Avaya Solution & Interoperability Test Lab

Application Notes for IPC UnigyV2 with Avaya Aura® Session Manager 6.2 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC UnigyV2 to interoperate with Avaya Aura® Session Manager 6.2 using SIP trunks.

IPC UnigyV2 is a trading communication solution. In the compliance testing, IPC UnigyV2 used SIP trunks to Avaya Aura® Session Manager, 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 UnigyV2 to interoperate with Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

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 offers 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, 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.729, 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.

- Even when IPC UnigyV2 is configured with UDP, the TCP protocol must be configured to be allowed on Avaya Session Manager as UnigyV2 switches over to use TCP for diversions.

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® Session Manager, 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 (7200x and 7202x), and IPC turret users at the Remote site (7205x).

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

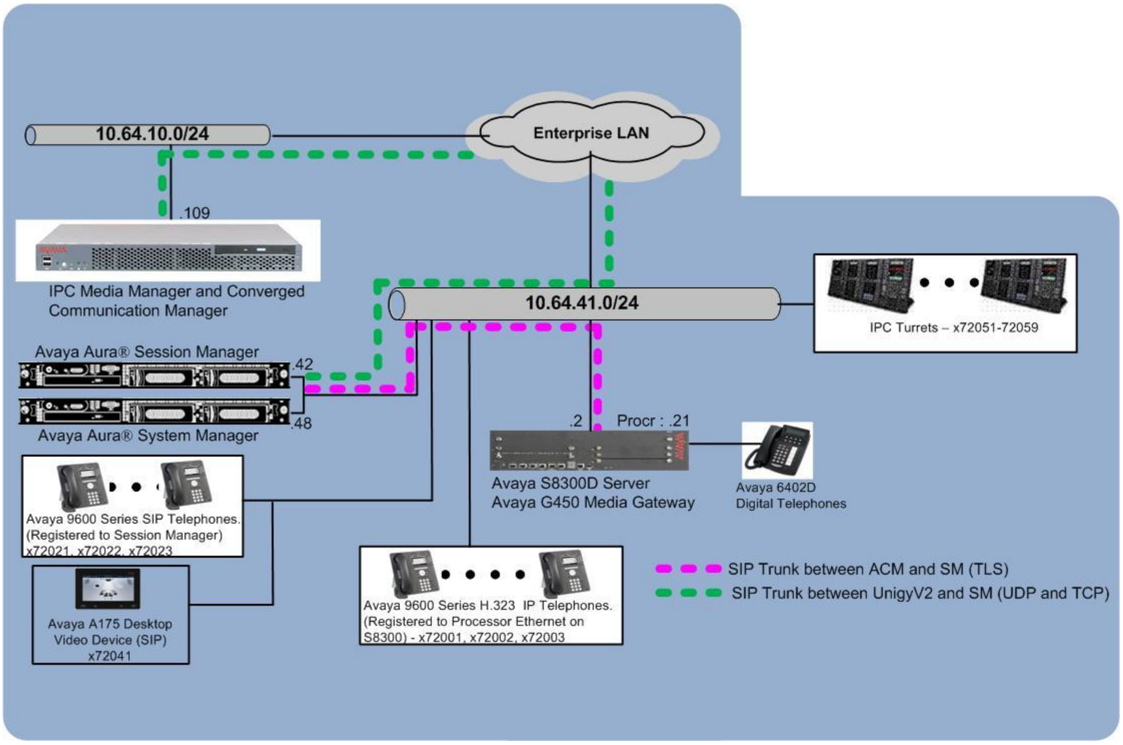

10.64.10.0/24
Enterprise LAN
.109
IPC Media Manager and Converged Communication Manager
10.64.41.0/24
IPC Turrets – x72051-72059
Avaya Aura® Session Manager
.42
.48
Avaya Aura® System Manager
.2
Procr : .21
Avaya S8300D Server
Avaya G450 Media Gateway
Avaya 6402D Digital Telephones
Avaya 9600 Series SIP Telephones. (Registered to Session Manager) x72021, x72022, x72023
Avaya A175 Desktop Video Device (SIP) x72041
Avaya 9600 Series H.323 IP Telephones. (Registered to Processor Ethernet on S8300) - x72001, x72002, x72003
SIP Trunk between ACM and SM (TLS)
SIP Trunk between UnigyV2 and SM (UDP and TCP)

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 S8300D Server	R016x.02.0.823.0-20001
Avaya G450 Media Gateway • TN464HP DS1 Interface	 HW02 FW024
Avaya Aura® Session Manager	6.2.2.0622005
Avaya Aura® System Manager	6.2.12.0
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 96xx IP Telephone (SIP)	2.6.4
Avaya A175 Desktop Video Device (SIP)	1.0.2
IPC UnigyV2 • Media Manager • Converged Communication Manage • 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:

