



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring the Carrier Access Adit 3500 Trunk Gateway with Avaya SIP Enablement Services and Avaya Communication Manager - Issue 1.0

### Abstract

These Application Notes describe the procedure for configuring the Carrier Access Adit 3500 Trunk Gateway to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager using the Session Initiation Protocol (SIP).

The Adit 3500 is an integrated SIP trunk gateway, router and stateful firewall that can terminate legacy PBX digital trunk traffic and route both voice and data across public and private IP networks. In addition, the Adit 3500 provides the capability to connect non-PBX analog endpoints (telephones, fax and modems) to the SIP VoIP infrastructure. The Adit 3500 also supports SIP endpoints connected to the local LAN and registering with remote servers by providing a SIP application level gateway (ALG) function. In the compliance test, the Adit 3500 was configured as an ISDN PRI to SIP gateway connecting two PBX sites of an enterprise.

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

# 1. Introduction

These Application Notes describe the procedure for configuring the Carrier Access Adit 3500 Trunk Gateway to interoperate with Avaya SIP Enablement Services (SES) and Avaya Communication Manager using the Session Initiation Protocol (SIP).

The Carrier Access Adit 3500 Trunk Gateway integrates the features of a trunk gateway, router, and stateful firewall with flexible WAN options. It replaces multiple elements at the edge of the customer premises that typically provide routing, security, and trunk gateway functions. Examples of these functions include network address translation (NAT/NAPT), DHCP support and multiple protocol application level gateway (ALG) capabilities. Additionally, a four-port FXS option provides connectivity for analog fax machines and modems. This single platform offers scalability and high-performance for Internet and IP access, LAN-to-LAN connectivity over private and public networks, and Voice over IP (VoIP) PBX trunk service applications using SIP. The configuration used for the compliance test was an ISDN PRI to SIP gateway connecting two sites of an enterprise.

The Adit 3500 can communicate to the Avaya SES using one of two approaches. These Application Notes will describe the configuration required for each. The first approach is using a SIP trunking model. In this approach, the Adit 3500 is treated as a SIP peer to the Avaya SES and is configured on the Avaya SES as a trusted host. The Adit 3500 does not register any endpoints with the Avaya SES. In this approach, only the Adit 3500 trunk ports are supported for voice. The Adit 3500 FXS ports are not used and no SIP telephones are connected behind the device. This is because the FXS ports and SIP telephones will always attempt to register to the Avaya SES and the Avaya SES does not expect registrations from a trusted host.

The second approach is using a SIP registration model. In this approach, the Adit 3500 is not a trusted host but instead registers all endpoints (both legacy PBX and analog) as SIP endpoints to the Avaya SES. Any SIP endpoint connected behind the Adit 3500 registers directly with the Avaya SES. Each of the three types of endpoints that can be registered using this approach require slightly different configuration and has slightly different behavior. Each is described below:

1. **Legacy PBX endpoints:** In the compliance test, these endpoints were connected to the Adit 3500 via an ISDN-PRI trunk. To support the ISDN-PRI trunk, the Adit 3500 registers a SIP endpoint to the Avaya SES for each number that can be passed to the Adit 3500 from the PBX as the calling party number up to a maximum of 300. The number of calling party numbers that will be passed is determined by the PBX configuration. The PBX may send a single calling party number for all users on the PBX or it may send each user's individual extension in the calling party number information. For the compliance test, the individual extensions were passed in the calling party information. Additional SIP endpoints need to be created for any incoming numbers from the main site that will be mapped to a PBX extension by the Adit 3500. Since it is not intended that these legacy PBX numbers/users obtain PBX features from the main site Avaya Communication Manager, these legacy PBX numbers/users are configured without media server extensions on the Avaya SES. In addition, no off-pbx stations (OPS) are created for these extensions on Avaya Communication Manager.

2. **SIP endpoints:** Since the legacy PBX at the branch site does not support SIP, any SIP telephones connected behind the Adit 3500 are intended to obtain PBX features from the main site PBX. Thus, these telephones are configured with media server extensions on the Avaya SES and OPS stations on Avaya Communication Manager.
3. **Analog endpoints:** Lastly, analog endpoints connected to the FXS ports of the Adit 3500 can be configured in one of two ways depending on whether or not these endpoints require PBX features. If these endpoints require PBX features, then these endpoints would obtain the features from the main site PBX and would be configured the same as the SIP endpoints in item 2. If not, then these endpoints would not be configured with media server extensions on the Avaya SES or OPS stations on Avaya Communication Manager at the main site. For example, one use of the FXS ports is to support fax machines that were formerly connected directly to POTS lines at the branch location. In this application, the FXS ports would not require PBX features but only basic dialing in and dialing out capabilities. In the compliance test, the FXS ports were tested in this manner.

If the Adit 3500 FXS ports are not needed and no SIP telephones are connected behind the device then it is recommended to use the SIP trunking model since it requires less configuration on the Avaya SES and Avaya Communication Manager. Otherwise, the SIP registration model should be used.

## 1.1. Configuration

**Figure 1** and **2** illustrates two similar but slightly different network configurations. **Figure 1** illustrates the configuration used for the compliance test of the Adit 3500 with the SIP trunking model. It shows the Adit 3500 connecting a branch location containing a legacy (non-SIP) PBX to a main location via SIP. The main site has an Avaya SES and Avaya S8300 Media Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Endpoints include three Avaya 4600 Series IP Telephones (with SIP firmware), an Avaya 4600 Series IP Telephone (with H.323 firmware), an Avaya 6408D Digital Telephone and a fax machine. An ISDN-PRI trunk connects the media gateway to the Public Switched Telephone Network (PSTN). A Windows PC serves as a TFTP server for the Avaya IP Telephones at the main site.

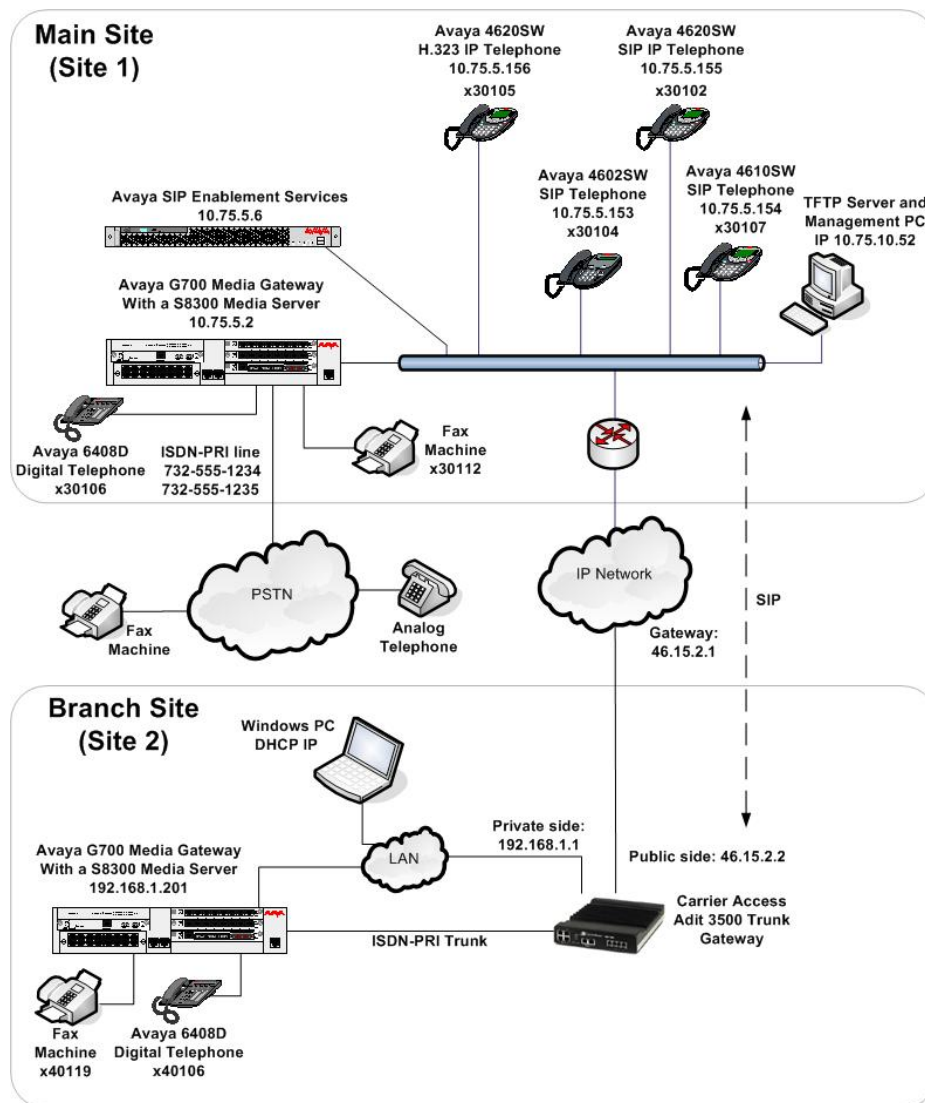
The branch site has a Carrier Access Adit 3500 Trunk Gateway with an ISDN-PRI connection to an Avaya G700 Media Gateway with an Avaya S8300 Media Server running Avaya Communication Manager. Avaya Communication Manager serves as a legacy (non-SIP) PBX. Endpoints connected to the Avaya G700 Media Gateway include an Avaya 6408D Digital Telephone and a fax machine. A Windows PC, representing a typical data user, is connected to one of the Ethernet switch ports of the Adit 3500. The Adit 3500 serves as the edge router for the branch site performing network address translation (NAT) between the private and public side of the device. The PC is used to verify basic data WAN access through the Adit 3500. The Adit 3500 is also configured to be the DHCP server for the branch site. It provides the IP address for the PC at the branch.

Calls from the main site to extensions 4xxxx are mapped to the branch site over the SIP connection. Optionally, other dialed digits can be routed to the SIP connection. In the case of the compliance test, 1-303-555-5436 was used to represent an 11-digit number that is associated with an extension at the branch (possibly from when the branch had its own local PSTN access). If the users at the

main site dial the Automatic Route Selection (ARS) feature access code plus the 11-digit number instead of the 5-digit extension, the call was configured to route over the SIP connection instead of attempting to route over the PSTN. From the Avaya SES and Adit 3500 point of view, this 11-digit number is treated like another extension/user associated with the legacy PBX at the branch. The Adit 3500 maps the 11-digit number to the local extension.

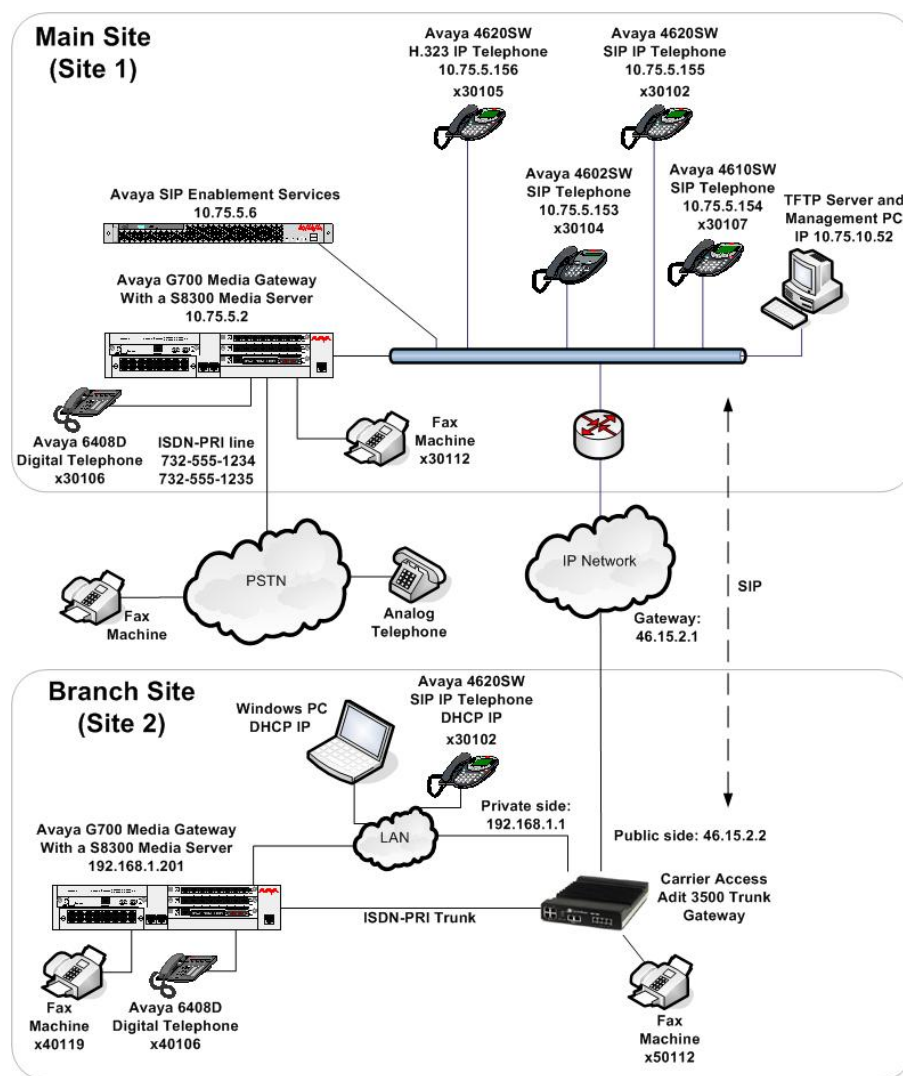
Calls from the branch site to extensions 3xxxx and 1-732-xxx-xxxx are mapped to the main site over the SIP connection. The numbers 1-732-xxx-xxxx represent numbers on the PSTN.

Lastly, one PSTN number of the ISDN-PRI trunk connected to the main site is mapped to a telephone extension at the main site and another is mapped to an extension at the branch site.



**Figure 1: Adit 3500 Test Configuration for SIP Trunking Model**

**Figure 2** illustrates the configuration used for the compliance test of the Adit 3500 using the SIP registration model. This model supports SIP telephones behind the Adit 3500 and analog endpoints connected to the FXS ports. The configuration is the same as **Figure 1** with the following additions. An Avaya 4600 Series SIP Telephone and a fax machine have been added to the branch location behind the Adit 3500. The fax machine is not associated with either PBX, so it is assigned a number which is outside the extension range of either PBX. The SIP telephone registers directly with the Avaya SES and is configured to use the Adit 3500 IP address as the default gateway. Thus, all SIP traffic between the SIP telephone and the Avaya SES will pass through the Adit 3500. The SIP telephone is associated with the main site Avaya Communication Manager, so it is assigned an extension consistent with the dial plan of the main site. The Adit 3500 provides all the same functionality as described in **Figure 1**. In addition, since NAT is being performed, a SIP ALG function is needed to translate private IP addresses in the SIP signaling messages from the SIP telephones at the branch to public IP addresses. The Adit 3500 performs this function for the branch. The TFTP server at the main site also services the branch site. The Adit 3500 is configured to allow TFTP traffic to pass between the sites.



**Figure 2: Adit 3500 Test Configuration for SIP Registration Model**

## 2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Media Server with Avaya G700 Media Gateway. (Main Site)	Avaya Communication Manager 3.1.3 (R013x.01.3.640.2)
Avaya S8300 Media Server with Avaya G700 Media Gateway. (Branch Site – Legacy PBX)	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1) Service Pack 12249
Avaya SIP Enablement Services (SES)	3.1.1
Avaya 4602SW IP Telephone Avaya 4620SW IP Telephones Avaya 4610SW IP Telephone	SIP version 2.2.2
Avaya 4620SW IP Telephones	H.323 version 2.7
Avaya 6408D Digital Telephone	-
Analog Telephones	-
Fax Machines	-
Windows PCs	Windows XP Professional
Carrier Access Adit 3500 Trunk Gateway	1.4.8

## 3. SIP Trunking Configuration

### 3.1. Configure Avaya Communication Manager

The following configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

### 3.1.1. Main Site

The communication between Avaya Communication Manager and Avaya SES at the main site is via a SIP trunk group. All SIP signaling for calls between Avaya Communication Manager and the Adit 3500 passes through Avaya SES via this trunk group. This section describes all the necessary steps to establish the SIP signaling path to the Avaya SES. For more information on configuring Avaya Communication Manager to support SIP, please refer to [3].

Step	Description
1.	<p>Use the <b>display system-parameters customer-options</b> command to verify that sufficient SIP trunk capacity exists. On <b>Page 2</b>, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.</p> <p>The license file installed on the system controls the maximum permitted. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.</p> <div><pre>display system-parameters customer-options                                Page 2 of 10                                 OPTIONAL FEATURES  IP PORT CAPACITIES     Maximum Administered H.323 Trunks: 100    USED     Maximum Concurrently Registered IP Stations: 20    10     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: 0    0     Maximum Video Capable H.323 Stations: 0    0     Maximum Video Capable IP Softphones: 0    0     <b>Maximum Administered SIP Trunks: 100    24</b>      Maximum Number of DS1 Boards with Echo Cancellation: 0    0     Maximum TN2501 VAL Boards: 0    0     Maximum G250/G350/G700 VAL Sources: 5    1     Maximum TN2602 Boards with 80 VoIP Channels: 0    0     Maximum TN2602 Boards with 320 VoIP Channels: 0    0     Maximum Number of Expanded Meet-me Conference Ports: 10    0  (NOTE: You must logoff &amp; login to effect the permission changes.)</pre></div>

Step	Description
2.	<p>On <b>Page 4</b>, verify that the features shown in bold in the example below are enabled.</p> <pre> display system-parameters customer-options                                Page  4 of 10                                 OPTIONAL FEATURES  Emergency Access to Attendant? y                                IP Stations? y   Enable 'dadmin' Login? y                                Internet Protocol (IP) PNC? n   Enhanced Conferencing? y                                ISDN Feature Plus? n     <b>Enhanced EC500? y</b>                                ISDN Network Call Redirection? n   Enterprise Survivable Server? n                                ISDN-BRI Trunks? n   Enterprise Wide Licensing? n                                <b>ISDN-PRI? y</b>     ESS Administration? n                                Local Survivable Processor? n   Extended Cvg/Fwd Admin? n                                Malicious Call Trace? n   External Device Alarm Admin? n                                Media Encryption Over IP? n   Five Port Networks Max Per MCC? n  Mode Code for Centralized Voice Mail? n     Flexible Billing? n   Forced Entry of Account Codes? n                                Multifrequency Signaling? y   Global Call Classification? n  Multimedia Appl. Server Interface (MASI)? n   Hospitality (Basic)? y                                Multimedia Call Handling (Basic)? n   Hospitality (G3V3 Enhancements)? n  Multimedia Call Handling (Enhanced)? n     <b>IP Trunks? y</b> </pre>
3.	<p>On <b>Page 5</b>, verify that the features shown in bold in the example below are enabled.</p> <pre> display system-parameters customer-options                                Page  5 of 10                                 OPTIONAL FEATURES                                  Multinational Locations? n                                Station and Trunk MSP? n   Multiple Level Precedence &amp; Preemption? n                                Station as Virtual Extension? n                                 Multiple Locations? n                                 System Management Data Transfer? n   Personal Station Access (PSA)? n                                Tenant Partitioning? n   Posted Messages? n                                Terminal Trans. Init. (TTI)? n   PNC Duplication? n                                Time of Day Routing? n   Port Network Support? n                                Uniform Dialing Plan? n                                 Usage Allocation Enhancements? y   Processor and System MSP? n                                TN2501 VAL Maximum Capacity? y     <b>Private Networking? y</b>   Processor Ethernet? y                                Wideband Switching? n                                 Wireless? n                                 Remote Office? n   Restrict Call Forward Off Net? y   Secondary Data Module? y </pre>
4.	<p>Use the <b>change node-names ip</b> command to assign the node name and IP address for the Avaya SES. In this case, <b>SES</b> and <b>10.75.5.6</b> are being used, respectively. The node name <b>SES</b> will be used throughout the other configuration forms of Avaya Communication Manager. In this example, <b>procr</b> and <b>10.75.5.2</b> are the name and IP address assigned to the Avaya S8300 Media Server.</p> <pre> change node-names ip                                Page  1 of  1                                  IP NODE NAMES                                 Name                                IP Address   Name                                IP Address <b>SES</b>                                10 .75 .5 .6 default                                0 .0 .0 .0 myaudix                                10 .75 .5 .7 <b>procr</b>                                10 .75 .5 .2 </pre>



Step	Description
5.	<p>Use the <b>change ip-network-region <i>n</i></b> command, where <i>n</i> is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the region. Select an IP network region that will contain the Avaya SES server. The association between this IP network region and the Avaya SES server will be done on the <b>Signaling Group</b> form as shown in <b>Step 7</b>. In the case of the compliance test, the same IP network region that contains the Avaya S8300 Media Server and Avaya IP Telephones was selected to contain the Avaya SES server. By default, the Media Server and IP telephones are in IP network region 1.</p> <p>On the <b>IP Network Region</b> form:</p> <ul style="list-style-type: none"> <li>▪ The <b>Authoritative Domain</b> field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is <b><i>business.com</i></b>. This name will appear in the “From” header of SIP messages originating from this IP region.</li> <li>▪ By default, <b>IP-IP Direct Audio</b> (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G700 Media Gateway. This is true for both intra-region and inter-region IP-IP Direct Audio. Shuffling can be further restricted at the trunk level on the <b>Signaling Group</b> form.</li> <li>▪ The <b>Codec Set</b> is set to the number of the IP codec set to be used for calls within this IP network region. If different IP network regions are used for the Avaya S8300 Media Server and the Avaya SES server, then <b>Page 3</b> of each <b>IP Network Region</b> form (not shown) must be used to specify the codec set for inter-region communications.</li> <li>▪ The default values can be used for all other fields.</li> </ul> <div data-bbox="316 1134 1401 1690"> <pre> change ip-network-region 1                                     Page 1 of 19   IP NETWORK REGION Region: 1 Location: Authoritative Domain: business.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: 3327 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 </pre> </div>

Step	Description																
6.	<p>Use the <b>change ip-codec-set <i>n</i></b> command, where <b><i>n</i></b> is the codec set value specified in <b>Step 5</b>, to enter the supported audio codecs for calls routed to Avaya SES. Multiple codecs can be listed in priority order to allow the codec to be negotiated during call establishment. The list should include the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test.</p> <div><div>change ip-codec-set 1</div><div>Page 1 of 2</div><div>IP Codec Set</div><div>Codec Set: 1</div><table><thead><tr><th>Audio Codec</th><th>Silence Suppression</th><th>Frames Per Pkt</th><th>Packet Size(ms)</th></tr></thead><tbody><tr><td>1: <b>G.711MU</b></td><td><b>n</b></td><td><b>2</b></td><td><b>20</b></td></tr><tr><td>2: <b>G.729AB</b></td><td><b>n</b></td><td><b>2</b></td><td><b>20</b></td></tr><tr><td>3:</td><td></td><td></td><td></td></tr></tbody></table></div>	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	1: <b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>	2: <b>G.729AB</b>	<b>n</b>	<b>2</b>	<b>20</b>	3:			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)														
1: <b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>														
2: <b>G.729AB</b>	<b>n</b>	<b>2</b>	<b>20</b>														
3:																	

Step	Description
7.	<p>Use the <b>add signaling group <i>n</i></b> command, where <i>n</i> is the number of an unused signaling group, to create the SIP signaling group as follows:</p> <ul style="list-style-type: none"> <li>▪ Set the <b>Group Type</b> field to <i>sip</i>.</li> <li>▪ The <b>Transport Method</b> field will default to <i>tls</i> (Transport Layer Security). TLS is the only link protocol that is supported for communication between Avaya SES and Avaya Communication Manager.</li> <li>▪ Specify the Avaya S8300 Media Server (node name <i>procr</i>) and the Avaya SES Server (node name <i>SES</i>) as the two ends of the signaling group in the <b>Near-end Node Name</b> and the <b>Far-end Node Name</b> fields, respectively. These field values are taken from the <b>IP Node Names</b> form shown in <b>Step 4</b>. For alternative configurations that use a C-LAN board, the near (local) end of the SIP signaling group will be the C-LAN board instead of the Media Server.</li> <li>▪ Ensure that the TLS port value of <b>5061</b> is configured in the <b>Near-end Listen Port</b> and the <b>Far-end Listen Port</b> fields.</li> <li>▪ In the <b>Far-end Network Region</b> field, enter the IP network region value assigned in the <b>IP Network Region</b> form in <b>Step 5</b>. This defines which IP network region contains the Avaya SES server. If the <b>Far-end Network Region</b> field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the inter-region connectivity for the pair of network regions.</li> <li>▪ Enter the domain name of Avaya SES in the <b>Far-end Domain</b> field. In this configuration, the domain name is <i>business.com</i>. This domain is specified in the Uniform Resource Identifier (URI) of the SIP “To” header in the INVITE message.</li> <li>▪ The <b>Direct IP-IP Audio Connections</b> field is set to <i>n</i>. For interoperability with the Adit 3500, Direct IP-IP Audio (shuffling) must be disabled for the SIP trunk.</li> <li>▪ The <b>DTMF over IP</b> field must be set to the default value of <i>rtp-payload</i> for a SIP trunk. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833.</li> <li>▪ The default values for the other fields may be used.</li> </ul> <div data-bbox="316 1354 1404 1837" style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <pre> add signaling-group 1                                     Page 1 of 1                                 SIGNALING GROUP  Group Number: 1                      Group Type: sip                                 Transport Method: tls  Near-end Node Name: procr              Far-end Node Name: SES Near-end Listen Port: 5061            Far-end Listen Port: 5061                                 Far-end Network Region: 1 Far-end Domain: business.com                                  Bypass If IP Threshold Exceeded? n  DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? n                                 IP Audio Hairpinning? n  Session Establishment Timer(min): 120 </pre> </div>

