Avaya Solution & Interoperability Test Lab

Configuring Secure SIP Connectivity Utilizing Transport Layer Security (TLS) Between Avaya Communication Manager and the Avaya Meeting Exchange S6100 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 S6100 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 S6100 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 call flows for accessing a conference on Avaya Meeting Exchange have been verified:

- DirectCallFlow, where conference participants Dial-In and enter a conference as moderator, without entering a passcode.
- BasicCallFlow, where conference participants Dial-In and enter a conference via a passcode.

The following features have been verified for adding participants to an active conference:

- Blast Dial, where a moderator on a conference call can enter a touchtone command (*9 in these Application Notes) to invoke a Blast Dial to a pre-provisioned list of one or more participants. The participants have the option of joining the conference call.
- Originator Dial-Out, where a moderator on a conference call can Dial-Out and add a participant to the conference call.

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**).

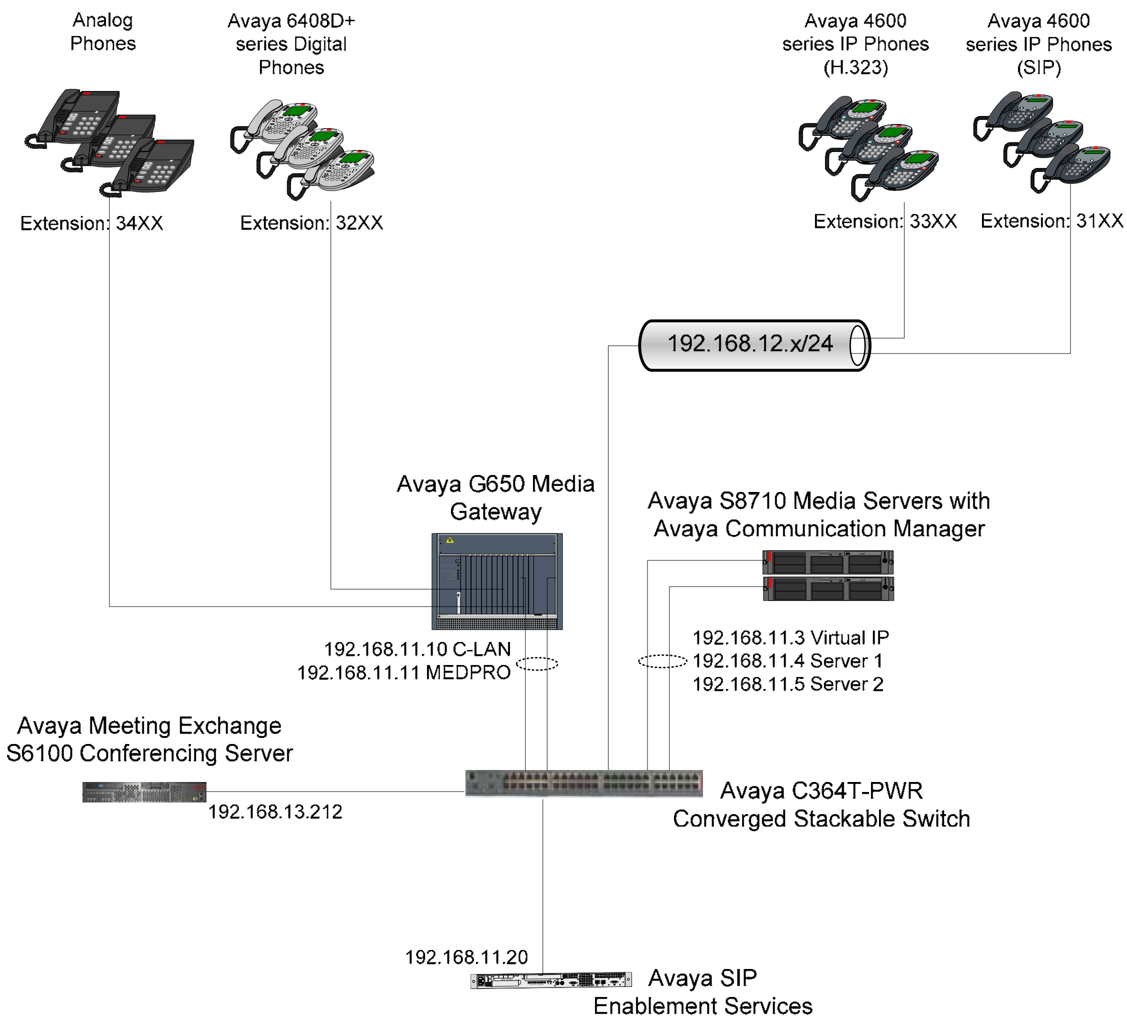


Figure 1: Network Configuration

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**).

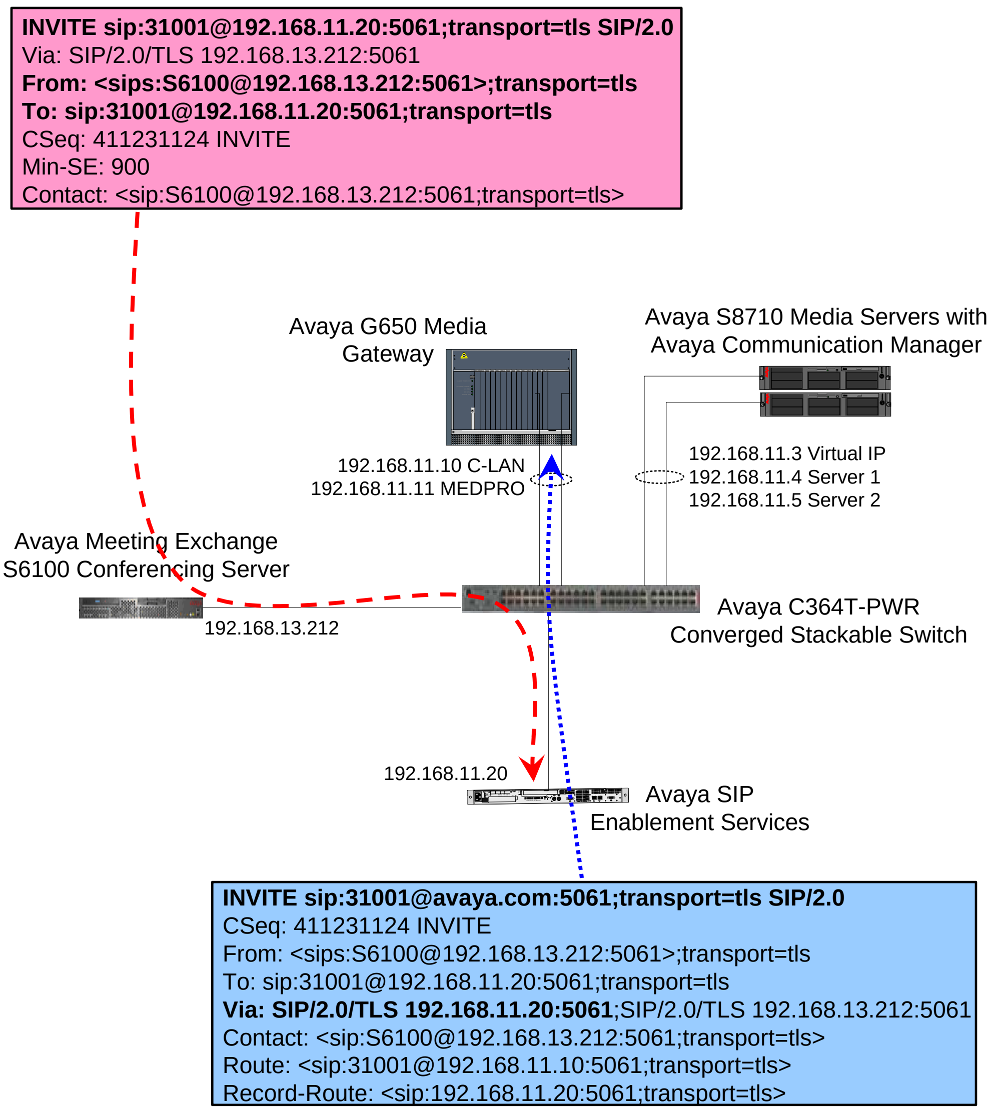


Figure 2: Dial-Out from Avaya Meeting Exchange

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** 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**).

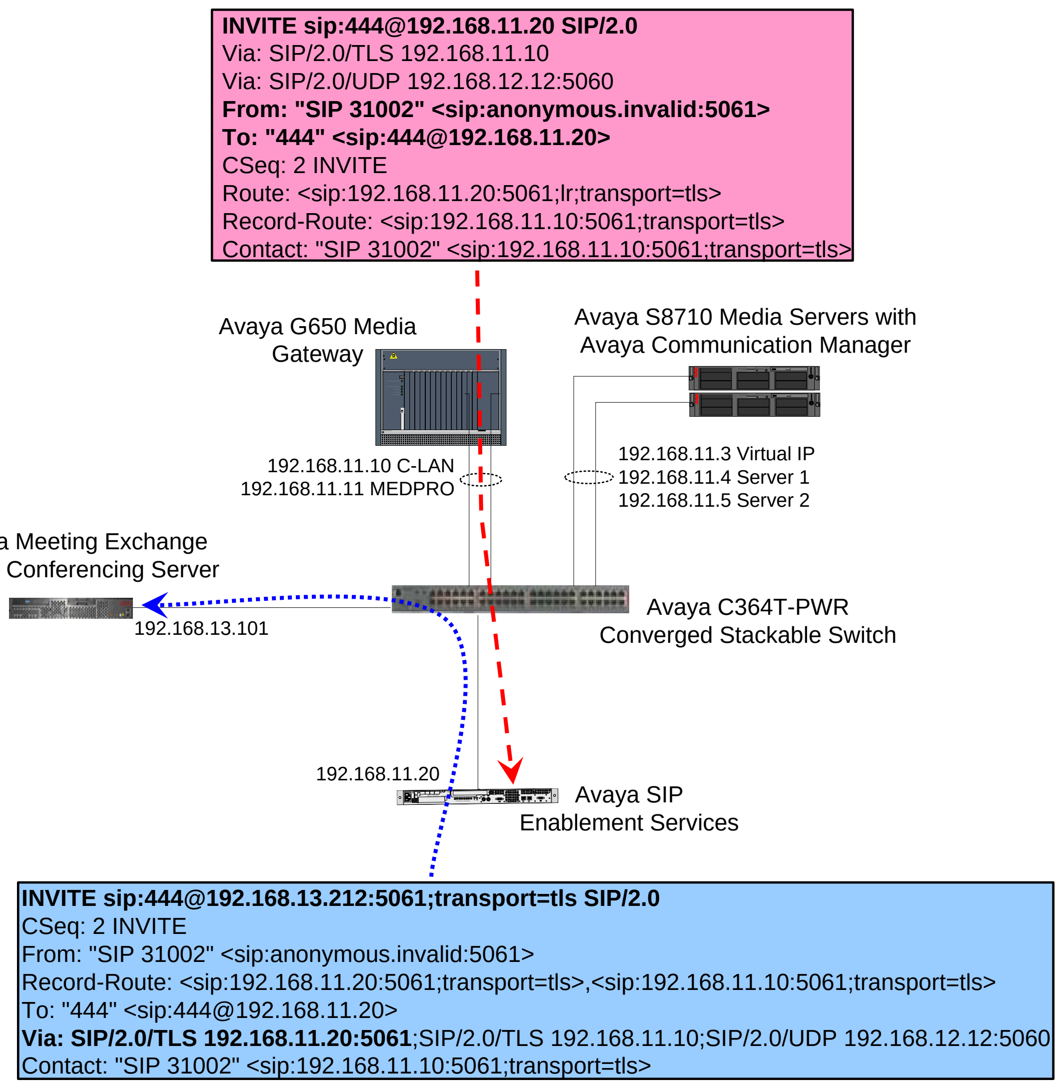


Figure 3: Dial-In to Avaya Meeting Exchange

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 S6100 Conferencing Server	2.0.22.2
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.

