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 - 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. Secure SIP connectivity is enabled by utilizing the Transaction Layer Security (TLS) authentication and encryption standard providing customers with a secure standards based solution. This configuration leverages the flexibility offered by Avaya Communication Manager to support a rich set of conferencing options provided by 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. Secure SIP connectivity is enabled by utilizing the Transaction Layer Security (TLS) authentication and encryption standard providing customers with a secure standards based solution.

This configuration leverages the inherent flexibility of protocols supported on Avaya Communication Manager by enabling any station or trunk type associated with Avaya Communication Manager to interoperate with Avaya Meeting Exchange. Thus, this configuration will allow access to a rich selection of conferencing features supported on 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 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 feature access code (e.g., ***9**, see **Step 6.2**) to Dial-Out 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.

Note: The convention for Dial-In/Dial-Out assigns Avaya Meeting Exchange as the point of reference; e.g., *Dial-In to Avaya Meeting Exchange*, *Dial-Out from Avaya Meeting Exchange*.

These Application Notes will provide the administrative steps for configuring Avaya Communication Manager to interoperate with Avaya Meeting Exchange via secure SIP connectivity utilizing TLS/TCP (see **Figure 1**).

Note: In this configuration, Avaya SIP Enablement Services is strictly utilized for registering SIP endpoints.

