Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy with Avaya Aura® Communication Manager 5.2.1 and Avaya Aura® SIP Enablement Services using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy to interoperate with Avaya Aura® Communication Manager 5.2.1 and Avaya Aura® SIP Enablement Services.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy used SIP trunks to Avaya Aura® SIP Enablement Services, for turret users on IPC to reach users on Avaya Aura® Communication Manager and on the PSTN.

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 Unigy to interoperate with Avaya Aura® Communication Manager using Avaya Aura® SIP Enablement Services (SES).

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy used SIP trunks to Avaya Aura® SIP Enablement Services for turret users on IPC to reach users on Avaya Aura® Communication Manager and on the PSTN.

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 Unigy.

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 Unigy to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to IPC Unigy.

2.2. Test Results

All test cases were executed and verified. The following were the observations on IPC Unigy 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.
- 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.
- In an outgoing call from IPC turret to the PSTN, the IPC turret display will show "null" as the connected number. Note that the name of the PSTN endpoint can still be shown on the display, and that incoming calls from the PSTN to the IPC turrets have proper displays.
- In transfer scenarios involving IPC turrets transferring calls to Avaya SIP endpoints, the Avaya SIP endpoints will see "wlssuser" in the display upon completion of transfer, as sent from IPC.
- The dial pattern string specified on IPC must contain the exact number of digits.
- For call forwarding scenarios involving Avaya SIP endpoints calling IPC turrets that are forwarded back to Avaya endpoints, the Avaya SIP endpoint will show two active call appearances after the call diverts.
- Multiple divert buttons on the turret can lead to turret performance degradation.

2.3. Support

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

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

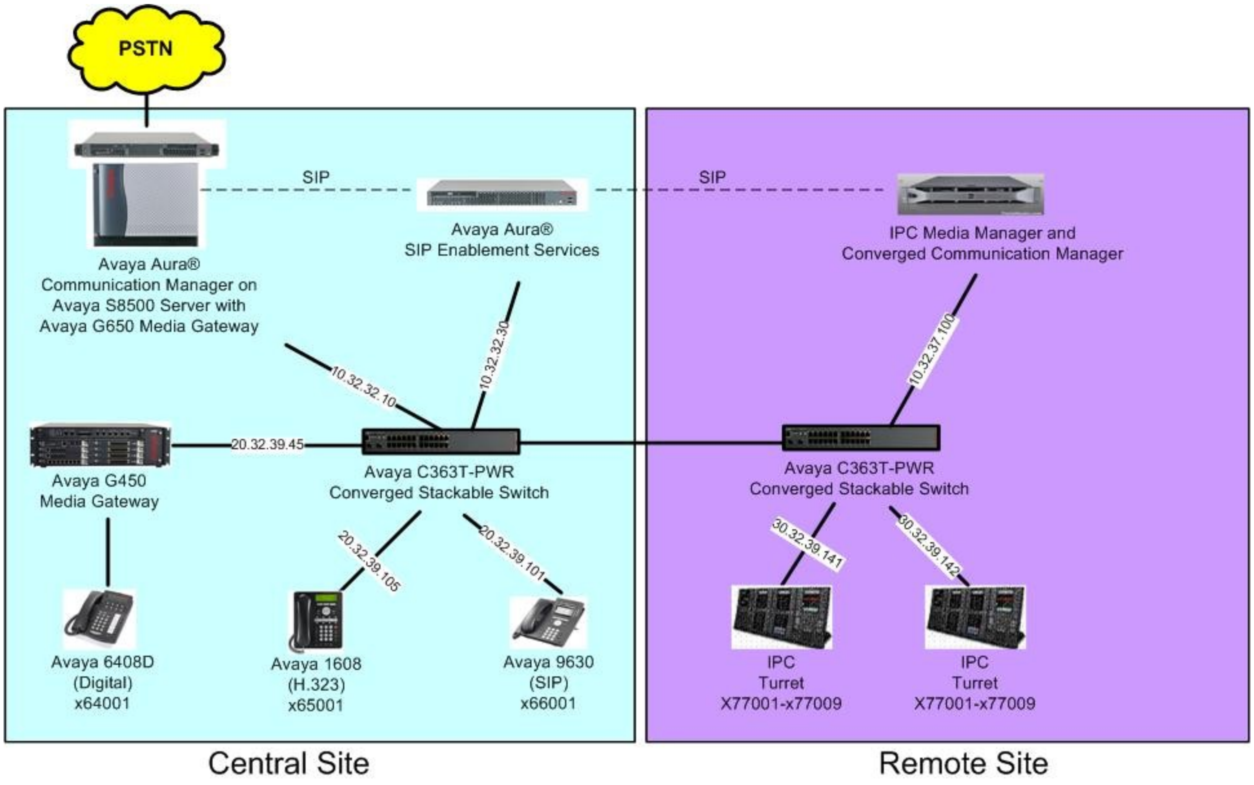
3. Reference Configuration

As shown in the test configuration below, IPC Unigy 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 Unigy 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 (64xxx-66xxx), and IPC turret users at the Remote site (77xxx).

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.


PSTN
SIP
SIP
Avaya Aura® SIP Enablement Services
IPC Media Manager and Converged Communication Manager
Avaya Aura® Communication Manager on Avaya S8500 Server with Avaya G650 Media Gateway
10.32.32.10
10.32.32.30
10.32.37.100
20.32.39.45
Avaya G450 Media Gateway
Avaya C363T-PWR Converged Stackable Switch
Avaya C363T-PWR Converged Stackable Switch
20.32.39.105
20.32.39.101
30.32.39.141
30.32.39.142
Avaya 6408D (Digital) x64001
Avaya 1608 (H.323) x65001
Avaya 9630 (SIP) x66001
IPC Turret X77001-x77009
IPC Turret X77001-x77009
Central Site
Remote Site

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 S8500 Server	5.2.1 SP8 (R015x.02.1.016.4-18855)
Avaya G650 Media Gateway - TN799DP C-LAN Circuit Pack - TN2302AP IP Media Processor - TN464HP DS1 Interface	 HW01 FW038 HW20 FW122 HW02 FW024
Avaya G450 Media Gateway - MM712AP DCP	28.17 HW07 FW011
Avaya Aura® SIP Enablement Services	5.2.1 SP4 (SES-5.2.1.0-016.4-SP4C)
Avaya 1608 IP Telephone (H.323)	1.3
Avaya 9630 IP Telephone (SIP)	2.6.4
Avaya 6408D Digital Telephone	NA
IPC Unigy - Media Manager - Converged Communication Manage - Turrets	 01.00.00.01.0003 01.00.00.01.0003 01.00.00.01.0003

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.

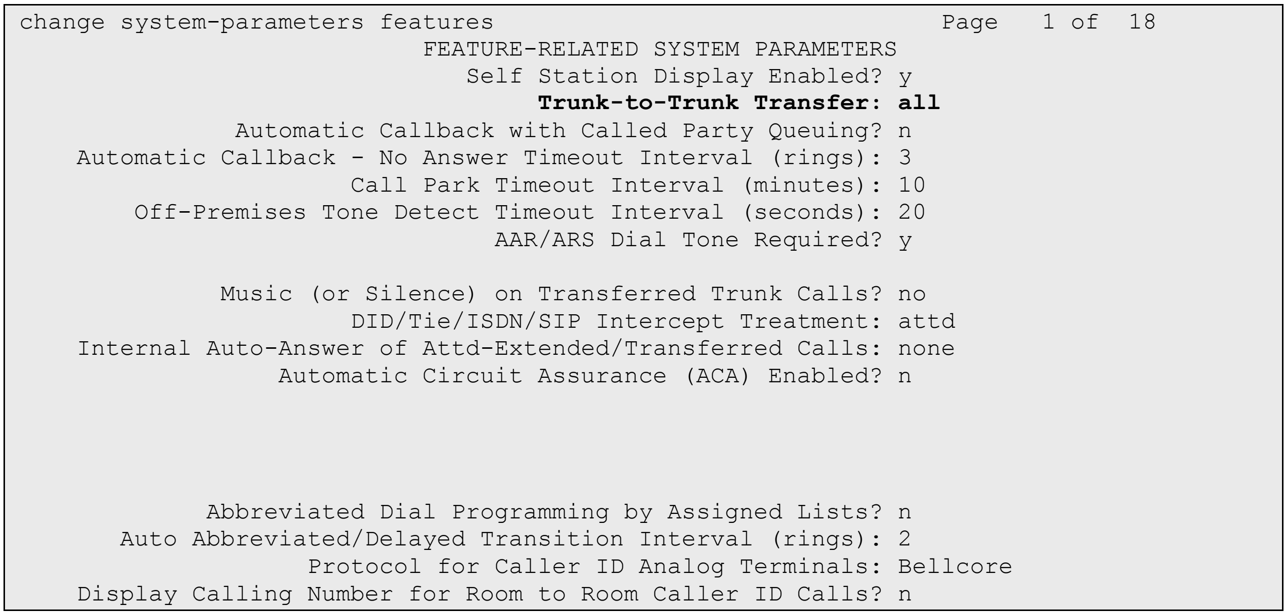
The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   6
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 8000  0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 10    0
  Max Concur Registered Unauthenticated H.323 Stations: 10    0
                  Maximum Video Capable H.323 Stations: 100   0
                   Maximum Video Capable IP Softphones: 100   0
                       Maximum Administered SIP Trunks: 100   10
  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.



```
change system-parameters features                               Page   1 of  18
                            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 (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: none
                  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 “5”.

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. Note that a call between an Avaya SIP user and an IPC user uses two SIP trunks, whereas a call between an Avaya non-SIP user and an IPC user uses one SIP trunk. Make a note of the **Signaling Group** number.

