Avaya Solution & Interoperability Test Lab

Application Notes for IPC UnigyV2 with Avaya Aura® SIP Enablement Services using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC UnigyV2 to interoperate with Avaya Aura® Communication Manager 5.2.1 and Avaya Aura® 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

These Application Notes describe the configuration steps required for IPC UnigyV2 to interoperate with Avaya Aura® Communication Manager using Avaya Aura® SIP Enablement Services (SES).

The Unigy Platform is a unified trading communications system designed specifically to make the entire trading ecosystem more productive, intelligent and efficient. Based on an SIP-enabled, open and distributed architecture, Unigy utilizes the latest, standards-based technology to create a groundbreaking, innovative Unified Trading Communications (UTC) solution.

Unigy is the first to offer a portfolio of devices and applications that serve the entire trading workflow, across the front, middle and back offices

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among IPC turret users with Avaya SIP, Avaya H.323, Avaya Digital, and/or PSTN users. Call controls were performed from various users to verify the call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to IPC UnigyV2.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, display, G.711MU, G.729AB, codec negotiation, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and attended conference.

The serviceability testing focused on verifying the ability of IPC UnigyV2 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to IPC UnigyV2.

2.2. Test Results

All test cases were executed and verified. The following were the observations on IPC UnigyV2 from the compliance testing.

- IPC does not support domain name, therefore the domain name on the Avaya SIP trunk group and network region must be left blank to accommodate this. During the test IP address was utilized on IPC side.

- IPC does not support media shuffling, therefore corresponding parameters must be disabled on the Avaya signaling group and network region. Furthermore, IPC does not support asymmetric codec, so the supported codec order must be in sync between IPC and Avaya.

- IPC does not support interpretation of DMTF digits from Avaya endpoints, so the DTMF tests only covered the Avaya interpretation of DMTF digits from IPC turrets.

- For call forwarding scenarios involving Avaya SIP endpoints calling IPC turrets that are forwarded back to PSTN, the Avaya SIP endpoint will show two active call appearances after the call diverts.

2.3. Support

Technical support on IPC UnigyV2 can be obtained through the following:

- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** systems.support@ipc.com

3. Reference Configuration

As shown in the test configuration below, IPC UnigyV2 at the Remote Site consists of the Media Manager, Converged Communication Manager, and Turrets. The Media Manager and Converged Communication Manager are typically deployed on separate servers. In the compliance testing, the same server hosted the Media Manager and Converged Communication Manager.

SIP trunks are used from IPC UnigyV2 to Avaya Aura® SIP Enablement Services, to reach users on Avaya Aura® Communication Manager and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges were associated with Avaya Aura® Communication Manager users at the Central site (H.323 - 2200x, SIP – 2800x, DCP - 22009), and IPC turret users at the Remote site (7205x).

The detailed administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® SIP Enablement Services is not the focus of these Application Notes and will not be described.

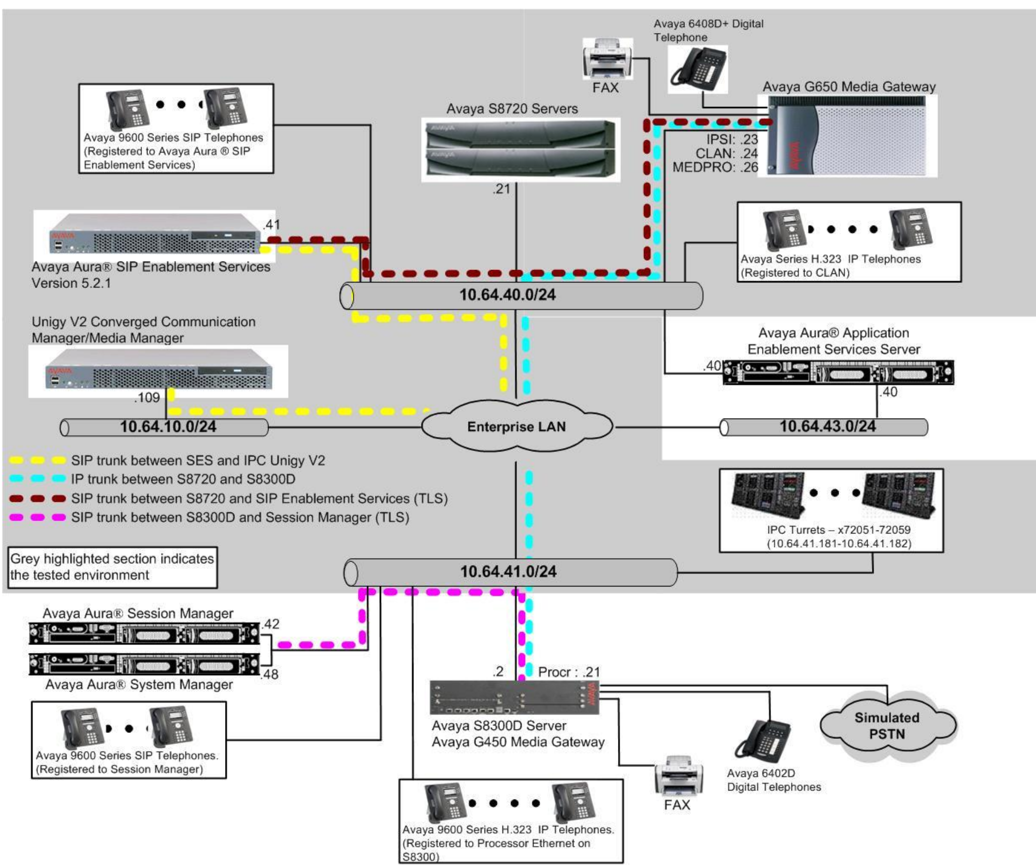


Figure 1: Test Configuration of IPC UnigyV2

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8720 Servers	(R015x.02.1.016.4-19880)
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor	 HW01 FW028 HW20 FW118
Avaya Aura® SIP Enablement Services	5.2.1 SP4 (SES-5.2.1.0-016.4-SP4C)
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 9630 IP Telephone (SIP)	2.6.8
Avaya 6408D Digital Telephone	NA
IPC UnigyV2 • Media Manager • Converged Communication Manager • Turrets	 02.00.00.00.1495 02.00.00.00.1495 02.00.00.00.1495

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer public unknown numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer ISDN trunk group
- Administer tandem calling party number

In the compliance testing, the same set of codec set, network region, trunk group, and signaling group were used for the Avaya SIP and IPC turret users, which enabled IPC turret users to use the same digits dialing as Avaya SIP users, to reach other users on Communication Manager and on the PSTN.

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2**, and 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 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.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   25
           Maximum Concurrently Registered IP Stations: 18000 4
             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: 5     0
                  Maximum Video Capable H.323 Stations: 5     0
                   Maximum Video Capable IP Softphones: 5     0
                       Maximum Administered SIP Trunks: 100   60
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
```

5.2. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming call from IPC back out to IPC (incoming trunk to outgoing trunk), and to transfer an outgoing call to IPC to another outgoing call to IPC (outgoing trunk to outgoing trunk). For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
display system-parameters features                              Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: none
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

5.3. Administer SIP Trunk Group

Use the "change trunk-group n" command, where "n" is the existing SIP trunk group number used to reach SES, in this case "201".

For **Group Name**, update as desired to reflect the same trunk group used to reach SES and IPC. For **Number of Members**, enter sufficient number for simultaneous calls to Avaya SIP and IPC users.

```
change trunk-group 201                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 201                  Group Type: sip           CDR Reports: y
  Group Name: To SES                      COR: 1        TN: 1        TAC: 116
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                     Signaling Group: 201
                                                   Number of Members: 10
```

Navigate to **Page 3**, and enter "public" for **Numbering Format**.

```
change trunk-group 201                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: internal
                                                          Maintenance Tests? y



                      Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

5.4. Administer SIP Signaling Group

Use the "change signaling-group n" command, where "n" is the existing SIP signaling group number used by the SIP trunk group from **Section 5.3**.