Step	Description
3.1	Verify feature 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 SIP 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.*

```
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
```

<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.
	(screen below)

```
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:
  - Set the **Group Type** to **sip**.
  - Set the **Transport Method** to **tls**.
  - Set the **Far-end Listen Port** to **5061**.
  - 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 **4** 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 **401** is used by Avaya Meeting Exchange for **BasicCallFlow** (see **Step 4.5**). • Dialed String **444** is used by Avaya Meeting Exchange for **DirectCallFlow** (see **Step 4.7**).

```
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
    401                   3    3     1        aar          n
    412                   3    3     12       aar          n
    413                   3    3     13       aar          n
    444                   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>

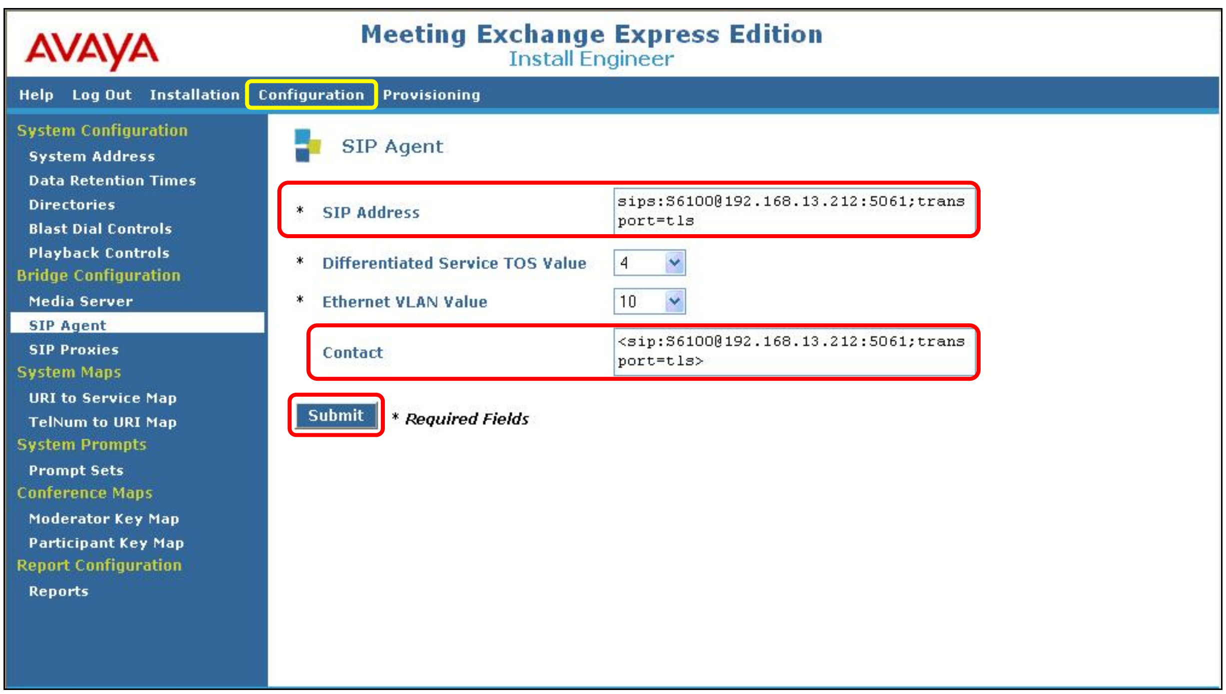
Verify licensing.

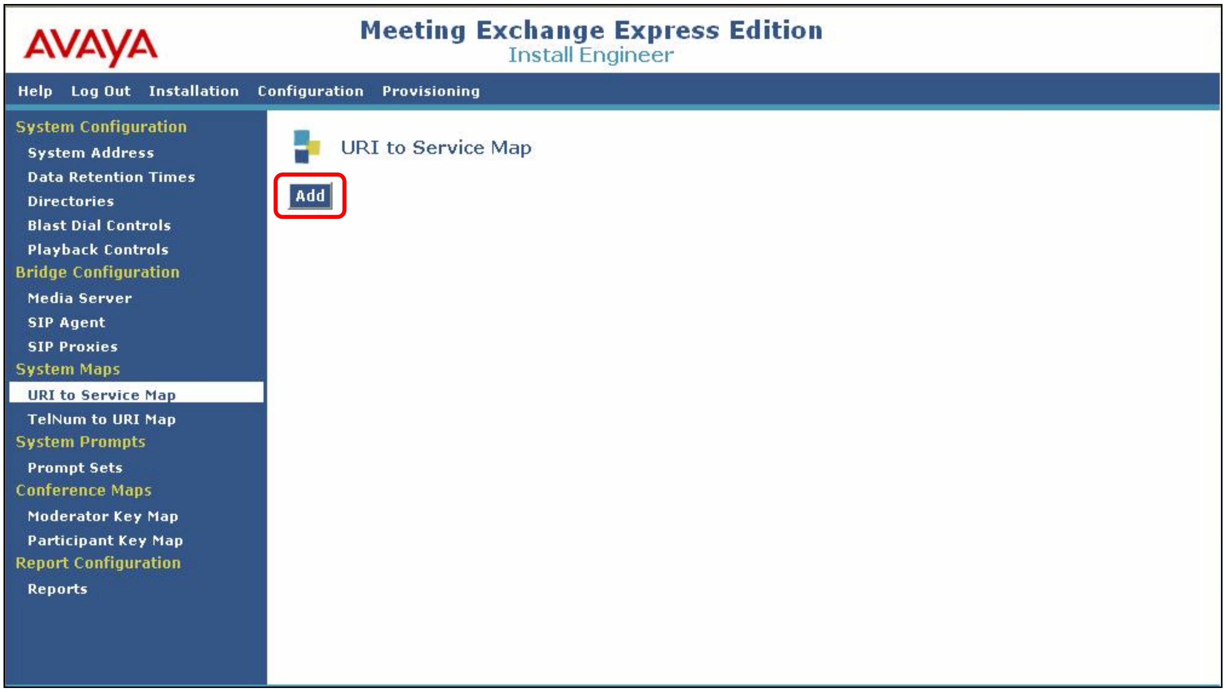
Avaya Meeting Exchange uses Avaya Web License Manager (WebLM) for licensing. WebLM is a Web-based license manager that runs on both Microsoft Windows and UNIX systems. The WebLM server provides a Web User Interface (UI) for license administration that can be accessed from a standard web browser over a secure SSL link.

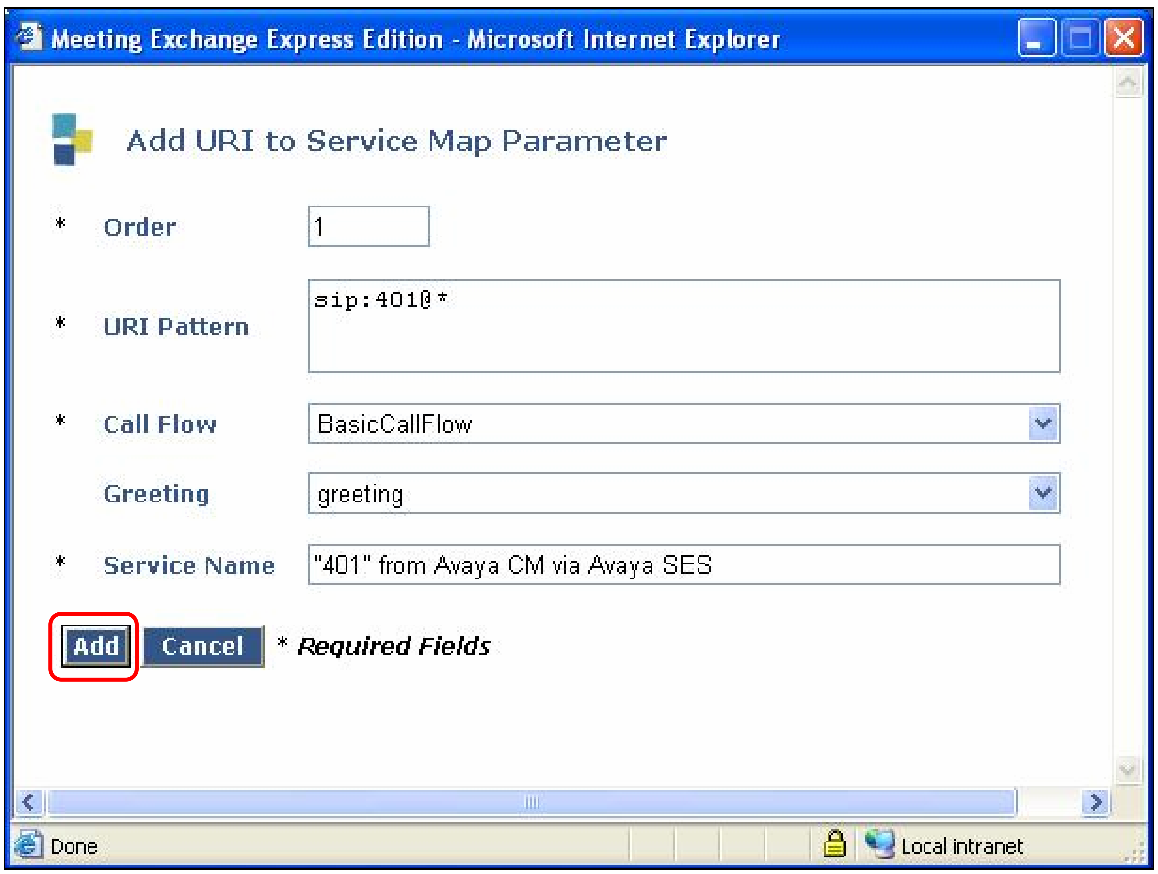
- Open a web browser and enter the following URL: **https://<IP Address of Avaya Meeting Exchange>/WebLM**
- Log in to the WebLM server with the appropriate credentials and verify Avaya Meeting Exchange is licensed for **Meeting Exchange Groupware Edition Ports**.