```
change trunk-group 5                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 5                    Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to SES/IPC        COR: 1        TN: 1        TAC: 1005
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 5
                                                     Number of Members: 10
```

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

```
change trunk-group 5                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          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 Unigy 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 5                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 5              Group Type: sip
                        Transport Method: tls
  IMS Enabled? n


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

                                             Bypass If IP Threshold Exceeded? n
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                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? 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. Enter “no” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. 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: SES/IPC Region
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? 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
```

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. Note that IPC Unigy supports the G.711 and G.729 codec variants, and requires the codec order on Avaya to match the codec order specified on IPC Unigy. The codec order shown below matched the default order on IPC Unigy.

In the compliance testing, the same codec set was used for all Avaya users.

```
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: G.729AB           n         2        20
 3:
 4:
 5:
```

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 "5". 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 5                                          Page   1 of   3
                    Pattern Number: 5   Pattern Name: To SES/IPC
                             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: 5    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: 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 6 and routed to trunk group 5 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: 3
 5  6             5                         5           Maximum Entries: 9999
```

5.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 77xxx 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 77xxx, 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

 77              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 77xxx. In the example shown below, calls with digits 77xxx will be routed as an AAR call using route pattern “5” 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
    77                   5    5     5         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 “10”.

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

```
change trunk-group 10                                           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: public
 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 77 and routed to trunk group 10 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   77               10                 90884            pub-unk
```

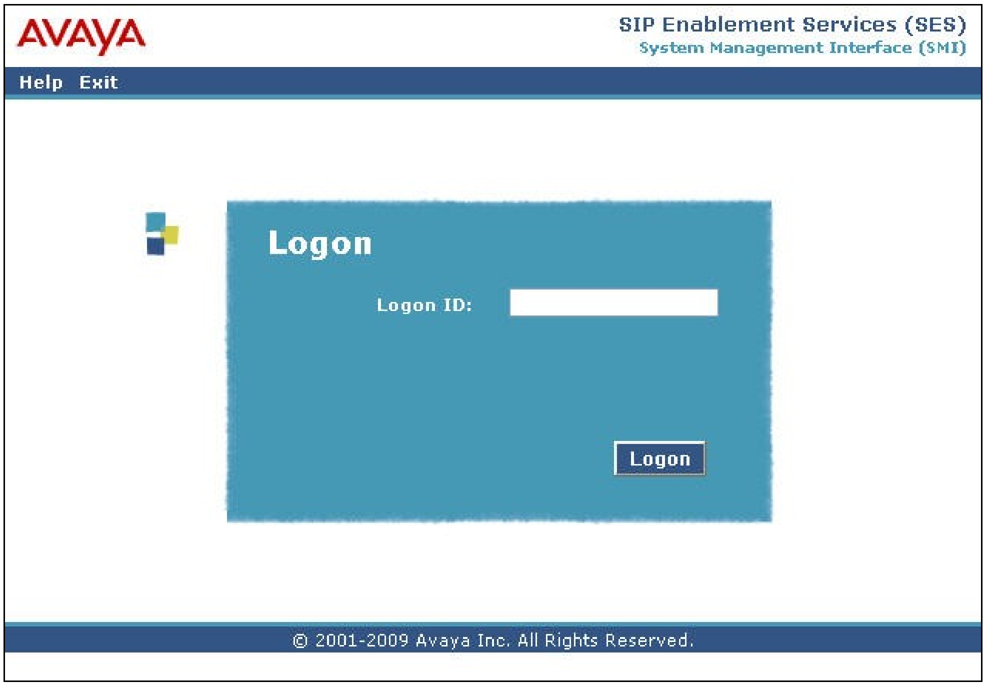
6. Configure Avaya Aura® SIP Enablement Services

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

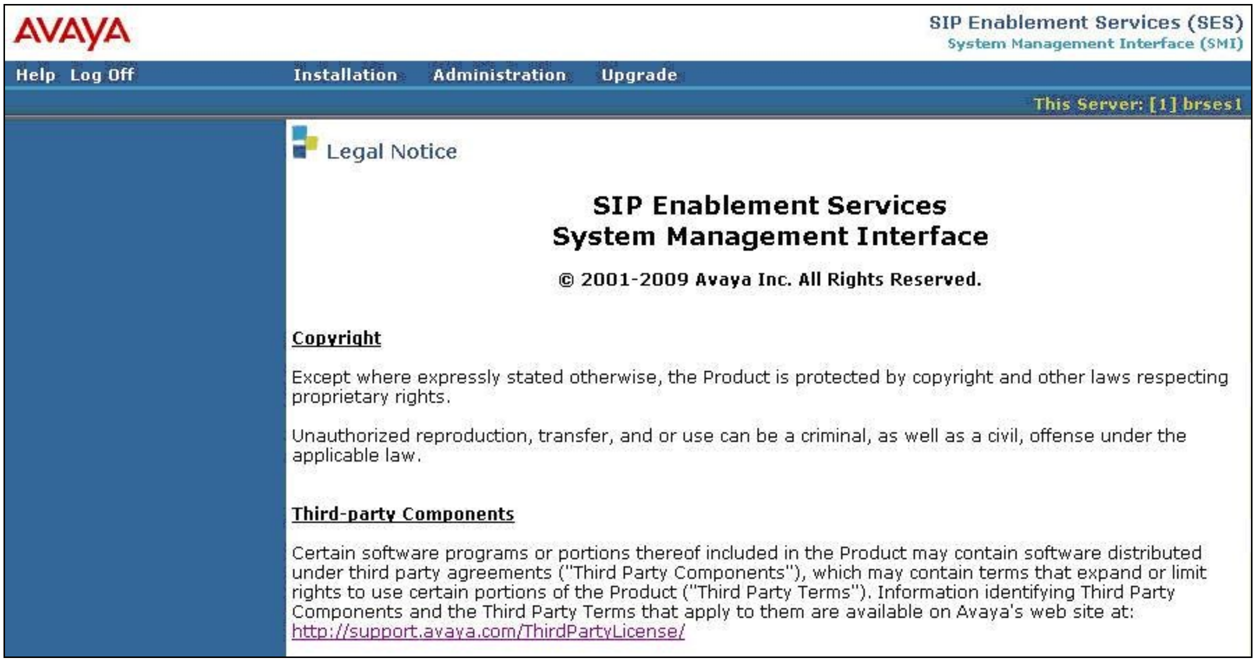
- Launch SES administration
- Administer host address map
- Administer host contact
- Administer trusted host

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.


AVAYA
SIP Enablement Services (SES)
System Management Interface (SMI)
Help
Exit
Logon
Logon ID:
Logon
© 2001-2009 Avaya Inc. All Rights Reserved.

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



SIP Enablement Services
System Management Interface

© 2001-2009 Avaya Inc. All Rights Reserved.

