Avaya Solution & Interoperability Test Lab

Configuring Secure SIP Connectivity Utilizing Transport Layer Security (TLS) Between Avaya Communication Manager and the Avaya Meeting Exchange S6200 Conferencing Server Via Avaya SIP Enablement Services - Issue 1.0

Abstract

These Application Notes present the procedures for configuring secure SIP connectivity between Avaya Communication Manager and the Avaya Meeting Exchange S6200 Conferencing Server via Avaya SIP Enablement Services. Secure SIP connectivity is enabled by utilizing Transport Layer Security (TLS) authentication and encryption standards, thus providing customers a secure, standards based solution. This configuration leverages the flexibility offered by Avaya Communication Manager and the scalability provided by Avaya SIP Enablement Services to support a rich set of conferencing options available from Avaya Meeting Exchange.

1. Introduction

These Application Notes present the procedures for configuring secure SIP connectivity between Avaya Communication Manager and the Avaya Meeting Exchange S6200 Conferencing Server via Avaya SIP Enablement Services. Secure SIP connectivity is enabled by utilizing Transport Layer Security (TLS) authentication and encryption standards, thus providing customers a secure, standards based solution. This configuration leverages the flexibility offered by Avaya Communication Manager and the scalability provided by Avaya SIP Enablement Services to support a rich set of conferencing options available from Avaya Meeting Exchange.

The following conferencing features have been verified:

- Dial-In Conferencing:
    - DNIS Direct call function, where conference participants enter a conference as moderator without entering a participant access code (passcode).
    - Scan call function, where conference participants enter a conference with a valid passcode.
- Dial-Out Conferencing from Avaya Meeting Exchange:
    - Blast dial
        - Auto, where a conference participant enters a conference via a DNIS direct call function and automatically invokes a Blast dial to a pre-provisioned dial list of one or more participants.
        - Manual, where a conference participant is already in a conference as a moderator and invokes a Blast dial to a pre-provisioned dial list of one or more participants.
    - Originator Dial-Out, where a conference participant is already in a conference as a moderator and invokes a Dial-Out to a single participant
    - Operator Fast Dial, where an operator can Dial-Out to a pre-provisioned dial list of one or more participants.
- Operator Dial-Out to set up an Audio Path.
- Operator Dial-In to set up an Audio Path.
- Dial-Out to an FDAPI channel for audio recording.
- Line Transfer initiated from Avaya Bridge Talk.
- Conference Transfer initiated from Avaya Bridge Talk.

The following codecs were verified:

- G711MU
- G.711A

The following SIP feature testing was verified:

- Call Hold/Resume, invoked from an endpoint associated with Avaya Communication Manager participating in an active conference call.
- Call Transfer, initiated from an endpoint associated with Avaya Communication Manager participating in an active conference call and transferred to another endpoint associated with Avaya Communication Manager.

These Application Notes provide the administrative steps for configuring:

- Connectivity between Avaya Communication Manager and Avaya SIP Enablement Services via secure SIP trunking utilizing TLS (see **Figure 1**).
- Connectivity between Avaya SIP Enablement Services and Avaya Meeting Exchange via secure SIP trunking utilizing TLS (see **Figure 1**).

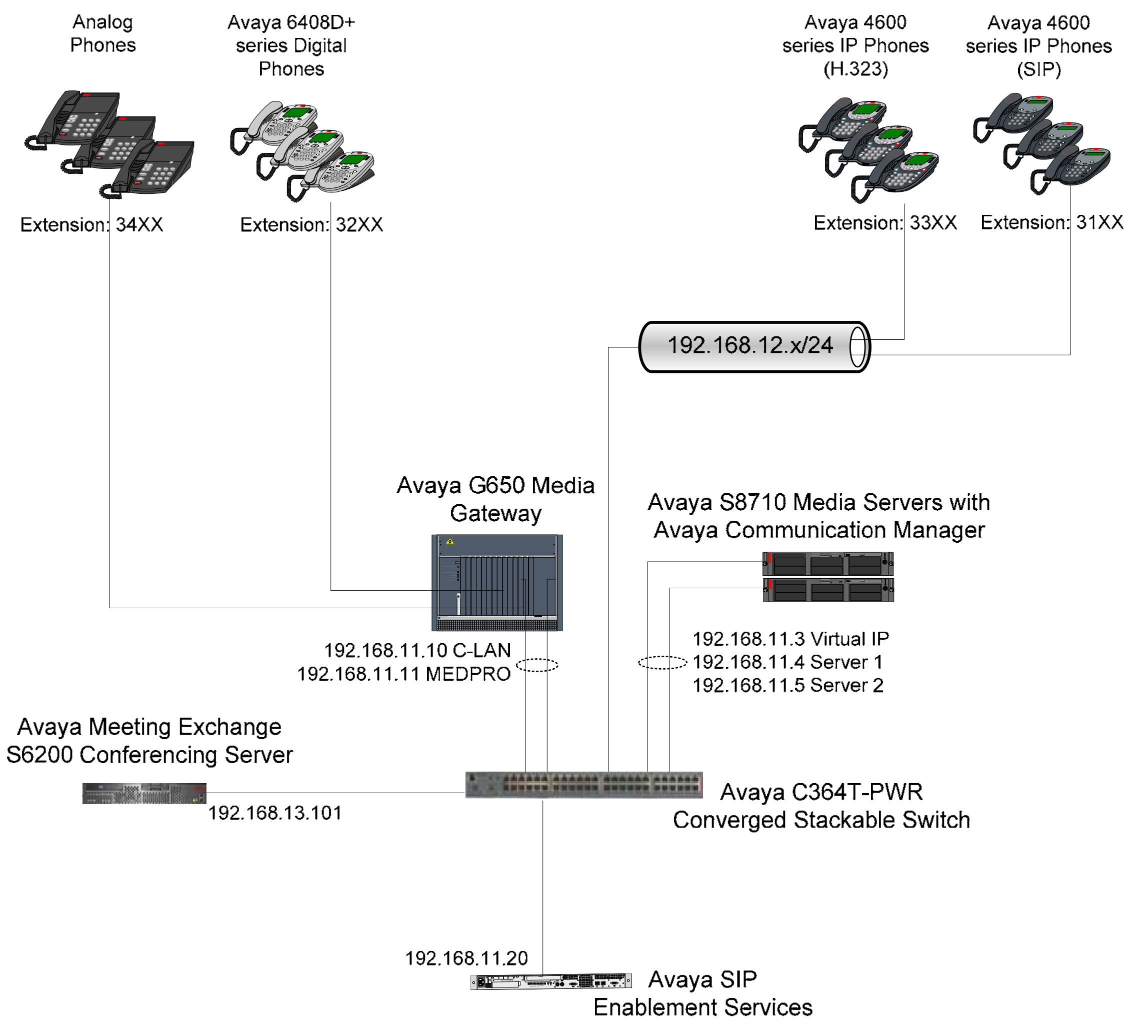


Figure 1: Network Configuration

1.1. Dial-Out from Avaya Meeting Exchange

The following figure shows how secure SIP trunking between Avaya SIP Enablement Services and Avaya Communication Manager is utilized to enable Dial-Out from Avaya Meeting Exchange to Avaya Communication Manager **Via** Avaya SIP Enablement Services. Since this configuration is configured for TLS, the SIP messages below (captured from a log file on Avaya SIP Enablement Services) are intended to illustrate the call flow.

- A SIP **INVITE** Message is sent **From** Avaya Meeting Exchange **To** Avaya SIP Enablement Services utilizing TLS (see red dashed line in **Figure 2**).
- The SIP **INVITE** Message is then sent to Avaya Communication Manager **Via** Avaya SIP Enablement Services utilizing TLS (see blue dotted line in **Figure 2**).

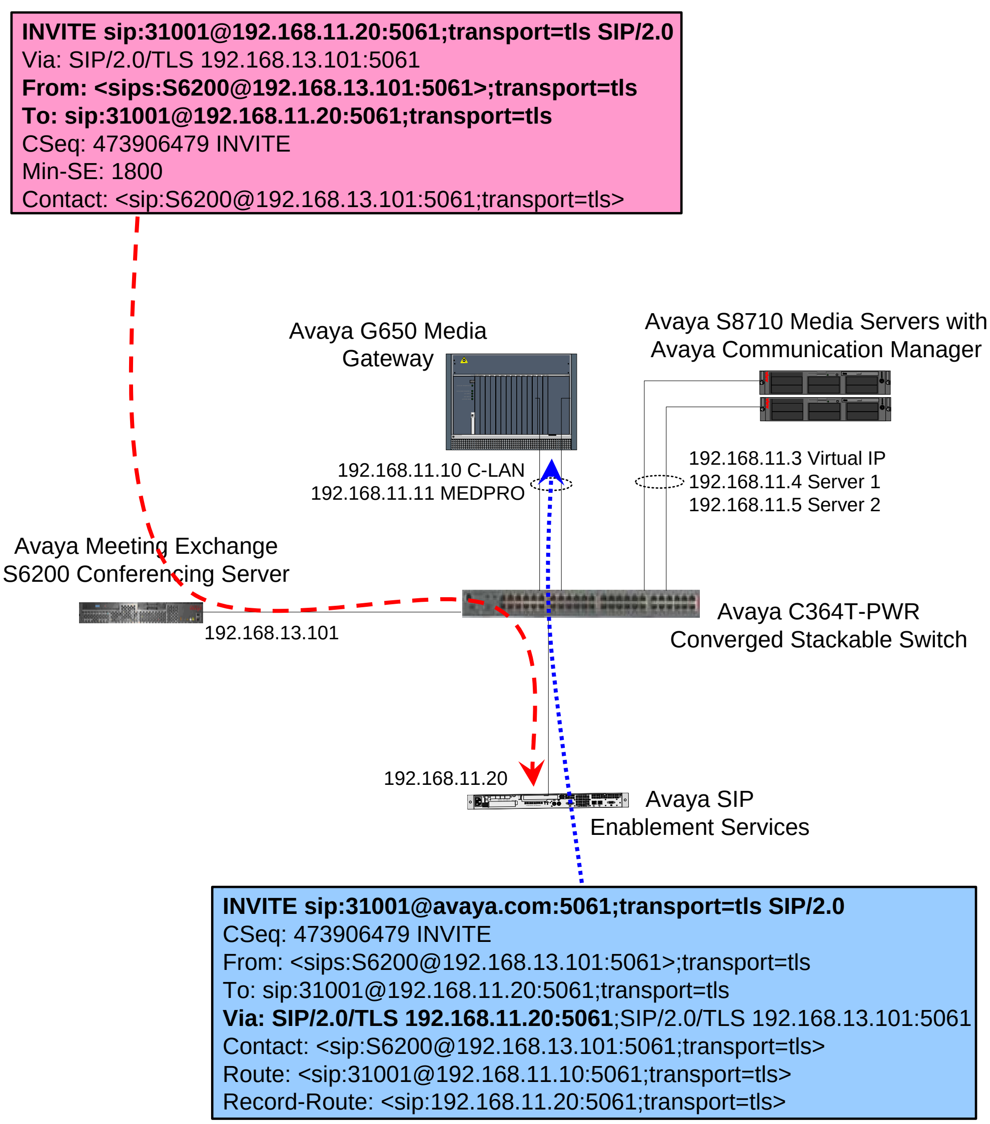


Figure 2: Dial-Out from Avaya Meeting Exchange

1.2. Dial-In to Avaya Meeting Exchange

The following figure shows how secure SIP trunking between Avaya SIP Enablement Services and Avaya Meeting Exchange is utilized to enable Dial-In to Avaya Meeting Exchange from Avaya Communication Manager **Via** Avaya SIP Enablement Services. Since this configuration is configured for TLS, the SIP messages below (captured from a log file on Avaya SIP Enablement Services) are intended to illustrate the call flow.

- A SIP **INVITE** Message is sent **From** a SIP telephone on Avaya Communication Manager **To** Avaya SIP Enablement Services utilizing TLS (see red dashed line in **Figure 3**).
- The SIP **INVITE** Message is then sent to Avaya Meeting Exchange **Via** Avaya SIP Enablement Services utilizing TLS (see blue dotted line in **Figure 3**).

