



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

---

# **Application Notes for the TeleData Technology T3 Platform with Avaya Communication Manager and Avaya SIP Enablement Services – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration procedures required for the TeleData Technology T3 Platform to successfully interoperate with Avaya Communication Manager and Avaya SIP Enablement Services using the Session Initiation Protocol (SIP).

The TeleData Technology T3 Platform is a unified messaging solution supporting voicemail, email, auto attendant, recorded announcements and speech recognition. The compliance test focused only on the auto attendant and voicemail capabilities.

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

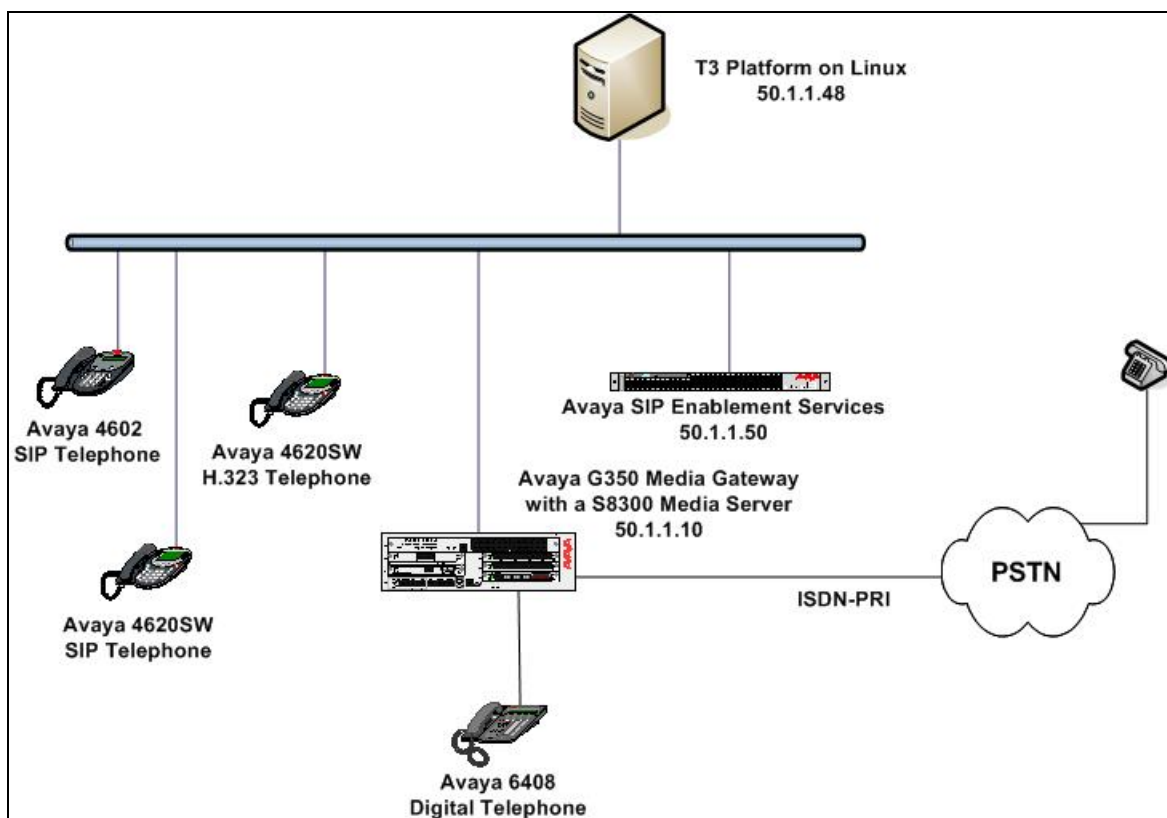
# 1. Introduction

These Application Notes describe the configuration procedures required for the TeleData Technology T3 Platform to successfully interoperate with Avaya Communication Manager and Avaya SIP Enablement Services using the Session Initiation Protocol (SIP).

The TeleData Technology T3 Platform is a unified messaging solution supporting voicemail, email, auto attendant, recorded announcements and speech recognition. The compliance test focused only on the auto attendant and voicemail capabilities.

**Figure 1** shows the test configuration used for the compliance test. The configuration is comprised of an Avaya S8300 Media Server running Avaya Communication Manager in an Avaya G350 Media Gateway and Avaya SIP Enablement Services (SES). Endpoints include an Avaya 6400D Series Digital Telephone, an Avaya 4600 Series H.323 IP Telephone and two Avaya 4600 Series SIP Telephones. An ISDN-PRI trunk provides a connection to the PSTN. The T3 Platform runs on a Linux server and establishes a SIP signaling connection to Avaya SES, which acts as a SIP proxy for Avaya Communication Manager. This allows the T3 Platform to originate and terminate SIP calls to Avaya Communication Manager.

The SIP signaling connection can be established in one of two ways. Both approaches were tested as part of the compliance test. In the first approach, a SIP trunk is established between the T3 Platform and Avaya SES. In the second approach, the T3 Platform registers as a number of SIP endpoints to Avaya SES. In either case, a hunt group is created to route calls to the SIP trunk or group of SIP endpoints. This hunt group is then used as the coverage point for local extensions to provide voicemail service. Calls from local extensions to the hunt group extension allow users the option to retrieve voicemail messages. External calls to the hunt group DID number connects callers to the automated attendant where an option is provided to transfer to another extension.



**Figure 1: TeleData Technology T3 SIP Test Configuration**

## 2. Equipment and Software Validated

The following equipment and software/firmware were used for the test configuration provided.

Equipment	Software/Firmware
Avaya S8300 Media Server	Avaya Communication Manager 3.1 (R013x.01.0.628.6) with Service Pack (R013x.01.0.628.6- 11410)
Avaya G350 Media Gateway	25.23.0
Avaya Services Enablement Services (SES)	3.1 (SES-3.1.0.0-018.0)
Avaya 4600 Series SIP Telephones	2.2.2 (4602) 2.2.2 (4620SW)
Avaya 4600 Series H.323 IP Telephones	2.3 (4620SW)
Avaya 6400D Series Digital Telephones	-
TeleData Technology T3 Platform	10.4.2 and pre-GA release of Service Pack 1 running on Linux CentOS 4.2 (kernel 2.6.9-22)

### 3. Configure the Solution to Use SIP Trunking (Approach 1)

This section describes the necessary configuration on Avaya Communication Manager, Avaya SES and the TeleData Technology T3 Platform to use SIP trunking as a means to establish the necessary SIP signaling connection between Avaya SES and the T3 Platform. In this approach, the Avaya SES server routes calls across a logical SIP trunking connection to the T3 Platform via address maps defined in Avaya SES. The T3 Platform does not register with Avaya SES, but instead is defined in Avaya SES as a trusted host. This in turn affects the way the voice mail hunt group and routing is defined on Avaya Communication Manager.

#### 3.1. Configure Avaya Communication Manager

Independent of which approach is used for the connection between Avaya SES and the T3 Platform, the connection between Avaya Communication Manager and Avaya SES is via a SIP trunk group. All SIP signaling for calls between Avaya Communication Manager and the T3 Platform pass through Avaya SES via this trunk group. This section describes the steps for configuring this trunk group, the associated signaling group, as well as the coverage path, hunt group and route pattern necessary to direct traffic to the trunk group.

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 translations** command to make the changes permanent.

Step	Description
1.	<p>Use the <b>display system-parameters customer-options</b> command to verify that sufficient SIP trunk capacity exists. On Page 2, 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                                 OPTIONAL FEATURES  IP PORT CAPACITIES                                 USED       Maximum Administered H.323 Trunks: 100    10       Maximum Concurrently Registered IP Stations: 20    0       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>
2.	<p>Use the <b>change node-name ip</b> command to assign the node name and IP address for Avaya SES at the enterprise site. In this case, <b>SES</b> and <b>50.1.1.50</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>50.1.1.10</b> are the name and IP address assigned to the Avaya S8300 Media Server.</p> <div> <pre> change node-names ip                                 IP NODE NAMES                                 Name      IP Address       Name      IP Address       SES      50 .1 .1 .50       default   0 .0 .0 .0       procr     50 .1 .1 .10 </pre> </div>

Step	Description
3.	<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 Step 5. In the case of the compliance test, the same IP network region that contains the Avaya S8300 Media Server was selected to contain the Avaya SES server. By default, the Media Server is 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>devcon.com</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 G350 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 Page 3 of each <b>IP Network Region</b> form 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="315 1180 1416 1738"> <pre> change ip-network-region 1                                     Page 1 of 19   IP NETWORK REGION Region: 1 Location: 1           Authoritative Domain: devcon.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? y       UDP Port Max: 3027 DIFFSERV/TOS PARAMETERS                RTCP Reporting Enabled? y Call Control PHB Value: 34              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																
4.	<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 Step 3, 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>Page1 of 2</div></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: G.711MU</td><td>n</td><td>2</td><td>20</td></tr><tr><td>2: G.729B</td><td>n</td><td>2</td><td>20</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: G.711MU	n	2	20	2: G.729B	n	2	20	3:			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)														
1: G.711MU	n	2	20														
2: G.729B	n	2	20														
3:																	

Step	Description
5.	<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 Step 2. For other Media Server platforms 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 recommended 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 Step 3. 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>devcon.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>y</i>.</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="315 1325 1414 1812" style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <pre> add signaling-group 1                                 SIGNALING GROUP                                 Page 1 of 1  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: devcon.com                                  Bypass If IP Threshold Exceeded? y  DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y                                 IP Audio Hairpinning? y  Session Establishment Timer(min): 120 </pre> </div>



Step	Description
6.	<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 Page 1, 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 Step 5.</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>Use the default values for the other fields.</li> </ul> <div data-bbox="315 921 1414 1268"> <pre> add trunk-group 1                                     Page 1 of 21                                      TRUNK GROUP  Group Number: 1                      Group Type: sip          CDR Reports: y   Group Name: To SES 50.1.1.50        COR: 1                TN: 1          TAC: 101     Direction: two-way                Outgoing Display? n     Dial Access? n                    Night Service:     Queue Length: 0   Service Type: tie                    Auth Code? n                                       Signaling Group: 1                                      Number of Members: 24 </pre> </div>
7.	<p>On Page 2:</p> <ul style="list-style-type: none"> <li>Set the <b>Numbering Format</b> field to <i>public</i>. This field specifies the format of the calling party number sent to the far-end.</li> <li>Use the default values for the other fields.</li> </ul> <div data-bbox="315 1486 1414 1814"> <pre> change 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
8.	<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 Step 6. In the example shown below, all calls originating from a 5-digit extension beginning with 4 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> <div>change public-unknown-numbering 0</div> <div> <div>NUMBERING - PUBLIC/UNKNOWN FORMAT</div> <div> <div>Page 1 of 2</div> <div>Total</div> <div> <div>Ext Ext Trk CPN</div> <div>CPN Ext Ext Trk CPN</div> <div> <div>Len Code Grp(s) Prefix</div> <div>Len Len Code Grp(s) Prefix</div> <div> <div>5 4 1</div> <div>5</div> <div>Total</div> <div>CPN</div> <div>Len</div> </div> </div> </div> </div> </div> </div>

Step	Description
9.	<p>Create a route pattern that will use the SIP trunk that connects to Avaya SES. 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 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. Although setting the Prefix Mark value was not required for the compliance test, the Prefix Mark (<b>Pfx Mrk</b>) field was set to <b>1</b>. The Prefix Mark is important when dialing 10 or 11 digit PSTN numbers and determines when the called number should be prefixed with a 1. Setting the <b>Pfx Mrk</b> field to 1 results in a 1 being prefixed to any 10-digit called number. An 11-digit called number, presumably already preceded with a 1, is left unchanged. Setting the Prefix Mark was not required since outbound PSTN numbers do not use this route pattern. Use default values for all other fields.</p> <pre> change route-pattern 3                                     Page 1 of 3       Pattern Number: 3   Pattern Name: SIP       SCCAN? n          Secure SIP? n       Grp FRL NPA Pfx Hop Toll No.  Inserted          DCS/ IXC       No      Mrk Lmt List Del  Digits              QSIG   Intw 1: 1      0      1 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 2: y y y y y n n      rest 3: y y y y y n n      rest 4: y y y y y n n      rest 5: y y y y y n n      rest 6: y y y y y n n      rest   none   none   none   none   none   none </pre>
10.	<p>Use the <b>change locations</b> command to assign the route pattern to the location. Only one location, Main, exists. Enter the route pattern number from the previous step in the <b>Proxy Sel. Rte Pat.</b> field. Use the default values 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      FAC  FAC      fix      Rte. Pat. 1:  Main      + 00:00  0 2: 3: </pre>

