Avaya Solution & Interoperability Test Lab

Application Notes for AlarmPoint Enterprise and Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the AlarmPoint Enterprise and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura™ SIP Enablement Services, Avaya Aura™ Communication Manager, and various Avaya SIP and H.323 endpoints.

AlarmPoint Enterprise is an alert management solution which accelerates decision making, improves operational effectiveness and increases IT service and application availability across the enterprise. The solution transforms complex, monitored event data into meaningful information which is instantly delivered to the appropriate recipient. This information may be acted on by business professionals or used by IT teams to accelerate the incident resolution process, delivering greater application availability.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between AlarmPoint Enterprise and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura™ SIP Enablement Services, Avaya Aura™ Communication Manager, and various Avaya SIP and H.323 endpoints.

AlarmPoint Enterprise is an alert management solution that helps to resolve IT events faster by ensuring incidents are properly assigned and resolution activities are coordinated, escalated and resolved within acceptable service levels. Within AlarmPoint Enterprise, users simply subscribe or are assigned to events. In addition, roles, alerts, languages, schedule reports, devices and escalation rules are all self-managed by users. Administrators can assign unlimited user attributes and create dynamic groups at the moment an event takes place – notifying people based on their skills, location, certifications and experience levels or identifying resources with a known ability to resolve an issue.

1.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance testing was primarily on verifying the interoperability between AlarmPoint Enterprise, Application Enablement Services, and Communication Manager. Basic calls were placed, including inbound calls, outbound calls, and transferred calls.

1.2. Support

Customers with active Technical Support agreements can receive support via email, web, and telephone. Please see https://connect.AlarmPoint.com or http://www.AlarmPoint.com for details.

2. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an Application Enablement Services server and an Avaya S8300 Server with a G450 Media Gateway. AlarmPoint Enterprise was located in a different VLAN. Endpoints include Avaya 9600 Series H.323 IP Telephones, an Avaya 4625 H.323 IP Telephone, and an Avaya 6408D Digital Telephone. An Avaya S8300 Server with an Avaya G450 Media Gateway was included in the test to provide an inter-switch scenario.

The specific configuration above was used for the compliance test. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and SIP Enablement Services.

