Avaya Solution & Interoperability Test Lab

Application Notes for Noble Systems with Avaya Aura™ SIP Enablement Services and Avaya Aura™ Communication Manager – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for Noble Systems Noble® Solution to interoperate with Avaya Aura™ SIP Enablement Services and Avaya Aura™ Communication Manager using SIP trunks.

The Noble® Solution is an outbound/predictive dialing and inbound call management solution that interfaces with Avaya Aura™ Communication Manager. The Noble® Solution supports various trunk interfaces to Communication Manager. This document covers only the SIP interface to Communication Manager via SIP Enablement Services.

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

The Noble® Solution is an automated contact handling system that combines outbound predictive dialing and inbound ACD (automatic call distributor) switch functionality with blended call management, an integrated relational database, real-time reporting, advanced solutions, and advanced network environments.

The Noble® Solution manages telephony resources to automate and organize outbound campaigns and resources. The predictive dialing solution controls the dialing process, voice detection, call switching and screen pops. The inbound ACD capabilities perform ANI/DNIS detection and use extensive logical call control management to direct the call to the appropriate agent. Noble Systems maintains all campaigns, programs, groups, and agents, whether inbound or outbound, and records extensive data logs to track overall system performance.

The Noble® Solution supports various trunk interfaces to Communication Manager. This document covers only the SIP interface to Communication Manager via SIP Enablement Services.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on feature functionality and serviceability. The feature functionality testing evaluated the ability of the Noble® Solution to successfully establish SIP trunks to Communication Manager via SIP Enablement Services and to use those trunks to perform the following functions:

- Outbound Calls/Predictive Dialing: the ability to place outbound calls and then deliver the answered calls to available agents.
- Inbound Call Management: the ability to automatically distribute inbounds calls to available agents.

The serviceability testing introduced several failure conditions to see if the Noble® Solution could properly resume operation after each failure recovery.

1.2. Support

Technical support for the Noble® Solution can be obtained by contacting Noble Systems at:

- Phone: 1 (888) 966-2539
- Web: http://www.noblesys.com/contact.aspx
- Email: info@noblesys.com

2. Reference Configuration

The figure below shows the configuration used during compliance testing. The configuration is comprised of an Avaya S8500 Media Server running Communication Manager (with an Avaya G650 Media Gateway), SIP Enablement Services, the Noble® Solution server, and agents (both H.323 and SIP endpoints). SIP trunks are used to connect Communication Manager and the Noble® Solution server via SIP Enablement Services. All calls to and from the Noble® Solution server are carried over these SIP trunks. Outbound calls are placed from the Noble® Solution server to the simulated PSTN. When the calls are answered, the calls are delivered to the agent endpoints on Communication Manager. Additionally, inbound trunks calls are placed from the PSTN to the Noble® Solution server, and then the calls are delivered to the agent endpoints on Communication Manager.

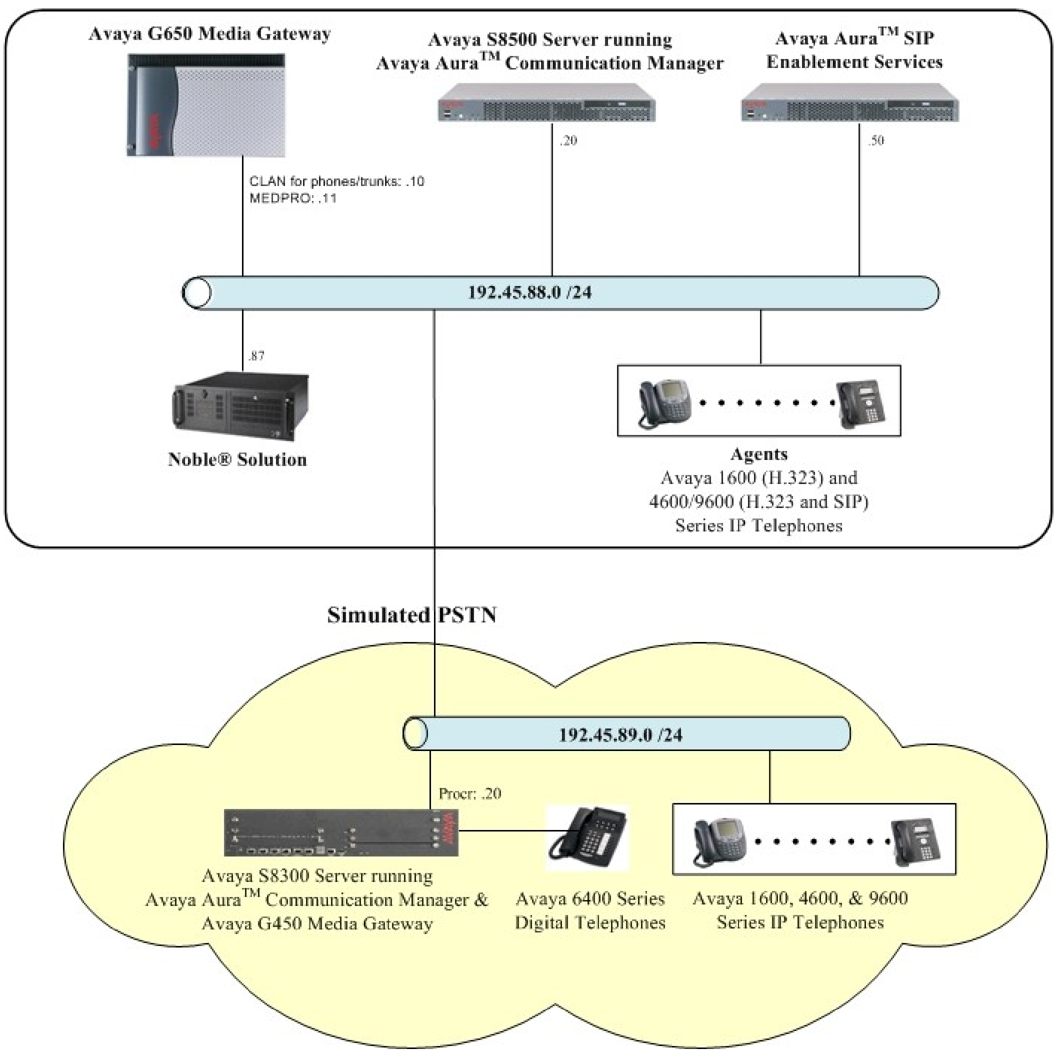


Figure 1: Noble® Solution with Communication Manager and SIP Enablement Services

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server (w/ G650)	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya S8300 Server (w/ G450)	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G650 Media Gateway:	
TN799DP (C-LAN)	HW01, FW026
TN2602AP (MEDPRO)	HW02, FW007
TN2312BP (IPSI)	HW15, FW030
Avaya G450 Media Gateway :	
MM710BP (DS1)	HW11, FW044
MM712AP (DCP)	HW07, FW009
Avaya Aura™ SIP Enablement Services (SES) Server	5.2 (SES05.2-02.0.947.3a)
Avaya 1600 Series IP Phones :	
1608SW (H.323)	1.0.3
1616SW (H.323)	1.0.3
Avaya 4600 Series IP Phones:	
4610SW (H.323)	2.9
4620SW (H.323)	2.9
4621SW (H.323)	2.9
Avaya 9600 Series IP Phones:	
9620 (H.323)	3.002
9630 (SIP)	2.4.1
Avaya 6400 Series Digital Phones	-
Noble® Solution Server	4000.12

4. Configure Communication Manager

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Communication Manager, refer to the Avaya product documentation, **Reference [1].**

The information shown on the screens throughout this section indicate the values that were used during compliance testing.