Step	Description																																																
11.	<p>Coverage to voicemail was accomplished by routing the call to the SIP trunk via Automatic Alternate Routing (AAR). Use the <b>change feature-access-codes</b> command to provide a digit string to be dialed to access AAR. The digit string must be consistent with the existing dial plan for a feature access code (FAC).</p> <div><div>change feature-access-codes</div><div>Page 1 of 6</div><div>FEATURE ACCESS CODE (FAC)</div><div>Abbreviated Dialing List1 Access Code:</div><div>Abbreviated Dialing List2 Access Code:</div><div>Abbreviated Dialing List3 Access Code:</div><div>Abbreviated Dial - Prgm Group List Access Code:</div><div>Announcement Access Code: *11</div><div>Answer Back Access Code: *12</div><div>Attendant Access Code:</div><div>Auto Alternate Routing (AAR) Access Code: 8</div><div>Auto Route Selection (ARS) - Access Code 1: 9</div><div>Access Code 2:</div><div>Automatic Callback Activation: *16</div><div>Deactivation: #16</div><div>Call Forwarding Activation Busy/DA: *17 All: *18</div><div>Deactivation: #18</div><div>Call Park Access Code: *19</div><div>Call Pickup Access Code: *20</div><div>CAS Remote Hold/Answer Hold-Unhold Access Code:</div><div>CDR Account Code Access Code:</div><div>Change COR Access Code:</div><div>Change Coverage Access Code:</div><div>Contact Closure Open Code:</div><div>Close Code:</div><div>Contact Closure Pulse Code:</div></div>																																																
12.	<p>Create an entry in the AAR Digit Analysis Table to map a set of dialed digits to the route pattern created in Step 9. Any dialed string that does not conflict with another entry in the table can be used. For the compliance test, the dial string of <b>79000</b> was used. Use the <b>change aar analysis 7</b> command to modify entries in the table that start with 7. Add an entry in the table for <b>79000</b>. Set each field of the entry to the value shown in bold below.</p> <div><div>change aar analysis 7</div><div>Page 1 of 2</div><div>AAR DIGIT ANALYSIS TABLE</div><div>Percent Full: 3</div><table><thead><tr><th>Dialed String</th><th>Total Min Max</th><th>Route Pattern</th><th>Call Type</th><th>Node Num</th><th>ANI Req'd</th></tr></thead><tbody><tr><td>7</td><td>7 7</td><td>254</td><td>aar</td><td></td><td>n</td></tr><tr><td>79000</td><td>5 5</td><td>3</td><td>aar</td><td></td><td>n</td></tr><tr><td>8</td><td>7 7</td><td>254</td><td>aar</td><td></td><td>n</td></tr><tr><td>9</td><td>7 7</td><td>254</td><td>aar</td><td></td><td>n</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>n</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>n</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>n</td></tr></tbody></table></div>	Dialed String	Total Min Max	Route Pattern	Call Type	Node Num	ANI Req'd	7	7 7	254	aar		n	79000	5 5	3	aar		n	8	7 7	254	aar		n	9	7 7	254	aar		n						n						n						n
Dialed String	Total Min Max	Route Pattern	Call Type	Node Num	ANI Req'd																																												
7	7 7	254	aar		n																																												
79000	5 5	3	aar		n																																												
8	7 7	254	aar		n																																												
9	7 7	254	aar		n																																												
					n																																												
					n																																												
					n																																												

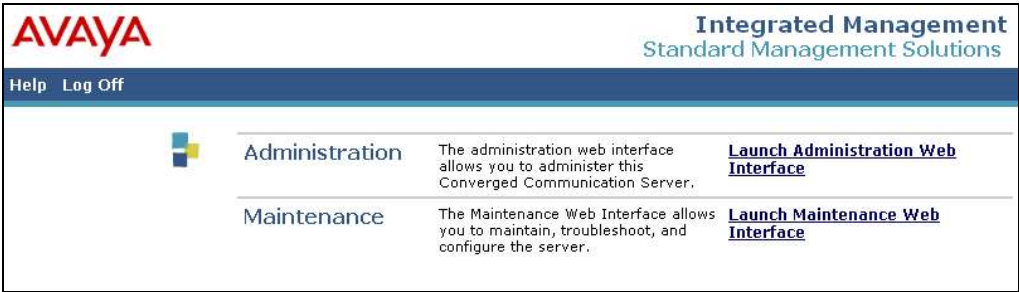
Step	Description
13.	<p>Create a hunt group using the <b>add hunt-group <i>n</i></b> command, where <b><i>n</i></b> is the number of an unused hunt group. This hunt group will provide the access number for the T3 Platform. Enter any descriptive name for the <b>Name</b> field. Enter an unused extension for the <b>Group Extension</b> field. Use default values for all other fields.</p> <div> <pre> add hunt-group 2                                      Page 1 of 60                                       HUNT GROUP  Group Number: 2                      ACD? n Group Name: TeleData                 Queue? n Group Extension: 43000               Vector? n Group Type: ucd-mia                 Coverage Path: TN: 1                               Night Service Destination: COR: 1                               MM Early Answer? n Security Code:                      Local Agent Preference? n ISDN/SIP Caller Display: </pre> </div>
14.	<p>On Page 2, set the <b>Message Center</b> field to <i>sip-adjunct</i>. Calls to the T3 Platform will be routed to the proper route pattern via AAR. As a result, set the <b>Routing Digits</b> field to the AAR feature access code defined in Step 11. Set the <b>Voice Mail Number</b> and <b>Voice Mail Handle</b> to the digit string that is used by AAR to select the correct route pattern to access the T3 Platform as defined in Step 12.</p> <div> <pre> change hunt-group 2 60                                     Page 2 of                                       HUNT GROUP                                       Message Center: sip-adjunct  Voice Mail Number    Voice Mail Handle    Routing Digits                                      (e.g., AAR/ARS Access Code) 79000                79000                8 </pre> </div>

Step	Description
15.	<p>Create a coverage path that will use the T3 Platform hunt group when calls are busy, sent to coverage or not answered. Use the <b>change coverage path <i>n</i></b> command where <b><i>n</i></b> is the number of an unused coverage path. Set the first point in the coverage path to be hunt group 2 by setting the <b>Point1</b> field to <b><i>h2</i></b>.</p> <pre> change coverage path 3                                     Page 1 of 1                                  COVERAGE PATH  Coverage Path Number: 3                                Hunt after Coverage? n Next Path Number:   Linkage  COVERAGE CRITERIA  Station/Group Status   Inside Call   Outside Call Active?                n                n Busy?                  y                y Don't Answer?          y                y                Number of Rings: 2 All?                   n                n DND/SAC/Goto Cover?    y                y Holiday Coverage?      n                n  COVERAGE POINTS Terminate to Coverage Pts. with Bridged Appearances? n  Point1: h2           Rng:   Point2:                Point3: Point4:              Point5:                Point6: </pre>
16.	<p>Each station that will use the T3 Platform for voicemail must be configured to use the correct coverage path. To set the coverage path, use the <b>change station <i>n</i></b> command, where <b><i>n</i></b> is the extension number to be modified. Set the <b>Coverage Path 1</b> field to the coverage path defined in Step 15.</p> <pre> change station 40014                                     Page 1 of 4                                  STATION  Extension: 40014                                Lock Messages? n                BCC: 0 Type: 4620                                Security Code: *                TN: 1 Port: S00008                                Coverage Path 1: 3                COR: 1 Name: Tim H323-1                                Coverage Path 2:                COS: 1   Hunt-to Station:  STATION OPTIONS  Loss Group: 19                                Personalized Ringing Pattern: 1   Message Lamp Ext: 40014 Speakerphone: 2-way                                Mute Button Enabled? y Display Language: english                                Expansion Module? n Survivable GK Node Name:                                Media Complex Ext: Survivable COR: internal                                IP SoftPhone? n Survivable Trunk Dest? y  Customizable Labels? y </pre>

Step	Description
17.	<p>Lastly, each station that will use the T3 Platform for voicemail must be configured to use <i>sip-adjunct</i> as the <b>MWI Served User Type</b> on Page 2.</p> <pre> change station 40014                                     Page 2 of 4                                      STATION FEATURE OPTIONS     LWC Reception: spe                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          Restrict Last Appearance? n     Active Station Ringing: single     Conf/Trans on Primary Appearance? n                                      EMU Login Allowed? n     H.320 Conversion? n              Per Station CPN - Send Calling Number?     Service Link Mode: as-needed     Multimedia Mode: enhanced         Audible Message Waiting? n     MWI Served User Type: sip-adjunct Display Client Redirection? n                                      Select Last Used Appearance? n                                      Coverage After Forwarding? s                                       Direct IP-IP Audio Connections? y Emergency Location Ext: 40014        Always Use? n        IP Audio Hairpinning? y </pre>
18.	<p>To map a DID number to the T3 Platform hunt group, use the <b>change inc-call-handling-trmt trunk-group <i>n</i></b> command, where <i>n</i> is the trunk group number connected to the PSTN. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows an incoming 11-digit number being deleted and replaced with the extension number of the T3 Platform hunt group. This allows external callers to reach the T3 Platform to access the automated attendant.</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    43000 </pre>