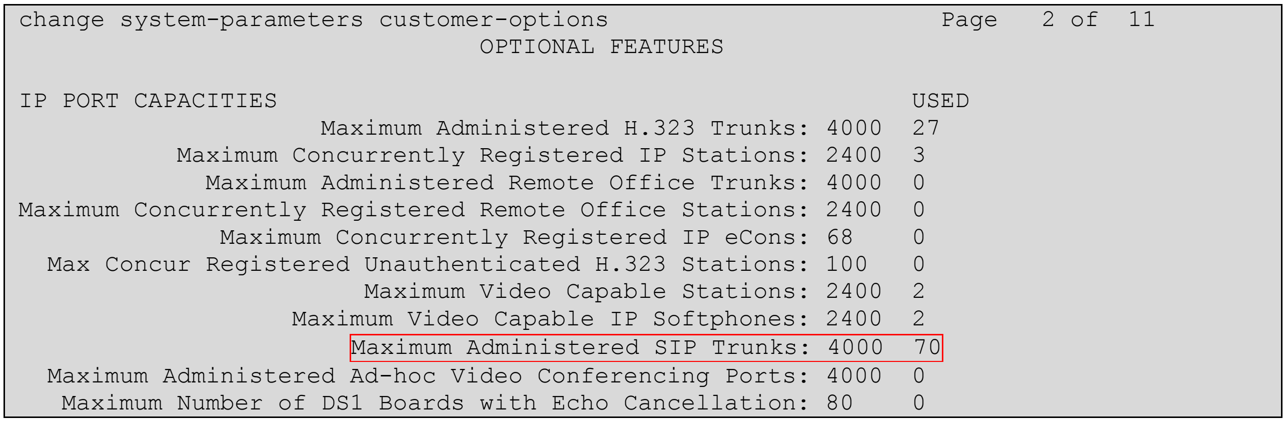
- Verify Communication Manager license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR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

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for the IPC turret users.

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.

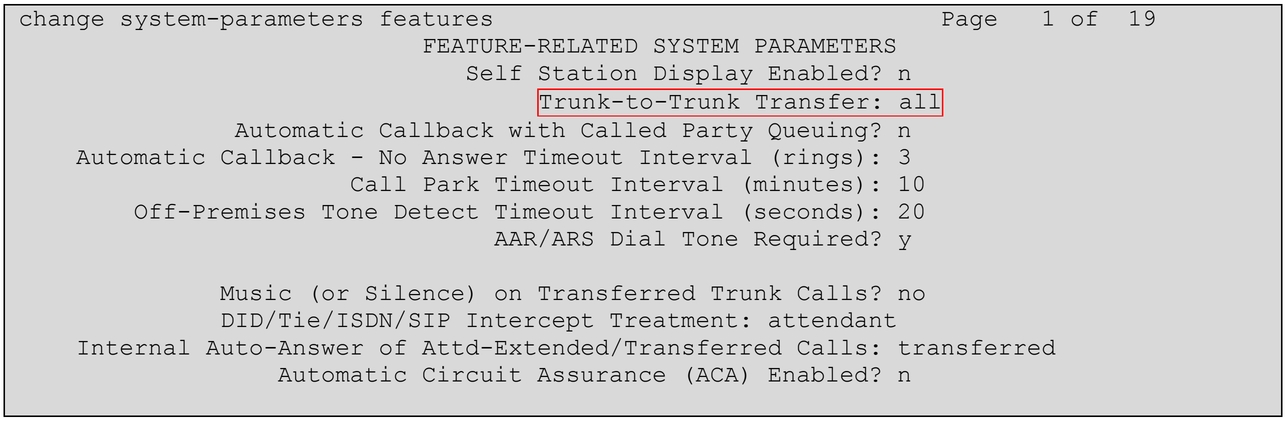


```
change system-parameters customer-options                       Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  27
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  2
                   Maximum Video Capable IP Softphones: 2400  2
                       Maximum Administered SIP Trunks: 4000  70
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    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.

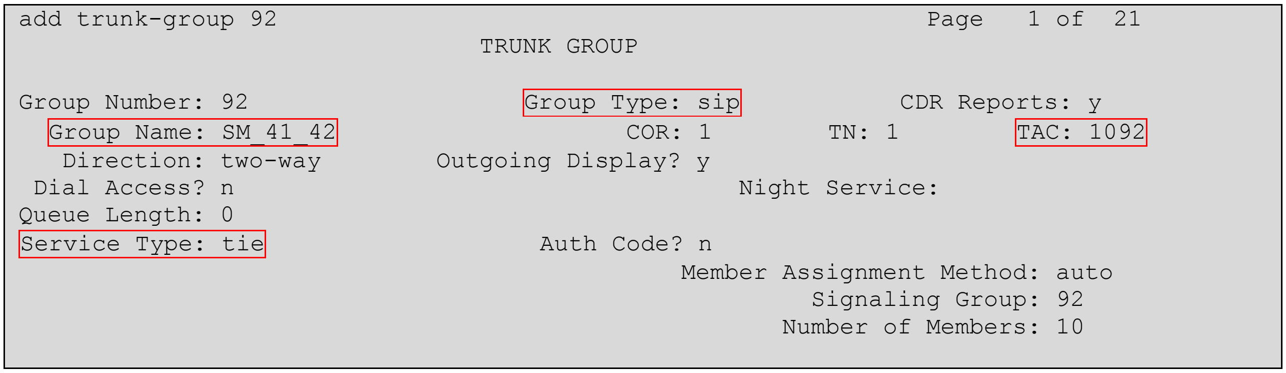