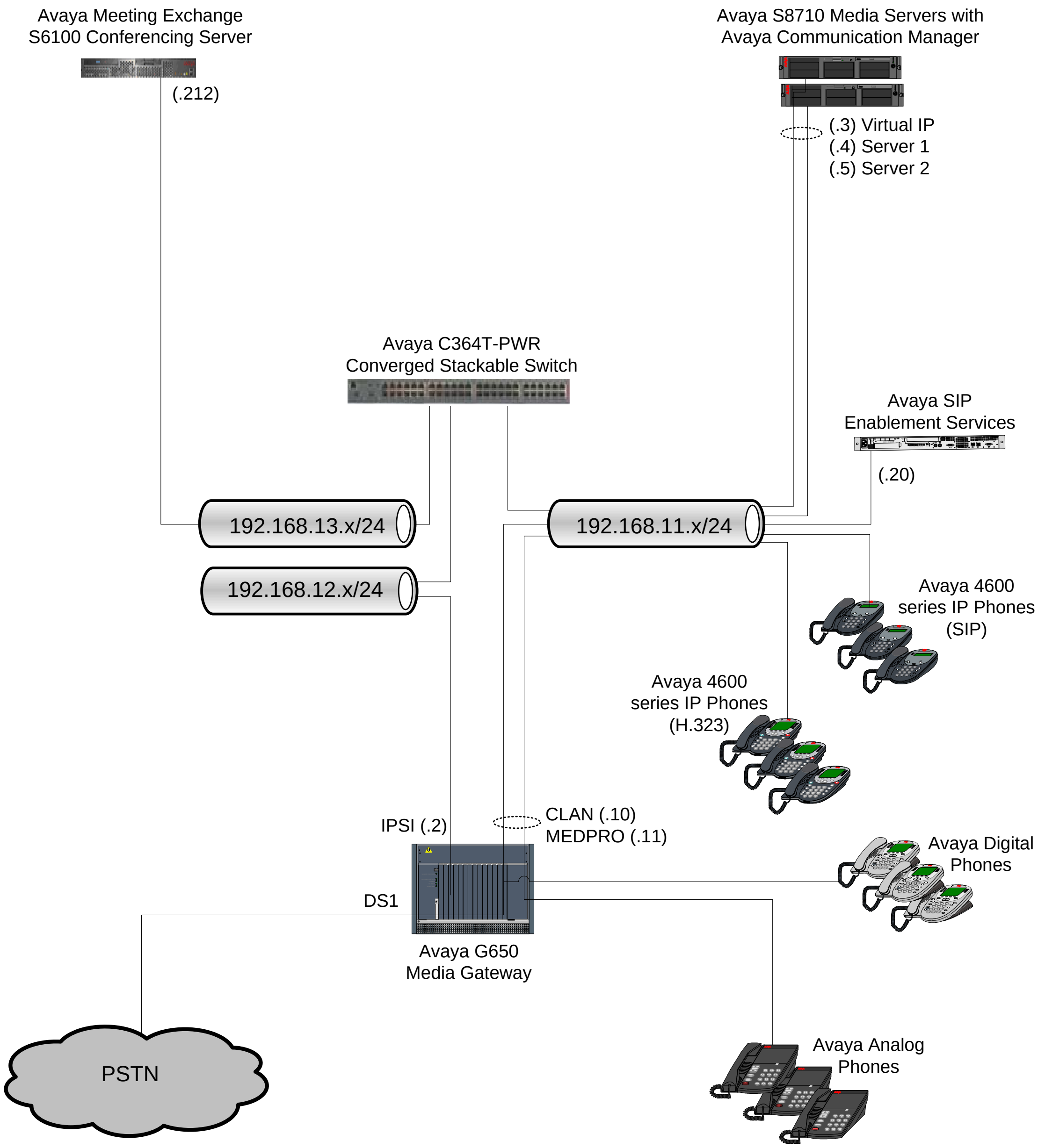


Figure 1: Network Configuration

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8710 Media Server	Avaya Communication Manager 3.1 (R013x.01.0.628.6)
Avaya G650 Media Gateway • Avaya TN2312BP (IPSI) • Avaya TN799DP (C-LAN) • Avaya TN2302AP (MEDPRO) • Avaya TN464F (DS1)	 HW12 FW031 HW01 FW017 HW20 FW112 000010
Avaya Meeting Exchange S6100 Conferencing Server	2.0.22.2
Avaya SIP Enablement Services	3.1 (03.1-03.1.018.0)
Avaya C364T-PWR Converged Stackable Switch	V4.5.14
Avaya 4620 IP Telephones	2.3 (H.323)
Avaya 4602 IP Telephones	2.2 (SIP)
Avaya Analog Telephones	--
Avaya Digital 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 Meeting Exchange via direct and secure SIP connectivity utilizing TLS/TCP (see **Figure 1**).

The following configuration of Avaya Communication Manager was performed 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 for OPTIONAL FEATURES

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.</td></tr>
<tr><td></td><td>

```
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
```

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

Step	Description
3.2	Proceed to Page 3 on the **OPTIONAL FEATURES** form and verify: • 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 3.10**) upon matching a **Dialed String** in the **DIAL PLAN ANALYSIS TABLE** (see **Step 3.9**).

```
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.)
```

Step	Description
3.3	Configure an **IP Codec Set**. Issue the command "**change ip-codec-set <n>**", where **n** is defined from 1-7; and administer settings as per below. • Configure an **Audio Codec** that is supported on Avaya Meeting Exchange; either **G.711MU**, or **G.711A**. For these Application Notes, **G.711MU** was selected.
	(screen below)

```
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 defined from 1-250; 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 **Intra-region IP-IP Direct Audio** to **yes**; thus allowing for direct IP-to-IP audio connectivity between endpoints registered to Avaya Communication Manager/Avaya SIP Enablement Services and Avaya Meeting Exchange. For these Application Notes; the C-LAN, and all the IP endpoints registered to Avaya Communication Manager/Avaya SIP Enablement Services are in IP Network Region 1 and Avaya Meeting Exchange is in IP Network Region 12.

Note: To enable direct IP-to-IP audio connectivity, the following must be administered:

- Direct IP-to-IP audio connectivity must be enabled at the system-level on Page 16 of the **FEATURE-RELATED SYSTEM PARAMETERS** form by setting the parameter: **Direct IP-IP Audio Connections** to **y**.
- Direct IP-to-IP audio connectivity must be enabled on the Station by setting the **Direct IP-IP Audio Connections** field to **y**.
- Direct IP-to-IP audio connectivity must be enabled on the **SIGNALING GROUP** form by setting the **Direct IP-IP Audio Connections** field to **y** (see **Step 3.7**).

```
Page 1 of 19
                               IP NETWORK REGION
  Region: 12
Location:         Authoritative Domain:
    Name: S6100
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 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	Proceed to Page 3 of the **IP NETWORK REGION** form and enable inter-region connectivity between regions **12** and **1** as per below. • For these Application Notes, the C-LAN is in region 1 and Avaya Meeting Exchange is in Region 12. o To enable interconnectivity between region 12 and region 1, enter the IP Codec Set provisioned in **Step 3.3** in the **codec set** field.

```
Page 3 of 19
                   Inter Network Region Connection Management

 src dst  codec  direct                                      Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway    IGAR
 12  1     1       y           :NoLimit                                    n
 12  2
 12  3
 12  4
 12  5
 12  6
 12  7
 12  8
 12  9
 12  10
 12  11
 12  12    1
 12  13
 12  14
 12  15
```

Step	Description
3.6	Configure **IP NODE NAMES**. Issue the command "**change node-names ip**"; and administer settings as per below. • Add a node name for Avaya Meeting Exchange. • Verify that node-names are configured for the **C-LAN** and **MEDPRO** boards.

```
Page 1 of 1
                                 IP NODE NAMES
    Name                 IP Address
CLAN-1A02           192.168.11 .10
MEDPRO-1A03         192.168.11 .11
S6100               192.168.13 .212
SES                 192.168.11 .20
```

Step	Description

3.7	Configure a SIP **SIGNALING GROUP**.
	
	Issue the command "**add signaling-group <n>**", where **n** is an unallocated Signaling Group; and administer settings as per below.
	• To enable secure SIP connectivity utilizing TLS, configure the **Group Type** to **sip** and the **Transport Method** to **tls**.
	    o Set the **Far-end Listen Port** to **5061** to match the configuration on Avaya Meeting Exchange (see **Steps 4.3, 4.8**).
	        Note: It is also RECOMMENDED that a server listen for requests on the default SIP port 5061 for TLS over TCP on all public interfaces.
	• Enter the IP Node Name of the C-LAN provisioned in **Step 3.6** in the **Near-end Node Name** field.
	• Enter the IP Node Name of Avaya Meeting Exchange provisioned in **Step 3.6** 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.

```
Page 1 of 1
                                SIGNALING GROUP

 Group Number: 12             Group Type: sip
                        Transport Method: tls





   Near-end Node Name: CLAN-1A02              Far-end Node Name: S6100
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 12
       Far-end Domain:

                                          Bypass If IP Threshold Exceeded? n

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

Step	Description
3.8	Configure a SIP **TRUNK GROUP**. Issue the command "**add trunk-group <n**>", where **n** is an unallocated Trunk Group; and administer settings as per below. • The setting for the **Group Type** is consistent with the Signaling Group provisioned in **Step 3.7**. • The setting for the Trunk Access Code (**TAC**) is a number that is consistent with the existing dial plan (see **Step 3.10**). • Enter the number of the Signaling Group provisioned in **Step 3.7** 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.