For **Far-end Domain**, leave the field blank since IPC UnigyV2 does not support domain name. For **DTMF over IP**, enter "rtp-payload". For **Direct IP-IP Audio Connections**, enter "n". Make a note of the **Far-end Network Region** number.

```
change signaling-group 201                                      Page   1 of   1
                                SIGNALING GROUP

 Group Number: 201             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
     IP Video? n




   Near-end Node Name: CLAN                    Far-end Node Name: SES
 Near-end Listen Port: 5060                  Far-end Listen Port: 5060
                                          Far-end Network Region: 1
Far-end Domain:

                                             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? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                                  Alternate Route Timer(sec): 6
```

5.5. Administer IP Network Region

Use the "change ip-network-region n" command, where "n" is the existing far-end network region number used by the SIP signaling group from **Section 5.4**.

For **Authoritative Domain**, leave the field blank. For **Name**, update as desired to reflect the same network region used to reach SES and IPC. In the compliance testing, the same network region was used for all Avaya users. Make a note of the **Codec Set** number.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? n
        Video PHB Value: 26             Server IP Address: 10 .64 .40 .14
```

5.6. Administer IP Codec Set

Use the "change ip-codec-set n" command, where "n" is the existing codec set number used by the IP network region from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. As specified in **Section 2.2**, the codec order should match the codec order programmed in the IPC.

```
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:
```

5.7. Administer Route Pattern

Use the "change route-pattern n" command, where "n" is the existing route pattern number to reach SES, in this case "201". For **Pattern Name**, update as desired to reflect the same route pattern used to reach SES and IPC. For **Secure SIP**, make certain the value is "n".

```
change route-pattern 201                                           Page   1 of   3
                    Pattern Number: 201 Pattern Name: SIP trunk
                             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: 201  0                                                                 n   user
 2:                                                                        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
```

5.8. Administer Public Unknown Numbering

Use the "change public-unknown-numbering 0" command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 5.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 2 and routed to trunk group 201 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change public-unknown-numbering 0                                  Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                         Total
Ext Ext             Trk       CPN         CPN
Len Code            Grp(s)    Prefix      Len
                                                   Total Administered: 12
 5   2              201                    5          Maximum Entries: 9999
```

5.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 7205x to IPC. Note that other methods of routing may be used. Use the "change uniform-dialplan 0" command, and add an entry to specify the use of AAR for routing digits 7205x, as shown below.

```
change uniform-dialplan 0                                         Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                Percent Full: 0

  Matching                   Insert              Node
  Pattern        Len Del     Digits      Net Conv Num
720              5   0                  aar  n
```

5.10. Administer AAR Analysis

Use the "change aar analysis 0" command, and add an entry to specify how to route calls to 7205x. In the example shown below, calls with digits 7205x will be routed as an AAR call using route pattern "201" from **Section 5.7**.

```
change aar analysis 0                                             Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    2

          Dialed             Total      Route     Call    Node   ANI
          String            Min   Max  Pattern    Type    Num    Reqd
    7205                    5     5     201       aar            n
```

5.11. Administer ISDN Trunk Group

Use the "change trunk-group n" command, where "n" is the existing ISDN trunk group number used to reach the PSTN, in this case "80".

For **Modify Tandem Calling Number**, enter "y" to allow for the calling party number from IPC to be modified.

```
change trunk-group 80                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: private
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
                                                     Send Connected Number: n
Network Call Redirection: none                   Hold/Unhold Notifications? n
             Send UUI IE? y                      Modify Tandem Calling Number? y
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                           Ds1 Echo Cancellation? n

    Apply Local Ringback? n               US NI Delayed Calling Name Update? n
 Show ANSWERED BY on Display? y
                             Network (Japan) Needs Connect Before Disconnect? n
```

5.12. Administer Tandem Calling Party Number

Use the "change tandem-calling-party-num" command, to define the calling party number to send to the PSTN for tandem calls from IPC turret users.

In the example shown below, all calls originating from a 5-digit extension beginning with 7205x and routed to trunk group 80 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case "pub-unk".

```
change tandem-calling-party-num                                 Page   1 of   8
                  CALLING PARTY NUMBER CONVERSION
                          FOR TANDEM CALLS
     CPN                Trk                               Number
 Len Prefix             Grp(s)     Delete  Insert         Format

 5   7205               80                 30353          pub-unk
```

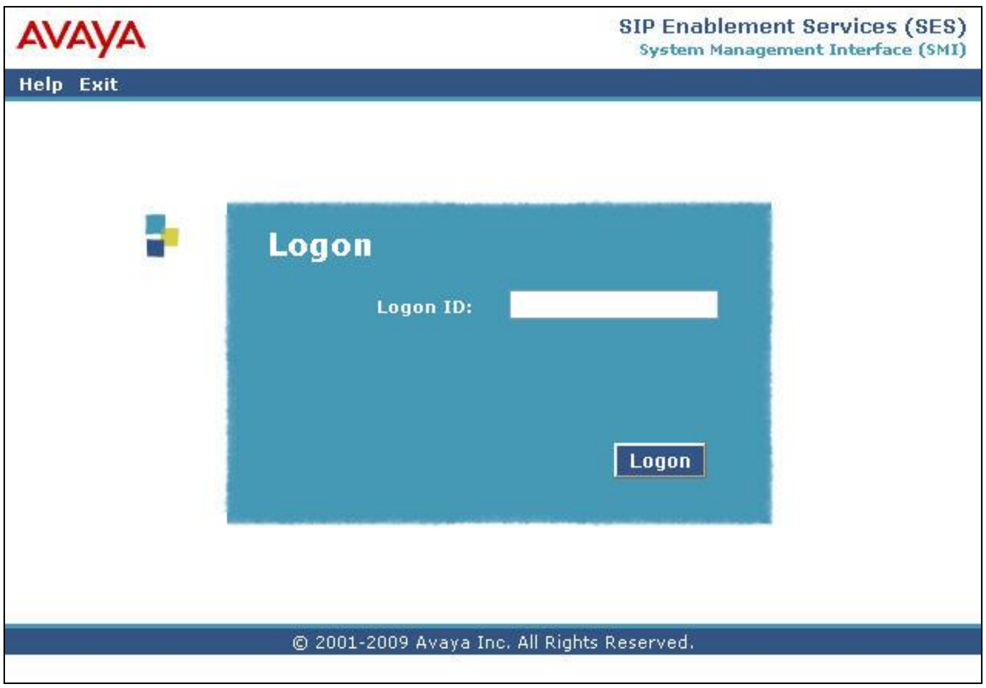
6. Configure Avaya Aura® SIP Enablement Services

This section provides the procedures for configuring SES. The procedures include the following areas:

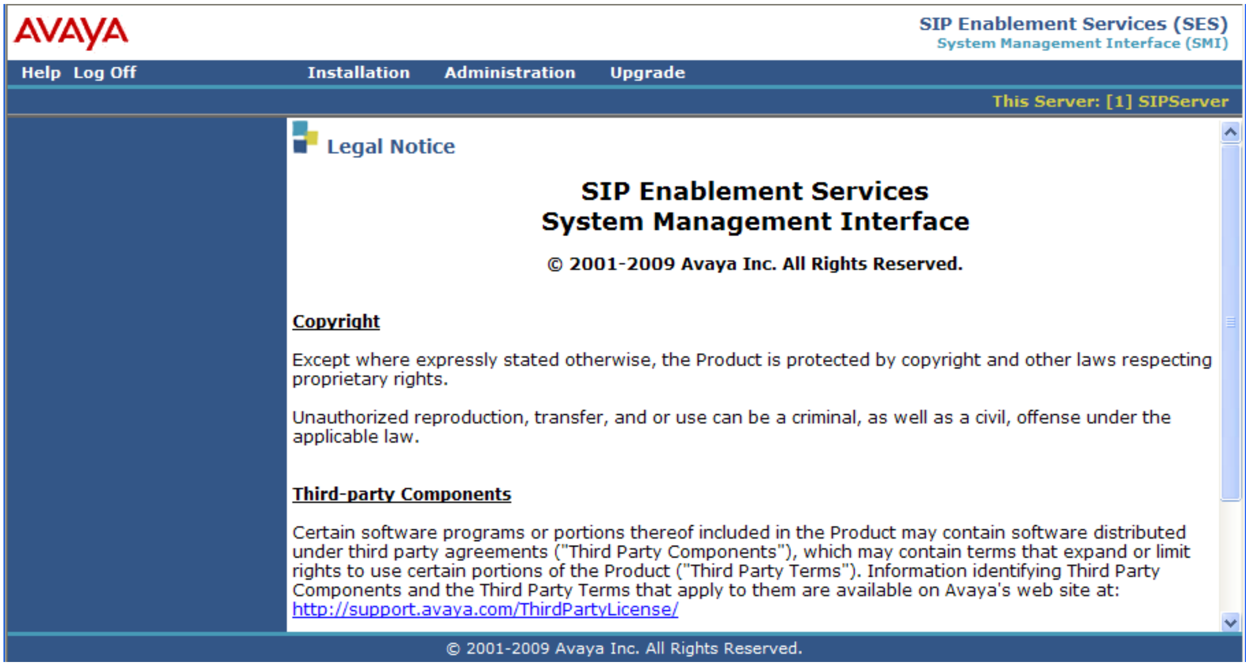
- Launch SES administration
- Administer host address map
- Administer host contact
- Administer trusted host