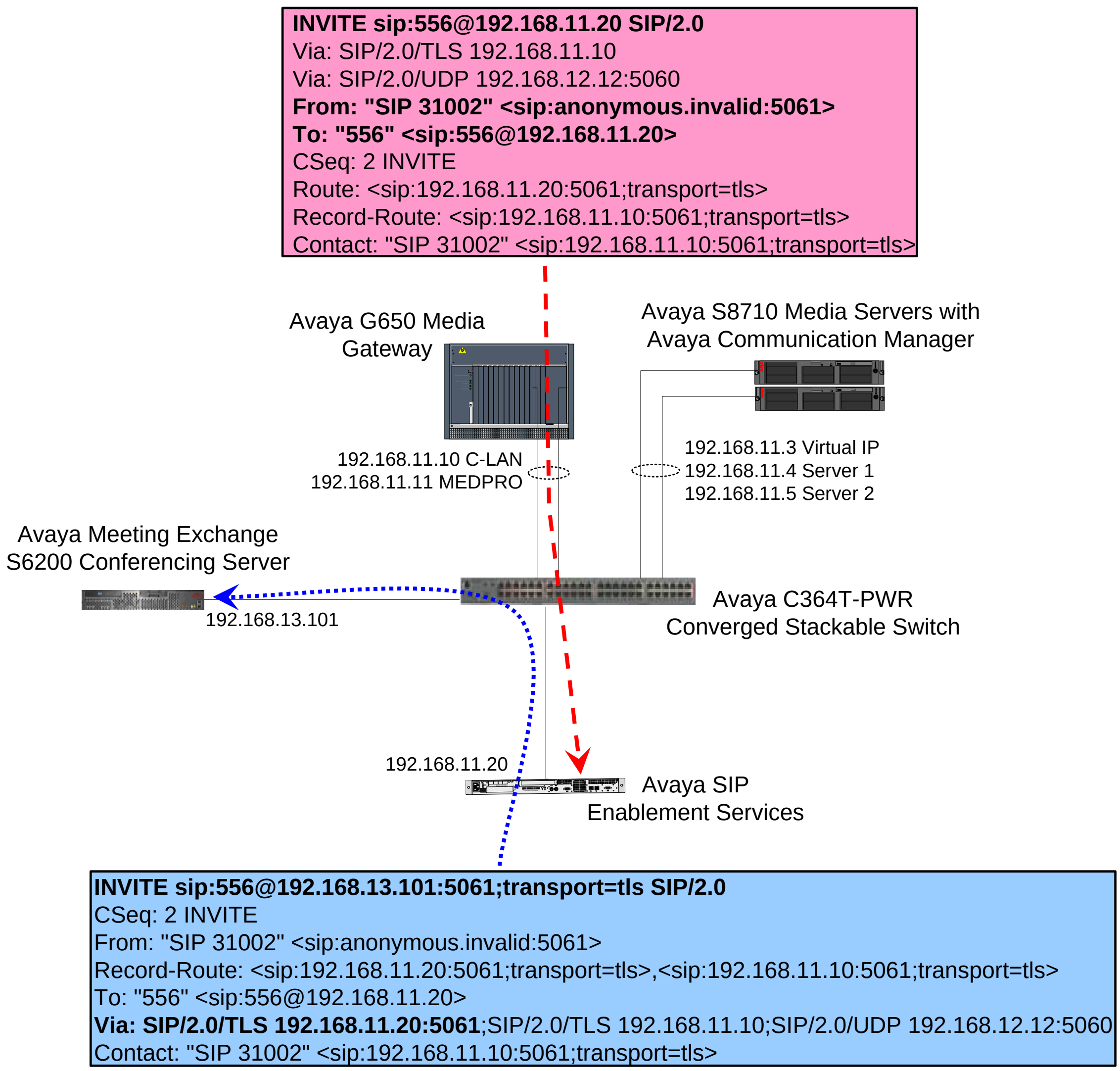


Figure 3: Dial-In to Avaya Meeting Exchange

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8710 Media Servers	Avaya Communication Manager 3.1 (R013x.01.0.628.6)
Avaya G650 Media Gateway • Avaya TN2312BP (IPSI) • Avaya TN799DP (C-LAN) • Avaya TN2302AP (MEDPRO)	 HW12 FW031 HW01 FW017 HW20 FW112
Avaya Meeting Exchange S6200 Conferencing Server • Software version • IPCB build version	 40102h mx7_1.3.00-84
Avaya SIP Enablement Services	SES-3.1.1.0-114.0
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Avaya 4620 IP Telephones	2.3 (H.323)
Avaya 4602 IP Telephones	2.2 (SIP)
Avaya 6408D+ Digital Telephones	--
Analog Telephones	--

Table 1: Hardware and Software Versions

3. Avaya Communication Manager Configuration

This section describes the steps for configuring Avaya Communication Manager to interoperate with Avaya SIP Enablement Services via secure SIP trunking utilizing TLS.

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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.1</td><td>Verify licensing.

Issue the command “display system-parameters customer-options” and proceed to Page 2. Verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed.

Note: Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. For these Application Notes, Avaya Meeting Exchange is treated as an external SIP endpoint. Thus, a call from a SIP telephone to Avaya Meeting Exchange will use two SIP trunks. A call between a non-SIP telephone and Avaya Meeting Exchange will use only one trunk. 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.
<pre>
display system-parameters customer-options   Page   2 of   10

                                OPTIONAL FEATURES

IP PORT CAPACITIES   USED
                     Maximum Administered H.323 Trunks: 1000 0
           Maximum Concurrently Registered IP Stations: 100   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
                       Maximum Administered SIP Trunks: 1000 0

   Maximum Number of DS1 Boards with Echo Cancellation: 0   0
                             Maximum TN2501 VAL Boards: 1   0
                     Maximum G250/G350/G700 VAL Sources: 0   0
           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: 0   0
</pre></td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.2</td><td>Proceed to Page 3 on the system-parameters customer-options form and verify that the system is licensed to utilize Automatic Alternate Routing (AAR) without Feature Access Code (FAC).

Note: AAR without FAC allows direct access to the AAR digit analysis table (see Step 3.9) upon matching a Dialed String in the dial plan analysis table (see Step 3.8).

<pre>
display system-parameters customer-options   Page   3 of   10

                                OPTIONAL FEATURES

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

        (NOTE: You must logoff & login to effect the permission changes.)
</pre></td></tr>
</table>

Step	Description
3.3	Configure an IP codec set. Issue the command “**change ip-codec-set <n>**”, where **n** is the number of an available codec set. Configure an **Audio Codec** that is supported on Avaya Meeting Exchange. For these Application Notes, **G.711MU** is selected.

```
change ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
 4:
 5:
 6:
 7:
```

Step	Description
3.4	Configure an IP network region. Issue the command "**change ip-network-region <n>**", where **n** is the number of an available IP network region and administer settings as per below. • Enter the number of the IP codec set provisioned in **Step 3.3** in the **Codec Set** field. • Configure the **Authoritative Domain** to match the configuration for the **System Properties** on Avaya SIP Enablement Services (see **Step 5.3**).

```
change ip-network-region 1                                      Page   1 of   19

                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 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
```

Step	Description
3.5	Configure IP node names. Issue the command "**change node-names ip**" and administer settings as per below. • Add a node **Name** and **IP Address** for Avaya SIP Enablement Services (**SES**). • Verify that node names and IP addresses are configured for the **C-LAN** and **MEDPRO** boards.

```
change node-names ip                                              Page   1 of   1

                                  IP NODE NAMES
    Name              IP Address
CLAN-1A02           192.168.11 .10
MEDPRO-1A03         192.168.11 .11
SES                 192.168.11 .20
```

Step	Description
3.6	Configure a SIP signaling group. Issue the command "**add signaling-group <n>**", where **n** is the number of an unallocated signaling group and administer settings as per below. • To enable secure SIP connectivity utilizing TLS, configure the following: o Set the **Group Type** to **sip**. o Set the **Transport Method** to **tls**. o Set the **Far-end Listen Port** to **5061**. o Leave the **Near-end Listen Port** at the default value (**5061**). • Enter the IP node name of the C-LAN displayed in **Step 3.5** in the **Near-end Node Name** field. • Enter the IP node name of Avaya SIP Enablement Services provisioned in **Step 3.5** in the **Far-end Node Name** field. • Enter the number of the IP network region provisioned in **Step 3.4** in the **Far-end Network Region** field. • Set the **Direct IP-IP Audio Connections** field to **y** to enable direct IP-to-IP audio connectivity for endpoints utilizing this signaling group. ***Note:*** *To enable direct IP-to-IP audio connectivity, the following must be administered:* • *[**Not Shown**] Direct IP-to-IP audio connectivity must be enabled at the system-level on Page 16 of the **system-parameters features** form by setting the parameter **Direct IP-IP Audio Connections** to **y**.* • *[**Not Shown**] Direct IP-to-IP audio connectivity must be enabled on the **station** form by setting the **Direct IP-IP Audio Connections** field to **y**.*

```
add signaling-group 1                                          Page   1 of   1

                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
                        Transport Method: tls






   Near-end Node Name: CLAN-1A02             Far-end Node Name: SES
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
       Far-end Domain:

                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
                                                        IP Audio Hairpinning? n
 Session Establishment Timer(min): 120
```

Step	Description
3.7	Configure a SIP trunk group. Issue the command "**add trunk-group <n>**", where **n** is the number of an unallocated trunk group and administer settings as per below. • Set the **Group Type** to **sip**, which is consistent with the signaling group provisioned in **Step 3.6**. • Set the Trunk Access Code (**TAC**) to a number that is consistent with the existing dial plan (see **Step 3.8**). • Set the **Service Type** to **tie**. • Enter the number of the signaling group provisioned in **Step 3.6** in the **Signaling Group** field. • Specify the **Number of Members** supported by this SIP trunk group. As mentioned in **Step 3.1**, each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. For these Application Notes, Avaya Meeting Exchange is treated as an external SIP endpoint. Thus, a call from a SIP telephone to Avaya Meeting Exchange will use two SIP trunks. A call between a non-SIP telephone and Avaya Meeting Exchange will use only one SIP trunk.

```
add trunk-group 1                                            Page   1 of   21

                                TRUNK GROUP

Group Number: 1                   Group Type: sip          CDR Reports: y
  Group Name: SES SIP                    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: 50
```

3.1. Call Routing

The following steps show procedures to enable call routing from Avaya Communication Manager to Avaya SIP Enablement Services. For these Application Notes, AAR is utilized (in conjunction with a route pattern) to route calls over the secure SIP trunk group provisioned in Step **3.7**.

Step	Description
3.8	Configure the dial plan analysis table. Issue the command "**change dialplan analysis**" and add an entry in the table to treat any digit string of **3** digits in **Total Length** with a leading **Dialed String** of **5** as a **Call Type** of **aar**.

```
change dialplan analysis                                    Page   1 of   12

                             DIAL PLAN ANALYSIS TABLE
                                                           Percent Full:    1

      Dialed  Total  Call      Dialed  Total  Call      Dialed  Total  Call
      String  Length Type      String  Length Type      String  Length Type
        0       1    attd
        1       3    dac
        2       5    ext
        3       5    ext
        4       3    aar
        5       3    aar
        6       3    ext
        7       4    ext
        7       5    ext
        8       1    fac
        9       1    fac
        *       3    fac
        #       3    fac
```

Step	Description
3.9	Configure the AAR digit analysis table.

Issue the command “**change aar analysis**” and administer settings as per below. Add entries in the table to send the following **Dialed Strings** to **Route Pattern 1**.

- Dialed String **501** is used by Avaya Meeting Exchange for a Scan call function (see **Step 4.8**).
- Dialed String **556** is used by Avaya Meeting Exchange for a Direct call function (see **Step 4.9**).

```
change aar analysis                                           Page   1 of   2

                             AAR DIGIT ANALYSIS TABLE
                                                            Percent Full:    1

          Dialed              Total     Route     Call   Node  ANI
          String            Min  Max   Pattern    Type   Num   Reqd
    501                     3    3      1         aar          n
    502                     3    3      2         aar          n
    503                     3    3      3         aar          n
    556                     3    3      1         aar          n
```

Step	Description
3.10	Configure a route pattern.

Issue the command “**change route-pattern <n>**”, where **n** is the number of the route pattern to be administered. Add an entry in the table to utilize the trunk group provisioned in **Step 3.7**.

```
change route-pattern 1                                            Page   1 of   3

                    Pattern Number: 1   Pattern Name: SES SIP
                             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: 1    0                    0                                            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
```

4. Avaya Meeting Exchange Configuration

This section describes the steps for configuring Avaya Meeting Exchange to interoperate with Avaya SIP Enablement Services via secure SIP connectivity utilizing TLS.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.1</td><td>Log in to the Avaya Meeting Exchange Server console with the appropriate credentials.</td></tr>
<tr><td>4.2</td><td>Configure settings that enable secure SIP connectivity between Avaya Meeting Exchange and other SIP User Agents by editing the system.cfg file as follows:

cd to /usr/ipcb/config.
Edit the system.cfg file with a text editor, e.g., vi.
Add a line to identify the IP address of Avaya Meeting Exchange (as defined in the /etc/hosts file), e.g.,
IPAddress=192.168.13.101
Add a line to populate the From header field in SIP INVITE messages from Avaya Meeting Exchange, e.g.,
MyListener=sips:S6200@192.168.13.101:5061;transport=tls
Note: To enable secure SIP connectivity utilizing TLS, the entry must contain sips, 5061 and transport=tls. The string “S6200” is arbitrarily chosen.
Add a line to provide User Agents a Contact address to use for acknowledging SIP messages from Avaya Meeting Exchange, e.g.,
respContact=<sip:S6200@192.168.13.101:5061;transport=tls>
Note: To enable secure SIP connectivity utilizing TLS, the entry for the Contact address must contain 5061 and transport=tls. The string “S6200” is arbitrarily chosen.
Add the following lines to set the Min-SE timer to 86400 seconds in SIP INVITE messages from Avaya Meeting Exchange, e.g.,
sessionRefreshTimerValue=86400
minSETimerValue=86400
</td></tr>
</table>

Step	Description
4.3	To associate incoming calls to Avaya Meeting Exchange with different call flows, edit the **UriToTelnum.tab** file to extract both Automatic Number Identification (ANI) and Direct Inward Dial (DID, also called DDI in Europe) values as follows: • cd to **/usr/ipcb/config**. • Edit the **UriToTelnum.tab** file with a text editor, e.g., vi. • Add a line to match the pattern of the To header field in SIP INVITE messages from Avaya SIP Enablement Services. If a match occurs, the DID is extracted from the To header field and the ANI is extracted from the From header field, e.g., o **""*"*<sip:*" $1** where **""*"*<sip:*"** matches: ▪ To: **"556" <sip:556@192.168.11.20>** and **$1** utilizes **556** (the variable contained in the first *****) as the DID for the call. ▪ From: **"SIP 31002" <sip:anonymous.invalid:5061>** and **$1** utilizes **SIP 31002** (the variable contained in the first *****) as the ANI for the call. • Enable an undefined caller to receive a prompt for operator assistance by administering for the condition of an unmatched SIP INVITE message by adding a wildcard entry as the last line in this file, e.g., o *** $0** ***Note**: Entries in this file are read sequentially; therefore, the line* **** $0** must be the last line in the file. Otherwise, all calls to Avaya Meeting Exchange would match the wildcard and thus receive a prompt for operator assistance.*

Step	Description
4.4	To enable Dial-Out from Avaya Meeting Exchange to Avaya SIP Enablement Services via secure SIP trunking, edit the **telnumToUri.tab** file as follows: • cd to **/usr/ipcb/config**. • Edit the **telnumToUri.tab** file with a text editor, e.g., vi. • Add a line to the file to route outbound calls from Avaya Meeting Exchange to Avaya SIP Enablement Services, e.g., o **3???? sip:$0@192.168.11.20:5061;transport=tls** where the pattern **3????** matches any five digit number with a leading "**3**" and routes the call to Avaya SIP Enablement Services (**192.168.11.20**) via TLS. To enable secure SIP connectivity utilizing TLS, the entry must contain: **5061** and **transport=tls**. Avaya Meeting Exchange substitutes "**$0**" with the dialed number in outgoing SIP INVITE messages, e.g., if **31001** is dialed, Avaya Meeting Exchange sends a SIP INVITE message with: **sip:31001@192.168.11.20:5061;transport=tls** in the SIP URI and To header field. ***Note****: Alternatively, routing to Avaya SIP Enablement Services could have been enabled as a default gateway with a wildcard entry,* *e.g.,* **** sip:$0@192.168.11.20:5061;transport=tls*** *where* ******* *allows any dialed digits to be sent to Avaya SIP Enablement Services,* ***(192.168.11.20)*** via TLS.