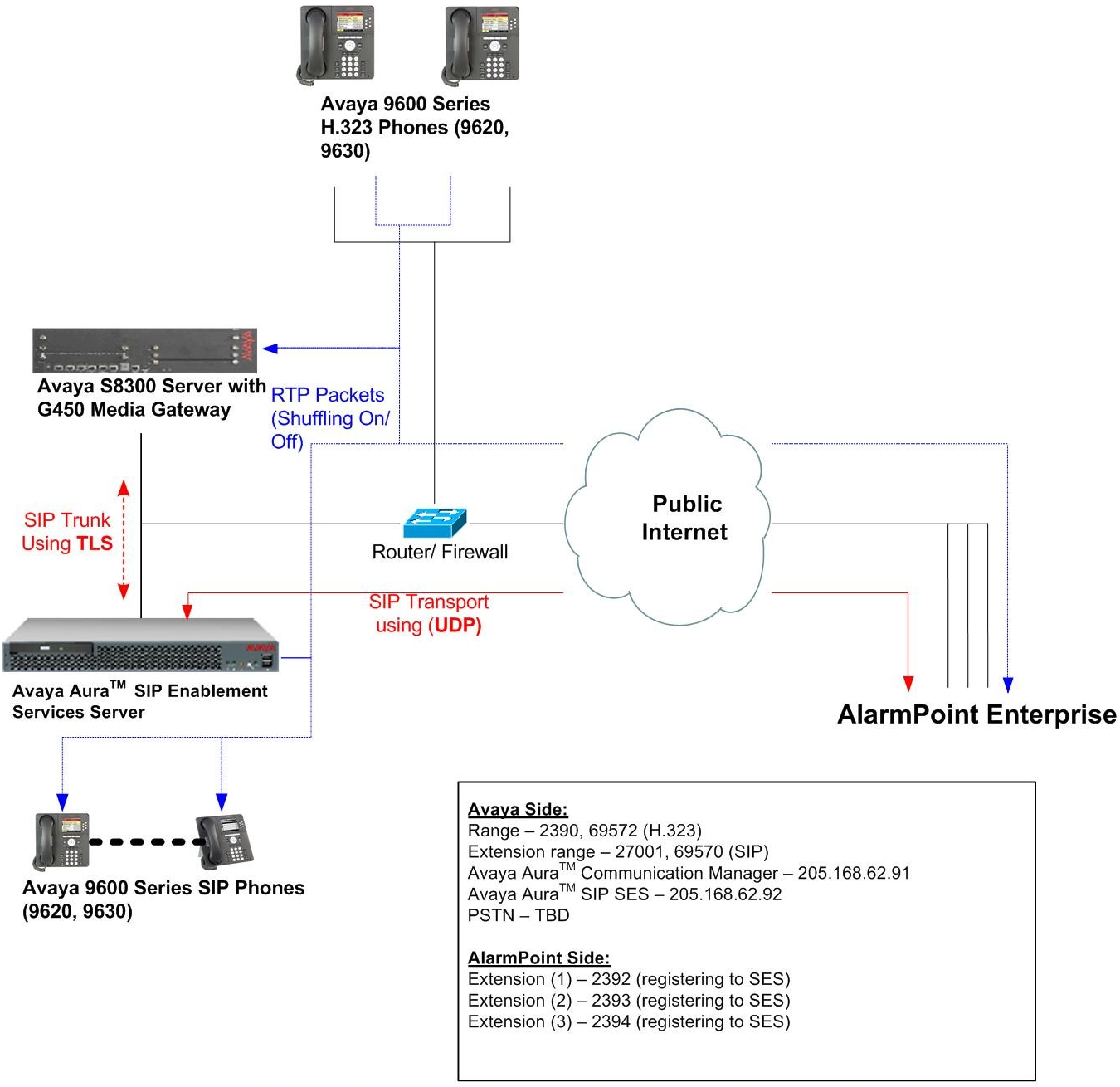


Figure 1: Avaya IP Telephony Network using AlarmPoint Enterprise

3. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura™ Communication Manager running on an Avaya S8300 Server	5.2.1 (R015x.02.1.016.4)
Avaya G450 Media Gateway	
Avaya Aura™ SIP Enablement Services running on an Avaya S8500B Server	5.2.1 (R015x.02.1.016.4)
Avaya 9600 IP Series Telephone (H.323)	Avaya one-X Deskphone Edition (H.323)
9620 9630	3.1 3.1
Avaya 9620 Series IP Telephone (SIP)	Avaya one-X Deskphone Edition (SIP)
9620 9630	2.5 2.5
AlarmPoint Enterprise Solution Components	
Component	Release
AlarmPoint Enterprise	4.0 Patch 9

Table 1: Equipment and Software Tested

4. Configure Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and SIP Enablement Services (SES). A trunk is created as part of the initial SES installation and is meant to carry SIP signaling between SIP endpoints within the SES domain.

It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and SIP Enablement Services has been previously completed. In addition, it is also assumed that any initial SIP configuration on Communication Manager that is required to support the SES installation has also been completed.

The Communication Manager configuration was performed using the System Access Terminal (SAT).

4.1. Configure Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunk** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. Each Avaya SIP telephone on a 2-party call with the SIP service provider uses two SIP trunk members for the duration of the call. Each non-SIP telephone (e.g., analog, digital, H.323) on a 2-party call with SIP service provider uses one SIP trunk member. The example shows that

100 licenses are available and 90 are in use. The license file installed on the system controls the maximum values for these attributes.

If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```
display system-parameters customer-options                    Page   2 of  11
                              OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   20
          Maximum Concurrently Registered IP Stations: 450   3
            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: 100   0
                   Maximum Video Capable H.323 Stations: 5     0
                    Maximum Video Capable IP Softphones: 5     0
                        Maximum Administered SIP Trunks: 100   90
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                            Maximum TN2501 VAL Boards: 0     0
                    Maximum Media Gateway 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
```

4.2. Configure IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and SES. Use the **change node-names ip** command to create a mapping between a logical name and an IP address. In the test environment, node-name ***procr*** is mapped to IP address ***205.168.62.91*** (an Avaya S8300 Server processor) and node name ***SES*** is mapped to ***205.168.62.92*** (the IP address of the SIP Enablement Service server).

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                 IP Address
IA770                  10.64.41.22
SES                    205.168.62.92
default                0.0.0.0
procr                  205.168.62.91
```

4.3. Configure IP Network Regions

In the test environment, the Avaya S8300 Server, Avaya G450 Media Gateway, SES server, IP (H.323/SIP) endpoints, and AlarmPoint SIP endpoints are located in a single IP network region. These components are located in the default IP network region 1. The **change ip-network-region 1** command was used to configure the region with the parameters described below.

- Set the **Authoritative Domain** field to match the domain name configured on SES. In this configuration, the domain name is ***testroom.avaya.com***. This name appears in the "From" header of SIP messages originating from this IP region.

- Enter a descriptive name for the **Name** field.
- Set the **Codec Set** field to the IP codec set to be used for calls within this IP network region. In this case, IP codec set **1** was selected.
- Default values may be used for all other fields.

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: testroom.avaya.com
    Name:Avaya Devices
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: 3329
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
```

4.4. Configure Codecs

Use the **change ip-codec-set 1** command to define the codec(s) contained in this set which is used for calls within the enterprise as defined in the previous section. Which codecs are used and their order of preference is defined by the end customer. The example below uses only G.711MU.

```
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:
```

4.5. Configure Signaling Group

The **add signaling-group** command was used to create a signaling group between Communication Manager and the SES for use by intra-site traffic. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.

- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.***
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the processor ethernet in the Avaya S8300 Server that terminates the SIP trunk. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to ***SES***. This node name maps to the IP address of SES as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined **Section 4.3**.
- Set the **Far-end Domain** to the domain of the SES.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```
add signaling-group 3                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 3                      Group Type: sip
                                Transport Method: tls
  IMS Enabled? n


   Near-end Node Name: procr                 Far-end Node Name: SES
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1
Far-end Domain: testroom.avaya.com

                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                                 Alternate Route Timer(sec): 6
```

4.6. Configure Trunk Group

The **add trunk-group** command was used to create a trunk group for the signaling group created in the previous section. For the compliance test, trunk group 3 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***tie***.
- Set the **Signaling Group** to the signaling group shown in the previous step.

- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- The default values were used for all other fields.

```
add trunk-group 3                                              Page   1 of  21
                                 TRUNK GROUP

Group Number: 3                      Group Type: sip           CDR Reports: y
  Group Name: ToSES                          COR: 1        TN: 1        TAC: 1003
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                      Signaling Group: 3
                                                    Number of Members: 20
```

4.7. Configure Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound PSTN calls via the ISDN-PRI trunk. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". The common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).

```
change dialplan analysis                                       Page   1 of  12
                          DIAL PLAN ANALYSIS TABLE
                               Location:  all           Percent Full:    3

       Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
       String   Length Type     String   Length Type     String   Length Type
     0            1    attd     7          5    ext
     10           4    dac      79000      5    ext
     11           4    dac      8          1    fac
     12           3    fac      9          1    fac
     13           3    fac      *          3    fac
     14           3    fac      #          3    fac
     2            5    ext
     23           4    ext
```

Use the **change feature-access-codes** command to configure ***9*** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                    Page   1 of   8
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *01
         Abbreviated Dialing List2 Access Code: *02
         Abbreviated Dialing List3 Access Code: *03
Abbreviated Dial - Prgm Group List Access Code: *04
                      Announcement Access Code: *05
                       Answer Back Access Code: #06

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
                  Automatic Callback Activation: *09    Deactivation: #09
Call Forwarding Activation Busy/DA: #11    All: *10    Deactivation: #10
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test including domestic long-distance calls. The highlighted section that shown below describes the area code with 732 will go out through the route pattern 80. Other calls that go out to a different area code have to be configured, so that the call is allowed to go out to the PSTN.

```
change ars analysis 173                                        Page   1 of   2
                           ARS DIGIT ANALYSIS TABLE
                                  Location:  all           Percent Full:    3

          Dialed           Total      Route    Call    Node  ANI
          String          Min  Max   Pattern   Type    Num   Reqd
    173                   11   11    80        fnpa          n
    174                   11   11    deny      fnpa          n
    175                   11   11    deny      fnpa          n
    176                   11   11    deny      fnpa          n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 80 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group to PSTN. For the compliance test, trunk group 80 was assigned to go out to PSTN.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.

```
change route-pattern 80                                          Page   1 of   3
                    Pattern Number: 80  Pattern Name:
                                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: 80   0                                                          n    user
 2:                                                                 n    user
 3:                                                                 n    user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 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
```

4.8. Configure AlarmPoint Enterprise SIP Station

This section describes the steps for administering OPS stations in Communication Manager and associating the OPS station extensions with the telephone numbers of AlarmPoint Enterprise. Enter **add station s**, where **s** is an extension valid in the provisioned dial plan. The following fields were configured for the compliance test.

- Type – Set to **9620SIP**.
- Name – Enter a descriptive name

```
add station 2392                                                 Page   1 of   6
                                    STATION

Extension: 2392                        Lock Messages? n               BCC: 0
    Type: 9620SIP                      Security Code:                  TN: 1
    Port: S00023                     Coverage Path 1:                 COR: 1
    Name: 9620SIP                    Coverage Path 2:                 COS: 1
                                     Hunt-to Station:
STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19
                                               Message Lamp Ext: 2392

        Display Language: english

          Survivable COR: internal
   Survivable Trunk Dest? y                          IP SoftPhone? n
```

On **Page 6**, provide the SIP trunk that configured in **Section 4.6**. This step will automatically create the station 2392 as an off-pbx-telephone station.

```
add station 2392                                                 Page   6 of   6
                                    STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: None
                    SIP Trunk: 3
```

Repeat this step as necessary to configure additional SIP endpoint extensions for AlarmPoint Enterprise.

The following screen shows the off-pbx-telephone station-mapping form.

```
display off-pbx-telephone station-mapping 2392                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 2392            OPS           -     2392             3          1
 2393            OPS           -     2393             3          1
 2394            OPS           -     2394             3          1
```

4.9. Configure Incoming Call Handling Treatment form

To send PSTN calls from the SIP extension, including AlarmPoint Enterprise, the Incoming Call Handling Treatment form needs to be configured. Enter the **change inc-call-handling trmt trunk-group <t>**, where **t** is the SIP trunk between Communication Manager and SIP Enablement Services. The follow example shows that a call coming into the SIP trunk will be inspected. Calls starting with "1250", "1614" and "1732" will be added "9" when the call passes the SIP trunk. The Prefix "9" is needed since Communication Manager utilize "9 " as ARS access code. Using "9", the call will be sent to the ARS table for rerouting.