6.1. Launch Avaya Aura® SIP Enablement Services Administration

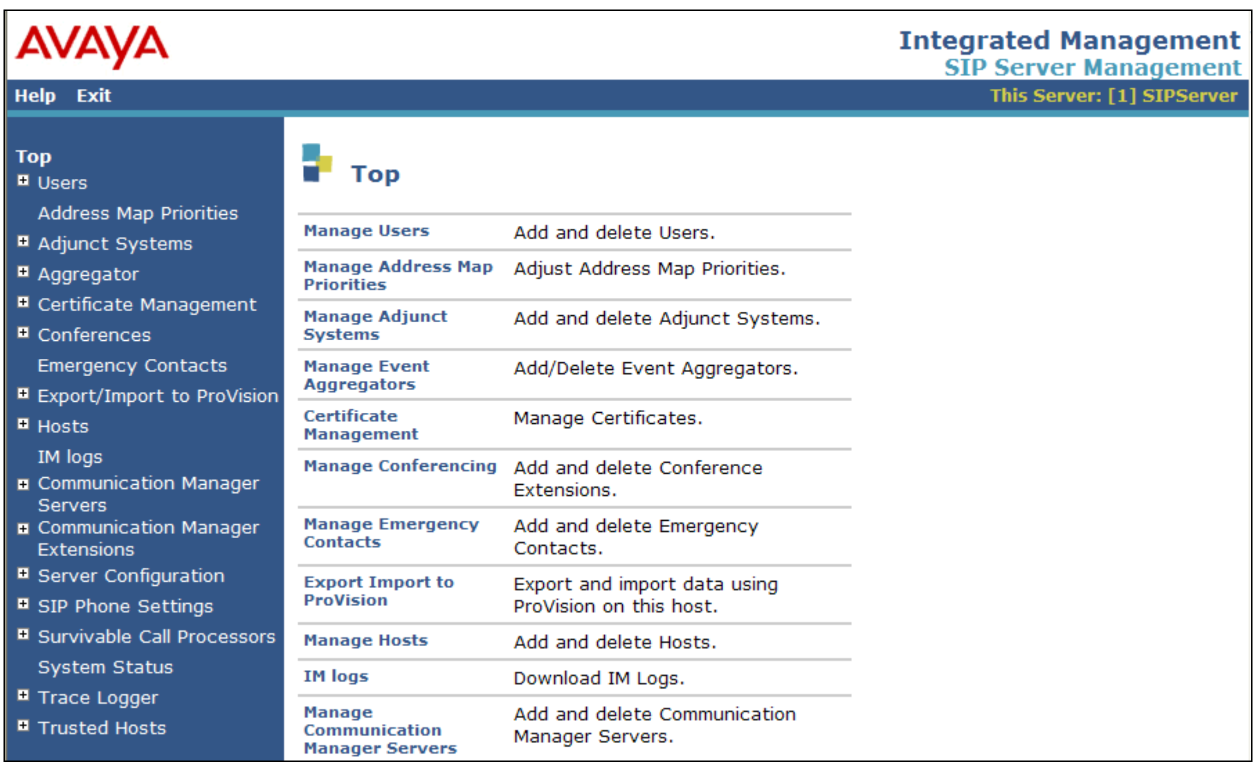
Access the SES web interface by using the URL "http://ip-address/admin" in an Internet browser window, where "ip-address" is the IP address of the SES server. Log in using the appropriate credentials.



In the subsequent screen, select **Administration → SIP Enablement Services** from the top menu.

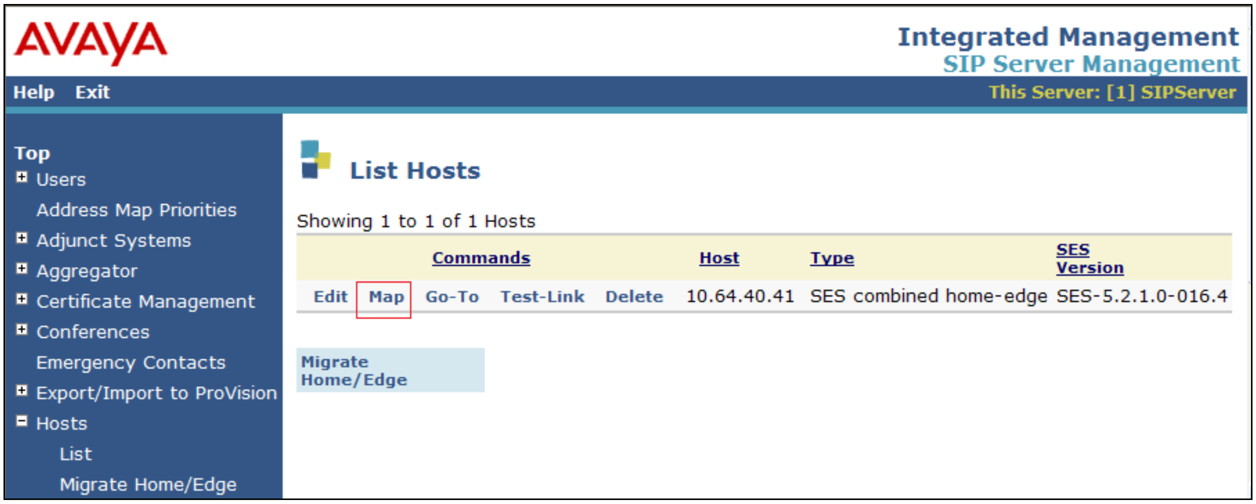


The **Top** screen is displayed next.

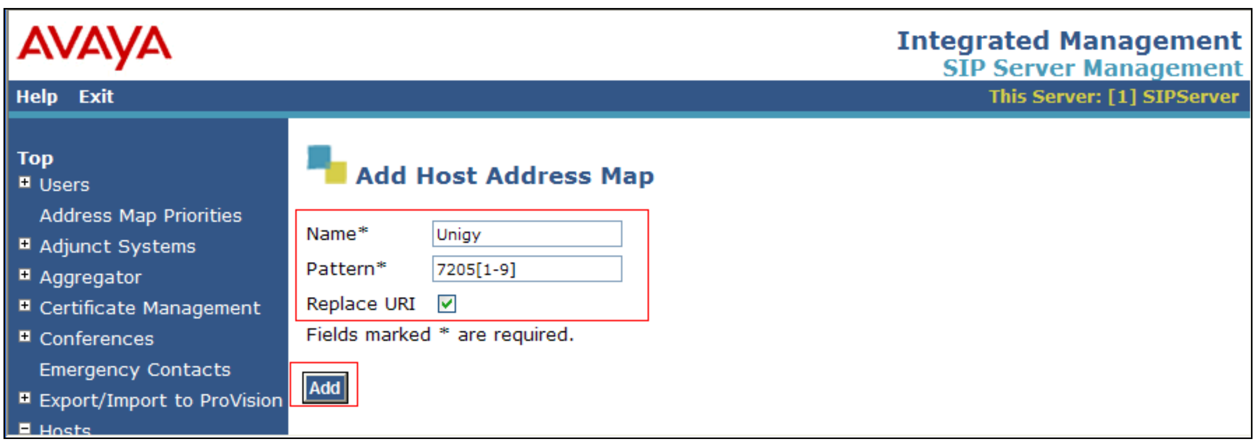


6.2. Administer Host Address Map

Select **Hosts → List** from the left pane. The **List Hosts** screen is displayed. Click on the **Map** link.

