP address.

```
change node-names ip                                                Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
CLAN                    10.32.8.24
CLAN-AES                10.32.8.25
G450                    10.32.9.21
MEDPRO                  10.32.8.26
SES                     10.32.8.41
VAL                     10.32.8.45
default                 0.0.0.0
```

4.5. Configure SIP Signaling Group

This section describes the steps for administering a signaling group in Communication Manager for signaling between Communication Manager and SES. Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- Group Type – Set to **sip**.
- Transport Method – Set to **tls** (Transport Layer Security).
- Near-end Node Name - Set to **CLAN** as displayed in **Section 4.4**.
- Far-end Node Name - Set to the SES name configured in **Section 4.4**.
- Far-end Network Region - Set to the region configured in **Section 4.3**.
- Far-end Domain - Set to **testroom.avaya.com**. This should match the SIP Domain value in **Section 5.1**.
- Direct IP-IP Audio Connections –Set to **n**, since the shuffling is disabled during the compliance test.

The screenshot below shows the signaling group that was added for the compliance test.

```
change signaling-group 201                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 201              Group Type: sip
                          Transport Method: tls
  IMS Enabled? n




   Near-end Node Name: CLAN                       Far-end Node Name: SES
 Near-end Listen Port: 5061                     Far-end Listen Port: 5061
                                             Far-end Network Region: 1
Far-end Domain: testroom.avaya.com

                                                  Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                       RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload                 Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                          IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                                       Alternate Route Timer(sec): 6
```

4.6. Configure SIP Trunk

This section describes the steps for administering a trunk group in Communication Manager for trunking between Communication Manager and SES. Enter the **add trunk-group <t>** command, where **t** is an unallocated trunk group and configure the following:

- Group Type – Set the Group Type field to **sip**.
- Group Name – Enter a descriptive name.
- TAC (Trunk Access Code) – Set to any available trunk access code.
- Service Type – Set the Service Type field to **tie**.
- Signaling Group – Set to the Group Number field value configured in **Section 4.5**.
- Number of Members – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

Note: *Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunk members for the duration of the call. The license file installed on the system controls the maximum permitted*

```
add trunk-group 201                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 201                  Group Type: sip          CDR Reports: y
  Group Name: to SIP                      COR: 1        TN: 1        TAC: 116
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                     Signaling Group: 201
                                                   Number of Members: 10
```

4.7. Configure SIP Endpoint

This section describes the steps for administering OPS stations in Communication Manager and associating the OPS station extensions with the telephone numbers of Newfound Communication VMG. Enter **add station s**, where **s** is an extension valid in the provisioned dial plan. The following fields were configured for the compliance test.

- Type – Set to **9600SIP**.
- Name – Enter a descriptive name

Repeat this step as necessary to configure additional SIP endpoint extensions.

```
add station 28003                                               Page   1 of   6
                                     STATION

Extension: 28003                        Lock Messages? n               BCC: 0
     Type: 9600SIP                      Security Code:                  TN: 1
     Port: IP                         Coverage Path 1:                 COR: 1
     Name: SIP-28003                  Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 28003
            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? n



                                             Customizable Labels? y
```

Enter the **add off-pbx-telephone station-mapping** command and configure the following:

- Station Extension – Set the extension of the OPS station as configured above.
- Application – Set to **OPS**.
- Phone Number – Enter the number that the VMG will use for registration and call termination. In the example below, the Phone Number is the same as the Station Extension, but is not required to be the same.

- Trunk Selection – Set to the trunk group number configured in **Section 4.6**.
- Config Set – Set to **1**

Repeat this step as necessary to configure additional off-pbx-telephone station-mapping.

```
add off-pbx-telephone station-mapping                          Page   1 of   2
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station          Application Dial   CC  Phone Number       Trunk        Config
 Extension                    Prefix                        Selection    Set
 28003                OPS          -     28003                201          1
```

4.8. Configure Switch Connection and CTI Links between Communication Manager and Application Enablement Services

The AES server forwards CTI requests, responses, and events between the VMG and Communication Manager. The AES server communicates with Communication Manager over a switch connection link. Within the switch connection link, CTI links may be configured to provide CTI services to CTI applications such as the VMG. The following steps demonstrate the configuration of the Communication Manager side of the switch connection and CTI links. See **Section 6** for the details of configuring the AES side of the switch connection and CTI links.

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid extension under the provisioned dial plan in Communication Manager, set the Type field to **ADJ-IP**, and assign a descriptive Name to the CTI link.

```
add cti-link 4                                             Page   1 of   2
                                    CTI LINK
 CTI Link: 4
Extension: 20006
     Type: ADJ-IP
                                                                     COR: 1
     Name: JTAPI
```

4.9. Configure IP Services

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in **Section 4.4**. During the compliance test, the default port was utilized for the Local Port field.

```
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**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname –a**. Enter 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 6.1**.

```
change ip-services                                                 Page    4 of    4
                               AE Services Administration