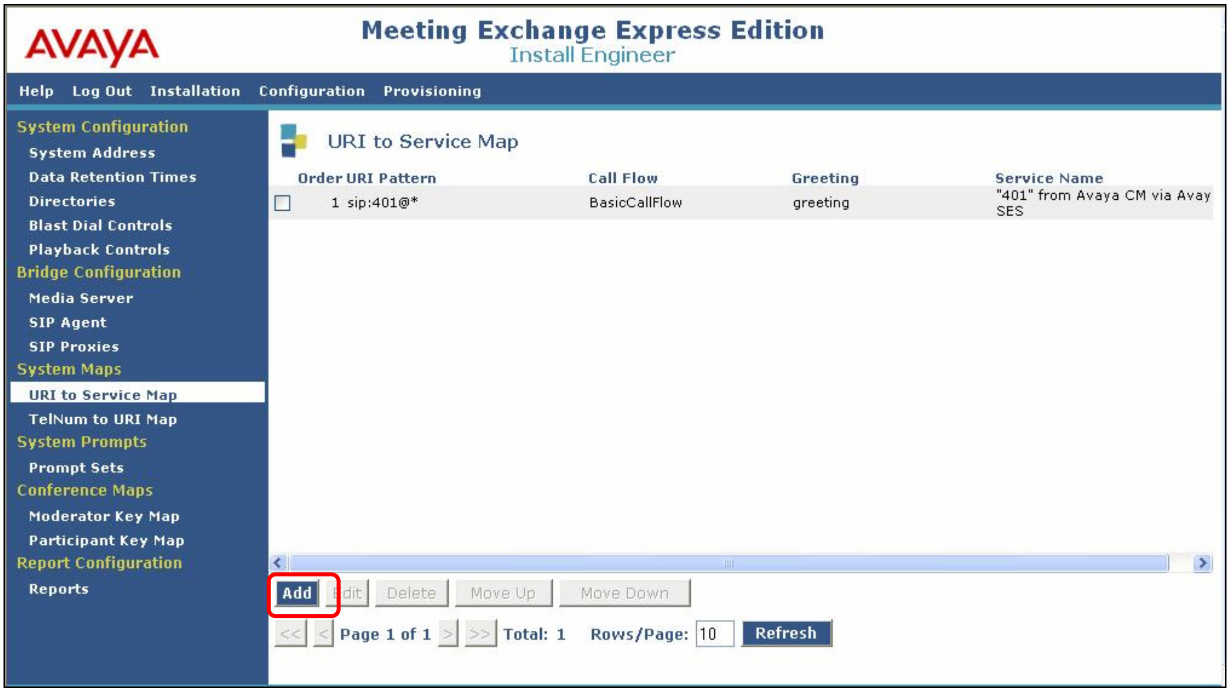
Note: *Each conference participant in a conference on Avaya Meeting Exchange requires one port for the duration of the conference call. The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.*

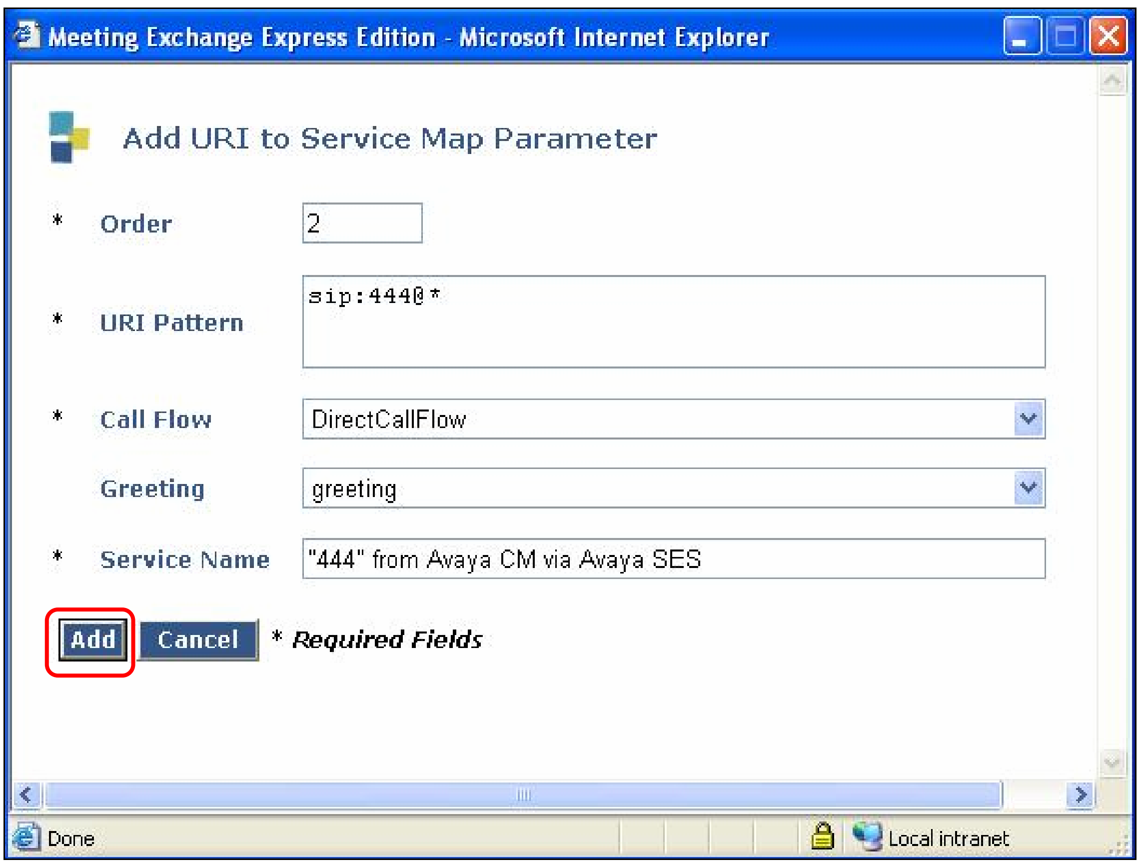
</td></tr>
</table>

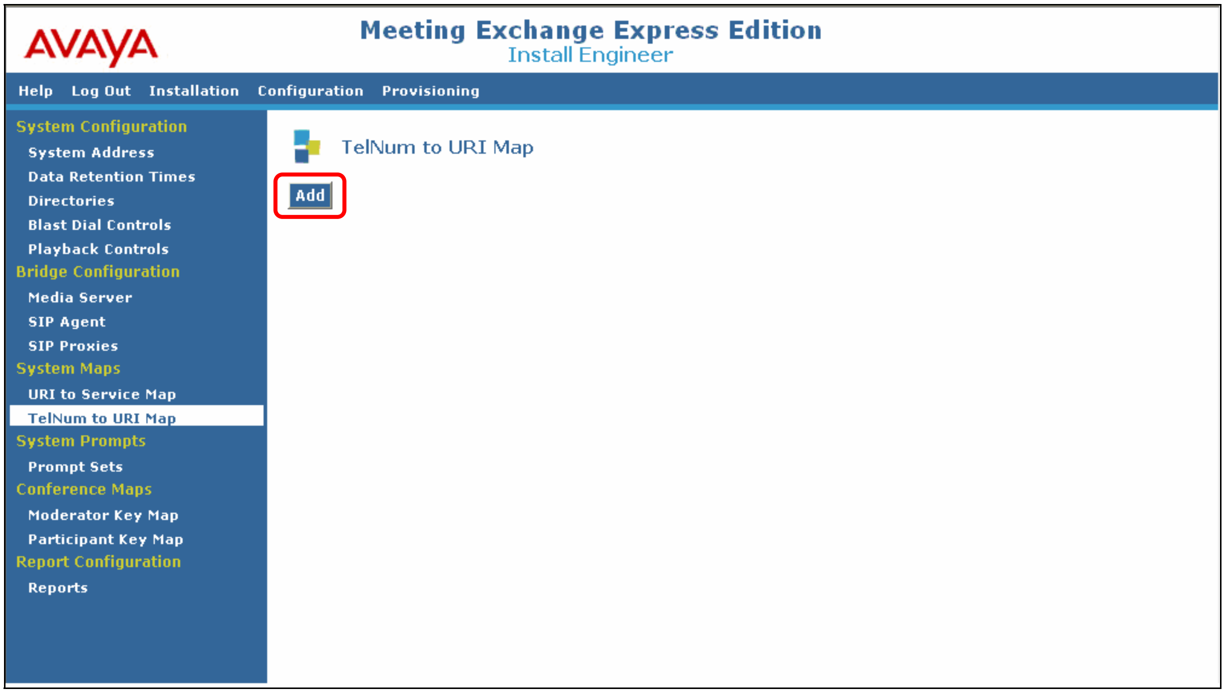
Step	Description
4.2	Administer settings for Avaya Meeting Exchange as follows: • Open a web browser and enter the following URL: **https://<IP Address of Avaya Meeting Exchange>/mx** • Log in to Avaya Meeting Exchange with the appropriate credentials.
4.3	Configure settings that enable secure SIP connectivity between Avaya Meeting Exchange and other SIP User Agents by administering **SIP Agent** parameters as follows: • Click **Configuration** from the S6100 web interface toolbar. • Click **SIP Agent** under **Bridge Configuration**. • Add a **SIP Address** for Avaya Meeting Exchange. To enable secure SIP connectivity utilizing TLS, the entry for the **SIP Address** must contain **sips**, **5061** and **transport=tls**. Avaya Meeting Exchange uses this field to populate the From header in SIP INVITE messages from Avaya Meeting Exchange. • Add a **Contact** address to provide User Agents a Contact to use for acknowledging SIP messages from Avaya Meeting Exchange. To enable secure SIP connectivity utilizing TLS, the entry for the **Contact** address must contain **5061** and **transport=tls**. • Leave all remaining required fields at the default settings. • When finished, click the **Submit** button. 

Step	Description
4.4	To associate incoming calls to Avaya Meeting Exchange with a BasicCallFlow, add a **URI to Service Map** entry follows: • Click **URI to Service Map** under **System Maps**. • Click the **Add** button. 

Step	Description
4.5	Configure a **URI to Service Map Parameter** for a **BasicCallFlow** as follows: • Leave the **Order** field at the default value. *__Note__: Avaya Meeting Exchange parses all __URI to Service Map__ entries, searching for pattern matches in descending order, terminating the search once a pattern is matched. For these Application Notes, order is irrelevant as the patterns for __BasicCallFlow__ and __DirectCallFlow__ (see __Step 4.7__) are mutually exclusive.* • Add a **URI Pattern** to match the pattern of incoming Request URIs in SIP INVITE messages from Avaya SIP Enablement Services. o For example, assume Avaya SIP Enablement Services sends the following URI: **sip:401@192.168.13.212:5061;transport=tls SIP/2.0**. The URI Pattern below is configured to match **sip:401@***, which will match **sip:401@**, then any string following the **@**. • Set the **Call Flow** to **BasicCallFlow** to allow conference participants to enter a conference by entering a passcode. • Enter a descriptive name for the **Service Name** field. • When finished, click the **Add** button. 