```
change system-parameters features                              Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback 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: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n
```

5.3. Administer SIP Trunk Group

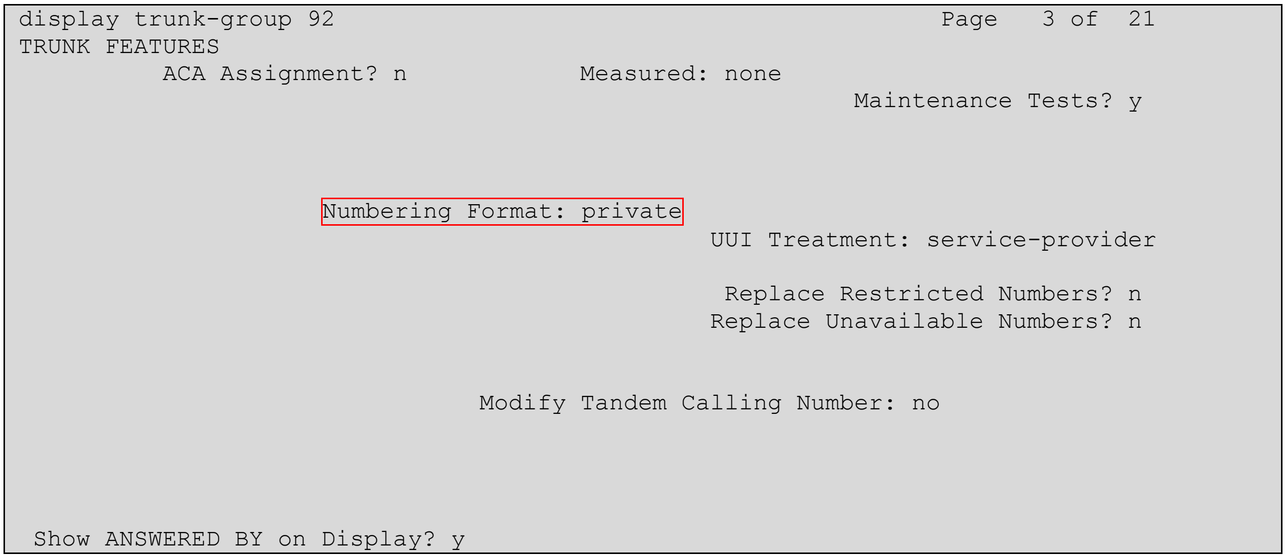
Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “92”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”



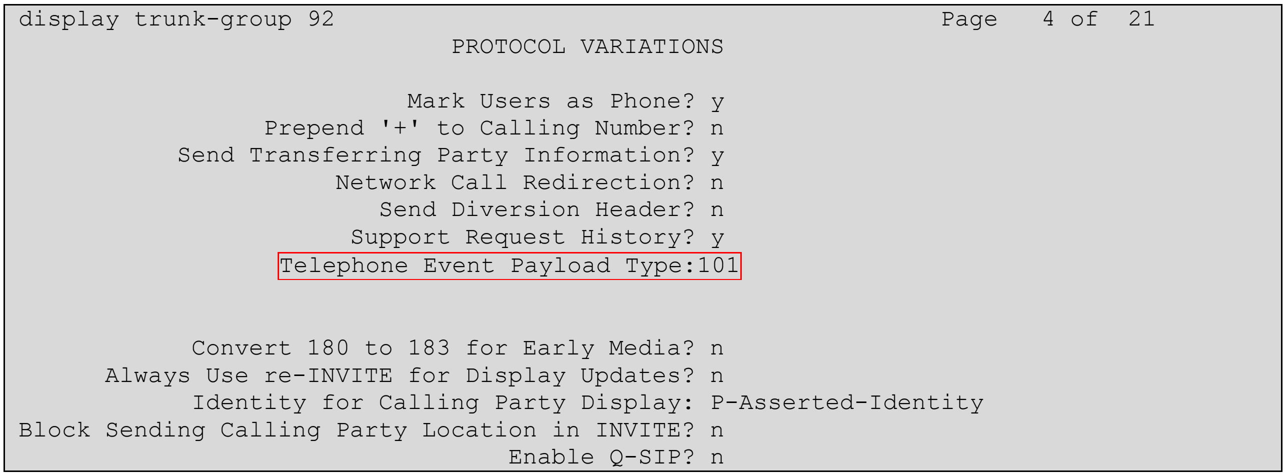
```
add trunk-group 92                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 92                   Group Type: sip           CDR Reports: y
  Group Name: SM_41_42                    COR: 1        TN: 1        TAC: 1092
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 92
                                                     Number of Members: 10
```

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



```
display trunk-group 92                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Navigate to **Page 4**, and enter “101” for **Telephone Event Payload Type**.