Step	Description
8.	<p>Add a SIP trunk group by using the <b>add trunk-group <i>n</i></b> command, where <i>n</i> is the number of an unused trunk group. For the compliance test, trunk group number 1 was chosen.</p> <p>On <b>Page 1</b>, set the fields to the following values:</p> <ul style="list-style-type: none"> <li>▪ Set the <b>Group Type</b> field to <i>sip</i>.</li> <li>▪ Choose a descriptive <b>Group Name</b>.</li> <li>▪ Specify an available trunk access code (<b>TAC</b>) that is consistent with the existing dial plan.</li> <li>▪ Set the <b>Service Type</b> field to <i>tie</i>.</li> <li>▪ Specify the signaling group associated with this trunk group in the <b>Signaling Group</b> field as previously specified in <b>Step 7</b>.</li> <li>▪ Specify the <b>Number of Members</b> supported by this SIP trunk group. As mentioned earlier, each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <div data-bbox="316 877 1401 1220"> <pre> add trunk-group 1                                     Page 1 of 21                                      TRUNK GROUP  Group Number: 1                      Group Type: sip          CDR Reports: y   Group Name: SES Trk Grp              COR: 1              TN: 1          TAC: 101     Direction: two-way                Outgoing Display? n     Dial Access? n     Queue Length: 0   Service Type: tie                      Auth Code? n                                       Signaling Group: 1                                      Number of Members: 24 </pre> </div>
9.	<p>On <b>Page 3</b>:</p> <ul style="list-style-type: none"> <li>▪ Verify the <b>Numbering Format</b> field is set to <i>public</i>. This field specifies the format of the calling party number sent to the far-end.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <div data-bbox="316 1444 1401 1770"> <pre> add trunk-group 1                                     Page 3 of 21 TRUNK FEATURES     ACA Assignment? n                      Measured: none  Maintenance Tests? y   Numbering Format: public  Prepend '+' to Calling Number? n  Replace Unavailable Numbers? n </pre> </div>

Step	Description																																																																																																																																																													
10.	<p>Use the <b>change public-unknown-numbering 0</b> command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in <b>Step 8</b>. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across trunk group 1 will be sent as a 5 digit calling number. This calling party number will be sent to the far-end in the SIP “From” header.</p> <div><pre>change public-unknown-numbering 0</pre><div>Page1 of 2</div><table><tr><th colspan="10">NUMBERING - PUBLIC/UNKNOWN FORMAT</th></tr><tr><th colspan="5"></th><th>Total</th><th colspan="5"></th><th>Total</th></tr><tr><th>Ext</th><th>Ext</th><th>Trk</th><th>CPN</th><th></th><th>CPN</th><th>Ext</th><th>Ext</th><th>Trk</th><th>CPN</th><th></th><th>CPN</th></tr><tr><th>Len</th><th>Code</th><th>Grp(s)</th><th>Prefix</th><th></th><th>Len</th><th>Len</th><th>Code</th><th>Grp(s)</th><th>Prefix</th><th></th><th>Len</th></tr><tr><td>5</td><td>3</td><td>1</td><td></td><td></td><td>5</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>5</td><td>3</td><td>99</td><td></td><td></td><td>5</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table></div>	NUMBERING - PUBLIC/UNKNOWN FORMAT															Total						Total	Ext	Ext	Trk	CPN		CPN	Ext	Ext	Trk	CPN		CPN	Len	Code	Grp(s)	Prefix		Len	Len	Code	Grp(s)	Prefix		Len	5	3	1			5							5	3	99			5																																																																																													
NUMBERING - PUBLIC/UNKNOWN FORMAT																																																																																																																																																														
					Total						Total																																																																																																																																																			
Ext	Ext	Trk	CPN		CPN	Ext	Ext	Trk	CPN		CPN																																																																																																																																																			
Len	Code	Grp(s)	Prefix		Len	Len	Code	Grp(s)	Prefix		Len																																																																																																																																																			
5	3	1			5																																																																																																																																																									
5	3	99			5																																																																																																																																																									
11.	<p>Automatic Alternate Routing (AAR) was used by Avaya Communication Manager to route calls to the Avaya SES that were bound for the branch office PBX and dialed with a 5 digit extension (4xxxx). Automatic Route Selection (ARS) was used to route calls to the branch dialed with an 11-digit number (1303555xxxx). AAR and ARS require a route pattern for this purpose that points to the SIP trunk created in <b>Step 8</b>. Create a route pattern that will use the SIP trunk that connects to Avaya SES. The compliance test defined route pattern 1 as the route for calls to the branch office. For more information on AAR and ARS see [1] and [2].</p> <p>To create a route pattern, use the <b>change route-pattern <i>n</i></b> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level (<b>FRL</b>) field to a level that allows access to this trunk for all users that require it. The value of <b>0</b> is the least restrictive level. The default values may be retained for all other fields.</p> <div><pre>change route-pattern 1</pre><div>Page1 of 3</div><div>Pattern Number: 3Pattern Name: SIP</div><table><tr><th>Grp</th><th>FRL</th><th>NPA</th><th>Pfx</th><th>Hop</th><th>Toll</th><th>No.</th><th>Inserted</th><th>DCS/</th><th>IXC</th></tr><tr><th>No</th><th></th><th></th><th>Mrk</th><th>Lmt</th><th>List</th><th>Del</th><th>Digits</th><th>QSIG</th><th></th></tr><tr><td>1:</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td>Intw</td><td></td></tr><tr><td>2:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n</td><td>user</td></tr><tr><td>3:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n</td><td>user</td></tr><tr><td>4:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n</td><td>user</td></tr><tr><td>5:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n</td><td>user</td></tr><tr><td>6:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>n</td><td>user</td></tr></table><table><tr><th>BCC</th><th>VALUE</th><th>TSC</th><th>CA-TSC</th><th>ITC</th><th>BCIE</th><th>Service/Feature</th><th>PARM</th><th>No.</th><th>Numbering</th><th>LAR</th></tr><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>W</td><td>Request<td><td>Dgts<td>Format<td></td></td></td></td></td></tr><tr><td>1:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td></td><td>none</td></tr><tr><td>2:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td></td><td>none</td></tr><tr><td>3:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td></td><td>none</td></tr><tr><td>4:</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td></td><td></td><td>none</td></tr><tr><td>5:</td><td>v</td><td>v</td><td>v</td><td>v</td><td>v</td><td>n</td><td>n</td><td></td><td></td><td>none</td></tr></table></div>	Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC	No			Mrk	Lmt	List	Del	Digits	QSIG		1:	1	0						Intw		2:								n	user	3:								n	user	4:								n	user	5:								n	user	6:								n	user	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR	0	1	2	3	4	W	Request <td><td>Dgts<td>Format<td></td></td></td></td>	<td>Dgts<td>Format<td></td></td></td>	Dgts <td>Format<td></td></td>	Format <td></td>		1:	y	y	y	y	y	n	n			none	2:	y	y	y	y	y	n	n			none	3:	y	y	y	y	y	n	n			none	4:	y	y	y	y	y	n	n			none	5:	v	v	v	v	v	n	n			none
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC																																																																																																																																																					
No			Mrk	Lmt	List	Del	Digits	QSIG																																																																																																																																																						
1:	1	0						Intw																																																																																																																																																						
2:								n	user																																																																																																																																																					
3:								n	user																																																																																																																																																					
4:								n	user																																																																																																																																																					
5:								n	user																																																																																																																																																					
6:								n	user																																																																																																																																																					
BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR																																																																																																																																																				
0	1	2	3	4	W	Request <td><td>Dgts<td>Format<td></td></td></td></td>	<td>Dgts<td>Format<td></td></td></td>	Dgts <td>Format<td></td></td>	Format <td></td>																																																																																																																																																					
1:	y	y	y	y	y	n	n			none																																																																																																																																																				
2:	y	y	y	y	y	n	n			none																																																																																																																																																				
3:	y	y	y	y	y	n	n			none																																																																																																																																																				
4:	y	y	y	y	y	n	n			none																																																																																																																																																				
5:	v	v	v	v	v	n	n			none																																																																																																																																																				

Step	Description
12.	<p>Use the <b>change locations</b> command to assign the default SIP route pattern to the location. In the compliance test, all SIP endpoints at the main site are part of a single location defined in Avaya Communication Manager. This location uses the default name of <b>Main</b> and is shown in the example below. Enter the route pattern number from the previous step in the <b>Proxy Sel. Rte. Pat.</b> field. The default values may be retained for all other fields.</p> <pre> change locations                                     Page 1 of 4                                  LOCATIONS                                  ARS Prefix 1 Required For 10-Digit NANP Calls? y  Loc.  Name          Timezone Rule  NPA  ARS  Attd      Pre-  Proxy Sel. No.   Offset        Offset        FAC  FAC  fix      Rte. Pat. 1:    Main          + 00:00  0 2: 3: </pre>
13.	<p>To map a PSTN number to an extension at either the main site or the branch site, use the <b>change inc-call-handling-trmt trunk-group <i>n</i></b> command, where <b><i>n</i></b> is the ISDN-PRI trunk group number connected to the PSTN. For the compliance test, trunk group 2 was used for the ISDN-PRI trunk to the PSTN. The example below shows two incoming 11-digit numbers being deleted and replaced with extensions. The first entry is mapped to an extension at the main site. The second entry is mapped to an extension at the branch site.</p> <pre> change inc-call-handling-trmt trunk-group 2          Page 1 of 3                                  INCOMING CALL HANDLING TREATMENT  Service/   Called   Called   Del   Insert Feature    Len      Number tie        11    17325551234    11    30107 tie        11    17325551235    11    40106 </pre>
14.	<p>Add an entry in the dial plan that defines that any 5-digit string beginning with a 4 will be routed by AAR. To do this, use the <b>change dialplan analysis</b> command and add the entry highlighted below.</p> <pre> change dialplan analysis                             Page 1 of 12                                  DIAL PLAN ANALYSIS TABLE                                  Percent Full: 3  Dialed   Total   Call   Dialed   Total   Call   Dialed   Total   Call String   Length  Type   String   Length  Type   String   Length  Type 1        3      dac    3        5      ext    4        5      aar 3        5      ext    8        1      fac    9        1      fac 4        5      aar    *        3      fac    #        3      fac </pre>

Step	Description
15.	<p>Create an entry in the <b>AAR Digit Analysis Table</b> to route dialed digits beginning with a <b>4</b> and length of <b>5</b> to route pattern <b>1</b> that points to the SIP trunk connected to the Avaya SES (see <b>Step 8</b>). To do this, use the <b>change aar analysis n</b> command, where <b>n</b> is a set of dialed digits in the table. A portion of the table will be displayed starting at <b>n</b>. Tab to the bottom of the displayed entries and create a new entry in the table like the one highlighted below.</p> <pre> change aar analysis 1 Page 1 of 2 AAR DIGIT ANALYSIS TABLE Percent Full: 3 Dialed      Total      Route      Call      Node      ANI String      Min   Max   Pattern   Type      Num      Req'd 2           7     7     254      aar        n 3           4     4      4        aar        n 39001      5     5     99       aar        n <b>4</b>         <b>5</b>    <b>5</b>    <b>1</b>       <b>aar</b>       <b>n</b> 5           7     7     254      aar        n 6           7     7     254      aar        n 7           7     7     254      aar        n 8           7     7     254      aar        n 9           7     7     254      aar        n </pre>
16.	<p>Create an entry in the <b>ARS Digit Analysis Table</b> to route dialed digits beginning with <b>1303555</b> and length of <b>11</b> to route pattern <b>1</b> that points to the SIP trunk connected to the Avaya SES (see <b>Step 8</b>). To do this, use the <b>change ars analysis n</b> command, where <b>n</b> is a set of dialed digits in the table. A portion of the table will be displayed starting at <b>n</b>. Tab to the bottom of the displayed entries and create a new entry in the table like the one highlighted below.</p> <pre> change ars analysis 1303 Page 1 of 2 ARS DIGIT ANALYSIS TABLE Location: all Percent Full: 3 Dialed      Total      Route      Call      Node      ANI String      Min   Max   Pattern   Type      Num      Req'd <b>1303555</b>   <b>11</b>  <b>11</b>    <b>1</b>       <b>fnpa</b>      <b>n</b> 131        11    11    deny     fnpa        n 132        11    11    deny     fnpa        n 133        11    11    deny     fnpa        n 134        11    11    deny     fnpa        n </pre>

### 3.1.2. Branch Site

This section describes the configuration required for establishing the ISDN-PRI connection between the branch site Avaya Communication Manager and the Adit 3500.

Step	Description																																																																																	
1.	<p>Automatic Alternate Routing (AAR) was used to route calls to the ISDN-PRI trunk connected to the Adit 3500. In addition, AAR was invoked without the need to dial a feature access code (FAC). Automatic Route Selection (ARS) was used to route calls bound for the PSTN via the main site. Use of ISDN-PRI trunks and routing calls in this manner requires certain features be enabled.</p> <p>On the various pages of the <b>display system-parameters customer-options</b> command, verify that the following fields have been set to <b>y</b>.</p> <p><b>Page 3: ARS? y</b> <b>Page 3: ARS/AAR Dialing without FAC? y</b> <b>Page 4: ISDN-PRI? y</b> <b>Page 5: Private Networking? y</b></p> <p>If a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.</p>																																																																																	
2.	<p>Add an entry in the dial plan that defines that any 5-digit string beginning with a <b>3</b> will be routed by AAR. To do this, use the <b>change dialplan analysis</b> command and add the entry highlighted below.</p> <div><pre>change dialplan analysis</pre><div><div>DIAL PLAN ANALYSIS TABLE</div><div>Percent Full: 1</div><table><tr><th>Dialed String</th><th>Total Length</th><th>Call Type</th><th>Dialed String</th><th>Total Length</th><th>Call Type</th><th>Dialed String</th><th>Total Length</th><th>Call Type</th></tr><tr><td>0</td><td>1</td><td>attd</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>1</td><td>3</td><td>dac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>3</td><td>5</td><td>aar</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>4</td><td>5</td><td>ext</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>8</td><td>1</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>9</td><td>1</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>*</td><td>3</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>#</td><td>3</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table></div></div>	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	0	1	attd							1	3	dac							3	5	aar							4	5	ext							8	1	fac							9	1	fac							*	3	fac							#	3	fac						
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type																																																																										
0	1	attd																																																																																
1	3	dac																																																																																
3	5	aar																																																																																
4	5	ext																																																																																
8	1	fac																																																																																
9	1	fac																																																																																
*	3	fac																																																																																
#	3	fac																																																																																



Step	Description
3.	<p>Create an entry in the <b>AAR Digit Analysis Table</b> to route dialed digits beginning with a <b>3</b> and length of <b>5</b> to route pattern <b>3</b> that points to the ISDN-PRI trunk (see <b>Step 7</b>). To do this, use the <b>change aar analysis n</b> command, where <b>n</b> is a set of dialed digits in the table. A portion of the table will be displayed starting at <b>n</b>. Tab to the bottom of the displayed entries and create a new entry in the table like the one highlighted below.</p> <pre> change aar analysis 0 Page 1 of 2 AAR DIGIT ANALYSIS TABLE Percent Full: 1  Dialed      Total      Route      Call      Node      ANI String      Min   Max   Pattern   Type      Num      Req'd 2           7     7     254      aar             n 3           4     4     254      aar             n <b>3</b>         <b>5</b>    <b>5</b>    <b>3</b>       <b>aar</b>          <b>n</b> 4           7     7     254      aar             n 5           5     5     3         aar             n 6           5     5     6         aar             n 65          5     5     65       aar             n 7           7     7     254      aar             n 8           5     5     2         aar             n </pre>
4.	<p>Create an entry in the <b>ARS Digit Analysis Table</b> to route dialed digits beginning with a <b>1732</b> and length of <b>11</b> to route pattern <b>4</b> that points to the ISDN-PRI trunk (see <b>Step 7</b>). To do this, use the <b>change ars analysis n</b> command, where <b>n</b> is a set of dialed digits in the table. A portion of the table will be displayed starting at <b>n</b>. Tab to the bottom of the displayed entries and create a new entry in the table like the one highlighted below.</p> <pre> change ars analysis 1732 Page 1 of 2 ARS DIGIT ANALYSIS TABLE Location: all Percent Full: 1  Dialed      Total      Route      Call      Node      ANI String      Min   Max   Pattern   Type      Num      Req'd <b>1732</b>      <b>11</b>  <b>11</b>  <b>4</b>       <b>fnpa</b>          <b>n</b> 1xxx555     11    11    deny      fnpa             n 1xxx976     11    11    deny      fnpa             n 2           7     7     2         hnpa             n 3           7     7     2         hnpa             n 4           7     7     2         hnpa             n 411         3     3     deny      svcl             n 5           7     7     2         hnpa             n </pre>

Step	Description
5.	<p>Add the DS1 board to the configuration by using the <b>add ds1 x</b> command, where <i>x</i> indicates the carrier and slot where the board is installed. Enter any descriptive name in the <b>Name</b> field. Set all fields in bold to the values indicated. The Adit 3500 is always shipped pre-configured as the network side of the ISDN-PRI interface. Thus, on Avaya Communication Manager the <b>Interface</b> field must be set to <i>user</i>. The combination of <b>Country Protocol 1</b> and <b>Protocol Version b</b> defines the use of the NI-2 version of ISDN-PRI. Use default values for all other fields.</p> <pre> add ds1 1v3                                     Page 1 of 2                                  DS1 CIRCUIT PACK  Location: 001V3                                Name: G3R1 PRI Bit Rate: 1.544                                Line Coding: b8zs Line Compensation: 1                            Framing Mode: esf Signaling Mode: isdn-pri Connect: pbx                                    Interface: user TN-C7 Long Timers? n                            Country Protocol: 1 Interworking Message: PROGRESS                  Protocol Version: b Interface Companding: mulaw                     CRC? n Idle Code: 11111111                            DCP/Analog Bearer Capability: 3.1kHz                                  T303 Timer(sec): 4  Slip Detection? n                             Near-end CSU Type: other                                  Block Progress Indicator? n </pre>
6.	<p>Create a signaling group by using the <b>add signaling-group n</b> command, where <i>n</i> is the number of an unused signaling group. Set the fields in bold to the values shown below. The <b>Group Type</b> is set to <i>isdn-pri</i>. The <b>Primary D-Channel</b> field is set to the 24<sup>th</sup> channel of the DS1 board in slot 1v3. This board was added to the configuration in the previous step. The <b>Trunk Group for Channel Selection</b> field will be populated at a later step after the trunk group has been created.</p> <pre> add signaling-group 3                             Page 1 of 5                                  SIGNALING GROUP  Group Number: 3                                Group Type: isdn-pri Associated Signaling? y                        Max number of NCA TSC: 0 Primary D-Channel: 001V324                    Max number of CA TSC: 0 Trunk Group for Channel Selection:              Trunk Group for NCA TSC: Supplementary Service Protocol: a </pre>

Step	Description
7.	<p>Create a trunk group by using the <b>add trunk-group <i>n</i></b> command, where <i>n</i> is the number of an unused trunk group. Set the fields in bold to the values shown below. The <b>Group Name</b> can be any descriptive name. The <b>TAC</b> must be chosen to be consistent with the existing dial plan. Use default values for all other fields.</p> <pre> add trunk-group 3                                     Page 1 of 21                                      TRUNK GROUP  Group Number: 3                                     Group Type: isdn       CDR Reports: y   Group Name: Adit PRI                               COR: 1               TN: 1          TAC: 103     Direction: two-way                             Outgoing Display? n   Carrier Medium: PRI/BRI     Dial Access? y                               Busy Threshold: 255   Night Service:     Queue Length: 0   Service Type: tie                                Auth Code? n         TestCall ITC: rest                                      Far End Test Line No:     TestCall BCC: 4 </pre>
8.	<p><b>On Page 3:</b></p> <ul style="list-style-type: none"> <li>Set the <b>Send Name</b> field to <i>y</i>.</li> <li>Set the <b>Send Calling Number</b> field to <i>y</i>.</li> <li>Verify the <b>Numbering Format</b> field is set to <i>public</i>. This field specifies the format of the calling party number sent to the far-end.</li> <li>The default values may be retained for the other fields.</li> </ul> <pre> add trunk-group 3                                     Page 3 of 21 TRUNK FEATURES   ACA Assignment? n                               Measured: none       Wideband Support? n  Internal Alert? n     Maintenance Tests? y  Data Restriction? n   NCA-TSC Trunk Member:  Send Name: y          Send Calling Number: y  Used for DCS? n       Send EMU Visitor CPN? n   Suppress # Outpulsing? n                     Format: public   Outgoing Channel ID Encoding: preferred        UII IE Treatment: service-provider   Replace Restricted Numbers? n  Replace Unavailable Numbers? n  Send Connected Number: n  Hold/Unhold Notifications? n  Modify Tandem Calling Number? n   Send UII IE? y </pre>

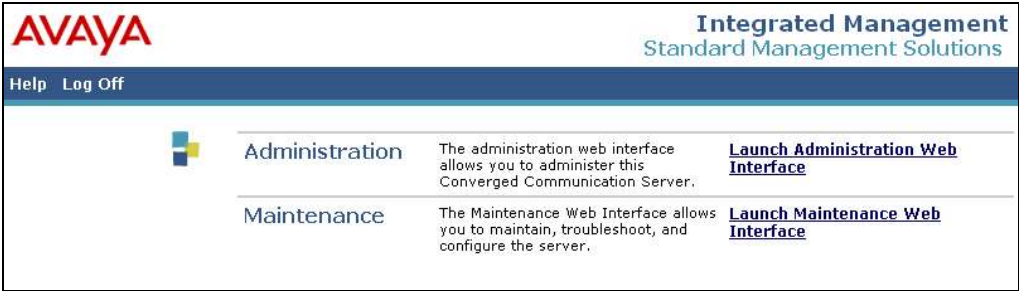
Step	Description																																																
9.	<p>On <b>Page 5</b>, enter the group members. For each DS1 port to be added as a member of the trunk group, enter the port number in the <b>Port</b> field and the corresponding signaling group for that port in the <b>Sig Grp</b> field. The <b>Code</b> field is filled in automatically. In the compliance test, each of the 23 bearer channels of the DS1 board added in <b>Step 5</b> were added to this group. The signaling channel for each of these ports is the signaling channel added in <b>Step 6</b>.</p> <div><div>add trunk-group 3</div><div>Page5 of 21</div><div>TRUNK GROUP</div><div>Administered Members (min/max):1/19</div><div>GROUP MEMBER ASSIGNMENTS</div><div>Total Administered Members:19</div><table><thead><tr><th></th><th>Port</th><th>Code</th><th>Sfx Name</th><th>Night</th><th>Sig Grp</th></tr></thead><tbody><tr><td>1:</td><td>001V301</td><td>MM710</td><td></td><td></td><td>3</td></tr><tr><td>2:</td><td>001V302</td><td>MM710</td><td></td><td></td><td>3</td></tr><tr><td>3:</td><td>001V303</td><td>MM710</td><td></td><td></td><td>3</td></tr><tr><td>4:</td><td>001V304</td><td>MM710</td><td></td><td></td><td>3</td></tr><tr><td>5:</td><td>001V305</td><td>MM710</td><td></td><td></td><td>3</td></tr><tr><td>6:</td><td>001V306</td><td>MM710</td><td></td><td></td><td>3</td></tr><tr><td>7:</td><td>001V307</td><td>MM710</td><td></td><td></td><td>3</td></tr></tbody></table></div>		Port	Code	Sfx Name	Night	Sig Grp	1:	001V301	MM710			3	2:	001V302	MM710			3	3:	001V303	MM710			3	4:	001V304	MM710			3	5:	001V305	MM710			3	6:	001V306	MM710			3	7:	001V307	MM710			3
	Port	Code	Sfx Name	Night	Sig Grp																																												
1:	001V301	MM710			3																																												
2:	001V302	MM710			3																																												
3:	001V303	MM710			3																																												
4:	001V304	MM710			3																																												
5:	001V305	MM710			3																																												
6:	001V306	MM710			3																																												
7:	001V307	MM710			3																																												
10.	<p>Use the <b>change signaling-group 3</b> command to modify the signaling group created in <b>Step 6</b>. Set the <b>Trunk Group for Channel Selection</b> field to the number of the trunk group created in <b>Step 7</b>.</p> <div><div>change signaling-group 3</div><div>Page1 of 5</div><div>SIGNALING GROUP</div><div>Group Number:3</div><div>Group Type:isdn-pri</div><div>Associated Signaling?y</div><div>Max number of NCA TSC:0</div><div>Primary D-Channel:001V324</div><div>Max number of CA TSC:0</div><div>Trunk Group for NCA TSC:</div><div>Trunk Group for Channel Selection:3</div><div>Supplementary Service Protocol:a</div></div>																																																
11.	<p>Use the <b>change public-unknown-numbering 0</b> command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in <b>Step 7</b>. In the example shown below, all calls originating from a 5-digit extension beginning with 4 and routed across trunk group 3 will be sent as a 5 digit calling number.</p> <div><div>change public-unknown-numbering 0</div><div>Page1 of 2</div><div>NUMBERING - PUBLIC/UNKNOWN FORMAT</div><div>Total</div><table><thead><tr><th>Ext Len</th><th>Ext Code</th><th>Trk Grp(s)</th><th>CPN Prefix</th><th>CPN Len</th><th>Ext Len</th><th>Ext Code</th><th>Trk Grp(s)</th><th>CPN Prefix</th><th>Total CPN Len</th></tr></thead><tbody><tr><td>5</td><td>4</td><td>3</td><td></td><td>5</td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table></div>	Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	CPN Len	Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	5	4	3		5																																	
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	CPN Len	Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len																																								
5	4	3		5																																													


Step	Description
12.	<p>Create a route pattern that will be used by AAR to route calls bound for extensions at the main site to the ISDN-PRI trunk that connects to the Adit 3500. To do this, use the <b>change route-pattern <i>n</i></b> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the ISDN-PRI trunk. Set the Facility Restriction Level (<b>FRL</b>) field to a level that allows access to this trunk for all users that require it. The value of <b>0</b> is the least restrictive level. Use default values for all other fields.</p> <pre> change route-pattern 3                                     Page 1 of 3       Pattern Number: 3   Pattern Name: Adit 3500       SCCAN? n           Secure SIP? n    Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC   No      Mrk Lmt List Del  Digits      QSIG                                 Dgts      Intw 1: 3      0 2: 3: 4: 5: 6:                                n  user                                 n  user                                 n  user                                 n  user                                 n  user                                 n  user        BCC VALUE  TSC CA-TSC   ITC BCIE Service/Feature PARM  No. Numbering LAR       0 1 2 3 4 W      Request      Dgts Format                                 Subaddress 1: y y y y y n  n          rest          none 2: y y y y y n  n          rest          none 3: y y y y y n  n          rest          none 4: y y y y y n  n          rest          none 5: y y y y y n  n          rest          none 6: y y y y y n  n          rest          none </pre>