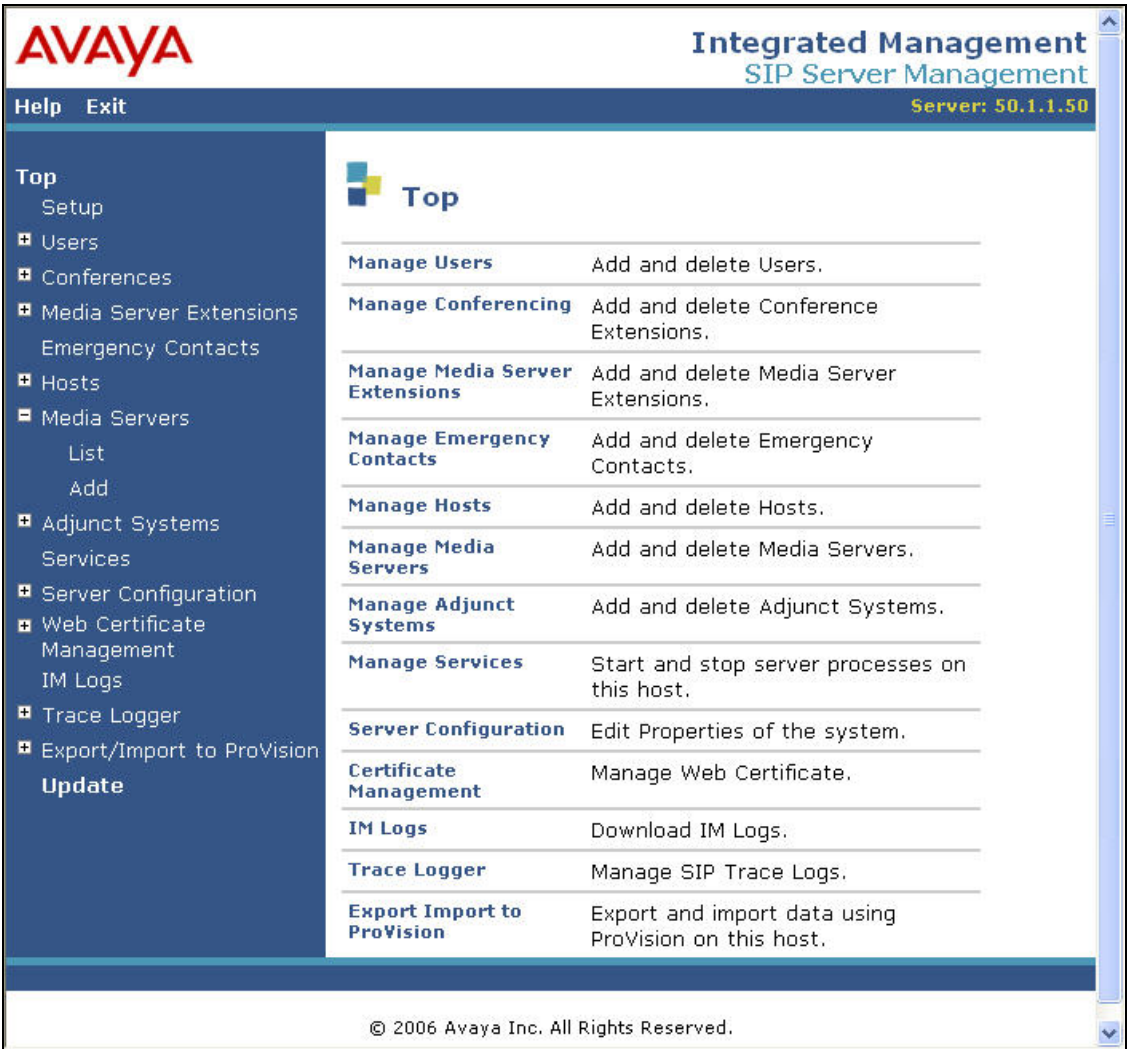
### 3.2. Configure Avaya SES

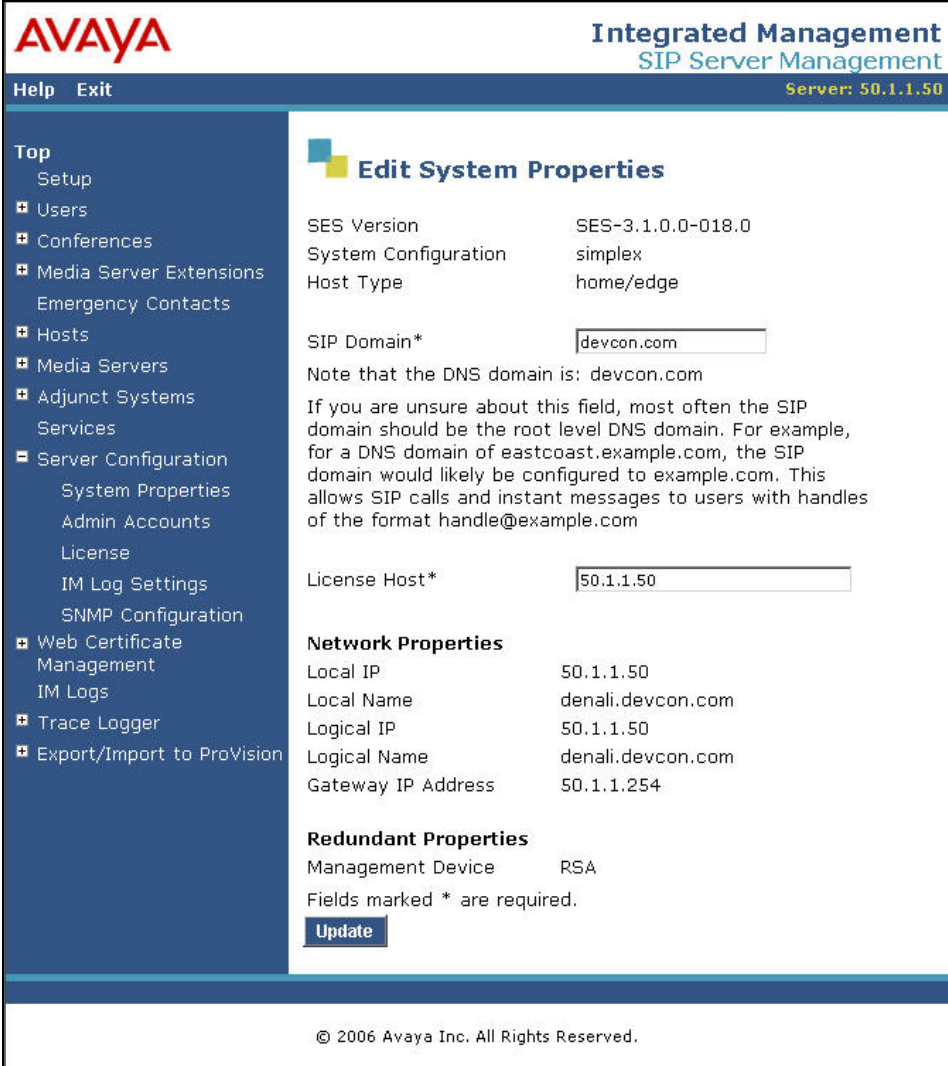
This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that Avaya SES software and the license file have already been installed on the server. During the software installation, the installation script is 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 [3].

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 an Internet 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> 

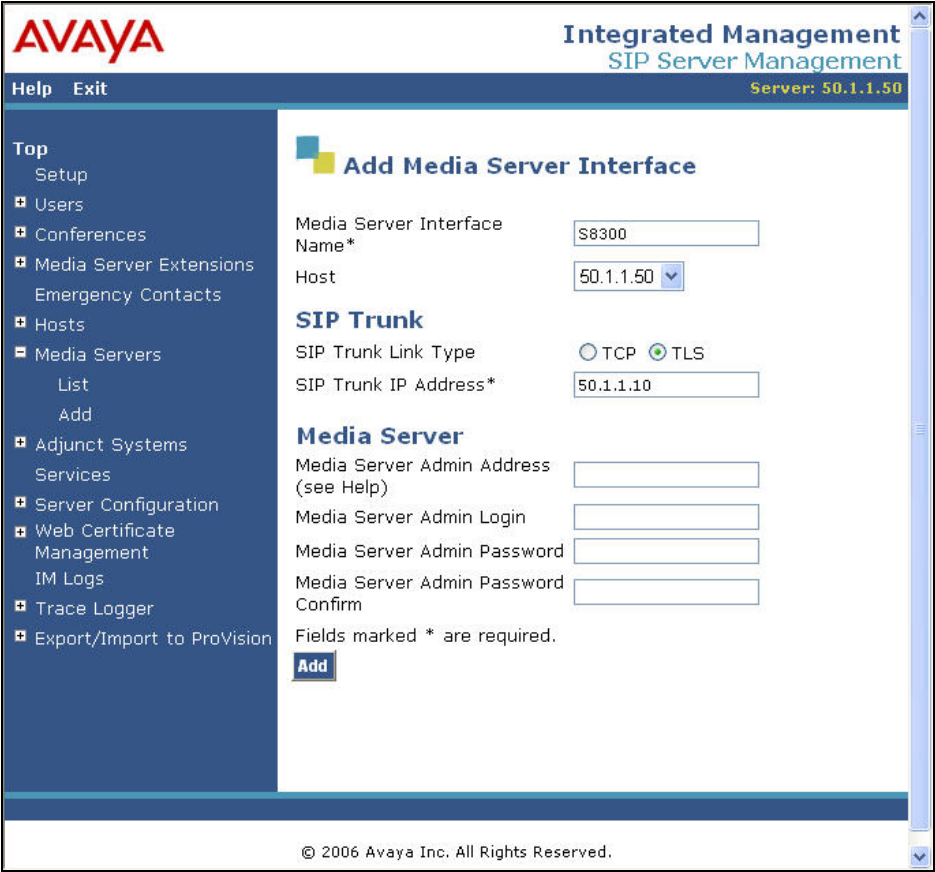



Step	Description
2.	<p>The Avaya SES Administration Home Page will be displayed as shown below.</p>  <p>The screenshot shows the Avaya SES Administration Home Page. At the top left is the Avaya logo. To its right is the text 'Integrated Management SIP Server Management' and 'Server: 50.1.1.50'. Below this is a navigation bar with 'Help' and 'Exit' links. On the left side, there is a vertical menu with the following items: Top, Setup, Users, Conferences, Media Server Extensions, Emergency Contacts, Hosts, Media Servers, Adjunct Systems, Services, Server Configuration, Web Certificate Management, IM Logs, Trace Logger, and Export/Import to ProVision. The main content area on the right is titled 'Top' and contains a list of management tasks, each with a description:</p> <ul style="list-style-type: none"> <li><b>Manage Users</b>: Add and delete Users.</li> <li><b>Manage Conferencing</b>: Add and delete Conference Extensions.</li> <li><b>Manage Media Server Extensions</b>: Add and delete Media Server Extensions.</li> <li><b>Manage Emergency Contacts</b>: Add and delete Emergency Contacts.</li> <li><b>Manage Hosts</b>: Add and delete Hosts.</li> <li><b>Manage Media Servers</b>: Add and delete Media Servers.</li> <li><b>Manage Adjunct Systems</b>: Add and delete Adjunct Systems.</li> <li><b>Manage Services</b>: Start and stop server processes on this host.</li> <li><b>Server Configuration</b>: Edit Properties of the system.</li> <li><b>Certificate Management</b>: Manage Web Certificate.</li> <li><b>IM Logs</b>: Download IM Logs.</li> <li><b>Trace Logger</b>: Manage SIP Trace Logs.</li> <li><b>Export Import to ProVision</b>: Export and import data using ProVision on this host.</li> </ul> <p>At the bottom of the page, it says '© 2006 Avaya Inc. All Rights Reserved.'</p>

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> 

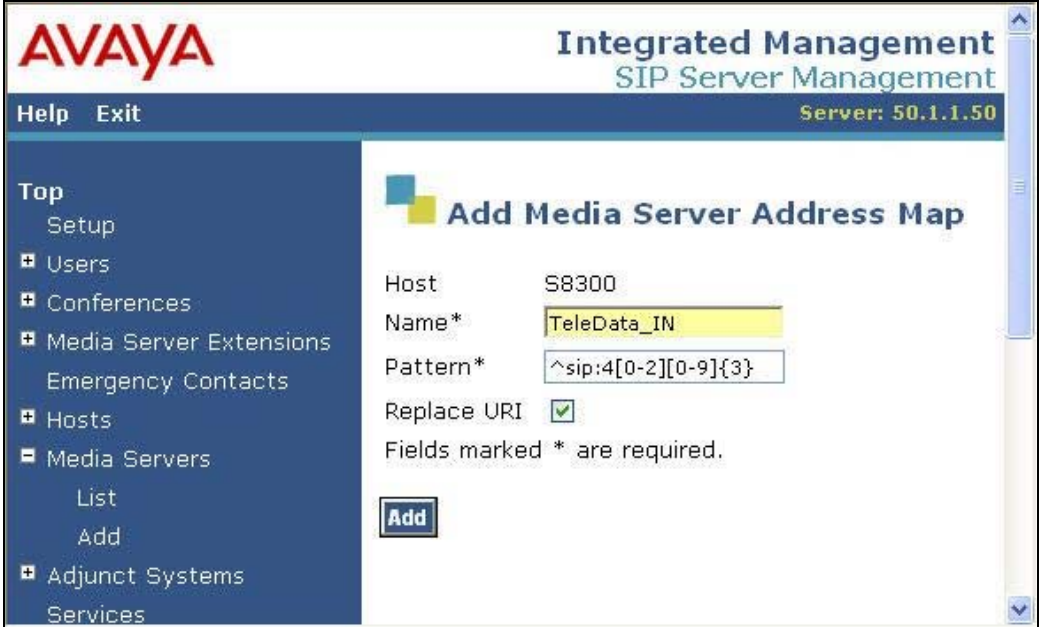
Step	Description
4.	<p>From the left pane of the administration web interface, expand the <b>Server Configuration</b> option and select <b>System Properties</b>. The <b>Edit System Properties</b> page displays the software version in the <b>SES Version</b> field and the network properties entered during the installation process.</p> <p>On the <b>Edit System Properties</b> page:</p> <ul style="list-style-type: none"> <li>Enter 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 Section 3.2, Step 3.</li> <li>Enter 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 configuring the <b>Edit System Properties</b> page, click the <b>Update</b> button.</li> </ul>  <p>The screenshot shows the 'Edit System Properties' page in the Avaya Integrated Management SIP Server Management interface. The left sidebar contains a navigation menu with options like Top, Setup, Users, Conferences, Media Server Extensions, Emergency Contacts, Hosts, Media Servers, Adjunct Systems, Services, Server Configuration (expanded), System Properties, Admin Accounts, License, IM Log Settings, SNMP Configuration, Web Certificate Management, IM Logs, Trace Logger, and Export/Import to ProVision. The main content area displays the following information:</p> <ul style="list-style-type: none"> <li><b>SES Version:</b> SES-3.1.0.0-018.0</li> <li><b>System Configuration:</b> simplex</li> <li><b>Host Type:</b> home/edge</li> <li><b>SIP Domain*:</b> devcon.com</li> <li><b>Note:</b> Note that the DNS domain is: devcon.com</li> <li><b>License Host*:</b> 50.1.1.50</li> <li><b>Network Properties:</b> <ul style="list-style-type: none"> <li>Local IP: 50.1.1.50</li> <li>Local Name: denali.devcon.com</li> <li>Logical IP: 50.1.1.50</li> <li>Logical Name: denali.devcon.com</li> <li>Gateway IP Address: 50.1.1.254</li> </ul> </li> <li><b>Redundant Properties:</b> <ul style="list-style-type: none"> <li>Management Device: RSA</li> </ul> </li> </ul> <p>Fields marked * are required. An 'Update' button is located at the bottom of the form.</p>