4.1. Verify Communication Manager License

This section provides the steps required to verify that Communication Manager has the proper licenses for the features illustrated in these Application Notes.

1. Enter the **display system-parameters customer-options** command and navigate to **Page 2**. Verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 450   44
           Maximum Concurrently Registered IP Stations: 18000 5
             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: 50    0
                        Maximum Video Capable Stations: 50    0
                   Maximum Video Capable IP Softphones: 50    0
                       Maximum Administered SIP Trunks: 450   48
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                          Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

        (NOTE: You must logoff & login to effect the permission changes.)
```

The license file installed on the system controls the maximum permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

4.2. Configure IP Codec Sets & IP-Network Regions

This section provides the steps required for configuring an ip-codec-set and ip-network regions.

1. Enter the **change ip-codec-set <codec set number>** command, where **<codec set number>** is the codec set number to be used with the Noble® Solution.

   - In the **Audio Codec** field(s), type the codec(s) to be used with the Noble® Solution (e.g. **G.711MU**).*

   *** NOTE:** If any G.729 codec is used with the Noble® Solution, it is required to administer all of the G.729 codecs (G.729, G.729A, G.729B, and G.729AB) on this form.

```
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:


     Media Encryption
 1: none
 2:
 3:
```

2. Enter the **change ip-network-region <region number>** command, where **<region number>** is the ip network region number to be used with the Noble® Solution.

    - In the **Authoritative Domain** field, enter the SIP domain name of the SES server from **Section 5.1.**
    - In the **Code Set** field, enter the **<codec set number>** administered in **Step 1**. The **Codec Set** field reflects the codec set that must be used for connections between phones within this region or between phones and media processor boards within this region.
    - Direct media shuffling must be disabled with the Noble® Solution. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields to **no**.

```
change ip-network-region 1                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: dev8.com
    Name: interop
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 48      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 48       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
```

4.3. Configure Node Names and IP Interfaces

This section provides the steps required for configuring node names and IP interfaces.

1. Enter the **change node-names ip** command and create node entries for the Communication Manager CLAN (or procr) to be used for the SIP trunk, the SIP Enablement Services (SES) server, and the Noble® Solution server.

    - In the **Name** field, type a descriptive name to assign to each node.
    - In the **IP Address** field, type the IP address that will be assigned to each node.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
8300                    192.45.89.20
CLAN                    192.45.88.10
CLAN2                   192.45.88.13
CLAN3                   192.45.88.14
CLAN4                   192.45.88.15
Gateway001              192.45.88.1
LSP-8300                192.45.88.30
Member-CDR              192.168.199.69
NobleSystems            192.45.88.85
RDTT-CDR                192.45.88.45
SES                     192.45.88.50
cf-medpro               192.45.88.11
default                 0.0.0.0
ipoffice                192.45.88.40
procr                   192.45.88.20
```

2. Enter the **add ip-interface <board location>** command, where **<board location>** is the board location for the CLAN, for example: 01A02.

   - In the **Enable Interface** field, type **y**.
   - In the **Network Region** field, type the network region number administered in **Section 4.2**.
   - In the **Node Name** field, type the CLAN node name from **Step 1** above.
   - In the **Ethernet Link** field, type an available Ethernet link number.

```
add ip-interface 01a08                                          Page   1 of   3
                                  IP INTERFACES


                  Type: C-LAN
                  Slot: 01A02       Target socket load and Warning level: 400
           Code/Suffix: TN799  D          Receive Buffer TCP Window Size: 8320
     Enable Interface? y                           Allow H.323 Endpoints? y
                  VLAN: n                           Allow H.248 Gateways? y
       Network Region: 1                             Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: CLAN
           Subnet Mask: /24
     Gateway Node Name:

         Ethernet Link: 1
```

4.4. Configure Signaling Group (CM - Noble Systems)

This section provides the steps required for configuring a signaling group.

1. Administer a signaling group by using the "**add signaling-group s**" command, where **s** is an available signaling-group number. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit the form.

   - **Group Type: sip**
   - **Transport Method: tls**
   - **Near-end Node Name:** Enter the CLAN node name from **Section 4.3**.
   - **Far-end Node Name:** Enter the SES server node name from **Section 4.3**.
   - **Near-end Listen Port: 5061**
   - **Far-end Listen Port: 5061**
   - **Far-end Network Region:** Enter the network region number from **Section 4.2.**
   - **Far-end Domain:** Enter the IP Address of the Noble® Solution server.
   - **Direct IP-IP Audio Connections? n**

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

 Group Number: 1             Group Type: sip
                       Transport Method: tls
  IMS Enabled? n
     IP Video? n




   Near-end Node Name: CLAN                  Far-end Node Name: SES
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
Far-end Domain: 192.45.88.85

                                     Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                   IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                          Alternate Route Timer(sec): 6
```

4.5. Configure Trunk Group (CM – Noble Systems)

This section provides the steps required for configuring a trunk group.

1. Administer a SIP trunk group by using the "**add trunk-group t**" command, where **t** is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

   - **Group Type: sip**
   - **Group Name:** Enter a descriptive name (e.g. **To Noble**).
   - **TAC:** Enter a Trunk Access Code that is valid under the provisioned dial plan (e.g. ***001**).
   - **Service Type: tie**
   - **Signaling Group:** Enter the signaling group number from **Section 4.4**.
   - **Number of Members:** Enter desired number of members.

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

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: To Noble                    COR: 1        TN: 1        TAC: *001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                     Signaling Group: 1
                                                   Number of Members: 24
```

4.6. Configure Signaling Group (CM - SES)

This section provides the steps required for configuring a signaling group.

1. Administer a signaling group by using the "**add signaling-group s"** command, where **s** is an available signaling-group number. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit the form.