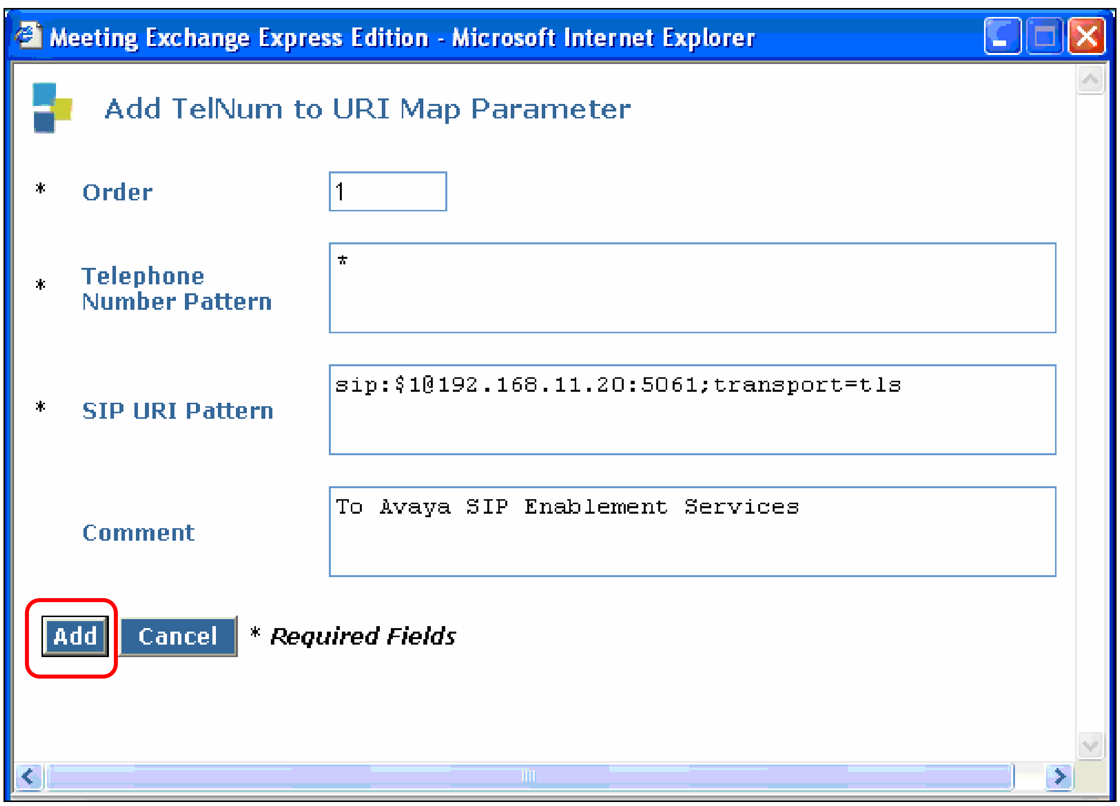
Step	Description
4.6	To associate incoming calls to Avaya Meeting Exchange with a DirectCallFlow, add a **URI to Service Map** entry follows: • Click **URI to Service Map** under **System Maps**. *__Note__: The entry for a __BasicCallFlow__ was configured in __Step 4.5__.* • Click the **Add** button. 

Step	Description
4.7	Configure a **URI to Service Map Parameter** for a **DirectCallFlow** as follows: • Leave the **Order** field at the default value. *__Note__: Avaya Meeting Exchange parses all __URI to Service Map__ entries, searching for pattern matches in descending order, terminating the search once a pattern is matched. For these Application Notes, order is irrelevant as the patterns for __BasicCallFlow__ (see __Step 4.5__) and __DirectCallFlow__ are mutually exclusive.* • Add a **URI Pattern** to match the pattern of incoming Request URIs in SIP INVITE messages from Avaya SIP Enablement Services. o For example, assume Avaya SIP Enablement Services sends the following URI: **sip:444@192.168.13.212:5061;transport=tls SIP/2.0**. The URI Pattern below is configured to match **sip:444@***, which will match **sip:444@**, then any string following the **@**. • Set the **Call Flow** to **DirectCallFlow** to allow conference participants to enter a conference as moderator, without entering a passcode. • Enter a descriptive name for the **Service Name** field. • When finished, click the **Add** button. 

Step	Description
4.8	To configure routing of outbound calls from Avaya Meeting Exchange, add a **TelNum to URI Map** entry as follows: • Click **TelNum to URI Map** under **System Maps**. • Click the **Add** button. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.9</td><td>Configure a TelNum to URI Map Parameter as follows:

Leave the Order field at the default value.
Note: Avaya Meeting Exchange parses all TelNum to URI Map entries, searching for pattern matches in descending order, terminating the search once a pattern is matched. For these Application Notes, order is irrelevant as there is only one entry in the table.
Add a Telephone Number Pattern and SIP URI Pattern to allow for Dial-Out from Avaya Meeting Exchange.
Note: The configuration for these Application Notes sends all Dial-Out traffic (* = match all) to Avaya SIP Enablement Services (192.168.11.20). To enable secure SIP connectivity utilizing TLS for Dial-Out, the SIP URI Pattern must contain 5061 and transport=tls in the entry. Avaya Meeting Exchange will substitute "$1" with the dialed number in outgoing SIP INVITE messages, e.g., if 31001 is dialed, Avaya Meeting Exchange will send a SIP INVITE message with:
sip:31001@192.168.11.20:5061;transport=tls in the SIP URI and To header field.
Enter a descriptive label for the Comment field
When finished, click the Add button.



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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.10</td><td>Following all updates to Avaya Meeting Exchange configured via the web browser, reboot Avaya Meeting Exchange as follows:

Log in to the Avaya Meeting Exchange Server console with the appropriate credentials.
At the command prompt, enter the command init 6.

Note: Rebooting Avaya Meeting Exchange is service impacting.
<hr>
<code>[S6100]> init 6</code></td></tr>
</table>

4.1. Provision Accounts

The following steps provide examples of how to provision accounts on Avaya Meeting Exchange. Accounts are utilized in conjunction with the Call Flows provisioned in **Step 4.5** and **Step 4.7**.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.11</td><td>To utilize the DirectCallFlow provisioned in Step 4.7, administer an Account CSV file as follows:

Log in to the Avaya Meeting Exchange Server console with the appropriate credentials.
Create an Account CSV file with the format of the myAccount.csv shown below.
Note: The myAccount.csv file is correlated to the URI Pattern provisioned in Step 4.7 via the def_modpass_code entry. The myAccount.csv file is also correlated to the myBlastDial.csv file provisioned in Step 4.12 via the import_tag entry.

<pre>
[S6100]> cat /usr/tmp/csvFiles/myAccount.csv
account_note,def_confpass_code,def_modpass_code,mx_conf_size,mx_confdur_mins,import_
tag,disabled_ind,logon_password,contact_name,contact_phone,contact_email,import_tag,
conf_profile_id,message_profile_id
"DirectDial_444","1444","444","250","30","444_Tag","f","444","CSV Account
444","1234551444","csv@account444.com","CSV_Company_5","5",""
</pre>

Write the myAccount.csv file to the database by running the bulk-loader.sh utility as follows:

cd to /usr/crystal/bulkloader.
At the command prompt, enter the command shown below.

<pre>
[S6100]> sh bulk-loader.sh -A/usr/tmp/csvFiles/myAccount.csv
com.avaya.crystal.common.Logger.LogDir not set, setting log location to default ...
com.avaya.crystal.common.Logger.LogDir set to: /usr/crystal/config/../logs
Log configuration file [/usr/crystal/config/CrystalLog.xml] loaDING.
Log configuration file [/usr/crystal/config/CrystalLog.xml] was loaded.
Write Account File :All 1 row(s) were successfull
</pre></td></tr>
</table>

Step	Description
4.12	To enable the Blast Dial feature, administer a Blast Dial CSV file as follows: • Create a Blast Dial CSV file with the format of the **myBlastDial.csv** shown below. ***Note****: The* ***myBlastDial.csv*** *file is correlated to the* ***myAccount.csv*** *file provisioned in* ***Step 4.11*** *via the* ***reservation_import_tag*** *entry. The* ***contact_phone*** *variable is the number dialed when the Blast Dial feature is invoked.*

	`[S6100]> cat /usr/tmp/csvFiles/myBlastDial.csv`
	`reservation_import_tag,contact_name,contact_phone,contact_email,person_import_tag`
	`"444_Tag","BlastDialContact4","31001","csv@blastdialcontact4.com","PersonImportTag4"`
	`"444_Tag","BlastDialContact5","32001","csv@blastdialcontact5.com","PersonImportTag5"`
	`"444_Tag","BlastDialContact6","32002","csv@blastdialcontact6.com","PersonImportTag6"`
	`"444_Tag","BlastDialContact7","33002","csv@blastdialcontact7.com","PersonImportTag7"`

	• Write the **myBlastDial.csv** file to the database by running the **bulk-loader.sh** utility as follows:
	  o cd to **/usr/crystal/bulkloader**.
	  o At the command prompt, enter the command shown below.

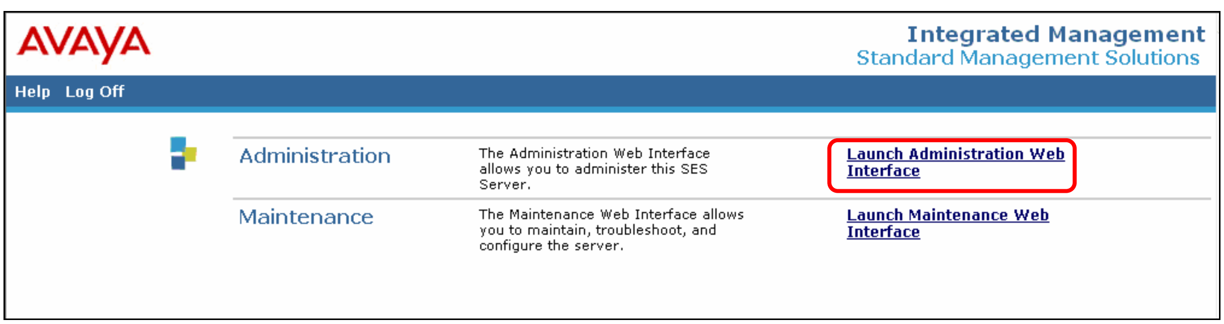
	`[S6100]> sh bulk-loader.sh -B/usr/tmp/csvFiles/myBlastDial.csv`
	`com.avaya.crystal.common.Logger.LogDir not set, setting log location to default ...`
	`com.avaya.crystal.common.Logger.LogDir set to: /usr/crystal/config/../logs`
	`Log configuration file [/usr/crystal/config/CrystalLog.xml] loaDING.`
	`Log configuration file [/usr/crystal/config/CrystalLog.xml] was loaded.`
	`Write BlastDial File :All 4 row(s) were successfull`