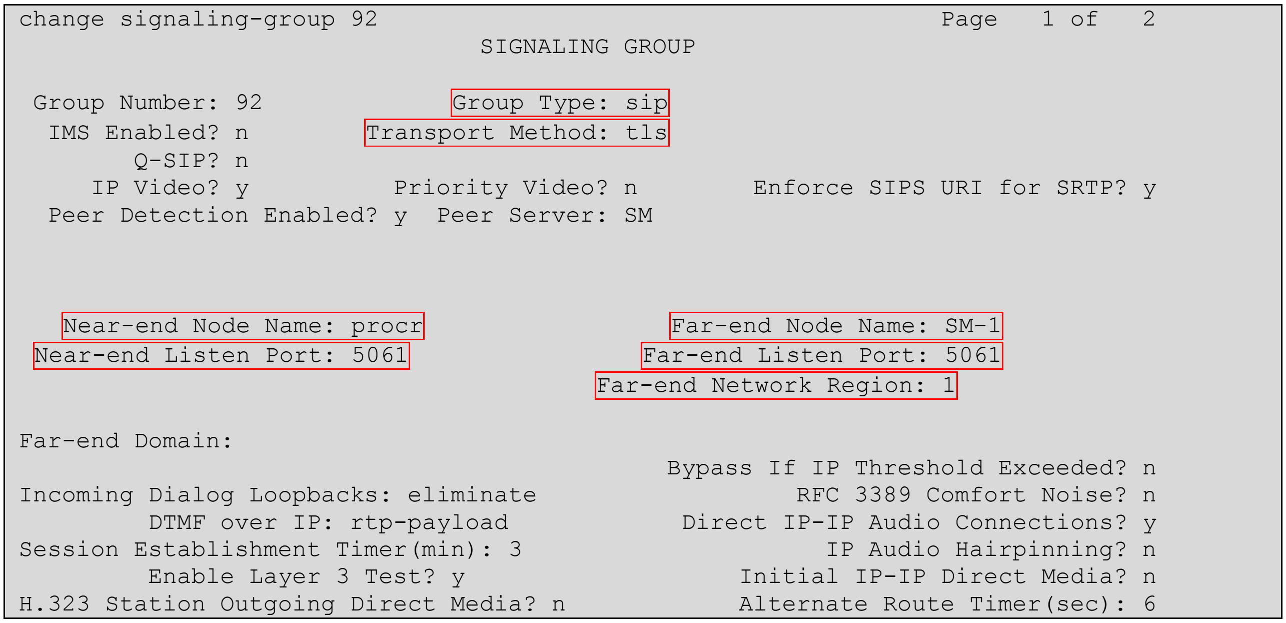


```
display trunk-group 92                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                           Mark Users as Phone? y
                 Prepend '+' to Calling Number? n
           Send Transferring Party Information? y
                      Network Call Redirection? n
                         Send Diversion Header? n
                       Support Request History? y
                  Telephone Event Payload Type:101


            Convert 180 to 183 for Early Media? n
      Always Use re-INVITE for Display Updates? n
            Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                  Enable Q-SIP? n
```

5.4. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “92”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** An existing C-LAN node name or procr.
- **Far-end Node Name:** The existing Session Manager node name.
- **Near-end Listen Port:** An available port for integration on Communication Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region for integration with IPC UnigyV2.