   - **Group Type: sip**
   - **Transport Method: tls**
   - **Near-end Node Name:** Enter the CLAN node name from **Section 4.3**.
   - **Far-end Node Name:** Enter the SES server node name from **Section 4.3**.
   - **Near-end Listen Port: 5061**
   - **Far-end Listen Port: 5061**
   - **Far-end Network Region:** Enter the network region number from **Section 4.2**.
   - **Far-end Domain:** Enter the SIP domain name of SES server from **Section 5.1**.
   - **Direct IP-IP Audio Connections? n**

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

 Group Number: 1             Group Type: sip
                       Transport Method: tls
  IMS Enabled? n
     IP Video? n




   Near-end Node Name: CLAN                   Far-end Node Name: SES
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1
Far-end Domain: dev8.com

                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                                  Alternate Route Timer(sec): 6
```

4.7. Configure Trunk Group (CM - SES)

This section provides the steps required for configuring a trunk group.

1. Administer a SIP trunk group by using the "**add trunk-group t**" command, where **t** is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type: sip**
- **Group Name:** Enter a descriptive name (e.g. **To SES**).
- **TAC:** Enter a Trunk Access Code that is valid under the provisioned dial plan (e.g. ***007**).
- **Service Type: tie**
- **Signaling Group:** Enter the signaling group number from **Section 4.6**.
- **Number of Members:** Enter desired number of members.