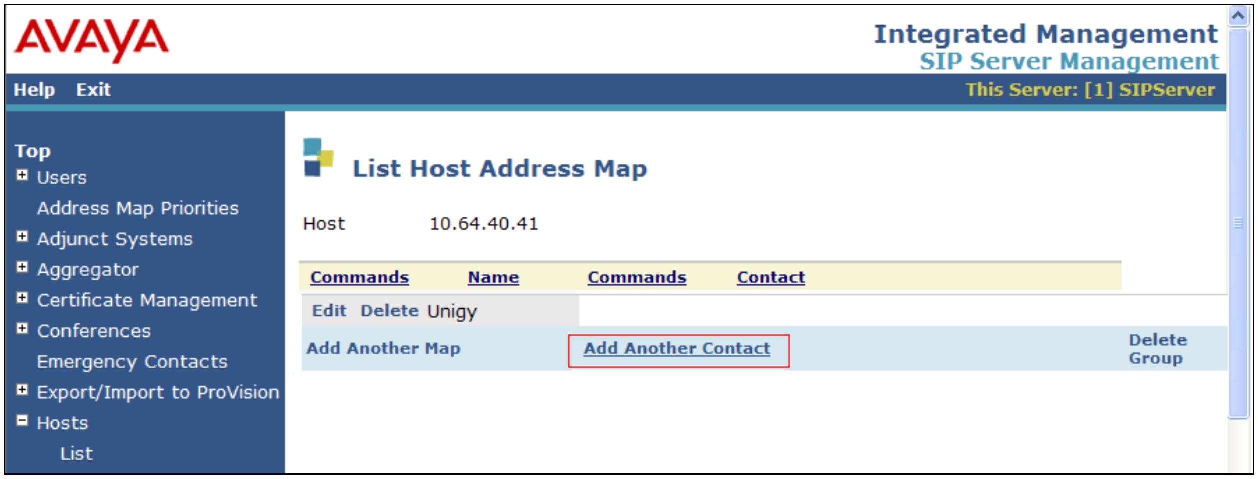


In the **List Host Address Map** screen below, click **Add Map In New Group** in the right pane (not shown). The **Add Host Address Map** screen is displayed next. This screen is used to specify which calls are to be routed to IPC. For **Name**, enter a descriptive name to denote the routing. For **Pattern**, enter an appropriate syntax for address mapping. For the compliance testing, a pattern of "^sip:7205[0-9]" is used to match to any IPC turret user extensions of 7205x. Maintain the check in **Replace URI**. Click **Add**.

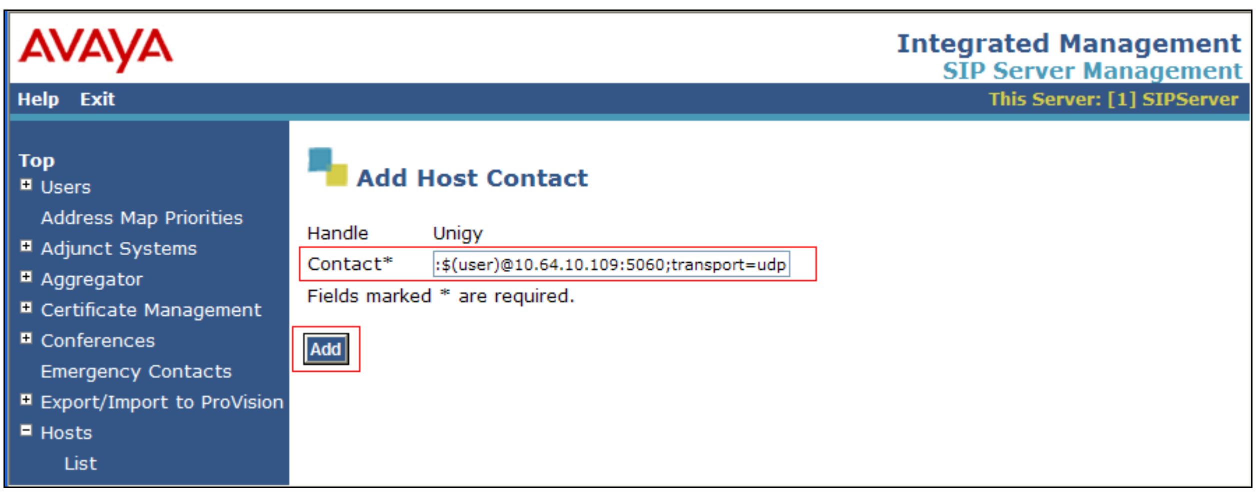


6.3. Administer Host Contact

The **List Host Address Map** screen is displayed again, and updated with the newly created address map. Click **Add Another Contact** in the right pane.

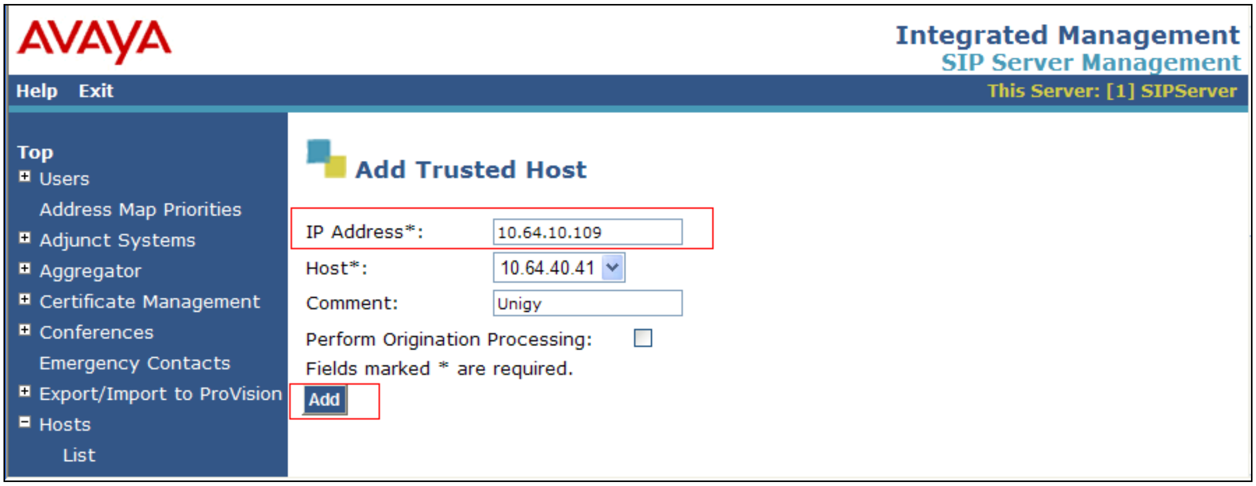


In the **Add Host Contact** screen, enter the contact "sip:$(user)@<destination-IP-address> :5060;transport=udp", where the <destination-IP-address> is the IP address of IPC Media Manager. SES will substitute "$(user)" with the user portion of the request URI before sending the message. Click **Add**.



6.4. Administer Trusted Host

Select **Trusted Hosts → Add** from the left pane (not shown). The **Add Trusted Host** screen is displayed. For the **IP Address** field, enter the IP address of the IPC server from **Section 6.3**. Enter a desired description for **Comment**.



7. Configure IPC Converged Communication Manager

This section provides the procedures for configuring IPC Converged Communication Manager. The procedures include the following areas:

- Launch UnigyV2 Management System
- Administer SIP trunks
- Administer trunk groups
- Administer route lists
- Administer dial patterns
- Administer route plans

The configuration of Media Manager and/or Converged Communication Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch UnigyV2 Management System

Access the UnigyV2 Management System web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Media Manager. Log in using the appropriate credentials.