   Server ID     AE Services         Password             Enabled     Status
                    Server
      1:        server2             xxxxxxxxxxxxxxxx         y           idle
      2:
      3:
```

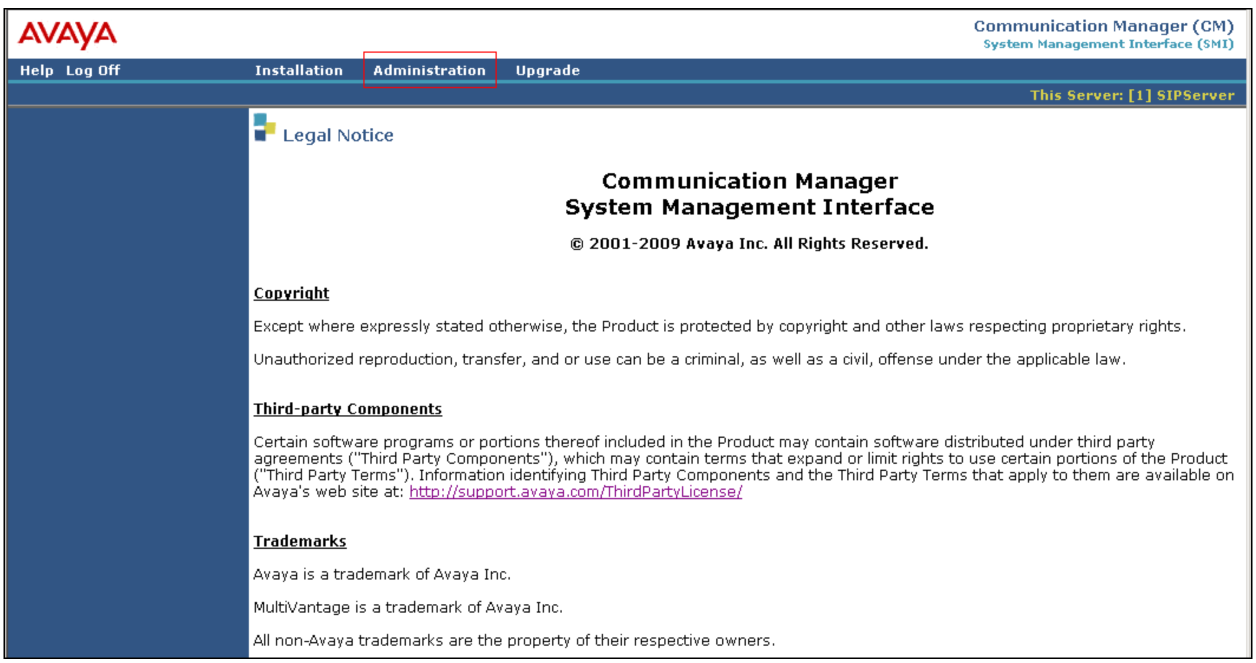
5. Configure Avaya SIP Enablement Services

This section describes the steps for creating a SIP trunk between SES and Communication Manager. SIP user accounts are configured in Avaya SES and associated with a Communication Manager OPS station extension. Newfound Communications IP Call Recorder will register with Avaya SES using the SIP user accounts. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

5.1. Configure SES Server Properties

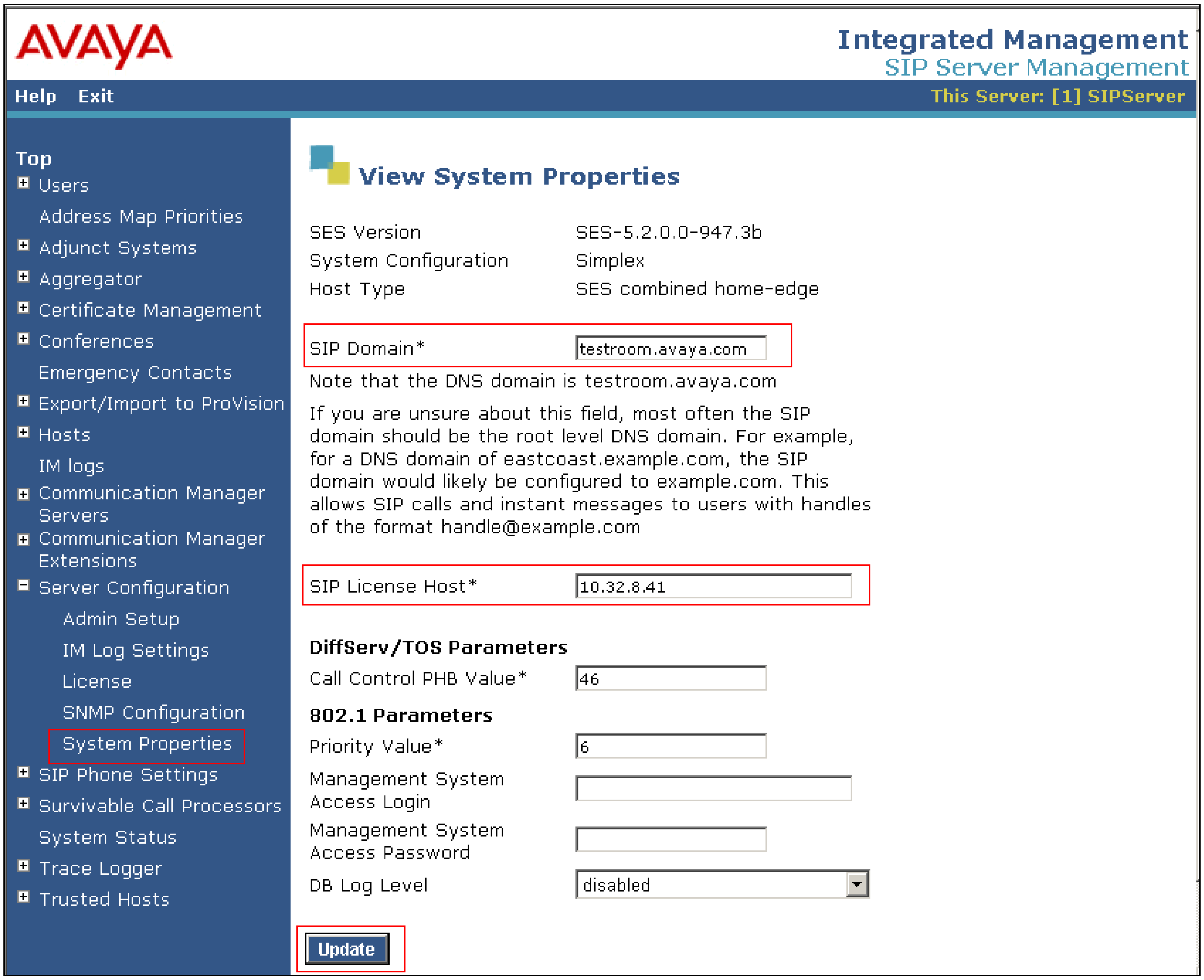
Launch a web browser, enter **https://<IP address of SES server>/admin** in the URL, and log in with the appropriate credentials. Click on the **Launch SES Administration Interface** link upon successful login.

Navigate to **Administration → SIP Enablement Services**.



In the Integrated Management SIP Server Management page, select the **Server Configuration → System properties** link from the left pane of the window. Verify the SIP Domain matches the Far-end Domain field value configured for the signaling group on Communication Manager in **Section 4.5**.

Click on the **Update** button, after the completion.

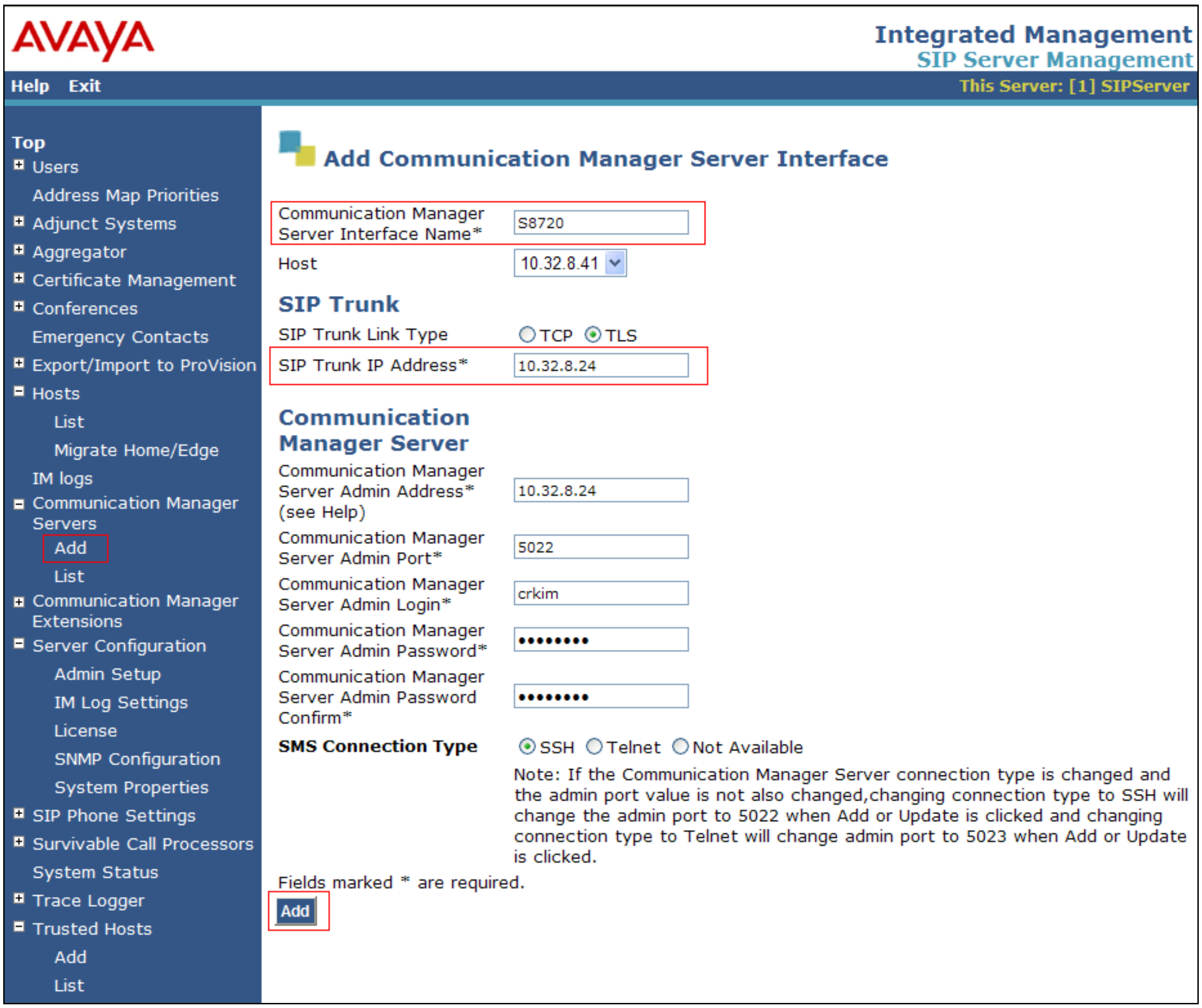


5.2. Configure Communication Manager Server Interface

This section provides steps to add Communication Manager servers to the SIP domain. In the Integrated Management SIP Server Management page, select the **Communication Manager Servers → Add** link from the left pane of the screen. The following screen shows the Add Communication Manager Server Interface page. The highlighted fields were configured for the compliance test:

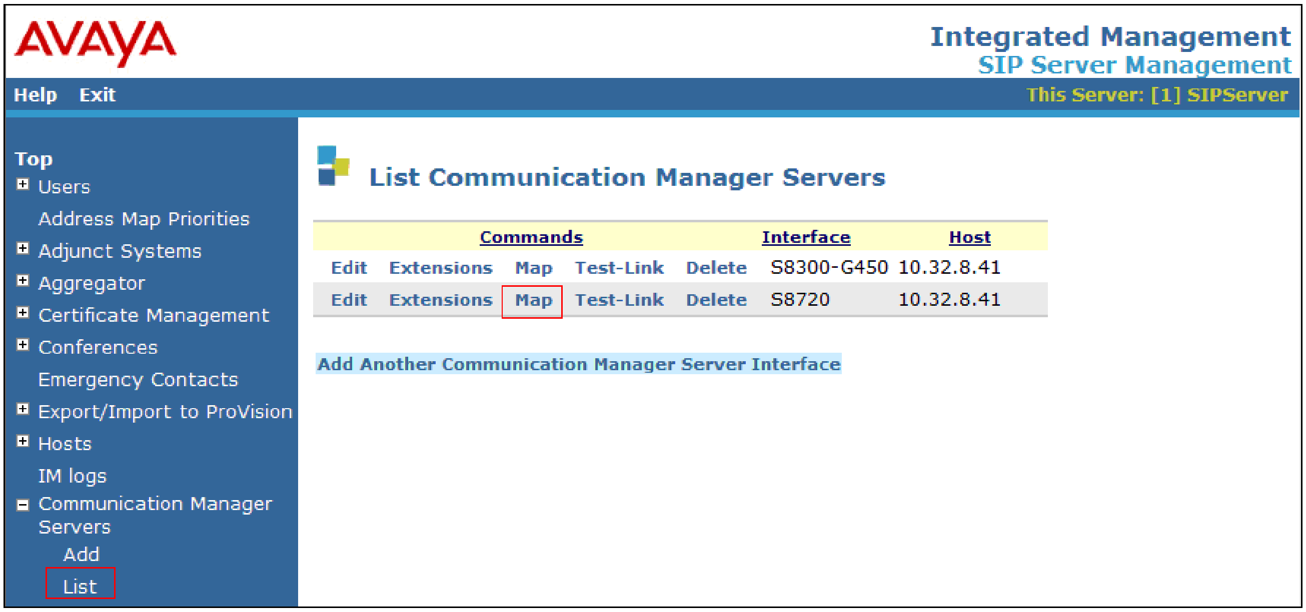
- Communication Manager Server Interface Name – Enter a descriptive name for the communication manager server interface.
- SIP Trunk IP Address – Enter the IP address for the CLAN that terminates the SIP link from SES. The CLAN IP address is included in the IP NODE NAMES form in **Section 4.4**.