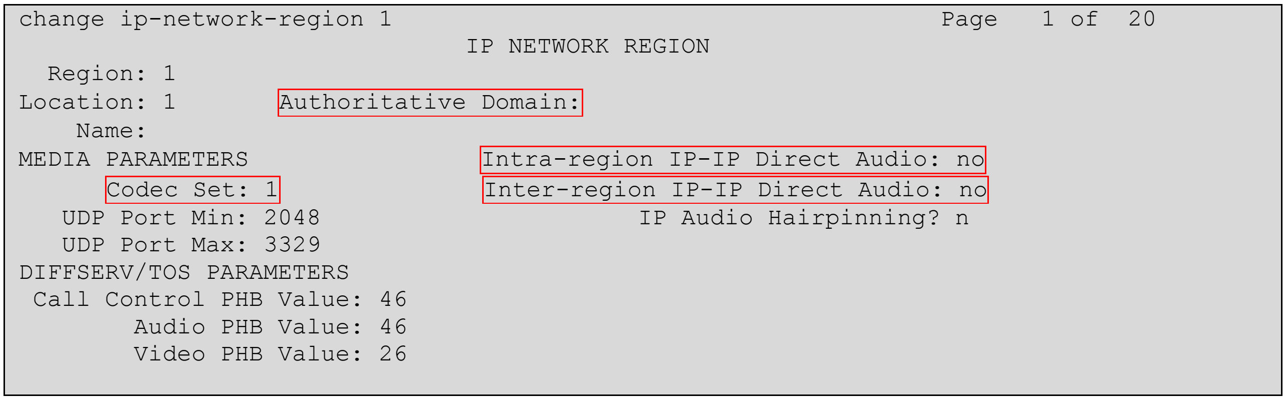


```
change signaling-group 92                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 92             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM-1
 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? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct 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 0**.

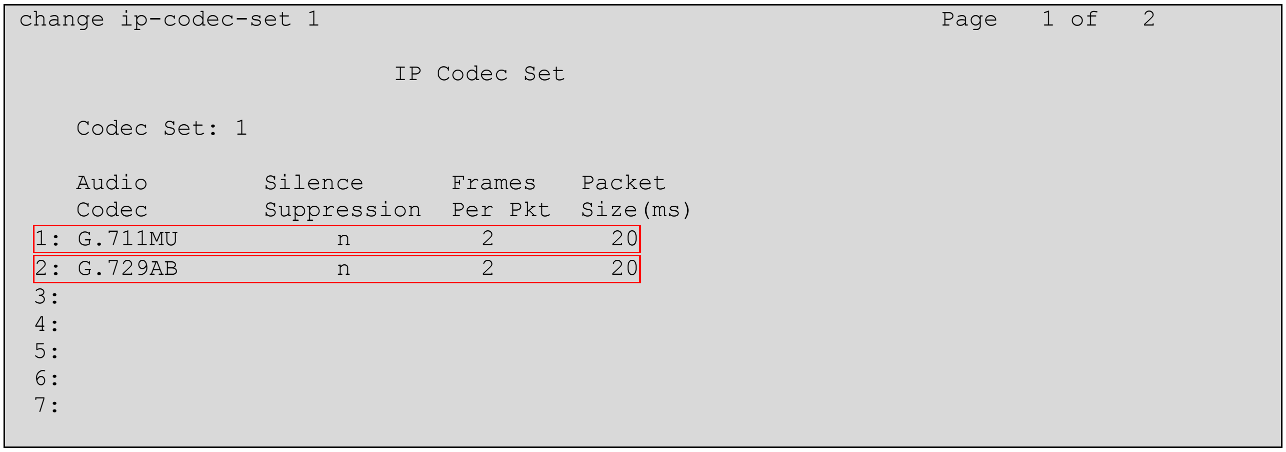
For **Authoritative Domain**, leave the field blank. Enter a descriptive **Name**. Enter “no” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with IPC UnigyV2.



```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain:
    Name:
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
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```

5.6. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that IPC UnigyV2 supports the G.711 and G.729 codec variants, and requires the codec order on Avaya to match the codec order specified on IPC UnigyV2. The codec order shown below matched the default order on IPC UnigyV2.

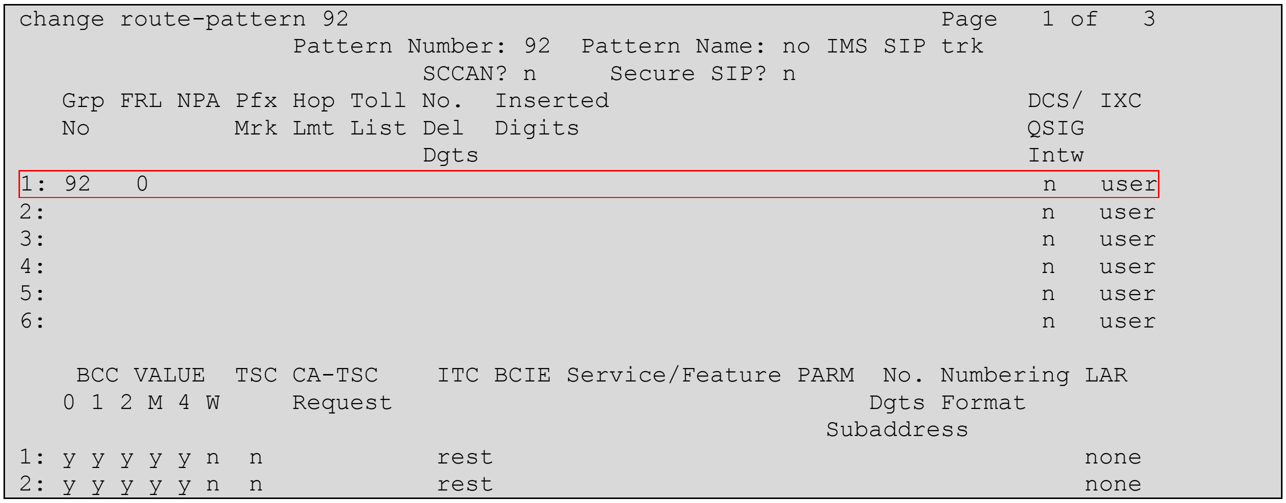


```
change ip-codec-set 1                                           Page   1 of   2

                          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:
 6:
 7:
```