```
change inc-call-handling-trmt trunk-group 3                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 tie             11 1250                  9
 tie             11 1614                  9
 tie             11 1732                  9
 tie
 tie
```

5. Configure SIP Enablement Services

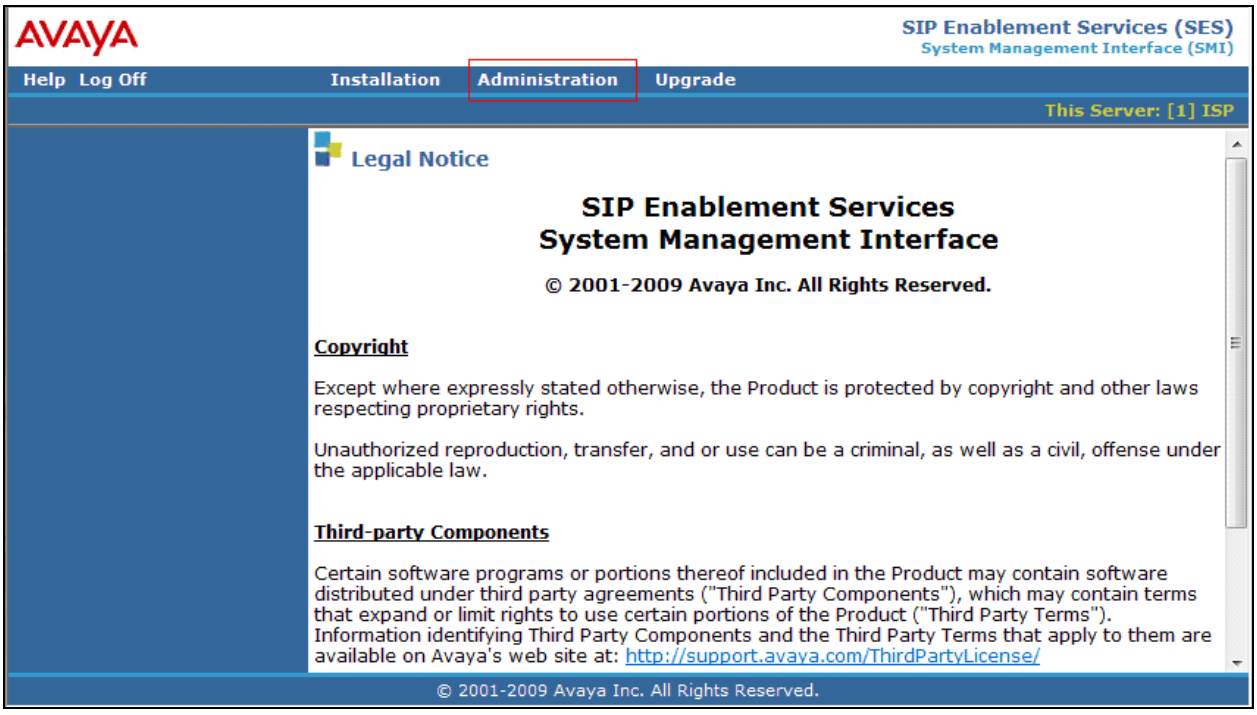
This section covers the configuration of SIP Enablement Services. SIP Enablement Services is configured via an Internet browser using the administration web interface. It is assumed that the SIP Enablement Services software and the license file have already been installed on the server. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure SIP Enablement Services.

Each SIP endpoint at the enterprise used in the compliance test, including extensions used for AlarmPoint Enterprise, requires that a user and media server extension be created on SIP Enablement Services.

5.1. Login

Access the SES administration web interface by entering http://<*ip-addr*>/admin as the URL in an Internet browser, where <*ip-addr*> is the IP address of the SIP Enablement Services server.

Log in with the appropriate credentials and then navigate to the **Administration→ SIP Enablement Services** link from the main page shown below.



The SES **Top** page will be displayed as shown below.

5.2. Configuration Parameters

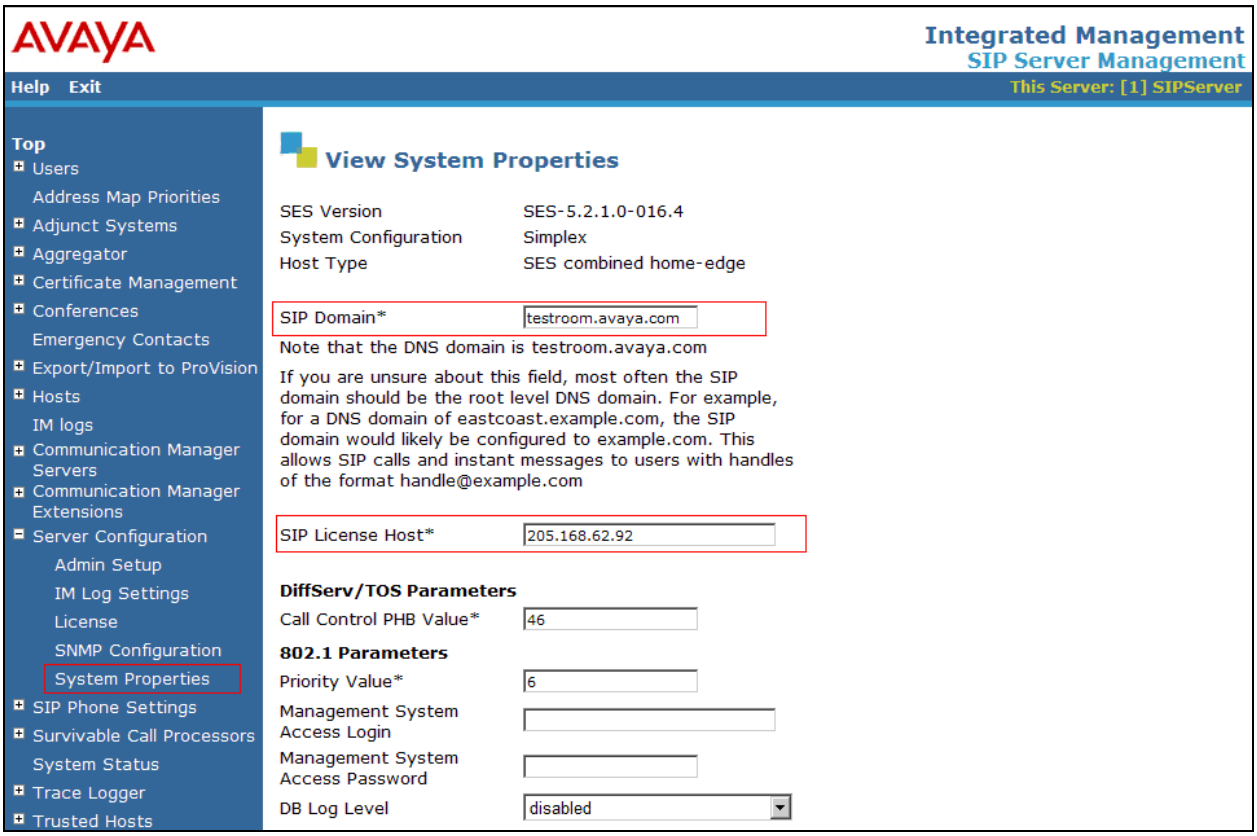
As part of the SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the SES administration home page shown in the previous step.

As part of the SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the SES administration home page shown in the previous step.

5.2.1. System Properties

To view the System Properties page, navigate to **Server Configuration→System Properties**

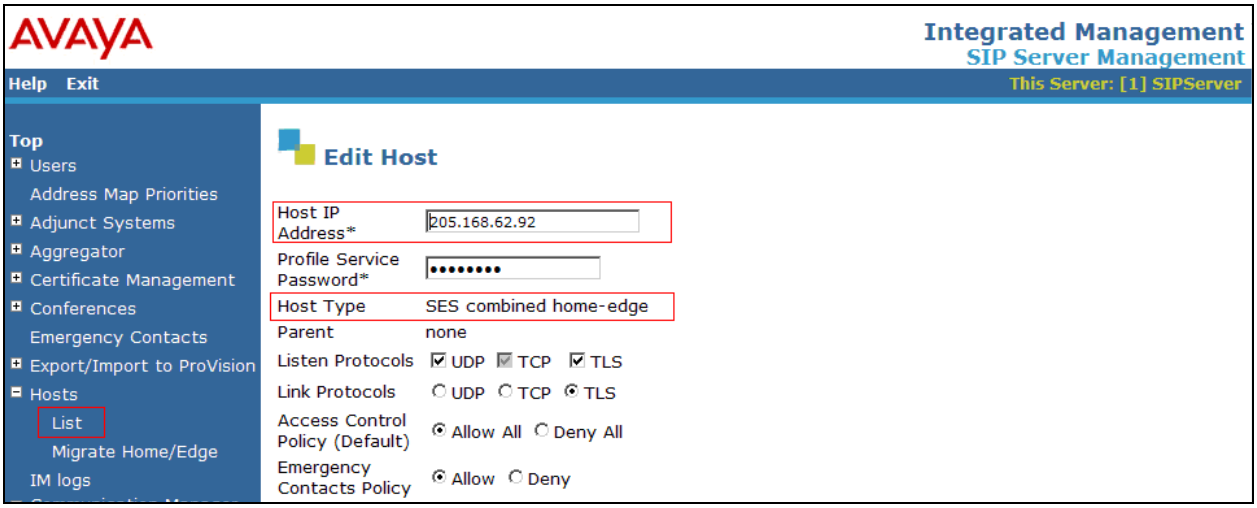
- SIP Domain: ***testroom.avaya.com***
- SIP License Host: ***205.168.62.92***



5.2.2. Host

To view the Host page, navigate to **Hosts→List**; click **Edit**.

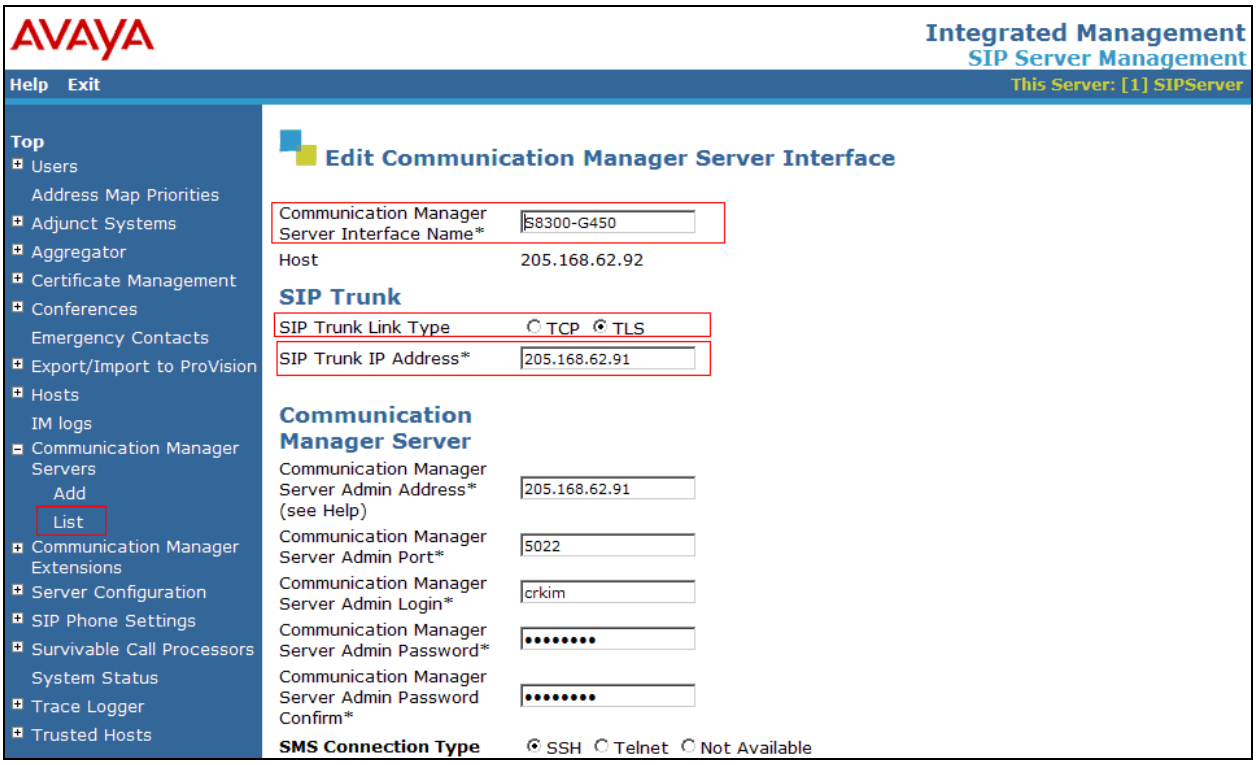
- Host IP Address (SES IP address): ***205.168.62.92***