Step	Description
13.	<p>Create a second route pattern that will be used by ARS to route calls bound for the PSTN to the ISDN-PRI trunk that connects to the Adit 3500. To do this, use the <b>change route-pattern <i>n</i></b> command, where <i>n</i> is the number of an unused route pattern. Enter a descriptive name for the <b>Pattern Name</b> field. Set the <b>Grp No</b> field to the trunk group number created for the ISDN-PRI trunk. Set the Facility Restriction Level (<b>FRL</b>) field to a level that allows access to this trunk for all users that require it. The value of <b>0</b> is the least restrictive level. The Prefix Mark (<b>Pfx Mrk</b>) field defaults to blank which will suppress the user dialed 1 on 1 + 10 digit calls. The main site Avaya Communication Manager needs the 1 plus an additional prefix of 9 to route the call to the PSTN. Thus, a 91 is prefixed to the dialed digits by adding <b>91</b> to the <b>Inserted Digits</b> column. Use default values for all other fields.</p> <pre> change route-pattern 4 Pattern Number: 4    Pattern Name: Adit Ext SCCAN? n            Secure SIP? n Grp FRL NPA Pfx Hop Toll No.  Inserted DCS/ IXC No      Mrk Lmt List Del  Digits  QSIG                                 Intw 1: 3      0                      91      n  user 2:                                n  user 3:                                n  user 4:                                n  user 5:                                n  user 6:                                n  user        BCC VALUE  TSC CA-TSC  ITC BCIE Service/Feature PARM No. Numbering LAR       0 1 2 3 4 W      Request      Dgts Format                                 Subaddress 1: y y y y y n n      rest      none 2: y y y y y n n      rest      none 3: y y y y y n n      rest      none 4: y y y y y n n      rest      none 5: y y y y y n n      rest      none 6: y y y y y n n      rest      none </pre>

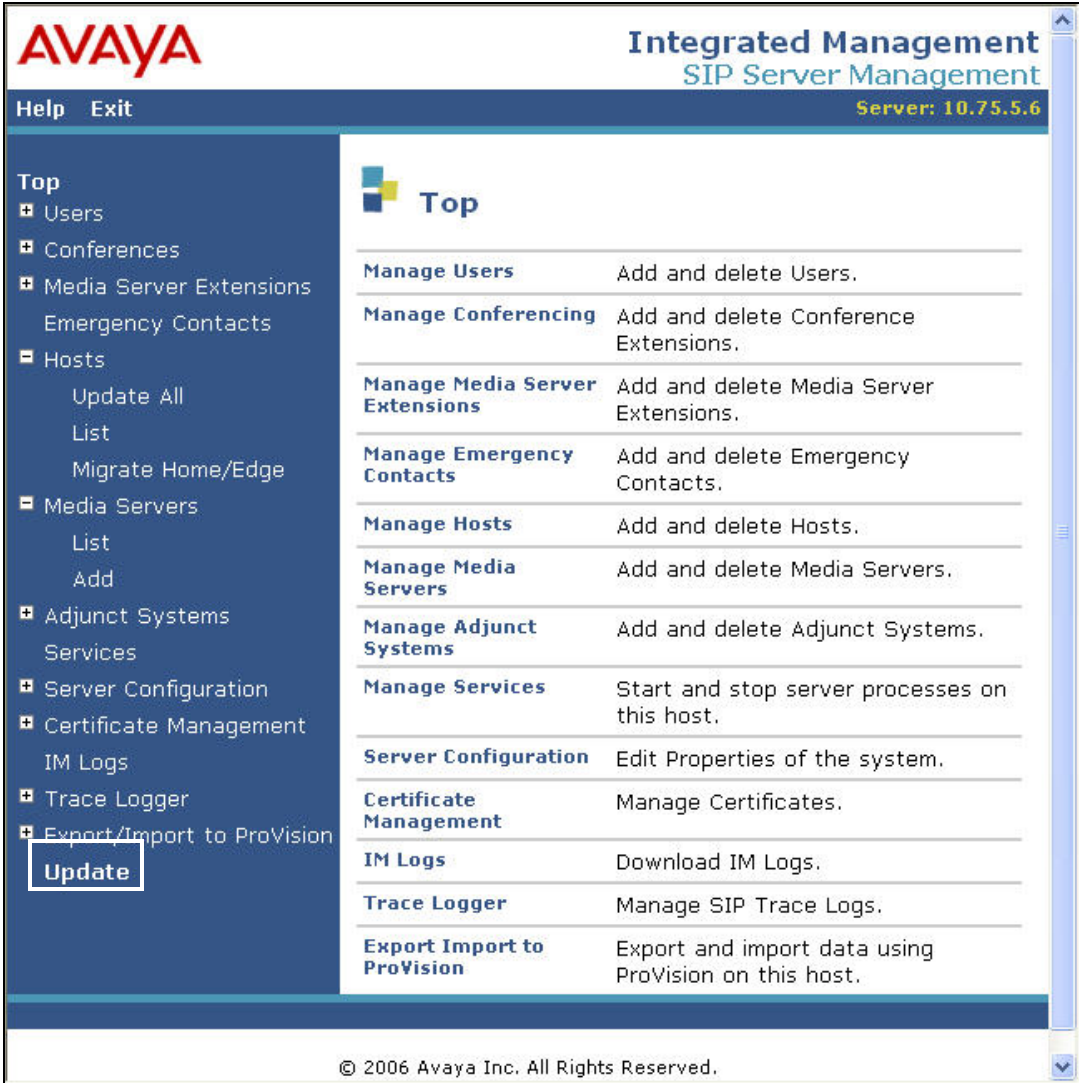
### 3.2. Configure Avaya SES

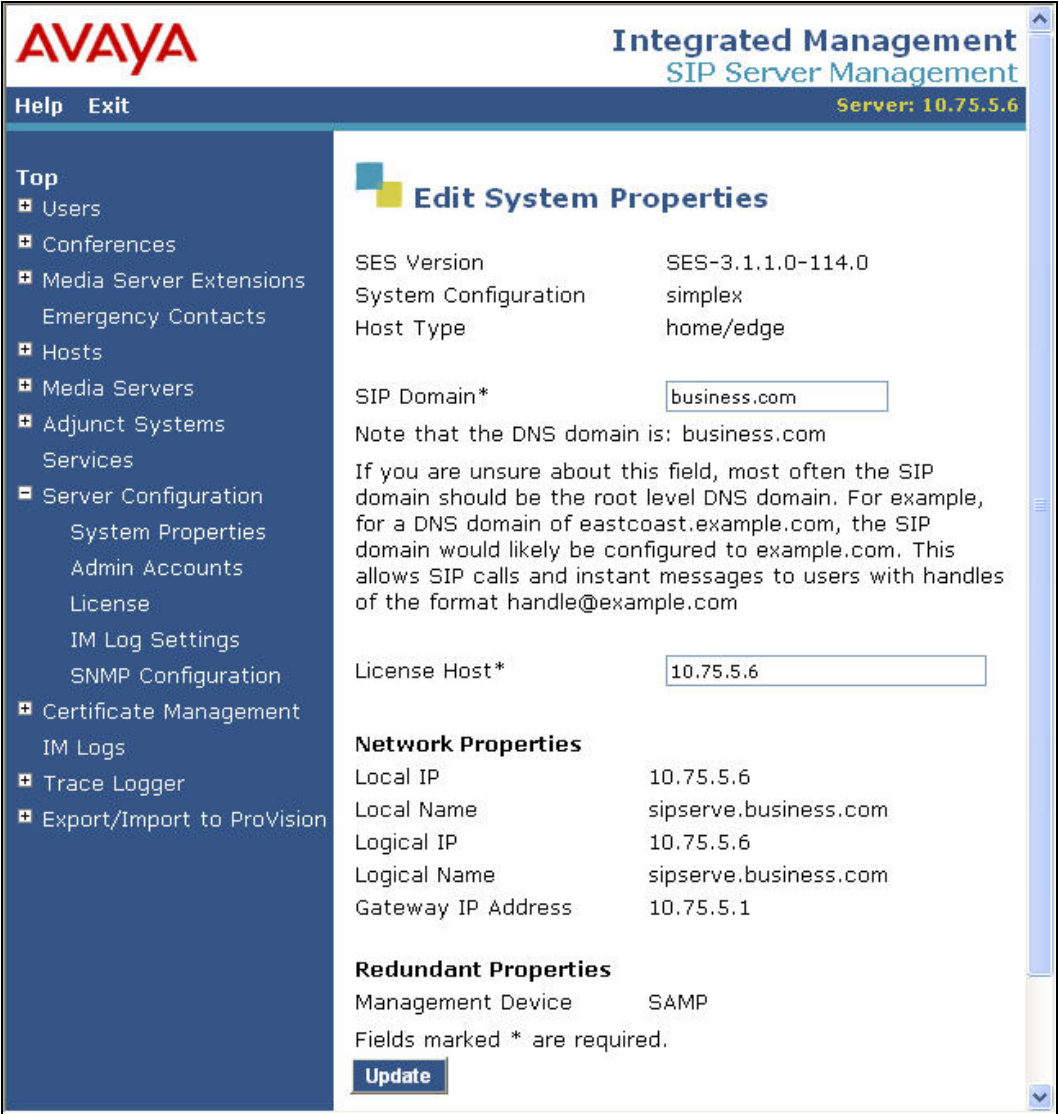
This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that Avaya SES software and the license file have already been installed on the server. During the software installation, the installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. For additional information on these installation tasks, refer to [4].

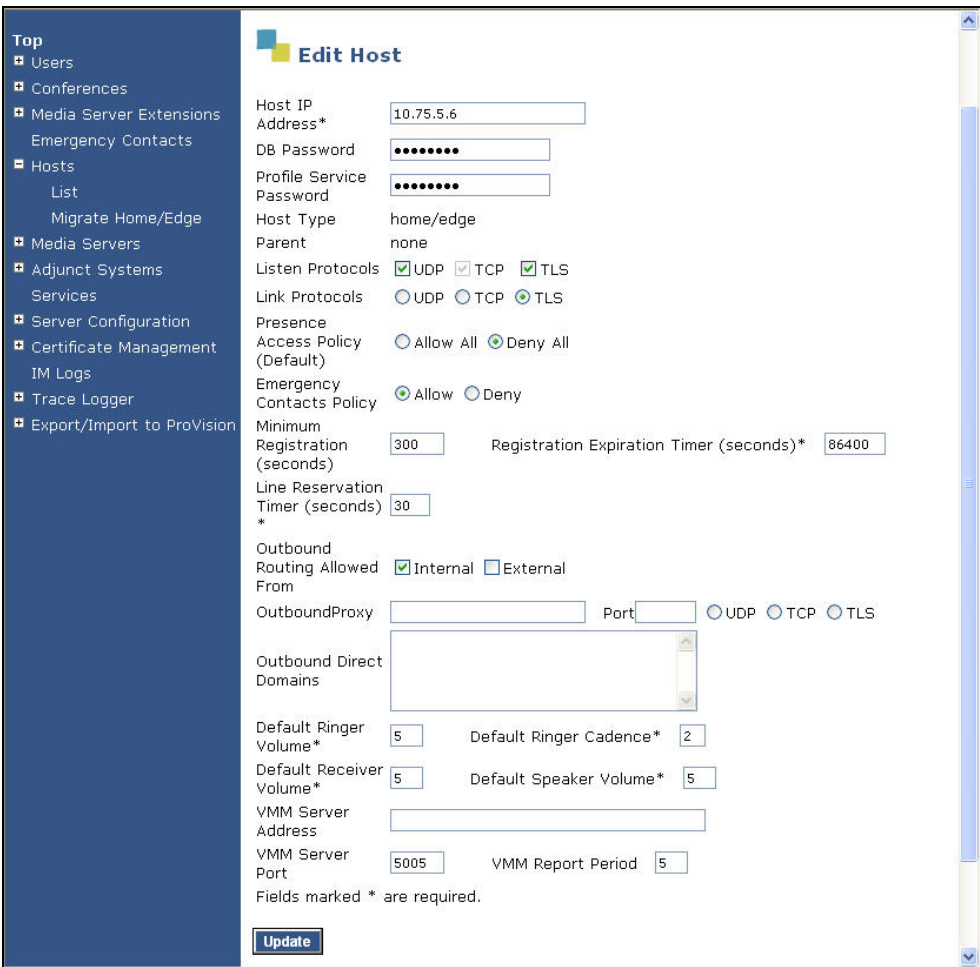
Step	Description
1.	<p>Access the Avaya SES administration web interface by entering <a href="http://&lt;ip-addr&gt;/admin">http://&lt;ip-addr&gt;/admin</a> as the URL in a Web browser, where &lt;ip-addr&gt; is the IP address of the Avaya SES server.</p> <p>Log in with the appropriate credentials and then select the <b>Launch Administration Web Interface</b> link from the main page as shown below.</p> 

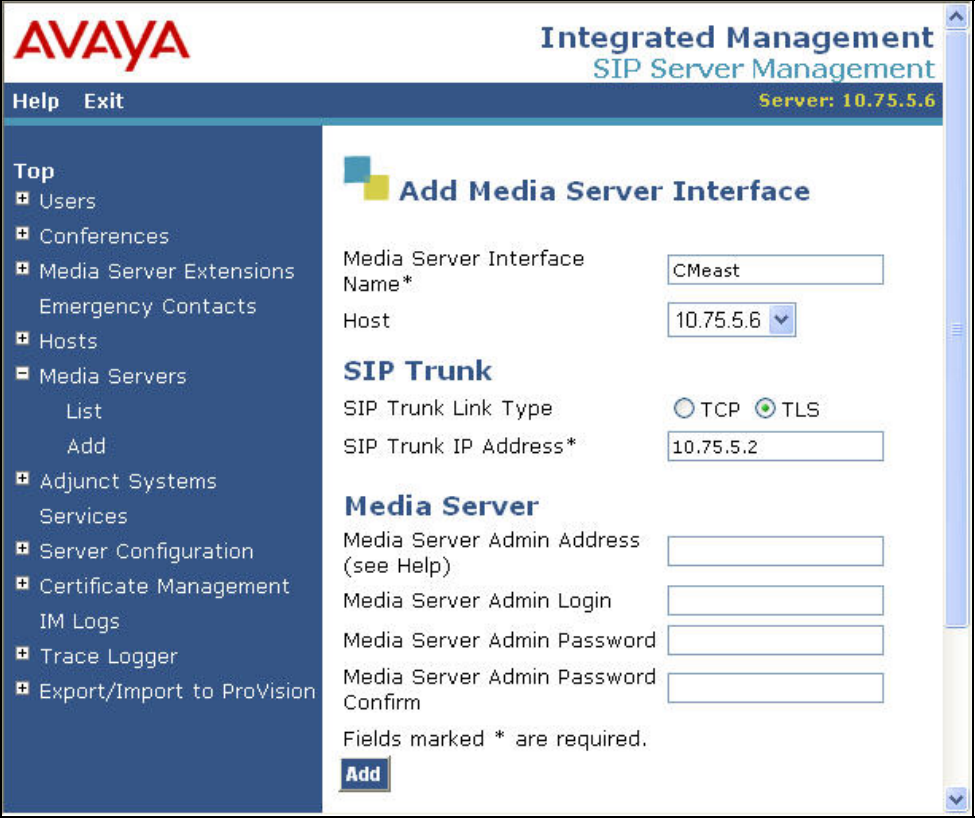
Step	Description																												
2.	<p>The Avaya SES Administration Home Page will be displayed as shown below.</p>  <p>The screenshot displays the Avaya Integrated Management SIP Server Management interface. At the top, the Avaya logo is on the left, and the title 'Integrated Management SIP Server Management' is on the right, with 'Server: 10.75.5.6' below it. A navigation bar contains 'Help' and 'Exit'. A left sidebar lists various management options: Top, Users, Conferences, Media Server Extensions, Emergency Contacts, Hosts, Media Servers, Adjunct Systems, Services, Server Configuration, Certificate Management, IM Logs, Trace Logger, and Export/Import to ProVision. The main content area features a 'Top' section with a table of management functions:</p> <table border="1"> <thead> <tr> <th colspan="2">Top</th> </tr> </thead> <tbody> <tr> <td><b>Manage Users</b></td> <td>Add and delete Users.</td> </tr> <tr> <td><b>Manage Conferencing</b></td> <td>Add and delete Conference Extensions.</td> </tr> <tr> <td><b>Manage Media Server Extensions</b></td> <td>Add and delete Media Server Extensions.</td> </tr> <tr> <td><b>Manage Emergency Contacts</b></td> <td>Add and delete Emergency Contacts.</td> </tr> <tr> <td><b>Manage Hosts</b></td> <td>Add and delete Hosts.</td> </tr> <tr> <td><b>Manage Media Servers</b></td> <td>Add and delete Media Servers.</td> </tr> <tr> <td><b>Manage Adjunct Systems</b></td> <td>Add and delete Adjunct Systems.</td> </tr> <tr> <td><b>Manage Services</b></td> <td>Start and stop server processes on this host.</td> </tr> <tr> <td><b>Server Configuration</b></td> <td>Edit Properties of the system.</td> </tr> <tr> <td><b>Certificate Management</b></td> <td>Manage Certificates.</td> </tr> <tr> <td><b>IM Logs</b></td> <td>Download IM Logs.</td> </tr> <tr> <td><b>Trace Logger</b></td> <td>Manage SIP Trace Logs.</td> </tr> <tr> <td><b>Export Import to ProVision</b></td> <td>Export and import data using ProVision on this host.</td> </tr> </tbody> </table> <p>At the bottom of the page, the copyright notice '© 2006 Avaya Inc. All Rights Reserved.' is displayed.</p>	Top		<b>Manage Users</b>	Add and delete Users.	<b>Manage Conferencing</b>	Add and delete Conference Extensions.	<b>Manage Media Server Extensions</b>	Add and delete Media Server Extensions.	<b>Manage Emergency Contacts</b>	Add and delete Emergency Contacts.	<b>Manage Hosts</b>	Add and delete Hosts.	<b>Manage Media Servers</b>	Add and delete Media Servers.	<b>Manage Adjunct Systems</b>	Add and delete Adjunct Systems.	<b>Manage Services</b>	Start and stop server processes on this host.	<b>Server Configuration</b>	Edit Properties of the system.	<b>Certificate Management</b>	Manage Certificates.	<b>IM Logs</b>	Download IM Logs.	<b>Trace Logger</b>	Manage SIP Trace Logs.	<b>Export Import to ProVision</b>	Export and import data using ProVision on this host.
Top																													
<b>Manage Users</b>	Add and delete Users.																												
<b>Manage Conferencing</b>	Add and delete Conference Extensions.																												
<b>Manage Media Server Extensions</b>	Add and delete Media Server Extensions.																												
<b>Manage Emergency Contacts</b>	Add and delete Emergency Contacts.																												
<b>Manage Hosts</b>	Add and delete Hosts.																												
<b>Manage Media Servers</b>	Add and delete Media Servers.																												
<b>Manage Adjunct Systems</b>	Add and delete Adjunct Systems.																												
<b>Manage Services</b>	Start and stop server processes on this host.																												
<b>Server Configuration</b>	Edit Properties of the system.																												
<b>Certificate Management</b>	Manage Certificates.																												
<b>IM Logs</b>	Download IM Logs.																												
<b>Trace Logger</b>	Manage SIP Trace Logs.																												
<b>Export Import to ProVision</b>	Export and import data using ProVision on this host.																												

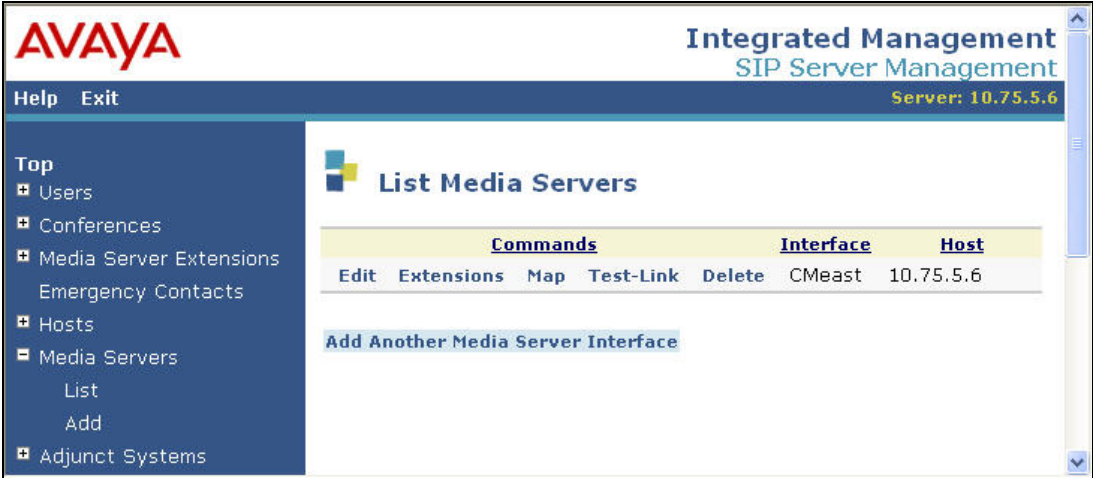


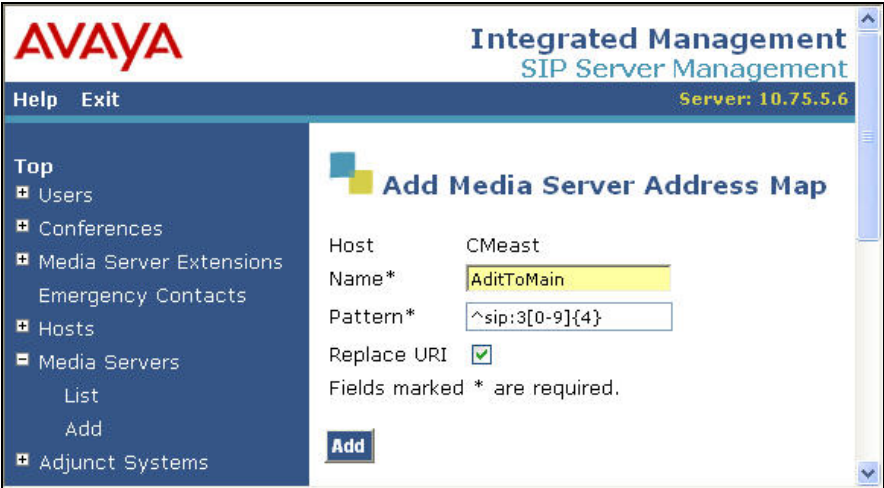
Step	Description																												
3.	<p>After making changes within Avaya SES, it is necessary to commit the database changes using the <b>Update</b> link that appears when changes are pending. Perform this step by clicking on the <b>Update</b> link found in the bottom of the blue navigation bar on the left side of any of the Avaya SES administration pages as shown below. It is recommended that this be done after making each set of changes described in the following steps.</p>  <p>The screenshot displays the Avaya Integrated Management SIP Server Management interface. On the left, a blue navigation bar contains a list of menu items: Top, Users, Conferences, Media Server Extensions, Emergency Contacts, Hosts, Media Servers, Adjunct Systems, Server Configuration, Certificate Management, Trace Logger, and Export/Import to ProVision. The 'Update' link is highlighted with a white box at the bottom of this bar. The main content area is white and shows a 'Top' section with a list of management tasks and their descriptions:</p> <table border="1"> <thead> <tr> <th>Task</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Manage Users</td> <td>Add and delete Users.</td> </tr> <tr> <td>Manage Conferencing</td> <td>Add and delete Conference Extensions.</td> </tr> <tr> <td>Manage Media Server Extensions</td> <td>Add and delete Media Server Extensions.</td> </tr> <tr> <td>Manage Emergency Contacts</td> <td>Add and delete Emergency Contacts.</td> </tr> <tr> <td>Manage Hosts</td> <td>Add and delete Hosts.</td> </tr> <tr> <td>Manage Media Servers</td> <td>Add and delete Media Servers.</td> </tr> <tr> <td>Manage Adjunct Systems</td> <td>Add and delete Adjunct Systems.</td> </tr> <tr> <td>Manage Services</td> <td>Start and stop server processes on this host.</td> </tr> <tr> <td>Server Configuration</td> <td>Edit Properties of the system.</td> </tr> <tr> <td>Certificate Management</td> <td>Manage Certificates.</td> </tr> <tr> <td>IM Logs</td> <td>Download IM Logs.</td> </tr> <tr> <td>Trace Logger</td> <td>Manage SIP Trace Logs.</td> </tr> <tr> <td>Export Import to ProVision</td> <td>Export and import data using ProVision on this host.</td> </tr> </tbody> </table> <p>The footer of the interface indicates '© 2006 Avaya Inc. All Rights Reserved.'</p>	Task	Description	Manage Users	Add and delete Users.	Manage Conferencing	Add and delete Conference Extensions.	Manage Media Server Extensions	Add and delete Media Server Extensions.	Manage Emergency Contacts	Add and delete Emergency Contacts.	Manage Hosts	Add and delete Hosts.	Manage Media Servers	Add and delete Media Servers.	Manage Adjunct Systems	Add and delete Adjunct Systems.	Manage Services	Start and stop server processes on this host.	Server Configuration	Edit Properties of the system.	Certificate Management	Manage Certificates.	IM Logs	Download IM Logs.	Trace Logger	Manage SIP Trace Logs.	Export Import to ProVision	Export and import data using ProVision on this host.
Task	Description																												
Manage Users	Add and delete Users.																												
Manage Conferencing	Add and delete Conference Extensions.																												
Manage Media Server Extensions	Add and delete Media Server Extensions.																												
Manage Emergency Contacts	Add and delete Emergency Contacts.																												
Manage Hosts	Add and delete Hosts.																												
Manage Media Servers	Add and delete Media Servers.																												
Manage Adjunct Systems	Add and delete Adjunct Systems.																												
Manage Services	Start and stop server processes on this host.																												
Server Configuration	Edit Properties of the system.																												
Certificate Management	Manage Certificates.																												
IM Logs	Download IM Logs.																												
Trace Logger	Manage SIP Trace Logs.																												
Export Import to ProVision	Export and import data using ProVision on this host.																												