Click **Add** when finished.



A Communication Manager Server Address Map is required on the SES to direct calls inbound to Communication Manager in the same way that outbound calls from Communication Manager require a Host Address Map.

To configure a Communication Manager Server Address Map, select **Communication Manage Servers → List**. This will display the List Communication Manager Servers page below. Click on the **Map** link associated with the appropriate Communication Manager server to display the List Communcation Manager Server Address Map page.

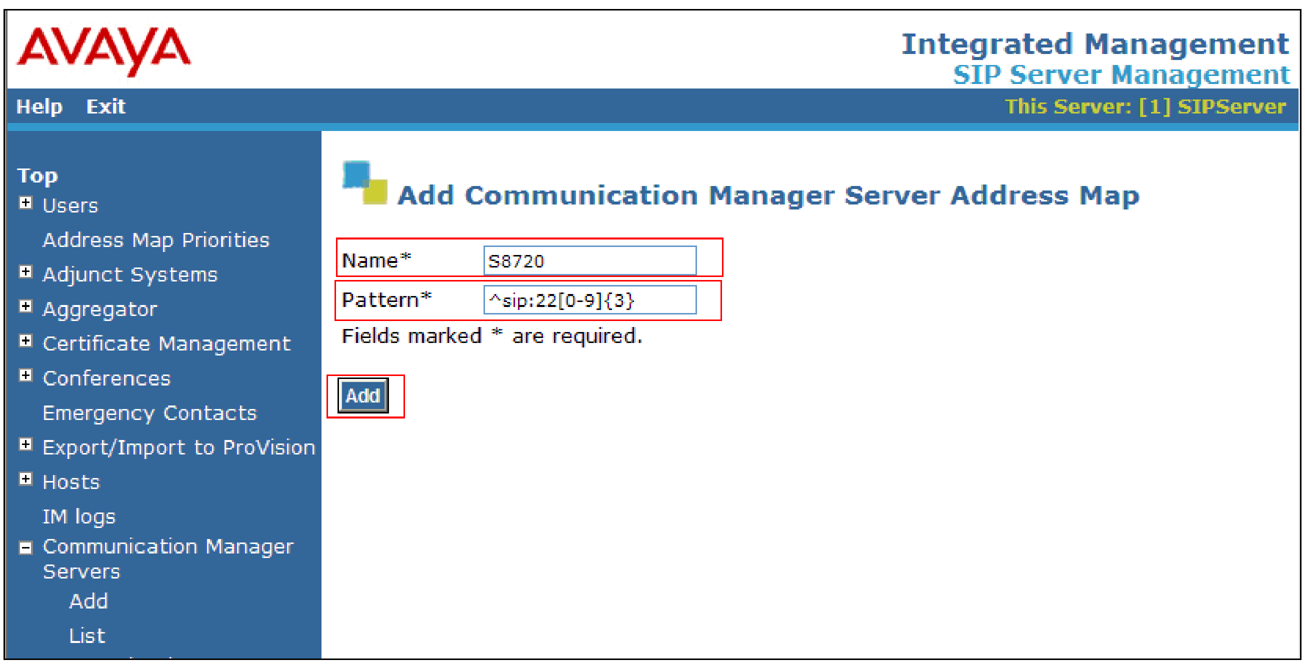


On the List Communication Manager Server Address Map page, click on the **Add Map In New Group** link.

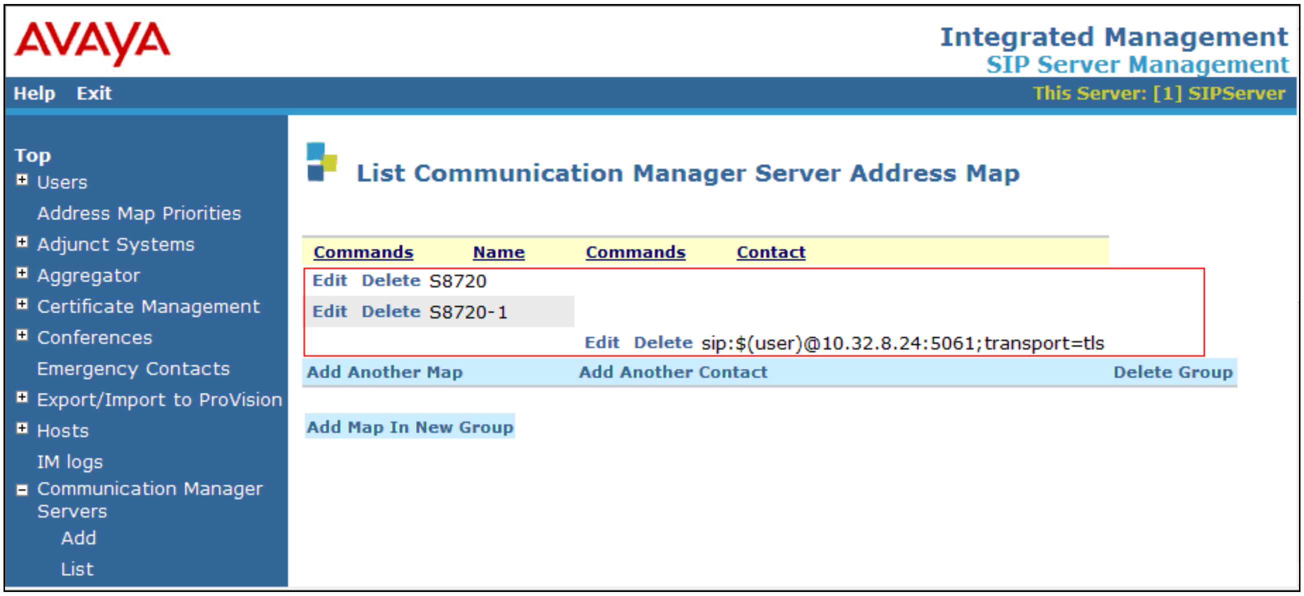
On the Add Communication Manager Server Address Map page, provide the following information:

- Enter a descriptive name in the Name field.
- In the Pattern field, enter an expression to define the matching criteria for calls to be routed from the demo VoiceXML application to Communication Manager. The example below shows the expression used in the compliance test. This expression will match any URI that begins with ***sip:22*** followed by any digit between ***0-9*** for the next ***3*** digits.

Click the **Add** button.



After configuring the Communication Manager Server Address Map, the List Communication Manager Server Address Map page appears as shown below. The first Communication Manager Contact is created automatically and directs the calls to the IP address of the Communication Manager (*10.32.8.24*) using port 5061 and TLS as the transport protocol. The user portion in the original request URI is substituted for "$(user)". For the compliance test, the Contact field for the Communication Manager Server Address Map is displayed as:
sip:$(user)@10.32.8.24;transport=tls



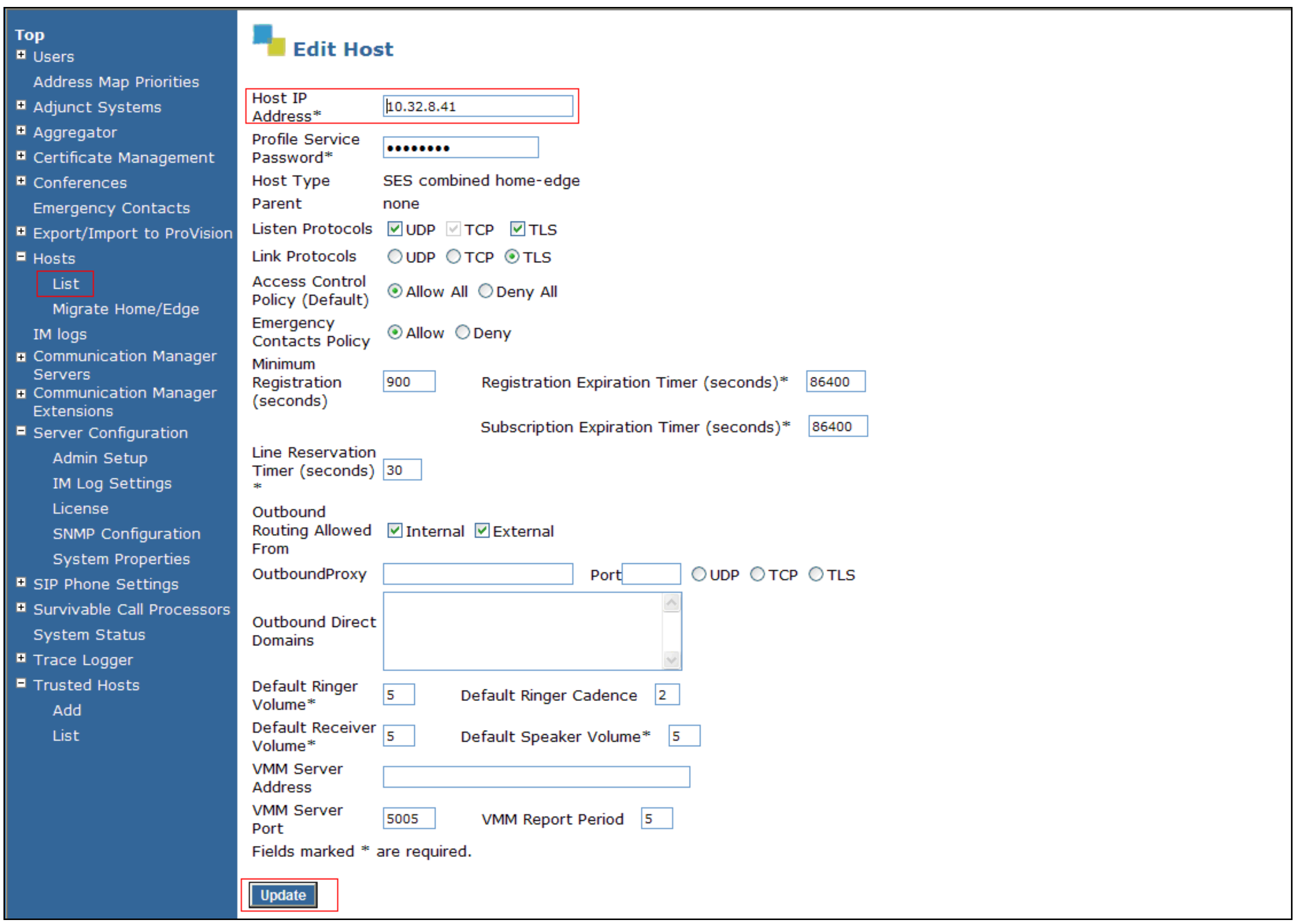
5.3. Configure Host

After verifying the domain on the View System Properties page in **Section 5.1**, verify the host computer entry for SES. The following example shows the Edit Host page since the host had already been added to the system.