5.7. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach IPC, in this case “92”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 0**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.



```
change route-pattern 92                                         Page   1 of   3
                   Pattern Number: 92  Pattern Name: no IMS SIP trk
                            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: 92   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
2: y y y y y n  n            rest                                          none
```

5.8. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 0**. In the example shown below, all calls originating from a 5-digit extension beginning with 72 and routed to trunk group 92 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext               Trk        Private          Total
Len Code              Grp(s)     Prefix           Len
 5  72                92                          5     Total Administered: 10
 5  72                93                          5        Maximum Entries: 540
```

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
 141044          11   0                   ars   n
 2               5    0                   aar   n
 20004           5    0                   aar   n
 33              5    0                   aar   n
 50000           5    0                   aar   n
 53005           5    0                   aar   n
 7050            4    0                   aar   n
 7202            5    0                   aar   n
 7203            5    0                   aar   n
 7204            5    0                   aar   n
 7205            5    0                   aar   n
```

5.10. Administer AAR Analysis

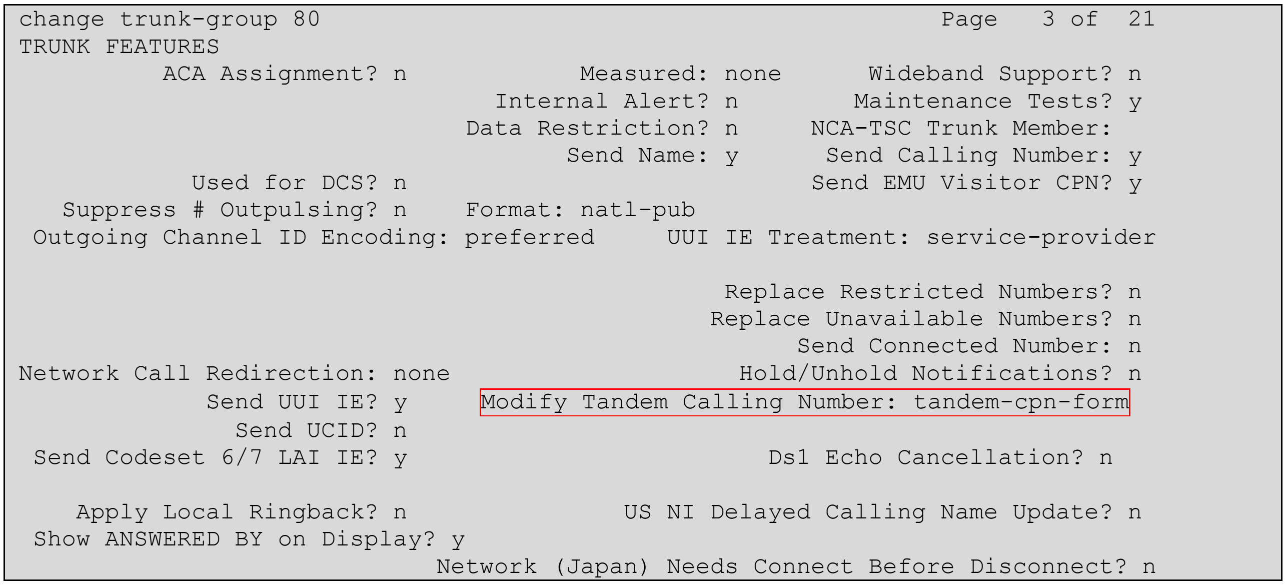
Use the “change aar analysis 0” command, and add an entry to specify how to route calls to 7205x. In the highlighted example shown below, calls with digits 7205x will be routed using route pattern “92” from **Section 0**.

```
change aar analysis 0                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 3

          Dialed                Total     Route     Call    Node   ANI
          String               Min  Max  Pattern    Type    Num    Reqd
    600                        4    4     14        aar            n
    6000                       5    5     92        unku           n
    7202                       5    5     92        unku           n
    7204                       5    5     92        unku           n
    7205                       5    5     92        unku           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”.

Navigate to **Page 3**. For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow for the calling party number from IPC to be modified.

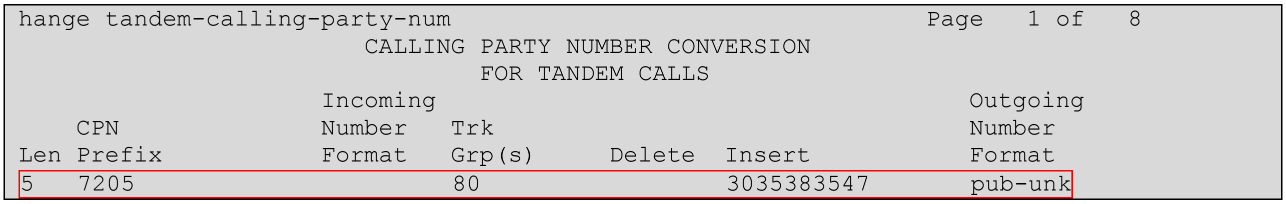