Copyright

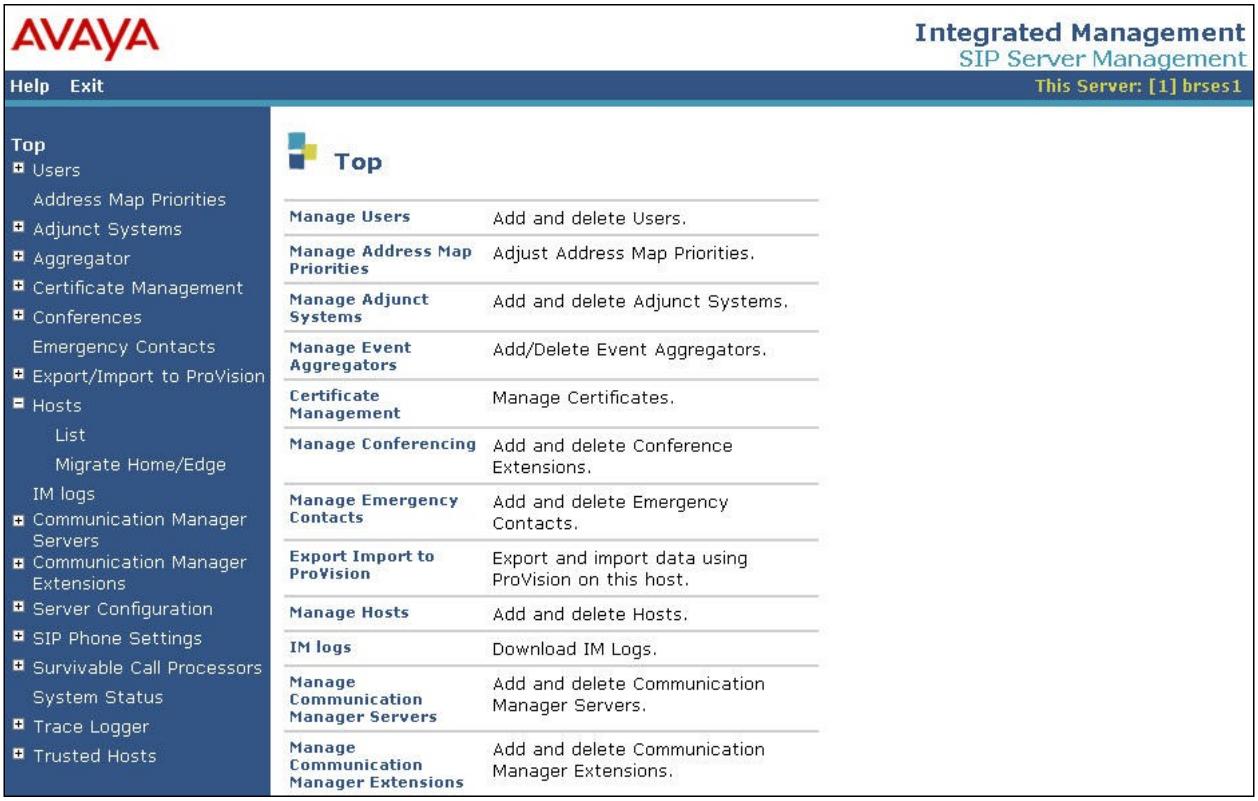
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

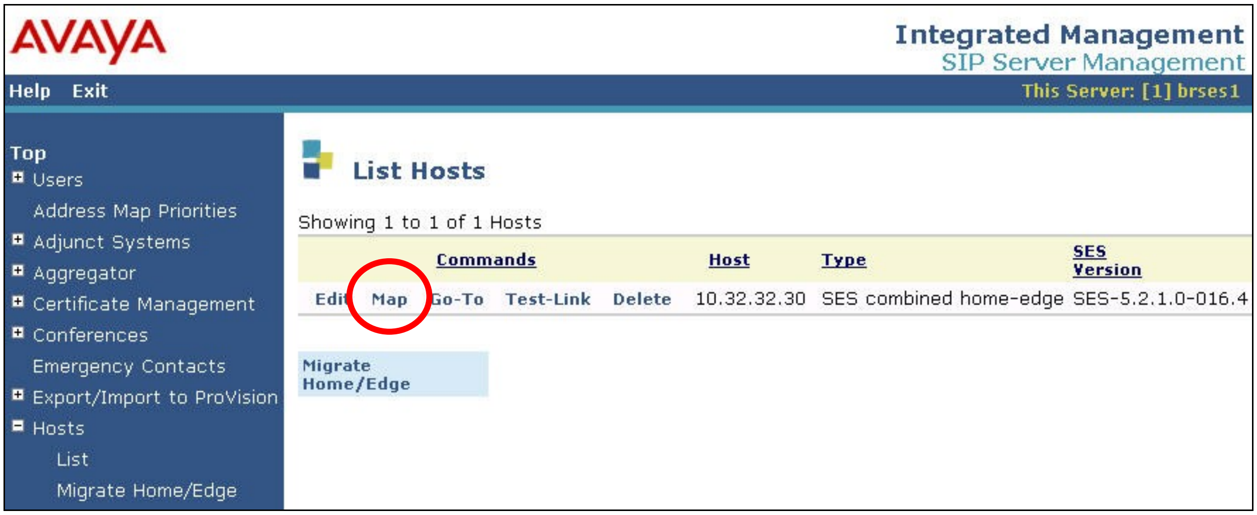
The **Top** screen is displayed next.



Manage Users	Add and delete Users.
Manage Address Map Priorities	Adjust Address Map Priorities.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Event Aggregators	Add/Delete Event Aggregators.
Certificate Management	Manage Certificates.
Manage Conferencing	Add and delete Conference Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Export Import to ProVision	Export and import data using ProVision on this host.
Manage Hosts	Add and delete Hosts.
IM logs	Download IM Logs.
Manage Communication Manager Servers	Add and delete Communication Manager Servers.
Manage Communication Manager Extensions	Add and delete Communication Manager Extensions.

6.2. Administer Host Address Map

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

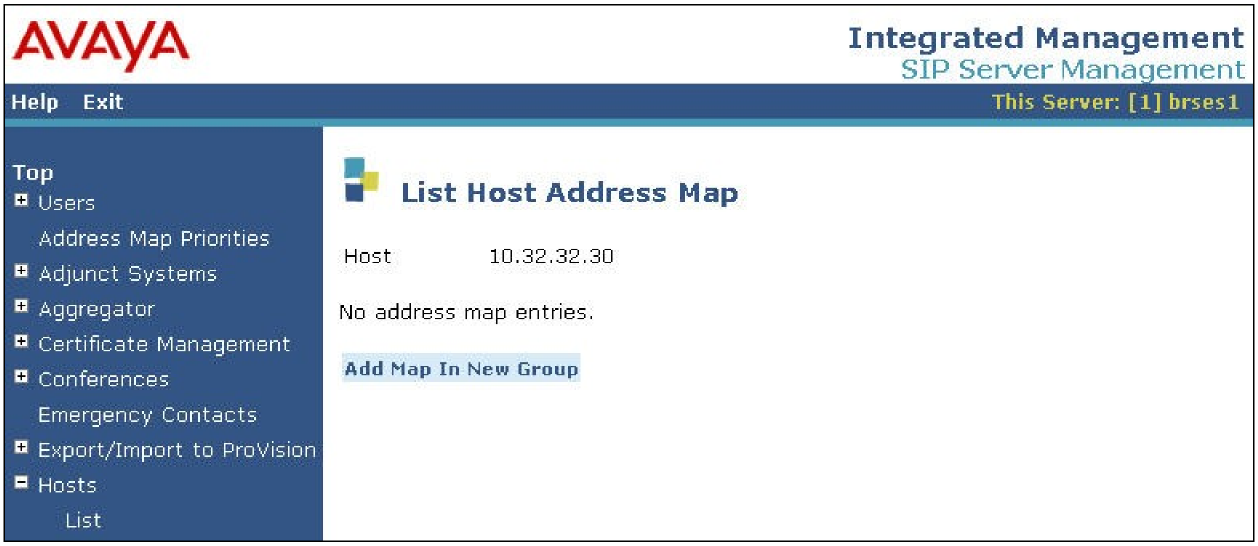


List Hosts

Showing 1 to 1 of 1 Hosts

Commands					Host	Type	SES Version
Edit	Map	Go-To	Test-Link	Delete	10.32.32.30	SES combined home-edge	SES-5.2.1.0-016.4

In the **List Host Address Map** screen below, click **Add Map In New Group** in the right pane.

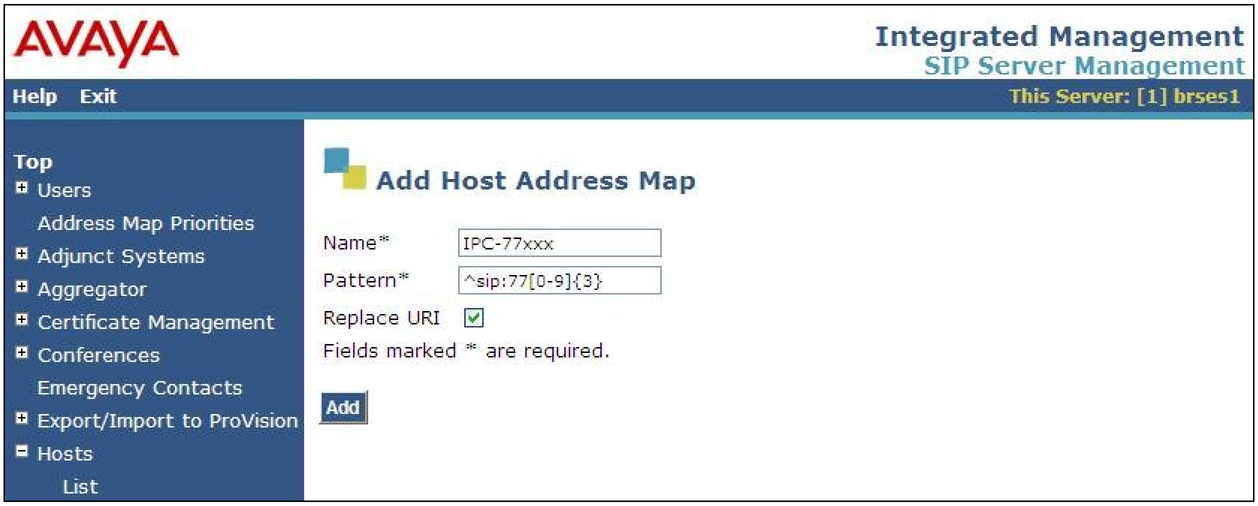


List Host Address Map

Host 10.32.32.30

No address map entries.