Step	Description
4.5	To configure Avaya Meeting Exchange as software media server (softms, which utilizes software based DSP resources), edit the **processTable.cfg** file as follows: • cd to **/usr/ipcb/config**. • Edit the **processTable.cfg** file with a text editor, e.g., vi. ***Note**: The **processTable.cfg** for these Application Notes contains IP Addresses of **0.0.0.0**, which are equivalent to the IP address (**192.168.13.101**) of Avaya Meeting Exchange.*

	`# processes file, enumerates the number of processes in the network.`
	`# will have the name of the process   Key ID and the IP address`
	`proccessName   ipcKeyNumber   ProcessExe               ipAddress  route  ProcessArgs`
	`initipcb       110            noexecute                  0.0.0.0`
	`bridget700     100            noexecute                  0.0.0.0`
	`dspEvents/msDispatcher,netEvents/sipAgent`
	`commsProcess   111            /usr/dcb/bin/serverComms   0.0.0.0`
	`sipAgent       101            /usr/dcb/bin/sipagent      0.0.0.0`
	`dspEvents/msDispatcher,appEvents/bridget700`
	`msDispatcher   102            /usr/dcb/bin/msdispatcher  0.0.0.0`
	`netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer`
	`mediaServer    103            /usr/dcb/bin/softms        0.0.0.0`
	`appEvents/msDispatcher,netEvents/msDispatcher   1`
	`snmpAgent      120            noexecute                  0.0.0.0`

4.6	Reboot Avaya Meeting Exchange for changes to take effect. ***Note**: Rebooting Avaya Meeting Exchange is service impacting.*
	`[S6200]> init 6`

4.1. CBUTIL Utility

The following steps provide examples of how to provision Direct and Scan call functions by utilizing the cbutil utility on Avaya Meeting Exchange. DID values (obtained from procedures in the previous section) are associated with call functions to access conferences provisioned on Avaya Meeting Exchange.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.7</td><td>To map DID values obtained in Step 4.3 to DNIS entries, run the cbutil utility as follows:

Log in to the Avaya Meeting Exchange Server console with the appropriate credentials.
At the command prompt, enter tcsh to set the UNIX shell on Avaya Meeting Exchange.
At the command prompt, run the cbutil utility to verify DNIS entries provisioned on Avaya Meeting Exchange.

Note: The cbutil command line utility enables administrators to assign a specific annunciator message, line name, company name, system function, reservation group and prompt sets to a maximum of 30,000 DNIS or DID patterns. Each reservation group may use one passcode to enter a conference. In this way, administrators can create different reservation groups on Avaya Meeting Exchange, rather than relying on a single, bridge-wide passcode. Avaya Meeting Exchange stores this assignment information in the Call Branding table of the database. Avaya Meeting Exchange sorts the information in the Call Branding table in ascending order of the DNIS or DID number with the wildcard character "?" last in a series. For example, 129? follows 1299. The last entry in the table consists entirely of wildcard characters. The number of characters in this entry corresponds to the number of DNIS/DID digits specified in the Digit Parameters configuration.</td></tr>
<tr><td></td><td><pre>S6200>cbutil
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.

Usage: cbutil <command> [command-specific args...]
 where <command> may be one of:
  add   Add an entry to the Call Branding table
  remove   Remove an entry from the Call Branding table
  update   Update an entry in the Call Branding table
  lookup   Display an entry in the Call Branding table
  count   Display the number of entries in the Call Branding table
  list   List entries in the Call Branding table
  dnissize   Set system configured max dnis length (1-16)
   Note: This command should only be used when the bridge is not running.
Use "cbutil<command> -help" to get help on a specific command</pre></td></tr>
<tr><td></td><td></td></tr>
</table>

Step	Description

4.8 Enable Dial-In access (via passcode) to conferences provisioned on Avaya Meeting Exchange as follows:

- Add a DNIS entry for a **Scan call function** corresponding to DID **501** by entering the following command at the command prompt:
  cbutil add <**dnis**> <**rg**> <**msg**> <**ps**> <**ucps**> <**func**> [**-l** <**ln**> **-c** <**cn**>], where the variables for add command are defined as follows:
  - <**dnis**> DNIS
  - <**rg**> Reservation Group
  - <**msg**> Annunciator message number
  - <**ps**> Prompt Set number (0-20)
  - <**ucps**> Use Conference Prompt Set (y/n)
  - <**func**> One of: DIRECT/SCAN/ENTER/HANGUP/AUTOVL/FLEX
  - **-l** <**"ln"**> Optional line name to associate with caller
  - **-c** <**"cn"**> Optional company name to associate with caller

```
S6200>cbutil add 501 0 1 1 n scan
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

4.9 Enable Dial-In access (as moderator without entering a passcode) to conferences provisioned on Avaya Meeting Exchange by adding a DNIS entry for a **Direct call function** corresponding to DID **556**.

```
S6200>cbutil add 556 0 301 1 n direct
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

4.10 At the command prompt, enter **cbutil list** to verify the DNIS entries provisioned in **Steps 4.8** and **4.9** were provisioned and entered correctly.

***Note**: The last entry in the call brand table is the wild card entry "**???**". This entry captures any wrong number (e.g., unmatched **DID** values) and places the call into the Enter queue for operator assistance.*

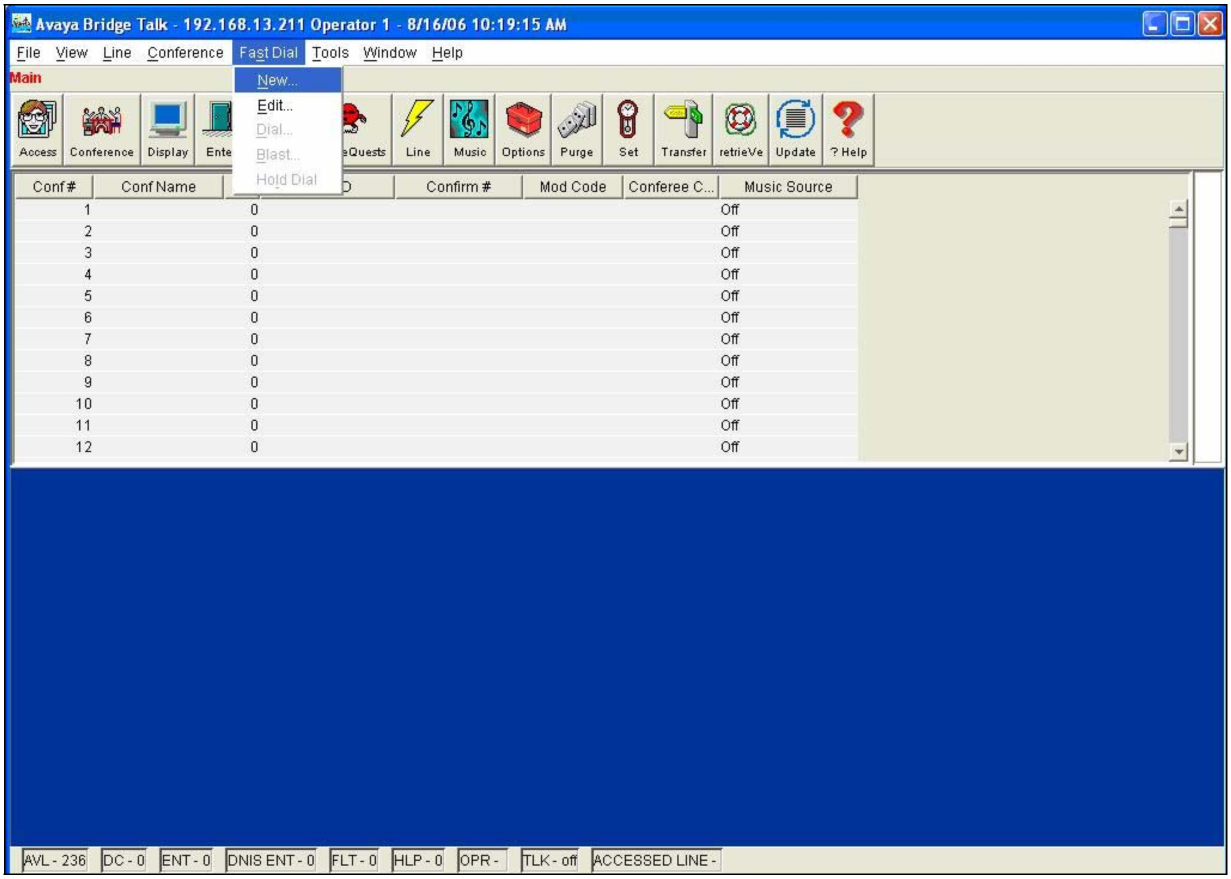
```
S6200>cbutil list
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.

DNIS             Grp Msg PS  CP Function Line Name            Company Name
---------------- --- --- --- -- -------- -------------------- -----------------
501              0   1   1   N  SCAN
556              0   301 1   N  DIRECT
???              0   208 1   N  ENTER
```

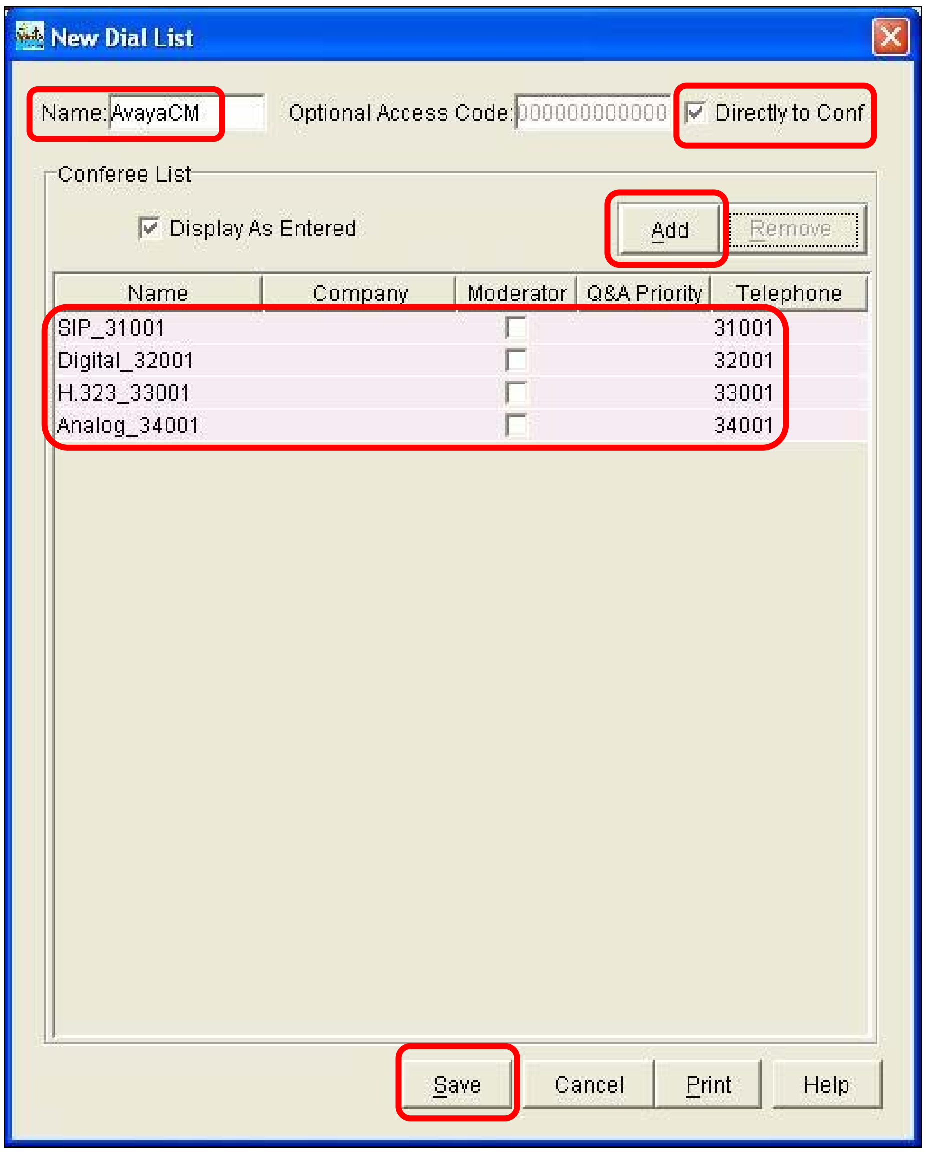
4.2. Bridge Talk

The following steps provide an example of how to provision a conference on Avaya Meeting Exchange from the Avaya Bridge Talk application. This sample conference is utilized in conjunction with the Direct and Scan call functions (provisioned in the previous section) to enable both Dial-In and Dial-Out access to audio conferencing for endpoints associated with Avaya Communication Manager.