```
add trunk-group 7                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 7                   Group Type: sip            CDR Reports: y
  Group Name: To SES                     COR: 1        TN: 1        TAC: *007
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                      Signaling Group: 7
                                                    Number of Members: 24
```

This completes the Avaya Aura™ Communication Manager configuration.

5. Configure SIP Enablement Services

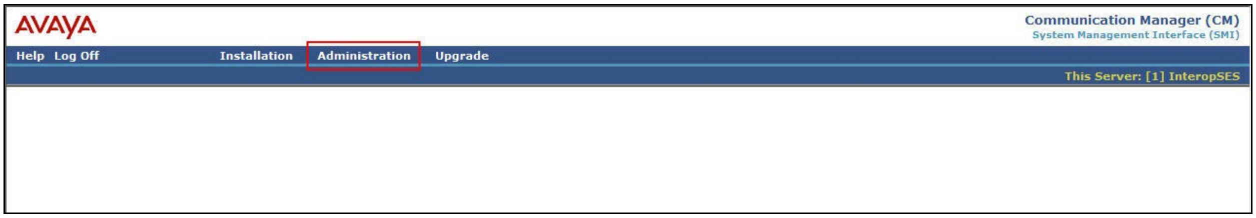
This section provides the procedures for configuring Avaya Aura™ SIP Enablement Services. The procedures include the following:

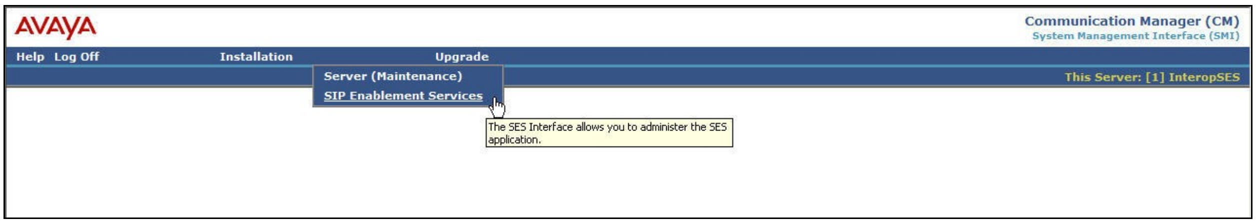
- Obtain SIP Domain
- Obtain Host Information
- Configure Communication Manager Server Interface
- Configure Communication Manager Server Address Maps
- Configure Trusted Hosts

This section assumes that the installation and basic administration of the SIP Enablement Services server has already been performed. For more information on administering SIP Enablement Services, refer to the Avaya product documentation, **Reference [2]**.

1. Launch a web browser and enter https://<IP address of SES Server>/admin in the address field. Log in with the appropriate credentials.

2. Select **Administration > SIP Enablement Services**.



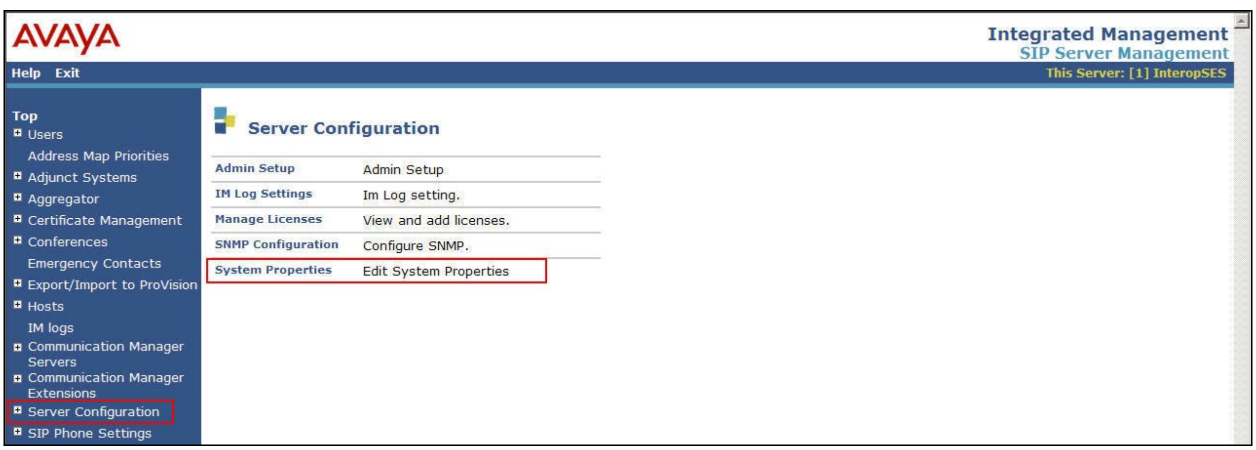


Note: These Application Notes assume the SIP Enablement server has already been configured with the proper domain and host information.

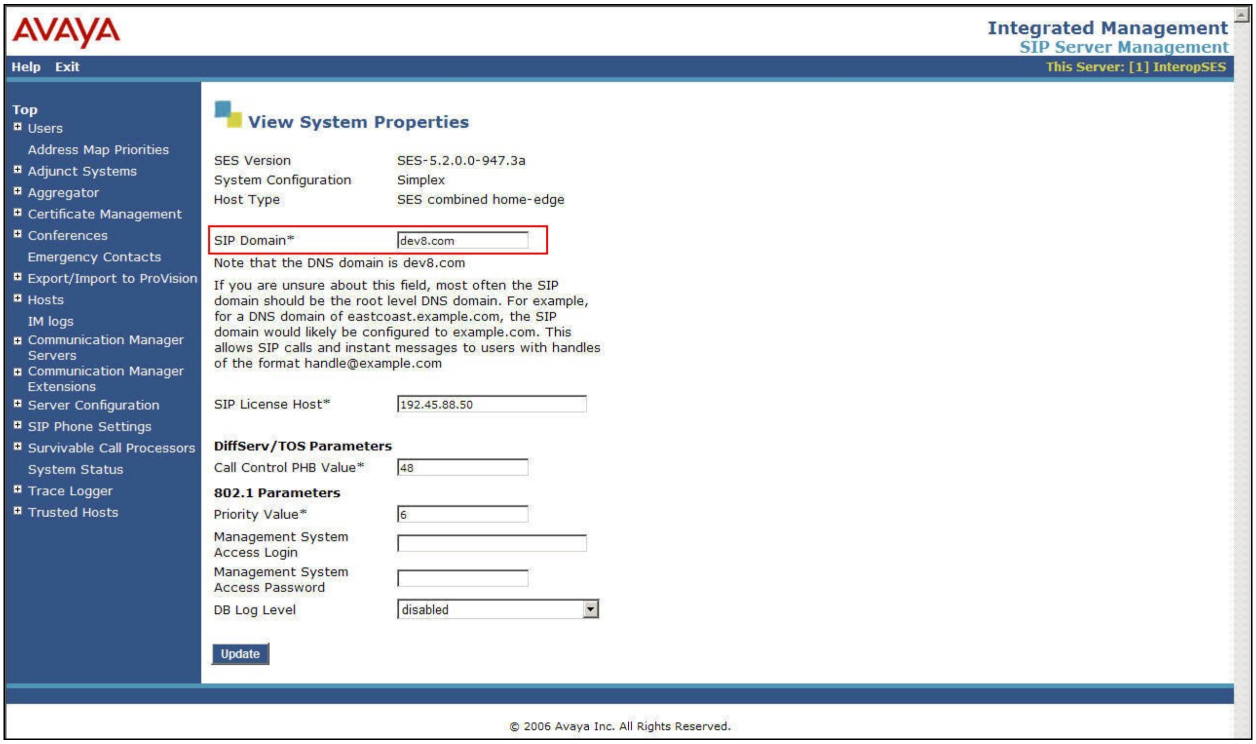
5.1. Obtain SIP Domain

This section provides the steps required to obtain the SIP Domain.

1. Select **Server Configuration** from the left pane and then select **System Properties**.



2. Use the value in the **SIP Domain** field (in this case **dev8.com**) for configuring the **Authoritative Domain** and **Far-end Domain fields** in **Sections 4.2** and **4.6** respectively.

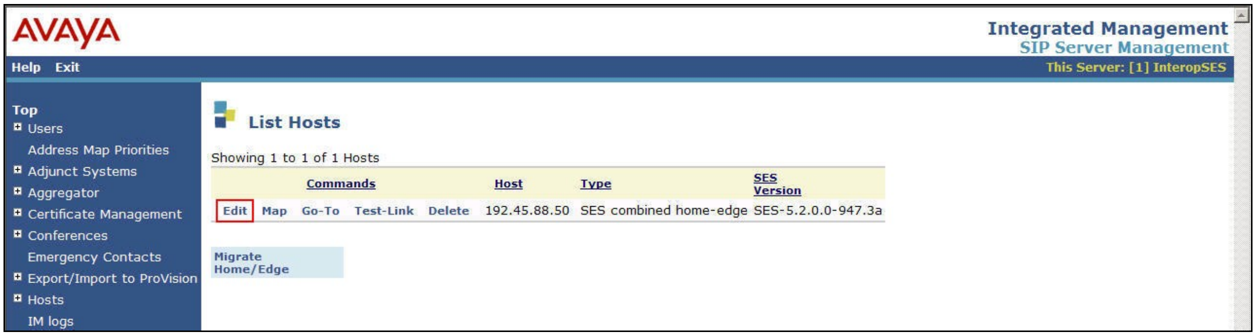


5.2. Obtain Host Information

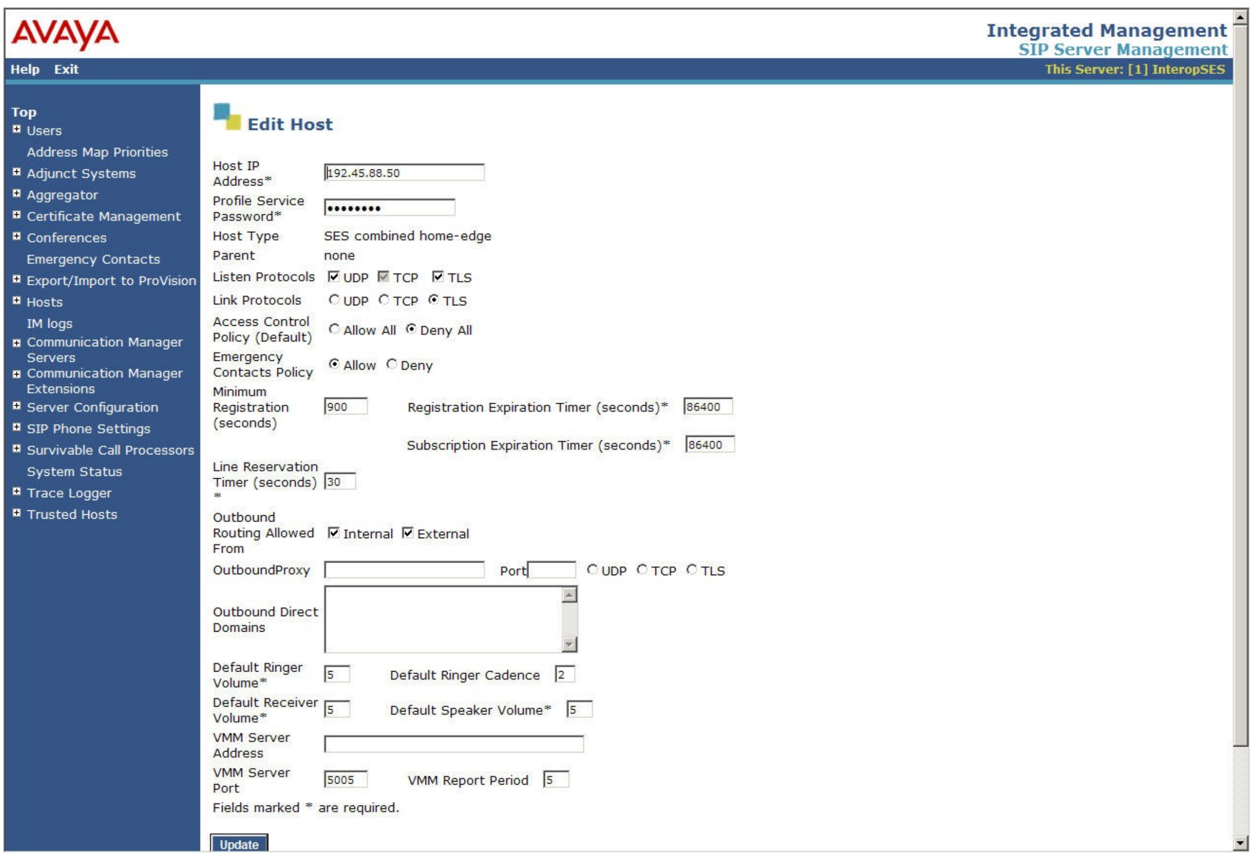
This section provides the steps required to obtain the Host information.