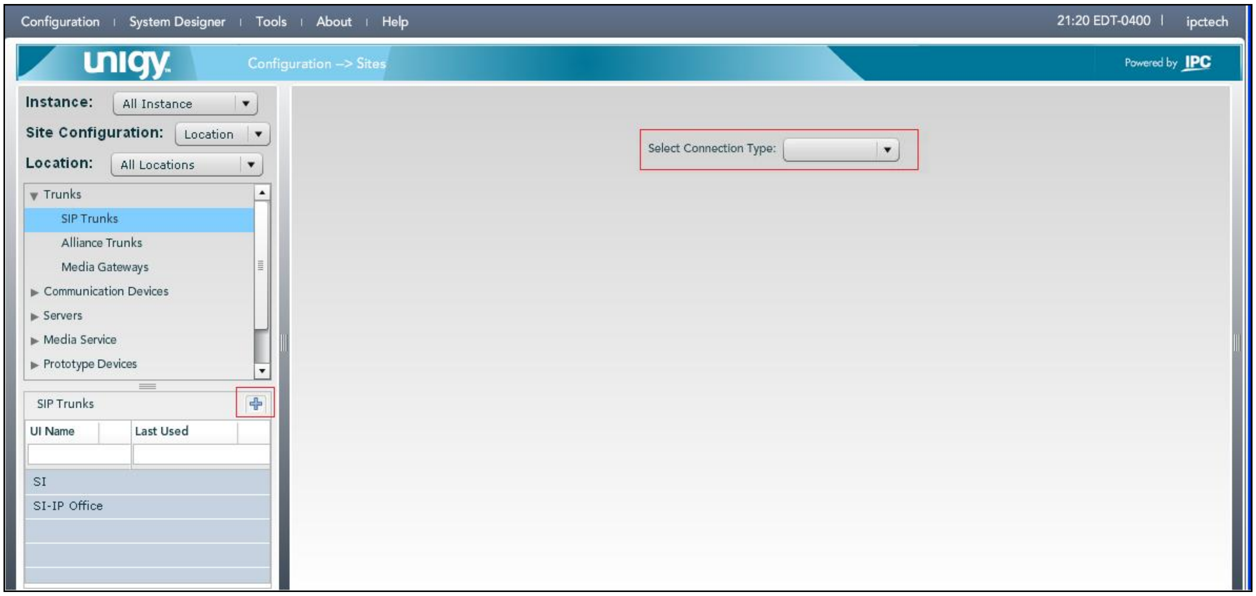
The screen below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use**, and click **Login**.

In the subsequent screen (not shown), click **Continue**.

7.2. Administer SIP Trunks

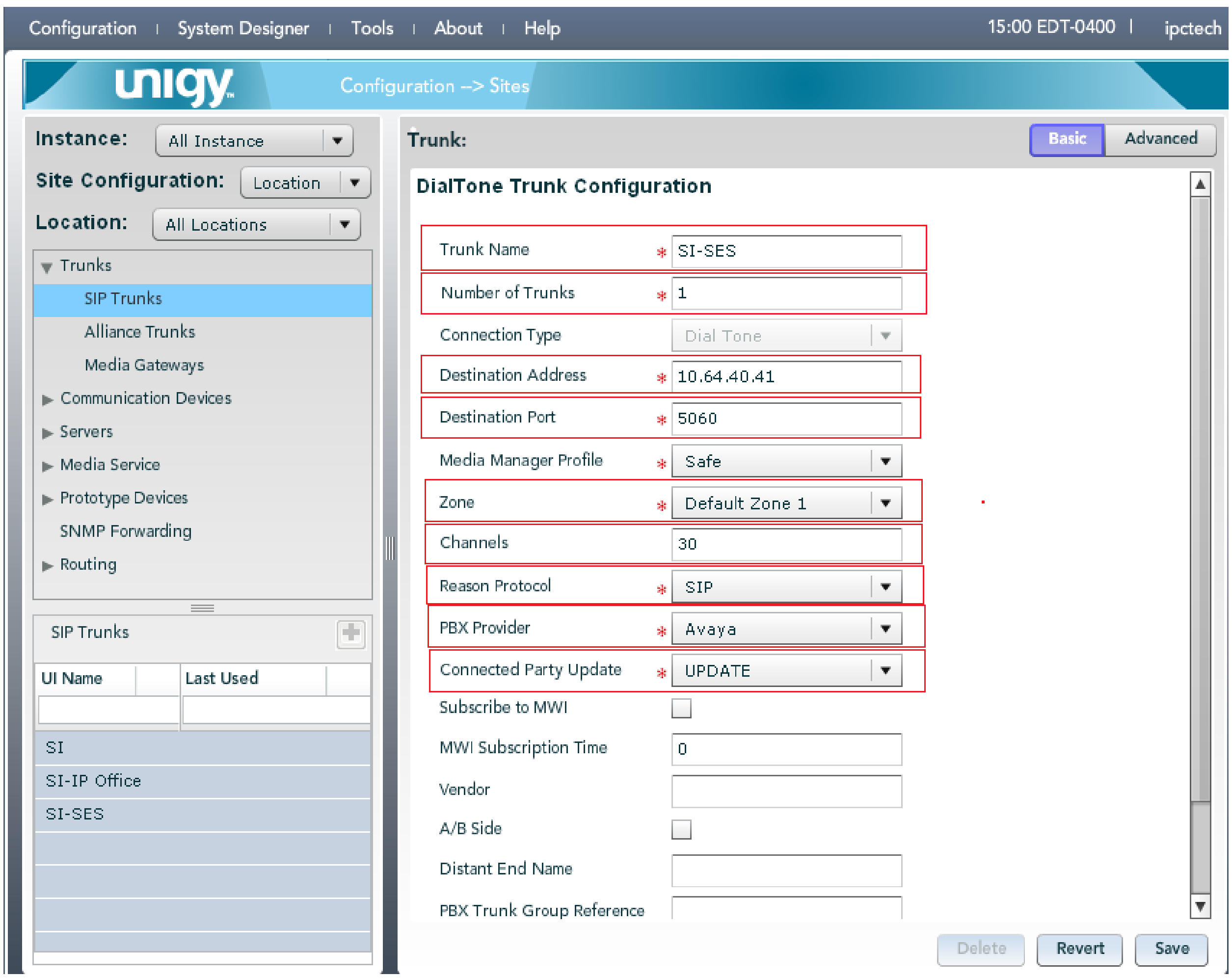
Select **Configuration → Sites → Trunks→ SIP Trunks** in the left pane, and click the **Add** icon () in the lower left pane to add a new SIP trunk.

The screen below is displayed. Select “Dial Tone” from the **Select Connection Type** drop-down list.