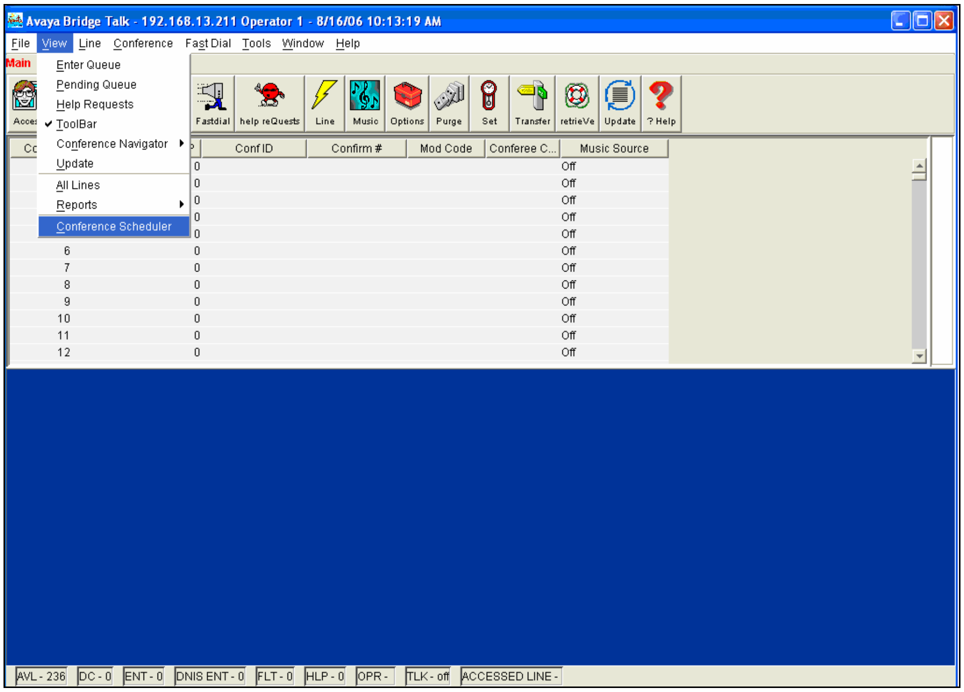
***Note**: If any of the features shown in the following Avaya Bridge Talk screen captures are not present, contact an authorized Avaya sales representative to make the appropriate changes.*

Step	Description
4.11	Open the Avaya Bridge Talk application and log in to Avaya Meeting Exchange with the appropriate credentials. 

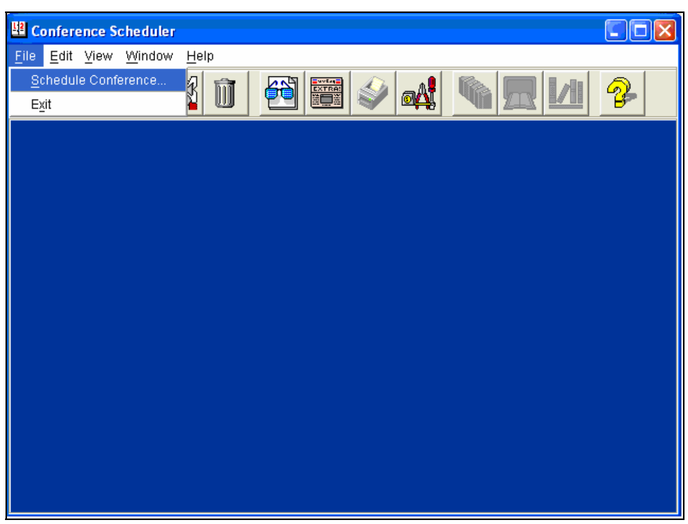
Step	Description
4.12	Provision a dial list that is utilized for Dial-Out (e.g., Blast dial and Fast Dial) from Avaya Meeting Exchange. From the Avaya Bridge Talk menu bar, click **Fast Dial → New**. 

Step	Description
4.13	From the **New Dial List** window that is displayed: • Enter a descriptive name for the **Name** field. • Allow conference participants on the dial list to enter the conference without a passcode by checking the **Directly to Conf** box as shown below. • Add entries to the dial list by clicking the **Add** button for each entry. o Assign moderator privileges to a conference participant by checking the **Moderator** box. • See **Reference 3** in **Section 8** for provisioning of the remaining entries in this screen. • When finished, click the **Save** button on the bottom of the screen. 

Step	Description
4.14	Provision a conference with Auto Blast enabled. From the Avaya Bridge Talk menu bar, click **View → Conference Scheduler**.



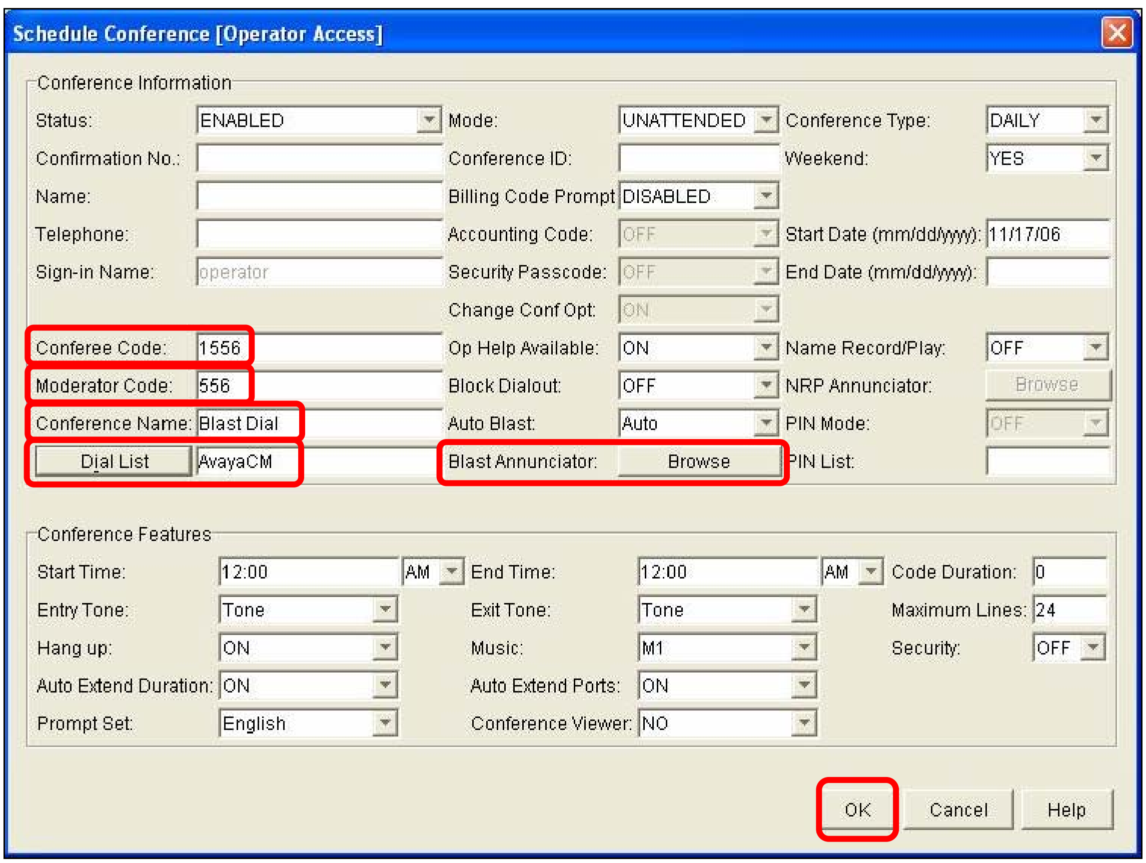
Step	Description
4.15	From the **Conference Scheduler** window that is displayed, click **File → Schedule Conference**.



Step	Description
4.16	From the **Schedule Conference** window that is displayed, provision a conference as follows:

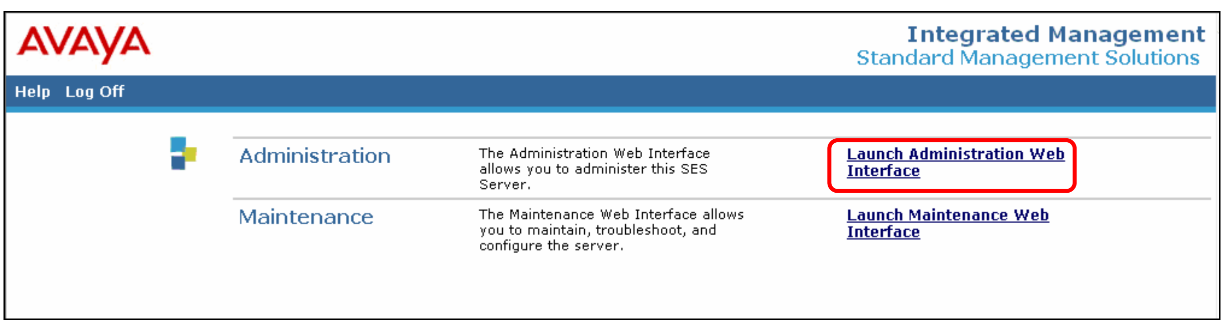
- Enter a unique Conferee code to allow participants access to this conference.
- Enter a unique Moderator code to allow participants access to this conference with moderator privileges. Enable moderator access without a passcode for this conference call by configuring the following:
    - o The **Moderator Code** "**556**" must have an associated **Direct call function** provisioned for "**556**" (see **Step 4.9**).

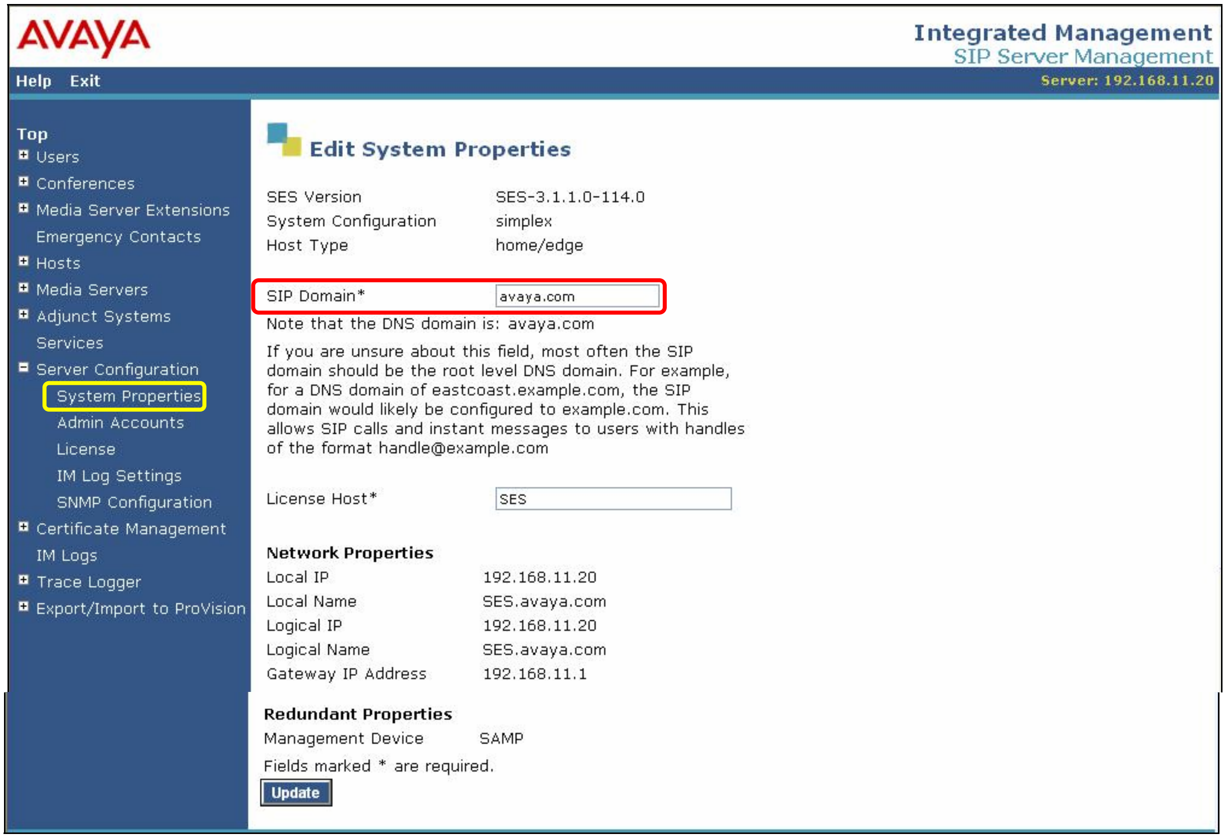
  Note: *This conference remains open for participants to enter as either moderator or participant by entering the appropriate code when prompted.*
- Enter a descriptive name for the **Conference Name** field.
- Administer settings to enable an Auto Blast dial by setting **Auto Blast** to **Auto** and selecting the dial list provisioned in **Step 4.13**.
    - o [***Not Shown***] *Select a dial list by clicking the **Dial List** button, then selecting a dial list from the **Create, Select or Edit Dial List** window that is displayed and clicking the **Select** button.*
- See **Reference 3** in **Section 8** for provisioning of the remaining entries in this screen.
- When finished, click the **OK** button on the bottom of the screen.