1. Select **Hosts** from the left pane and then select **List Hosts**.

2. For the compliance testing, only one host was administered as both the edge and home server, as indicated by the **SES combined home-edge** value in the **Type** field shown below. The IP address of this home server is **192.45.88.50**, indicated in the **Host** field. This IP Address will be used to configure the Communication Manager server interface. To view more details or to make any modifications, click **Edit**.



3. Verify the configuration.



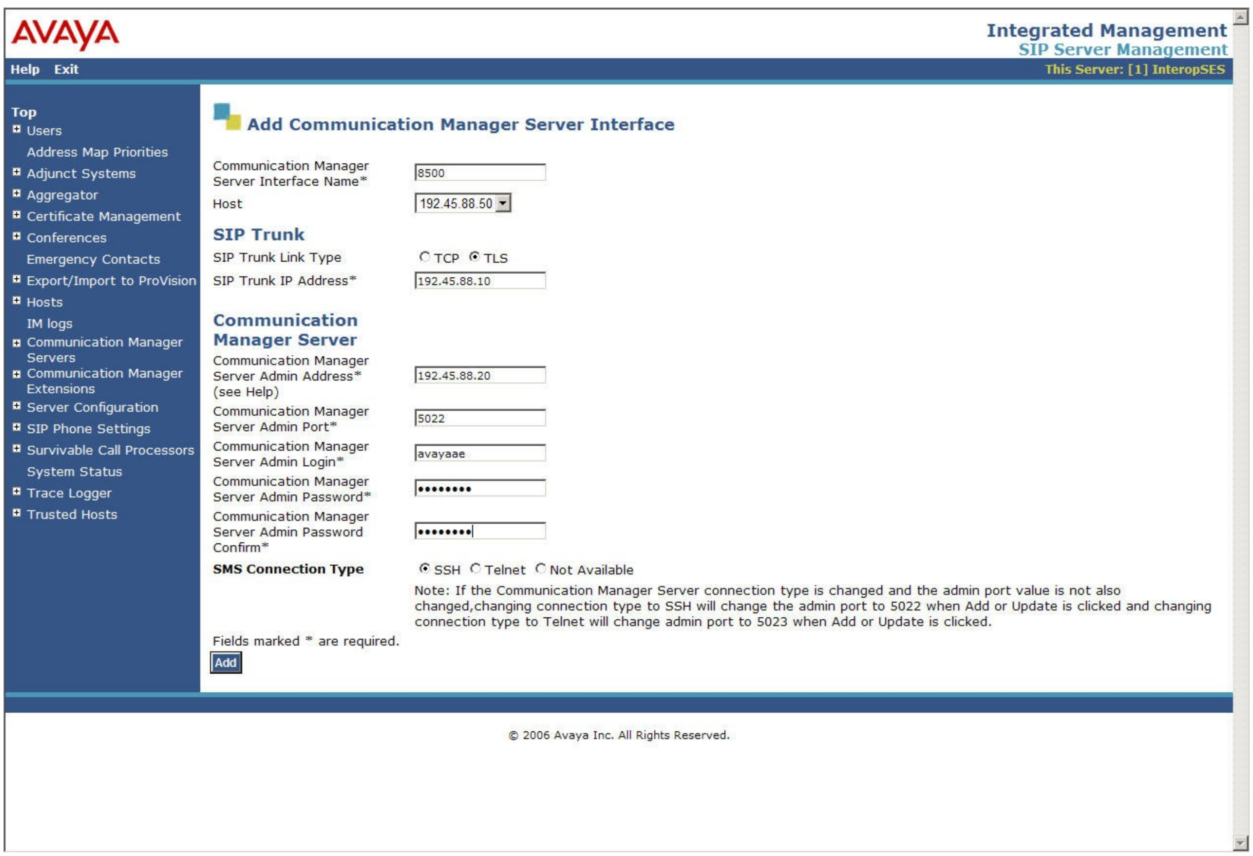
5.3. Configure Communication Manager Server Interface

This section provides the steps required to configure a Communication Manager server interface.

1. Select **Communication Manager Servers** from the left pane and then select **Add Communication Manager Server**.

2. This screen associates a Communication Manager server with a host. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click on **Add** at the bottom of the screen to submit these changes.

- **Communication Manager Server Interface Name:** Enter a descriptive name.
- **Host:** Select the IP address of the SES server.
- **SIP Trunk Link Type: TLS**
- **SIP Trunk IP Address:** Enter the CLAN IP address from **Section 4.3**.
- **Communication Manager Server Admin Address:** Enter the IP address of the Communication Manager.
- **Communication Manager Server Admin Port: 5022**
- **Communication Manager Server Admin Login:** Enter valid credentials.
- **Communication Manager Server Admin Password:** Enter valid credentials.
- **Communication Manager Server Admin Password Confirm:** Enter valid credentials.

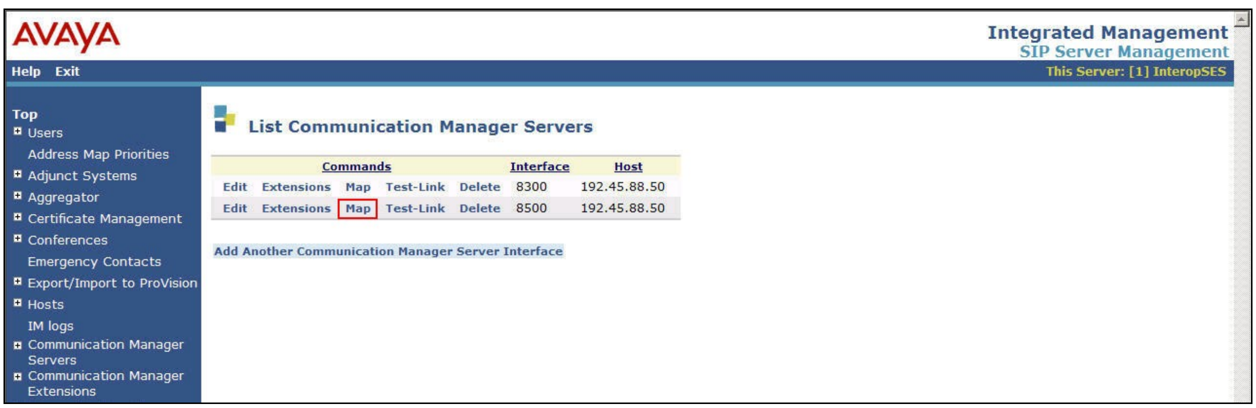


5.4. Configure Communication Manager Server Address Maps

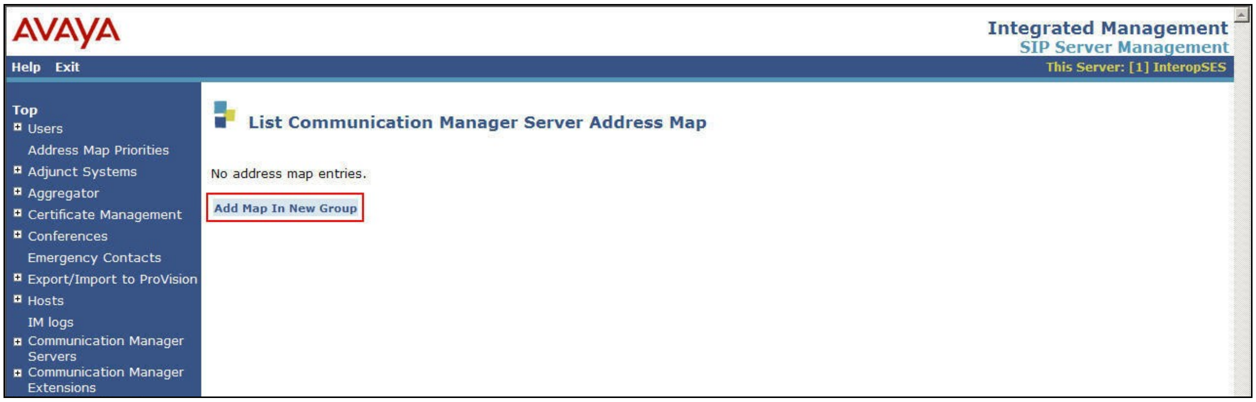
This section provides the steps required to configure Communication Manager server address maps.

1. Select **Communication Manager Servers** from the left pane and then select **List Communication Manager Servers**.

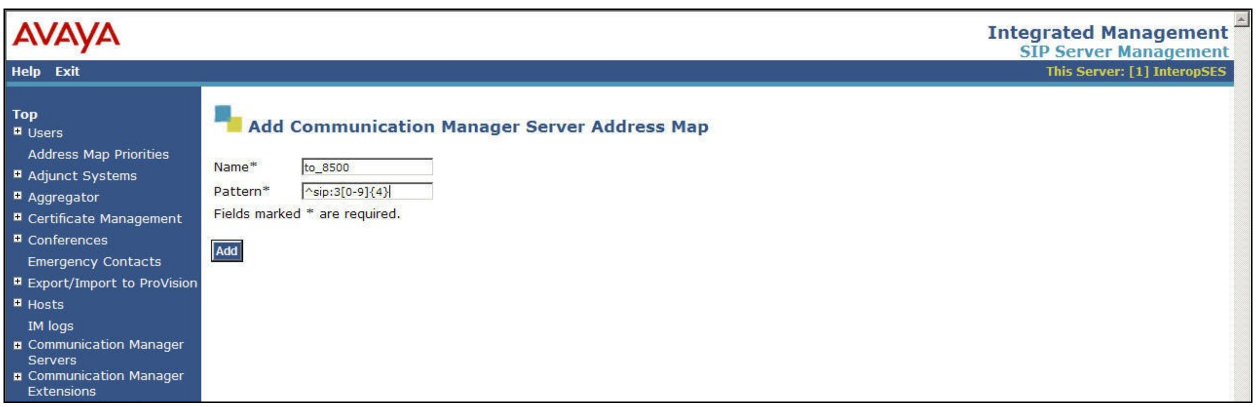
2. Click on the **Map** link.



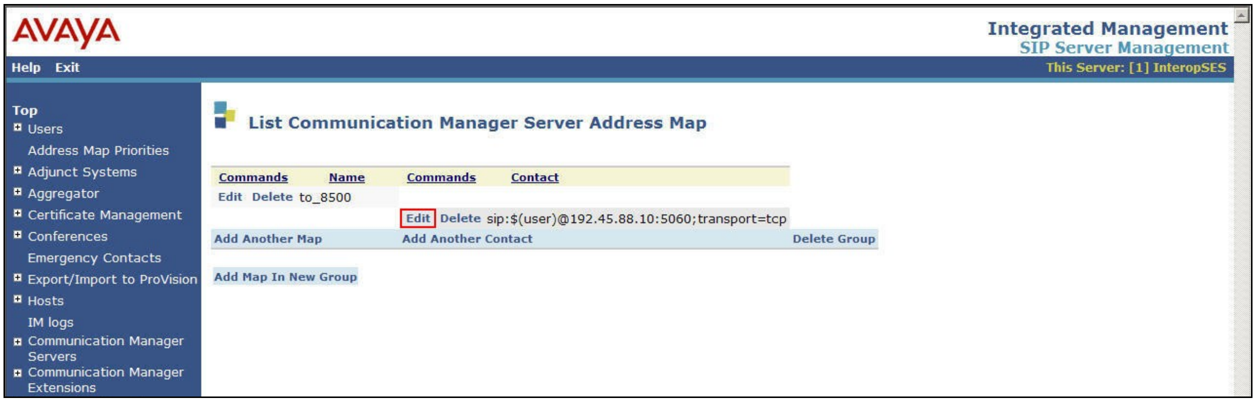
3. Select **Add Map In New Group**.