The Edit Host page shown below is accessible by clicking on the **Hosts → List** link in the left pane and then clicking on the **Edit** link under the **Commands** section of the subsequent page that is displayed (but not shown).

- In the Host IP Address field, verify the IP address of the SES server.
- Although the field is hidden, the DB Password will reflect the value that was specified during the system installation.
- The Profile Service Password field will also reflect the value that was specified during the system installation.
- Since only one Avaya SES is used in the configuration, the Host Type will be set to **SES combined home-edge**.

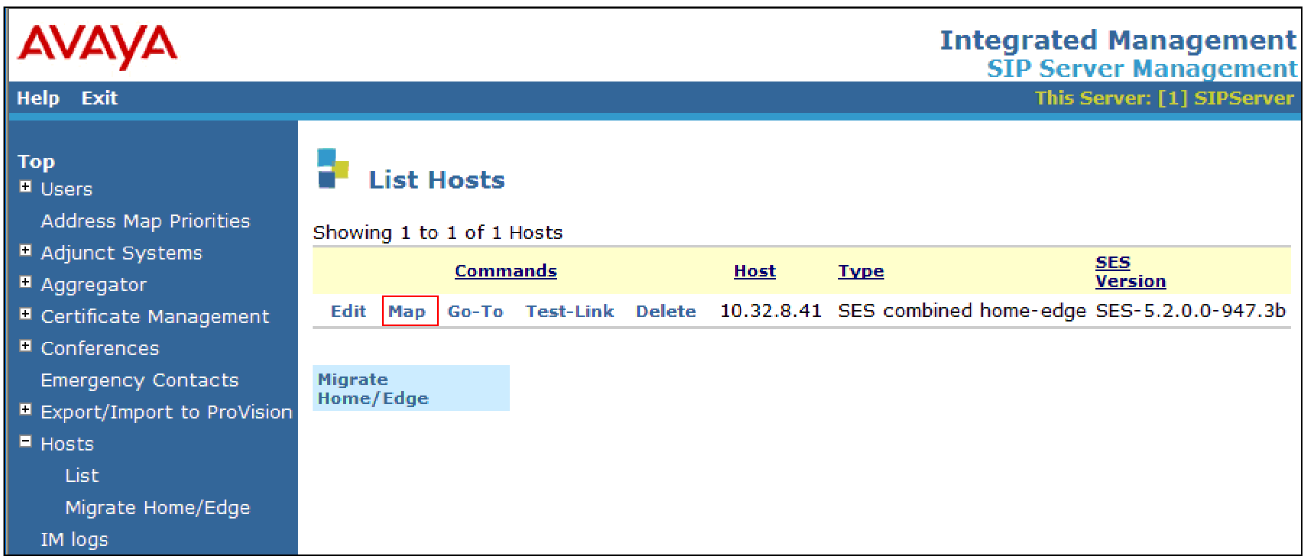
If any changes were made, scroll down to the bottom of the page and click the **Update** button.



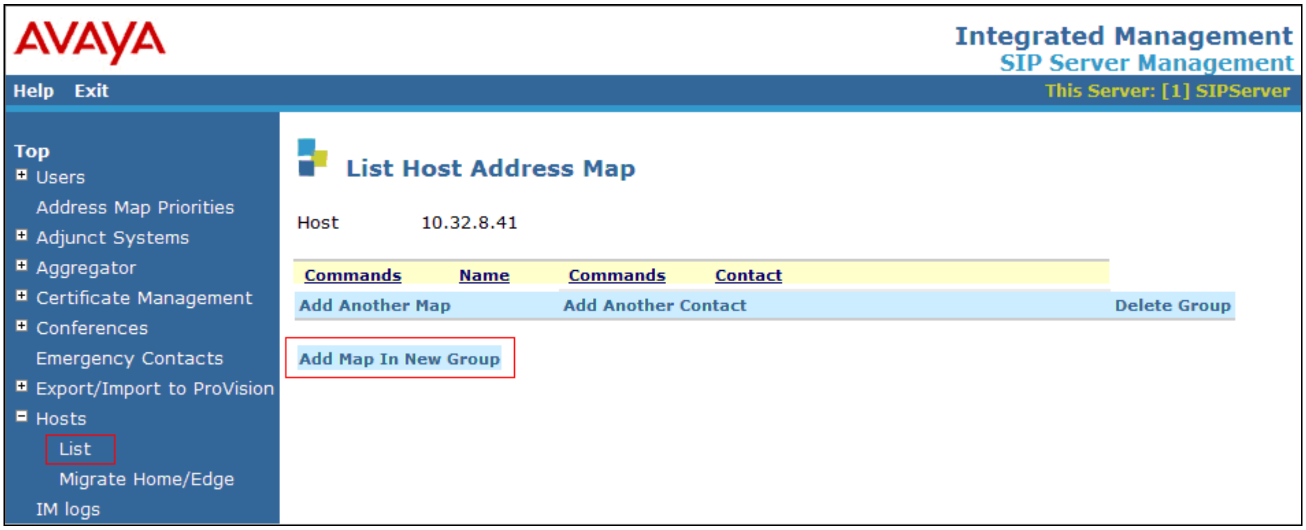
A Host Address Map is required on SES to direct calls outbound from Communication Manager to the VMG. The VMG does not register as an endpoint with SES so calls are not automatically routed to the VMG based on a registered extension. Instead, a Host Address Map is used to route calls based on the contents of the SIP INVITE URI matching a specified pattern to determine the proper destination of the call. The URI takes the form of *sip:user@domain*, where *domain* can be a domain name or an IP address. The user portion can be an alpha-numeric name, telephone number or extension.

In the case of the compliance test, the user portion contained the called party number. Calls with a called party number of 28009 were routed to the VMG. Thus, the Host Address Map was configured to match all calls dialing 28009.

To configure a Host Address Map, expand the **Hosts** option in the left pane, and select **List**. This will display the List Hosts page below. Click on the **Map** link to display the List Host Address Map page.



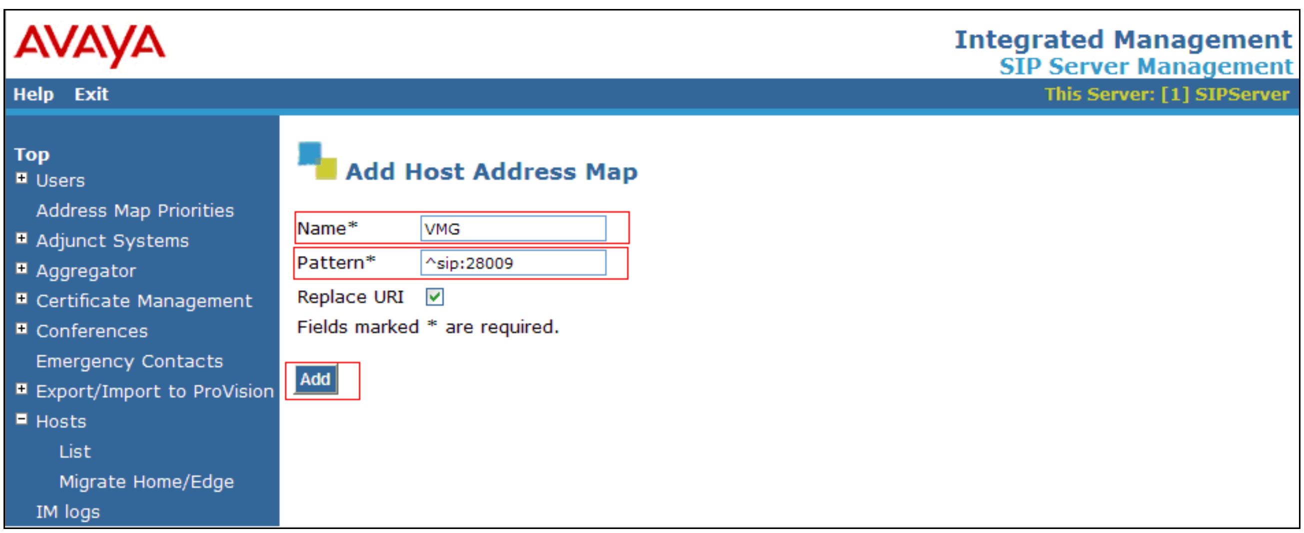
On the List Host Address Map page, click on the **Add Map In New Group** link.



On the Add Host Address Map page, provide the following information:

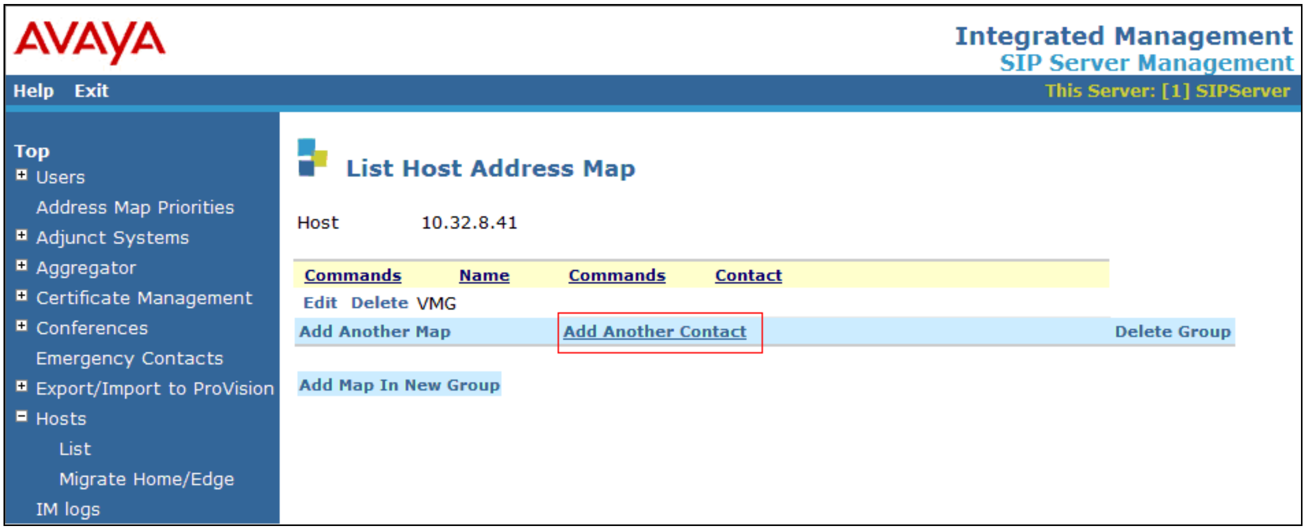
- Enter a descriptive name in the Name field.