- Host Type: ***SES combined home-edge***



5.2.3. Communication Manager Server Interface

To view the Communication Manager Server Interface page, navigate to **Communication Manager Servers→List**; click **Edit**.

- Communication Manager Server Interface Name: ***S8300-G450***
- SIP Trunk Link Type: ***TLS***
- SIP Trunk IP Address (procr IP address): ***205.168.62.91***

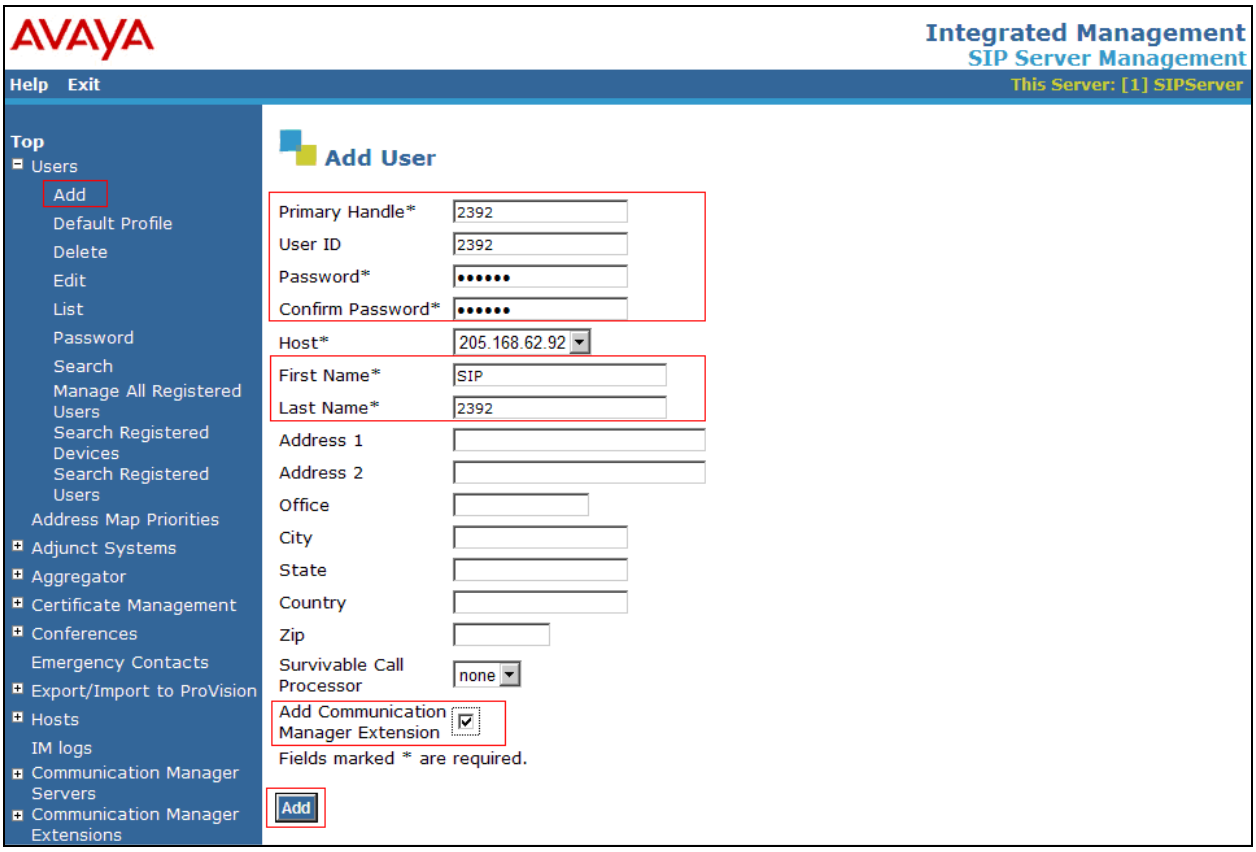


5.3. Configure Users

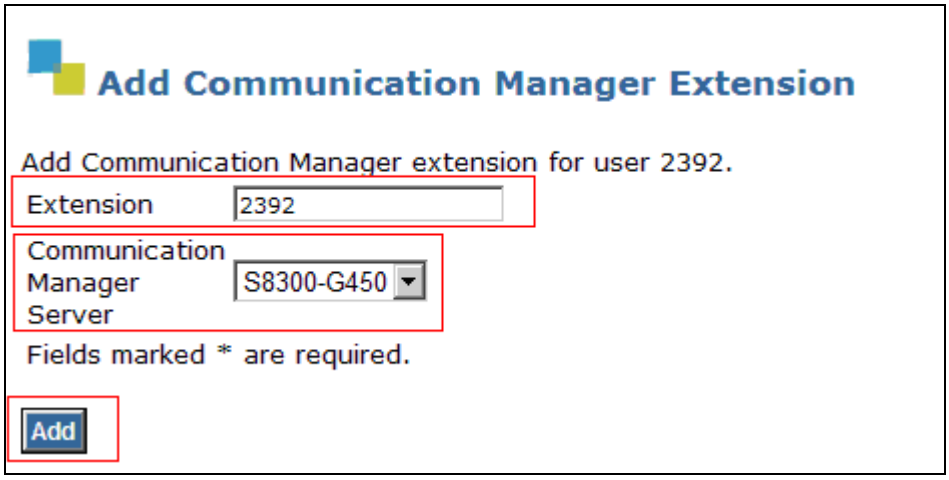
This section provides steps to add users to be administered in the SIP Enablement Services (SES) database. In the Integrated Management SIP Server Management page, select the **Users → Add** link from the left pane of the screen. The highlighted fields were configured for the compliance test:

- Primary Handle – Enter the telephone extension of AlarmPoint Enterprise. This number was configured in **Section 4.8**.
- Password / Confirm Password – Enter a password; both field entries must match exactly.
- First Name – Enter the first name of the user in alphanumeric characters.
- Last Name – Enter the last name of the user in alphanumeric characters.
- Add Media Server Extension - Select this field if you want to associate a new extension number with this user in the database now. If so, the Add MS Extension screen will be displayed next, after this user profile has been added. If not, in the future you may choose to associate extensions with the user.

Click **Add** when finished.



From the next screen, enter the numeric telephone extension you want to create in the database. Select the extension's Communication Manager Server from the drop-down list. Click on the **Add** button.



Repeat this step as necessary to configure additional users in SIP Enablement Services.

6. AlarmPoint Configuration

This section describes how to configure an AlarmPoint SIP-based notification service. The SIP notification capability is configured by accessing the AlarmPoint Web User interface with a web browser. The following sections assume that AlarmPoint is properly installed and licensed.