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:77[0-9]{3}" is used to match to any IPC turret user extensions of 77xxx. Maintain the check in **Replace URI**.



Name* IPC-77xxx

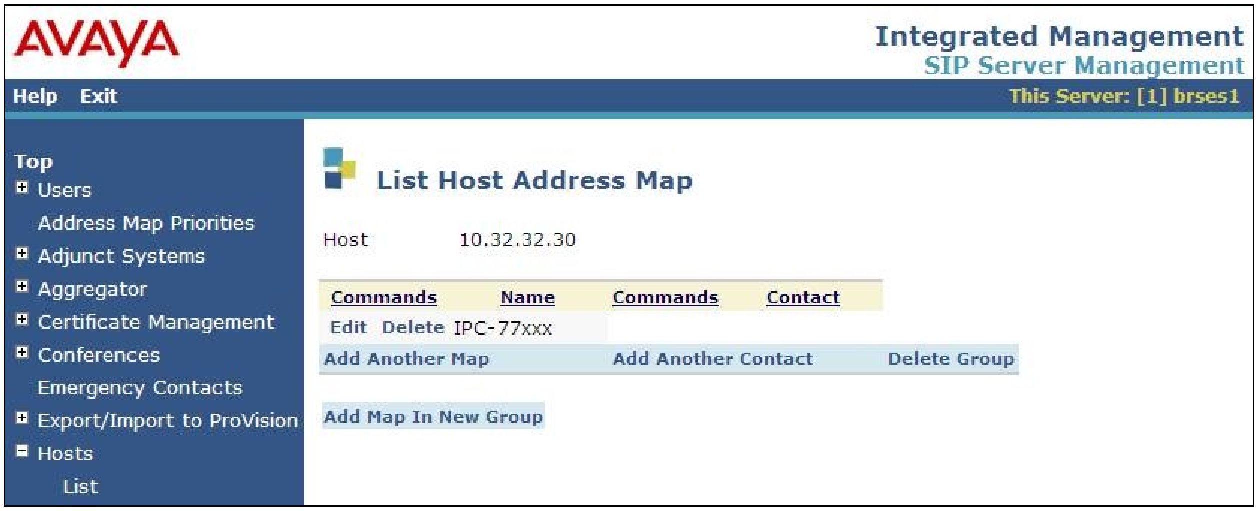
Pattern* ^sip:77[0-9]{3}

Replace URI ☑

Fields marked * are required.

6.3. Administer Host Contact

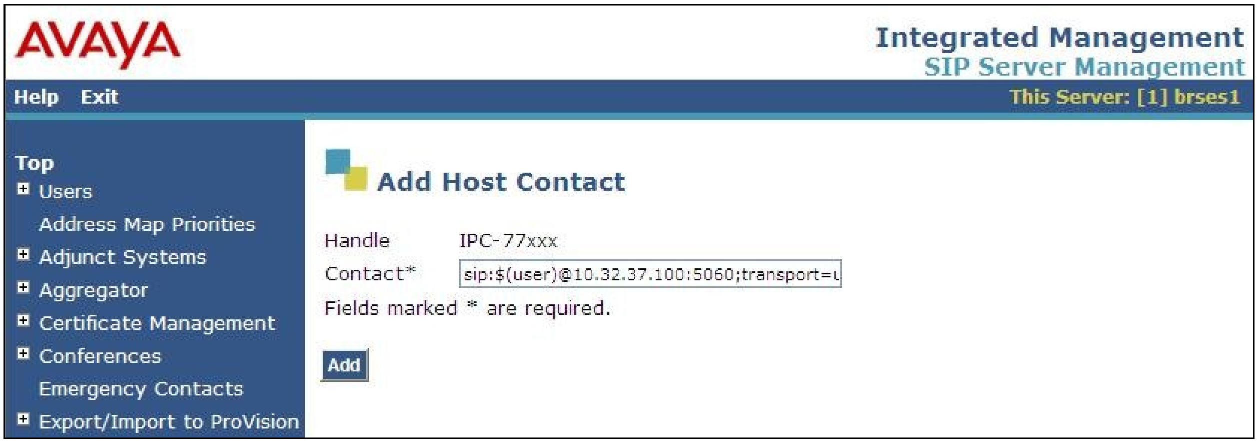
The **List Host Address Map** screen is displayed again, and updated with the newly created address map. Click **Add Another Contact** in the right pane.



Host 10.32.32.30

Commands	Name	Commands	Contact
Edit Delete	IPC-77xxx		

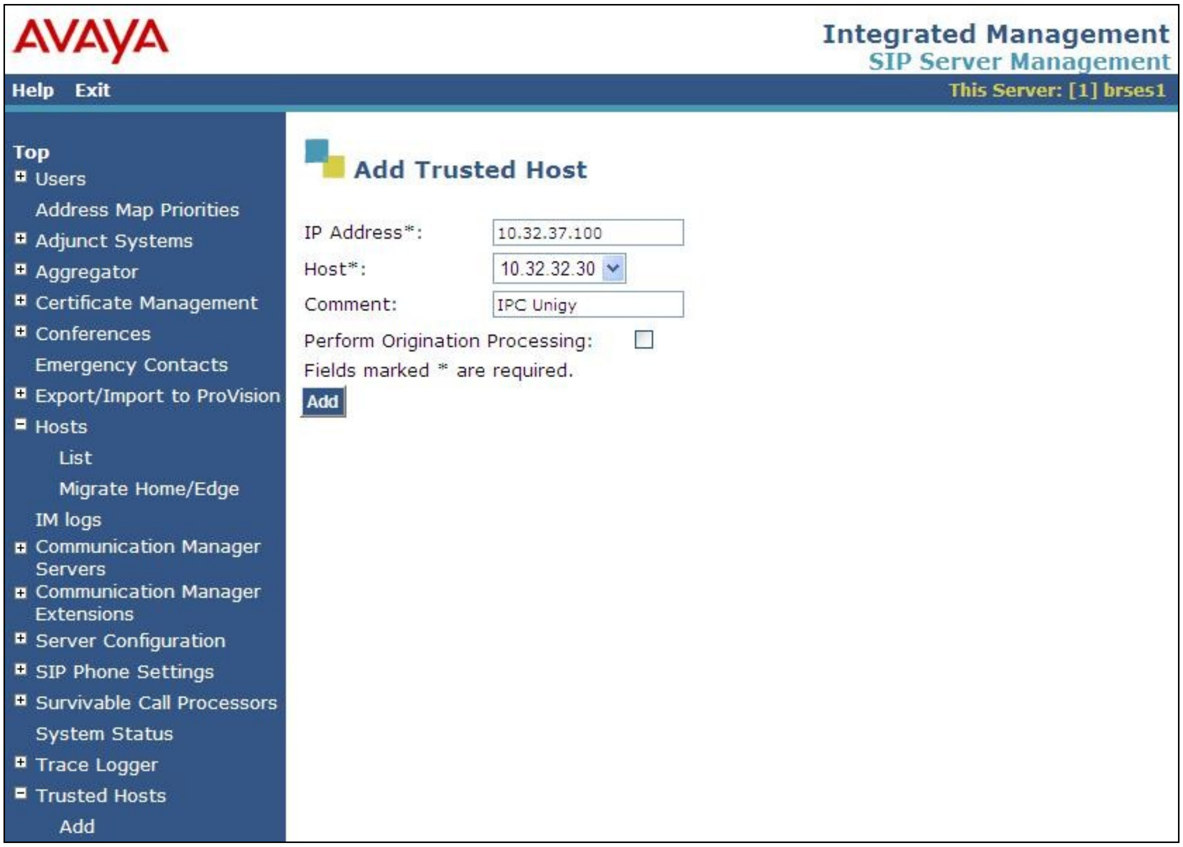
In the **Add Host Contact** screen, enter the contact "sip:$(user)@<destination-IP-address> :5060;transport=udp", where the <destination-IP-address> is the IP address of IPC Media Manager. SES will substitute "$(user)" with the user portion of the request URI before sending the message.