```
change trunk-group 80                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n        Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? y
   Suppress # Outpulsing? n    Format: natl-pub
 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: tandem-cpn-form
               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 7 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”.



```
hange tandem-calling-party-num                                 Page   1 of   8
                        CALLING PARTY NUMBER CONVERSION
                                FOR TANDEM CALLS
                     Incoming                                     Outgoing
    CPN              Number   Trk                                 Number
Len Prefix           Format   Grp(s)     Delete  Insert           Format
5   7205                      80                 3035383547       pub-unk
```

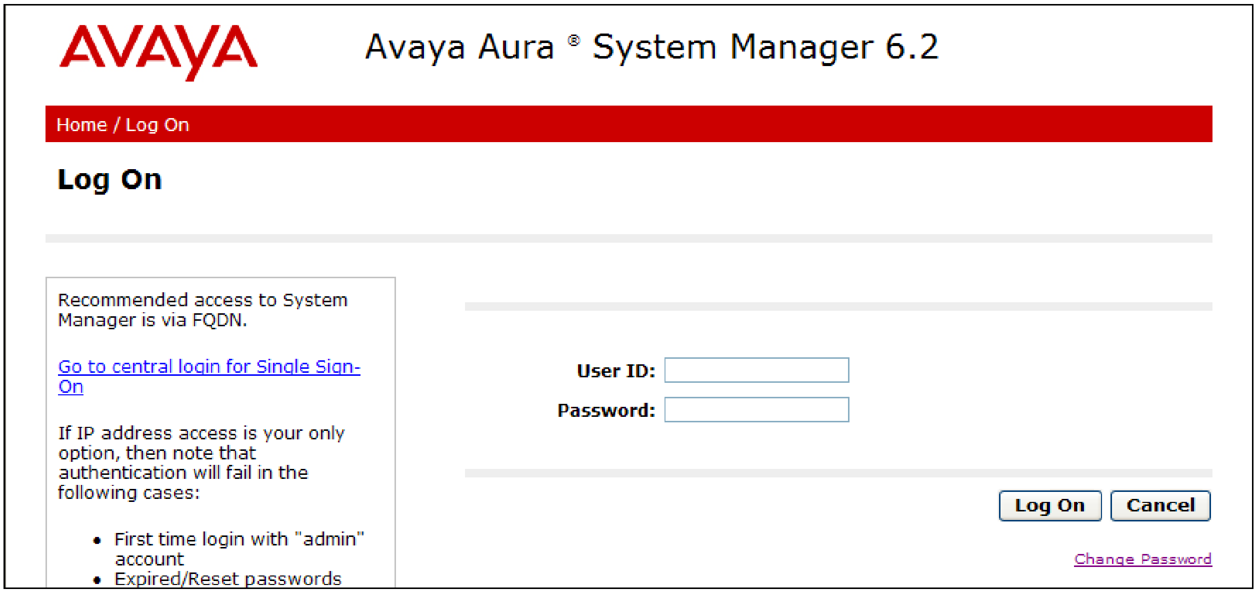
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer adaptations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

6.1. Launch System Manager

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



Recommended access to System Manager is via FQDN.

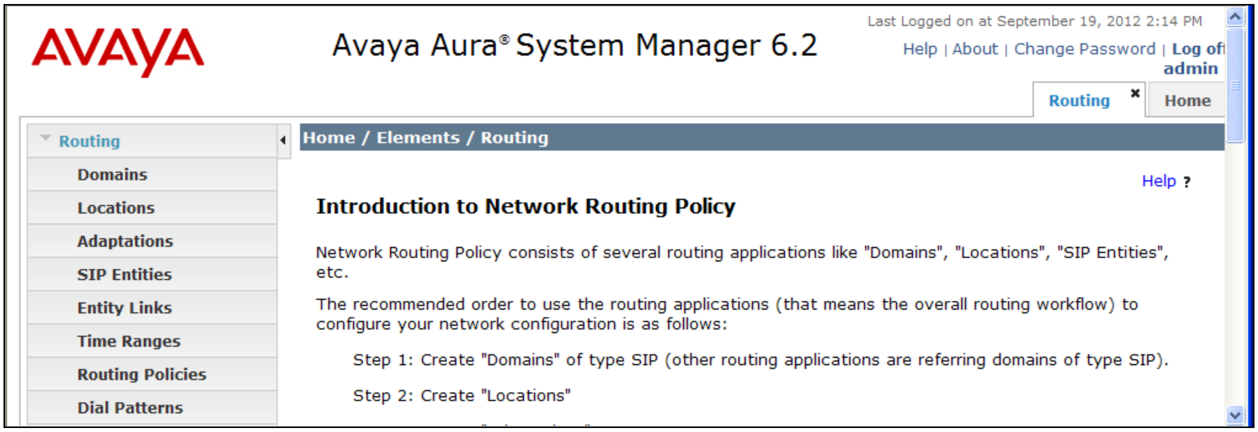
Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

6.2. Administer Locations

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing → Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for IPC.