6.1. Configure SIP Device Engine

The *AlarmPoint Installation and Administration Guide* provides configuration details for the SIP Engine. During compliance testing, the configuration settings described in the following sections were used.

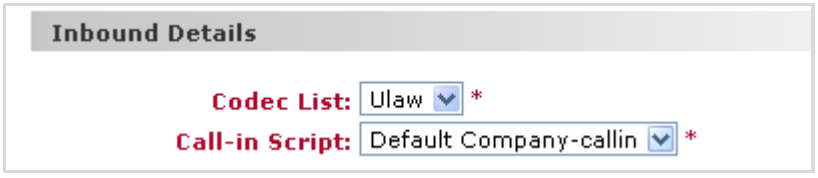
Protocol Specific Details

- Set the **Number of Line Appearances** to **9**.
  Note: *This represents the total lines available for outgoing and incoming SIP calls. The number of lines available for outgoing calls is the total number of line appearances less those reserved for incoming calls.*
  Note: *When using multiple registrations (as defined in the Registration List below) the number of line appearances should be set to a multiple of the number of registrations to fully utilize all line appearances.*

Inbound Details

- Initially select **Codec List** set to **Ulaw**.
- Ensure that **Call-in Script Name** is set to **Default Company-callin**.

Note: *AlarmPoint supports Ulaw and Alaw and during compliance testing both of these codecs were tested.*
Note: *Avaya **must** be configured to support the codec selected here.*



Inbound SIP Registration List

During compliance testing, both a single Inbound SIP Registration (Registration1 below) and three registrations were used. The following table shows the registrations used (non-default values are highlighted in red text):

Parameter	Registration 1	Registration 2	Registration 3
SIP Server Address	205.168.62.92	205.168.62.92	205.168.62.92
SIP Server Port	5060	5060	5060
SIP Local Port	5060	5061	5062
SIP Local Address	24.69.128.116	24.69.128.116	24.69.128.116
SIP Domain			
SIP Outbound Proxy Address			
SIP Outbound Proxy Port	5060	5060	5060
RTP Port (min)	60000	60200	60300
RTP Port (max)	60199	60299	60399
DTMF Payload ID	101	101	101
Registration Attempts	1	1	1
Registration Timeout	60	60	60
Session Timeout	3600	3600	3600
User Name	2392	2393	2394
Password	******	******	******
Display Name	x2392	x2393	x2394

Notes:

- *The **SIP Server Address** is the IP address of the Avaya SIP Enablement Services server.*