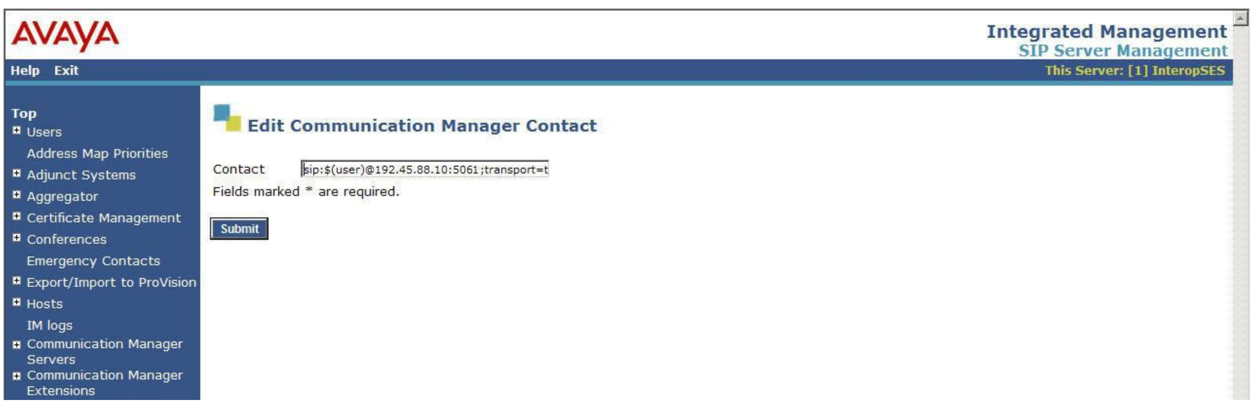
4. The **Add Communication Manager Server Address Map** screen is displayed next. This screen is used to specify which calls are to be routed to Communication Manager. For the **Name** field, enter a descriptive name to denote the routing. For the **Pattern** field, enter an appropriate syntax for address mapping. For the interoperability testing, a pattern of **^sip:3[0-9]{4}** was used to match to any Communication Manager extensions in the range of 30000-39999. Click **Add**.



5. The **List Communication Manager Server Address Map** screen is displayed, and it is updated with the new address map and contact information. If **Contact** is not correct, click **Edit** to modify the information.



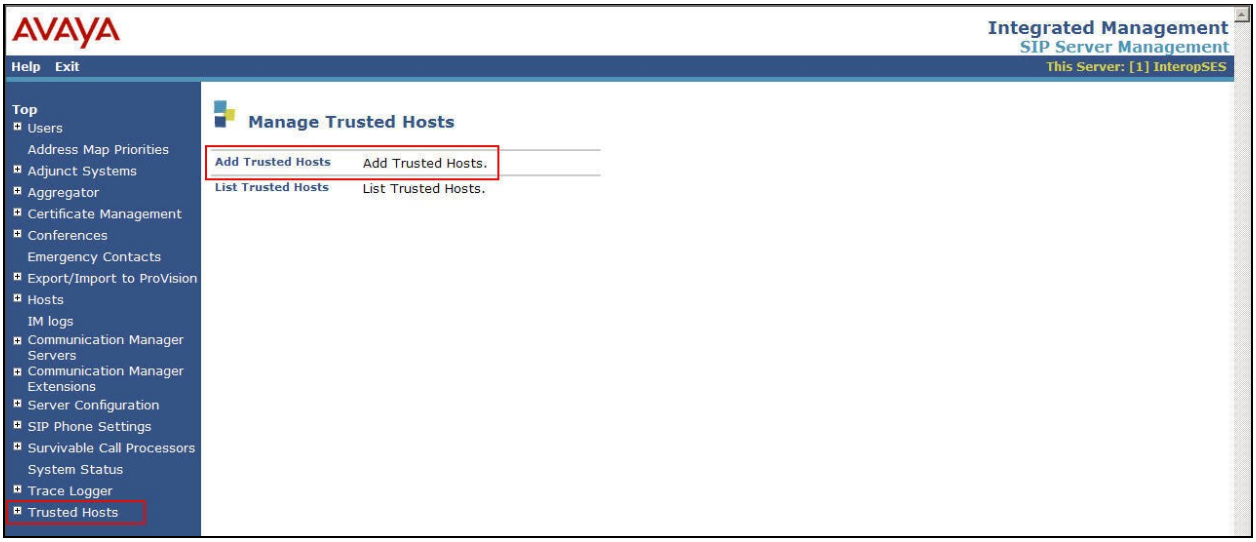
6. Enter the contact **sip:$(user)@<destination-IP-address>:5061;transport=tls**, where the **<destination-IP-address>** is the IP address of the CLAN from **Section 4.3**. Avaya SES will substitute "$(user)" with the user portion of the request URI before sending the message. Click **Submit**.



5.5. Configure Trusted Hosts

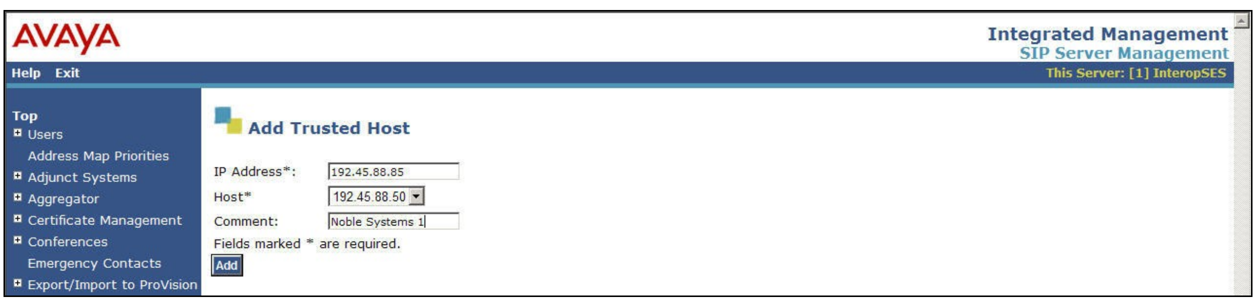
This section provides the steps required for configuring a trusted host.

1. Select **Trusted Hosts** from the left pane and then click on **Add Trusted Hosts**.

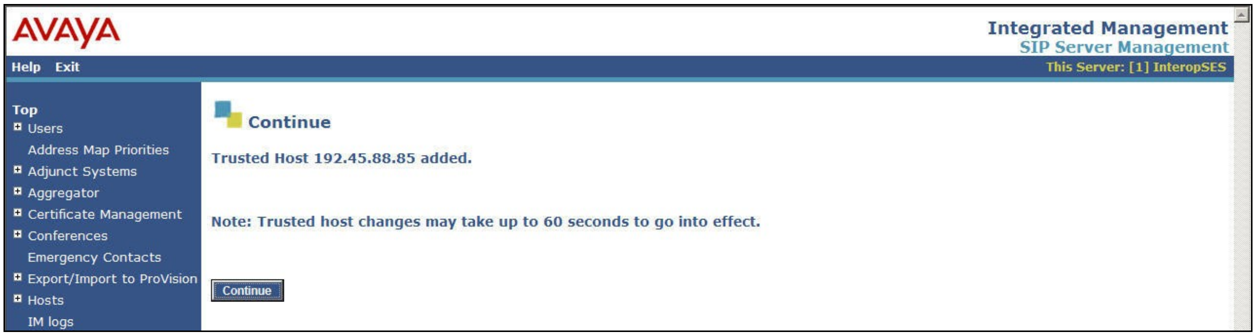


2. Administer a trusted host by entering the following values for the specified fields and then click **Add**.

- **IP Address:** IP Address of the Noble® Solution server
- **Host:** Use the pull down menu to select the Host IP Address obtained in **Section 5.2**.



3. Click **Continue** and the repeat Steps 1 and 2 for any additional IP addresses used by the Noble® Solution server.



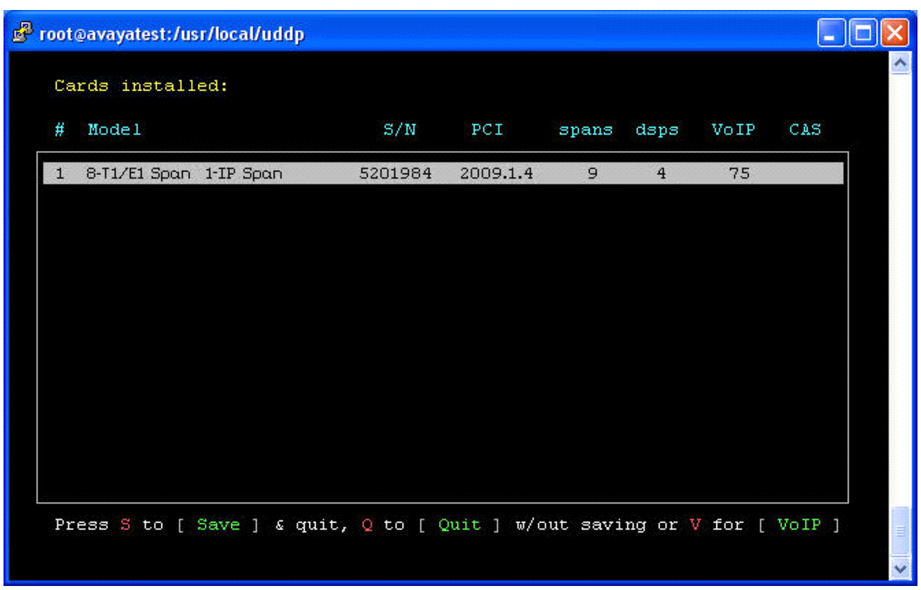
This completes the Avaya Aura™ SIP Enablement Services configuration.

6. Configure the Noble® Solution Server

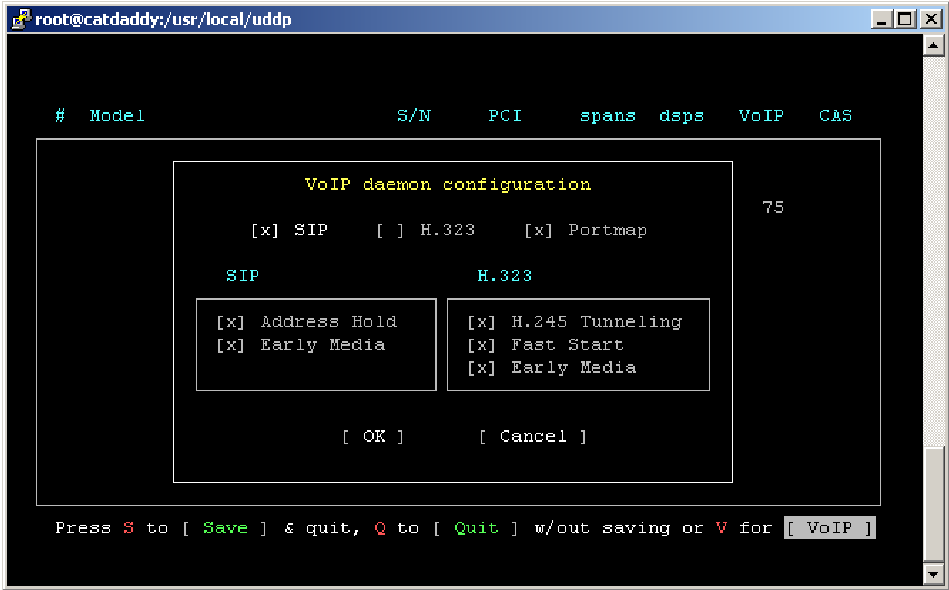
This section describes the configuration required on the Noble® Solution server to establish a SIP trunk with Avaya Aura™ Communication Manager. This configuration change can only be performed by authorized Noble personnel.