Step	Description
5.	<p>After setting up the domain on the <b>Edit System Properties</b> page, create a 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</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 that is displayed.</p> <ul style="list-style-type: none"> <li>▪ In the <b>Host IP Address</b> field, enter the <b>Logical IP</b> or <b>Logical Name</b> of this server as shown in Step 4.</li> <li>▪ Enter the <b>DB Password</b> that was specified during the system installation.</li> <li>▪ The default values for the other fields may be used.</li> </ul> <div data-bbox="313 667 1437 1234"> <p>The screenshot displays the 'Edit Host' configuration page in the Avaya Integrated Management SIP Server Management interface. The left-hand navigation pane is expanded to show the 'Hosts' section, which includes sub-links for 'List' and 'Migrate Home/Edge'. The main content area is titled 'Edit Host' and contains several configuration fields. The 'Host IP Address*' field is populated with '50.1.1.50'. The 'DB Password' and 'Profile Service Password' fields are masked with dots. The 'Host Type' is set to 'home/edge' and the 'Parent' is set to 'none'. Under 'Listen Protocols', the checkboxes for UDP, TCP, and TLS are all checked. Under 'Link Protocols', the radio buttons for UDP and TCP are unselected, while the radio button for TLS is selected. The 'Presence' field is empty. The 'Access Policy' section shows 'Allow All' as an unselected radio button and 'Deny All' as a selected radio button. At the bottom of the page, there is a note stating 'Fields marked * are required.' and an 'Update' button.</p> </div> <ul style="list-style-type: none"> <li>▪ Scroll down to the bottom of the page and click the <b>Update</b> button.</li> </ul> <div data-bbox="313 1339 1437 1518"> <p>This screenshot shows the bottom portion of the 'Edit Host' page. It features a blue sidebar on the left and a white main area. In the white area, there is a text label 'Fields marked * are required.' and a blue button labeled 'Update'.</p> </div>

Step	Description
6.	<p>From the left pane of the administration web interface, expand the <b>Media Server</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>▪ A descriptive name in the <b>Media Server Interface Name</b> field (e.g. S8300).</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 Step 4.</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 other media server platforms, 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>▪ Use the default values for all other fields.</li> <li>▪ After completing the <b>Add Media Server</b> page, click the <b>Add</b> button.</li> </ul> 

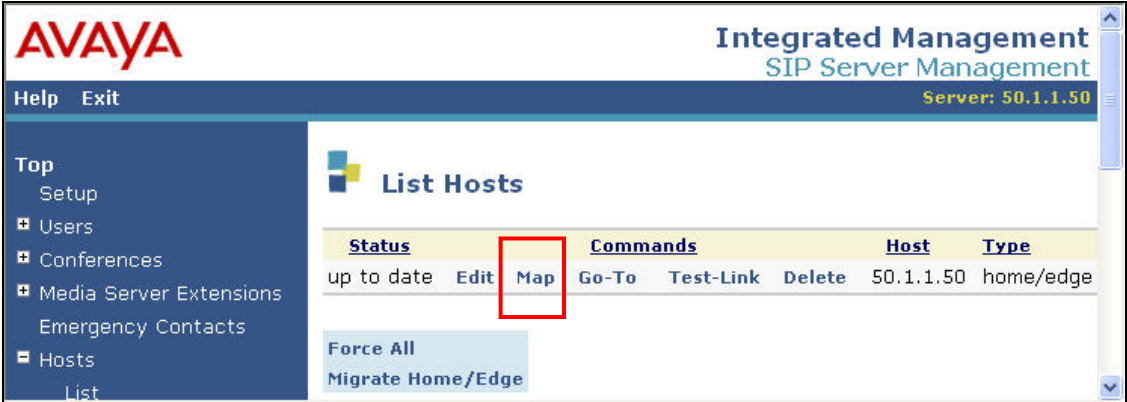
Step	Description
7.	<p>Inbound SIP calls arriving at Avaya SES are routed to Avaya Communication Manager. This routing is specified in a Media Server Address Map configured on Avaya SES. This routing compares the Uniform Resource Identifier (URI) of an incoming INVITE message to the pattern configured in the Media Server Address Map, and if there is a match, the call is routed to Avaya Communication Manager. The URI usually takes the form of <i>sip:user@domain</i>, where <i>domain</i> can be a domain name or an IP address.</p> <p>Calls originated by Avaya SIP telephones configured as OPS stations do not require a Media Server Address Map. These calls are automatically routed to Avaya Communication Manager by the assignment of a media server extension to that phone.</p> <p>In the test configuration, incoming calls from the T3 Platform, which occur when transferring from the automated attendant or voicemail, require a Media Server Address Map entry. The Media Server Address Map was defined to match 5 digit extensions in the range of 40000 – 42999 using the regular expression of <code>^sip:4[0-2][0-9]{3}</code>. Appendix A provides a detailed description of the syntax for address map patterns.</p> <p>To view the <b>Media Server Address Maps</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 shown below.</li> <li>On the <b>List Media Servers</b> page, select the <b>Map</b> link associated with the media server to display the <b>List Media Server Address Map</b> page. The <b>Map</b> link is highlighted in the example below.</li> </ul> 





Step	Description
8.	<p>The <b>List Media Server Address</b> page is displayed. On the <b>List Media Server Address</b> page, select the <b>Add Map In New Group</b> link. The <b>Add Media Server Address Map</b> page is displayed as shown below.</p> <p>To add a new <b>Media Server Address Map</b>, configure or verify the following:</p> <ul style="list-style-type: none"> <li>▪ The <b>Host</b> field displays the name of the media server to which this map applies.</li> <li>▪ Enter a descriptive name in the <b>Name</b> field.</li> <li>▪ In the <b>Pattern</b> field, enter the regular expression to be used for the pattern matching.</li> <li>▪ Click the <b>Add</b> button once the form is completed.</li> </ul> 

Step	Description
9.	<p>After configuring the Media Server Address Map, the <b>List Media Server Address Map</b> page appears as shown below.</p>  <p>After the first Media Server Address Map is added, the Media Server Contact is created automatically. For the Media Server Address Map that was added, the following contact was created and displayed in the <b>Contact</b> field:</p> <pre> sip:\$(user)@50.1.1.10:5061;transport=tls </pre> <p>The contact specifies the IP address of the Avaya S8300 Media Server and the transport protocol used to send SIP signaling messages. The user in the original request URI is substituted for <code>\$(user)</code>.</p>



Step	Description
10.	<p>Outbound SIP calls are first directed by Avaya Communication Manager routing decisions to the SIP trunk group. These calls are then subject to further routing decisions determined by the Host Address Maps in Avaya SES. Similar to the inbound Media Server Address Maps, these Host Address Maps use pattern matching to direct outbound SIP messages to the proper destination. Furthermore, to ensure correct routing of calls by Avaya SES, the Host Address Maps and Media Server Address Maps must be mutually exclusive. Stated differently, any sequence of dialed digits or received digits in an external SIP call should match only one address map.</p> <p>It should be noted that a user dialed access code, such as a 9 to place an outbound call, is deleted by Avaya Communication Manager prior to routing the call to Avaya SES. Thus, these access codes do not appear in the matching patterns.</p> <p>In the test configuration, outgoing calls to the T3 Platform, which occur when calls go to coverage, go to the automated attendant or users retrieve messages, require a Host Address Map entry. The Host Address Map was defined to match the digit string 79000 which is the digit string used to route the call using AAR in Section 3.2 Step 12. The address map used the following regular expression: <code>^sip:79000</code>. Appendix A provides a detailed description of the syntax for address map patterns.</p> <p>To view the <b>Host Address Maps</b>:</p> <ul style="list-style-type: none"> <li>Expand the <b>Hosts</b> link in the left pane of the administration web interface and select <b>List</b>. This will display the <b>List Hosts</b> page as shown below.</li> <li>On the <b>List Host</b> page, select the <b>Map</b> link associated with the appropriate host to display the <b>List Host Address Map</b> page. The <b>Map</b> link is highlighted in the example below.</li> </ul> 

Step	Description
11.	<p>The <b>List Host Address</b> page is displayed. From the <b>List Host Address</b> page, select the <b>Add Map In New Group</b> link. The <b>Add Host Address Map</b> page is displayed as shown below.</p> <p>To add a new <b>Host Address Map</b>, configure the following:</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 the regular expression to be used for the pattern matching.</li> <li>▪ Leave the <b>Replace URI</b> checkbox selected.</li> <li>▪ Click the <b>Add</b> button once the form is completed.</li> </ul> 

Step	Description
12.	<p>The IP address for the T3 Platform must be administered in Avaya SES. In the example below, the IP address 50.1.1.48 is used.</p> <p>To enter the SIP proxy information:</p> <ul style="list-style-type: none"> <li>Display the <b>List Host Address Map</b> page as described Step 10.</li> <li>From <b>List Host Address Map</b> page, select the <b>Add Another Contact</b> link associated with the address map added previously to display the <b>Add Host Contact</b> page. On this page, the <b>Contact</b> field specifies the destination for the call and it is entered as:</li> </ul> <pre>sip:\$(user)@50.1.1.48:5060;transport=udp</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 T3 Platform.</p> <ul style="list-style-type: none"> <li>Click the <b>Add</b> button when completed.</li> </ul> <p>After configuring the host contact information, the <b>List Host Address Map</b> page will appear as shown below.</p> 

Step	Description
13.	<p>Complete the administration of Avaya SES by designating the IP address of the T3 Platform as a trusted host. As a trusted host, Avaya SES will not issue SIP authentication challenges for incoming requests from the designated IP address.<sup>1</sup></p> <p>To configure a trusted host:</p> <ul style="list-style-type: none"><li>Connect to the Avaya SES IP address (50.1.1.50) and log in using the administrative login and password.</li><li>Enter the following <b>trustedhost</b> command at the Linux shell prompt.</li></ul> <pre>trustedhost -a 50.1.1.48 -n 50.1.1.50 -c Teledata</pre> <p>The <b>-a</b> argument specifies the address to be trusted; <b>-n</b> specifies the Avaya SES host name or IP address; <b>-c</b> adds a comment.</p> <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> <p>The screen below illustrates the results of the <b>trustedhost</b> commands.<sup>2</sup></p> <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 on the <b>Update</b> link as shown in Step 3. If the <b>Update</b> link is not visible, refresh the page by selecting <b>Top</b> from the left hand menu. This step is required even though the trusted host was configured via the Linux shell.</li></ul> <div><pre>admin@k2&gt; trustedhost -a 50.1.1.48 -n 50.1.1.50 -c Teledata 20.1.1.54 is added to trusted host list.  admin@k2&gt; trustedhost -L Third party trusted hosts.       Trusted Host             CCS Host Name             Comment ----- ----- ----- 50.1.1.48                50.1.1.50                 Teledata</pre></div>

<sup>1</sup> Note, if the trusted host step is not done, authentication challenges to incoming SIP messages (such as INVITEs and BYEs) will be issued but not responded to. This may cause call setup to fail, active calls to be disconnected after timeout periods, and/or SIP protocol errors.