- *The **SIP Local Address** is the IP address of the AlarmPoint Notification server.*
- ***SIP Local Port** must be unique per registration.*
- *The span of values defined between **RPT Port (min) and (max)** mast be unique and cannot overlap with the values for any other registration.*
- *Avaya supplied the **User Names** and **Passwords**.*

6.2. Configure SIP Protocol Provider

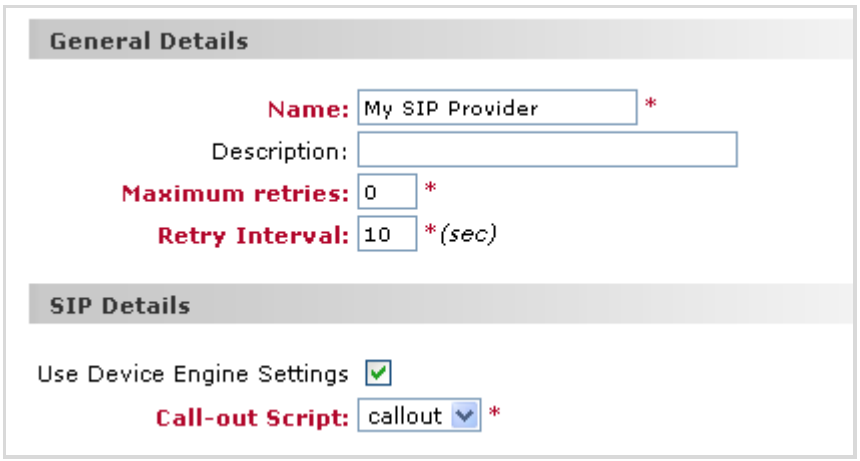
The *AlarmPoint Installation and Administration Guide* provides configuration details for SIP Protocol Providers. During compliance testing, the configuration settings described in the following sections were used.

General Details

- Set **Maximum Retries** to **0**.
  ***Note:** The number of retries was set to 0 to avoid retries during testing.*

SIP Details

- Ensure that **Use Device Engine Settings** is selected.
- Ensure that the **Call-out Script** default is **callout**.



7. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify interoperability between the AlarmPoint Enterprise and an Avaya IP Telephony Solution.

Inbound scenario: A call to AlarmPoint Enterprise
Outbound scenario: A call from AlarmPoint Enterprise

The compliance test included the following:

- AlarmPoint Enterprise successfully registers with SIP Enablement Services.
- Establish calls between AlarmPoint Enterprise and Avaya SIP and H.323 IP telephones attached to SIP Enablement Service or Communication Manager.
- Inbound blind transfer
- Inbound consult transfer ***(see observation 1 below)***
- Outbound blind transfer
- Outbound consult transfer
- Multiple Inbound calls (three) and consult transfer to a simulated conference bridge, using Avaya 9630 H.323 telephone
- Multiple outbound calls (three) and consult transfer to a simulated conference bridge, using Avaya 9630 H.323 telephone
- With Multiple outbound calls, dropping a call and adding a call ***(see observation 2 below)***
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones. This allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