5. Avaya SIP Enablement Services Configuration

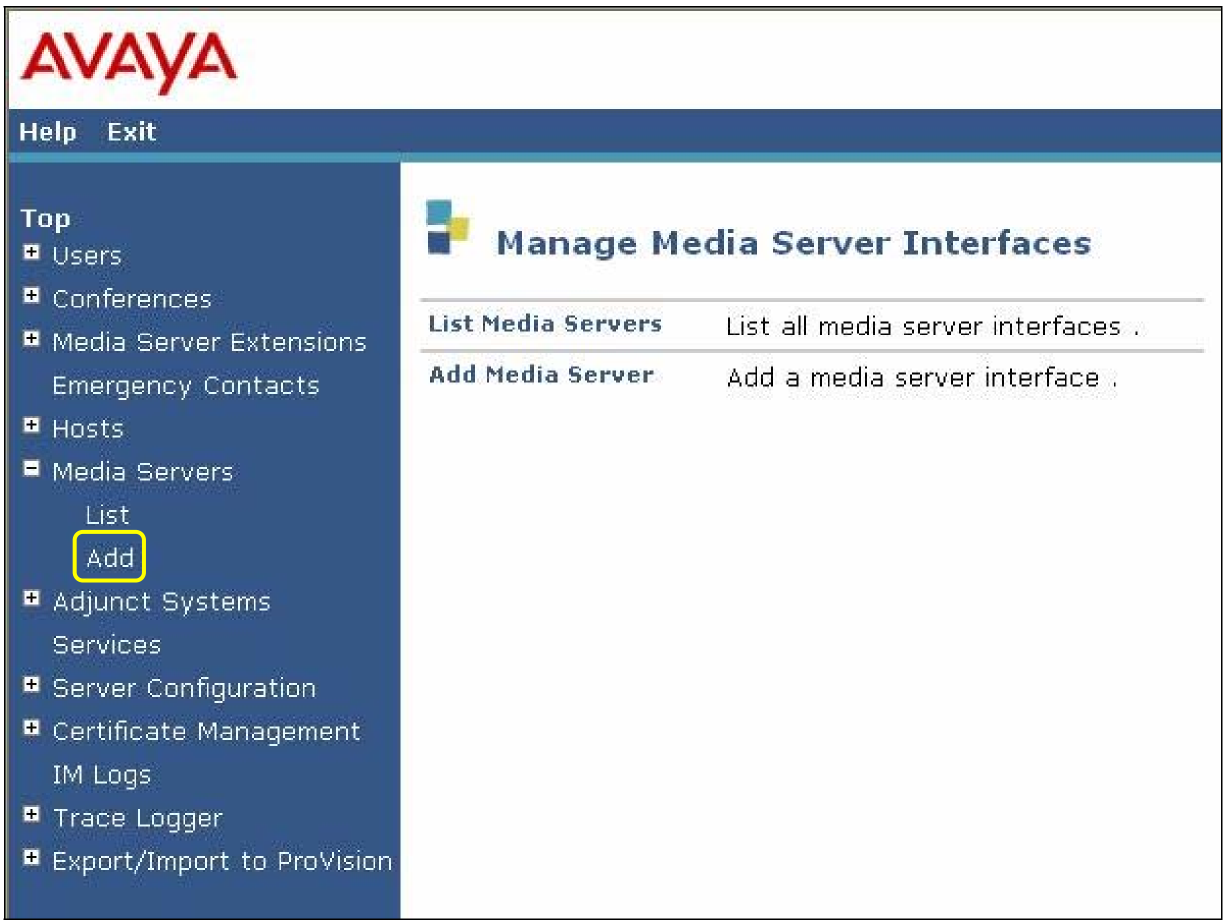
This section describes the steps for configuring Avaya SIP Enablement Services to enable secure SIP connectivity between Avaya Communication Manager and Avaya Meeting Exchange utilizing TLS.

Step	Description
5.1	Administer settings for Avaya SIP Enablement Services as follows: • Open a web browser and enter the following URL: **https://<IP address of Avaya SIP Enablement Services>/admin** • Log in to Avaya SIP Enablement Services with the appropriate credentials. 
5.2	Click **Launch Administration Web Interface**. 

Step	Description
5.3	Verify the **System Properties** for Avaya SIP Enablement Services as follows. From the Administration Web Interface: • Click the **+** sign to expand the options under **Server Configuration**. • Click **System Properties**. • Verify the **SIP Domain** matches the authoritative domain configured for the IP network region on Avaya Communication Manager in **Step 3.4**. 

5.1. Enable Dial-Out from Avaya Meeting Exchange

The following steps enable secure SIP trunking between Avaya SIP Enablement Services and Avaya Communication Manager. This will allow Dial-Out from Avaya Meeting Exchange to Avaya Communication Manager via Avaya SIP Enablement Services (see **Figure 2**).

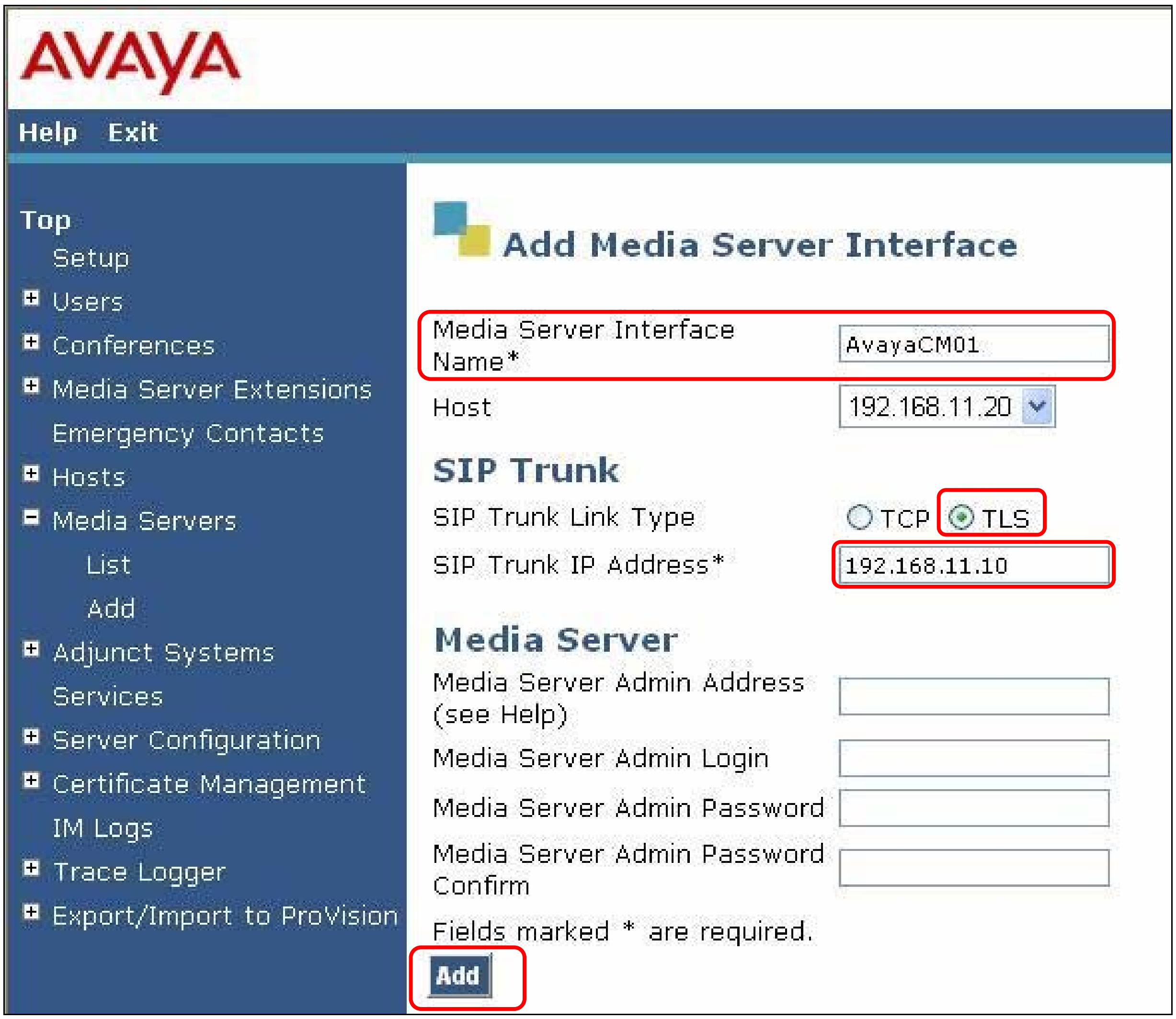
Step	Description
5.4	To enable secure SIP trunking between Avaya SIP Enablement Services and Avaya Communication Manager, add a **Media Server** corresponding to Avaya Communication Manager as follows. From the Administration Web Interface: • Click the **+** sign to expand the options under **Media Servers**. • Click **Add**. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.5</td><td>

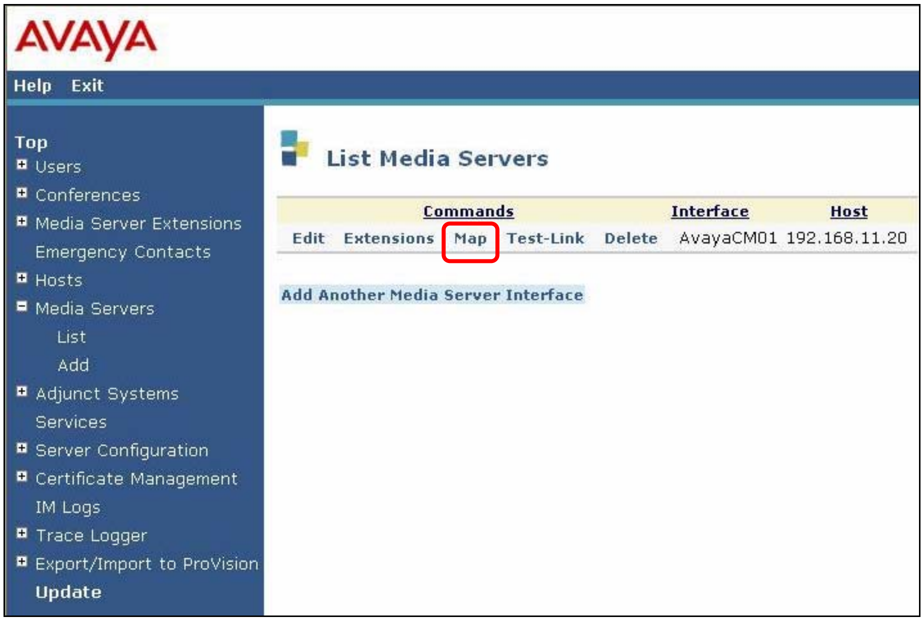
The **Add Media Server Interface** page is displayed.

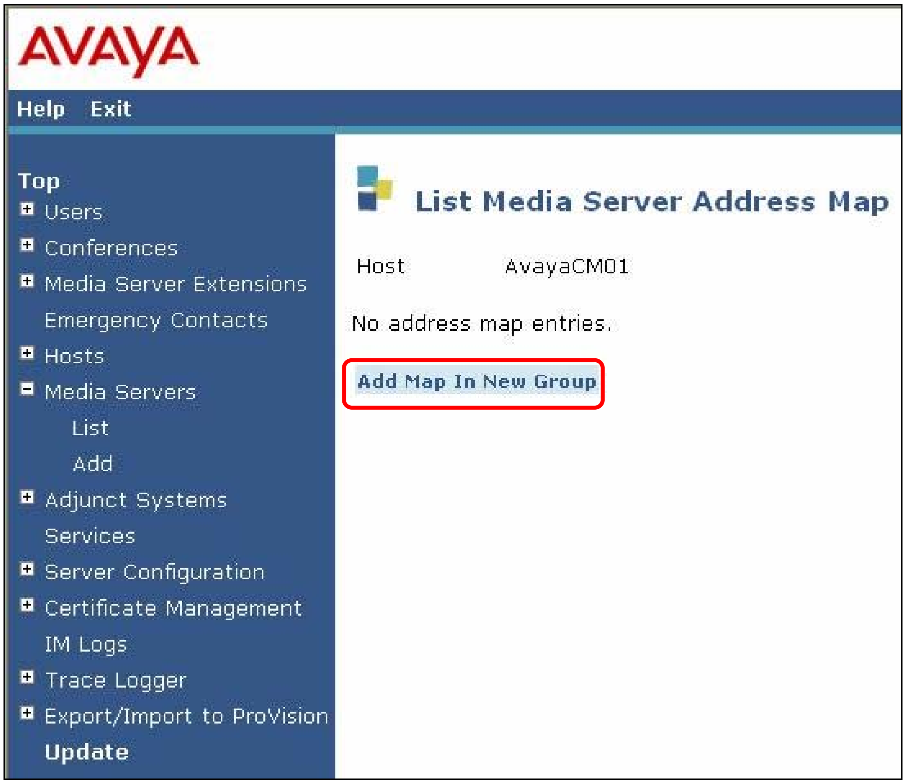
To enable secure SIP connectivity to Avaya Communication Manager, provision **SIP Trunk** parameters as follows:

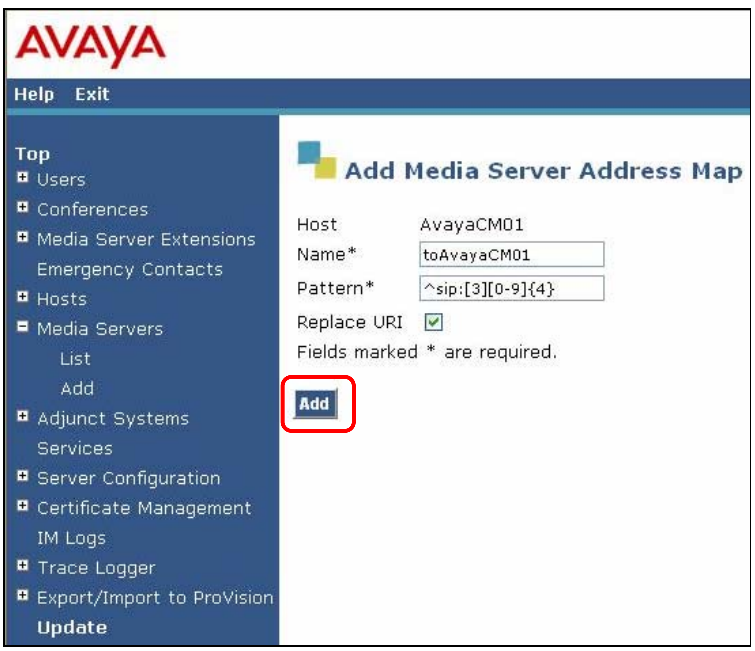
- Enter a descriptive name for **Media Server Interface Name** field.
- Set the **SIP Trunk Link Type** to **TLS**, consistent with the configuration for the signaling group provisioned on Avaya Communication Manager in **Step 3.6**.
- Enter the IP address of the C-LAN on Avaya Communication Manager (see **Step 3.5**) in the **SIP Trunk IP Address** field.
- Click the **Add** button when finished.
    - [***Not Shown***] *Click the* ***Continue*** *button on the confirmation page*.