```
Page 1 of 21
                                TRUNK GROUP

Group Number: 12                   Group Type: sip           CDR Reports: y
  Group Name: S6100 SIP                   COR: 1        TN: 1        TAC: 112
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                          Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                       Signaling Group: 12
                                                     Number of Members: 50
```

Step	Description
3.9	Configure the **DIAL PLAN ANALYSIS TABLE** Issue the command "**change dialplan analysis**". 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**.

```
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

3.10	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 12**.
	  o Dialed String **412** will be used by Avaya Meeting Exchange for **BasicCallFlow** (see **Step 4.4**).
	  o Dialed String **444** will be used by Avaya Meeting Exchange for **DirectCallFlow** (see **Steps 4.5, 4.11**).

```
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     12       aar          n
```

Step	Description
3.11	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 3.8**.

```
Page 1 of 3
                    Pattern Number: 12  Pattern Name: S6100 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: 12   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

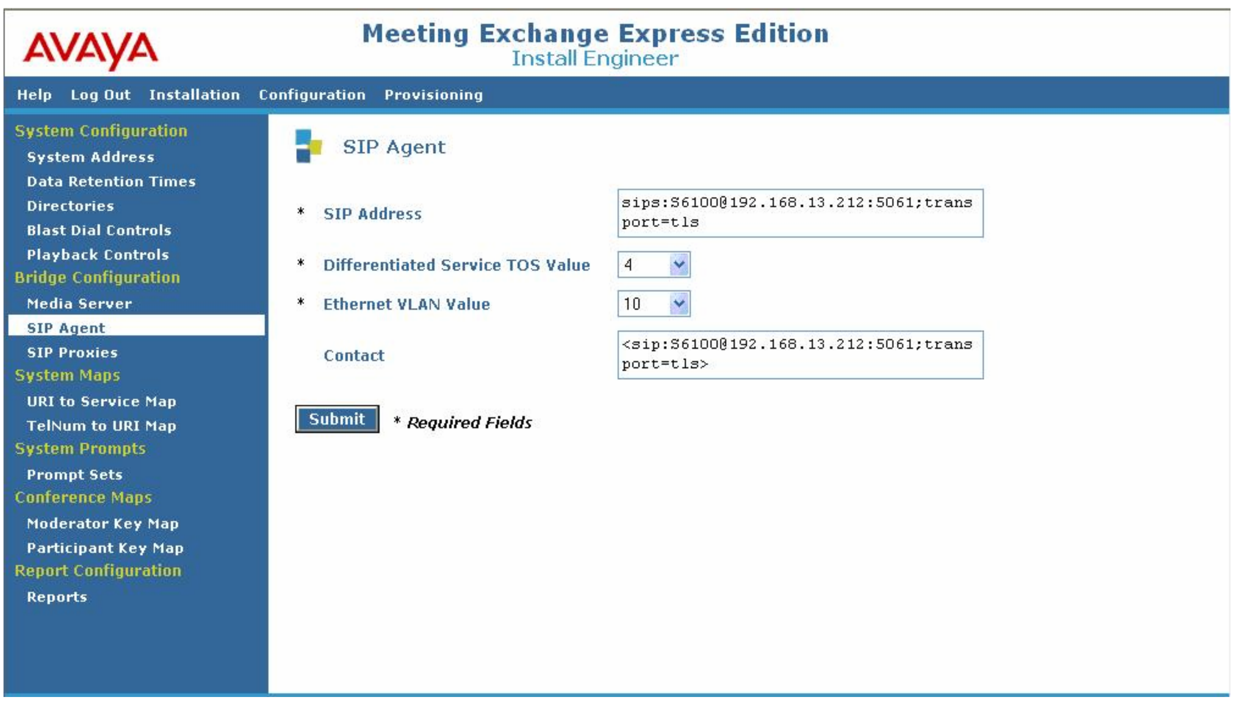
This section describes the steps for configuring Avaya Meeting Exchange to interoperate with Avaya Communication Manager via direct and secure SIP connectivity utilizing TLS/TCP (see **Figure 1**).

Step	Description
4.1	Verify Licensing as follows:

- Avaya Meeting Exchange uses Avaya Web License Manager (WebLM) to support Avaya software products that require 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 which can be accessed from a standard web browser over a secure SSL link.
  - Open a web browser and enter the following URL: **http://<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 on Avaya Meeting Exchange requires one port for the duration they are on a 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.

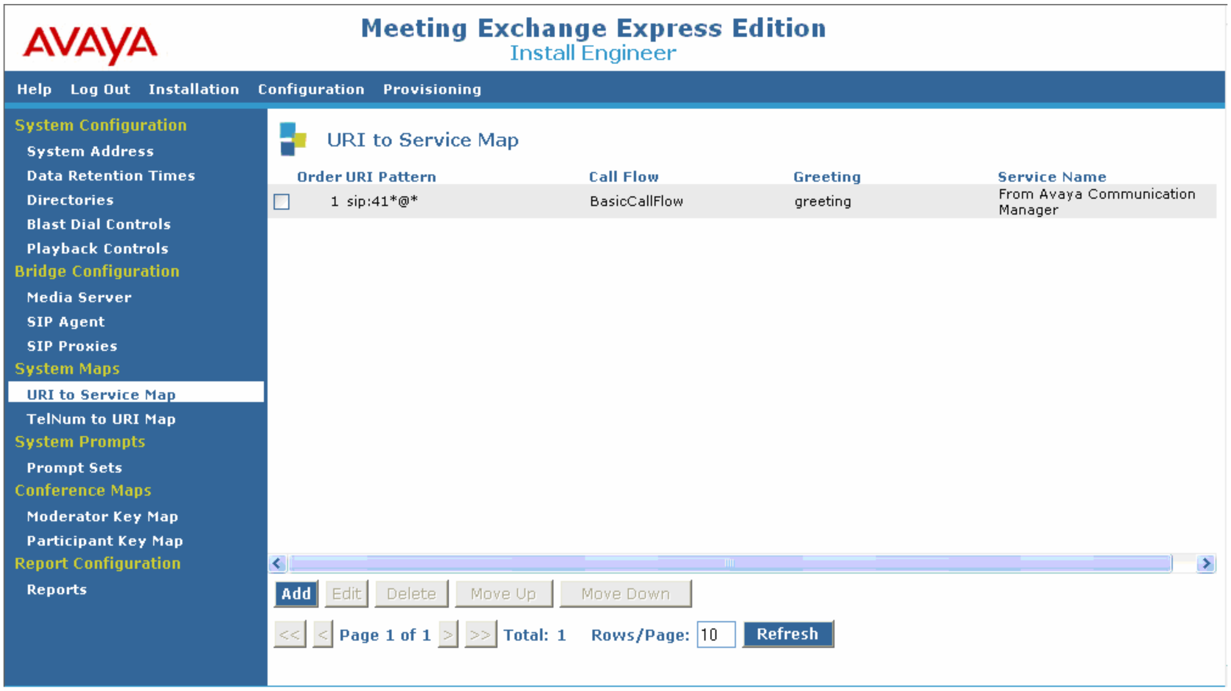
Step	Description
4.2	Administer settings for Avaya Meeting Exchange as follows: • Open a web browser and enter the following URL: **http://<IP Address of Avaya Meeting Exchange>** • Log In to Avaya Meeting Exchange with the appropriate credentials.