Step	Description
4.	<p>From the left pane of the administration web interface, expand the <b>Server Configuration</b> option and select <b>System Properties</b>. The <b>Edit System Properties</b> page displays the software version in the <b>SES Version</b> field and the network properties entered during the installation process.</p> <p>On the <b>Edit System Properties</b> page:</p> <ul style="list-style-type: none"> <li>▪ Verify the <b>SIP Domain</b> name assigned to Avaya SES. This must match the <b>Authoritative Domain</b> field configured on Avaya Communication Manager shown in <b>Section 3.1.1, Step 5</b>.</li> <li>▪ Verify the <b>License Host</b> field. This is the host name, the fully qualified domain name, or the IP address of the SIP proxy server that is running the WebLM application and has the associated license file installed.</li> <li>▪ After reviewing the <b>Edit System Properties</b> page, if any changes have been made, click the <b>Update</b> button.</li> </ul> 


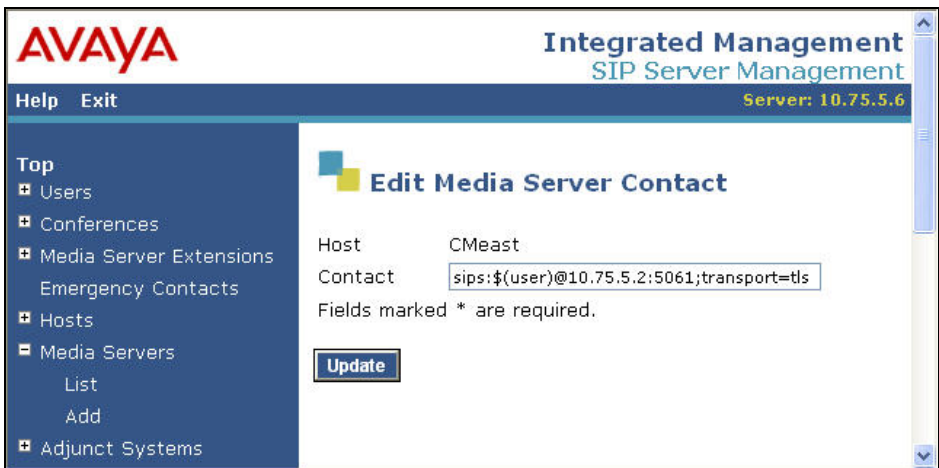
Step	Description
5.	<p>After verifying the domain on the <b>Edit System Properties</b> page, verify the host computer entry for Avaya SES. The following example shows the <b>Edit Host</b> page since the host had already been added to the system.</p> <p>The <b>Edit Host</b> page shown below is accessible by clicking on the <b>Hosts → List</b> link in the left pane and then clicking on the <b>Edit</b> link under the <b>Commands</b> section of the subsequent page (not shown).</p> <ul style="list-style-type: none"> <li>▪ In the <b>Host IP Address</b> field, verify the IP address of the Avaya SES server.</li> <li>▪ Although the fields are hidden, the <b>DB Password</b> and <b>Profile Service Password</b> will reflect the values that were specified during the system installation.</li> <li>▪ Since only one Avaya SES is used in the configuration, the <b>Host Type</b> is set to <i>home/edge</i>.</li> <li>▪ The default values for the other fields were used.</li> </ul> <p>If any changes were made, scroll down to the bottom of the page and click the <b>Update</b> button.</p> 

Step	Description
6.	<p>From the left pane of the administration web interface, expand the <b>Media Servers</b> option and select <b>Add</b> to add the Avaya Media Server to the list of media servers known to Avaya SES. Adding the media server will create the Avaya SES side of the SIP trunk previously created in Avaya Communication Manager.</p> <p>On the <b>Add Media Server Interface</b> page, enter the following information:</p> <ul style="list-style-type: none"> <li>Enter a descriptive name in the <b>Media Server Interface Name</b> field (e.g. CMeast).</li> <li>In the <b>Host</b> field, select the Avaya SES server from the pull-down menu that will serve as the SIP proxy for this media server. Since there is only one Avaya SES server in this configuration, the <b>Host</b> field is set to the host shown in <b>Step 5</b>.</li> <li>Select <b>TLS</b> (Transport Link Security) for the <b>SIP Trunk Link Type</b>. TLS provides encryption at the transport layer. TLS is the only link protocol that is supported for communication between Avaya SES and Avaya Communication Manager.</li> <li>Enter the IP address of the Avaya S8300 Media Server in the <b>SIP Trunk IP Address</b> field. In alternative configurations that use a C-LAN board, the <b>SIP Trunk IP Address</b> would be the IP address of the C-LAN board.</li> <li>The default values may be retained for all other fields.</li> <li>After completing the <b>Add Media Server Interface</b> page, click the <b>Add</b> button.</li> </ul> 

Step	Description
7.	<p>Since the dialed numbers associated with the Adit 3500 do not have media server extensions associated with them, then calls from these numbers to the main site are not routed automatically to Avaya Communication Manager at the main site. Two Media Server Address Map are required on Avaya SES to direct calls inbound to Avaya Communication Manager from these numbers.</p> <p>In the case of the compliance test, a Media Server Address Map was created to match all calls dialed with a 5 digit number beginning with a 3. This matches the extensions at the main site. A Media Server Address Map was also created to match external calls 12 digits in length and beginning with 91732.</p> <p>To configure a <b>Media Server Address Map</b>:</p> <ul style="list-style-type: none"> <li>Expand the <b>Media Servers</b> option in the left pane of the administration web interface and select <b>List</b>. This will display the <b>List Media Servers</b> page below.</li> <li>Click on the <b>Map</b> link to display the <b>List Media Server Address Map</b> page (not shown). On the <b>List Media Server Address Map</b> page, click on the <b>Add Map In New Group</b> link.</li> </ul> 

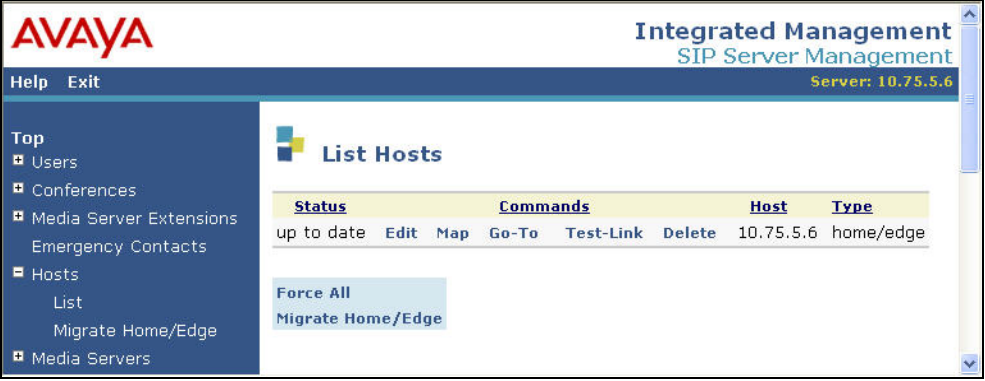
Step	Description
8.	<p>On the <b>Add Media Server Address Map</b> page that appears:</p> <ul style="list-style-type: none"> <li>Enter a descriptive name in the <b>Name</b> field.</li> <li>In the <b>Pattern</b> field, enter an expression to define the matching criteria for calls to be routed to the main site from the ISDN-PRI interface on the Adit 3500. The example below shows the expression used in the compliance test. This expression will match an URI that begins with <i>sip:3</i> followed by any digit between <i>0-9</i> for the next <i>4</i> digits. <b>Appendix A</b> contains additional information on the syntax used for address map patterns.</li> </ul> <p>Click the <b>Add</b> button.</p> 
9.	<p>Repeat <b>Steps 7 – 8</b>, to add the Media Server Address Map for external calls. The <b>Pattern</b> expression will match an URI that begins with <i>sip:91732</i> followed by any digit between <i>0-9</i> for the next <i>7</i> digits.</p> <p>Use the following values:</p> <p><b>Name:</b> <i>AditToExt</i></p> <p><b>Pattern:</b> <i>^sip:91732[0-9]{7}</i></p>

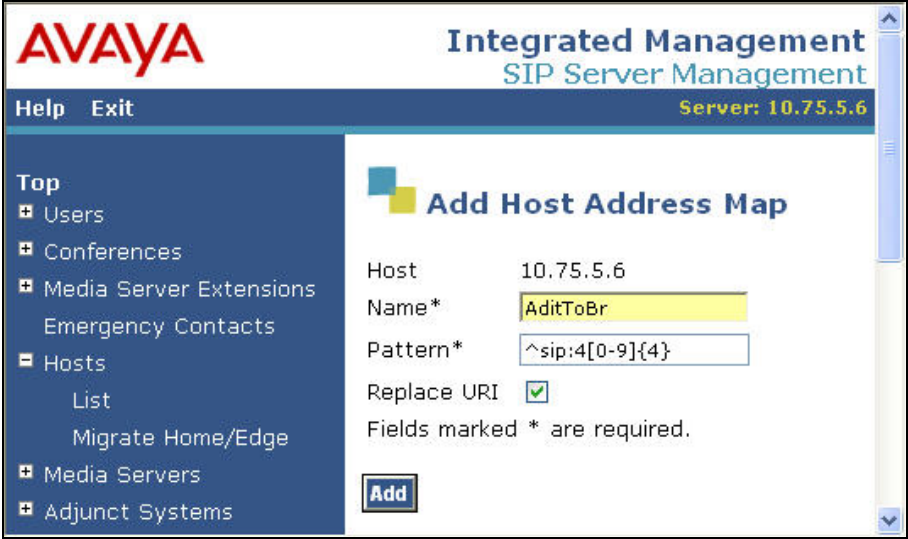
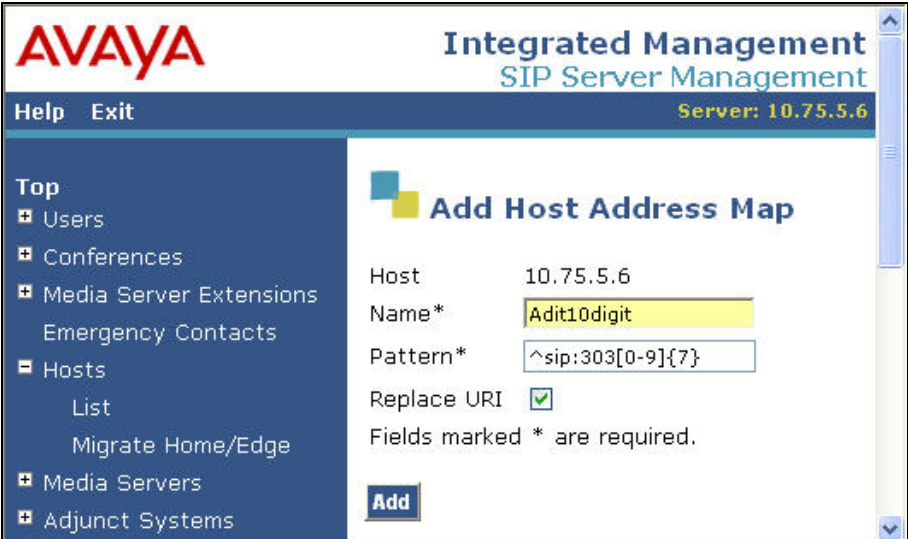


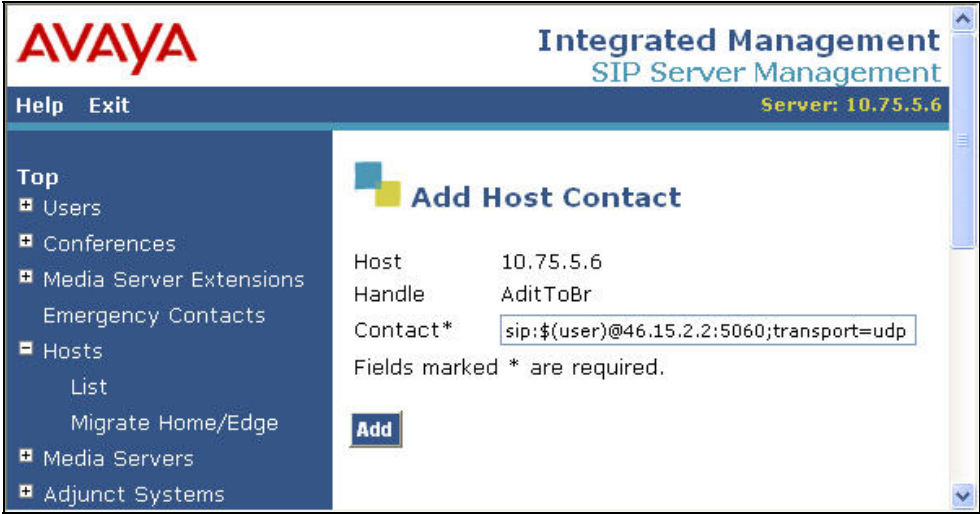
Step	Description
10.	<p>After configuring the Media Server Address Maps, the <b>List Media Server Address Map</b> page appears. The Media Server Contact is created automatically and directs the calls to the IP address of the Avaya Media Server (<b>10.75.5.2</b>) using port 5061 and TLS as the transport protocol. The user portion in the original request URI is substituted for “\$(user)”. The <b>Contact</b> field that is automatically generated is shown below:</p> <p style="text-align: center;"><b><i>sip:\$(user)@10.75.5.2:5061;transport=tls</i></b></p> <p><b>Important Note:</b> For interoperability between the stated releases of Avaya SES and the Adit 3500 used for the compliance test, the <b>Contact</b> field must be changed to specify <b>sips</b> instead of <b>sip</b>.</p> <p>To edit the <b>Contact</b> field, click on the <b>Edit</b> link next to the contact.</p> 
11.	<p>On the <b>Edit Media Server Contact</b> page, enter the following in the <b>Contact</b> field: <b><i>sips:\$(user)@10.75.5.2:5061;transport=tls</i></b></p> <p>Click Update.</p> 


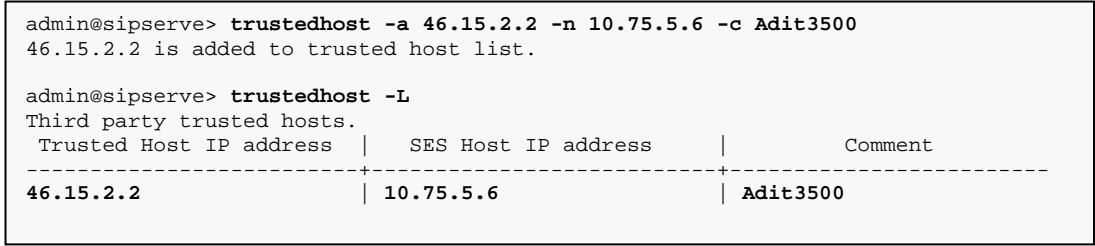
Step	Description																
12.	<p>The final list of Media Server Address Maps and Contact information is shown below.</p> <div><div><div>AVAYA</div><div>Integrated Management SIP Server Management Server: 10.75.5.6</div></div><div><div>Help Exit</div><div>Top<ul style="list-style-type: none"><li>Users</li><li>Conferences</li><li>Media Server Extensions<ul style="list-style-type: none"><li>Emergency Contacts</li></ul></li><li>Hosts</li><li>Media Servers<ul style="list-style-type: none"><li>List</li><li>Add</li></ul></li><li>Adjunct Systems<ul style="list-style-type: none"><li>Services</li></ul></li><li>Server Configuration</li><li>Certificate Management</li></ul></div><div><div>List Media Server Address Map</div><div>HostCMeast</div><table><thead><tr><th>Commands</th><th>Name</th><th>Commands</th><th>Contact</th></tr></thead><tbody><tr><td>Edit Delete AditToExt</td><td></td><td></td><td></td></tr><tr><td>Edit Delete AditToMain</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td>Edit Delete</td><td>sips:\${user}@10.75.5.2:5061;transport=tls</td></tr></tbody></table><div><div>Add Another Map</div><div>Add Another Contact</div><div>Delete Group</div></div><div>Add Map In New Group</div></div></div></div>	Commands	Name	Commands	Contact	Edit Delete AditToExt				Edit Delete AditToMain						Edit Delete	sips:\${user}@10.75.5.2:5061;transport=tls
Commands	Name	Commands	Contact														
Edit Delete AditToExt																	
Edit Delete AditToMain																	
		Edit Delete	sips:\${user}@10.75.5.2:5061;transport=tls														



Step	Description
13.	<p>Host Address Maps are required on Avaya SES to direct calls outbound from Avaya Communication Manager to the numbers associated with the Adit 3500. In the SIP trunking model, these numbers are not registered as users with Avaya SES. Thus, calls are not automatically routed to the Adit 3500 based on a registered user contact. Instead, an 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 <i>sip:user@domain</i>, where <i>domain</i> can be a domain name or an IP address. The user portion can be an alpha-numeric name, telephone number or extension.</p> <p>In the case of the compliance test, the user portion contained the called party number. Calls with a called party number of 4xxxx were routed to the Adit 3500. Thus, the Host Address Map was configured to match all calls with 5 digits and beginning with a 4. In addition, a Host Address Map was configured to match calls with 10 digits and beginning with 303.</p> <p>To configure a <b>Host Address Map</b>:</p> <ul style="list-style-type: none"> <li>Expand the <b>Hosts</b> option in the left pane of the administration web interface and select <b>List</b>. This will display the <b>List Hosts</b> page below.</li> <li>Click on the <b>Map</b> link to display the <b>List Host Address Map</b> page (not shown). On the <b>List Host Address Map</b> page, click on the <b>Add Map In New Group</b> link.</li> </ul> 

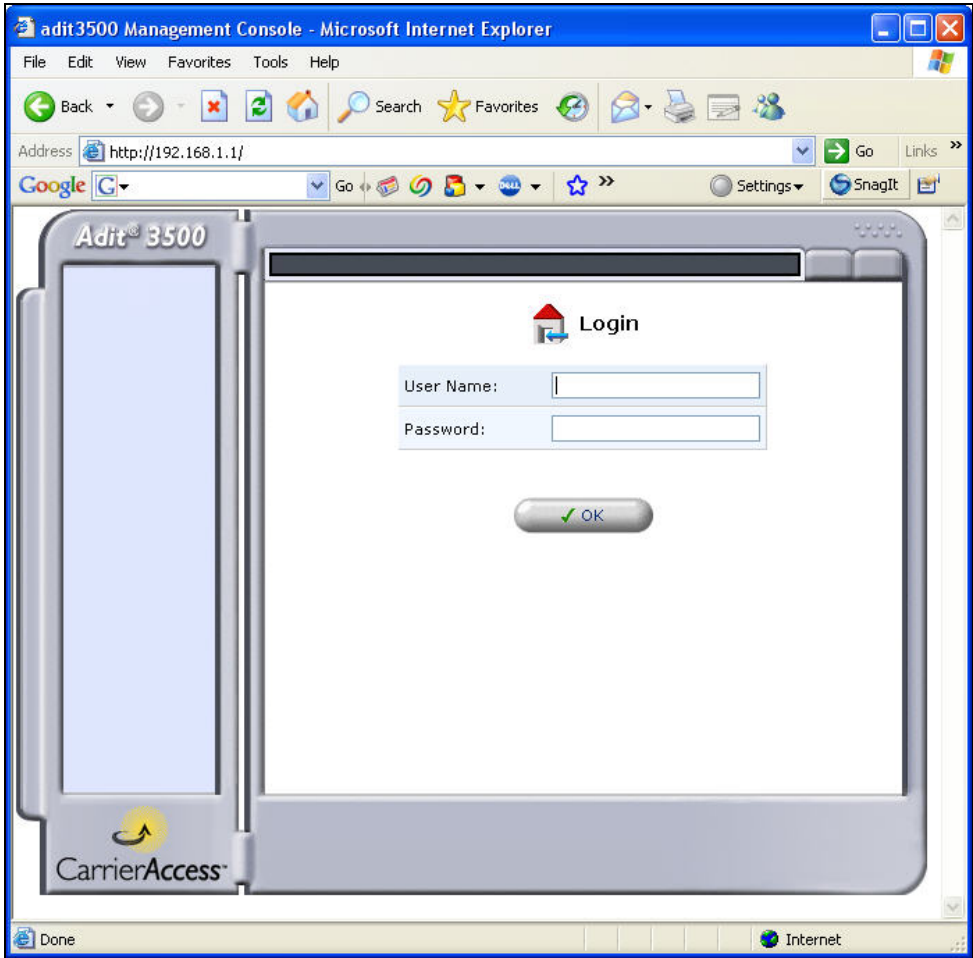
Step	Description
14.	<p>On the <b>Add Host Address Map</b> page that appears:</p> <ul style="list-style-type: none"> <li>Enter a descriptive name in the <b>Name</b> field.</li> <li>In the <b>Pattern</b> field, enter an expression to define the matching criteria for calls to be routed to the Adit 3500. The example below shows the expression used in the compliance test. This expression will match an URI that begins with <b>sip:4</b> followed by any digit between <b>0-9</b> for the next <b>4</b> digits. <b>Appendix A</b> contains additional information on the syntax used for address map patterns.</li> </ul> <p>Click the <b>Add</b> button.</p> 
15.	<p>Create a second Host Address Map using an expression in the <b>Pattern</b> field that will match an URI that begins with <b>sip:303</b> followed by any digit between <b>0-9</b> for the next <b>7</b> digits.</p> 