</td></tr>
</table>

Step	Description
5.6	To route SIP traffic to Avaya Communication Manager, provision a **Media Server Address Map** for the corresponding media server configured in **Step 5.5** by clicking **Map**. 

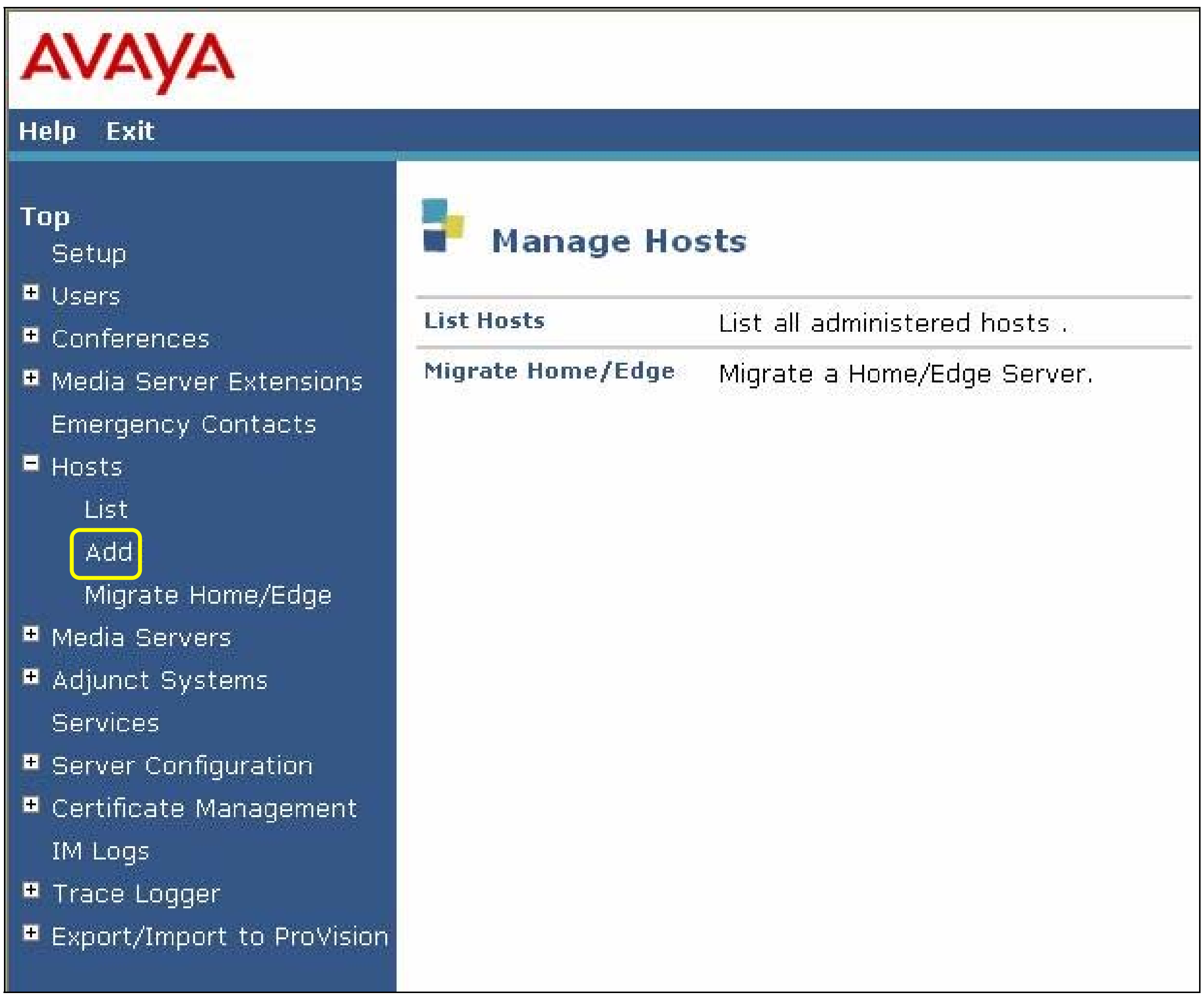
Step	Description
5.7	Click **Add Map In New Group**. 

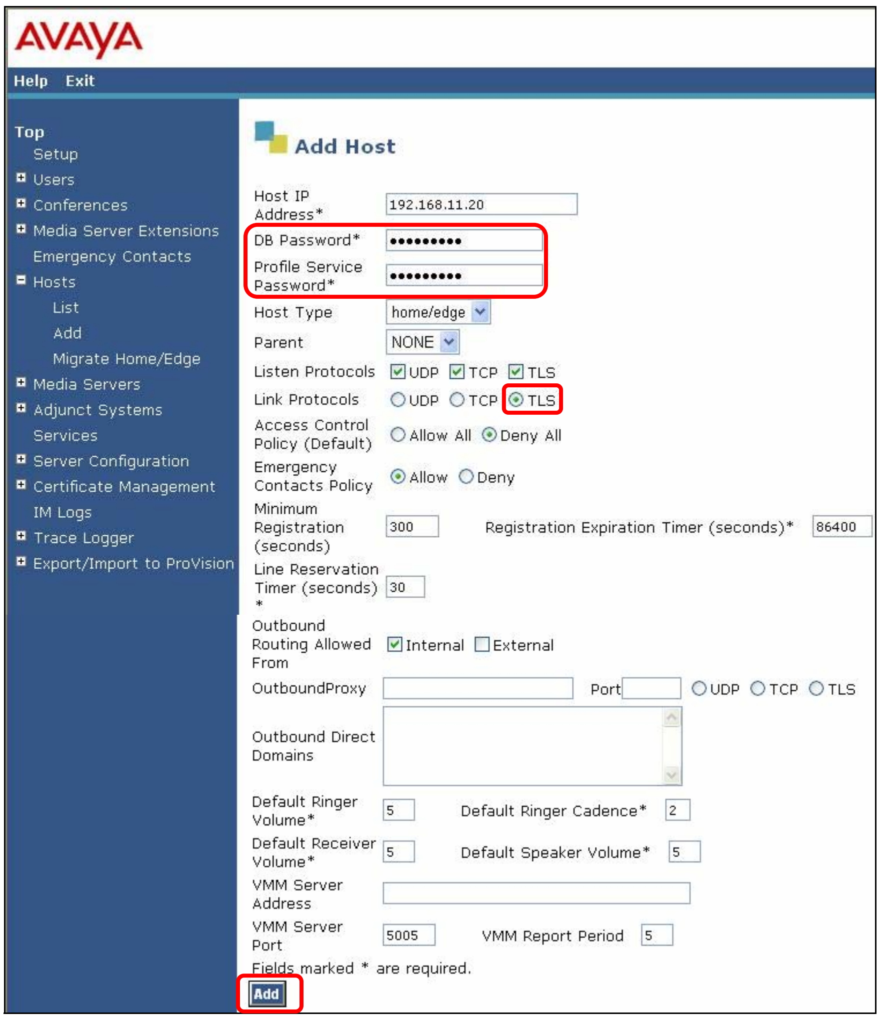
Step	Description
5.8	The **Add Media Server Address Map** page is displayed. To match the pattern of incoming SIP INVITE messages (from Avaya Meeting Exchange) destined for Avaya Communication Manager, configure settings for the **Media Server Address Map** as follows: • Enter a descriptive name for the **Name** field. • Enter a **Pattern** that corresponds to the following: o The dial plan configuration for station extensions on Avaya Communication Manager (for these Application Notes, station extensions on Avaya Communication Manager are 5 digits in length with a leading 3, see **Step 3.8** and **Figure 1**). *__Note__: The URI usually takes the form sip:user@domain, where domain can be a domain name or an IP address. For these Application Notes, user is actually the telephone number of the phone. An example of a URI sent by a SIP endpoint to Avaya SIP Enablement Services would be __sip:31001@192.168.11.20__. The __Pattern ^sip:[3][0-9]{4}__ means match the string __sip:3__ (if it occurs at the beginning of the URI), followed by __4__ more digits, each in the range __0__ through __9__.* • To replace the URI with the contact displayed in **Step 5.9**, select **Replace URI.** • Click the **Add** button when finished. o [***Not Shown***] *Click the **Continue** button on the confirmation page.* 

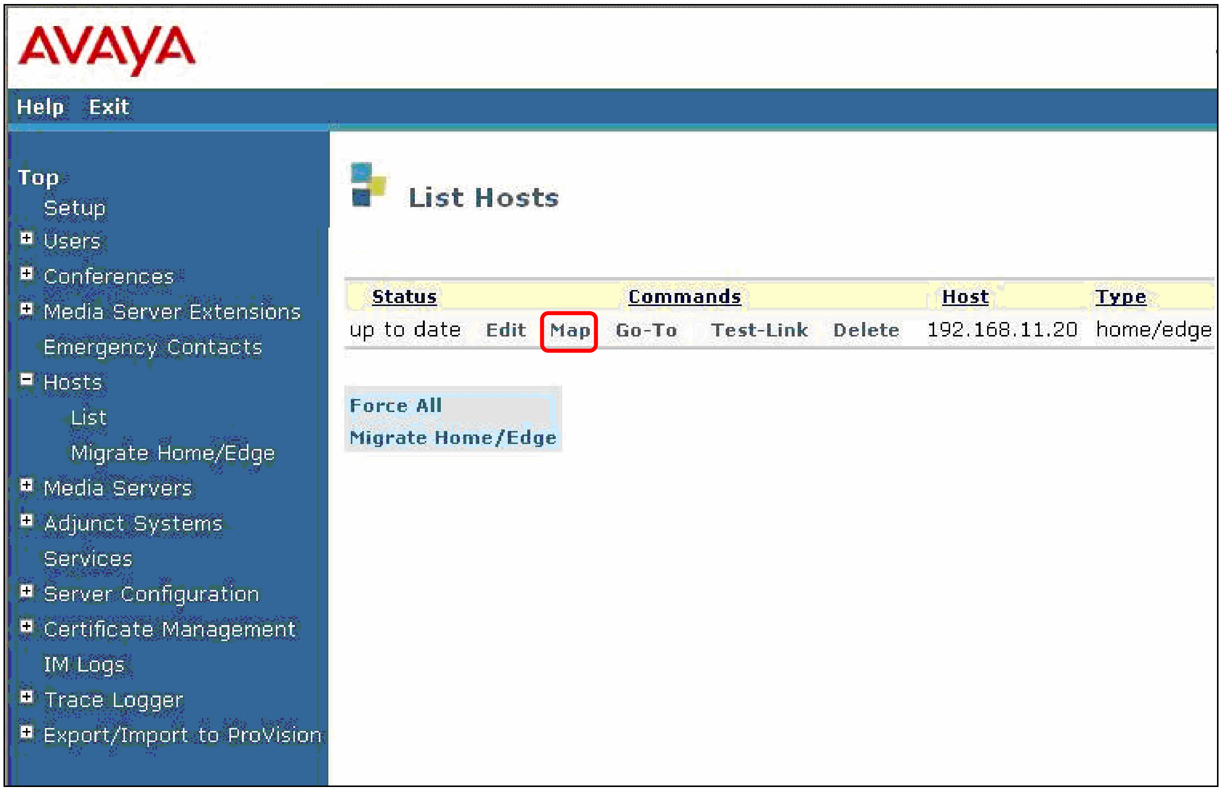
Step	Description
5.9	The media server address map is added. To apply the administration in the above steps, click on **Update** on the left side of the page. ***Note***: *The **Update** link appears on the current page whenever updates are outstanding and can be used at any time to save the administration provisioned to that point. The SIP URI in the **Contact** field is populated from the media server interface configuration, provisioned in **Step 5.5**.* 

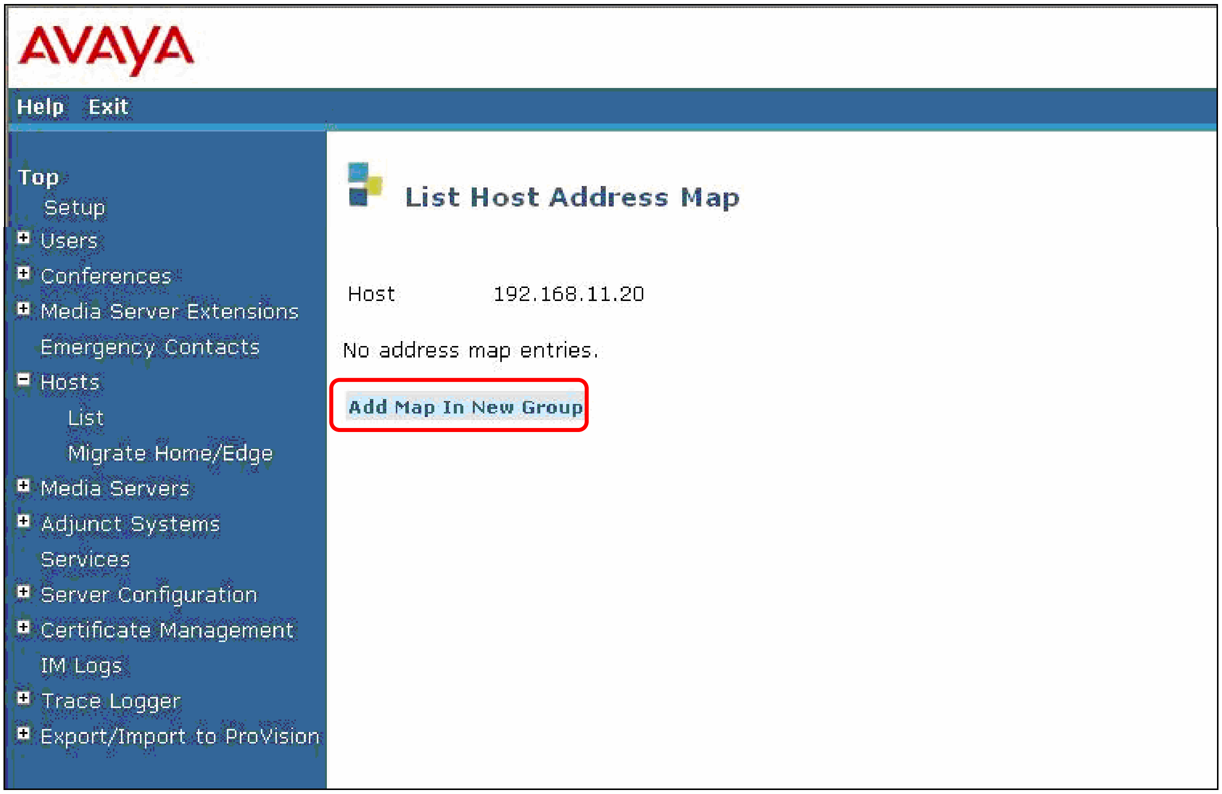
5.2. Enable Dial-In to Avaya Meeting Exchange

The following steps enable secure SIP trunking between Avaya SIP Enablement Services and Avaya Meeting Exchange. This will allow Dial-In to Avaya Meeting Exchange from Avaya Communication Manager Via Avaya SIP Enablement Services (see **Figure 3**).