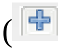


The screen below is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

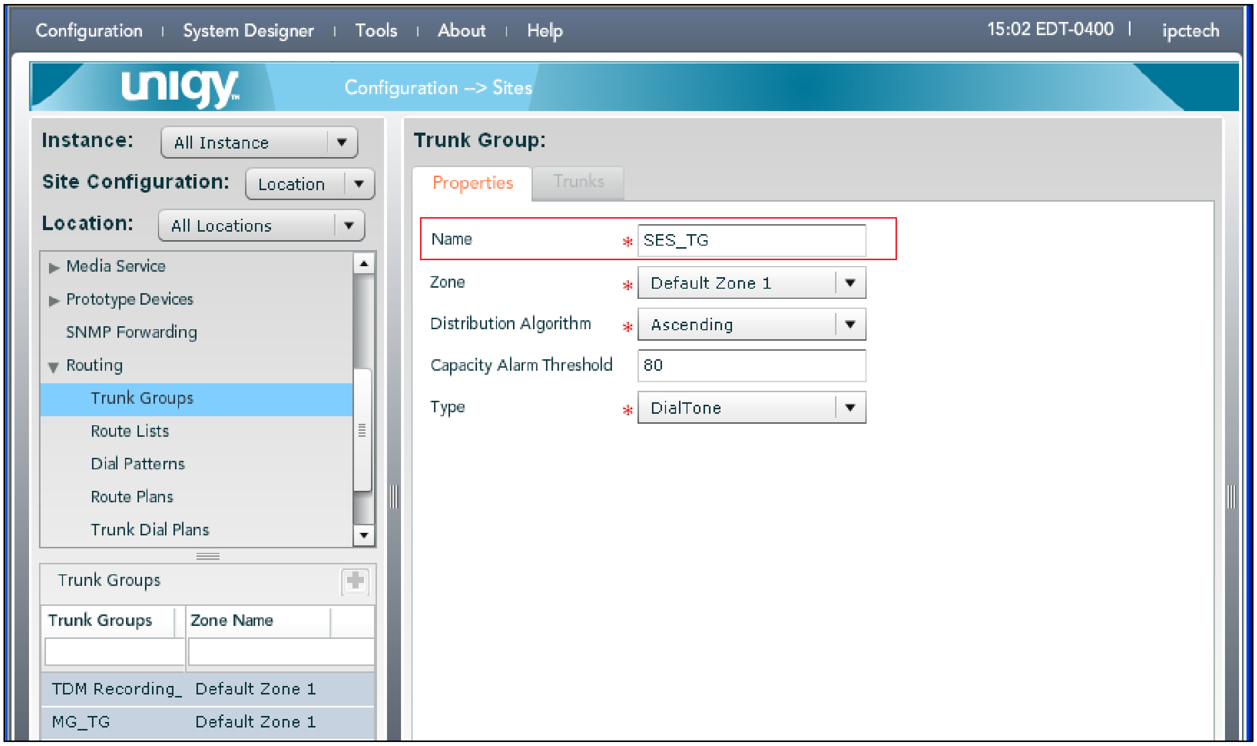
- **Trunk Name:** A descriptive name
- **Number of Trunks** **"1"**
- **Destination Address:** IP address of Avaya Aura® SIP Enablement Services server
- **Destination Port:** The host contact port number from **Section 6.3**
- **Zone:** An available zone, in this case "Default Zone 1"
- **Channels:** The number of SIP trunk group members
- **Reason Protocol** **Select "SIP"**
- **PBX Provider:** "Avaya"
- **Connected Party Update:** "UPDATE"



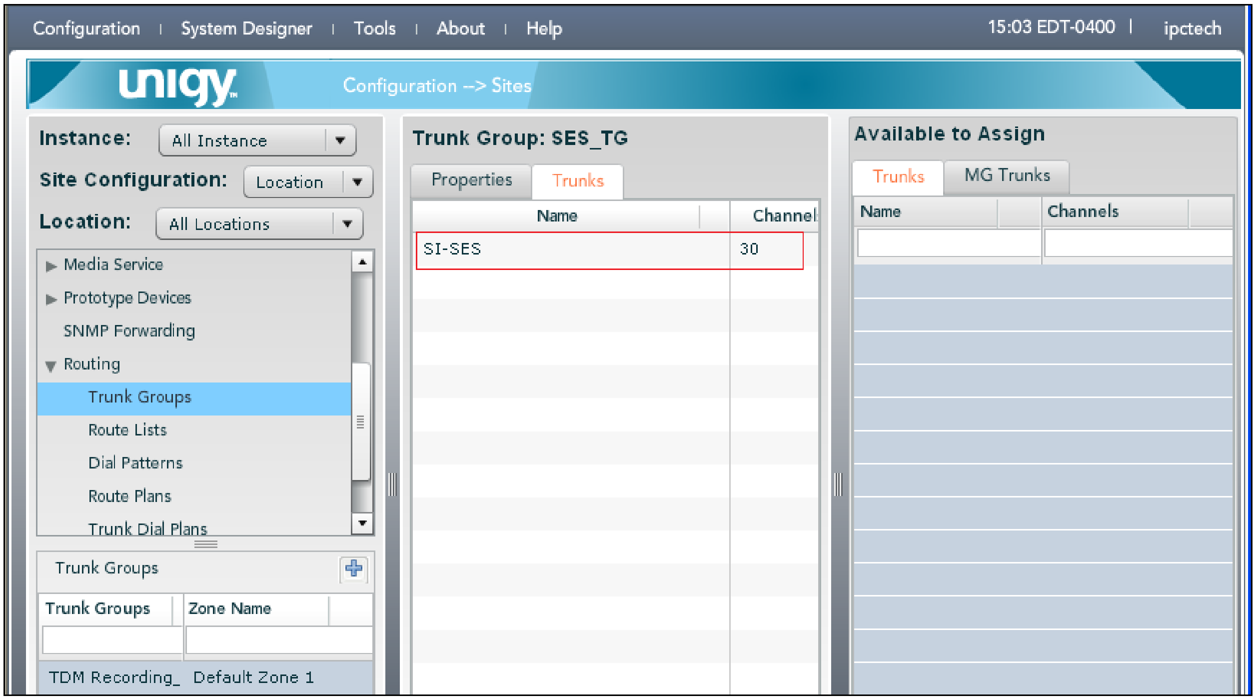
7.3. Administer Trunk Groups

Select **Routing → Trunk Groups** in the left pane, and click the **Add** icon () in the lower left pane to add a new trunk group.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, and click **Save** (not shown). Select the **Trunks** tab in the right pane.



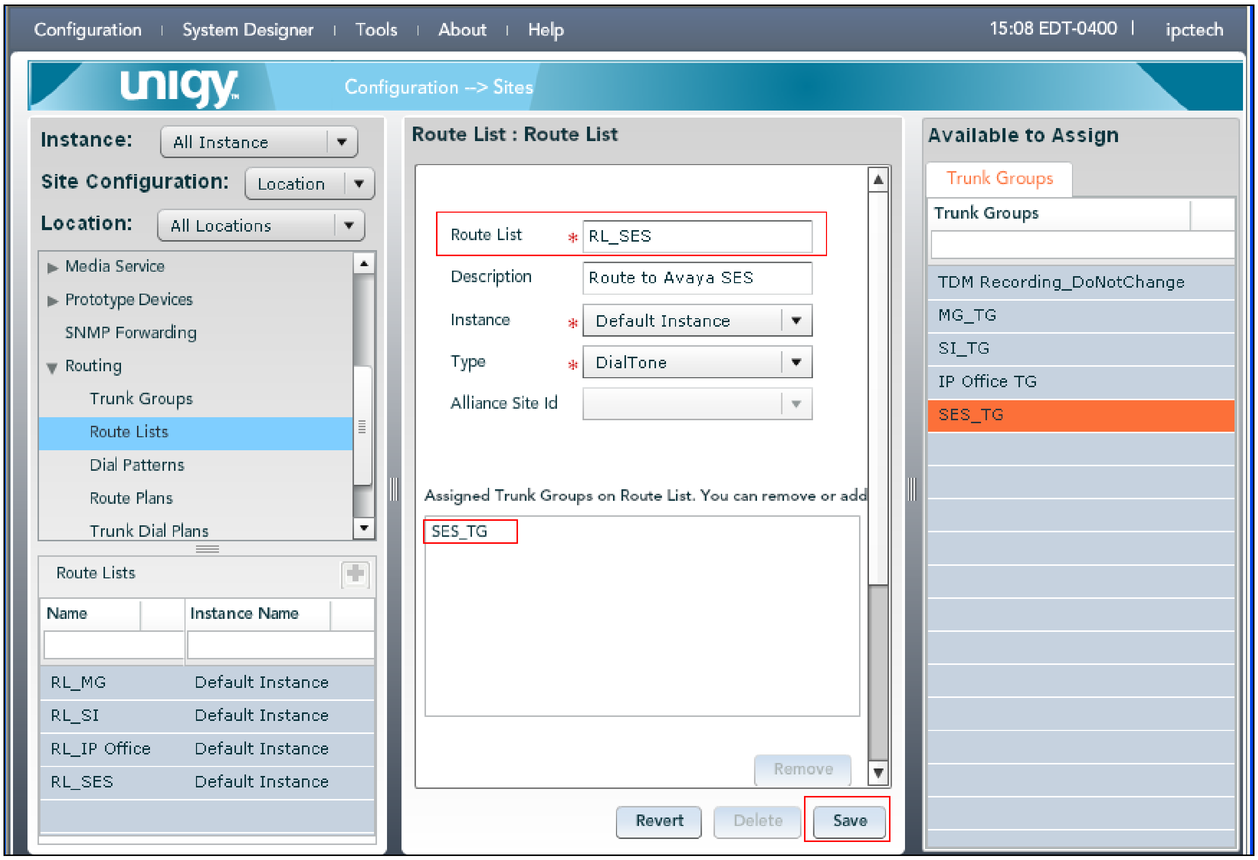
The screen is updated with three panes. In the rightmost pane, select the MG Trunks tab. In the listing, select the SIP trunk from **Section 7.2** in the rightmost pane to the middle pane as shown below. Click **Save** (not shown).