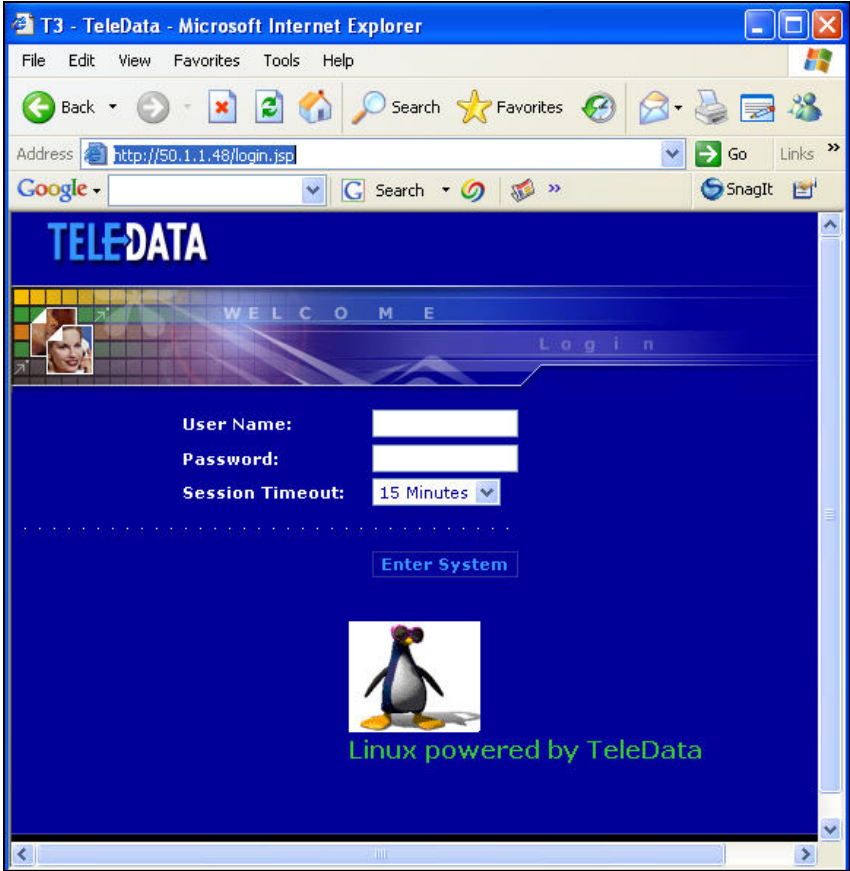
<sup>2</sup> For completeness, the **-d** argument allows the trust relationship to be deleted. For, example,


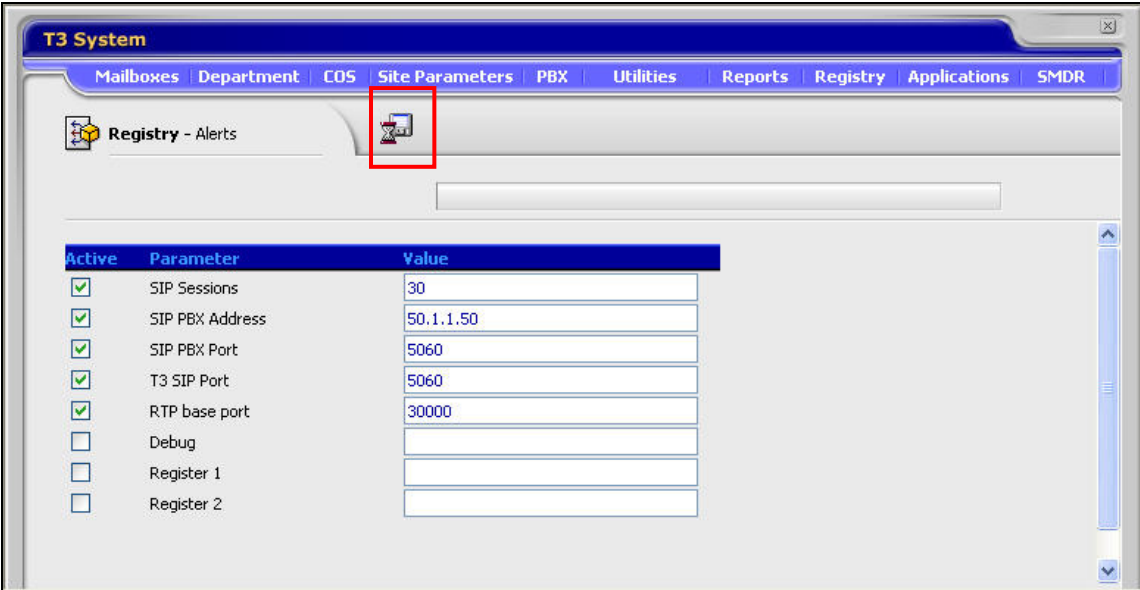
```
trustedhost -d 50.1.1.48 -n 50.1.1.50
```

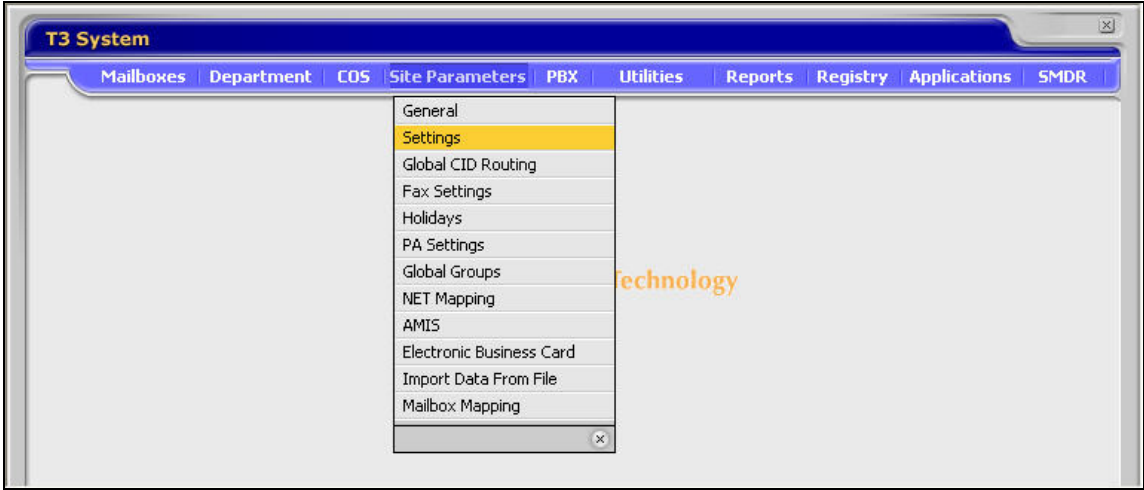
removes the trust relationship added above.

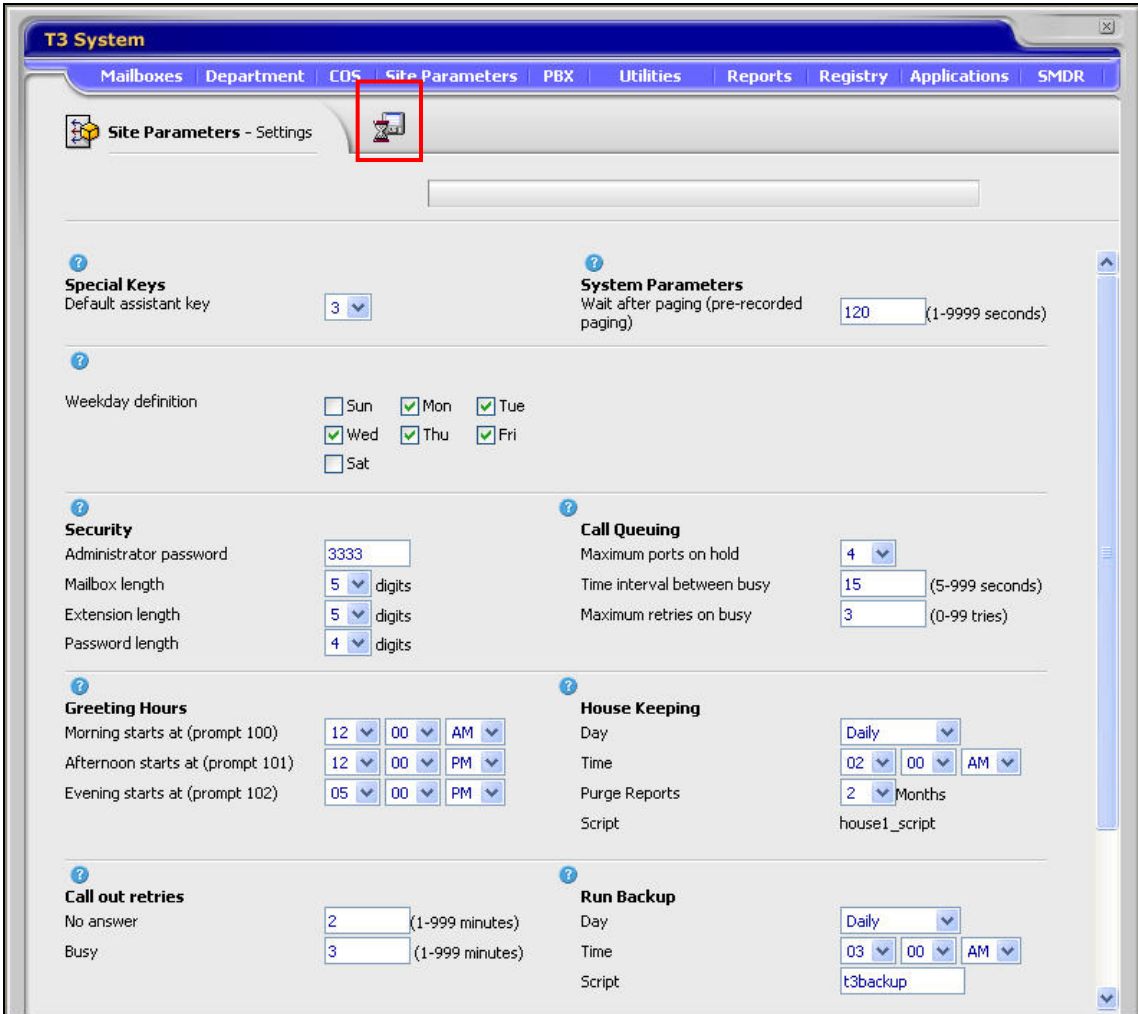
### 3.3. Configure the TeleData Technology T3 Platform

This section describes the configuration of the T3 Platform to use SIP trunking. In addition, this section will cover the creation of user mailboxes in order to use the voicemail features. No additional configuration is necessary to use the automated attendant feature. The default configuration of the automated attendant was sufficient for the compliance test providing the ability for a user to access voicemail, transfer to another extension and verify correct DTMF detection. For information on how to further customize the automated attendant, voicemail or any other features of the T3 Platform, please refer to [7].