4.3	Configure settings that relate to the existence of Avaya Meeting Exchange within the SIP network by administering **SIP Agent** parameters as follows: • Click **Configuration** from the S6100 web interface toolbar. • Click **SIP Agent** from the **Configuration** menu. • Add a **SIP Address** for Avaya Meeting Exchange. To enable secure SIP connectivity utilizing TLS, the **SIP Address** must have **sips**, **5061** and **transport=tls** in the entry. • Add a **Contact** address to overwrite the contact field for SIP responses from Avaya Meeting Exchange. To enable secure SIP connectivity utilizing TLS, the **Contact** address must have **5061** and **transport=tls** in the entry. • When finished, click the **Submit** button.



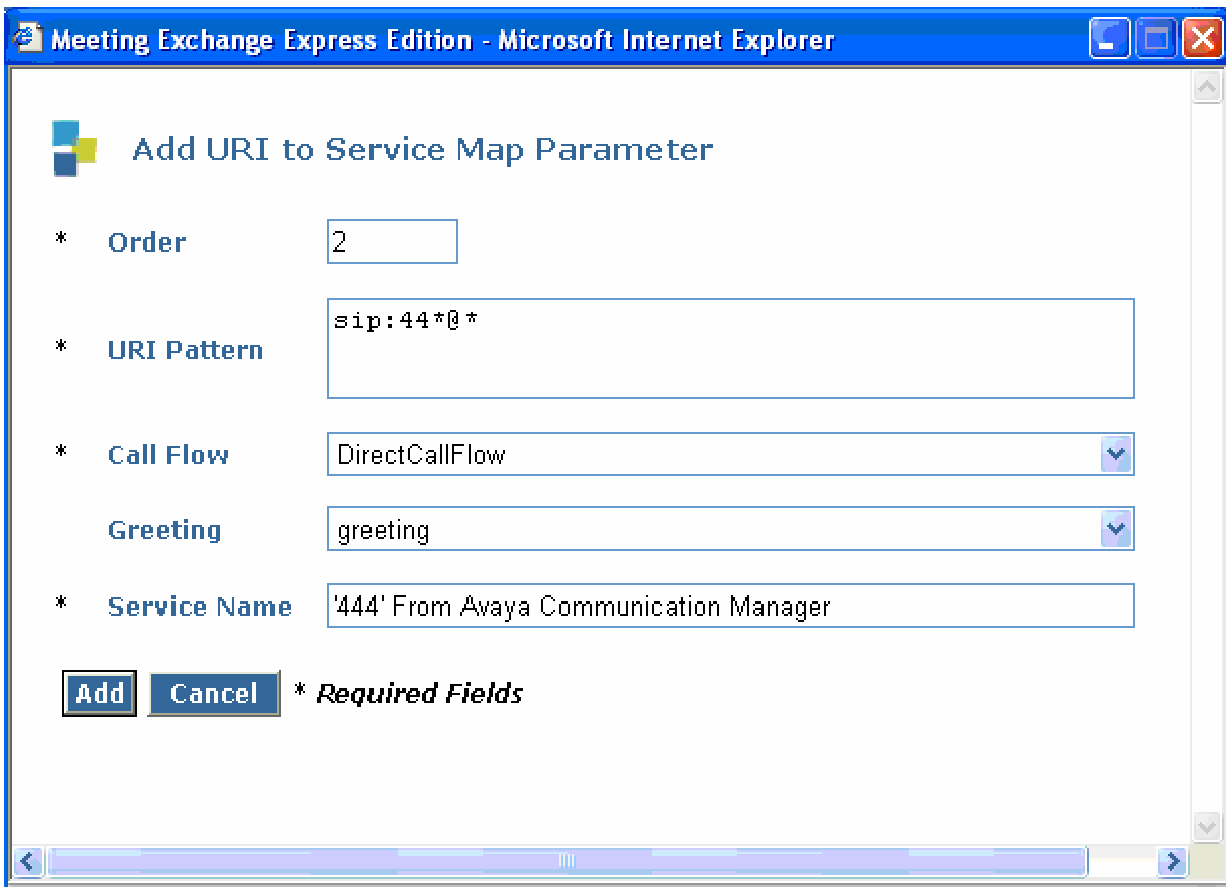
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.4</td><td>
To associate incoming calls to Avaya Meeting Exchange with a corresponding Call Flow, add a URI to Service Map entry as follows:

Click URI to Service Map from the Configuration menu.
Click the Add button.

Note: There is an entry for a BasicCallFlow already provisioned. Step 4.5 describes how to provision a new call flow (e.g., DirectCallFlow).