Handle IPC-77xxx
Contact* sip:$(user)@10.32.37.100:5060;transport=u
Fields marked * are required.

6.4. Administer Trusted Host

Select **Trusted Hosts > Add** from the left pane. The **Add Trusted Host** screen is displayed. For the **IP Address** field, enter the IP address of the IPC ESS server from **Section 6.3**. Enter a desired description for **Comment**.



IP Address*: 10.32.37.100
Host*: 10.32.32.30
Comment: IPC Unigy
Perform Origination Processing: ☐
Fields marked * are required.

7. Configure IPC Media Manager

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

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

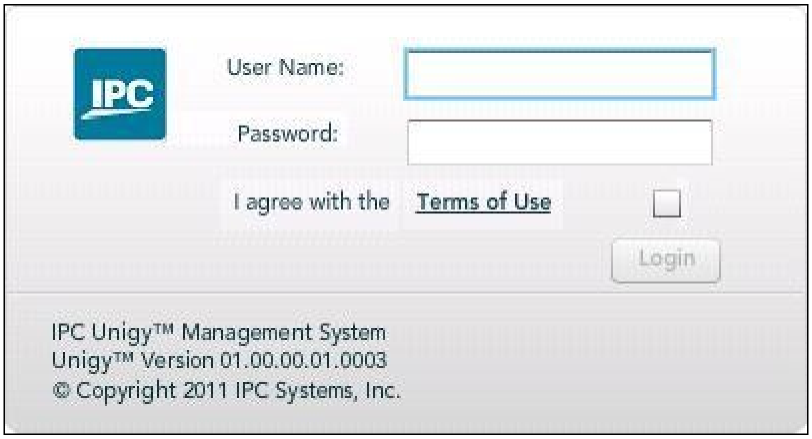
The configuration of Media Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy Management System

Access the Unigy 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**.

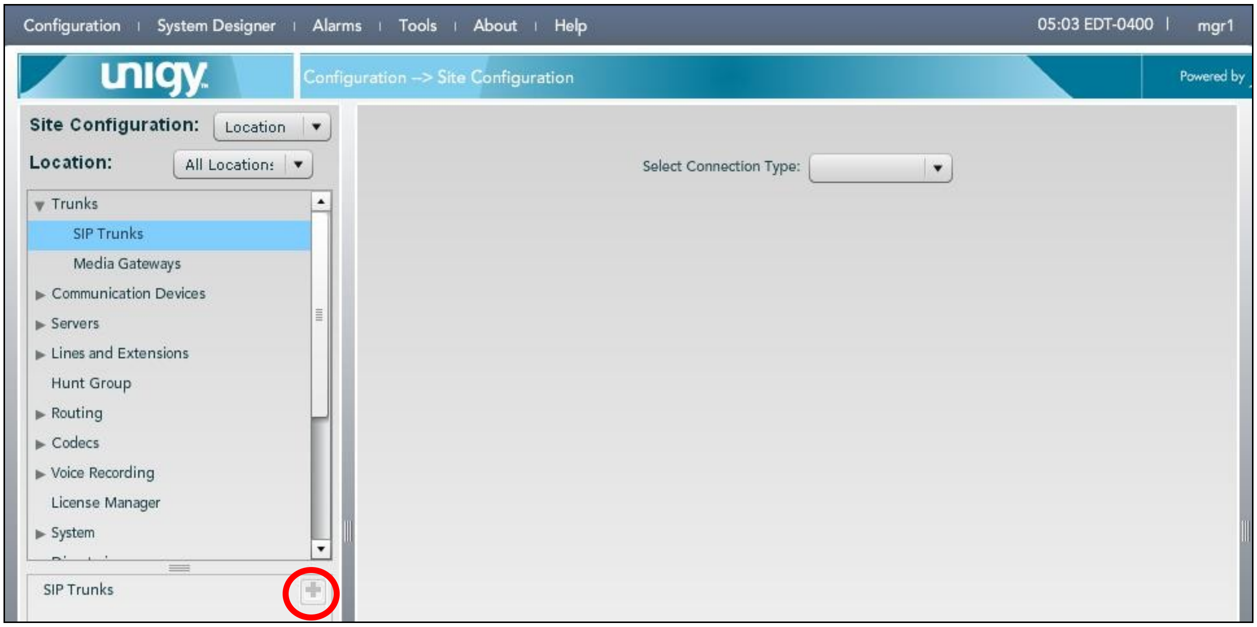


IPC Unigy™ Management System
Unigy™ Version 01.00.00.01.0003
© Copyright 2011 IPC Systems, Inc.

7.2. Administer SIP Trunks

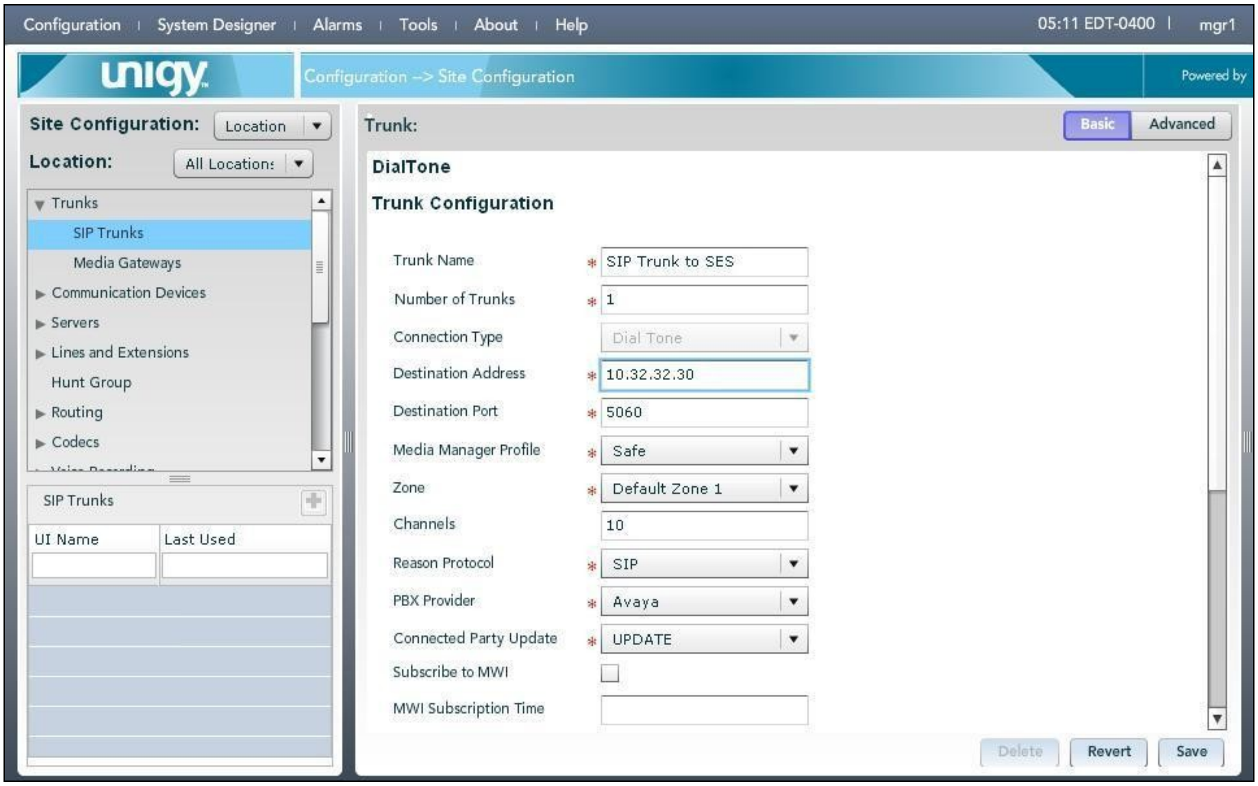
Select **Trunks** > **SIP Trunks** in the left pane, and click the **Add** icon in the lower left pane to add a new SIP trunk.