Step	Description
1.	<p>From a web browser, enter the IP address of the T3 Platform in the <b>Address</b> field. Enter an authorized <b>User Name</b> and <b>Password</b> on the login page. Select <b>Enter System</b> to continue.</p> 

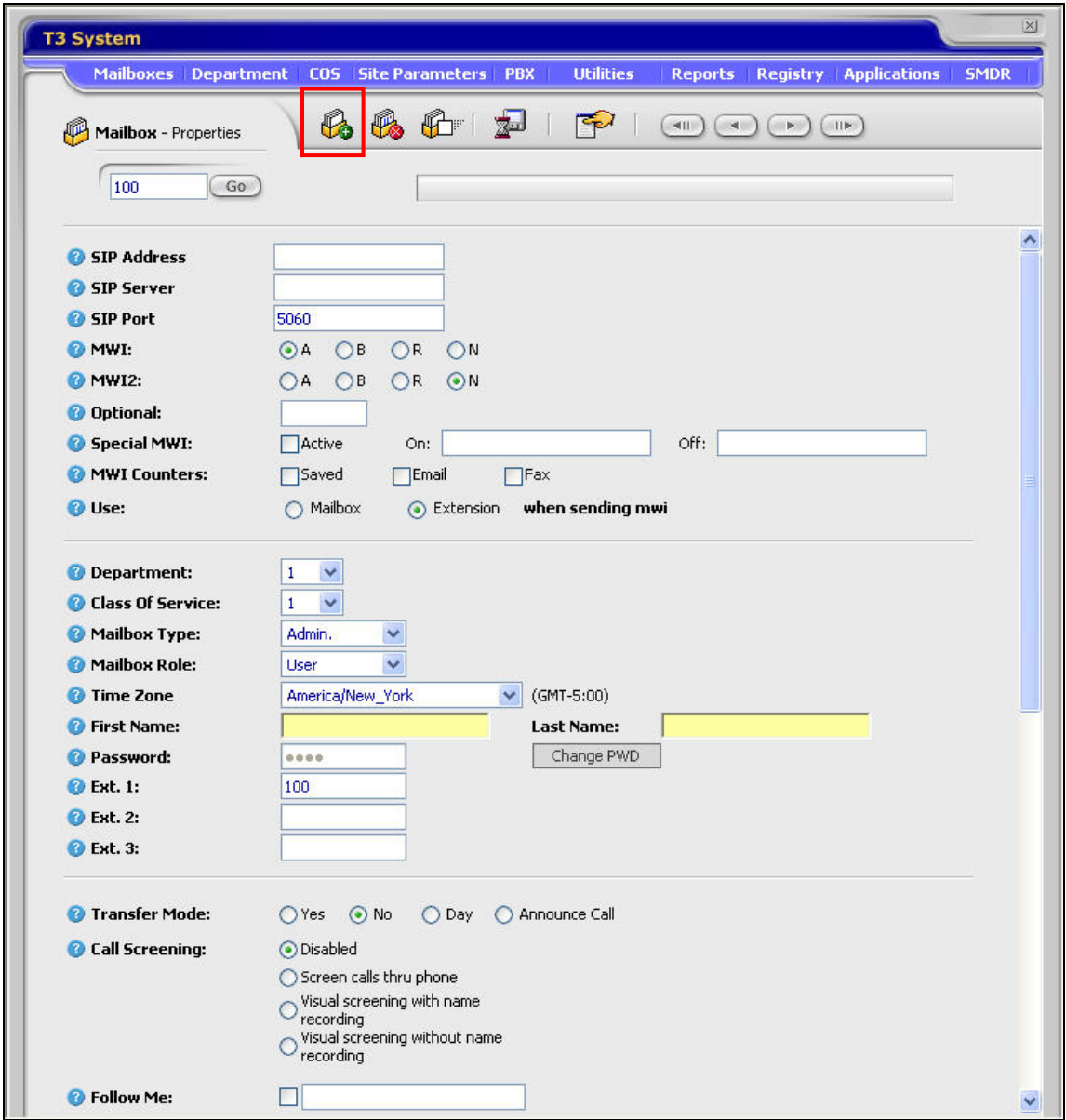
Step	Description
2.	<p>To set SIP parameters, navigate to <b>Registry</b> → <b>VoIP</b> from the <b>T3 System</b> main window.</p> <div></div>
3.	<p>In the <b>Registry</b> window that appears, enter the IP address of the Avaya SES server in the <b>SIP PBX Address</b> field. Enter port <b>5060</b> in the <b>SIP PBX Port</b> field. Verify that the checkbox next to each of these fields is selected. Select the <b>Save</b> icon highlighted below to save the changes.</p> <div></div>

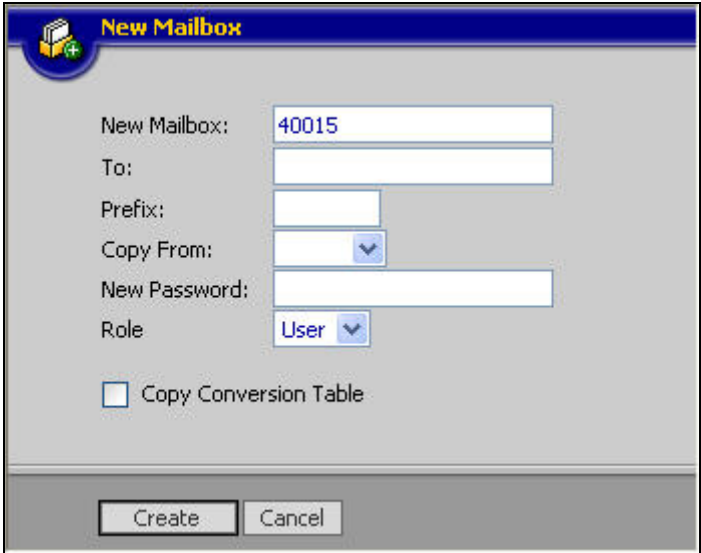
Step	Description
4.	<p data-bbox="298 233 1252 268">From the <b>T3 System</b> main page, navigate to <b>Site Parameters</b> → <b>Settings</b>.</p>  <p>The screenshot shows the 'T3 System' web application interface. At the top, there is a blue header bar with the title 'T3 System' and a close button. Below the header is a navigation menu with tabs: 'Mailboxes', 'Department', 'COS', 'Site Parameters', 'PBX', 'Utilities', 'Reports', 'Registry', 'Applications', and 'SMDR'. The 'Site Parameters' tab is selected. A dropdown menu is open under 'Site Parameters', listing the following options: 'General', 'Settings' (highlighted in yellow), 'Global CID Routing', 'Fax Settings', 'Holidays', 'PA Settings', 'Global Groups', 'NET Mapping', 'AMIS', 'Electronic Business Card', 'Import Data From File', and 'Mailbox Mapping'. The background of the page is light gray with a faint 'Technology' watermark.</p>

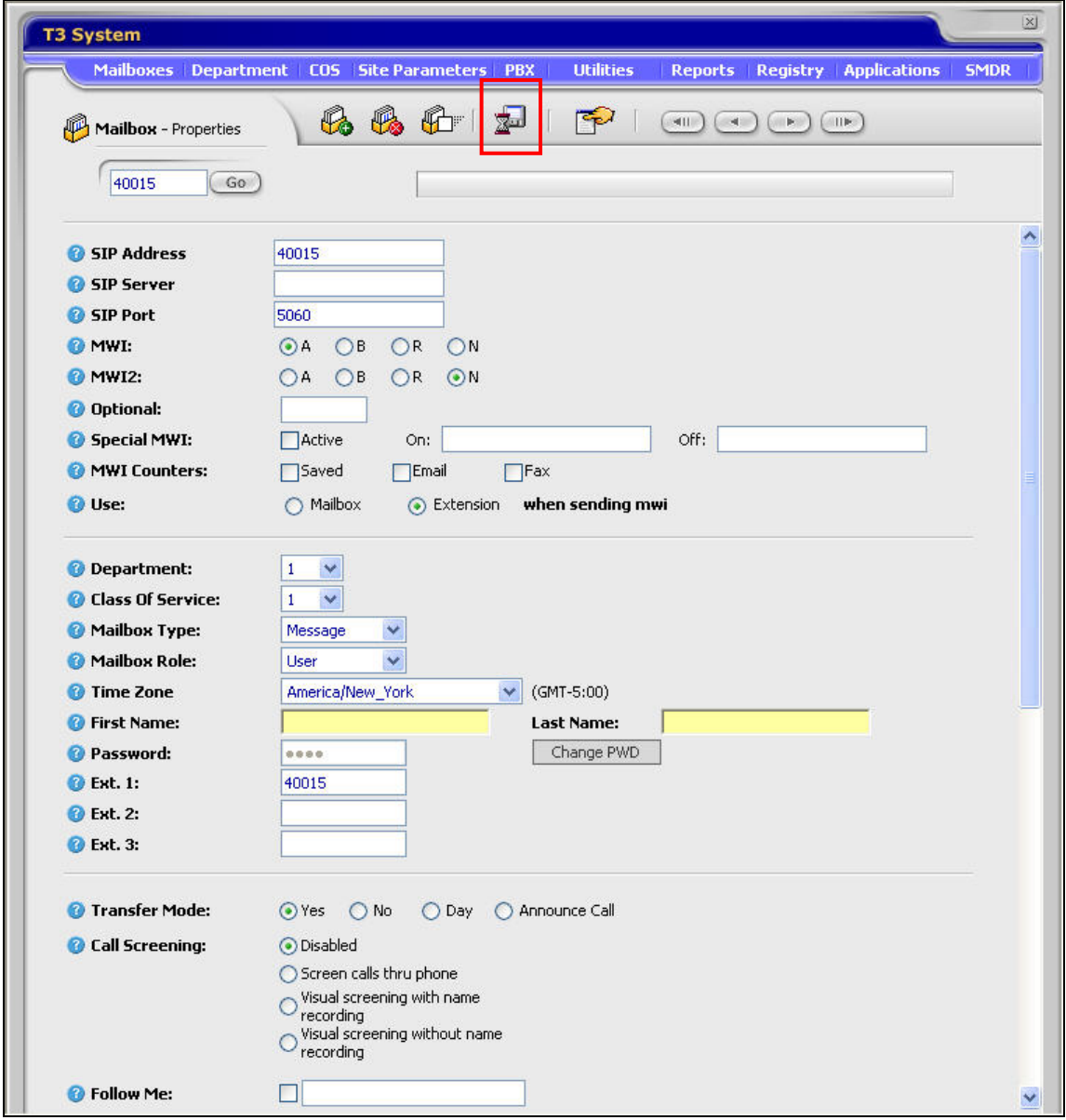
Step	Description
5.	<p>Under <b>Security</b>, set the <b>Mailbox length</b> and <b>Extension length</b> to the same length used for extensions in the Avaya Communication Manager dial plan. Use the default values for all other fields. Select the <b>Save</b> icon highlighted below to save the changes.</p>  <p>The screenshot shows the 'T3 System' interface with the 'Site Parameters' tab selected. The 'Security' section is expanded, showing fields for 'Mailbox length' (5 digits) and 'Extension length' (5 digits). The 'Save' icon (a floppy disk) is highlighted with a red box in the top navigation bar.</p>



Step	Description
6.	<p>To edit mailbox properties, navigate to <b>Mailboxes</b> → <b>Properties</b> from the <b>T3 System</b> main window.</p>  <p>The screenshot shows the T3 System application window. The title bar reads 'T3 System'. Below the title bar is a menu bar with the following items: Mailboxes, Department, COS, Site Parameters, PBX, Utilities, Reports, Registry, Applications, and SMDR. The 'Mailboxes' menu is open, displaying a list of options: Properties (highlighted in yellow), CID Routing, Conversion Table, Message Notification, Script, Email Settings, Email Accounts, Email reply Settings, Forwarding Options, Groups, Cascading Messages, PIN, Viometrics, and Fax -&gt;. The main content area of the window displays the TeleData Technology logo, which consists of a stylized blue wave graphic above the text 'TeleData Technology' in orange.</p>

Step	Description
7.	<p>The <b>Mailbox - Properties</b> screen for default mailbox 100 appears. To create a new mailbox, select the <b>New Mailbox</b> icon from the row of icons at the top of the window. The <b>New Mailbox</b> icon is highlighted in the example below.</p> 

Step	Description
8.	<p>A pop-up window appears. Enter the desired number for the new mailbox in the <b>New Mailbox</b> field. In the compliance test, the mailbox was given the same number as the user's extension on Avaya Communication Manager.</p> <p>Select <b>Create</b> to continue.</p> 

Step	Description
9.	<p>The <b>Mailbox – Properties</b> window is updated with the properties of the newly created mailbox 40015. In the <b>SIP Address</b> field, enter the user's extension on Avaya Communication Manager. For the compliance test, the default values were used for all other fields as shown below. The <b>Ext. 1</b> field is automatically populated with the mailbox number, which is the same as the user's extension. The mailbox could be further customized by making changes to this form including a first and last name.</p> <p>After making changes, save the properties by selecting the <b>Save</b> icon from the row of icons at the top of the window. The <b>Save</b> icon is highlighted in the example below.</p> 

Step	Description
10.	Repeat Steps 6 -9 for each station on Avaya Communication Manager that requires a voice mailbox.