7.4. Administer Route Lists

Select **Routing → Route Lists** in the left pane, and click the **Add** icon in the lower left pane to add a new route list.

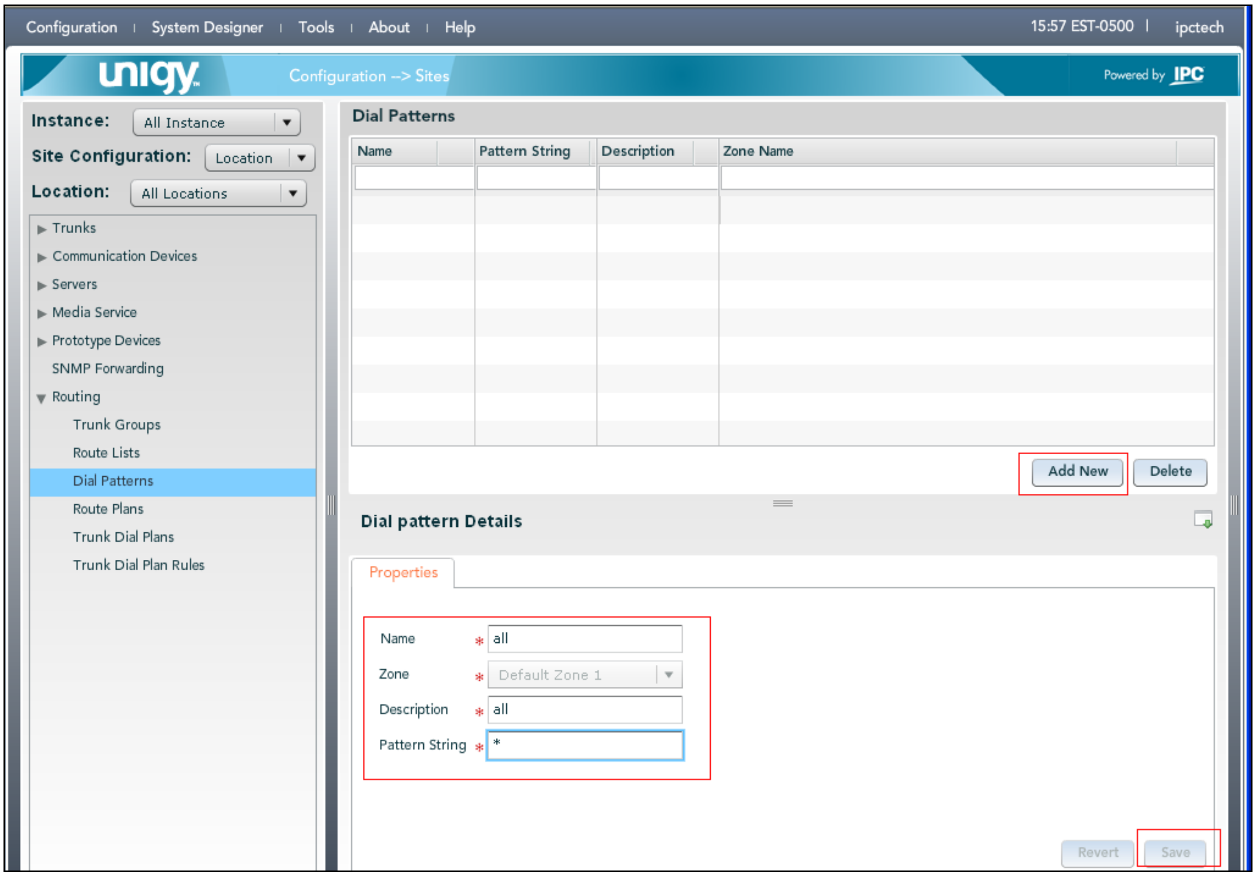
The **Route List** screen is displayed in the middle pane. For **Route List**, enter a descriptive name. In the right pane, select the trunk group from **Section 7.3** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below. Click **Save**.



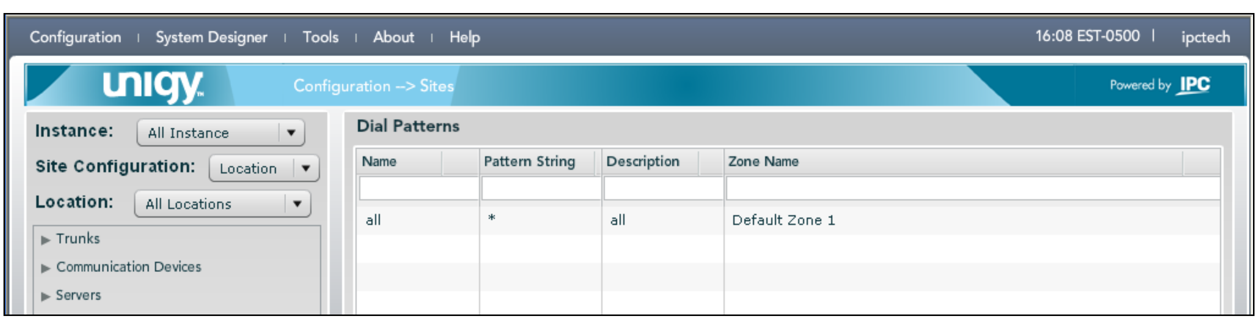
7.5. Administer Dial Patterns

Select **Routing → Dial Patterns** in the left pane, to display the **Dial Patterns** screen in the right pane. Click **Add New** in the upper right pane.

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya endpoints, in this case "*". Click **Save**.



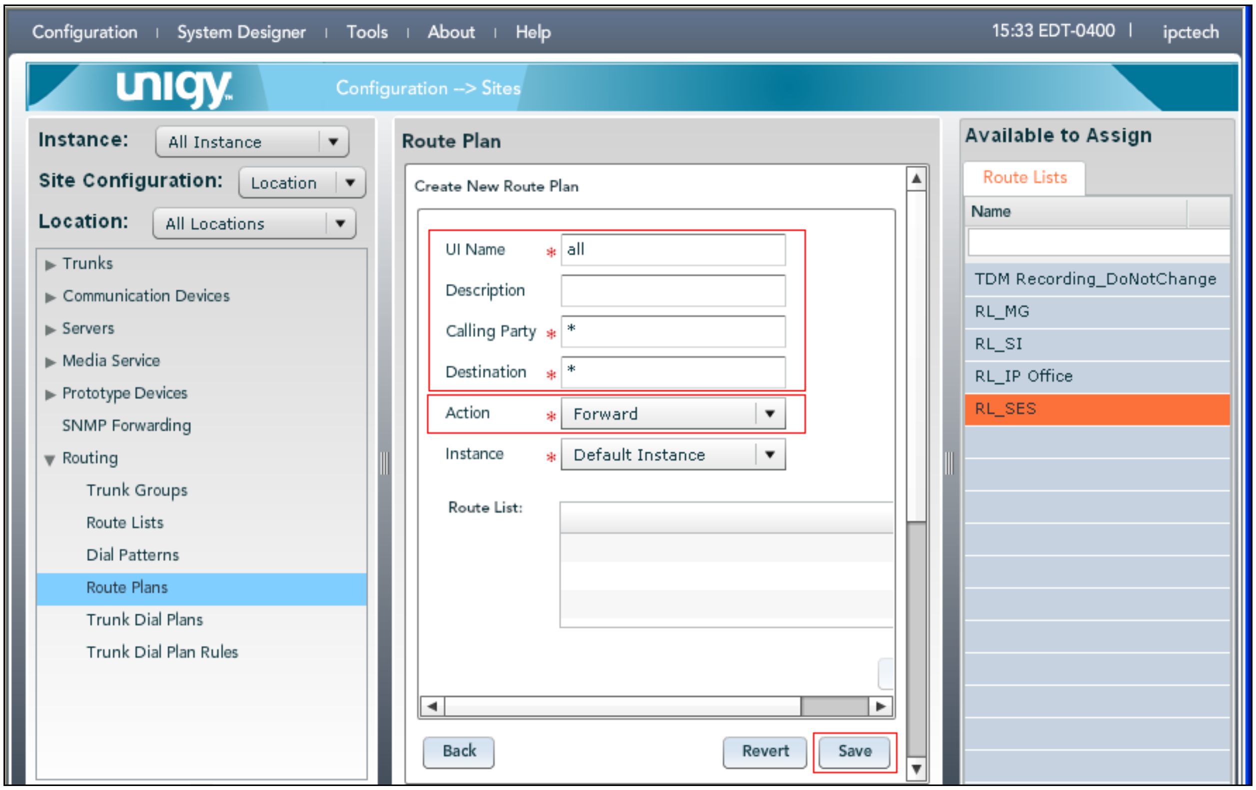
Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Communication Manager. In the compliance testing, one dial pattern was created as shown below.