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.
- **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 from **Section 5.3**.
- **PBX Provider:** "Avaya"
- **Connected Party Update:** "UPDATE"



DialTone

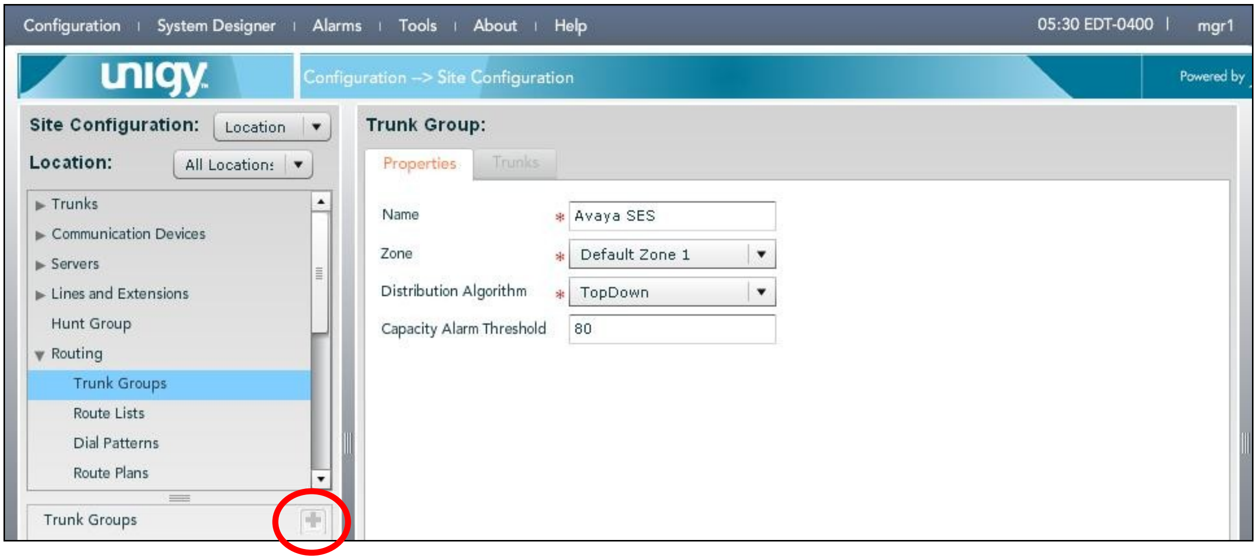
Trunk Configuration

Trunk Name *	SIP Trunk to SES
Number of Trunks *	1
Connection Type	Dial Tone
Destination Address *	10.32.32.30
Destination Port *	5060
Media Manager Profile *	Safe
Zone *	Default Zone 1
Channels	10
Reason Protocol *	SIP
PBX Provider *	Avaya
Connected Party Update *	UPDATE
Subscribe to MWI	☐
MWI Subscription Time	

7.3. Administer Trunk Groups

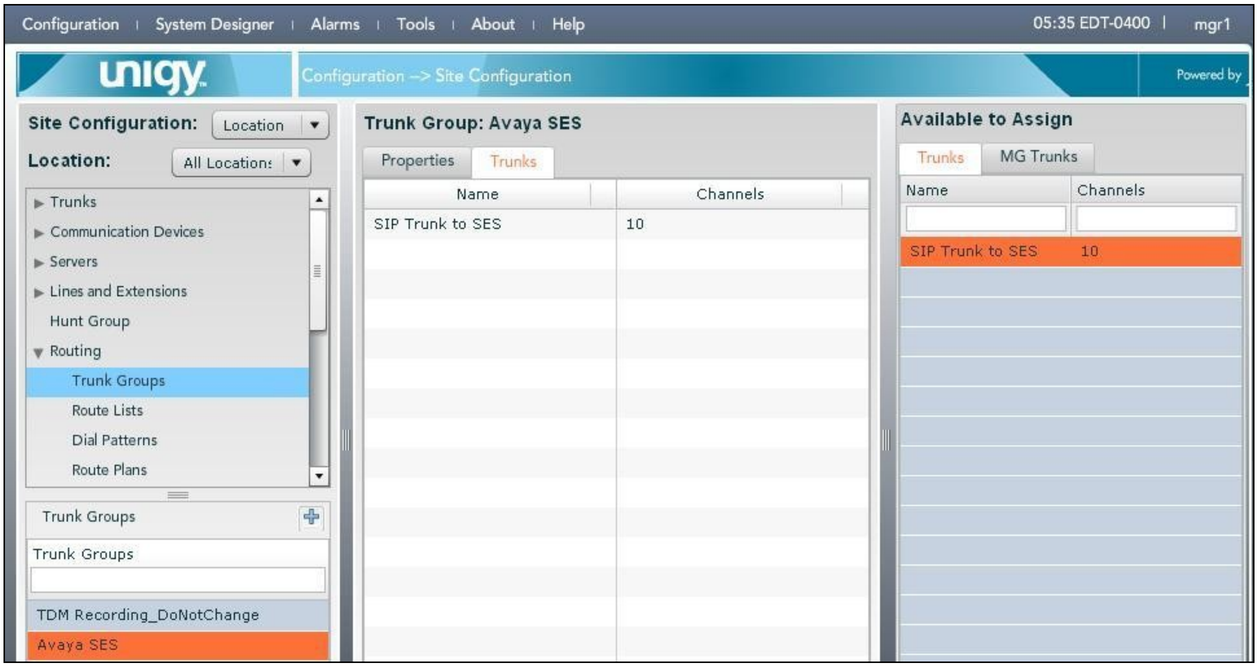
Select **Routing > Trunk Groups** in the left pane, and click the **Add** icon in the lower left pane to add a new trunk group.

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.



Name: Avaya SES
Zone: Default Zone 1
Distribution Algorithm: TopDown
Capacity Alarm Threshold: 80

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).



Trunk Groups:
TDM Recording_DoNotChange
Avaya SES

Trunk Group: Avaya SES

Name	Channels
SIP Trunk to SES	10

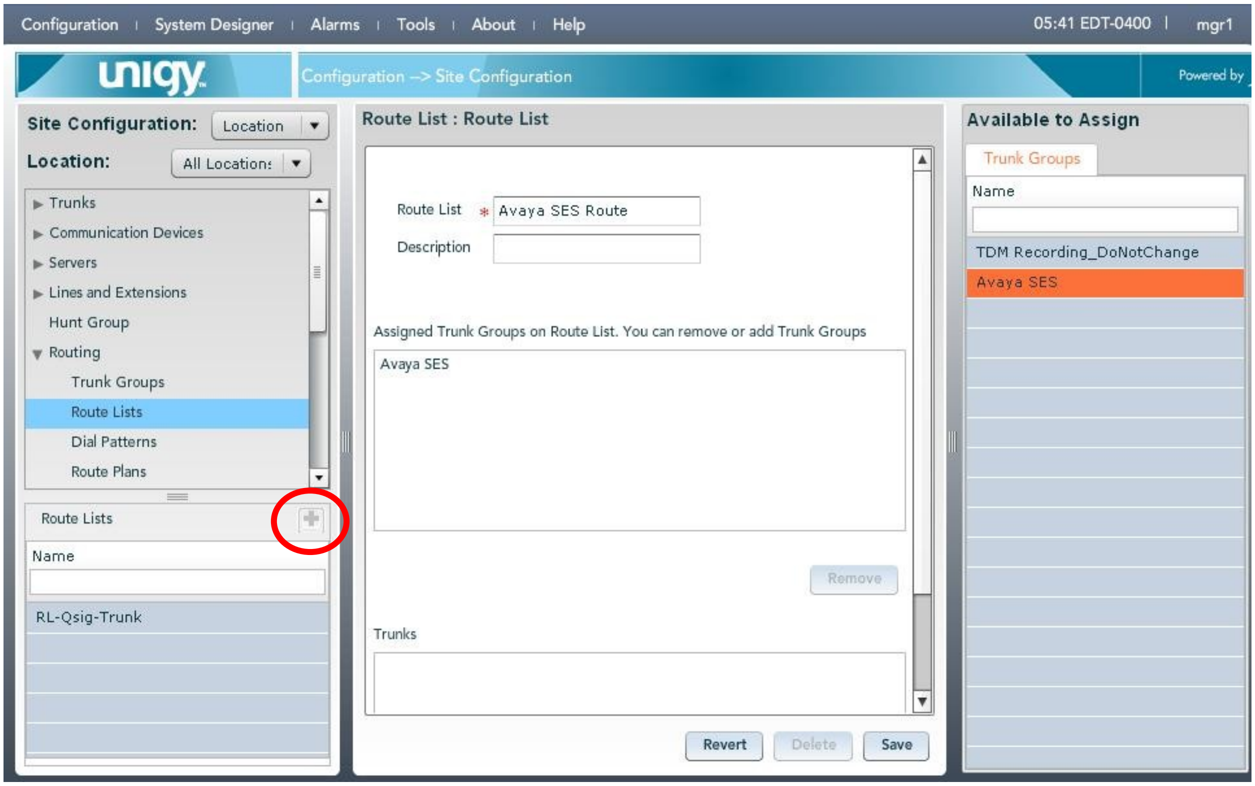
Available to Assign

Name	Channels
SIP Trunk to SES	10

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**.