Step	Description
5.10	To enable secure SIP trunking between Avaya SIP Enablement Services and Avaya Meeting Exchange, add a **Host** corresponding to Avaya SIP Enablement Services as follows. From the Administration Web Interface: • Click the **+** sign to expand the options under **Hosts**. • Click **Add**. 

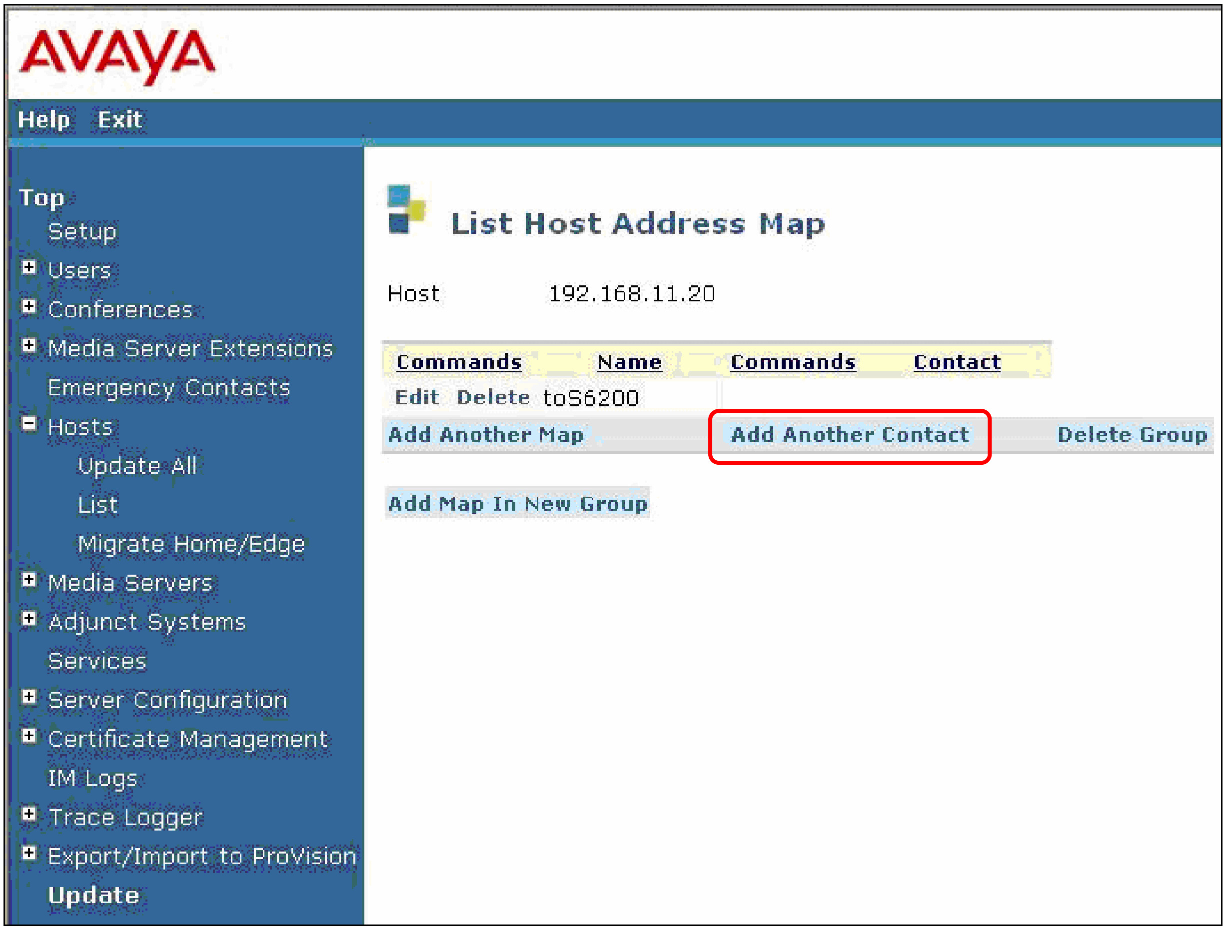
Step	Description
5.11	The **Add Host** page is displayed. To enable secure SIP connectivity for this host, provision as follows: • Enter the password assigned to the database at installation for the **DB Password** field. • Enter a password which uniquely identifies Avaya SIP Enablement Services for intra- and inter-proxy communication for the **Profile Service Password** field. • Select **TLS** from the available **Link Protocols**, which is consistent with the system.cfg file provisioned for Avaya Meeting Exchange in **Step 4.2**. • Leave all remaining required fields at the default settings. • Click the **Add** button when finished. o [***Not Shown***] *Click the **Continue** button on the confirmation page.* o [***Not Shown***] *To apply the administration, click on **Update** on the left side of the page.* 

Step	Description
5.12	To route SIP traffic to Avaya Meeting Exchange, provision a **Host Address Map** for the corresponding host configured in **Step 5.11** by clicking **Map**. 

Step	Description
5.13	Click **Add Map In New Group**. 

Step	Description
5.14	The **Add Host Address Map** page is displayed. To match the pattern of incoming SIP INVITE messages destined for Avaya Meeting Exchange, configure settings for the **Host Address Map** as follows: • Enter a descriptive name for the **Name** field. • Enter a **Pattern** that corresponds to the call functions provisioned for Avaya Meeting Exchange in **Step 4.8** and **Step 4.9**. *__Note__: The __Pattern__, __^sip:[5][0-9]{2}__ matches the string __sip:5__ (if it occurs at the beginning of the URI), followed by __2__ more digits, each in the range __0__ through __9__.* • To replace the URI with the contact provisioned in **Step 5.16**, select **Replace URI.** • Click the **Add** button when finished. o [***Not Shown***] *Click the **Continue** button on the confirmation page.* 

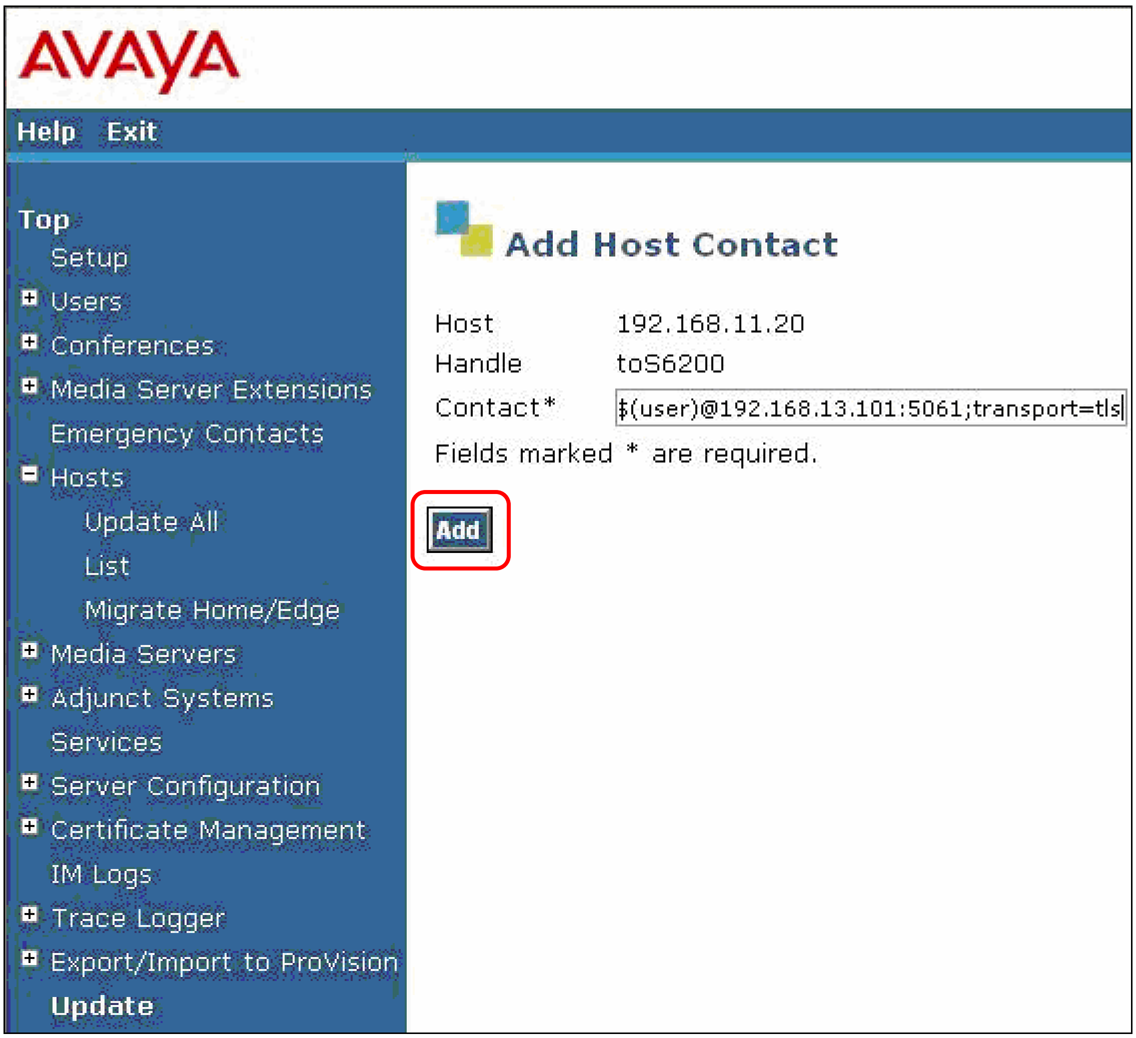
Step	Description
5.15	The host address map is added. To specify routing information for the address map defined in **Step 5.14**, click on **Add Another Contact**.



<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.16</td><td>

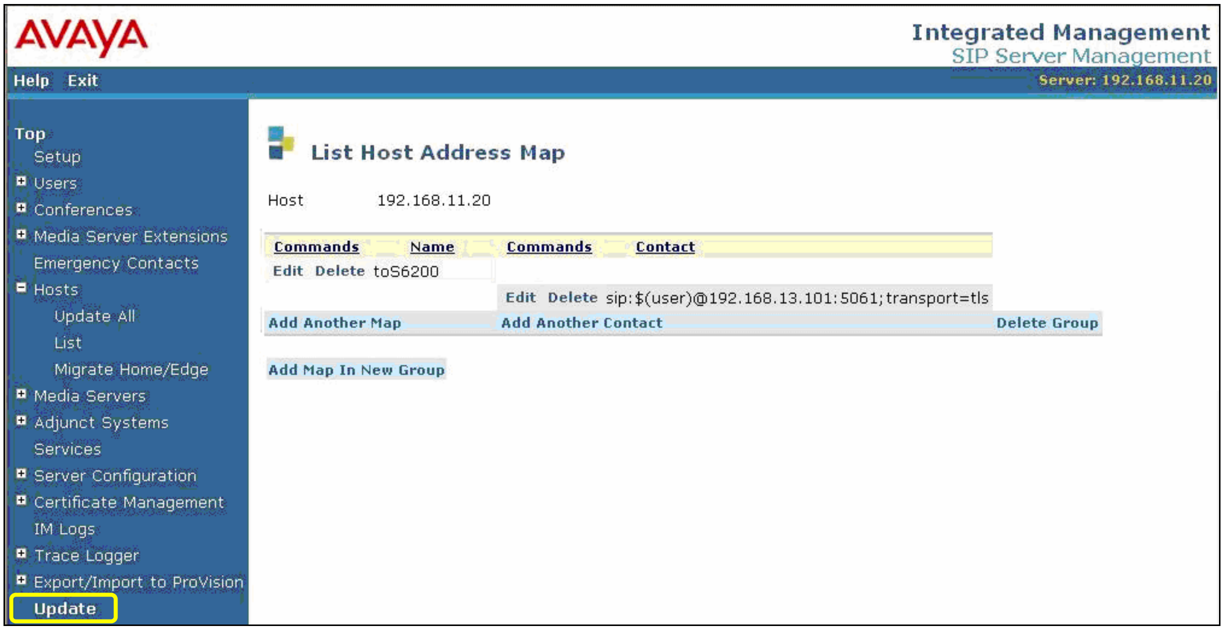
The **Add Host Contact** page is displayed.

- To enable secure SIP connectivity to Avaya Meeting Exchange, enter **sip:$(user)@192.168.13.101:5061;transport=tls** in the **Contact** field.
  - ***Note****: The IP address, port number and transport protocol are consistent with the system.cfg file provisioned for Avaya Meeting Exchange in* ***Step 4.2****. Avaya SIP Enablement Services substitutes "****$(user)****" with the user field (i.e., the dialed number) in the incoming SIP INVITE message.*
- Click the **Add** button when finished.
  - o [***Not Shown***] *Click the* ***Continue*** *button on the confirmation page.*



</td></tr>
</table>

Step	Description
5.17	The host contact is added to the host address map group. To apply the administration in the above steps, click on **Update** on the left side of the page.