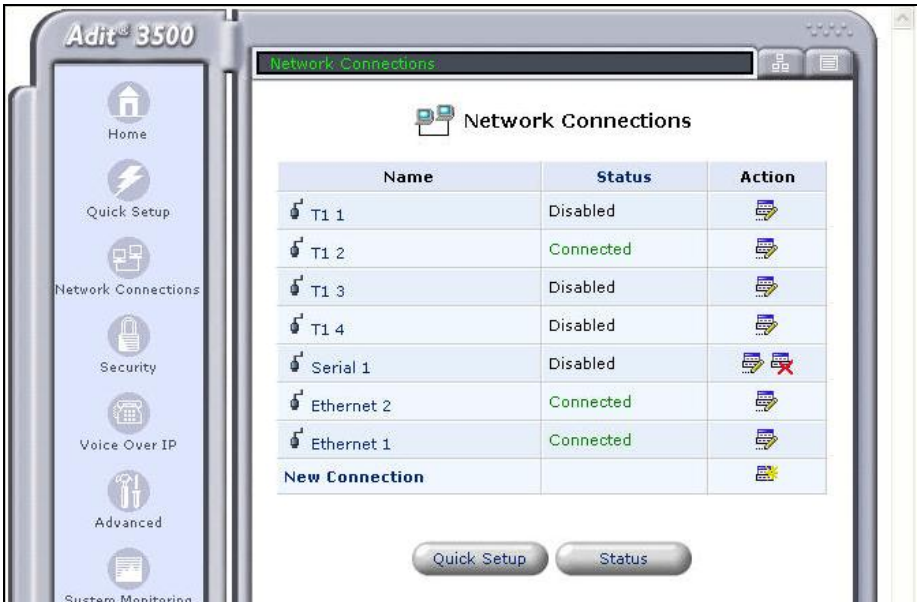
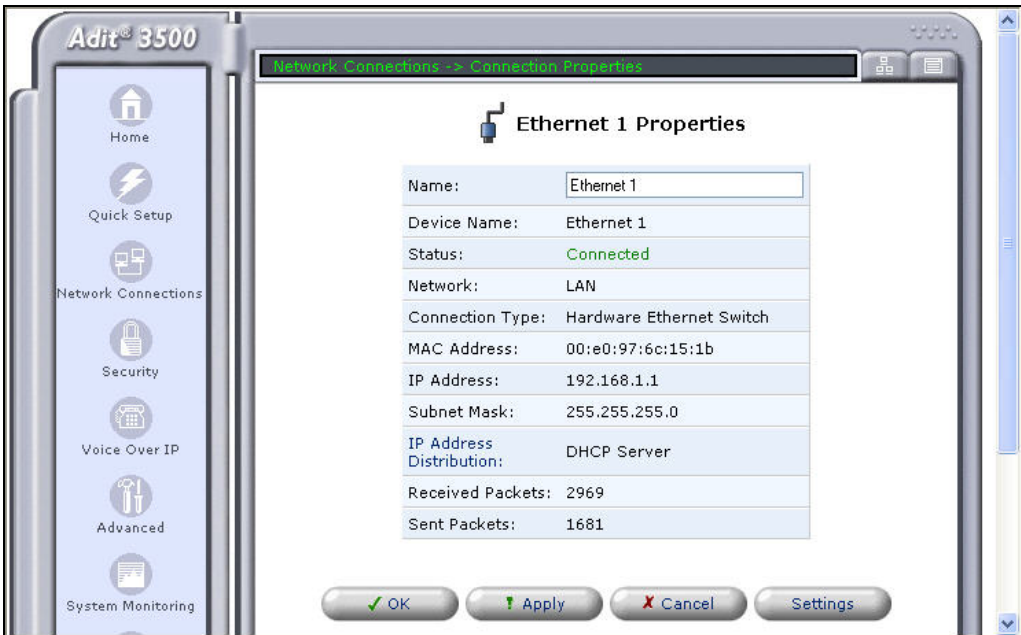
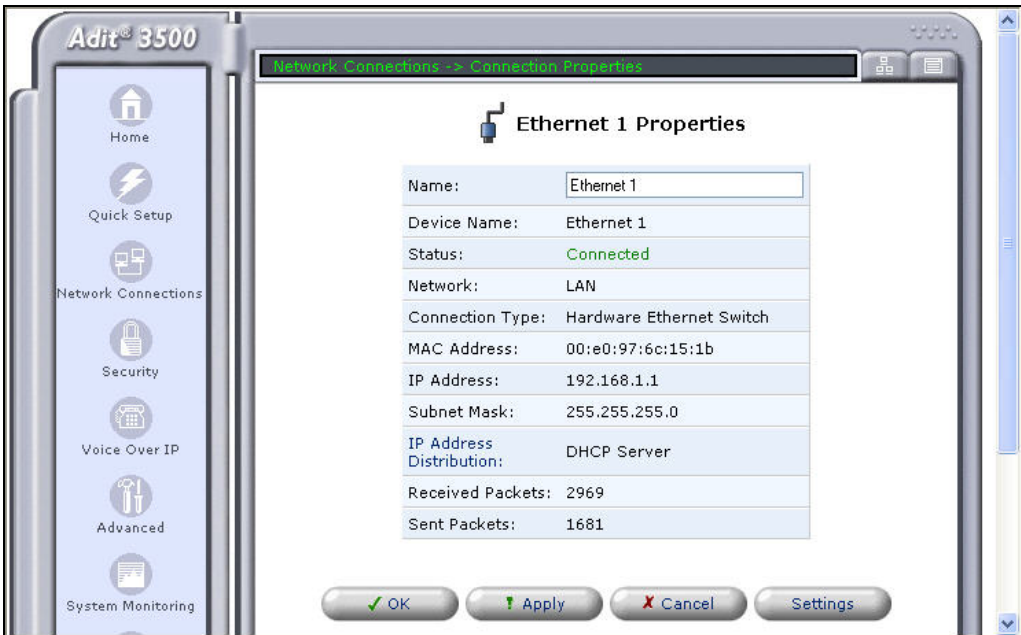
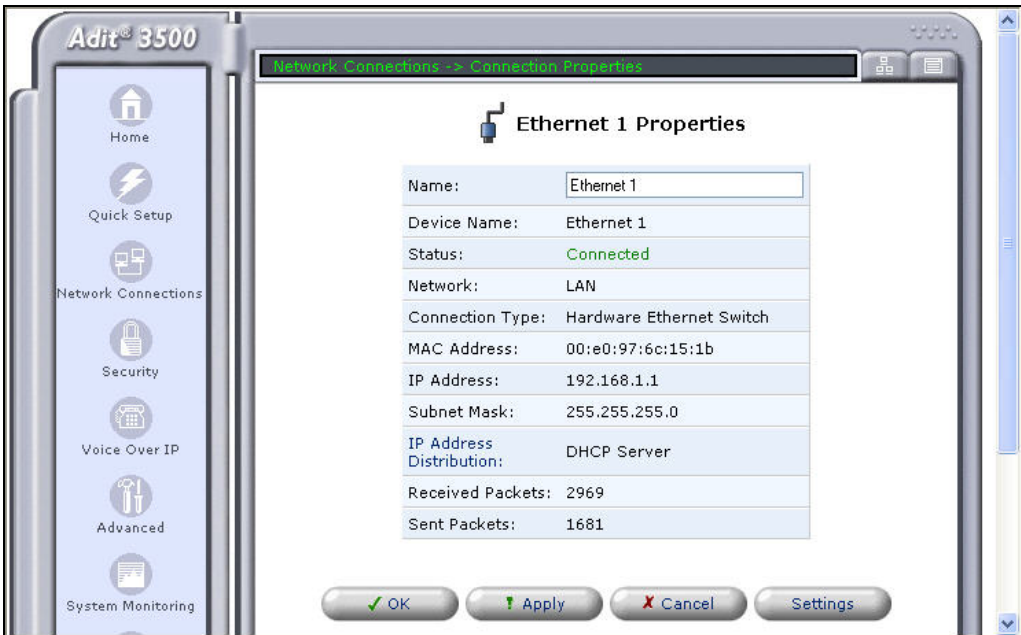
Step	Description
16.	<p>Next, a Host Contact must be entered for the Address Maps that were previously defined. The contact defines the destination IP address, port number and transport protocol to use when routing calls that match the Address Map.</p> <p>To add a Host Contact:</p> <ul style="list-style-type: none"> <li>▪ Open the <b>List Host Address Map</b> page as described (but not shown) in <b>Step 13</b>.</li> <li>▪ Click on the <b>Add Another Contact</b> link associated with the address map added previously to open the <b>Add Host Contact</b> page shown below.</li> <li>▪ In the <b>Contact</b> field, enter the destination IP address (<i>ip_addr</i>), port number (<i>port</i>) and transport protocol (<i>protocol</i>) in the following format.</li> </ul> <pre>sip:\${user}@ip_addr:port;transport=protocol</pre> <p>The user part in the original request URI is inserted in place of the “\$(user)” string before the message is sent to the destination.</p> <p>For the compliance test, the Adit 3500 had IP address of 46.15.2.2. Thus, the following contact value was used:</p> <pre>sip:\${user}@46.15.2.2:5060;transport=udp</pre> <p>Click the <b>Add</b> button.</p> 

Step	Description
17.	<p>After configuring the Host Address Map and Contact, the <b>List Host Address Map</b> page will appear as shown below.</p> 
18.	<p>Lastly, the IP address of the Adit 3500 must be configured as a trusted host on Avaya SES. As a trusted host, Avaya SES will not issue SIP authentication challenges for incoming requests from the designated IP address.</p> <p>To configure a trusted host:</p> <ul style="list-style-type: none"> <li>Connect to Avaya SES and log in using proper credentials.</li> <li>Enter the following <b>trustedhost</b> command at the Linux shell prompt.</li> </ul> <pre>trustedhost -a 46.15.2.2 -n 10.75.5.6 -c Adit3500</pre> <ul style="list-style-type: none"> <li>Use the following <b>trustedhost</b> command to verify the entry is correct.</li> </ul> <pre>trustedhost -L</pre> <ul style="list-style-type: none"> <li><b>Important Note:</b> Complete the trusted host configuration by returning to the main Avaya SES administration web interface and clicking the <b>Update</b> link as shown in <b>Section 3.2, Step 3</b>. If the Update link is not visible, refresh the page by selecting the <b>Top</b> link from the left menu. This step is required even though the trusted host was configured via the Linux shell.</li> </ul> <p>The screen below illustrates the results of the <b>trustedhost</b> commands.</p> 

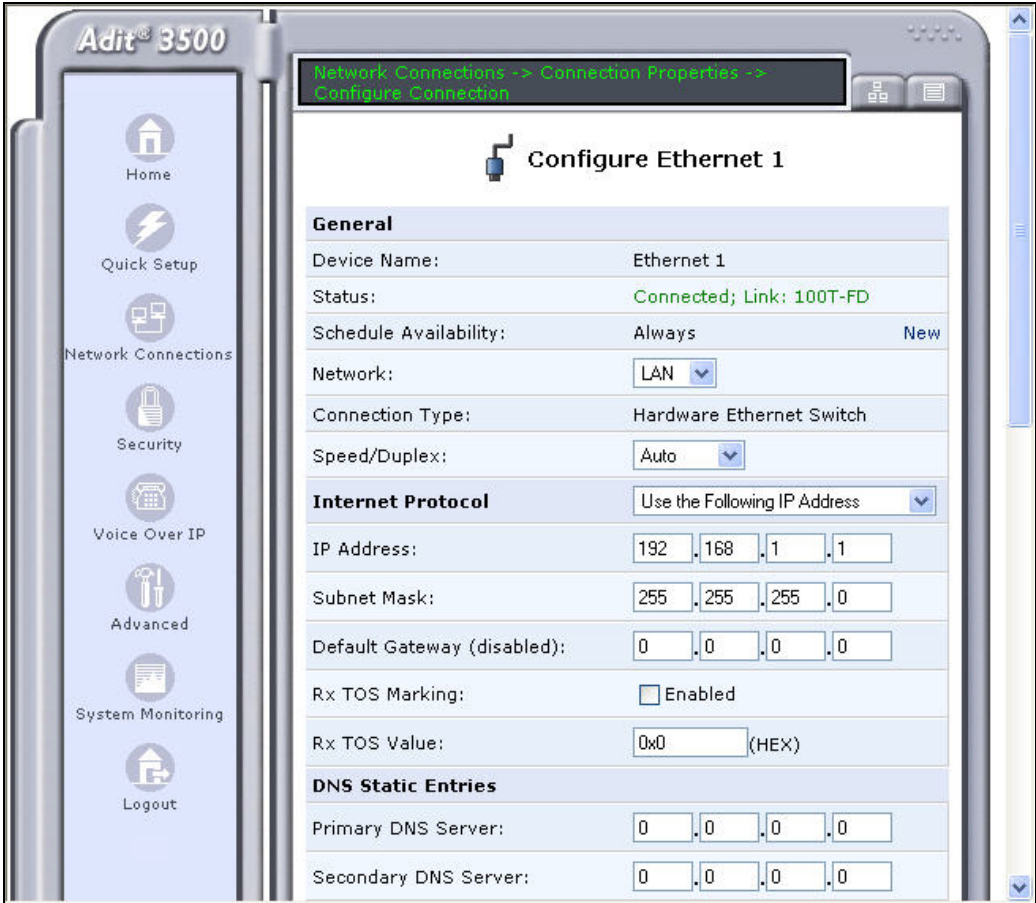
### 3.3. Configure the Adit 3500

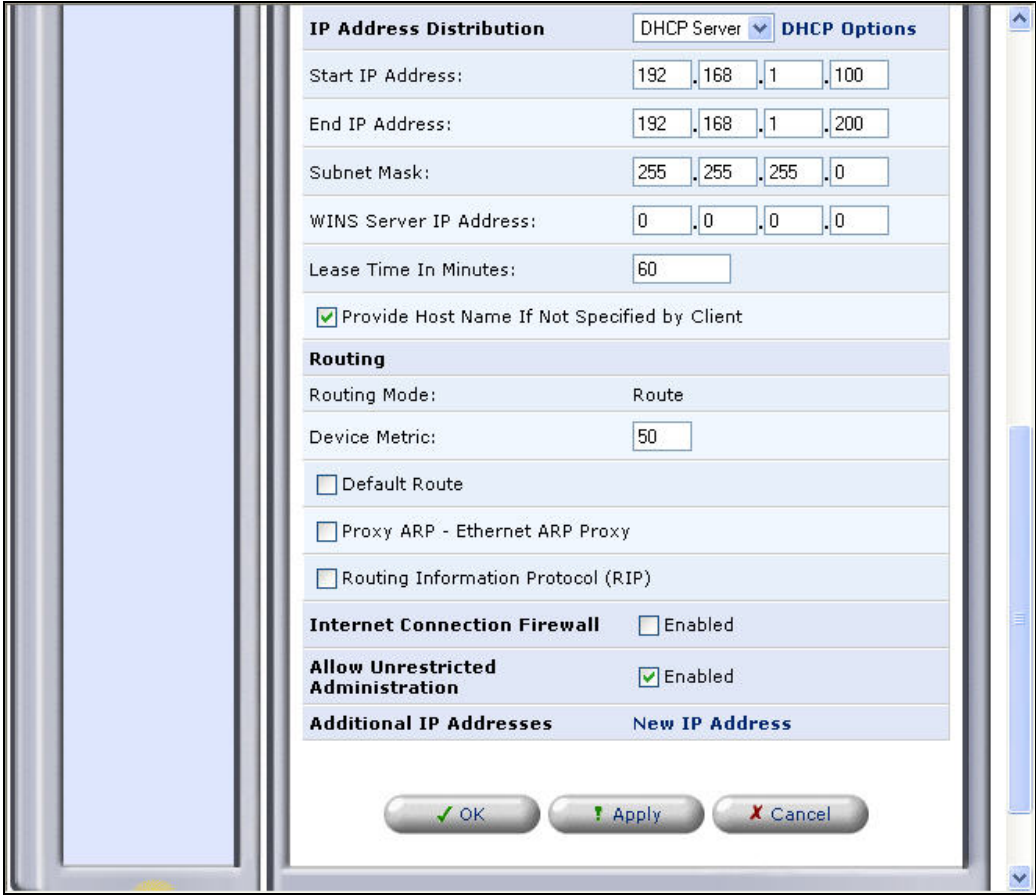
This section describes the procedure for configuring the Adit 3500. This procedure assumes the Adit 3500 has already been configured with IP addresses for both the private and public interfaces. The Adit 3500 configuration described in this section is performed using an Internet browser. For detailed information on the initial installation of the Adit 3500, consult references [7] and [8].

Step	Description
1.	<p>Launch an Internet browser from a PC on the private side of the Adit 3500. Enter the IP address of the Adit 3500 in the <b>Address</b> field. The login screen appears as shown below. Enter a valid <b>User Name</b> and <b>Password</b>.</p> <p>Click <b>OK</b> to proceed.</p> 


Step	Description																																																			
2.	<p>A list of configuration options will appear in the left pane of the window. To view the properties of the private interface of the device configured during installation, select <b>Network Connections</b>. A list of network connections appears in the right pane. Click the <b>Ethernet 1</b> entry in the list or the <b>Action</b> icon associated with this entry.</p> <div><table data-bbox="698 518 1245 850"><thead><tr><th>Name</th><th>Status</th><th>Action</th></tr></thead><tbody><tr><td>T1 1</td><td>Disabled</td><td></td></tr><tr><td>T1 2</td><td>Connected</td><td></td></tr><tr><td>T1 3</td><td>Disabled</td><td></td></tr><tr><td>T1 4</td><td>Disabled</td><td></td></tr><tr><td>Serial 1</td><td>Disabled</td><td></td></tr><tr><td>Ethernet 2</td><td>Connected</td><td></td></tr><tr><td>Ethernet 1</td><td>Connected</td><td></td></tr><tr><td>New Connection</td><td></td><td></td></tr></tbody></table></div> <tr><td>3.</td><td><p>A summary of the properties for <b>Ethernet 1</b> are show in the right pane. Click <b>Settings</b> at the bottom of the pane for the complete list of settings.</p><div><table data-bbox="771 1266 1177 1640"><tbody><tr><td>Name:</td><td>Ethernet 1</td></tr><tr><td>Device Name:</td><td>Ethernet 1</td></tr><tr><td>Status:</td><td>Connected</td></tr><tr><td>Network:</td><td>LAN</td></tr><tr><td>Connection Type:</td><td>Hardware Ethernet Switch</td></tr><tr><td>MAC Address:</td><td>00:e0:97:6c:15:1b</td></tr><tr><td>IP Address:</td><td>192.168.1.1</td></tr><tr><td>Subnet Mask:</td><td>255.255.255.0</td></tr><tr><td>IP Address Distribution:</td><td>DHCP Server</td></tr><tr><td>Received Packets:</td><td>2969</td></tr><tr><td>Sent Packets:</td><td>1681</td></tr></tbody></table></div></td></tr>	Name	Status	Action	T1 1	Disabled		T1 2	Connected		T1 3	Disabled		T1 4	Disabled		Serial 1	Disabled		Ethernet 2	Connected		Ethernet 1	Connected		New Connection			3.	<p>A summary of the properties for <b>Ethernet 1</b> are show in the right pane. Click <b>Settings</b> at the bottom of the pane for the complete list of settings.</p> <div><table data-bbox="771 1266 1177 1640"><tbody><tr><td>Name:</td><td>Ethernet 1</td></tr><tr><td>Device Name:</td><td>Ethernet 1</td></tr><tr><td>Status:</td><td>Connected</td></tr><tr><td>Network:</td><td>LAN</td></tr><tr><td>Connection Type:</td><td>Hardware Ethernet Switch</td></tr><tr><td>MAC Address:</td><td>00:e0:97:6c:15:1b</td></tr><tr><td>IP Address:</td><td>192.168.1.1</td></tr><tr><td>Subnet Mask:</td><td>255.255.255.0</td></tr><tr><td>IP Address Distribution:</td><td>DHCP Server</td></tr><tr><td>Received Packets:</td><td>2969</td></tr><tr><td>Sent Packets:</td><td>1681</td></tr></tbody></table></div>	Name:	Ethernet 1	Device Name:	Ethernet 1	Status:	Connected	Network:	LAN	Connection Type:	Hardware Ethernet Switch	MAC Address:	00:e0:97:6c:15:1b	IP Address:	192.168.1.1	Subnet Mask:	255.255.255.0	IP Address Distribution:	DHCP Server	Received Packets:	2969	Sent Packets:	1681
Name	Status	Action																																																		
T1 1	Disabled																																																			
T1 2	Connected																																																			
T1 3	Disabled																																																			
T1 4	Disabled																																																			
Serial 1	Disabled																																																			
Ethernet 2	Connected																																																			
Ethernet 1	Connected																																																			
New Connection																																																				
3.	<p>A summary of the properties for <b>Ethernet 1</b> are show in the right pane. Click <b>Settings</b> at the bottom of the pane for the complete list of settings.</p> <div><table data-bbox="771 1266 1177 1640"><tbody><tr><td>Name:</td><td>Ethernet 1</td></tr><tr><td>Device Name:</td><td>Ethernet 1</td></tr><tr><td>Status:</td><td>Connected</td></tr><tr><td>Network:</td><td>LAN</td></tr><tr><td>Connection Type:</td><td>Hardware Ethernet Switch</td></tr><tr><td>MAC Address:</td><td>00:e0:97:6c:15:1b</td></tr><tr><td>IP Address:</td><td>192.168.1.1</td></tr><tr><td>Subnet Mask:</td><td>255.255.255.0</td></tr><tr><td>IP Address Distribution:</td><td>DHCP Server</td></tr><tr><td>Received Packets:</td><td>2969</td></tr><tr><td>Sent Packets:</td><td>1681</td></tr></tbody></table></div>	Name:	Ethernet 1	Device Name:	Ethernet 1	Status:	Connected	Network:	LAN	Connection Type:	Hardware Ethernet Switch	MAC Address:	00:e0:97:6c:15:1b	IP Address:	192.168.1.1	Subnet Mask:	255.255.255.0	IP Address Distribution:	DHCP Server	Received Packets:	2969	Sent Packets:	1681																													
Name:	Ethernet 1																																																			
Device Name:	Ethernet 1																																																			
Status:	Connected																																																			
Network:	LAN																																																			
Connection Type:	Hardware Ethernet Switch																																																			
MAC Address:	00:e0:97:6c:15:1b																																																			
IP Address:	192.168.1.1																																																			
Subnet Mask:	255.255.255.0																																																			
IP Address Distribution:	DHCP Server																																																			
Received Packets:	2969																																																			
Sent Packets:	1681																																																			

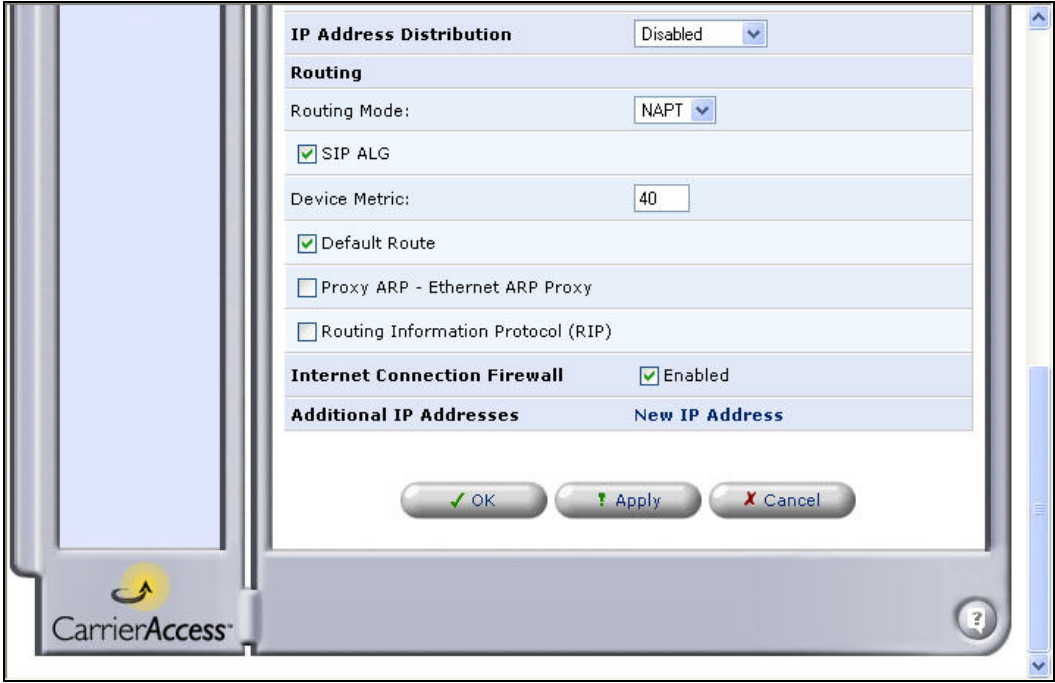


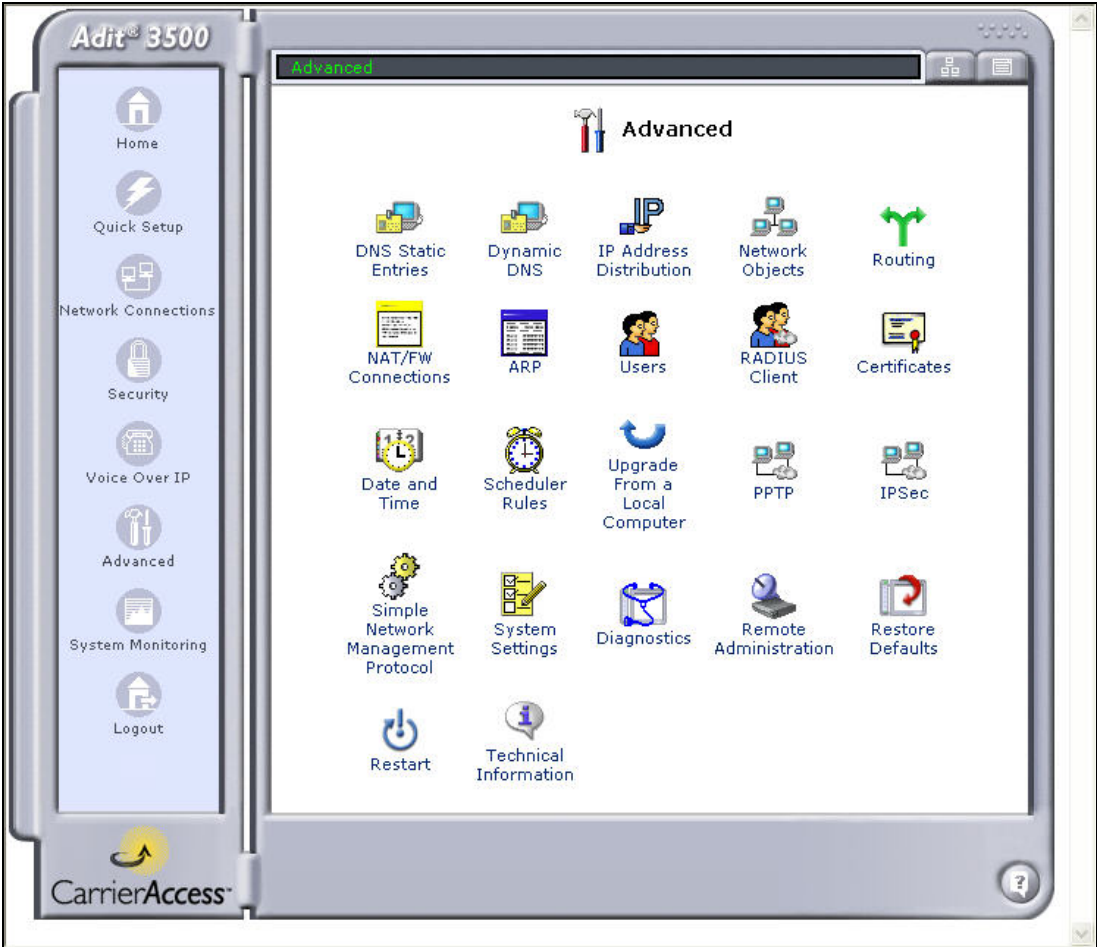
Step	Description
4.	<p>In the upper half of the right pane, verify the following settings for <b>Ethernet 1</b>. Make changes if necessary.</p> <ul style="list-style-type: none"> <li>▪ <b>Network:</b> Verify <i>LAN</i> is selected.</li> <li>▪ <b>Internet Protocol:</b> Verify <i>Use the Following IP Address</i> is selected.</li> <li>▪ <b>IP Address:</b> Verify this field is set to the IP address assigned to the private side of the device.</li> <li>▪ <b>Subnet Mask:</b> Verify the subnet mask is set to an appropriate value for the LAN addressing supported on the private side of the device.</li> <li>▪ <b>Default Gateway:</b> Verify the setting of the default gateway, if one is necessary. In the compliance test, no default gateway is required since the private side LAN is comprised of a single subnet.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Scroll down to view additional options.</p> 


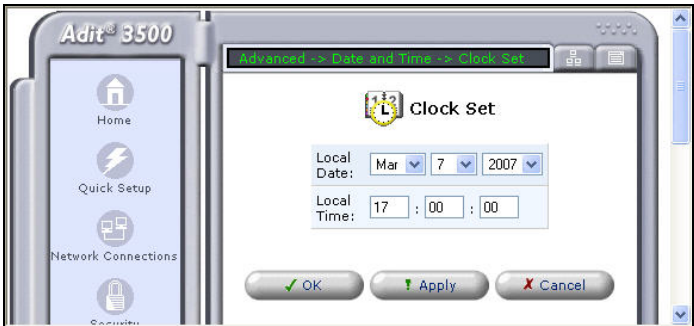
Step	Description
5.	<p>In the lower half of the right pane, configure the following settings for <b>Ethernet 1</b>.</p> <ul style="list-style-type: none"> <li>▪ <b>IP Address Distribution:</b> Select <i><b>DHCP Server</b></i>. This allows the Adit 3500 to serve as a DHCP server for the private LAN side of the device.</li> <li>▪ <b>Start IP Address:</b> Enter the first IP address that can be assigned by the DHCP server.</li> <li>▪ <b>End IP Address:</b> Enter the last IP address that can be assigned by the DHCP server.</li> <li>▪ <b>Subnet Mask:</b> Enter the subnet mask appropriate for the LAN addressing supported on the private side of the device.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Click <b>OK</b>.</p> 