5. Avaya SIP Enablement Services Configuration

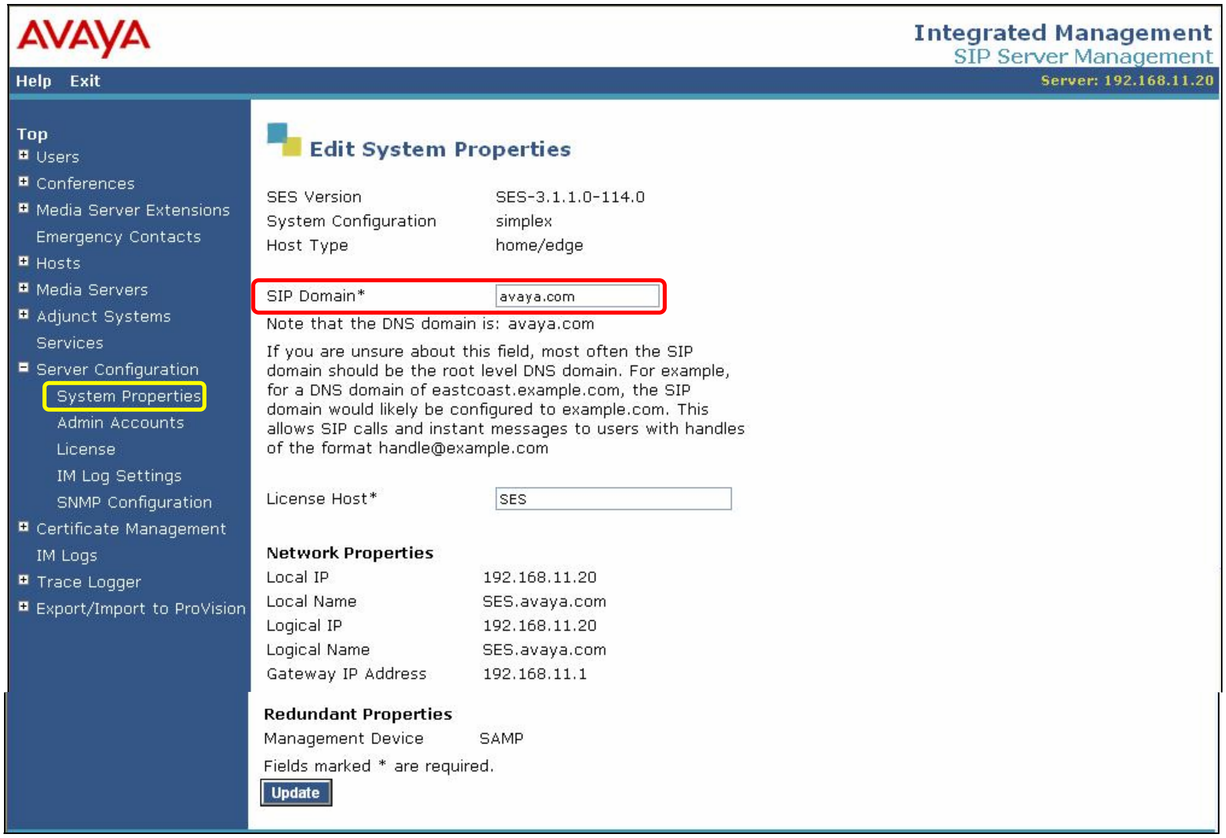
This section describes the steps for configuring Avaya SIP Enablement Services to enable secure SIP connectivity between Avaya Communication Manager and Avaya Meeting Exchange utilizing TLS.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.1</td><td>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.

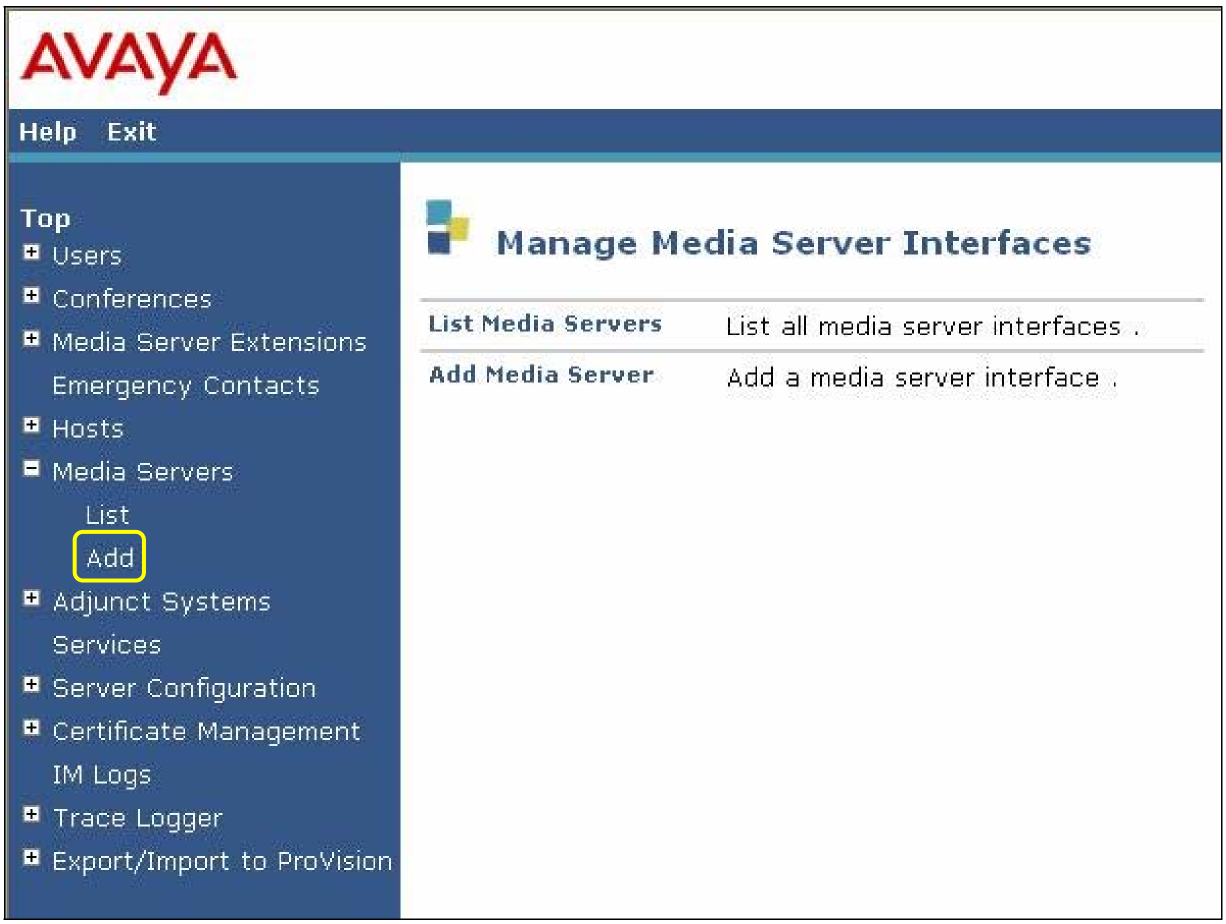
</td></tr>
<tr><td>5.2</td><td>Click Launch Administration Web Interface.


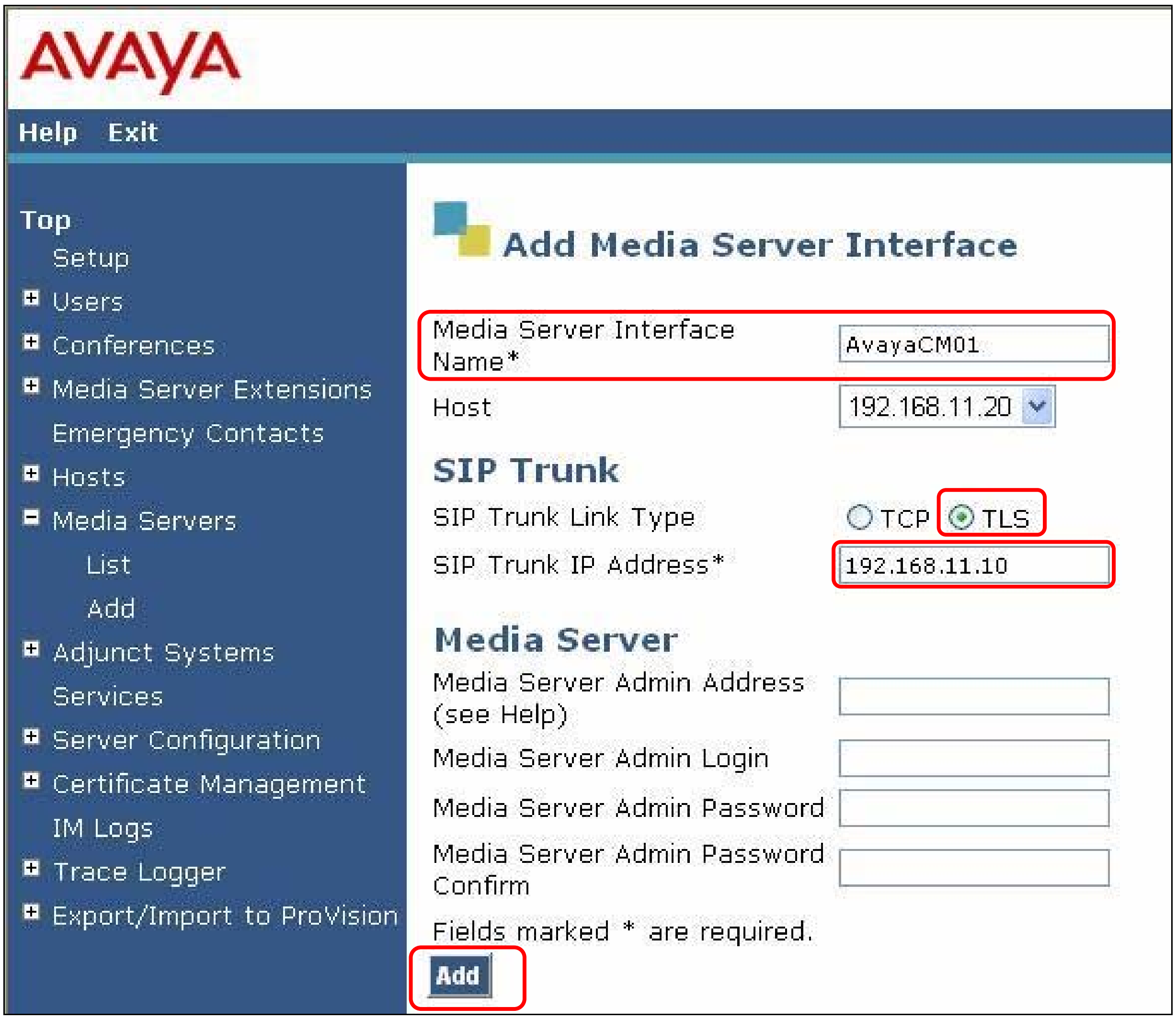
</td></tr>
</table>

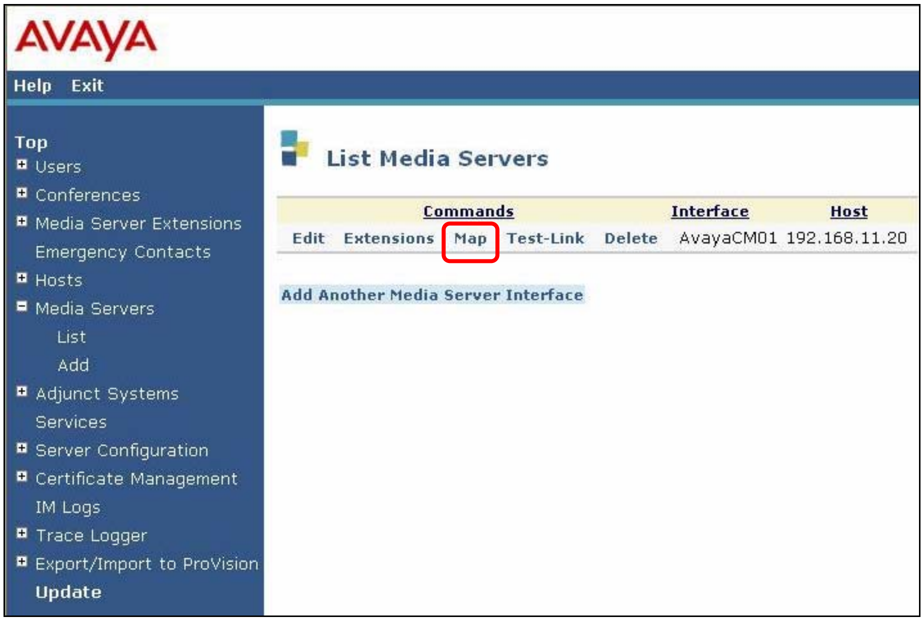
Step	Description
5.3	Verify the **System Properties** for Avaya SIP Enablement Services as follows. From the Administration Web Interface: • Click the **+** sign to expand the options under **Server Configuration**. • Click **System Properties**. • Verify the **SIP Domain** matches the authoritative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