- In the Pattern field, enter an expression to define the matching criteria for calls to be routed to the VMG. The example below shows the expression used in the compliance test. This expression will match any URI that begins with ***sip:28009***.

Click the **Add** button.



Next, a Host Contact must be entered for the Address Map that was previously defined. The contact defines the destination IP address, port number and transport protocol to use when routing calls that match the Address Map.

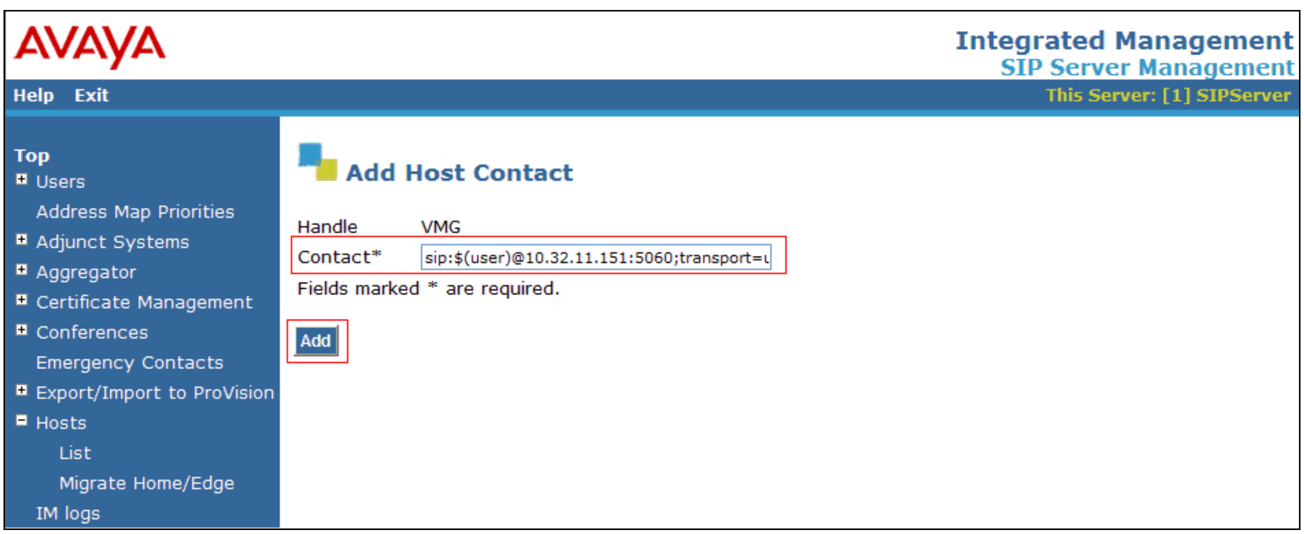
To add a Host Contact, click on the **Add Another Contact** link on the List Host Address Map page to open the Add Host Contact page.



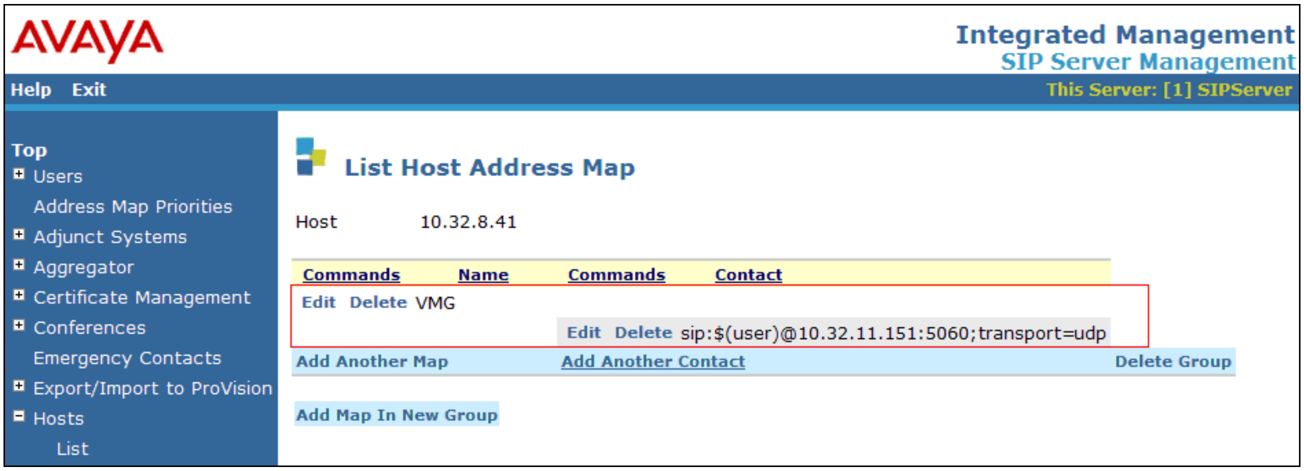
In the Contact field, enter the destination IP address (***ip_addr***), port number (***port***) and transport protocol (***protocol***). For the compliance test, the VMG had IP address of 10.32.11.151. Thus, the following contact value was used:

- **sip:$(user)@10.32.11.151:5060;transport=udp**

Click the **Add** button.



After configuring the Host Address Map and Contact, the List Host Address Map page will appear as shown below.

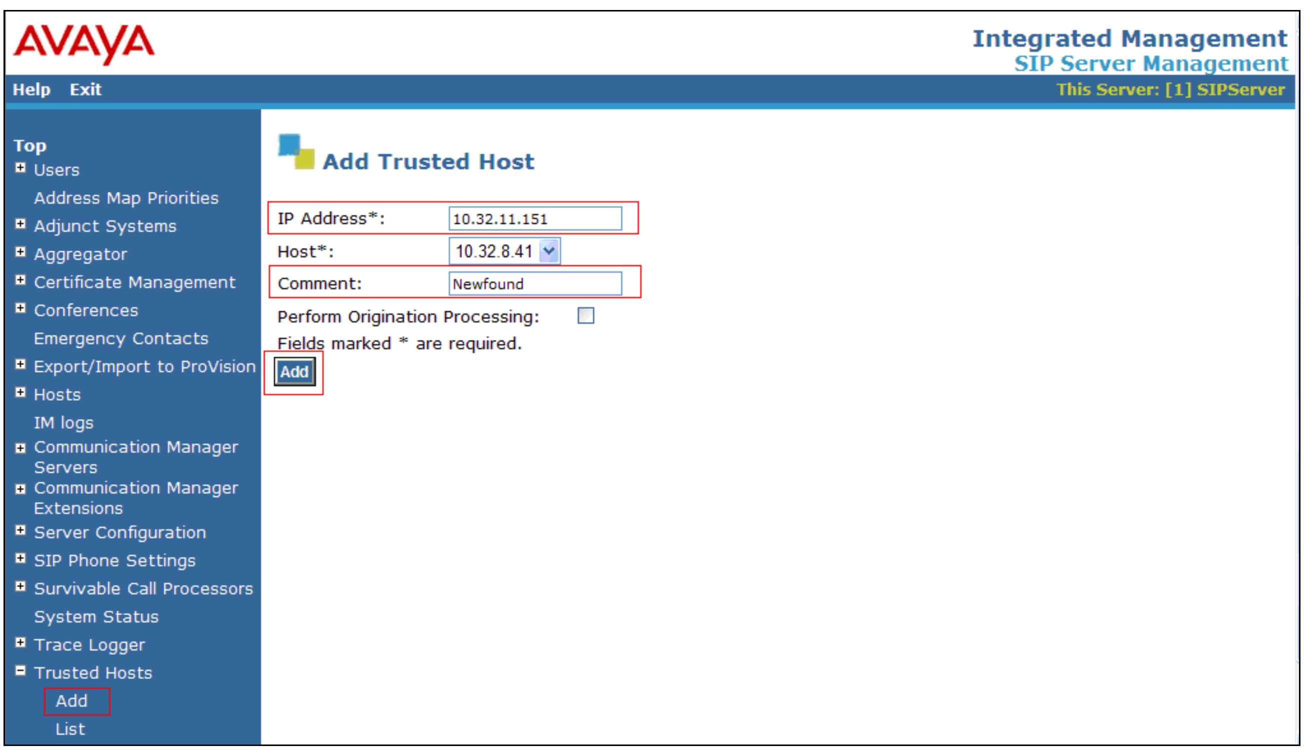


5.4. Trusted Hosts

Lastly, the IP address of the VMG must be configured as a trusted host on SES. As a trusted host, Avaya SES will not issue SIP authentication challenges for incoming requests from the designated IP address. To configure a trusted host, Navigate to **Trusted Hosts → Add**. On the Add Trusted Host page, provide the following information:

- In the IP address field, enter the IP address of the VMG.
- Enter a description of the trusted host in the Comment field.

Click the **Add** button.



6. Configure Avaya Application Enablement Services

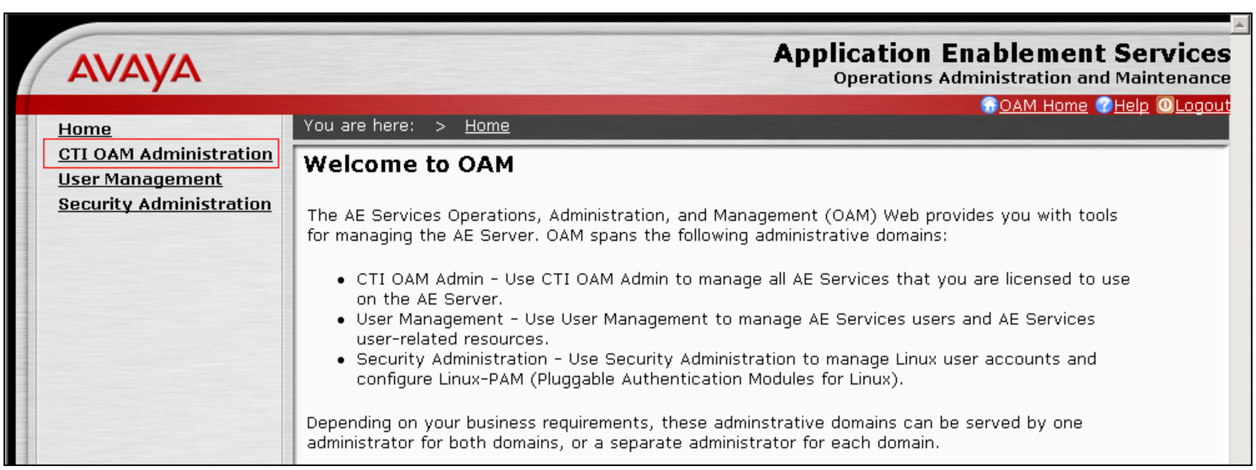
The AES server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager. The AES server receives requests from CTI applications, and forwards them to Communication Manager. Conversely, the AES server receives responses and events from Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI link for JTAP, and creating a CTI user.

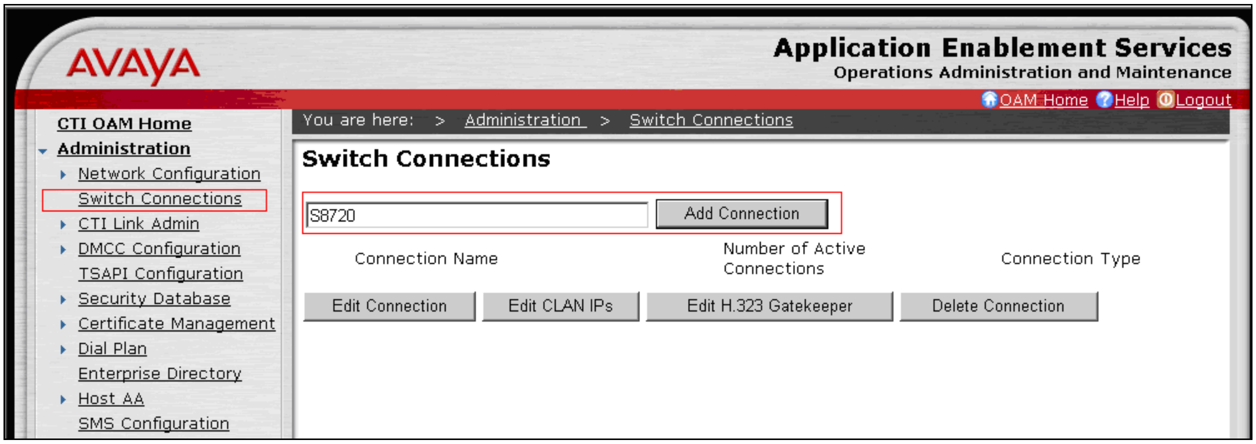