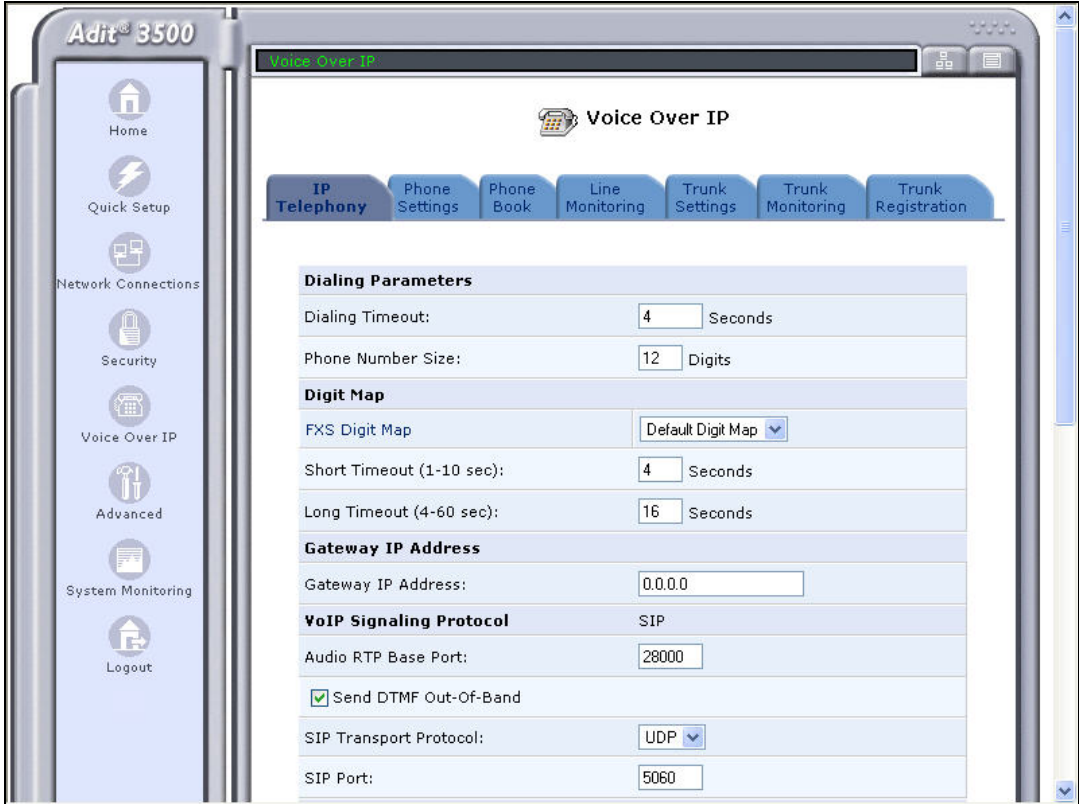


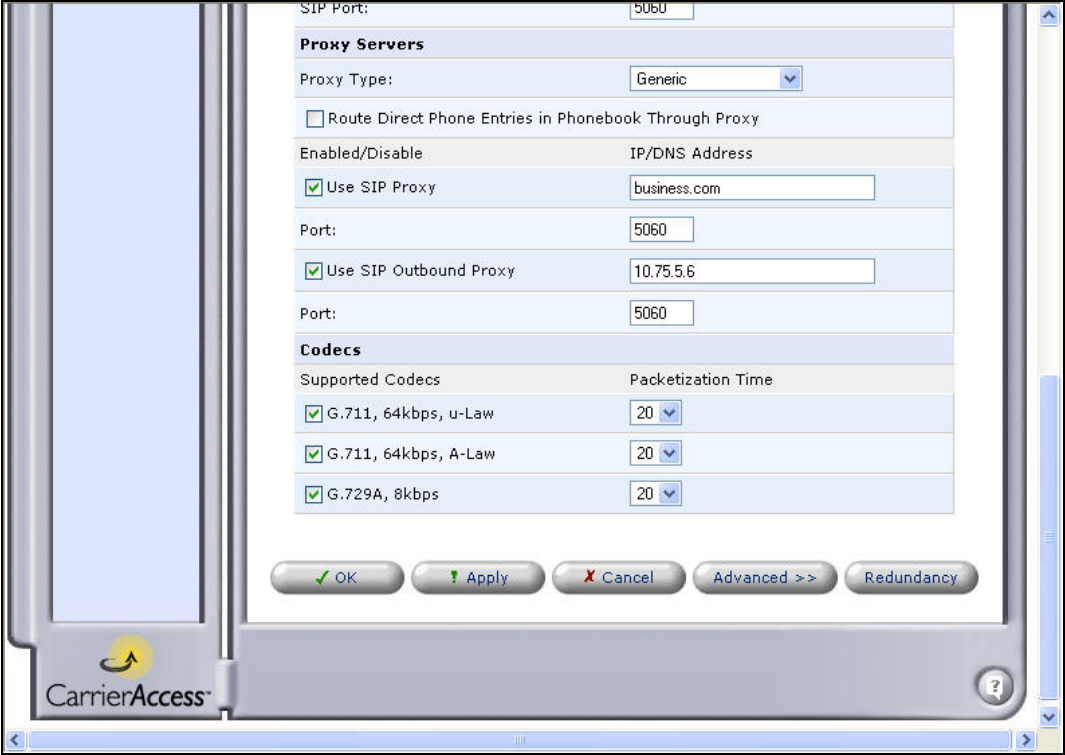
Step	Description
6.	<p>Perform the same procedure described in <b>Steps 2 -3</b> using <b>Ethernet 2</b> to view the properties of the public interface of the device configured during installation.</p> <p>In the upper half of the right pane, verify the following settings for <b>Ethernet 2</b>.</p> <ul style="list-style-type: none"> <li>▪ <b>Network:</b> Verify <b>WAN</b> is selected.</li> <li>▪ <b>Internet Protocol:</b> Verify <i>Use the Following IP Address</i> is selected.</li> <li>▪ <b>IP Address:</b> Verify this field is set to the IP address assigned to the public side of the device.</li> <li>▪ <b>Subnet Mask:</b> Verify the subnet mask is an appropriate value for the addressing supported on the public side of the device.</li> <li>▪ <b>Default Gateway:</b> Verify the IP address of the default gateway.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Scroll down to view additional options.</p> 


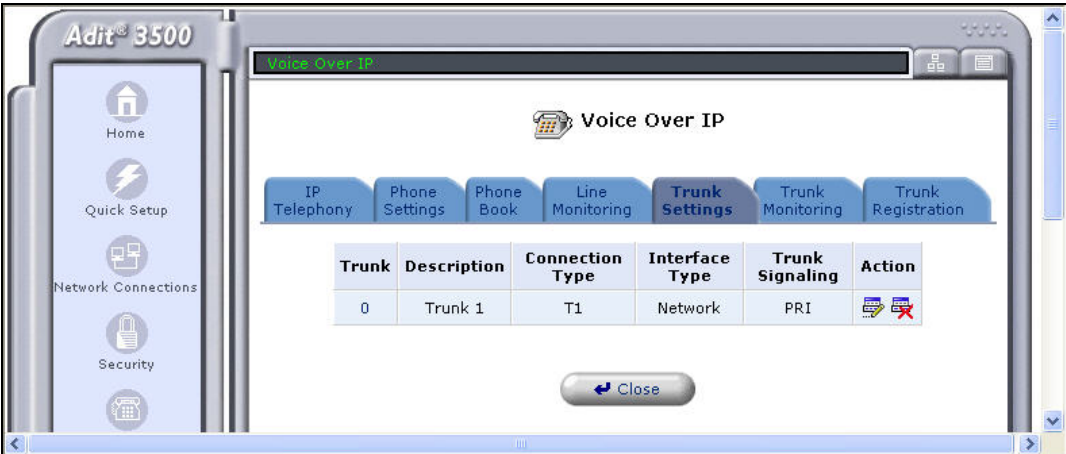
Step	Description
7.	<p>In the lower half of the right pane, configure the following settings for <b>Ethernet 2</b>.</p> <ul style="list-style-type: none"> <li>▪ <b>IP Address Distribution:</b> Select <i>Disabled</i>.</li> <li>▪ <b>Routing Mode:</b> Select <i>NAPT</i>. This enables the Adit 3500 to perform Network Address Translation between the public and private interfaces.</li> <li>▪ <b>SIP ALG:</b> By default the checkbox is checked, enabling this feature. For the SIP trunking model, the state of this field does not matter since it is only used when SIP endpoints are connected behind the Adit 3500. For the SIP registration model, this feature must be enabled. This enables the Adit 3500 to translate the IP address in the SIP messages between the public and private interfaces. Since this configuration will be referenced in Section 4.3 when configuring the Adit 3500 for the SIP registration model, the screen shot below shows the feature enabled.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Click <b>OK</b>.</p> 
8.	<p>Reboot all PCs at the branch so the PCs will make a DHCP request to the Adit 3500 for an IP address.</p>

Step	Description
9.	<p>Set the date and time. Navigate to <b>Advanced</b> → <b>Date and Time</b>.</p> 

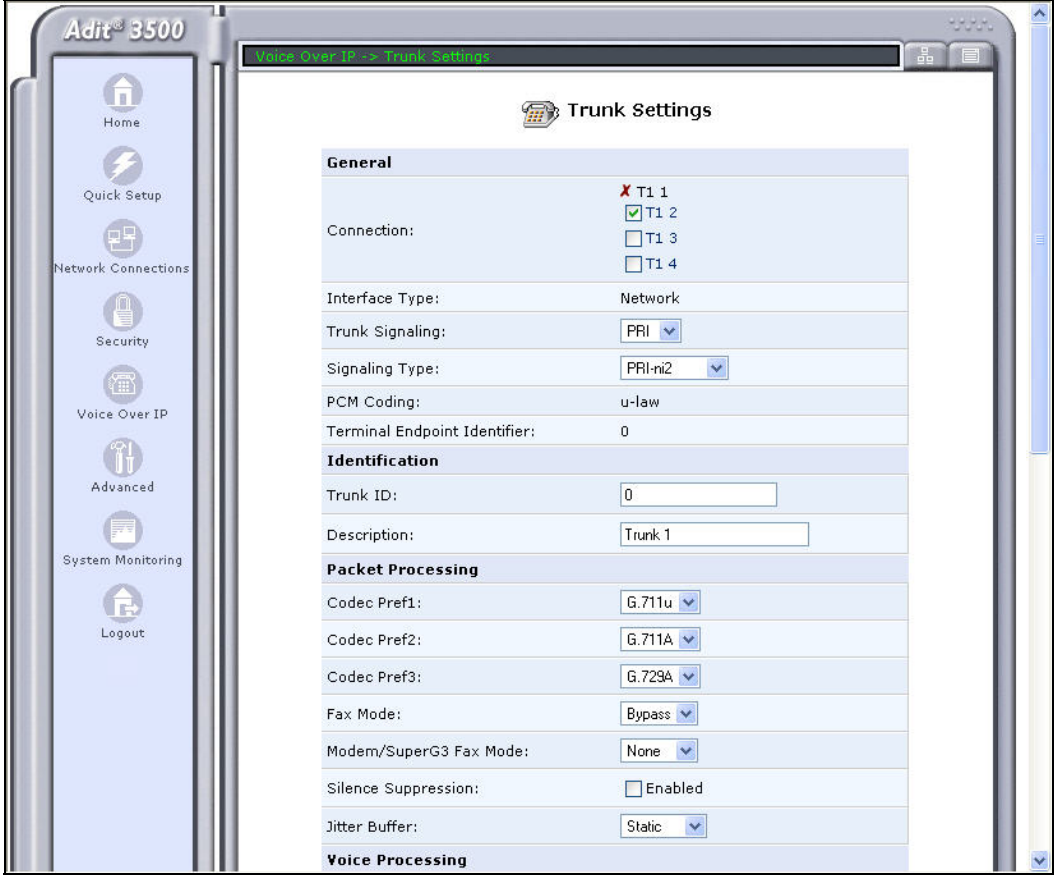
Step	Description
10.	<p>The <b>Data and Time</b> screen appears in the right pane. The clock can be set manually or can be automatically set from a time server if one is present. The clock was set manually for the compliance test. To do this, click the <b>Clock Set</b> button.</p> 
11.	<p>In the <b>Clock Set</b> screen, select the <b>Local Date</b> from the pull-down menus. Enter the <b>Local Time</b>. Click <b>OK</b>.</p> <p>The right-pane will return to the <b>Date and Time</b> screen above. Click <b>OK</b> on this screen to submit the changes.</p> 

Step	Description
12.	<p>To configure the Voice over IP parameters of the Adit 3500, select <b>Voice Over IP</b> in the left pane. The <b>Voice Over IP</b> screen appears. Select the <b>IP Telephony</b> tab in the right pane. In the upper half of the screen, configure or verify the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>Dialing Timeout:</b> Enter the maximum time to wait for the user to complete dialing.</li> <li>▪ <b>Phone Number Size:</b> Enter the maximum phone number size. The compliance test used 12 digits to accommodate a 1 digit feature access code plus an 11 digit phone number.</li> <li>▪ <b>Send DTMF Out-Of-Band:</b> Check the check box.</li> <li>▪ <b>SIP Transport Protocol:</b> <i>UDP</i></li> <li>▪ <b>SIP Port:</b> <i>5060</i></li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Scroll down to view additional options.</p> 

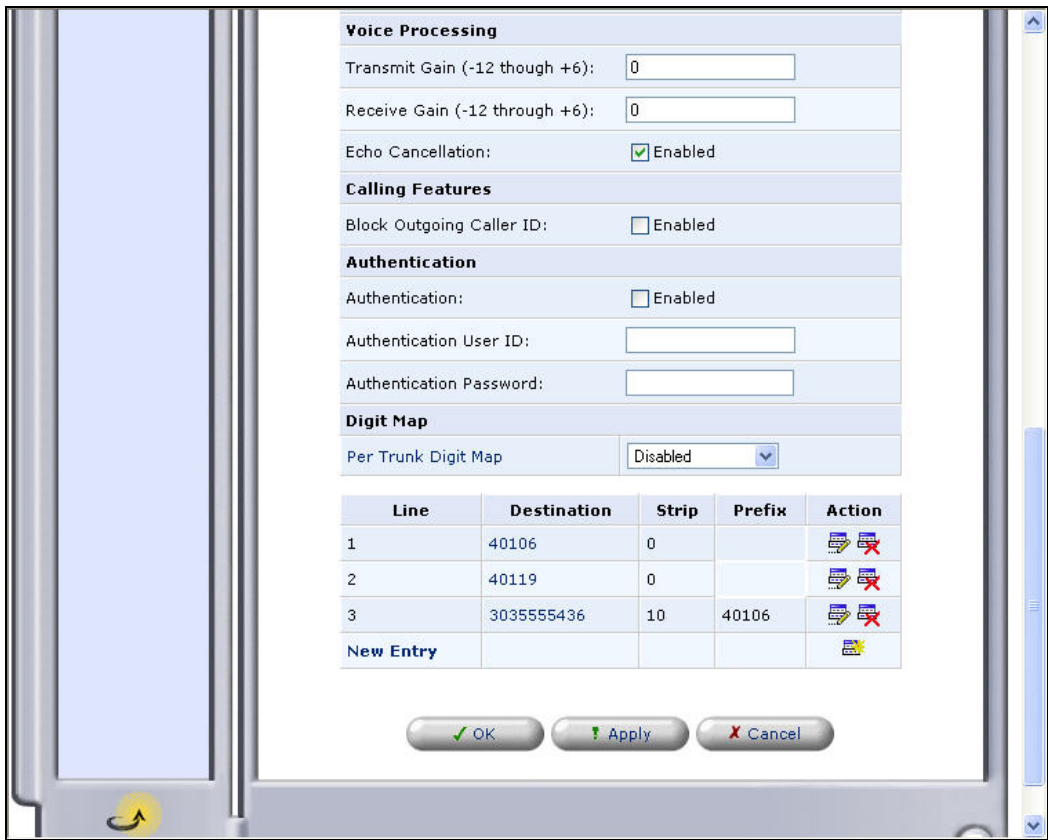
Step	Description
13.	<p>In the lower half of the screen, configure or verify the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>Use SIP Proxy:</b> Check the check box. Enter the SIP domain configured in the Avaya SES in <b>Section 3.2, Step 4</b>.</li> <li>▪ <b>Port: 5060</b></li> <li>▪ <b>Use SIP Outbound Proxy:</b> Check the check box. Enter the IP address of the Avaya SES as showed in <b>Section 3.2, Step 5</b>.</li> <li>▪ <b>Port: 5060</b></li> <li>▪ <b>Supported Codecs:</b> For each codec that will be supported by the device, place a check in the check box next to the codec. By default, all are selected. At a minimum, there must be at least one codec selected that is also in the codec list supported on Avaya Communication Manager defined in <b>Section 3.1.1, Step 6</b>.  <b>Note:</b> The G.729A codec will only be available if the license for this codec has been purchased.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Click <b>OK</b>.</p> 

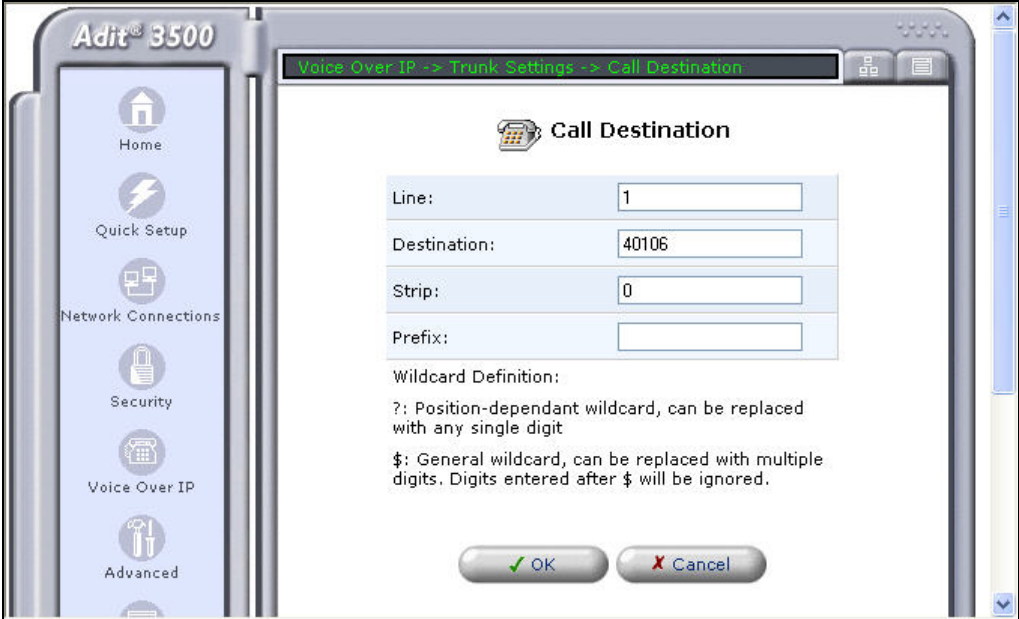
Step	Description																				
14.	<p>Return to the main <b>Voice Over IP</b> screen. Select the <b>Phone Settings</b> tab to verify that all lines are disabled (unchecked) since the FXS ports are not used in this configuration.</p> <p>Click <b>OK</b>.</p>  <table data-bbox="677 598 1266 791"><thead><tr><th>Line</th><th>User ID</th><th>Description</th><th>Action</th></tr></thead><tbody><tr><td><input type="checkbox"/> 1</td><td>0000000001</td><td>Line 1</td><td></td></tr><tr><td><input type="checkbox"/> 2</td><td>0000000002</td><td>Line 2</td><td></td></tr><tr><td><input type="checkbox"/> 3</td><td>0000000003</td><td>Line 3</td><td></td></tr><tr><td><input type="checkbox"/> 4</td><td>0000000004</td><td>Line 4</td><td></td></tr></tbody></table>	Line	User ID	Description	Action	<input type="checkbox"/> 1	0000000001	Line 1		<input type="checkbox"/> 2	0000000002	Line 2		<input type="checkbox"/> 3	0000000003	Line 3		<input type="checkbox"/> 4	0000000004	Line 4	
Line	User ID	Description	Action																		
<input type="checkbox"/> 1	0000000001	Line 1																			
<input type="checkbox"/> 2	0000000002	Line 2																			
<input type="checkbox"/> 3	0000000003	Line 3																			
<input type="checkbox"/> 4	0000000004	Line 4																			
15.	<p>Configure the trunk settings by selecting the <b>Trunk Settings</b> tab. To configure an entry, click on the <b>Trunk</b> number in the table or click on the first icon (“Edit” icon) in the <b>Action</b> column.</p>  <table data-bbox="677 1308 1266 1392"><thead><tr><th>Trunk</th><th>Description</th><th>Connection Type</th><th>Interface Type</th><th>Trunk Signaling</th><th>Action</th></tr></thead><tbody><tr><td>0</td><td>Trunk 1</td><td>T1</td><td>Network</td><td>PRI</td><td></td></tr></tbody></table>	Trunk	Description	Connection Type	Interface Type	Trunk Signaling	Action	0	Trunk 1	T1	Network	PRI									
Trunk	Description	Connection Type	Interface Type	Trunk Signaling	Action																
0	Trunk 1	T1	Network	PRI																	




Step	Description
16.	<p>In the upper half of the screen, configure or verify the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>Trunk Signaling:</b> <i>PRI</i></li> <li>▪ <b>Signaling Type:</b> <i>PRI-ni2</i></li> <li>▪ <b>Trunk ID:</b> Enter a unique number for this trunk. This value is not used for ISDN-PRI but only for CAS. However, a value must be entered.</li> <li>▪ <b>Description:</b> Enter a descriptive name.</li> <li>▪ <b>Codec Pref1 – CodePref3:</b> Select from the pull-down menu the codecs to be used for each codec preference. Codec Pref1 is the highest level of preference.</li> <li>▪ <b>Fax Mode:</b> <i>Bypass</i></li> <li>▪ <b>Silence Suppression:</b> Uncheck the <b>Enabled</b> box.</li> <li>▪ The default values may be retained for all other fields.</li> </ul> 



Step	Description
17.	<p>In the lower half of the screen, configure or verify the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>Authentication:</b> Verify that the checkbox next to <b>Enabled</b> is unchecked.</li> <li>▪ <b>Authentication User ID:</b> Leave this field blank.</li> <li>▪ <b>Authentication Password:</b> Leave this field blank</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>At the bottom of the screen, three entries are shown in the trunk line table. These entries were entered by selecting the <b>New Entry</b> link. An entry is entered for each logical extension/user that the Adit 3500 will use for calls on the ISDN-PRI trunk. For an example of creating a new entry, see <b>Step 18</b>. Otherwise, click <b>OK</b>.</p> <p>A confirmation window will appear. Click <b>OK</b> in this window also.</p> 

Step	Description
18.	<p>After clicking the <b>New Entry</b> link in the previous step, the <b>Call Destination</b> window appears. The call destination information is used to manipulate the dialed digits of incoming calls (if necessary) and route the call to the proper user. Configure or verify the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>Line:</b> Line number in the table.</li> <li>▪ <b>Destination:</b> Dialed digits of the destination.</li> <li>▪ <b>Strip:</b> The number of digits to strip from the destination digits.</li> <li>▪ <b>Prefix:</b> The digits to prefix to the remaining digits.</li> </ul> 
19.	<p>Repeat <b>Step 18</b> for the remaining trunk lines with the following information.</p> <ul style="list-style-type: none"> <li>▪ <b>Line:</b> 2</li> <li>▪ <b>Destination:</b> 40119</li> <li>▪ <b>Strip:</b> 0</li> <li>▪ <b>Prefix:</b></li> <li>▪ <b>Line:</b> 3</li> <li>▪ <b>Destination:</b> 3035555436</li> <li>▪ <b>Strip:</b> 10</li> <li>▪ <b>Prefix:</b> 40106</li> </ul>

Step	Description
20.	<p>Return to the main <b>Voice Over IP</b> screen. Select the <b>Trunk Registration</b> tab to verify that <b>Trunk Group Phone Registration</b> is disabled (unchecked).</p> <p>Click <b>OK</b>.</p> 

## 4. SIP Registration Configuration

This section describes the configuration to support the SIP registration model shown in **Figure 2**.

### 4.1. Configure Avaya Communication Manager

The section describes the procedure for configuring Avaya Communication Manager when using the SIP registration model to have the Adit 3500 communicate with the Avaya SES. This includes configuring OPS stations. An OPS station on Avaya Communication Manager is required for SIP endpoints connected behind the Adit 3500. In addition, an OPS station is necessary for each analog endpoint connected to the FXS ports of the Adit 3500, if the intent is to provide PBX features from the main site Avaya Communication Manager. These analog endpoints appear as SIP endpoints to Avaya Communication Manager. In the case of the compliance test, it was not the intent to provide PBX features to the fax machine connected to the Adit 3500. Thus, no OPS station was created for this endpoint.

Step	Description
1.	Perform all steps described in <b>Section 3.1.1</b> for configuring Avaya Communication Manager for the SIP trunking model. This configuration is also needed when using the SIP registration model.

2. Use the **display system-parameters customer-options** command to verify Avaya Communication Manager has sufficient OPS capacity available to add the OPS stations needed for the endpoints at the branch office in **Figure 1**. If there is insufficient capacity, contact an authorized Avaya sales representative or business partner to make the appropriate changes.

```
display system-parameters customer-options                               Page 1 of 10
                                OPTIONAL FEATURES

G3 Version: V13
Location: 1
Platform: 13

RFA System ID (SID): 1
RFA Module ID (MID): 1

Platform Maximum Ports: 900
Maximum Stations: 450
Maximum XMOBILE Stations: 0
Maximum Off-PBX Telephones - EC500: 50
Maximum Off-PBX Telephones - OPS: 50
Maximum Off-PBX Telephones - SCCAN: 0

USED
121
41
0
0
23
0
```

3. To add a station, use the **add station *n*** command where ***n*** is an unused extension number. Use the default value of **6408D+** for the Type field. Enter an **X** in the **Port** field. This indicates a station is being added without identifying a physical port for the station to use. Enter a descriptive name in the **Name** field. The **Coverage Path 1** field is set to **1**. Coverage path 1 directs the call to voicemail. The voicemail configuration is not covered in these Application Notes. The default values may be retained for all other fields.