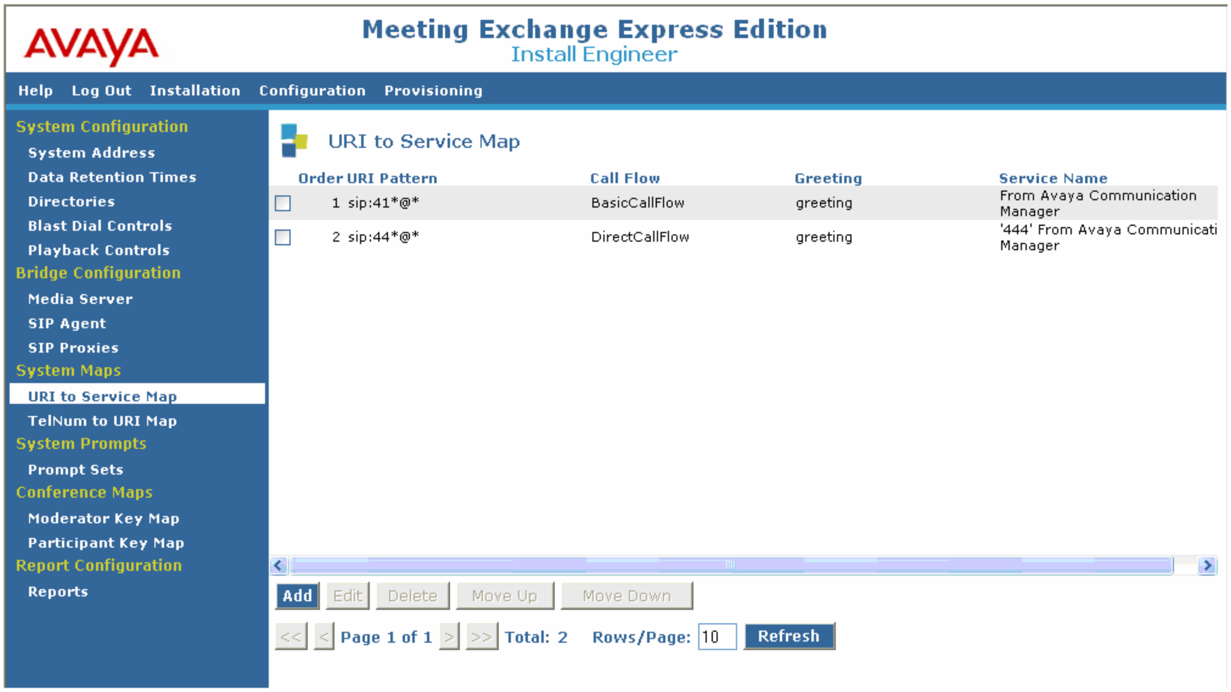


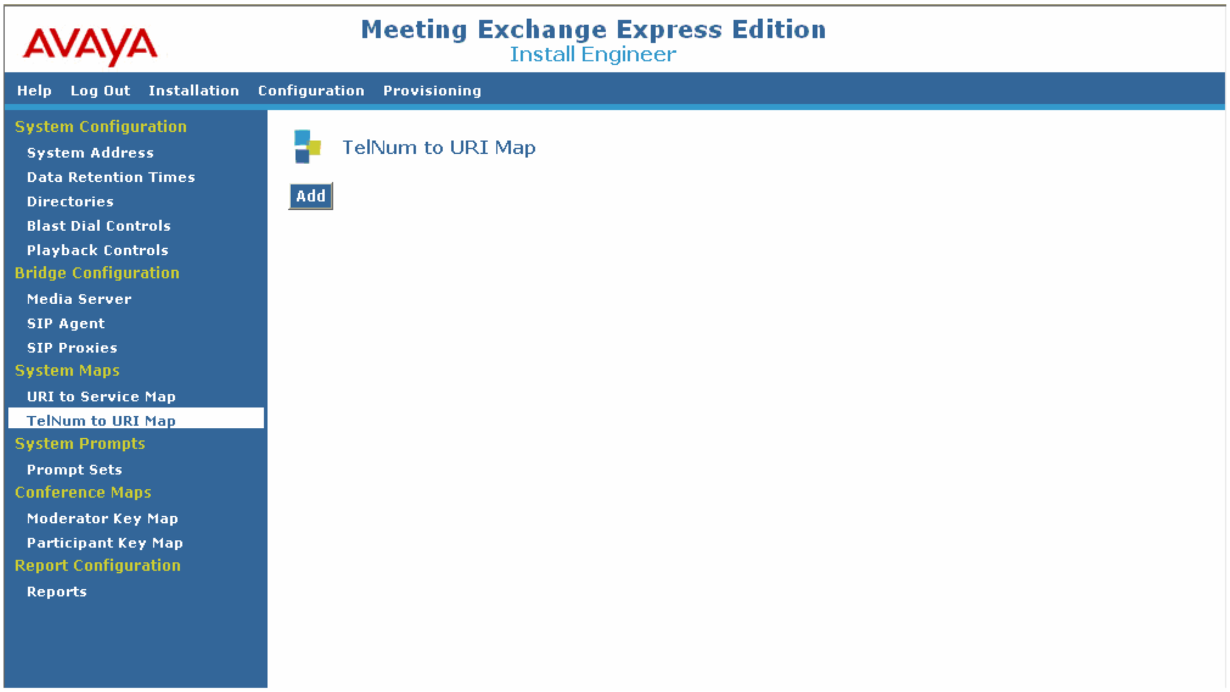
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.5</td><td>Configure a URI to Service Map Parameter for a DirectCallFlow as follows:
• The Order field is left at the default setting. It is defaulted to 2 due to the existing BasicCallFlow entry in the table (see Step 4.4).
Note: Avaya Meeting Exchange parses System Maps 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 DirectCallFlow and BasicCallFlow (see Step 4.4) are mutually exclusive.
• Add a URI Pattern to allow Dial-In to Avaya Meeting Exchange from Avaya Communication Manager by matching the pattern of incoming SIP URIs in SIP INVITE messages.
o For example, Avaya Communication Manager sends the following URI: sip:444@192.168.13.211. The URI Pattern is configured to match sip:44*@*, which will match sip:44 and any string until the @ is reached, then any string following the @.
• The Service Name field is a descriptive label.
• When finished, click the Add button.


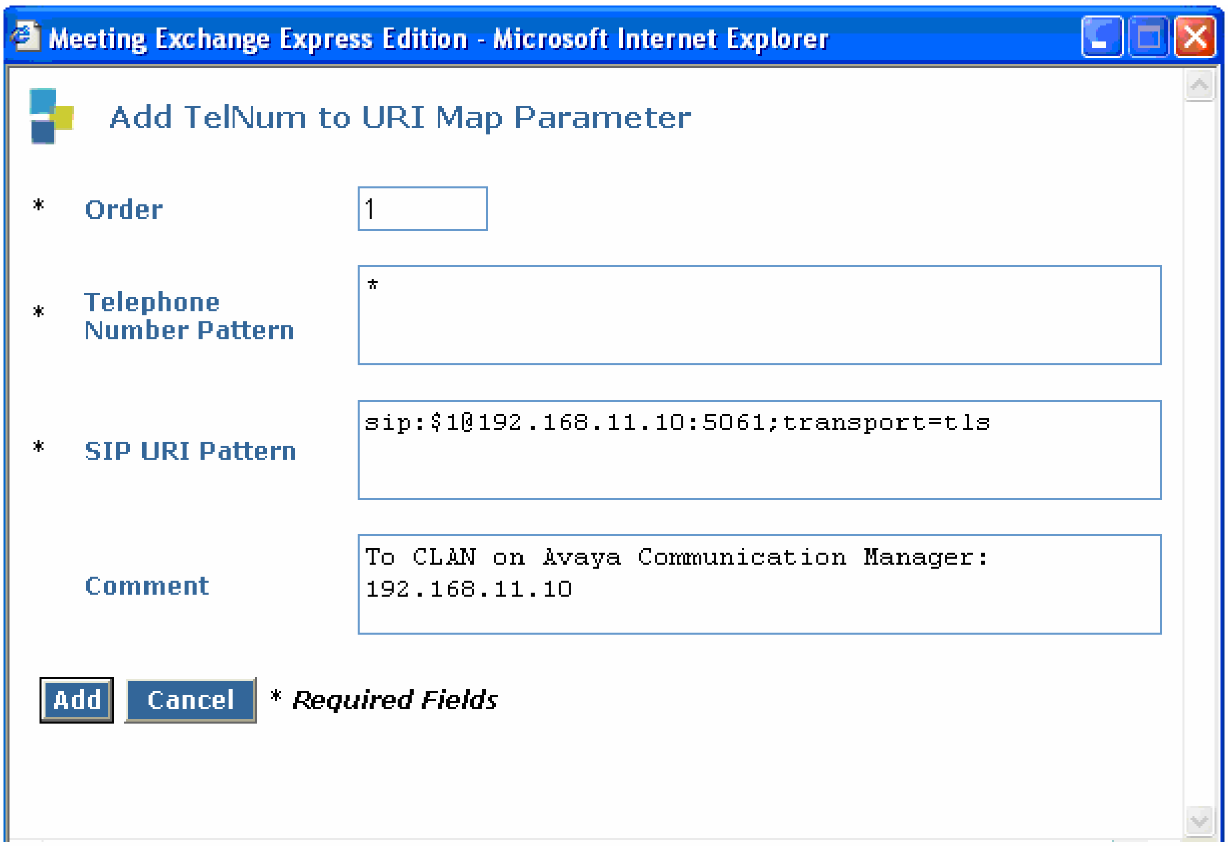
</td></tr>
</table>

Step	Description
4.6	The **URI to Service Map** entry is successfully added.