6.1. Configure Switch Connection

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

Select the **CTI OAM Administration** link from the left pane of the screen.



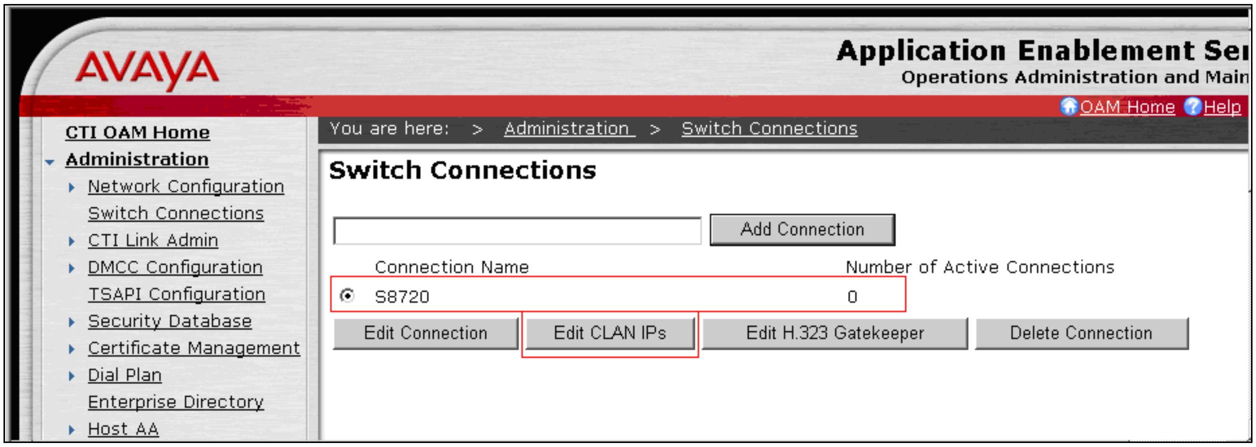
Click on **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between AES and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



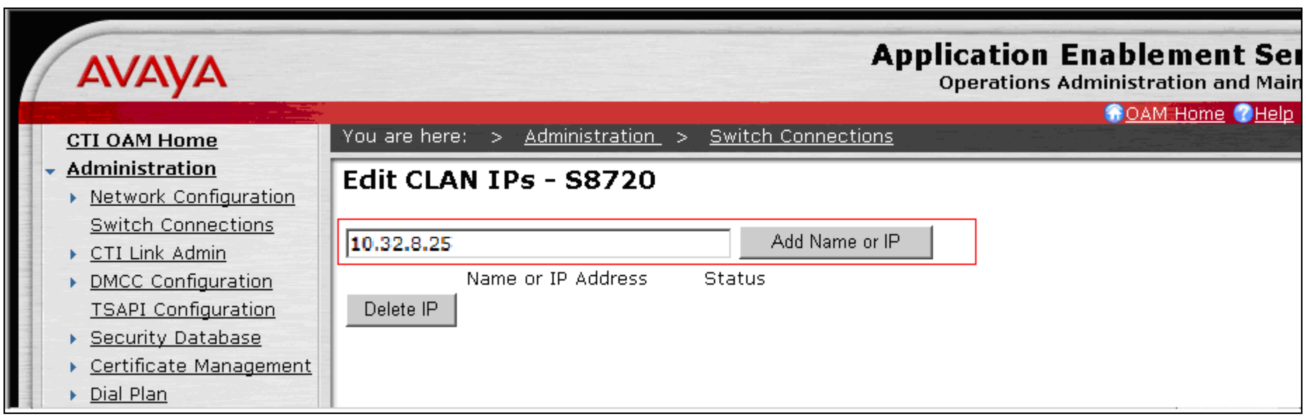
The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Communication Manager in **Section 4.9**.

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**.

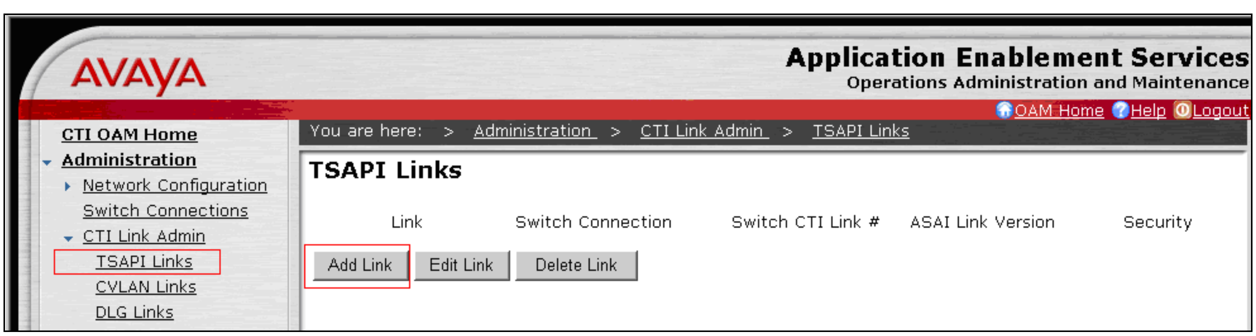


Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 4.4** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

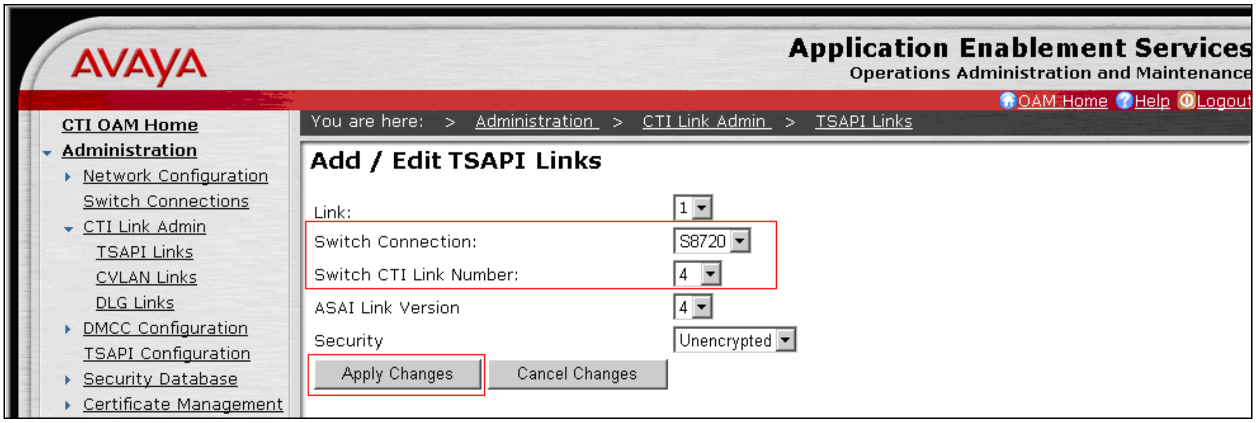


6.2. Configure the JTAPI CTI link

Navigate to **Administration → CTI Link Admin → TSAPI Links** in the left pane, and click on the **Add Link** button to create a JTAPI CTI link.



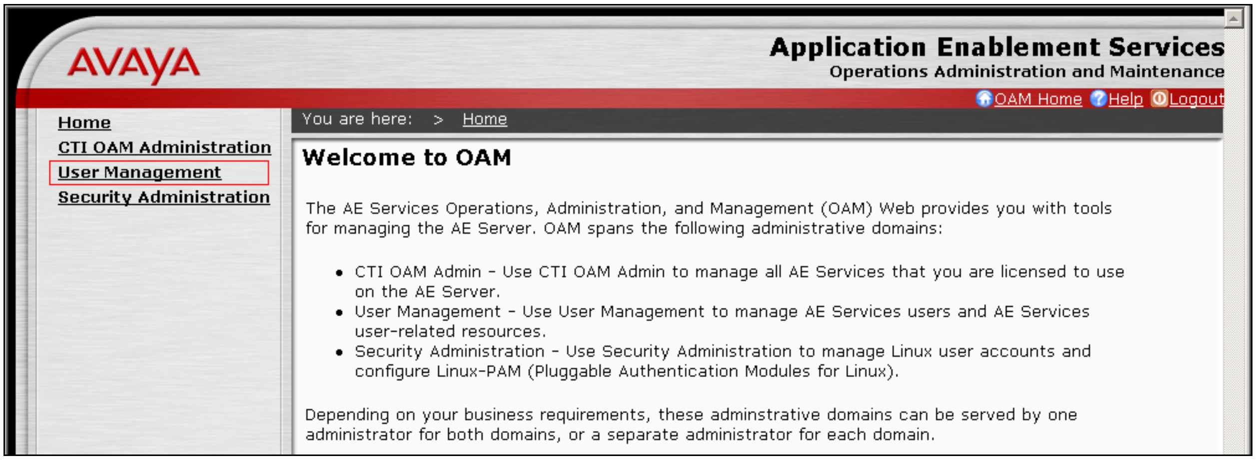
Select a Switch Connection using the drop down menu. The Switch Connection is configured in **Section 6.1**. Select the Switch CTI Link Number using the drop down menu. Switch CTI Link Number should match with the number configured in the CTI LINK form **in Section 4.8**. Click the **Apply Changes** button.



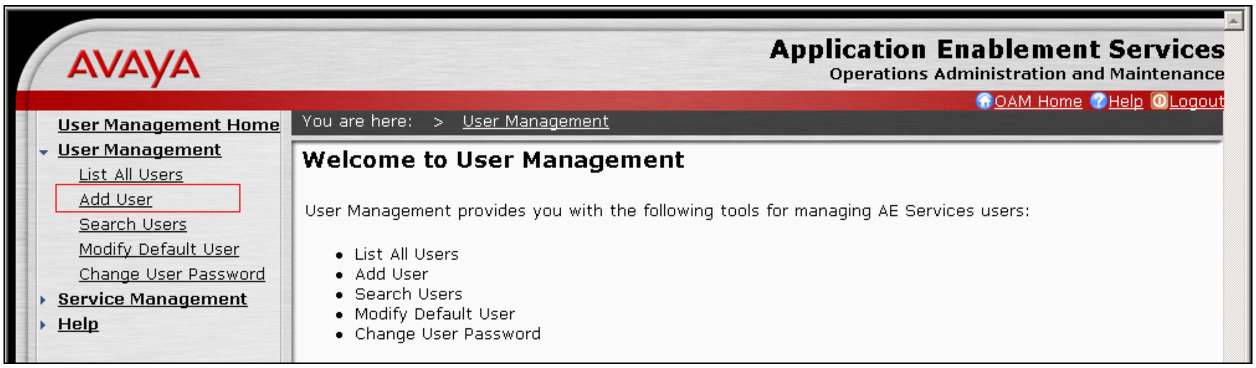
6.3. Configure the CTI Users

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter http://<IP address of AES server> in the URL, and log in with the appropriate credentials to access the relevant administration pages.

The Welcome to OAM page is displayed next. Select **User Management** from the left pane.



From the Welcome to User Management page, navigate to the **User Management → Add User** page to add a CTI user.

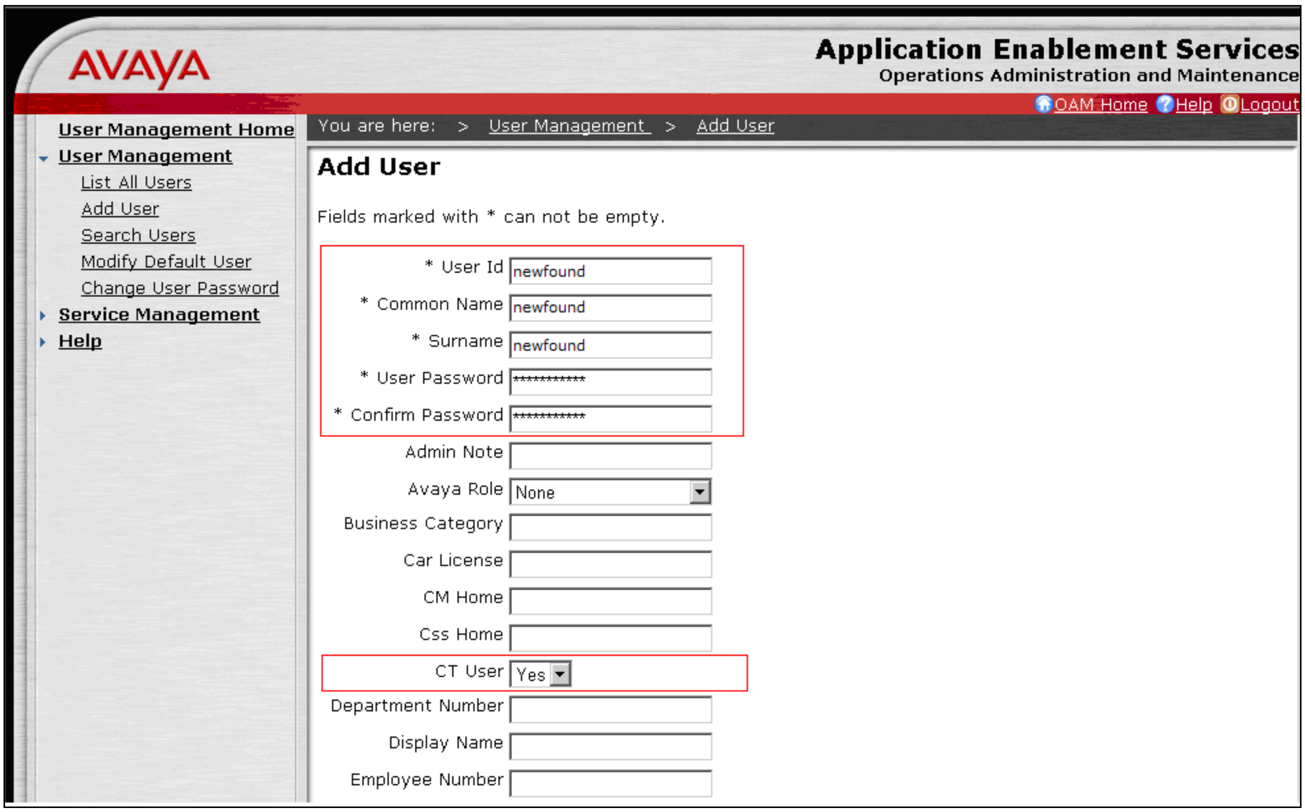


On the Add User page, provide the following information:

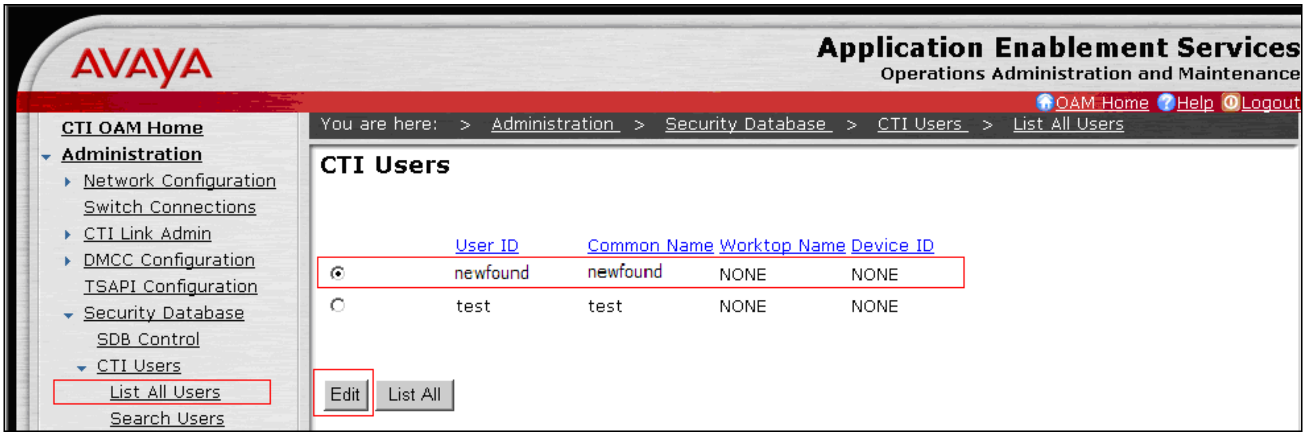
- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the VMG Configuration page in **Section 7**.

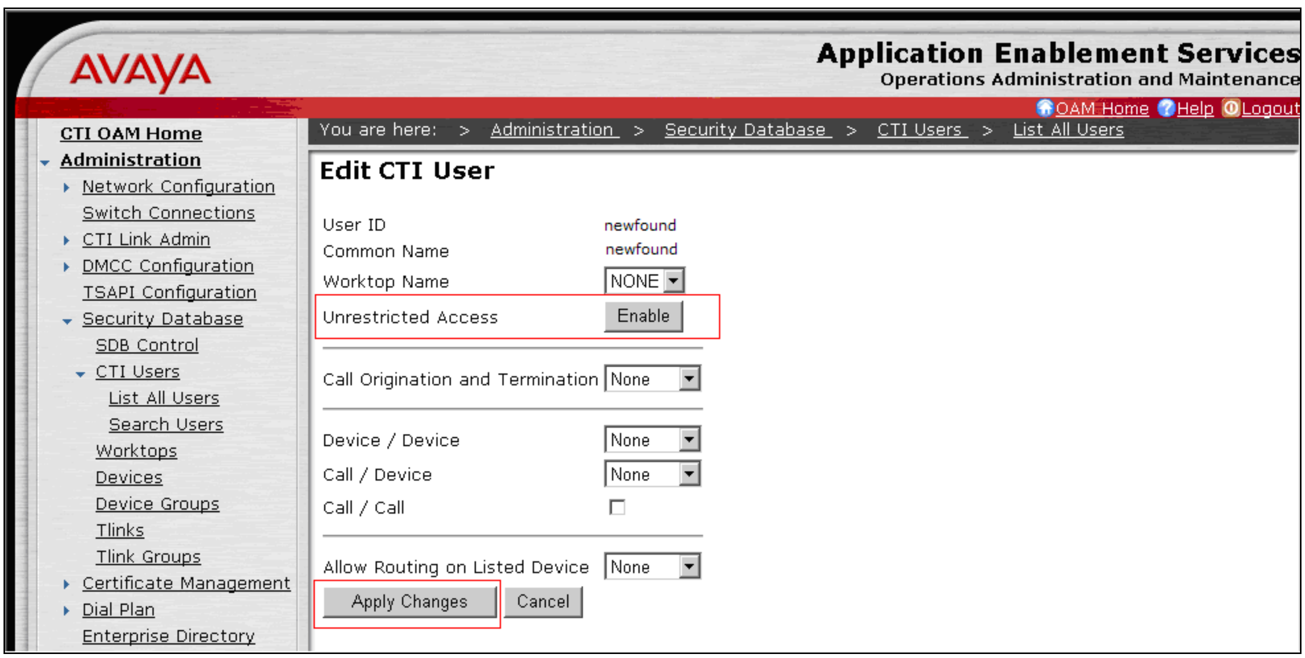
Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Click the **Apply** button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.