During the testing the following observations were made:

1) During the consult transfer scenario, the transfer was not successful (Protocol Mismatch). Communication Manager 5.2.1 with Service Pack 2 fixed the problem.

2) In some scenarios after a user dropped from the conference and AlarmPoint added another user to the conference, the conference party count increased by two, instead of one. This is being investigated by the Avaya team.

8. Verification Steps

This section provides verification steps that may be performed in the field to verify that AlarmPoint Enterprise can place outbound and receive inbound PSTN, H.323 and SIP calls.

1. Verify that SIP endpoints were able to register with SIP Enablement Services.
2. Verify the test cases in Section 7 using the **traceSES** command in the SIP Enablement Services server.
3. Verify that AlarmPoint Enterprise can make outbound call, and DTMF works.
4. Verify that AlarmPoint Enterprise can receive inbound call, and DTMF works.

9. Conclusion

These Application Notes describe the configuration necessary to connect Communication Manager and SIP Enablement Services to AlarmPoint Enterprise. The AlarmPoint Enterprise is a SIP-based endpoint solution. During the compliance test, all test cases passed except for the observations noted in Section 7.

10. References

This section references the documentation relevant to these Application Notes.
Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura™ Communication Manager*, May 2009, Document Number 03-300509.
[2] *Avaya Aura™ Communication Manager Feature Description and Implementation,* May 2009, *D*ocument Number 555-245-205.
[3] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, May 2009, Document Number 555-245-206.

Product information for AlarmPoint products may be found at http://connect.alarmpoint.com.
The following AlarmPoint Enterprise document was provided by AlarmPoint.

[4] *AlarmPoint Installation and Administration Guide,* Version 4.0, January 2010.

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 DevConnect Program at devconnect@avaya.com.