Route List * Avaya SES Route

Description

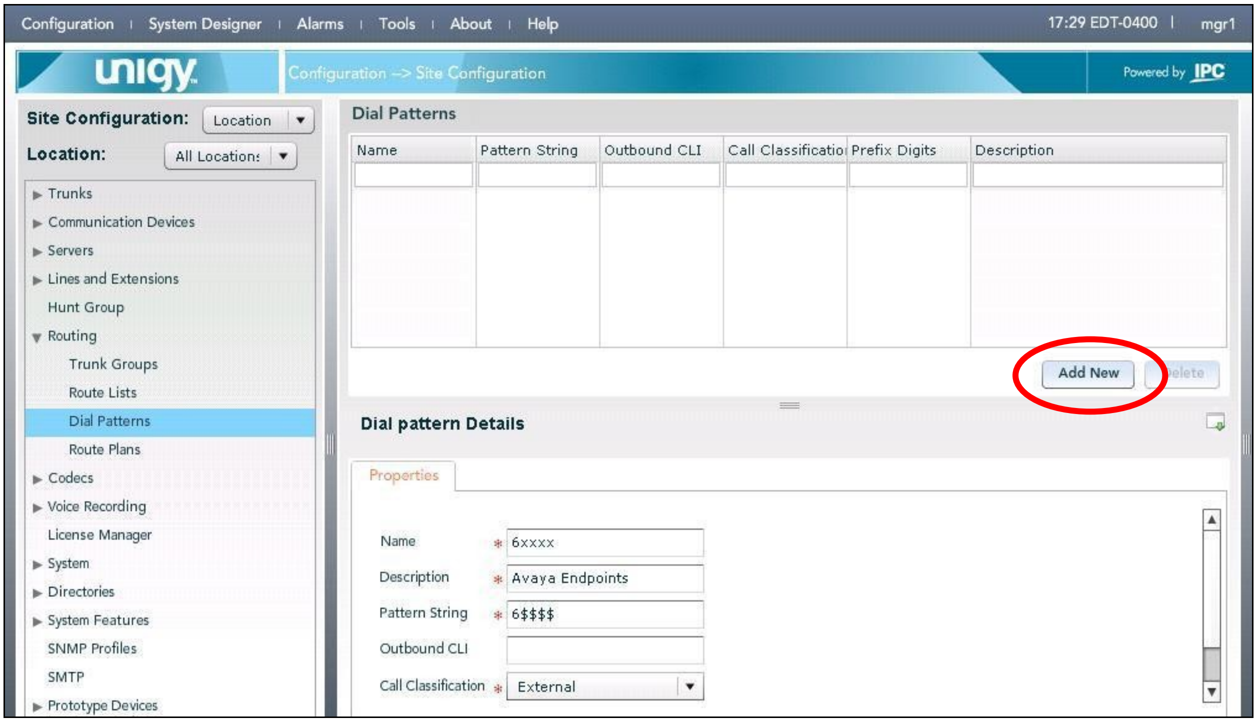
Assigned Trunk Groups on Route List. You can remove or add Trunk Groups

Avaya SES

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 “6$$$$” with “$” matching to any digit. For **Call Classification**, select “External”. Click **Save** (not shown).



Name * 6xxxx

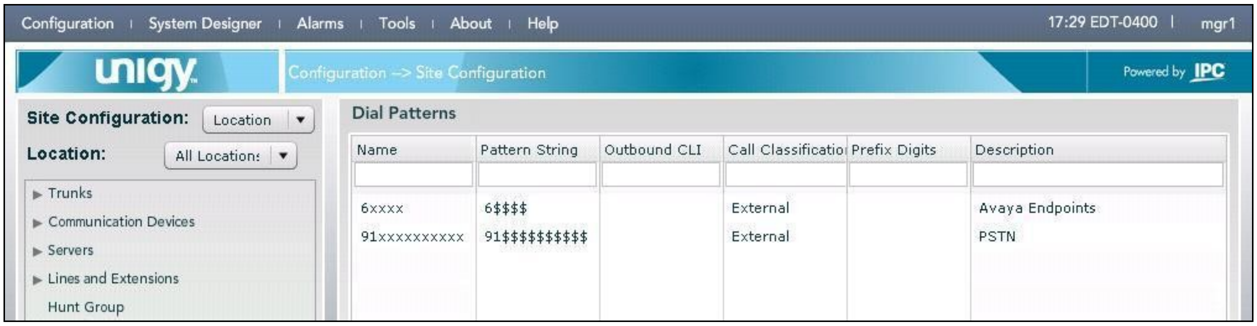
Description * Avaya Endpoints

Pattern String * 6$$$$

Outbound CLI

Call Classification * External

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

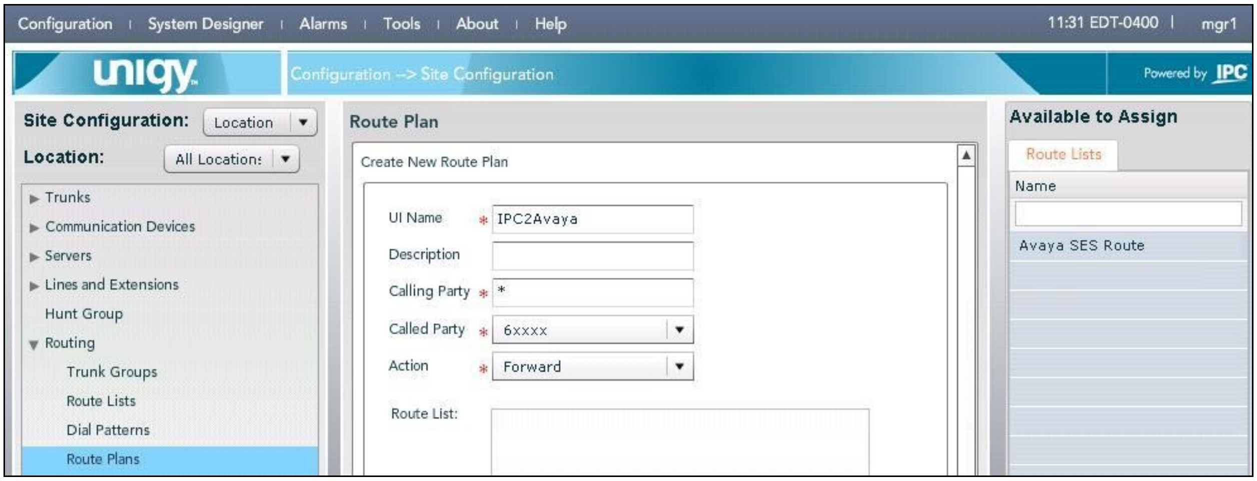


Name	Pattern String	Outbound CLI	Call Classificatio	Prefix Digits	Description
6xxxx	6$$$$		External		Avaya Endpoints
91xxxxxxxxxx	91$$$$$$$$$$		External		PSTN

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 Unigy. For **Called Party**, select the dial pattern for Avaya endpoints from **Section 7.5**. Select "Forward" for **Action**, and click **Save** (not shown).

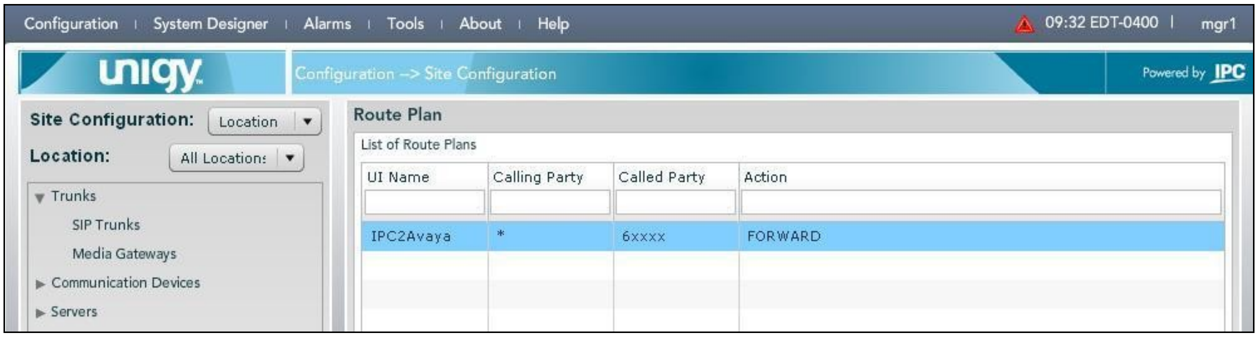


Route Plan

Create New Route Plan

UI Name * IPC2Avaya
Description
Calling Party * *
Called Party * 6xxxx
Action * Forward
Route List:

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).