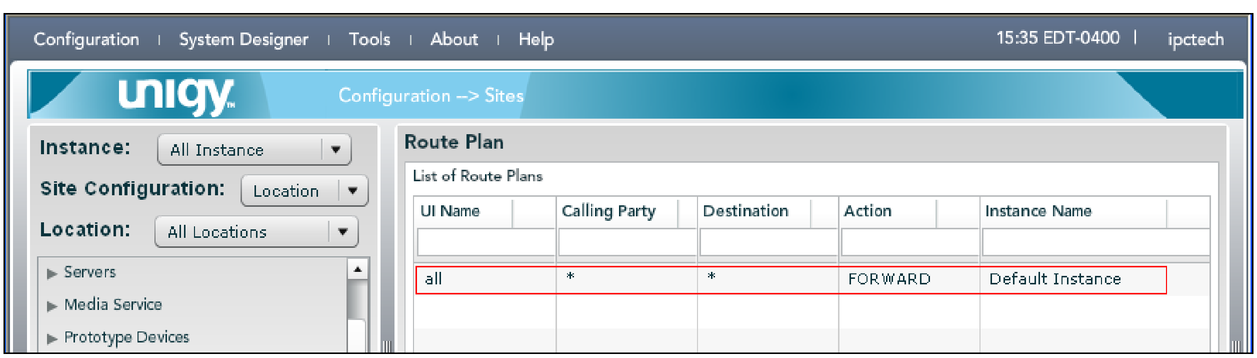
7.6. Administer Route Plans

Select **Routing → Route Plans** in the left pane, and click **Add New** (not shown) in the right pane to create a new route plan.

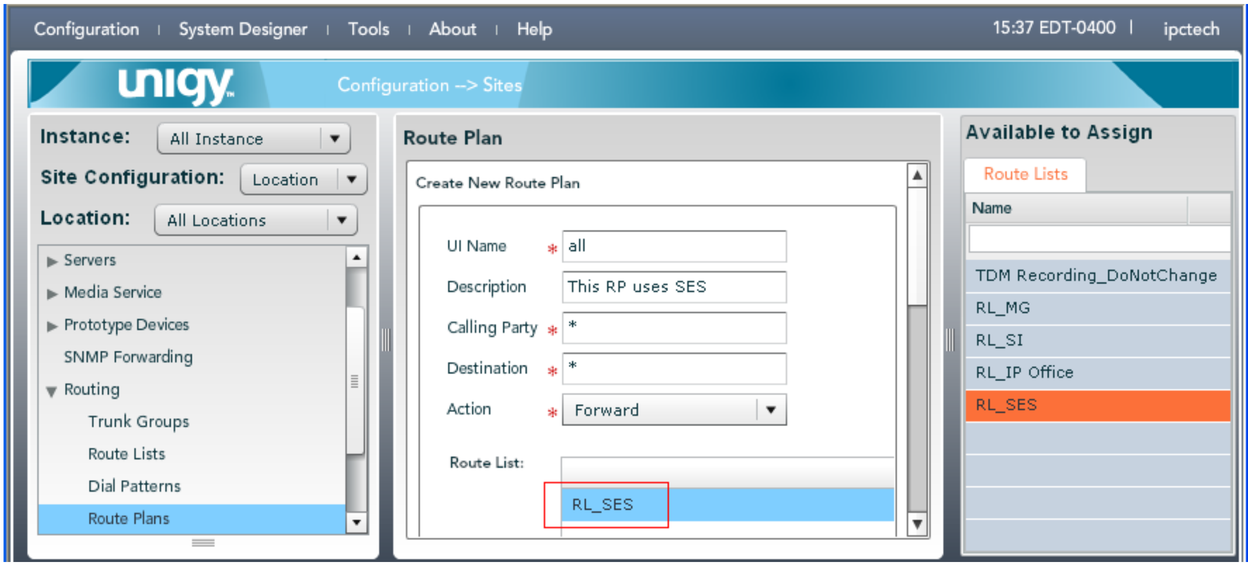
The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter "*" to denote any calling party from UnigyV2. For **Destination**, enter "*" to denote any called party for Avaya endpoints. Select "Forward" for **Action**, and click **Save**.



The screen is updated with the newly created route plan. Select the route plan, and click Edit toward the bottom of the screen (not shown).



The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 7.4** and drag into the **Route List** sub-section in the middle pane, as shown below. Click **Save** (not shown).



8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® SIP Enablement Services, and IPC UnigyV2.

8.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the "status trunk n" command, where "n" is the trunk group number administered in **Section 5.3**. Verify that all trunks are in the "in-service/idle" state as shown below.

```
status trunk 201

                            TRUNK GROUP STATUS

Member    Port     Service State      Mtce Connected Ports
                                      Busy

0201/001 T00100   in-service/idle    no
0201/002 T00101   in-service/idle    no
0201/003 T00102   in-service/idle    no
0201/004 T00103   in-service/idle    no
0201/005 T00104   in-service/idle    no
0201/006 T00105   in-service/idle    no
0201/007 T00106   in-service/idle    no
0201/008 T00107   in-service/idle    no
0201/009 T00108   in-service/idle    no
0201/010 T00109   in-service/idle    no
```

Verify the status of the SIP signaling groups by using the "status signaling-group n" command, where "n" is the signaling group number administered in **Section 5.4**. Verify that the signaling group is "in-service" as indicated in the **Group State** field shown below.

```
status signaling-group 201
                         STATUS SIGNALING GROUP

        Group ID: 201                         Active NCA-TSC Count: 0
      Group Type: sip                          Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

8.2. Verify Avaya Aura® SIP Enablement Services

From the SES web interface, select **Trusted Hosts → List** from the left pane, to display the **List Trusted Hosts** screen. Verify that the IPC Media Server is listed as a trusted host.

8.3. Verify IPC UnigyV2

Make a call from an IPC turret user to an Avaya endpoint. Verify that the call can be connected with two-way talk paths.

9. Conclusion

These Application Notes describe the configuration steps required for IPC UnigyV2 to successfully interoperate with Avaya Aura® Communication Manager 5.2.1 using Avaya Aura® SIP Enablement Services 5.2.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administrator Guide for Avaya Aura™ Communication Manager*, Document 03-300509, Issue 8.0, Release 5.2, May 2009, available at http://support.avaya.com.

2. *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services*, Document ID 03-600768, Issue 8.0, November 2009, available at http://support.avaya.com.

3. *UnigyV2 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

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.