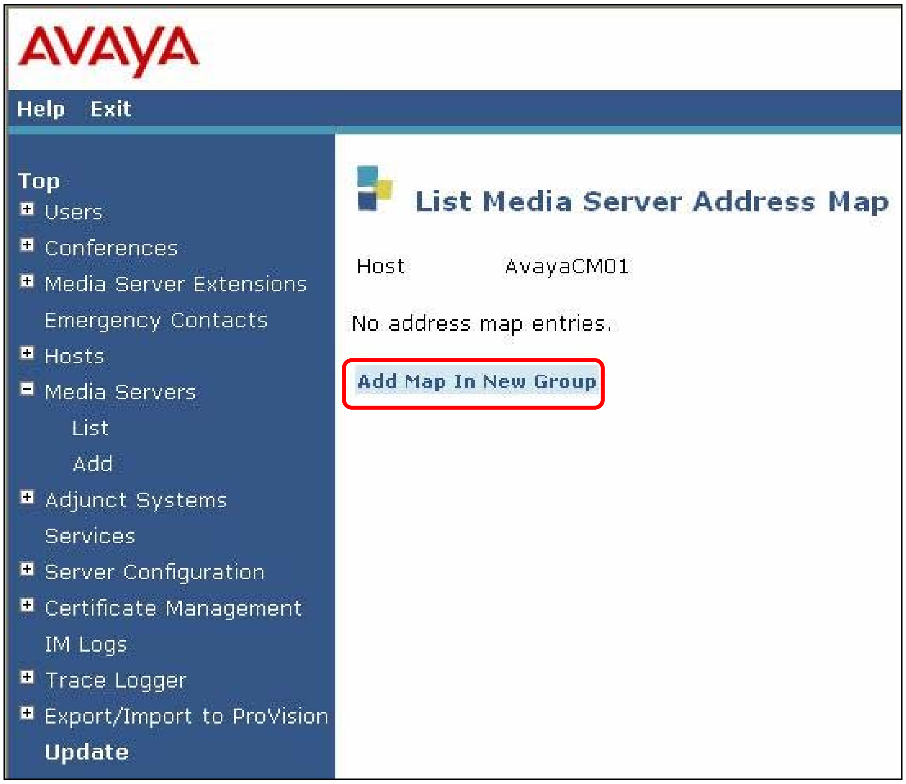
5.1. Enable Dial-Out from Avaya Meeting Exchange

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**).

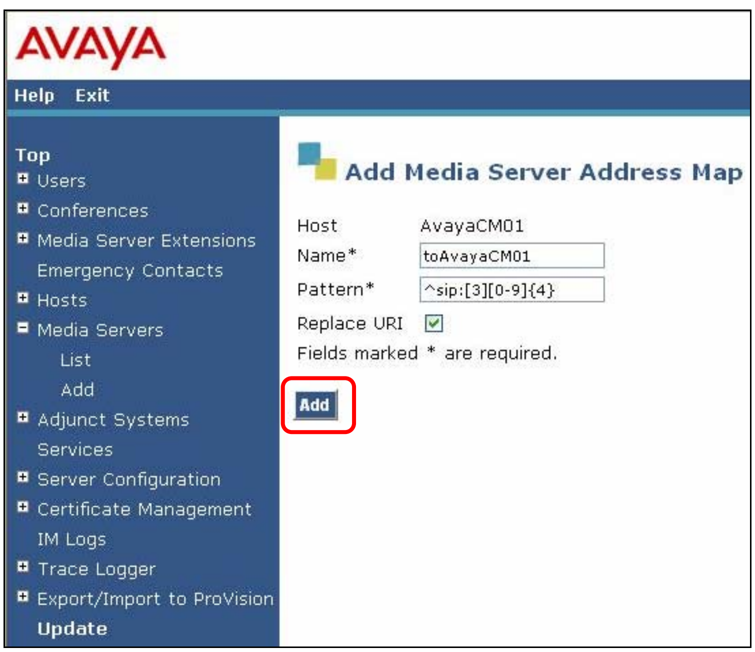
Step	Description
5.4	To enable secure SIP trunking between Avaya SIP Enablement Services and Avaya Communication Manager, add a **Media Server** corresponding to Avaya Communication Manager as follows. From the Administration Web Interface: • Click the **+** sign to expand the options under **Media Servers**.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

Step	Description
5.5	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. o [***Not Shown***] *Click the **Continue** button on the confirmation page*. 

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**. 

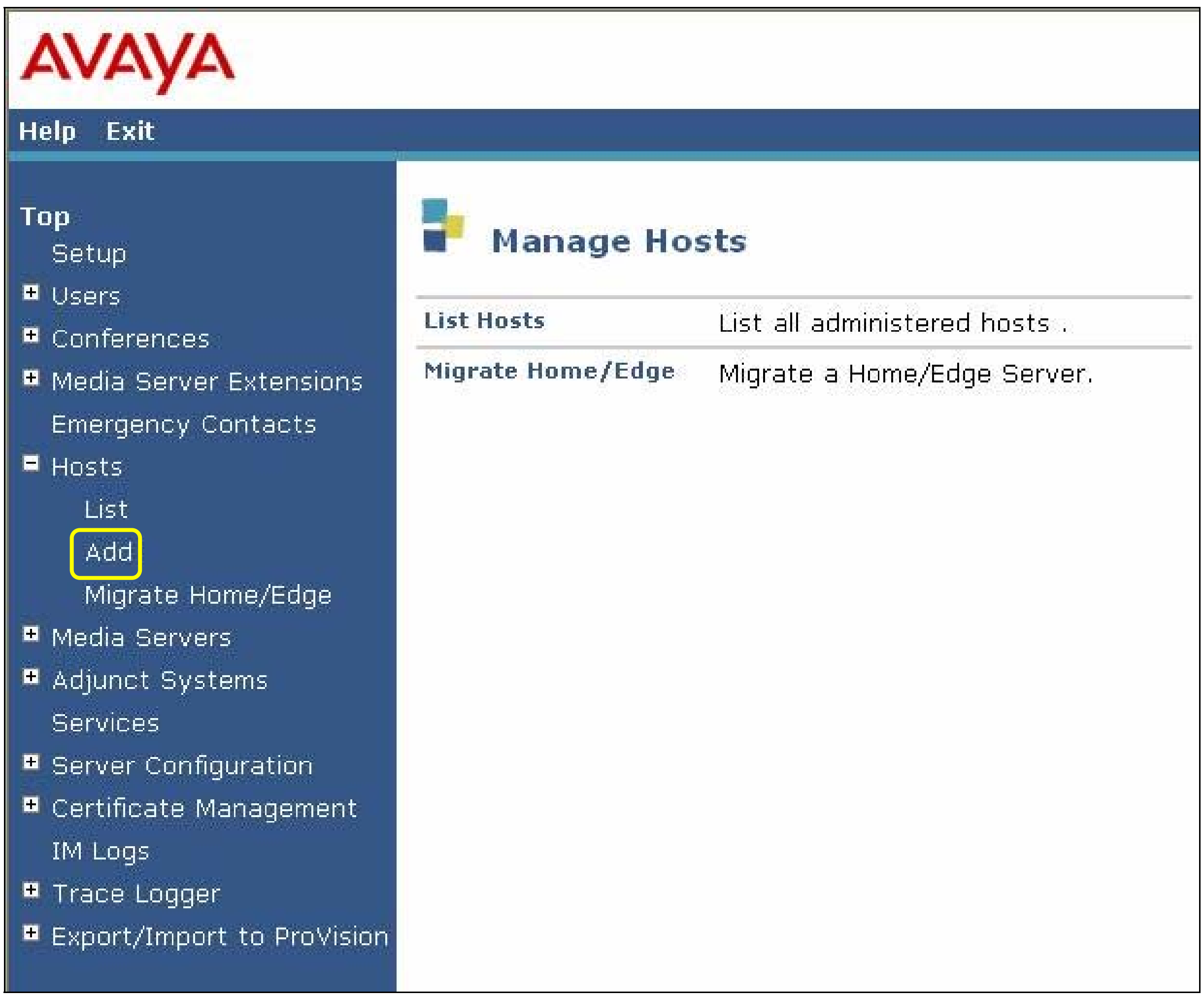
Step	Description

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}*** *matches 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**.* 

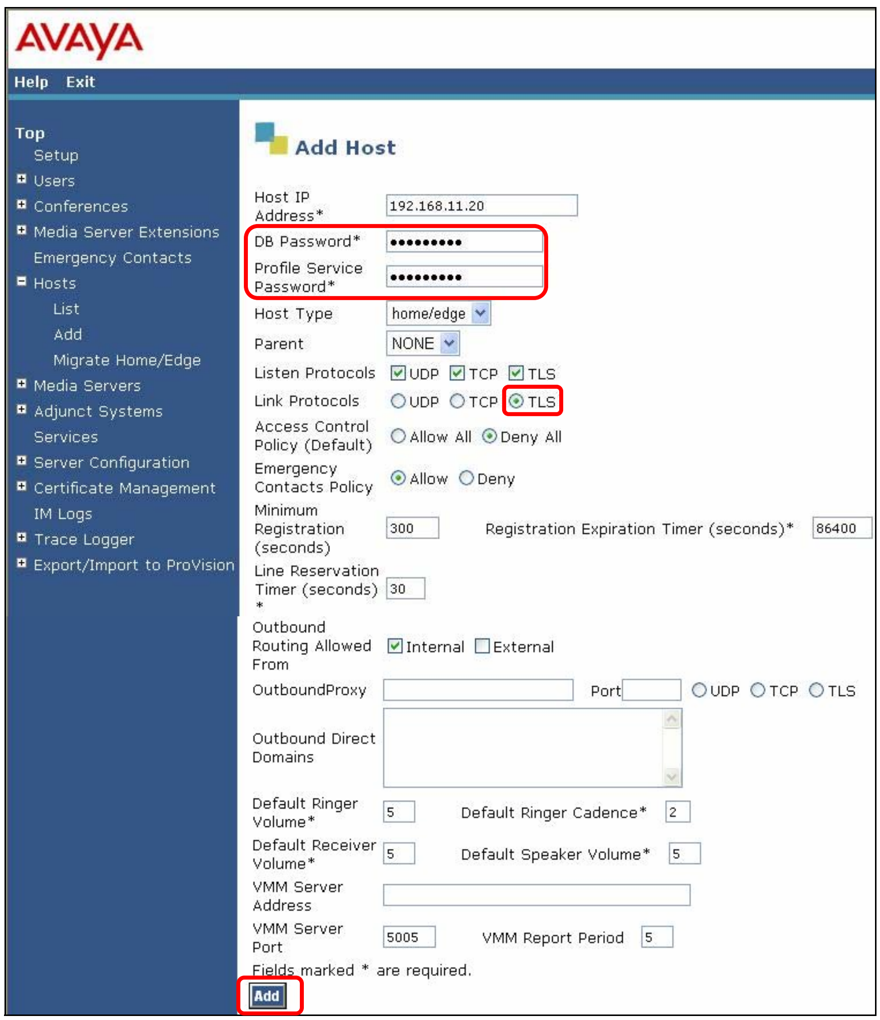
5.2. Enable Dial-In to Avaya Meeting Exchange