Step	Description
5.18	Add Avaya Meeting Exchange as a **trusted host** on Avaya SIP Enablement Services. All SIP user agents, proxies and/or gateways to which calls can be routed should be administered as trusted hosts on Avaya SIP Enablement Services. This permits call setup and termination by remote parties to be handled without authentication challenges to a trusted host. This is provisioned at the Avaya SIP Enablement Services command line of the edge server (or as per these Application Notes, at the edge/home server, if only one server is used). • Log in to the Avaya SIP Enablement Services console with the appropriate credentials. • Add Avaya Meeting Exchange as a trustedhost by entering the following command: **trustedhost -a trusted-host-IP-address -n trusting-SES-IP-address [-c 'comment text']**
	`SES>`**`trustedhost –a 192.168.13.101 –n 192.168.11.20 –c S6200`**
	• Verify trusted host entries by entering the following command: **trustedhost -L**

	`SES> `**`trustedhost -L`**
	`Third party trusted hosts.`
	` Trusted Host IP address  |   SES Host IP address     |         Comment`
	`-------------------------+-------------------------+------------------------`
	`192.168.13.101            | 192.168.11.20            | S6200`

5.19	To apply the administration defined in Step **5.18**, click on **Update** on the left side of the page on the web browser interface. 

6. Verification Steps

The following steps can be used to verify the configuration described in these Application Notes.

Step	Description
6.1	Verify all members for the SIP trunk group provisioned in **Step 3.7** are **in-service/idle**. From a SAT session: • Issue the command "**status trunk <n>**", where **n** is the number of the trunk group to status. • Verify that all members in the trunk group are **in-service/idle**.
6.2	Log in to the Avaya Meeting Exchange Server console with the appropriate credentials. Run the **dcbps** script to verify all conferencing related processes are running on Avaya Meeting Exchange. • cd to **/usr/dcb/bin**. • At the command prompt, run the script **dcbps** and confirm all processes below are running by verifying an associated Process ID (PID) for each process.

```
S6200>dcbps
  1786   FP 101 ?        0:00 log
  1776   FP 144 ?        0:01 initdcb
  1787   FP 101 ?        0:00 bridgeTr
  1788   FP 105 ?        0:00 netservi
  1791   FP 129 ?        0:00 timer
  1792   FP 101 ?        0:00 traffic
  1793   FP 104 ?        0:00 chdbased
  1794   FP 101 ?        0:00 startd
  1795   FP 109 ?        0:00 cdr
  1796   FP 101 ?        0:00 modapid
  1797   FP 101 ?        0:00 schapid
  1798   FP 104 ?        0:00 callhand
  1799   FP 139 ?        0:00 initipcb
  1800   FP 139 ?        0:00 sipagent
  1801   FP 139 ?        0:00 msdispat
  1802   FP 158 ?        0:00 softms
  1803   FP 139 ?        0:00 serverCo
  1554   TS  80 ?        0:00 sqlexecd with 5 children
```

Step	Description
6.3	Verify the SIP trunk provisioned in **Step 3.7** is utilized when a call from a SIP telephone Dials-In to Avaya Meeting Exchange. This step also verifies the conferencing applications provisioned in **Section 4**.

From a SAT session:

- Issue the command "**list trace tac <n>**", where **n** is the TAC defined for the trunk group provisioned in **Step 3.7**.
- From an endpoint associated with Avaya Communication Manager, dial **556** to enter a conference as moderator via a DNIS direct call flow (provisioned in **Section 4**) while simultaneously initiating an Auto Blast dial to participants in the dial list provisioned in **Step 4.13**.

Note*: The trace below shows a SIP telephone Dialing-In to Avaya Meeting Exchange via a Direct call function. A SIP telephone was arbitrarily selected to place the call (Dial-In), as the configuration presented in these Application Notes allows any station or trunk type (e.g., SIP, H.323, Digital or Analog) on Avaya Communication Manager access (both Dial-In and Dial-Out) to Avaya Meeting Exchange via secure SIP connectivity*.

```
list trace tac 101                                                   Page   1

                                LIST TRACE

time            data

10:53:42     Calling party station    31002 cid 0x1d1
10:53:42     Calling Number & Name 31002 SIP 31002
10:53:42     active station    31002 cid 0x1d1
10:53:42     G711MU ss:off ps:20 rn:1/1 192.168.12.13:34008 192.168.11.11:2952
10:53:42     xoip: fax:Relay modem:off tty:US 192.168.11.11:2952 uid:0x50020
10:53:42     dial 556 route:AAR
10:53:42     term trunk-group 1    cid 0x1d1
10:53:42     dial 556 route:AAR
10:53:42     route-pattern  1 preference 1  cid 0x1d1
10:53:42     seize trunk-group 1 member 1  cid 0x1d1
10:53:42     Calling Number & Name NO-CPNumber SIP 31002
10:53:42     Proceed trunk-group 1 member 1  cid 0x1d1
10:53:42     active trunk-group 1 member 1  cid 0x1d1
10:53:42     G711MU ss:off ps:20 rn:1/1 192.168.13.101:42212 192.168.11.11:2956
10:53:42     xoip: fax:Relay modem:off tty:US 192.168.11.11:2956 uid:0x50001
10:53:42     G711MU ss:off ps:20 rn:1/1 192.168.13.101:42212 192.168.12.13:34008
10:53:42     G711MU ss:off ps:20 rn:1/1 192.168.12.13:34008 192.168.13.101:42212
```

Step	Description
6.4	Verify the SIP trunk provisioned in **Step 3.7** is utilized for Dial-Out calls from Avaya Meeting Exchange. From a SAT session: • Issue the command "**list trace tac <n>**", where **n** is the TAC defined for the trunk group provisioned in **Step 3.7**. • Enter the appropriate touchtone command (for these Application Notes *1) to Dial-Out from Avaya Meeting Exchange and place a call to an endpoint associated with Avaya Communication Manager. ***Note**: The trace below shows a call originating from Avaya Meeting Exchange to a SIP telephone. A SIP telephone was arbitrarily selected for these verification steps, as the configuration presented in these Application Notes allows any station or trunk type (e.g., SIP, H.323, Digital or Analog) on Avaya Communication Manager access (both Dial-In and Dial-Out) to Avaya Meeting Exchange via secure SIP connectivity*.

```
list trace tac 101                                                  Page   1

                                LIST TRACE

time            data

10:54:48     Calling party trunk-group 1 member 1  cid 0x2191
10:54:48     Calling Number & Name NO-CPNumber NO-CPName
10:54:48     active trunk-group 1 member 1  cid 0x2191
10:54:48     G711MU ss:off ps:20 rn:1/1 192.168.13.101:42068 192.168.11.11:3248
10:54:48     xoip: fax:Relay modem:off tty:US 192.168.11.11:3248 uid:0x50001
10:54:48     dial 31001
10:54:48     term station    31001 cid 0x2191
10:54:49     active station    31001 cid 0x2191
10:54:49     G711MU ss:off ps:20 rn:1/1 192.168.13.101:42068 192.168.12.11:34008
10:54:49     G711MU ss:off ps:20 rn:1/1 192.168.12.11:34008 192.168.13.101:42068
```

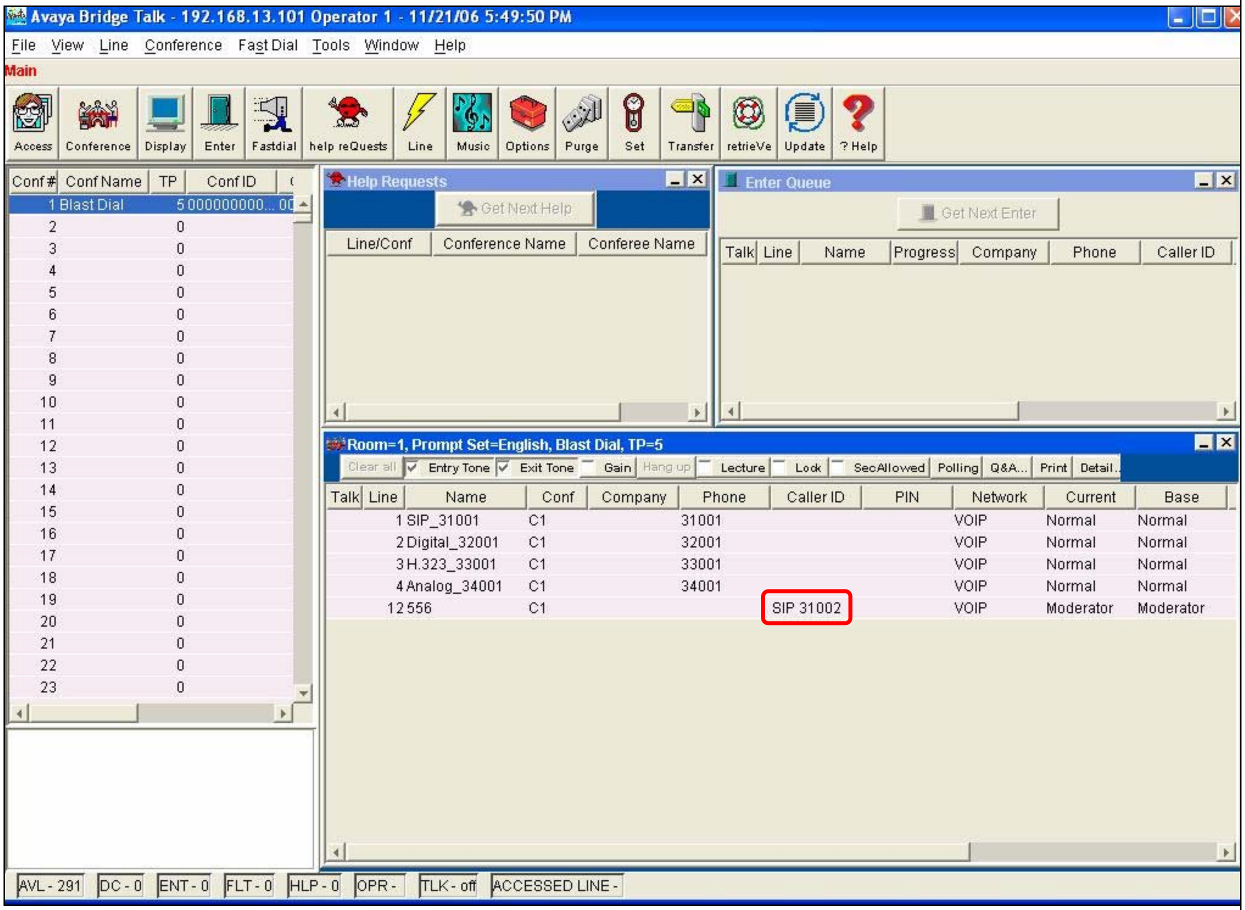
Step	Description
6.5	Verify direct IP-to-IP audio connectivity for the SIP telephone dialing in to Avaya Meeting Exchange. From a SAT session: • Issue the command "**status trunk t/m** (where **t** is the trunk group and **m** is the trunk group member obtained from the procedures in **Step 6.3**)". • The **Audio Connection Type = ip-direct** shows that direct IP-to-IP audio connectivity is enabled for this endpoint. ***Note***: *An* ***Audio Connection Type = ip-tdm*** *would indicate that direct IP-to-IP audio connectivity is* <u>*not*</u> *enabled for an endpoint. For brevity, the procedure to verify direct IP-to-IP audio connectivity is displayed only for a SIP telephone.*

```
status trunk 1/1                                              Page   1 of   2

                              TRUNK STATUS

 Trunk Group/Member: 0001/001             Service State: in-service/active
               Port: T00001            Maintenance Busy? no
 Signaling Group ID:



    Connected Ports: T00032




                   Port     Near-end IP Addr : Port    Far-end IP Addr : Port
        Signaling: 01A0217  192.168. 11. 10  : 5061    192.168. 11. 20 : 5061

G.711MU     Audio:          192.168. 12. 13  : 34008   192.168. 13.101 : 42212
            Video:
      Video Codec:
                                            Authentication Type: None
    Audio Connection Type: ip-direct
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.6</td><td>
Verify SIP trunking between Avaya Communication Manager and the Avaya Meeting Exchange S6200 Conferencing Server via Avaya SIP Enablement Services. This is accomplished by placing calls to and from Avaya Meeting Exchange. This step utilizes the Avaya Bridge Talk application to verify calls to and from Avaya Meeting Exchange are managed correctly, e.g., callers are added/removed from conferences.

Log in to the Avaya Bridge Talk application with the appropriate credentials.
Double-Click the highlighted Conf # to open a Conference Room window.
Verify conference participants are added/removed from conferences by observing the Conference Navigator and/or Conference Room windows.
The Caller ID column in the Conference Room window displays the ANI (SIP 31002) obtained from the procedures in Step 4.3.

Note: The screen below displays the conference invoked in Step 6.3.



</td></tr>
</table>

7. Conclusion

These Application Notes provide administrators with the procedures to configure connectivity between Avaya Communication Manager and the Avaya Meeting Exchange S6200 Conferencing Server via Avaya SIP Enablement Services. This configuration utilizes secure SIP connectivity via TLS based on industry standards.

8. Additional References

The following Avaya references are available at http://support.avaya.com.

1. *Administrator Guide for Avaya Communication Manager*, Issue 2.1, Doc ID 03-300509, May 2006.
2. *Meeting Exchange 4.1 Administration and Maintenance S6200/S6800 Media Server*, Issue 1, Doc ID 04-601168, July 2006.
3. *Avaya Meeting Exchange Groupware Edition Version 4.1 User's Guide for Bridge Talk*, Issue 2, Doc ID 04-600878, July 2006.
4. *SIP Enablement Services Implementation Guide*, Issue 3, Doc ID: 16-300140, February 2006.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com