1. Log in to the Noble® Solution server with the proper credentials.

2. Select the card to be configured and press **V** for **VOIP**.



3. Select **SIP** and save all changes.



7. General Test Approach and Test Results

The general test approach was to place calls to and from the Noble® Solution server to verify it could properly managed outbound and inbound calls while connected to Avaya Aura™ Communication Manager via a SIP interface. Outbound calls were placed from the Noble® Solution server to a simulated PSTN. When the calls were answered, they were delivered over a SIP trunk to agent endpoints on Communication Manager. Additionally, inbound calls were placed from the PSTN to the Noble® Solution server, and then the calls were delivered over a SIP trunk to agent endpoints on Communication Manager.

For serviceability testing, failure conditions were introduced into the test configuration to verify that the Noble® Solution server could properly resume operation after failure recovery. These failure conditions included network cable pulls, signaling-group and trunk-group busyouts, and server resets.

All test cases were executed and passed.

8. Verification Steps

This section provides the steps that can be performed to verify proper configuration of the SIP Enablement Server, Communication Manager and the Noble® Solution server.

1. From the SAT, enter the command **status signaling-group s**, where **s** is the number of the signaling group configured in **Section 4.4**, and verify that the **Group Stat**e is "**in-service**". Repeat this step for the signaling group configured in **Section 4.6**.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1                            Active NCA-TSC Count: 0
      Group Type: sip                           Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

2. From the SAT, enter the command **status trunk t**, where **t** is the number of the trunk group configured in **Section 4.5**, and verify that the **Service State** for each trunk group member is either "**in-service/idle**" or "**in-service/active**". Repeat this step for the trunk group configured in **Section 4.7**.