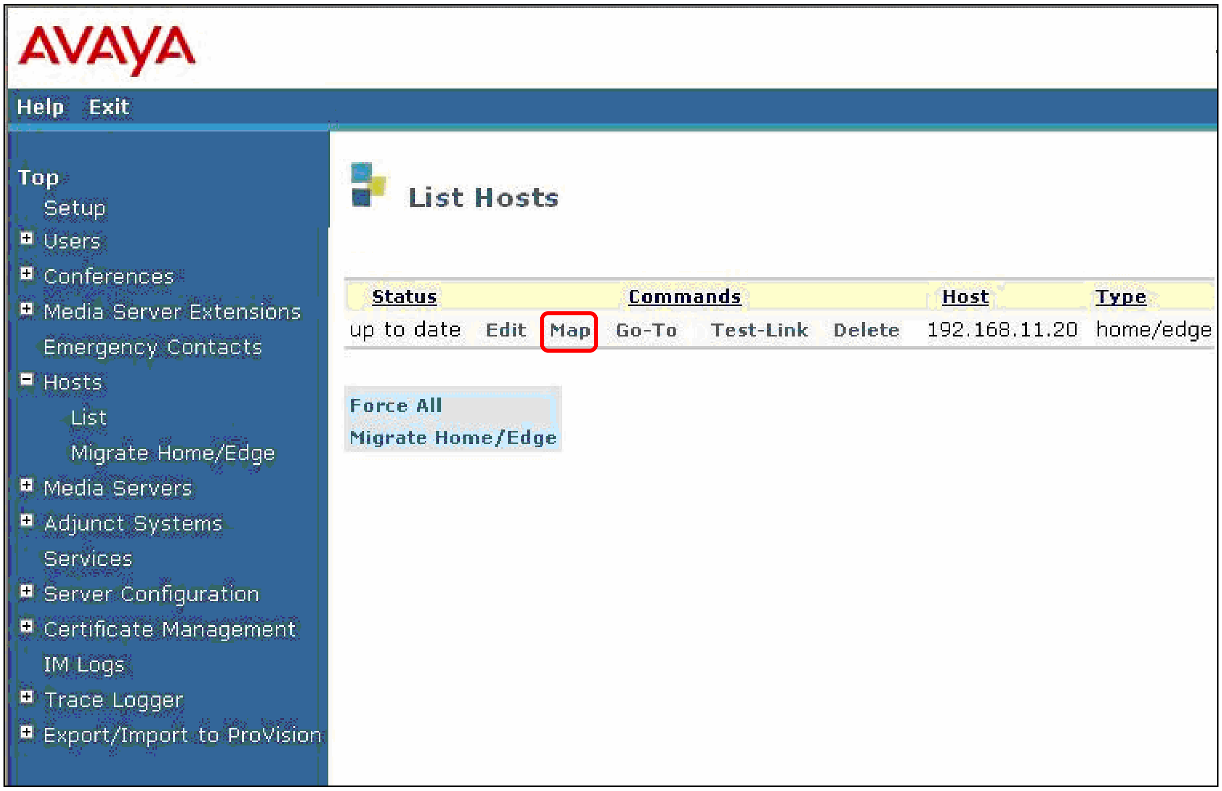
The following steps enable secure SIP trunking between Avaya SIP Enablement Services and Avaya Meeting Exchange. This will allow Dial-In to Avaya Meeting Exchange from Avaya Communication Manager via Avaya SIP Enablement Services (see **Figure 3**).

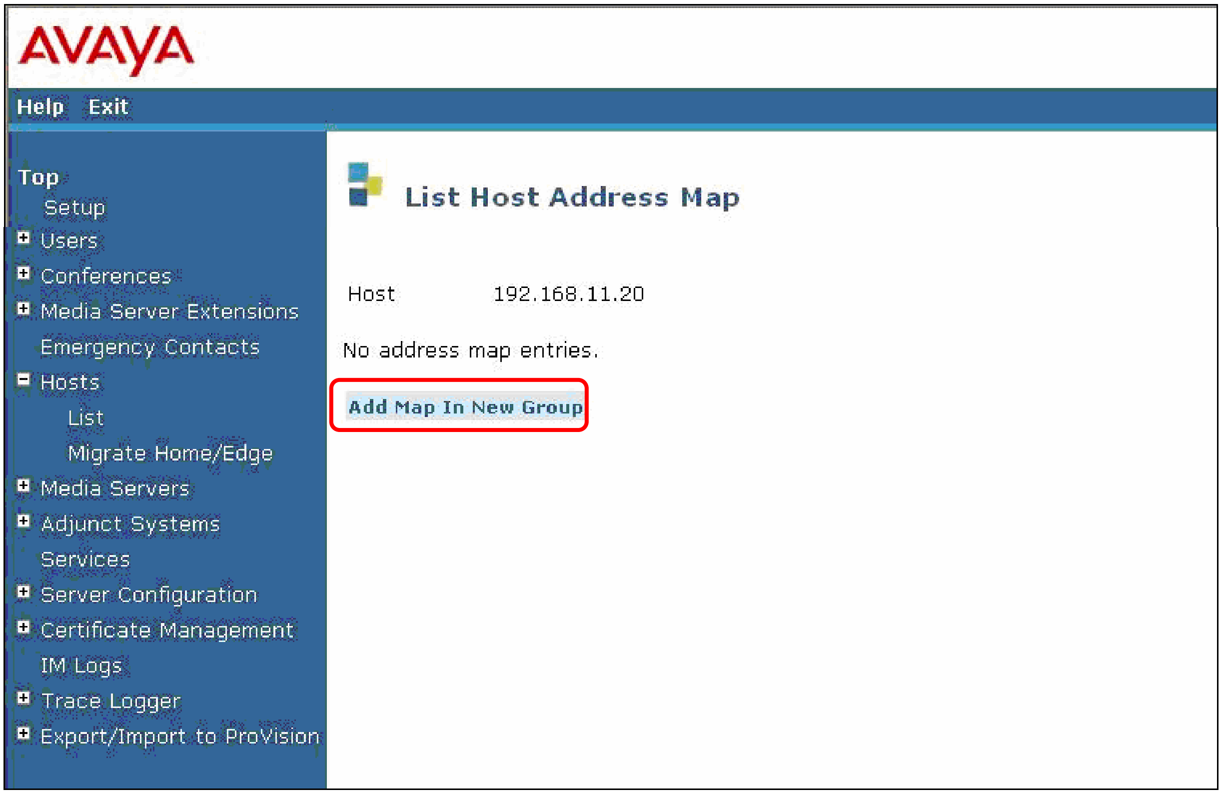
Step	Description
5.10	To enable secure SIP trunking between Avaya SIP Enablement Services and Avaya Meeting Exchange, add a **Host** corresponding to Avaya SIP Enablement Services as follows. From the Administration Web Interface: • Click the **+** sign to expand the options under **Hosts**. • Click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

Step	Description

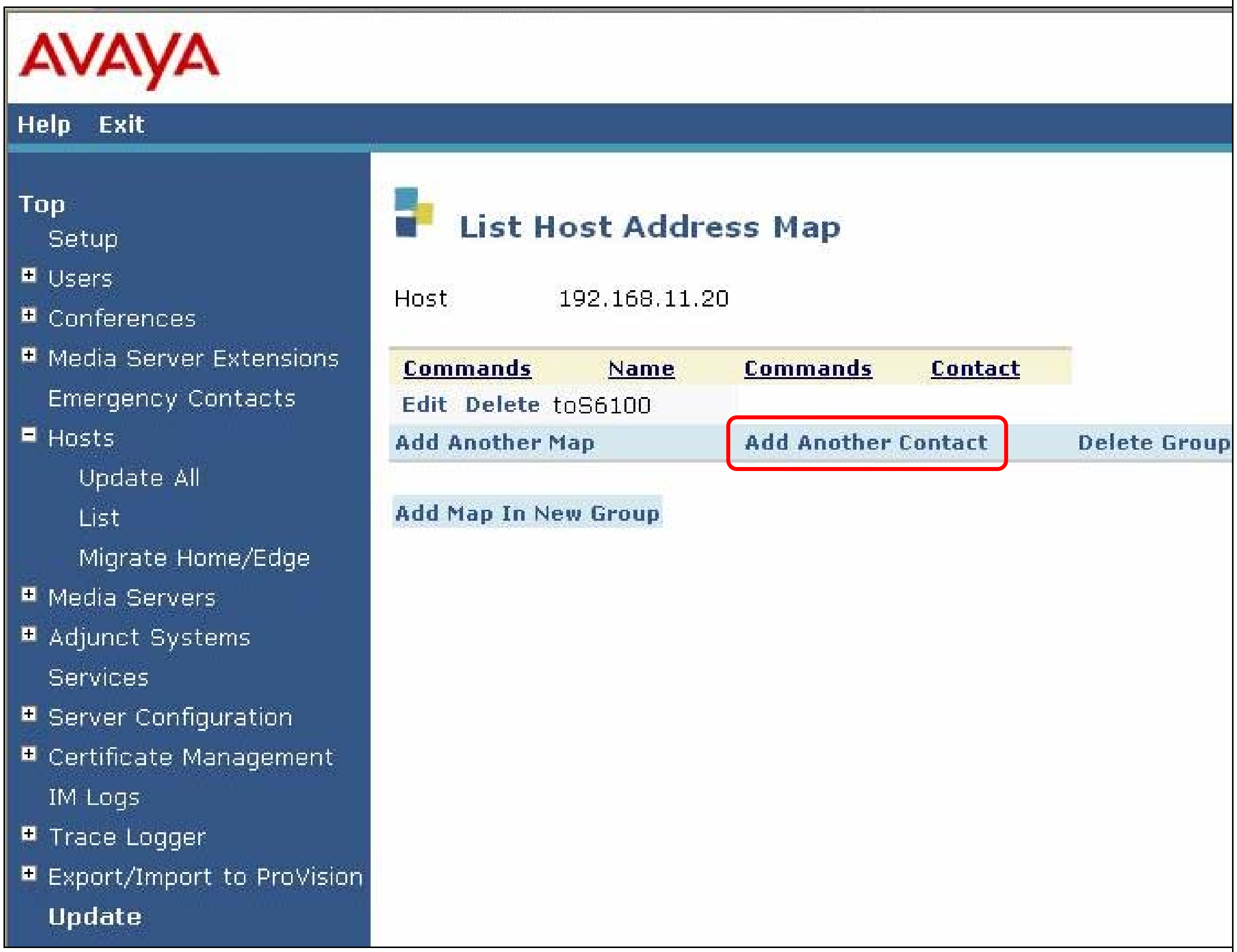
5.11	The **Add Host** page is displayed.
	