## 4. Configure the Solution to Use SIP Endpoints (Approach 2)

This section describes the necessary configuration on Avaya Communication Manager, Avaya SES and the TeleData Technology T3 Platform to use a set of SIP endpoints as a means to establish the necessary SIP signaling connection between Avaya SES and the T3 Platform. In this approach, the T3 Platform emulates a set of SIP endpoints, one for each simultaneous call to be supported. The T3 Platform is not defined in Avaya SES as a trusted host and each endpoint is registered with Avaya SES. Avaya SES routes calls to the T3 Platform as it would any other endpoint. This in turn affects the way the voice mail hunt group and routing is defined on Avaya Communication Manager.

For this approach, much of the configuration is the same as Approach 1. Steps that are the same refer to those steps in Section 3. Any necessary changes to the preceding configuration are outlined below.

### 4.1. 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 translations** command to make the changes permanent.

Step	Description
1.-10.	Same as in Approach 1.
11.-12.	Omit these steps from Approach 1. These steps are not needed because calls are not routed via AAR in Approach 2.

Step	Description
13.	<p>In this approach, a SIP station must be added to Avaya Communication Manager for each station that will be emulated by the T3 Platform. These stations will be part of the voicemail hunt group that will answer calls routed to the T3 Platform. All SIP stations are added as Outboard SIP Proxy (OPS) stations on Avaya Communication Manager. Thus, the T3 Platform stations are configured as any other SIP endpoint. For more details on configuring a SIP endpoints see the example in [6].</p> <p>Use the <b>display system-parameters customer-options</b> command to verify Avaya Communication Manager has sufficient OPS capacity available to add the OPS stations needed for the T3 Platform. The compliance test used four OPS stations for this purpose. If there is insufficient capacity, contact an authorized Avaya sales representative or business partner to make the appropriate changes.</p> <pre> display system-parameters customer-options                                Page 1 of 10                                 OPTIONAL FEATURES  G3 Version: V13 Location: 1                                RFA System ID (SID): 1 Platform: 13                               RFA Module ID (MID): 1                                  USED                                 Platform Maximum Ports: 900 121                                 Maximum Stations: 450 41                                 Maximum XMOBILE Stations: 0 0 Maximum Off-PBX Telephones - EC500: 50 0 Maximum Off-PBX Telephones - OPS: 50 23 Maximum Off-PBX Telephones - SCCAN: 0 0 </pre>
14.	<p>To add a station, use the <b>add station <i>n</i></b> command where <i>n</i> is an unused extension number. Use the default value of <b>6408D+</b> for the <b>Type</b> field. Enter an <b>X</b> in the <b>Port</b> field, this indicates a station is being added without identifying a physical port for it to use. Enter a descriptive name in the <b>Name</b> field. Use default values for all other fields.</p> <pre> add station 40101  Page 1 of 4                                 STATION  Extension: 40101                                Lock Messages? n            BCC: 0 Type: 6408D+                                Security Code:                TN: 1 Port: X                                Coverage Path 1:              COR: 1 Name: SIP VM1                            Coverage Path 2:              COS: 1                                 Hunt-to Station:  STATION OPTIONS Loss Group: 2                                Personalized Ringing Pattern: 1 Data Module? n                                Message Lamp Ext: 40101 Speakerphone: 2-way                            Mute Button Enabled? y Display Language: english                                  Media Complex Ext:                                 IP SoftPhone? n </pre>

Step	Description
15.	<p>On Page 3, under <b>BUTTON ASSIGNMENTS</b>, create four call appearances by entering <i>call-appr</i> in the first four entries. In general when connecting Avaya SIP Telephones, SIP stations are created with the number of call appearances equal to one more than the number defined in the telephone 46xxsettings.txt file. This is necessary to support certain transfer and conference scenarios. Even though these stations were not connected to Avaya SIP Telephones, these voicemail stations were configured the same way.</p> <div> <pre> add station 40101                                      STATION                                      Page 3 of 4  SITE DATA   Room:                               Headset? n   Jack:                               Speaker? n   Cable:                             Mounting: d   Floor:                             Cord Length: 0   Building:                           Set Color:  ABBREVIATED DIALING   List1:                               List2:                               List3:  BUTTON ASSIGNMENTS   1: call-appr                         5:   2: call-appr                         6:   3: call-appr                         7:   4: call-appr                         8: </pre> </div>
16.	<p>Map the Avaya Communication Manager extension to the Avaya SES media server extension defined in Section 4.2 Step 13 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</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> Any configuration set using the default values</li> </ul> <div> <pre> add off-pbx-telephone station-mapping                                      STATIONS WITH OFF-PBX TELEPHONE INTEGRATION                                      Page 1 of 2  Station      Application  Dial   Phone Number  Trunk   Configuration Extension    Prefix 40101        OPS                - 40101      1           1 </pre> </div>

Step	Description
17.	<p>On Page 2, set the <b>Call Limit</b> to the number of call appearances set on the station form in Step 15. Verify that the <b>Mapping Mode</b> is set to both.</p> <div> <pre> add off-pbx-telephone station-mapping                                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION                                 Page 2 of 2  Station      Call      Mapping      Calls      Bridged Extension    Limit      Mode        Allowed    Calls 40101        4          both        all        both </pre> </div>
18.	<p>Repeat Steps 14 -17 for each voicemail extension to be provided on the T3 Platform. The compliance test used four extensions: 40101, 40102, 40103, and 40104.</p>
19.	<p>Create a hunt group using the <b>add hunt-group <i>n</i></b> command, where <b><i>n</i></b> is the number of an unused hunt group. This hunt group will provide the access number for the T3 Platform. Enter any descriptive name for the <b>Name</b> field. Enter an unused extension for the <b>Group Extension</b> field. Use default values for all other fields.</p> <div> <pre> add hunt-group 3                                 HUNT GROUP                                 Page 1 of 60  Group Number: 2 Group Name: TeleData Endpts Group Extension: 43001 Group Type: ucd-mia TN: 1 COR: 1 Security Code: ISDN/SIP Caller Display:  ACD? n Queue? n Vector? n Coverage Path: Night Service Destination: MM Early Answer? n Local Agent Preference? n </pre> </div>
20.	<p>On Page 2, verify the <b>Message Center</b> field is set to <b>none</b>. Use default values for all other fields.</p> <div> <pre> change hunt-group 3                                 HUNT GROUP                                 Page 2 of 60  LWC Reception: none AUDIX Name:  Message Center: none </pre> </div>



Step	Description
21.	<p>On Page 3, enter each voicemail extension in the <b>Ext</b> column with a corresponding name for each extension in the <b>Name</b> column.</p> <pre> display hunt-group 3                                     Page 3 of 60                                  HUNT GROUP       Group Number: 3      Group Extension: 43001      Group Type: ucd-mia Member Range Allowed: 1 - 1500      Administered Members (min/max): 1 /4                                 Total Administered Members: 4  GROUP MEMBER ASSIGNMENTS   Ext      Name (24 characters)      Ext      Name (24 characters) 1: 40101    SIP VM1                  14: 2: 40102    SIP VM2                  15: 3: 40103    SIP VM3                  16: 4: 40104    SIP VM4                  17: 5:                                     18: </pre>
22.	<p>Create a coverage path that will use the T3 Platform hunt group when calls are busy, sent to coverage or not answered. Use the <b>change coverage path <i>n</i></b> command where <b><i>n</i></b> is the number of an unused coverage path. Set the first point in the coverage path to be hunt group 3 by setting the <b>Point1</b> field to <b>h3</b>.</p> <pre> change coverage path 3                                     Page 1 of 1                                  COVERAGE PATH        Coverage Path Number: 3                                  Hunt after Coverage? n       Next Path Number:      Linkage  COVERAGE CRITERIA    Station/Group Status      Inside Call      Outside Call       Active?                n                n       Busy?                  y                y       Don't Answer?          y                y      Number of Rings: 2       All?                   n                n       DND/SAC/Goto Cover?    y                y       Holiday Coverage?      n                n  COVERAGE POINTS   Terminate to Coverage Pts. with Bridged Appearances? n    Point1: h3      Rng:      Point2:      Point3:   Point4:          Point5:      Point6: </pre>