The example below shows the configuration of the SIP telephone at the branch site. Even though this telephone is located at the branch site, this telephone will register with the Avaya and get PBX features from the main site PBX. Thus, it requires an OPS station on the main site Avaya Communication Manager.

```
add station 30102                                                       Page 1 of 4
                                STATION

Extension: 30102
Type: 6408D+
Port: X
Name: Branch 1

Lock Messages? n
Security Code:
Coverage Path 1: 1
Coverage Path 2:
Hunt-to Station:

BCC: 0
TN: 1
COR: 1
COS: 1

STATION OPTIONS
Loss Group: 2
Data Module? n
Speakerphone: 2-way
Display Language: english

Personalized Ringing Pattern: 1
Message Lamp Ext: 30102
Mute Button Enabled? y

Media Complex Ext:
IP SoftPhone? n
```

4. On **Page 2**, set **Restrict Last Appearance** to *n*. This will allow the last call appearance to be used for either an incoming or outgoing call.

add station 30102	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: audix	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? y	<b>Restrict Last Appearance? n</b>
Active Station Ringing: single	
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	
Multimedia Mode: basic	Audible Message Waiting? n
MWI Served User Type:	Display Client Redirection? n
AUDIX Name: IA770	Select Last Used Appearance? n
	Coverage After Forwarding? s
Emergency Location Ext: 30102	Direct IP-IP Audio Connections? y
	IP Audio Hairpinning? n

5. On **Page 3**, under **BUTTON ASSIGNMENTS**, create the appropriate number of call appearances for the SIP endpoint being configured. In general, the appropriate number of call appearances on Avaya Communication Manager is the same as the number of call appearances supported by the endpoint. To create a call appearance, enter ***call-appr*** as the button assignment. The example below shows the configuration of the SIP phone connected behind the Adit 3500 in the compliance test.

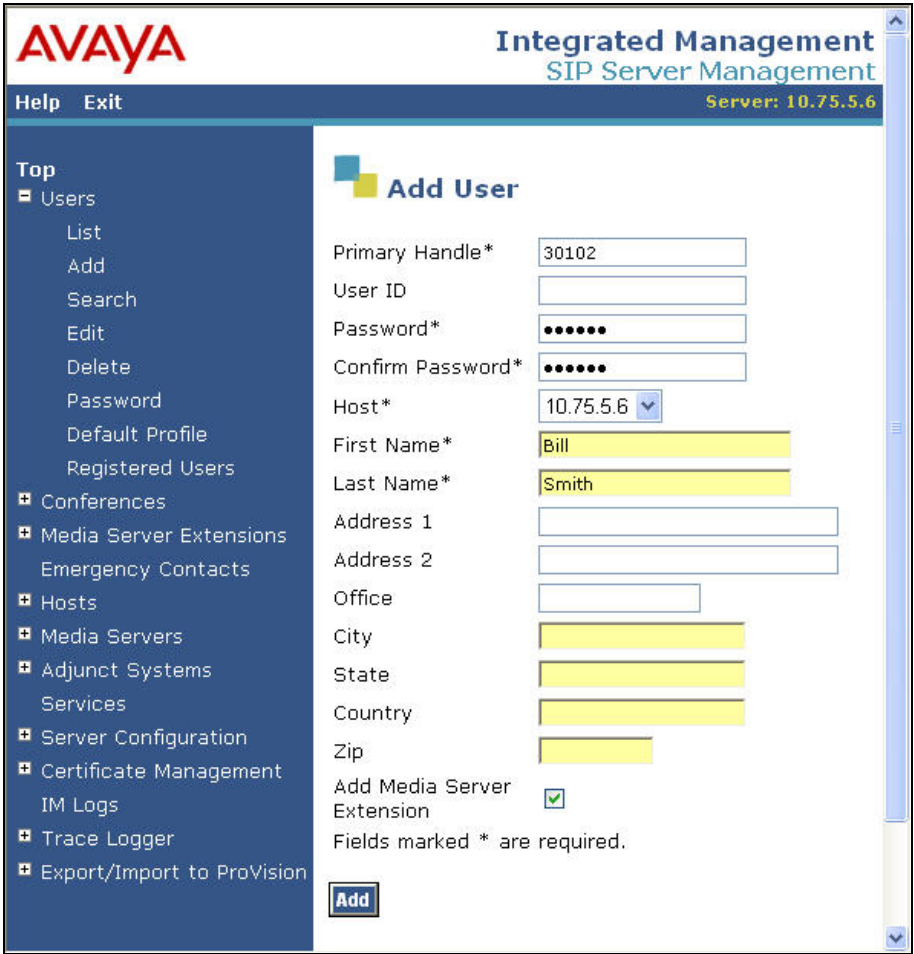
add station 30102	Page 3 of 4
STATION	
SITE DATA	
Room:	Headset? n
Jack:	Speaker? n
Cable:	Mounting: d
Floor:	Cord Length: 0
Building:	Set Color:
ABBREVIATED DIALING	
List1:	List2:
	List3:
<b>BUTTON ASSIGNMENTS</b>	
1: <b>call-appr</b>	5:
2: <b>call-appr</b>	6:
3: <b>call-appr</b>	7:
4:	8:

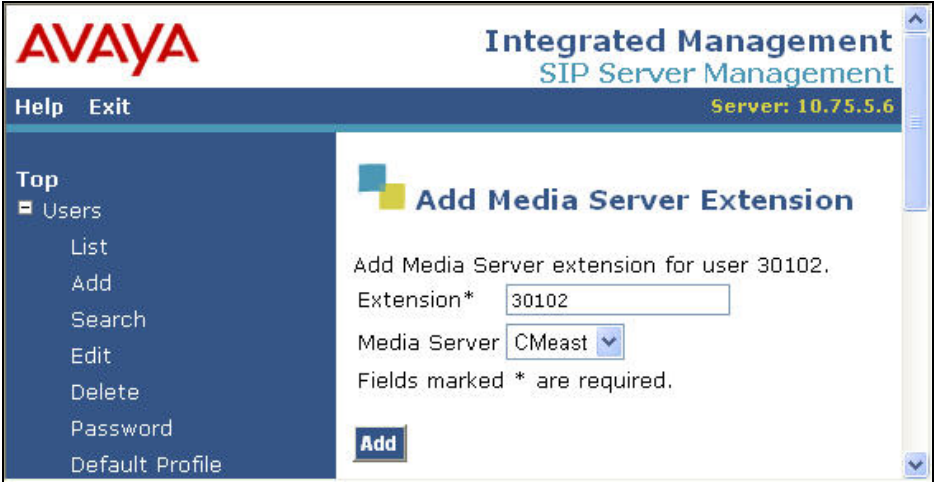
6.	<p>Map the Avaya Communication Manager extension to the Avaya SES media server extension defined in <b>Section 4.2, Step 3</b> with the <b>add off-pbx-telephone station-mapping</b> command. Enter the values as shown below:</p> <ul style="list-style-type: none"><li>▪ <b>Station Extension:</b> Avaya Communication Manager extension created in <b>Step 3</b>.</li><li>▪ <b>Application:</b> <i>OPS</i></li><li>▪ <b>Phone Number:</b> Avaya SES media server extension</li><li>▪ <b>Trunk Selection:</b> The SIP trunk group number</li><li>▪ <b>Configuration Set:</b> Enter a valid configuration set. The compliance test used configuration set 1 which contained the default values.</li></ul> <div><div>add off-pbx-telephone station-mapping</div><div>Page 1 of 2</div><div>STATIONS WITH OFF-PBX TELEPHONE INTEGRATION</div><table><tr><th>Station Extension</th><th>Application</th><th>Dial Prefix</th><th>Phone Number</th><th>Trunk Selection</th><th>Configuration Set</th></tr><tr><td>30102</td><td>OPS</td><td>-</td><td>30102</td><td>1</td><td>1</td></tr><tr><td></td><td></td><td>-</td><td></td><td></td><td></td></tr></table></div>	Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set	30102	OPS	-	30102	1	1			-			
Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set														
30102	OPS	-	30102	1	1														
		-																	
7.	<p>On <b>Page 2</b>, set the <b>Call Limit</b> to the number of call appearances set on the station form in <b>Step 5</b>. Verify that the <b>Mapping Mode</b> is set to <i>both</i>.</p> <div><div>add off-pbx-telephone station-mapping</div><div>Page 2 of 2</div><div>STATIONS WITH OFF-PBX TELEPHONE INTEGRATION</div><table><tr><th>Station Extension</th><th>Call Limit</th><th>Mapping Mode</th><th>Calls Allowed</th><th>Bridged Calls</th></tr><tr><td>30102</td><td>3</td><td>both</td><td>all</td><td>both</td></tr></table></div>	Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	30102	3	both	all	both								
Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls															
30102	3	both	all	both															
8.	<p>Repeat <b>Steps 3 - 7</b> for each remaining applicable endpoint located at the branch office. In the case of the compliance test, only one applicable endpoint (SIP telephone) was located at the branch.</p>																		

## 4.2. Configure Avaya SES

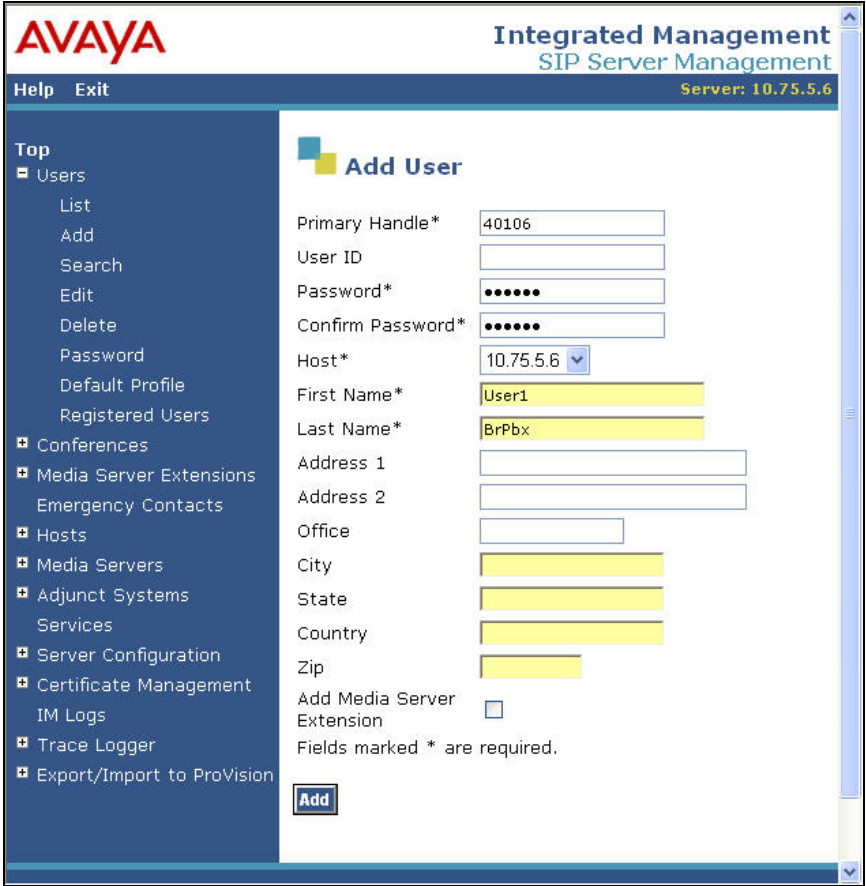
This section covers the configuration of Avaya SES using the SIP registration model.

Step	Description
1.	Perform <b>Steps 1 - 12</b> described in <b>Section 3.2</b> for the SIP trunking model. Omit <b>Steps 13 – 18</b> relating to Host Address Maps and configuring a trusted host.

Step	Description
2.	<p>A user must be added on Avaya SES for each of the extensions at the branch office created on Avaya Communication Manager in <b>Section 4.1, Steps 3 - 5</b>. From the left pane, navigate to <b>Users → Add</b>. Enter the values as shown below.</p> <ul style="list-style-type: none"> <li>▪ <b>Primary Handle:</b> Enter the extension for this user.</li> <li>▪ <b>Password:</b> Enter a valid password for logging into the SIP endpoint.</li> <li>▪ <b>Confirm Password:</b> Re-enter the password.</li> <li>▪ <b>Host:</b> Select the Avaya SES server from the pull-down menu.</li> <li>▪ <b>First Name:</b> Any descriptive name.</li> <li>▪ <b>Last Name:</b> Any descriptive name.</li> </ul> <p>Check the <b>Add Media Server Extension</b> checkbox. Click the <b>Add</b> button to proceed. A confirmation window will appear. Click <b>Continue</b> on this new page to proceed.</p> 

Step	Description
3.	<p>The <b>Add Media Server Extension</b> page will appear. In the <b>Extension</b> field, enter the same extension used in the previous step. In the <b>Media Server</b> field, select from the pull-down menu the name of the media server added in <b>Section 3.2, Step 6</b>.</p> <p>Click the <b>Add</b> button to complete the operation.</p> 



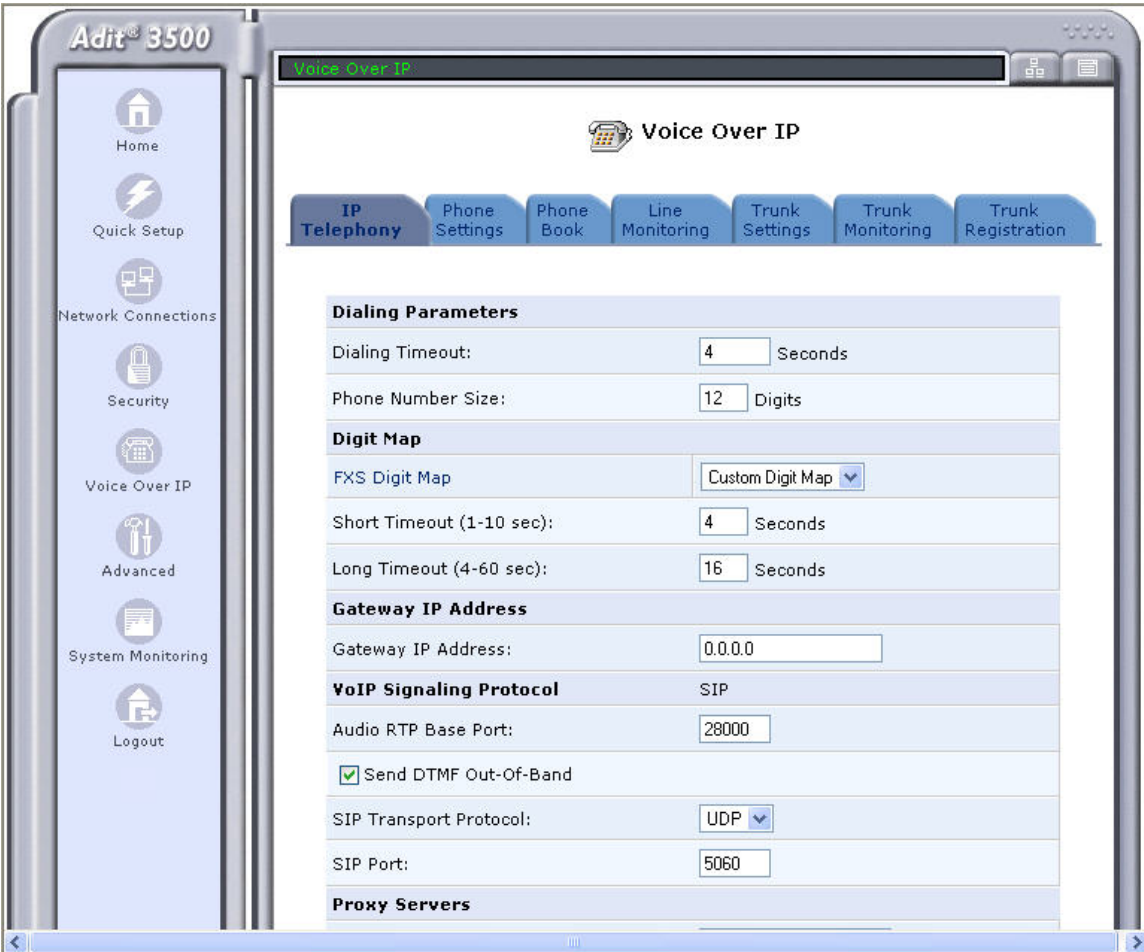
Step	Description
4.	<p>Users must also be added on Avaya SES for each of the extensions at the branch office which will not have media server extensions and OPS stations associated with them. This includes the fax machine behind the Adit 3500 and the numbers used by the legacy PBX endpoints. (For complete details on these endpoints, see <b>Section 1</b>). Repeat <b>Step 2</b> for the following users: 40106, 40119, 50112 and 3035555436 but do not check the <b>Add Media Server Extension</b> box. The example below shows the <b>Add User</b> page for the extension 40106.</p> 

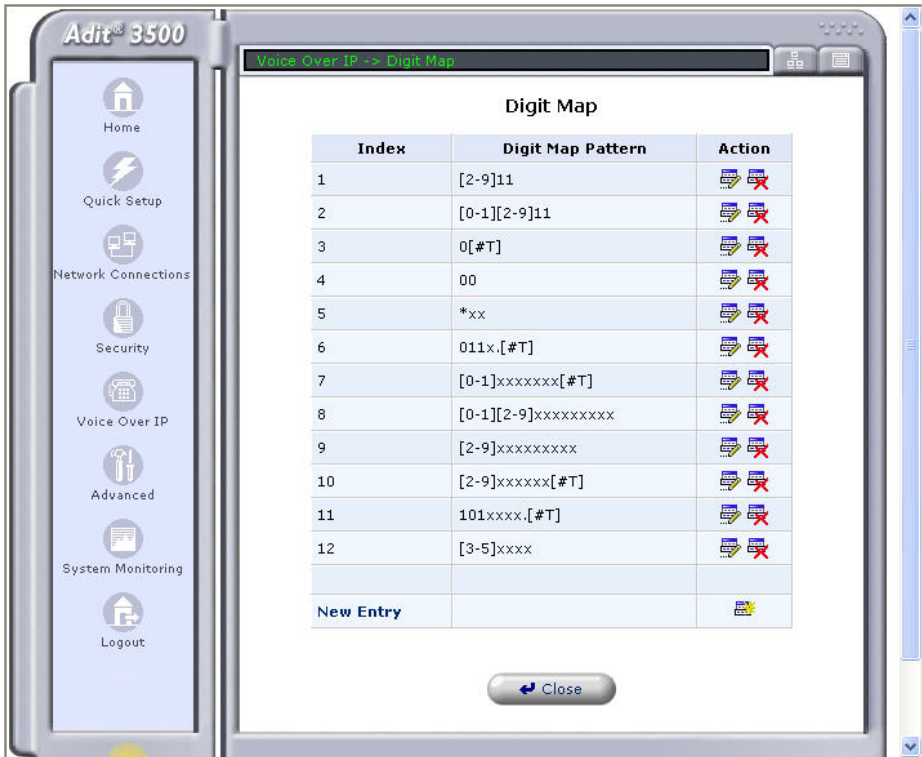
Step	Description																																																			
5.	<p>To verify the users created on Avaya SES, select <b>Users</b> → <b>List</b> from the left pane. All users that were part of the compliance test appear in the list below: 30102, 40106, 40119, and 3035555436.</p> <div><div><div><div>AVAYA</div><div>Integrated Management SIP Server Management</div><div>Help Exit</div><div>Server: 10.75.5.6</div></div><div><div>Top</div><div><div>Users</div><div>List</div><div>Add</div><div>Search</div><div>Edit</div><div>Delete</div><div>Password</div><div>Default Profile</div><div>Registered Users</div><div>Conferences</div><div>Media Server Extensions</div><div>Emergency Contacts</div><div>Hosts</div><div>Media Servers</div><div>Adjunct Systems</div><div>Services</div><div>Server Configuration</div><div>Certificate Management</div><div>IM Logs</div><div>Trace Logger</div><div>Export/Import to ProVision</div></div></div><div><div>List Users</div><div>Showing users 1 to 20 out of 20 users.</div><table><thead><tr><th>User ID</th><th>Host</th><th>Name</th></tr></thead><tbody><tr><td><input type="checkbox"/> 30101</td><td>10.75.5.6</td><td>Alice Smith</td></tr><tr><td><input type="checkbox"/> 30102</td><td>10.75.5.6</td><td>Bill Smith</td></tr><tr><td><input type="checkbox"/> 30103</td><td>10.75.5.6</td><td>Chris Smith</td></tr><tr><td><input type="checkbox"/> 30104</td><td>10.75.5.6</td><td>Dana Smith</td></tr><tr><td><input type="checkbox"/> 30107</td><td>10.75.5.6</td><td>Gary Smith</td></tr><tr><td><input type="checkbox"/> 30108</td><td>10.75.5.6</td><td>Harry Smith</td></tr><tr><td><input type="checkbox"/> 30109</td><td>10.75.5.6</td><td>Issac Smith</td></tr><tr><td><input type="checkbox"/> 30110</td><td>10.75.5.6</td><td>James Smith</td></tr><tr><td><input type="checkbox"/> 30111</td><td>10.75.5.6</td><td>Karen Smith</td></tr><tr><td><input type="checkbox"/> 30120</td><td>10.75.5.6</td><td>Tom Smith</td></tr><tr><td><input type="checkbox"/> 30200</td><td>10.75.5.6</td><td>SIP TEST</td></tr><tr><td><input type="checkbox"/> 30201</td><td>10.75.5.6</td><td>SIP Test2</td></tr><tr><td><input type="checkbox"/> 3035555436</td><td>10.75.5.6</td><td>ExternalNum Adit</td></tr><tr><td><input type="checkbox"/> 40106</td><td>10.75.5.6</td><td>User1 BrPbx</td></tr><tr><td><input type="checkbox"/> 40119</td><td>10.75.5.6</td><td>User2 BrPbx</td></tr><tr><td><input type="checkbox"/> 50112</td><td>10.75.5.6</td><td>Fax1 Adit</td></tr></tbody></table></div></div></div>	User ID	Host	Name	<input type="checkbox"/> 30101	10.75.5.6	Alice Smith	<input type="checkbox"/> 30102	10.75.5.6	Bill Smith	<input type="checkbox"/> 30103	10.75.5.6	Chris Smith	<input type="checkbox"/> 30104	10.75.5.6	Dana Smith	<input type="checkbox"/> 30107	10.75.5.6	Gary Smith	<input type="checkbox"/> 30108	10.75.5.6	Harry Smith	<input type="checkbox"/> 30109	10.75.5.6	Issac Smith	<input type="checkbox"/> 30110	10.75.5.6	James Smith	<input type="checkbox"/> 30111	10.75.5.6	Karen Smith	<input type="checkbox"/> 30120	10.75.5.6	Tom Smith	<input type="checkbox"/> 30200	10.75.5.6	SIP TEST	<input type="checkbox"/> 30201	10.75.5.6	SIP Test2	<input type="checkbox"/> 3035555436	10.75.5.6	ExternalNum Adit	<input type="checkbox"/> 40106	10.75.5.6	User1 BrPbx	<input type="checkbox"/> 40119	10.75.5.6	User2 BrPbx	<input type="checkbox"/> 50112	10.75.5.6	Fax1 Adit
User ID	Host	Name																																																		
<input type="checkbox"/> 30101	10.75.5.6	Alice Smith																																																		
<input type="checkbox"/> 30102	10.75.5.6	Bill Smith																																																		
<input type="checkbox"/> 30103	10.75.5.6	Chris Smith																																																		
<input type="checkbox"/> 30104	10.75.5.6	Dana Smith																																																		
<input type="checkbox"/> 30107	10.75.5.6	Gary Smith																																																		
<input type="checkbox"/> 30108	10.75.5.6	Harry Smith																																																		
<input type="checkbox"/> 30109	10.75.5.6	Issac Smith																																																		
<input type="checkbox"/> 30110	10.75.5.6	James Smith																																																		
<input type="checkbox"/> 30111	10.75.5.6	Karen Smith																																																		
<input type="checkbox"/> 30120	10.75.5.6	Tom Smith																																																		
<input type="checkbox"/> 30200	10.75.5.6	SIP TEST																																																		
<input type="checkbox"/> 30201	10.75.5.6	SIP Test2																																																		
<input type="checkbox"/> 3035555436	10.75.5.6	ExternalNum Adit																																																		
<input type="checkbox"/> 40106	10.75.5.6	User1 BrPbx																																																		
<input type="checkbox"/> 40119	10.75.5.6	User2 BrPbx																																																		
<input type="checkbox"/> 50112	10.75.5.6	Fax1 Adit																																																		