```
status trunk 1                                                    Page   1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
0001/011 T00011   in-service/idle    no
0001/012 T00012   in-service/idle    no
0001/013 T00013   in-service/idle    no
0001/014 T00014   in-service/idle    no
```

3. Place an outbound call from the Noble® Solution to the PSTN. Verify the call is originated successfully and when the call is answered, verify the Noble® Solution server successfully delivers the call over a SIP trunk to an available agent on Communication Manager.

9. Conclusion

These Application Notes describe the steps required for configuring a SIP trunk between Avaya Aura™ Communication Manager 5.2 and the Noble® Solution server 4000.12 via Avaya Aura™ SIP Enablement Services. During compliance testing, the Noble® Solution server successfully managed inbound and outbound calls while configured with SIP interfaces. All feature and serviceability test cases were completed and passed.

10. Additional References

This section references the Avaya and Noble Systems product documentation that are relevant to these Application Notes.

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

[1] *Administering Avaya Aura™ Communication Manager,* Doc ID: 03-300509, Issue 5.0, Release 5.2, May 2009
[2] *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server*, Doc ID: 03-602508, Issue 2.0, May 2009

The following Noble Systems documentation was used during installation and configuration, and can be obtained by contacting Noble Systems support by phone, 888.9NOBLE9 (888.966.2539) or email, info@noblesys.com.

[3] *Noble Installation and Configuration of UDDP*
[4] *Maestro 2008.3.2 Express User Reference Manual*
[5] *Maestro 2008.3.2 Enterprise User Reference Manual*
[6] *Composer 8 v2008.4.2 Agent Manual*
[7] *Composer 8 v2008.4.2 Product Reference Manual*

11. Change History

Issue	Date	Reason
1.1	03/10/2010	Updated text and picture in the sixth step of Section 5.4 to reference port 5061, rather than port 5060
1.0	08/20/2009	Initial issue

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.