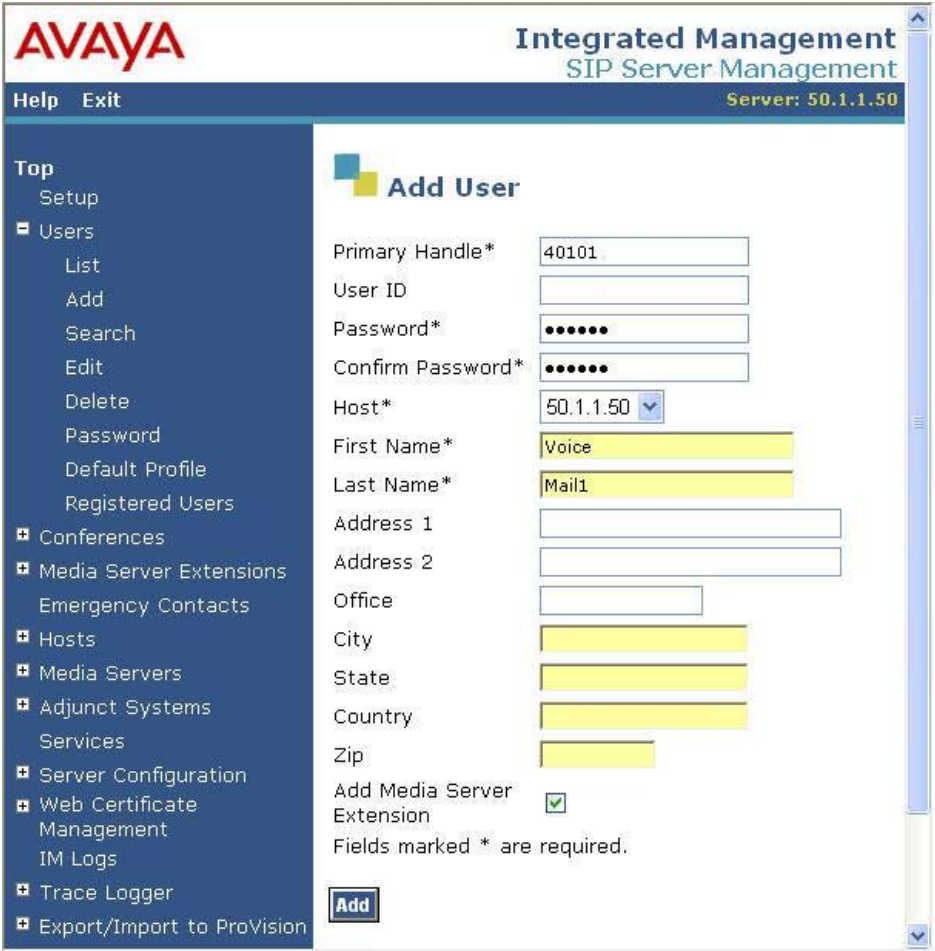
Step	Description
23.	<p>Each station that will use the T3 Platform for voicemail must be configured to use the correct coverage path. To set the coverage path, use the <b>change station <i>n</i></b> command, where <b><i>n</i></b> is the extension number to be modified. Set the <b>Coverage Path 1</b> field to the coverage path defined in Step 22.</p> <pre> change station 40014                                     Page 1 of 4                                  STATION  Extension: 40014                      Lock Messages? n          BCC: 0 Type: 4620                          Security Code: *          TN: 1 Port: S00008                        Coverage Path 1: 3        COR: 1 Name: Tim H323-1                    Coverage Path 2:          COS: 1                                 Hunt-to Station:  STATION OPTIONS     Loss Group: 19                      Personalized Ringing Pattern: 1                                 Message Lamp Ext: 40014     Speakerphone: 2-way                Mute Button Enabled? y     Display Language: english           Expansion Module? n Survivable GK Node Name:     Survivable COR: internal            Media Complex Ext:     Survivable Trunk Dest? y            IP SoftPhone? n                                  Customizable Labels? y </pre>
24.	<p>Lastly, each station that will use the T3 Platform for voicemail must be configured to use <i>sip-adjunct</i> as the <b>MWI Served User Type</b> on Page 2.</p> <pre> change station 40014                                     Page 2 of 4                                  STATION  FEATURE OPTIONS     LWC Reception: spe                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           Restrict Last Appearance? n     Active Station Ringing: single     Conf/Trans on Primary Appearance? n                                 EMU Login Allowed? n     H.320 Conversion? n               Per Station CPN - Send Calling Number?     Service Link Mode: as-needed     Multimedia Mode: enhanced          Audible Message Waiting? n     MWI Served User Type: sip-adjunct  Display Client Redirection? n                                 Select Last Used Appearance? n                                 Coverage After Forwarding? s                                  Direct IP-IP Audio Connections? y     Emergency Location Ext: 40014      Always Use? n          IP Audio Hairpinning? y </pre>


Step	Description
25.	<p>To map a DID number to the T3 Platform hunt group, use the <b>change inc-call-handling-trmt trunk-group <i>n</i></b> command, where <i>n</i> is the trunk group number connecting to the PSTN. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows an incoming 11-digit number being deleted and replaced with the extension number of the T3 Platform hunt group. This allows external callers to reach the T3 Platform to access the automated attendant.</p> <div> <pre>change inc-call-handling-trmt trunk-group 2</pre> <pre> Service/      Called      Called      Del  Insert Feature      Len       Number tie          11    17325551235      11    43001 </pre> </div>

## 4.2. Configure Avaya SES

This section covers the configuration of Avaya SES. In particular, it shows the steps that must be omitted from the previous procedure and the additional steps necessary to create SIP users for each of the voicemail extensions on Avaya Communication Manager.

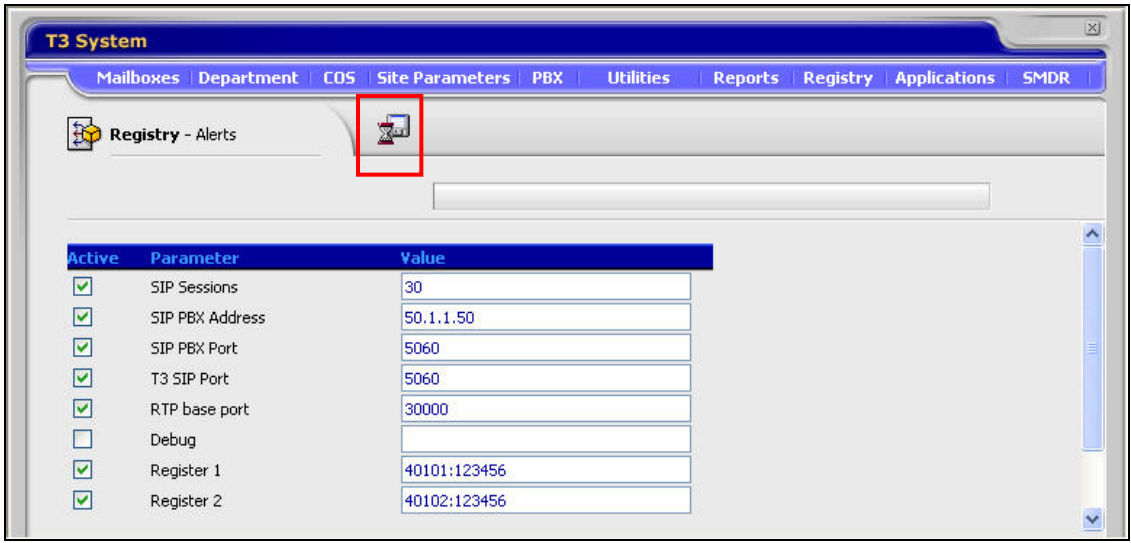
Step	Description
1.– 9.	Same as in Approach 1. Most of this configuration is related to the connection between Avaya SES and Avaya Communication Manager so it is still required. Also, even though the T3 Platform is configured as a set of SIP endpoints, the Media Server Address Map configured in Section 3.2 Steps 7 – 9 is still needed for the proper operation of MWI.
10.–13.	Omit these steps from Approach 1. Host Address Maps and configuring a trusted host are not needed in Approach 2.

Step	Description
14.	<p>A user must be added on Avaya SES for each of the voicemail SIP extensions created on Avaya Communication Manager in Section 4.1 Step 14. From the left pane, navigate to <b>Users</b> → <b>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. Select the <b>Add</b> button to proceed. A confirmation window will appear. Select <b>Continue</b> on this new page to proceed.</p> 

Step	Description
15.	<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 Section 3.2 Step 6.</p> <p>Select the <b>Add</b> button to complete the operation.</p> 
16.	Repeat Steps 14 - 15 for each of the remaining voicemail extensions added to Avaya Communication Manager.

### 4.3. Configure T3 Platform

This section describes the configuration of the T3 Platform to emulate a set of SIP endpoints and register each endpoint with Avaya SES.

Step	Description
1.-2.	Same as in Approach 1.
3.	<p>In order for the T3 Platform to register as an endpoint with Avaya SES, it must be configured with the extension to use and the password. Navigate to <b>Registry → VoIP</b> as shown in Step 2.</p> <p>In the <b>Registry</b> window that appears, enter the IP address of the Avaya SES in the <b>SIP PBX Address</b> field. Enter port <b>5060</b> in the <b>SIP PBX Port</b> field. In each of the <b>Register</b> fields, enter a single voicemail extension and password in the form <b>extension:password</b>. The extension and password must match the values configured on Avaya SES in Section 4.2 Step 14 - 15. The number of <b>Register</b> fields shown is controlled by the license file on the T3 Platform. The example below only shows two of the four extensions used in the compliance test. This is because this screen shot was captured before the license was increased to support four extensions.</p> <p>Verify that the checkbox next to each of these fields is selected. Select the <b>Save</b> icon highlighted below to save the changes.</p> 
4.-10.	Same as in Approach 1.

## 5. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability between the TeleData Technology T3 Platform, Avaya Communication Manager and Avaya SIP Enablement Services (SES) via the IP network using SIP. This section covers the general test approach and the test results.

### 5.1. General Test Approach

Using the configuration described in **Figure 1**, the T3 Platform was configured to provide voicemail to stations on Avaya Communication Manager. Each station was configured to cover to a hunt group that provided the access number for the T3 Platform. The hunt group routed all calls it received to the SIP connection of the T3 Platform. In the first approach, these calls were routed via AAR to the SIP trunk providing access to the T3 Platform. In the second approach, these calls were routed to SIP extensions associated with the T3 Platform.

In addition, a DID number was mapped to the hunt group extension so that the T3 Platform could be accessed from an external number. If the hunt group extension was called from an internal station, the T3 Platform prompted the user for their password and then played the subscriber menu, which allowed a user to retrieve his/her voicemail. If the hunt group DID number was dialed from an external number, the caller is connected to the T3 Platform automated attendant. The automated attendant allowed the caller to transfer to another extension, to hold for the operator, or access the caller's voicemail if the caller is a voicemail subscriber.

### 5.2. Test Results

The following features and functionality were successfully verified during the interoperability compliance test:

- Leaving and retrieving voice mail messages from an internal extension.
- Leaving and retrieving voice mail messages from an external number.
- Proper operation of message waiting indicators (MWI).
- Calls to the automated attendant from an external number.
- Calls to the automated attendant and then transferring to another extension.
- Calls to the automated attendant and voicemail using G.711 and G.729B codecs.
- Calls to the automated attendant and voicemail from SIP, H.323, and digital endpoints in the Avaya enterprise network.
- Proper recognition of DTMF transmissions.
- Proper feature operation with transfer and conference.
- Proper system recovery after network outages or system restarts.
- Proper operation during automated load test.

## 6. Verification Steps

This section provides verification steps that may be performed to verify that the solution described in these Application Notes is configured properly.



- Verify the SIP trunk group is in-service. To do this, use the **status trunk *n*** command, where ***n*** is the number of the trunk group to be verified.
- Verify the SIP signaling group is in-service. To do this, use the **status signaling-group *n*** command, where ***n*** is the number of the signaling group to be verified.
- Verify a call can be placed to the T3 Platform by dialing the hunt group extension.
- Verify a call can be placed to an internal extension and the call covers to voicemail. Leave a message. Verify that the MWI on the destination extension is activated.
- Verify the message can be retrieved for this extension from voicemail by dialing the hunt group extension. Verify that the MWI on the user's extension is deactivated.
- Verify a call from an external number to the hunt group DID number is answered by the automated attendant and can be transferred to a user's extension.

## 7. Support

Technical support for the T3 Platform can be obtained from TeleData Technology. See the website a [www.myt3.com](http://www.myt3.com) for contact information.

## 8. Conclusion

The T3 Platform has successfully passed interoperability compliance testing with Avaya Communication Manager and Avaya SIP Enablement Services (SES).

## 9. Additional References

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

- [1] *Feature Description and Implementation For Avaya Communication Manager*, Issue 4.0, February 2006, Document Number 555-245-205.
- [2] *Administrator Guide for Avaya Communication Manager*, Issue 2.1, May 2006, Document Number 03-300509.
- [3] *Installing and Administering SIP Enablement Services R3.1*, Issue 1.5, February 2006, Document Number 03-600768.
- [4] *SIP Support in Release 3.1 of Avaya Communication Manager Running on the Avaya S8300, S8500, S8500B, S8700, and S8710 Media Server*, Issue 6, February 2006, Document Number 555-245-206.
- [5] *4600 Series IP Telephone Release 2.4 LAN Administrator Guide*, Issue 2.3, April 2006, Document Number 555-233-507.
- [6] *Configuring SIP IP Telephony Using Avaya SIP Enablement Services, Avaya Communication Manager and Snom 190/220/360 SIP Telephones*, Issue 1.0, January, 2006.

The following T3 product documentation is available from TeleData Technology. Visit <http://www.myt3.com> for company and product information.

- [7] *T3 System Manual*, Version 10.4.1, 2006.
- [8] *TeleData User Guide*, December 2003.

## APPENDIX A: Specifying Pattern Strings in Address Maps

The syntax for the pattern matching used within the 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 the 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
```

---

**©2006 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).