	To enable secure SIP connectivity for this host, provision as follows:
	• Enter the password assigned to the database at installation for the **DB Password** field.
	• Enter a password which uniquely identifies Avaya SIP Enablement Services for intra- and inter-proxy communication for the **Profile Service Password** field.
	• Select **TLS** from the available **Link Protocols**, which is consistent with the SIP agent configuration defined for Avaya Meeting Exchange in **Step 4.3**.
	• 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.*

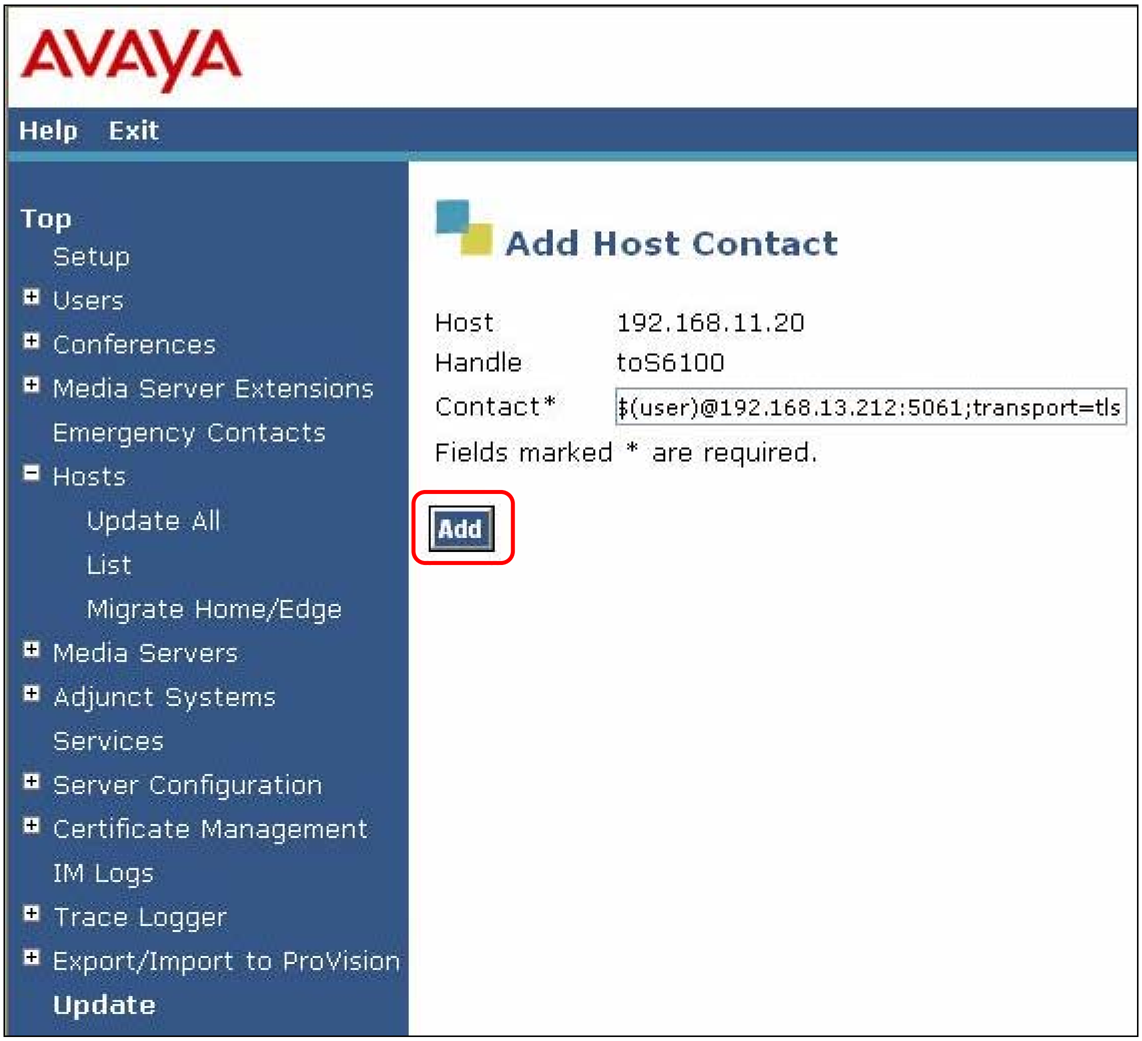


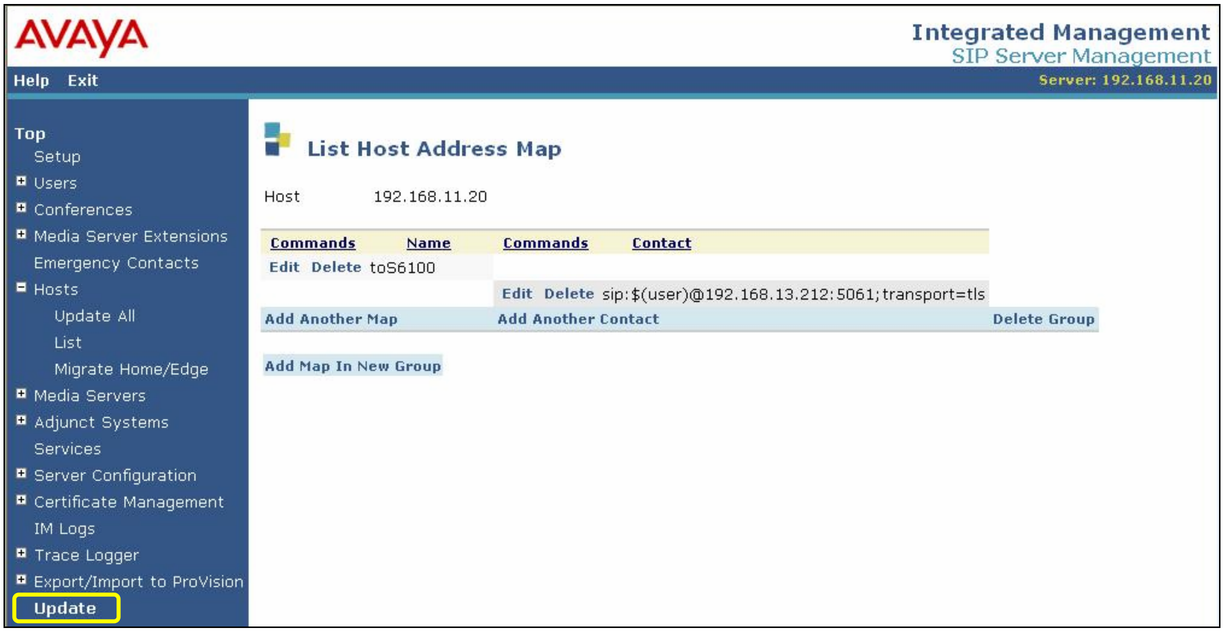
Step	Description
5.12	To route SIP traffic to Avaya Meeting Exchange, provision a **Host Address Map** for the corresponding host configured in **Step 5.11** by clicking **Map**. 

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 flows provisioned for Avaya Meeting Exchange in **Step 4.5** and **Step 4.7**. *__Note__: The __Pattern__ __^sip:[4][0-9]{2}__ matches the string __sip:4__ (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**. 

Step	Description
5.16	The **Add Host Contact** page is displayed. • To enable secure SIP connectivity to Avaya Meeting Exchange, enter **sip:$(user)@192.168.13.212:5061;transport=tls** in the **Contact** field. *__Note__: The IP address, port number and transport protocol are consistent with the SIP agent configuration for Avaya Meeting Exchange defined in __Step 4.3__. Avaya SIP Enablement Services substitutes "__$(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.* 

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. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.18</td><td>
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 192.168.13.212 –n 192.168.11.20 –c S6100
```

• 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
--------------------------+---------------------------+-------------------------
192.168.13.212            | 192.168.11.20             | S6100
```
</td></tr>
<tr><td>5.19</td><td>
To apply the administration defined in **Step 5.18**, click on **Update** on the left side of the page on the web browser interface.


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

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 verify. • Verify that all members in the trunk group are **in-service/idle**.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.2</td><td>Verify the SIP trunk provisioned in Step 3.7 is utilized when a call from an Avaya Communication Manager 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 444 to enter a conference as moderator via the DirectCallFlow scenario provisioned in Section 4.
Note: The trace below shows a SIP telephone dialing in to Avaya Meeting Exchange via a DirectCallFlow. 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.</td></tr>
</table>

```
list trace tac 101                                                   Page   1

                                LIST TRACE

time            data

16:13:40     Calling party station    31002 cid 0x5f
16:13:40     Calling Number & Name 31002 SIP 31002
16:13:40     active station    31002 cid 0x5f
16:13:40     G711MU ss:off ps:20 rn:1/1 192.168.12.13:34008 192.168.11.11:2512
16:13:40     xoip: fax:Relay modem:off tty:US 192.168.11.11:2512 uid:0x50020
16:13:40     dial 444 route:AAR
16:13:40     term trunk-group 1    cid 0x5f
16:13:40     dial 444 route:AAR
16:13:40     route-pattern  1 preference 1  cid 0x5f
16:13:40     seize trunk-group 1 member 40  cid 0x5f
16:13:40     Calling Number & Name NO-CPNumber SIP 31002
16:13:41     Proceed trunk-group 1 member 40  cid 0x5f
16:13:41     active trunk-group 1 member 40  cid 0x5f
16:13:41     G711MU ss:off ps:20 rn:1/1 192.168.13.212:42038 192.168.11.11:2516
16:13:41     xoip: fax:Relay modem:off tty:US 192.168.11.11:2516 uid:0x50028
16:13:41     G711MU ss:off ps:20 rn:1/1 192.168.13.212:42038 192.168.12.13:34008
16:13:41     G711MU ss:off ps:20 rn:1/1 192.168.12.13:34008 192.168.13.212:42038
```

Step	Description
6.3	Verify the SIP trunk provisioned in **Step 3.7** is utilized for Dial-Out calls from 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**. • Enter the appropriate touchtone command (for these Application Notes *9) to invoke a Blast Dial as provisioned is **Section 4**. ***Note***: *The trace below shows a call originating from Avaya Meeting Exchange to a SIP telephone. For brevity, only the trace for the SIP telephone is displayed*.

```
list trace tac 101                                                    Page   1

                                LIST TRACE

time            data

16:14:56     Calling party trunk-group 1 member 1  cid 0x2182
16:14:56     Calling Number & Name NO-CPNumber NO-CPName
16:14:56     active trunk-group 1 member 1  cid 0x2182
16:14:56     G711MU ss:off ps:20 rn:1/1 192.168.13.212:42054 192.168.11.11:3116
16:14:56     xoip: fax:Relay modem:off tty:US 192.168.11.11:3116 uid:0x50001
16:14:56     dial 31001
16:14:56     term station    31001 cid 0x2182
16:14:57     active station    31001 cid 0x2182
16:14:57     G711MU ss:off ps:20 rn:1/1 192.168.13.212:42054 192.168.12.11:34008
16:14:57     G711MU ss:off ps:20 rn:1/1 192.168.12.11:34008 192.168.13.212:42054
```

Step	Description
6.4	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 6.2**)". • 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 screen to verify direct IP-to-IP audio connectivity is displayed only for a SIP telephone.*

```
status trunk 1/40                                               Page   1 of   2

                              TRUNK STATUS

 Trunk Group/Member: 0001/040              Service State: in-service/active
               Port: T00040             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. 13.212 : 42038
            Video:
      Video Codec:
                                            Authentication Type: None
    Audio Connection Type: ip-direct
```

Step	Description
6.5	Verify that calls to and from Avaya Meeting Exchange are managed correctly, e.g., callers are added/removed from conferences. This is verified by the following procedures: • Log in to the Avaya Meeting Exchange Server console with the appropriate credentials. • At the command prompt, enter the command: **watch -t -n 5 -d "ipinfo -l |egrep -ci active"** o This command provides a real time, continuous update of port utilization on Avaya Meeting Exchange.

7. Conclusion

These Application Notes provide administrators with the procedures to configure connectivity between Avaya Communication Manager and the Avaya Meeting Exchange S6100 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. *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