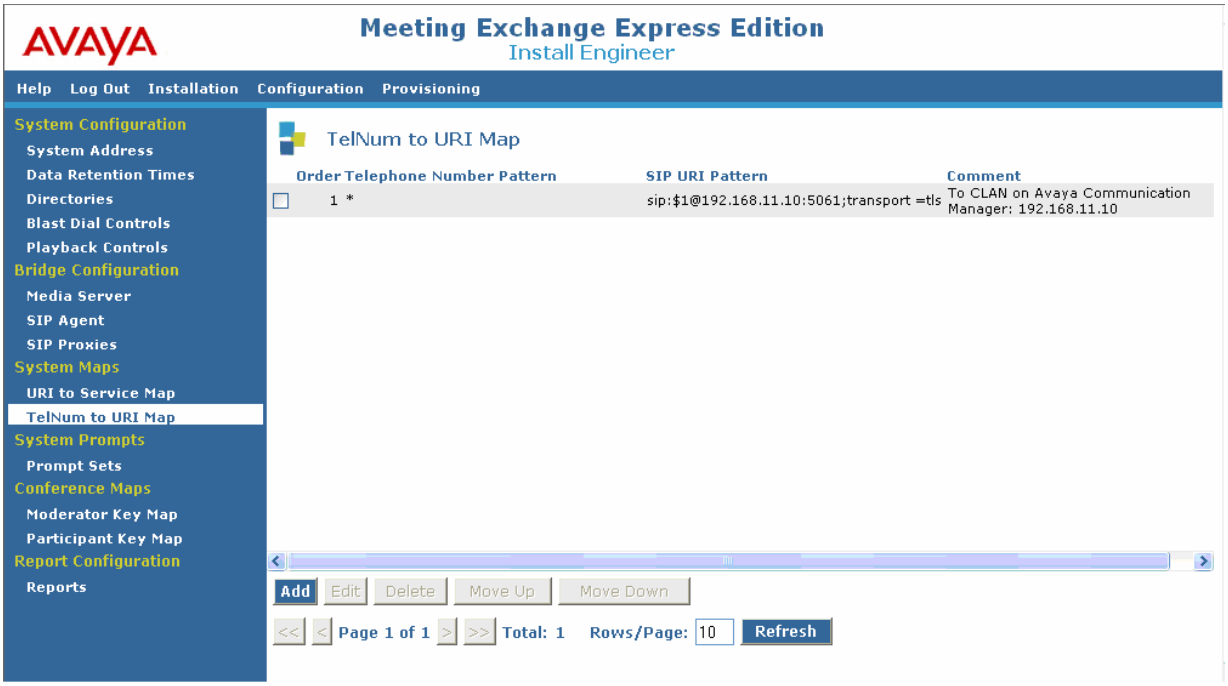


Step	Description
4.7	To configure routing of outbound call from Avaya Meeting Exchange, add a **TelNum to URI Map** entry as follows: • Click **TelNum to URI Map** from the **Configuration** menu. • When finished, click the **Add** button. 

Step	Description
4.8	Configure a **TelNum to URI Map Parameter** as follows: • Add a **Telephone Number 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 the C-LAN on Avaya Communication Manager (**192.168.11.10**). To enable secure SIP connectivity utilizing TLS for Dial-Out, the **SIP URI Pattern** must have **5061** and **transport=tls** in the entry. • The **Comment** field is a descriptive label. • When finished, click the **Add** button.



Step	Description
4.9	The **TelNum to URI Map** entry is successfully added.



Step	Description
4.10	Following all updates to Avaya Meeting Exchange via the web browser, reboot Avaya Meeting Exchange as follows:

- If not already logged on, log in to the Avaya Meeting Exchange Server console to access the command line interface with the appropriate credentials.
- At the command prompt, enter the command: **init 6**.