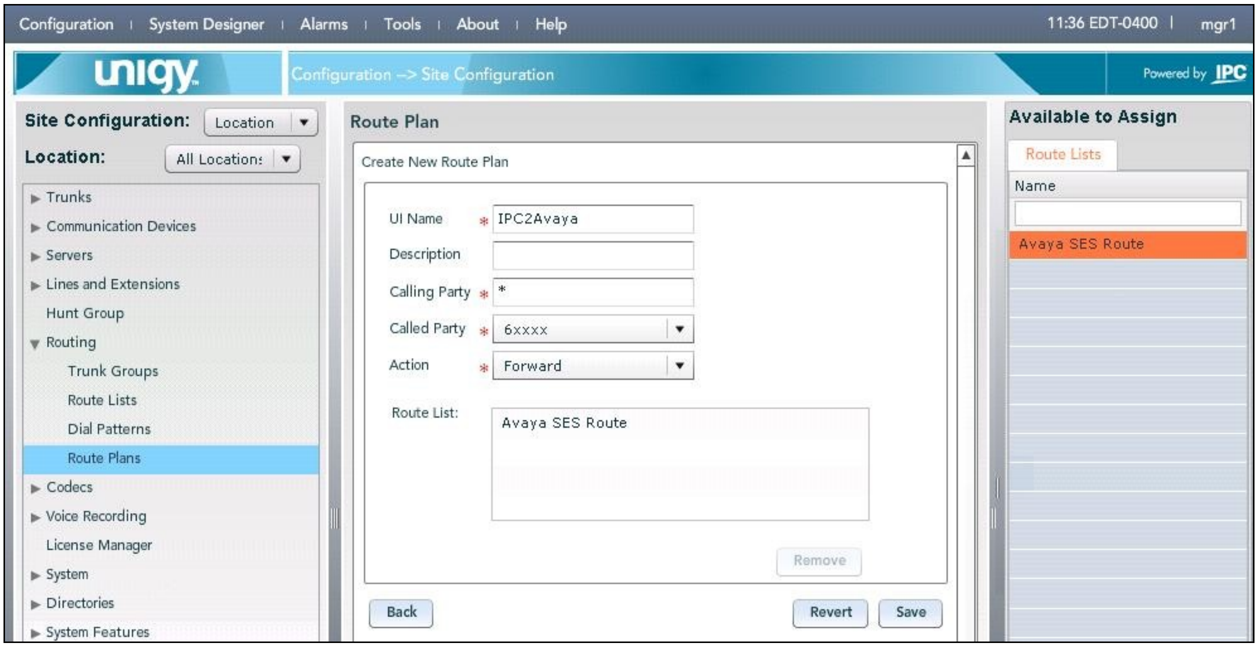

Configuration | System Designer | Alarms | Tools | About | Help
09:32 EDT-0400 | mgr1
unigy
Configuration --> Site Configuration
Powered by IPC
Site Configuration: Location
Location: All Locations
Trunks
SIP Trunks
Media Gateways
Communication Devices
Servers

Route Plan

List of Route Plans

UI Name	Calling Party	Called Party	Action
IPC2Avaya	*	6xxxx	FORWARD

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**.



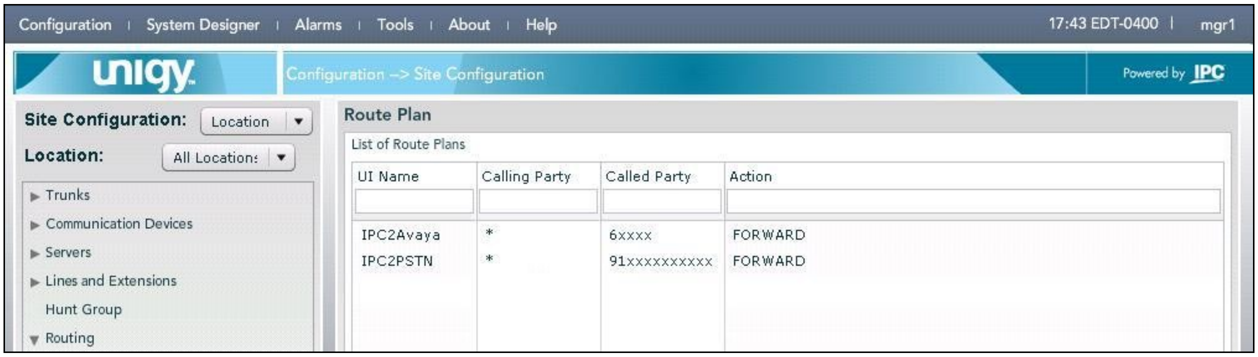
Route Plan

Create New Route Plan

UI Name * IPC2Avaya
Description
Calling Party * *
Called Party * 6xxxx
Action * Forward
Route List: Avaya SES Route

Avaya SES Route

Repeat this section to add another route plan for the PSTN. In the compliance testing, two route plans were created as shown below.



Route Plan

List of Route Plans

UI Name	Calling Party	Called Party	Action
IPC2Avaya	*	6xxxx	FORWARD
IPC2PSTN	*	91xxxxxxxxxx	FORWARD

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 Unigy.

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 5

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0005/001 T00083   in-service/idle    no
0005/002 T00084   in-service/idle    no
0005/003 T00085   in-service/idle    no
0005/004 T00086   in-service/idle    no
0005/005 T00087   in-service/idle    no
0005/006 T00082   in-service/idle    no
0005/007 T00088   in-service/idle    no
0005/008 T00089   in-service/idle    no
0005/009 T00090   in-service/idle    no
0005/010 T00091   in-service/idle    no
```

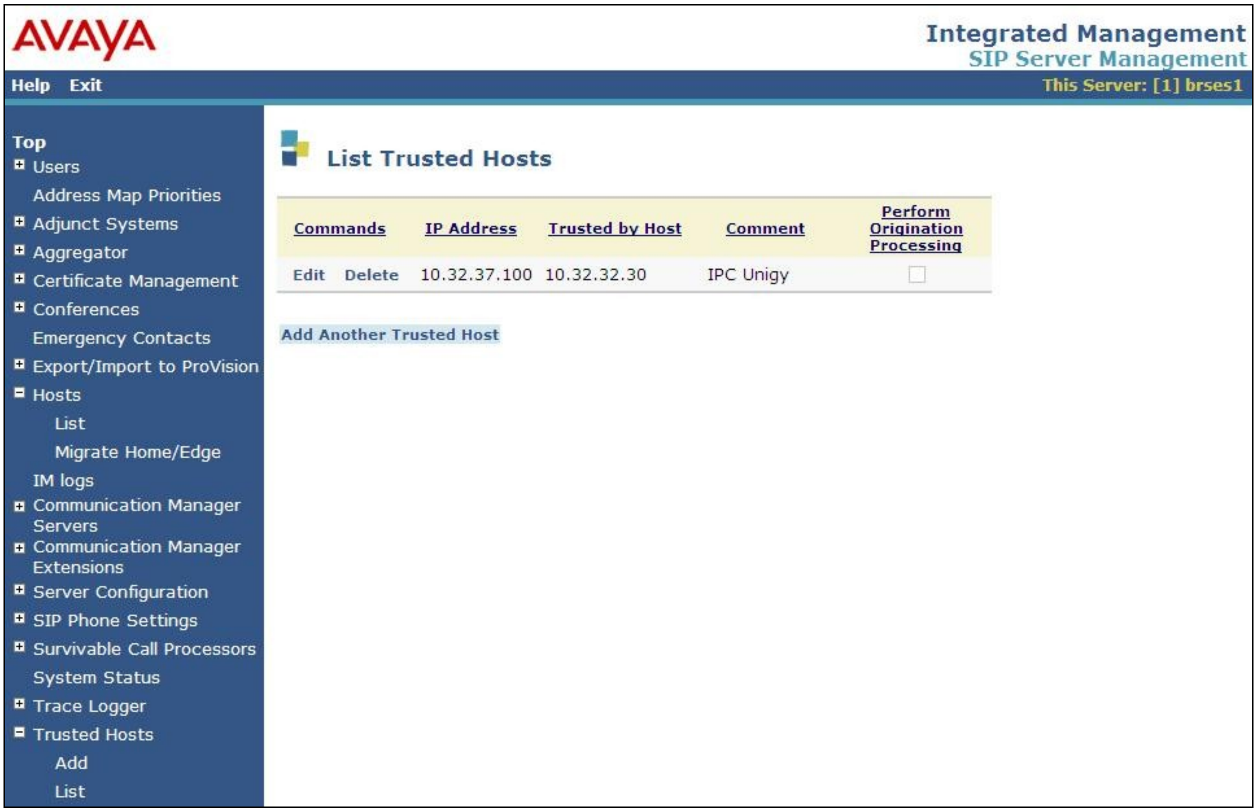
Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.4**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 5
                         STATUS SIGNALING GROUP

        Group ID: 5                             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.



List Trusted Hosts

Commands	IP Address	Trusted by Host	Comment	Perform Origination Processing
Edit Delete	10.32.37.100	10.32.32.30	IPC Unigy	☐

8.3. Verify IPC Unigy

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 Unigy 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. *Unigy 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.