Once the user is created, select **OAM Home** in upper right and navigate to **Administration → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.



Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.



7. Configure the Newfound IP Call Recorder

The Newfound IP Call Recorder does not require any additional configuration for interworking with SIP Enablement Services, Application Enablement services, and Communication Manager beyond the standard installation. This includes all components of the IP Call Recorder solution including the VMG and VoiceXML platform. As part of the standard installation, the IP addresses are defined or configured for the VMG, VoiceXML platform and SES, if necessary. All configurations are performed by Newfound prior to shipping the IP Call Recorder to the end customer.

For the Newfound IP Call Recorder configuration, contact Newfound Communication.

8. General Test Approach and Test Results

The general test approach was to perform call recording on calls to the VoiceXML application or transferred through the application to another user. All calls to the VoiceXML application pass through the IP Call Recorder residing on the VMG for this purpose. Both full call and ad-hoc recording modes were tested where applicable. The IP Call Recorder successfully passed compliance testing. The following functionality was verified for calls passing through the IP Call Recorder.

- Recording of inter-switch calls to the VoiceXML application.
- Recording of calls from SIP and non-SIP endpoints at the enterprise to the VoiceXML application.
- Recording of blind transferred calls to both SIP and non-SIP endpoints. In a blind transferred call, the VoiceXML application drops out of the call after initiating the transfer. The IP Call Recorder stays in the path.
- Recording of consultative transferred calls to both SIP and non-SIP endpoints. In a consultative transferred call, the VoiceXML application stays on the call until the transferred call is answered. If the call is not answered, then the caller can continue to interact with the VoiceXML application to select another menu option. The IP Call Recorder stays in the path.