```
[S6100]> init 6
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.11</td><td>To utilize the DirectCallFlow provisioned in Step 4.5, administer an Account CSV file as follows:
• If not already logged on, log in to the Avaya Meeting Exchange Server console to access the command line interface with the appropriate credentials.
• Create an Account CSV file with the format of the myAccount.csv shown below.
   o The myAccount.csv file is correlated to the URI Pattern provisioned in Step 4.5 via the def_modpass_code entry.</td></tr>
<tr><td></td><td><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></td></tr>
<tr><td></td><td>• Write the myAccount.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:
     sh bulk-loader.sh -A/usr/tmp/csvFiles/myAccount.csv</td></tr>
<tr><td></td><td><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>
<tr><td></td><td></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.
	    o The **myBlastDial.csv** file is correlated to the **myAccount.csv** file provisioned in **Step 4.11** via the **reservation_import_tag** entry.
	    o 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:
	    sh bulk-loader.sh -B/usr/tmp/csvFiles/ myBlastDial.csv

	`[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. Verification Steps

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

Step	Description
5.1	Verify all members for the SIP trunk group provisioned in **Step 3.8** are **in-service/idle**. From a SAT session: • Issue the command "**status trunk 12**". • Verify that all members in Trunk Group 12 are **in-service/idle**.
5.2	Verify the SIP trunk group is utilized when a call from a SIP station Dials-In to Avaya Meeting Exchange. From a SAT session: • Issue the command "**list trace tac 112**", where **112** is the TAC defined for the trunk group provisioned in **Step 3.8**. • From a SIP station, dial **444** to enter a conference as moderator via a **DirectCallFlow** scenario. • Enter ***9** to initiate a Blast Dial. **Note**: This trace shows the SIP Station Dialing-In via a **DirectCallFlow**. Dial-Out, (e.g., Blast Dial) is not shown in the list trace output below. A SIP station 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 112                                                      Page   1

                                LIST TRACE

time            data

16:33:41     dial 444 route:AAR
16:33:41     term trunk-group 12    cid 0x289
16:33:41     dial 444 route:AAR
16:33:41     route-pattern  12 preference 1  cid 0x289
16:33:41     seize trunk-group 12 member 48  cid 0x289
16:33:41     Calling Number & Name 31002 SIP 31002
16:33:41     Proceed trunk-group 12 member 48  cid 0x289
16:33:41     active trunk-group 12 member 48  cid 0x289
16:33:41     G711MU ss:off ps:20 rn:12/1 192.168.13.212:42004 192.168.11.11:2336
16:33:41     xoip: fax:Relay modem:off tty:US 192.168.11.11:2336 uid:0x500ab
16:33:41     G711MU ss:off ps:20 rn:12/1 192.168.13.212:42004 192.168.12.11:3400
16:33:41     G711MU ss:off ps:20 rn:1/12 192.168.12.11:34008 192.168.13.212:42004
```

Step	Description
5.3	Verify direct IP-to-IP audio connectivity for the SIP station Dialing-In to Avaya Meeting Exchange. From a SAT session: • Issue the command “**status trunk 12/48** (where **12/48** is obtained from **Step 5.2**)”. • 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.

```
status trunk 12/48                                          Page   1 of   2
                              TRUNK STATUS

 Trunk Group/Member: 0012/048              Service State: in-service/active
               Port: T00171             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. 13.212 : 5061

G.711MU     Audio:          192.168. 12. 11  : 34008   192.168. 13.212 : 42004
            Video:
      Video Codec:
                                            Authentication Type: None
    Audio Connection Type: ip-direct
```

Step	Description
5.4	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 to access the command line interface with the appropriate credentials. • At the command prompt, enter the command: **watch -t -n 5 -d "ipinfo -l |egrep -ci active"** o This command will provide a real time, continuous update of port utilization on Avaya Meeting Exchange.

6. Conclusion

These Application Notes provide administrators with the procedures to configure connectivity between Avaya Communication Manager and the Avaya Meeting Exchange S6100 Conferencing Server utilizing secure standards based SIP connectivity via TLS/TCP. With appropriate configuration, Dial-In and Dial-Out conferencing is successfully established between Avaya Meeting Exchange and Avaya Communication Manager.

7. Additional References

Avaya references, available at http://support.avaya.com

1. *Administrator Guide for Avaya Communication Manager*, Doc ID: 03-300509
2. *Administration for Network Connectivity for Avaya Communication Manager*, Doc ID: 555-233-504

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