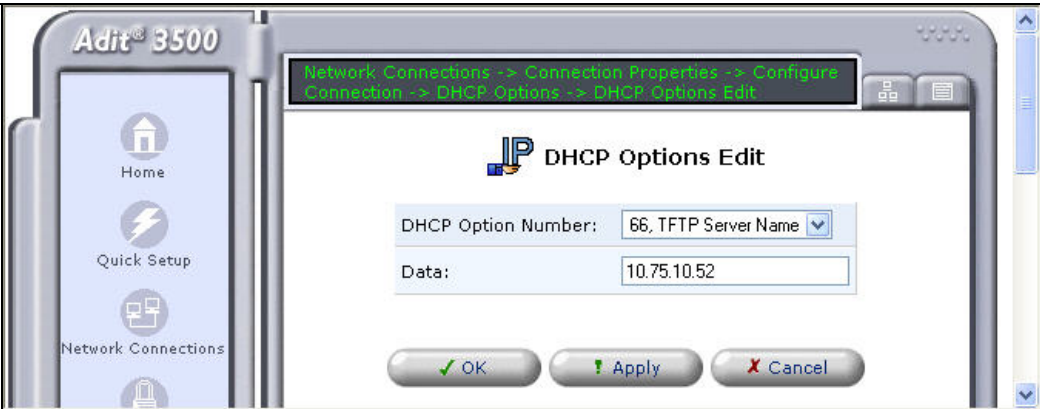
Step	Description																																																																																											
6.	<p>To verify the media server extensions created on Avaya SES, select <b>Media Server Extensions</b> → <b>List</b> from the left pane. Verify that of the users that were part of the compliance test, only 30102 has a media server extension.</p> <div><div><div><div>AVAYA</div><div>Integrated Management SIP Server Management Server: 10.75.5.6</div><div>Help Exit</div><div><div>Top</div><div><div>Users</div><div>Conferences</div><div>Media Server Extensions<ul style="list-style-type: none"><li>List</li><li>Add</li><li>Search</li><li>Emergency Contacts</li></ul></div><div>Hosts</div><div>Media Servers</div><div>Adjunct Systems</div><div>Services</div><div>Server Configuration</div><div>Certificate Management</div><div>IM Logs</div><div>Trace Logger</div><div>Export/Import to ProVision</div></div></div><div><div>List Media Server Extensions</div><div>Showing extensions 1 to 12 out of 12 extensions.</div><table><tr><th colspan="3">Commands</th><th>Extension</th><th>User</th><th>Media Server</th><th>Host</th></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30101</td><td>30101</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30102</td><td>30102</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30103</td><td>30103</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30104</td><td>30104</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30107</td><td>30107</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30108</td><td>30108</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30109</td><td>30109</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30110</td><td>30110</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30111</td><td>30111</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30120</td><td>30120</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30200</td><td>30200</td><td>CMeast</td><td>10.75.5.6</td></tr><tr><td>Free</td><td>Edit User</td><td>Delete</td><td>30201</td><td>30201</td><td>CMeast</td><td>10.75.5.6</td></tr></table><div>Add Another Media Server Extension</div></div></div></div></div>	Commands			Extension	User	Media Server	Host	Free	Edit User	Delete	30101	30101	CMeast	10.75.5.6	Free	Edit User	Delete	30102	30102	CMeast	10.75.5.6	Free	Edit User	Delete	30103	30103	CMeast	10.75.5.6	Free	Edit User	Delete	30104	30104	CMeast	10.75.5.6	Free	Edit User	Delete	30107	30107	CMeast	10.75.5.6	Free	Edit User	Delete	30108	30108	CMeast	10.75.5.6	Free	Edit User	Delete	30109	30109	CMeast	10.75.5.6	Free	Edit User	Delete	30110	30110	CMeast	10.75.5.6	Free	Edit User	Delete	30111	30111	CMeast	10.75.5.6	Free	Edit User	Delete	30120	30120	CMeast	10.75.5.6	Free	Edit User	Delete	30200	30200	CMeast	10.75.5.6	Free	Edit User	Delete	30201	30201	CMeast	10.75.5.6
Commands			Extension	User	Media Server	Host																																																																																						
Free	Edit User	Delete	30101	30101	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30102	30102	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30103	30103	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30104	30104	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30107	30107	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30108	30108	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30109	30109	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30110	30110	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30111	30111	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30120	30120	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30200	30200	CMeast	10.75.5.6																																																																																						
Free	Edit User	Delete	30201	30201	CMeast	10.75.5.6																																																																																						

### 4.3. Configure the Adit 3500



Step	Description
1.	<p>Perform all steps described in <b>Section 3.3</b> for configuring the Adit 3500 for the SIP trunking model. In particular, verify that the SIP ALG function has been enabled as described in <b>Section 3.3, Step 7</b>. The following steps will describe any modifications required to support SIP registration.</p>

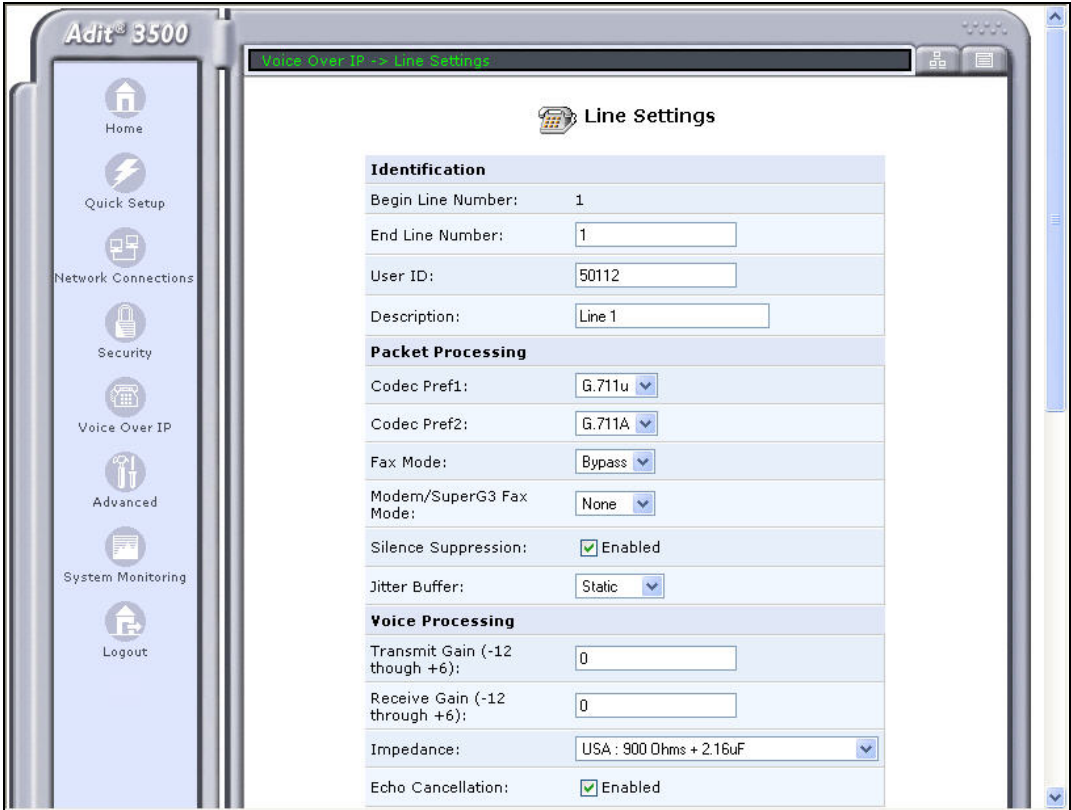
Step	Description
2.	<p>With the addition of the SIP and analog endpoints behind the Adit 3500, additional extensions were added to the test configuration. In order to dial these new extensions without waiting for the dialing timeout, a custom digit map was added to include these new extensions. To create a custom digit map, navigate to the <b>Voice Over IP</b> page by selecting <b>Voice Over IP</b> from the left pane. Select the <b>IP Telephony</b> tab. Select <b>Custom Digit Map</b> from the pull-down menu next to the <b>FXS Digit Map</b> link. Click the <b>FXS Digit Map</b> link to edit the map.</p> 

Step	Description																																										
3.	<p>The <b>Digit Map</b> page appears. Select a <b>New Entry</b>. Enter <b>[3-5]xxxx</b> in the <b>Pattern</b> field. This will allow the endpoints behind the Adit 3500 to dial 5 digit extensions beginning with a 3, 4 or 5 (e.g., 30102 and 50112). The page below shows the Digit Map after the new entry has been entered.</p>  <table><thead><tr><th>Index</th><th>Digit Map Pattern</th><th>Action</th></tr></thead><tbody><tr><td>1</td><td>[2-9]11</td><td> </td></tr><tr><td>2</td><td>[0-1][2-9]11</td><td> </td></tr><tr><td>3</td><td>0[#T]</td><td> </td></tr><tr><td>4</td><td>00</td><td> </td></tr><tr><td>5</td><td>*xx</td><td> </td></tr><tr><td>6</td><td>011x.[#T]</td><td> </td></tr><tr><td>7</td><td>[0-1]xxxxxxx[#T]</td><td> </td></tr><tr><td>8</td><td>[0-1][2-9]xxxxxxxx</td><td> </td></tr><tr><td>9</td><td>[2-9]xxxxxxxx</td><td> </td></tr><tr><td>10</td><td>[2-9]xxxxx[#T]</td><td> </td></tr><tr><td>11</td><td>101xxxx.[#T]</td><td> </td></tr><tr><td>12</td><td>[3-5]xxxx</td><td> </td></tr><tr><td colspan="2">New Entry</td><td></td></tr></tbody></table>	Index	Digit Map Pattern	Action	1	[2-9]11		2	[0-1][2-9]11		3	0[#T]		4	00		5	*xx		6	011x.[#T]		7	[0-1]xxxxxxx[#T]		8	[0-1][2-9]xxxxxxxx		9	[2-9]xxxxxxxx		10	[2-9]xxxxx[#T]		11	101xxxx.[#T]		12	[3-5]xxxx		New Entry		
Index	Digit Map Pattern	Action																																									
1	[2-9]11																																										
2	[0-1][2-9]11																																										
3	0[#T]																																										
4	00																																										
5	*xx																																										
6	011x.[#T]																																										
7	[0-1]xxxxxxx[#T]																																										
8	[0-1][2-9]xxxxxxxx																																										
9	[2-9]xxxxxxxx																																										
10	[2-9]xxxxx[#T]																																										
11	101xxxx.[#T]																																										
12	[3-5]xxxx																																										
New Entry																																											

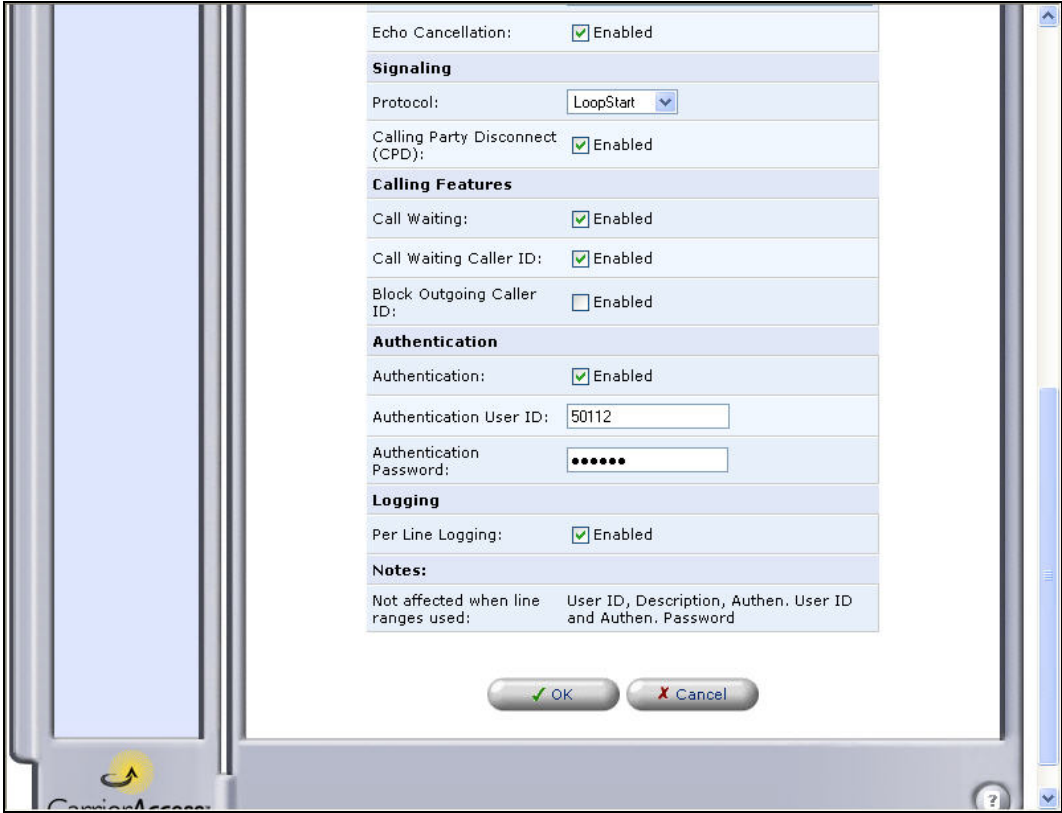
Step	Description
4.	<p>To support Avaya SIP telephones added behind the Adit 3500, a DHCP Option needs to be configured on interface <b>Ethernet 1</b> so the DHCP Server can supply the IP address of the TFTP server in the DHCP request. Navigate to <b>Network Connections → Ethernet 1</b>. On the <b>Configure Ethernet 1</b> page that appears (not shown), click on the <b>DHCP Options</b> link next to the <b>IP Address Distribution</b> field to configure these options (see <b>Section 3.3, Step 5</b>).</p> <p>On the <b>DHCP Options</b> page that appears, click on the <b>New Entry</b> link in the table.</p> 
5.	<p>From the pull-down menu for the <b>DHCP Option Number</b> field, select <b>66, TFTP Server Name</b>. In general, Avaya recommends using option 176 to provide this information. However, the Adit 3500 does not support option 176, so option 66 is used instead. In the <b>Data</b> field, enter the IP address of the TFTP server.</p> <p>Click <b>OK</b>.</p> 




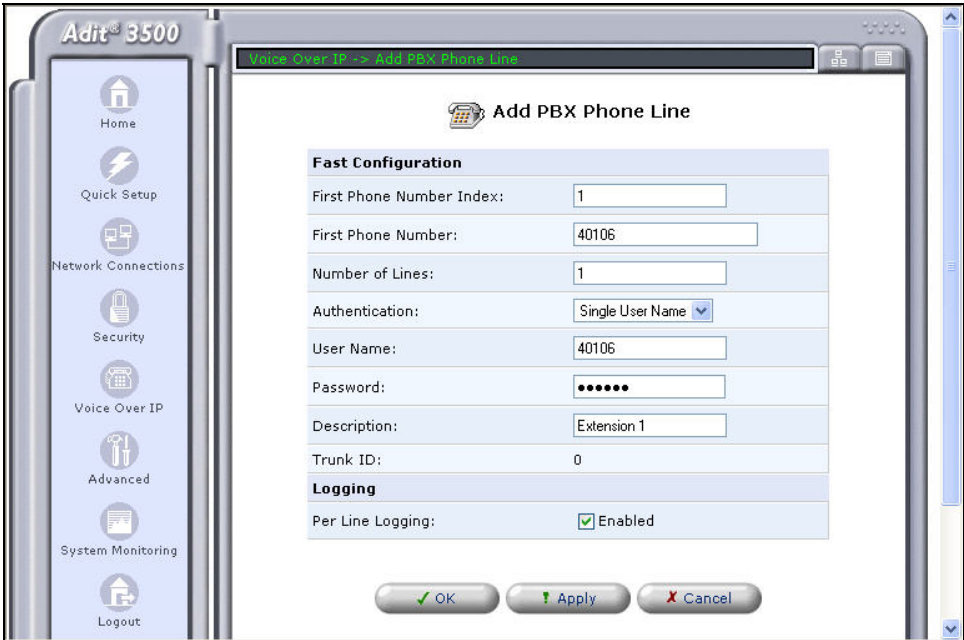
Step	Description
6.	<p>The newly selected option is displayed in the <b>DHCP Options</b> table. Click <b>OK</b>.</p> <p>The right-pane will return to the <b>Configure Ethernet 1</b> screen. Click <b>OK</b> on this screen to submit any changes.</p> <div></div>
7.	<p>To configure the properties of each line/port where an analog endpoint is connected, select <b>Voice Over IP</b> in the left pane, followed by the <b>Phone Settings</b> tab. The screen below shows the <b>Voice Over IP</b> screen after the lines have been configured, since the <b>User ID</b> column shows the extensions instead of the default IDs. To activate a line, check the check box next to the line. To configure the line, click the <b>Line</b> number or <b>Action</b> icon associated with this line in the right most column of the table.</p> <div></div>

Step	Description
8.	<p>The <b>Line Settings</b> screen appears. In the upper half of the screen, configure or verify the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>End Line Number:</b> Enter the same value as the <b>Begin Line Number</b> if configuring each line separately. A range of lines can be configured at the same time with similar values by selecting a value larger than the <b>Begin Line Number</b>.</li> <li>▪ <b>User ID:</b> Enter the extension to be used by the analog endpoint. In the case of the compliance test, the endpoint was a fax machine.</li> <li>▪ <b>Description:</b> Enter a descriptive name for this line.</li> <li>▪ <b>Codec Pref1 – Codec Pref2:</b> Select from the pull-down menu the codec to be used for each codec preference. <b>Codec Pref1</b> is the highest level preference.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Scroll down to view additional options.</p> 



Step	Description
<p><b>9.</b></p>	<p>In the lower half of the screen, configure or verify the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>Authentication:</b> Check the checkbox next to <b>Enabled</b>.</li> <li>▪ <b>Authentication User ID:</b> The same value as the <b>User ID</b> in the previous step.</li> <li>▪ <b>Authentication Password:</b> The password configured for this user ID on Avaya SES in <b>Section 4.2, Step 4</b>.</li> <li>▪ <b>Per Line Logging:</b> For the compliance test, logging was enabled by checking the check box next to <b>Enabled</b>.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <p>Click <b>OK</b>.</p> <p>A confirmation window will appear. Click <b>OK</b> in this window also.</p> 
<p><b>10.</b></p>	<p>Repeat <b>Steps 7 – 9</b> for each line where an analog endpoint is connected. After configuring all the lines, return to the <b>Voice Over IP</b> screen and click <b>OK</b>. A confirmation screen will appear, click <b>OK</b> on this screen to submit the changes. In the case of the compliance test, only one line was configured for the fax machine at the branch site.</p>

Step	Description
11.	<p>Return to the main <b>Voice Over IP</b> screen. Select the <b>Trunk Registration</b> tab. Enable trunk registration by checking the <b>Enabled</b> box next to the <b>Trunk Group Phone Registration</b> field. In addition, each trunk line must be added to the registration table. The screen bellows shows the table after all three lines were added. To add an entry, click the <b>New Entry</b> link and enter the fields described in the next step.</p> <p>Otherwise, click <b>OK</b>.</p> 

Step	Description
12.	<p>In the <b>Add PBX Phone Line</b> screen that appears, configure the following fields as described below:</p> <ul style="list-style-type: none"> <li>▪ <b>First Phone Number:</b> Enter the extension for this user.</li> <li>▪ <b>Authentication:</b> Select <i>Single User Name</i> from the pull-down menu.</li> <li>▪ <b>User Name:</b> Enter the <b>Primary Handle</b> used on Avaya SES in <b>Section 4.2, Step 4</b>.</li> <li>▪ <b>Password:</b> Enter the <b>Password</b> used on Avaya SES in <b>Section 4.2, Step 4</b>.</li> <li>▪ <b>Description:</b> Enter a descriptive name.</li> </ul> <p>Click <b>OK</b>. Repeat this step for 40119 and 3035555436.</p> 
13.	<p>Reboot all Avaya SIP telephones at the branch so the telephones will make a DHCP request to the Adit 3500 for an IP address and TFTP server address.</p>

## 5. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability between the Carrier Access Adit 3500 Trunk Gateway, Avaya Communication Manager and Avaya SIP Enablement Services (SES). This section covers the general test approach and the test results.

### 5.1. General Test Approach

The general test approach was to make calls to/from the telephones connected through the Adit 3500 at the branch site using various codec settings and exercising common PBX features. The calls were made to/from the main site, the PSTN and within the branch site.

## 5.2. Test Results

The Adit 3500 successfully passed compliance testing. The following features and functionality were verified during the interoperability compliance test. Each feature was tested with both the SIP trunking and SIP registration model, where applicable. Any limitations to a particular feature will be outlined in the “observations” that follow.

- Calls between the legacy PBX at the branch site and the main site.
- Calls between the legacy PBX at the branch site and the PSTN.
- Intra-branch calls between the legacy PBX and SIP or analog endpoints behind the Adit 3500.
- G.711mu and G.729AB codec support
- Proper recognition of DTMF transmissions
- Support for Hold, Transfer, and Call Waiting
- Conference calls between the two sites.
- Proper system recovery after an Adit 3500 restart.
- Proper operation of voicemail with message waiting indicators (MWI).
- Extended telephony features at the main site using Avaya Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Call Pickup, Automatic Redial and Send All Calls. For more details on FNEs, please refer to [5].
- Extended telephony features at the branch site using Avaya Communication Manager Feature Access Codes (FAC). For more details on FACs, please refer to [1] and [2].
- NAT'ed PC at the branch was able to connect to external sites.
- Bypass fax support. T.38 fax is not supported.

The following observations were made during the compliance test and apply to both configuration models.

- Some transfer scenarios fail intermittently if Direct IP-to-IP (shuffling) is enabled. For example, the transfer will fail if a SIP endpoint at the main site calls an endpoint on the legacy PBX at the branch and transfers the call to another legacy PBX endpoint at the branch. Thus, it is recommended that shuffling be disabled on the signaling group of the SIP trunk on Avaya Communication Manager at the main site (see **Section 3.1.1, Step 7**).
- No version of G.729 codec is supported on the FXS ports of the Adit 3500. The following observation applies to the G.729 configuration on the Adit 3500 Trunk Settings form. When using a codec setting of G.729A without silence suppression in the Adit 3500, the Adit 3500 does not send the parameter annexb=no (silence suppression disabled) in the SIP SDP information. The absence of this line implies the default setting of annexb=yes (silence suppression enabled). Thus, in order to interwork with this codec setting, Avaya Communication Manager was set to G.729AB which is equivalent to G.729A with silence suppression.
- When placing calls to busy endpoints on the legacy PBX, it takes 30 – 40 sec for the caller to hear busy tone.
- Due to an incompatibility between the stated releases of Avaya SES and the Adit 3500 used for the compliance test, the **Contact** field in the Media Server Maps of Avaya SES must specify *sips* instead of *sip*. (See **Section 3.2, Step 11**)

The additional observations were made during the compliance test and apply to the SIP registration model.

- DHCP Option 176 is not supported. Option 176 is used to provide the TFTP server IP address and other parameters to the Avaya SIP Telephones. However, DHCP Option 66 can be used instead to provide the TFTP server address.
- Faxes sent to the legacy PBX fail. Faxes sent to an analog fax machine directly connected to the Adit 3500 succeed.
- Endpoints behind the Adit 3500 can not unregister from the Avaya SES. If the endpoint is logged off or moved, the old registration will eventually timeout and be removed by the Avaya SES.
- Calls placed on hold for over three minutes from the FXS ports on the Adit 3500, require three flashes to retrieve the call instead of the normal one flash.
- If an endpoint connected to the FXS port of the Adit 3500 is configured without an OPS station on Avaya Communication Manager then some transfer scenarios involving this endpoint will fail. This configuration results in a REFER message being sent to the Adit 3500 during the transfer which the Adit 3500 does not support. In this configuration, the FXS ports on the Adit 3500 are expected to support FAX machines and modems and hence the Adit does not process REFER messages that is destined for the FXS ports. Thus, if these endpoints are intended to have more than just basic calling functionality, they should be configured as OPS stations on Avaya Communication Manager at the main site.
- Testing of the conference feature was limited to conference calls involving endpoints connected to the legacy PBX at the branch and endpoints directly connected or registered to the main site PBX. Conference calls involving the FXS ports of the Adit 3500 were not tested since it was intended, from the test configuration selected, that these endpoints only have basic call functionality.

## 6. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all endpoints connected to the Adit 3500, analog, SIP or via the ISDN-PRI trunk, are registered with the Avaya SES.
- Verify that calls can be placed to/from the analog, SIP or trunk endpoints connected to the Adit 3500.
- For further troubleshooting, logging of the SIP traffic can be enabled on the Adit 3500 by navigating to **System Monitoring → SIP Log** and checking the check box labelled **Enabled**.
- Logging of PRI traffic on the Adit 3500 can be enabled by navigating to **System Monitoring → PRI Log** and checking the check box labeled **Enabled**.

## 7. Support

For technical support on the Adit 3500 Trunk Gateway, contact Carrier Access toll-free at (800) 786-9929. Support can also be obtained via email at [tech-support@carrieraccess.com](mailto:tech-support@carrieraccess.com) or via the web site [www.carrieraccess.com](http://www.carrieraccess.com).

## 8. Conclusion

These Application Notes describe the procedures required to configure the Carrier Access Adit 3500 Trunk Gateway to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager. The Adit 3500 successfully passed compliance testing with the observations noted in **Section 5.2**.

## 9. Additional References

- [1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 4.0, February 2006.
- [2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2.1, May 2006.
- [3] *SIP Support in Release 3.1 of Avaya Communication Manager Running on the Avaya S8300, S8500, S8500B, S8700 and S8710 Media Server*, Doc # 555-245-206, Issue 6.1, March 2007.
- [4] *Installing and Administering SIP Enablement Services*, Doc# 03-600768, Issue 2.1, March 2007.
- [5] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, version 6.0, Doc # 210-100-500, Issue 9, June 2005.
- [6] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005.
- [7] *Carrier Access Adit 3500 Trunk Gateway Installation Guide*
- [8] *Carrier Access Adit 3500 Trunk Gateway Administration Guide*

Product documentation for Avaya products may be found at <http://support.avaya.com>.

Product documentation for the Carrier Access Adit 3500 Trunk Gateway may be found at <http://www.carrieraccess.com>.

## APPENDIX A: Specifying Pattern Strings in Address Maps

The syntax for the pattern matching used within Avaya SES is a Linux regular expression used to match against the URI string found in the SIP INVITE message.

Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special *metacharacters*, which may represent items like quantity, location or types of character(s).

In the pattern matching string used in Avaya SES:

- Normal text characters and numbers match themselves.
- Common metacharacters used are:
  - A period `.` matches any character once (and only once).
  - A asterisk `*` matches zero or more of the preceding characters.
  - Square brackets enclose a list of any character to be matched. Ranges are designated by using a hyphen. Thus, the expression `[12345]` or `[1-5]` both describe a pattern that will match any single digit between 1 and 5.
  - Curley brackets containing an integer 'n' indicate that the preceding character must be matched exactly 'n' time. Thus, `5{3}` matches '555' and `[0-9]{10}` indicates any 10 digit number.
  - The circumflex character `^` as the first character in the pattern indicates that the string must begin with the character following the circumflex.

Putting these constructs together as used in this document, the pattern to match the SIP INVITE string for any valid 1+ 10 digit number in the North American dial plan would be:

**`^sip:1[0-9]{10}`**

This reads as: “Strings that begin with exactly **sip:1** and having any 10 digits following will match.

A typical INVITE request below uses the shaded portion to illustrate the matching pattern.

```
INVITE sip:17325551638@20.1.1.54:5060;transport=udp SIP/2.0
```

---

**©2007 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](mailto:devconnect@avaya.com).