- Recording of bridged transferred calls to both SIP and non-SIP endpoints. In a bridged transferred call, the VoiceXML application stays on the call for the duration of the call. At any time, the caller can interact with the VoiceXML application to select another menu option. The IP Call Recorder stays in the path.
- Support for recording multiple calls simultaneously.
- VoiceXML control of the recording via DTMF input.
- Proper system recovery after an IP Call Recorder restart.

It should be noted that since media shuffling must be disabled for interoperability that the media of each call flows through the Avaya Media Gateway for the duration of the call. Thus, media processing resources of the Avaya Media Gateway are consumed for each call.

9. Verification Steps

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is **in-service**.

- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is **in-service**.
- Verify that calls can be placed to the VMG and that call recording can be enabled and disabled.

10. Conclusion

These Application Notes describe the procedures required to configure the Newfound IP Call Recorder to interoperate with SES, AES, and Communication Manager. The Newfound IP Call Recorder successfully passed compliance testing. For interoperability, media shuffling must be disabled.

11. Additional References

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

[1] *Administering Avaya Aura™ Communication Manager* Release 5.2, Issue 5, May 2009, Document Number 03-300509.
[2] *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server,* Issue 2.0, May 2009, Document Number 03-602508.
[3] *Avaya Aura™ Communication Manager Screen Reference*, Release 5.2, Issue 1.0, May 2009, Document Number 03-602878.
[4] *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide,* Release 5.2, Issue 11, November 2009, Document Number 02-300357.

The following document was provided by Newfound Communications.

[5] *Newfound MediaMixer, Newfound IP Call Recorder: Administration and Reference Guide for the VoIP Media Gateway [VoiceXML Edition],* Version 1.4, 2007.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.