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at September 19, 2012 2:14 PM
Help | About | Change Password | Log off
admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Home / Elements / Routing
Help ?

Introduction to Network Routing Policy

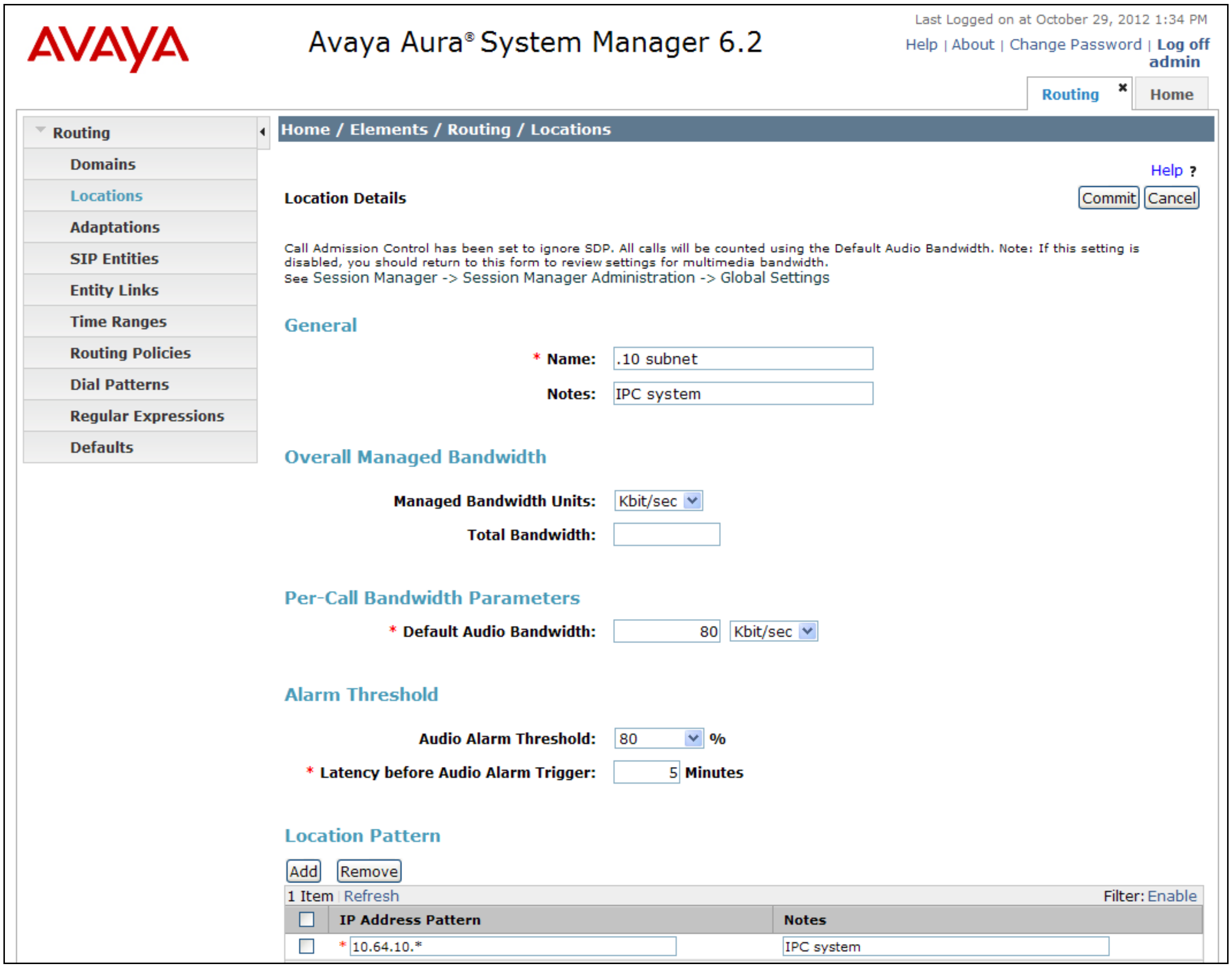
Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. In the **Location Pattern** sub-section, click **Add** and enter the applicable **IP Address Pattern** as shown below. Retain the default values in the remaining fields.



Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. Note: If this setting is disabled, you should return to this form to review settings for multimedia bandwidth.
See Session Manager -> Session Manager Administration -> Global Settings

General

* Name: .10 subnet

Notes: IPC system

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Audio Alarm Threshold: 80 %

* Latency before Audio Alarm Trigger: 5 Minutes

Location Pattern

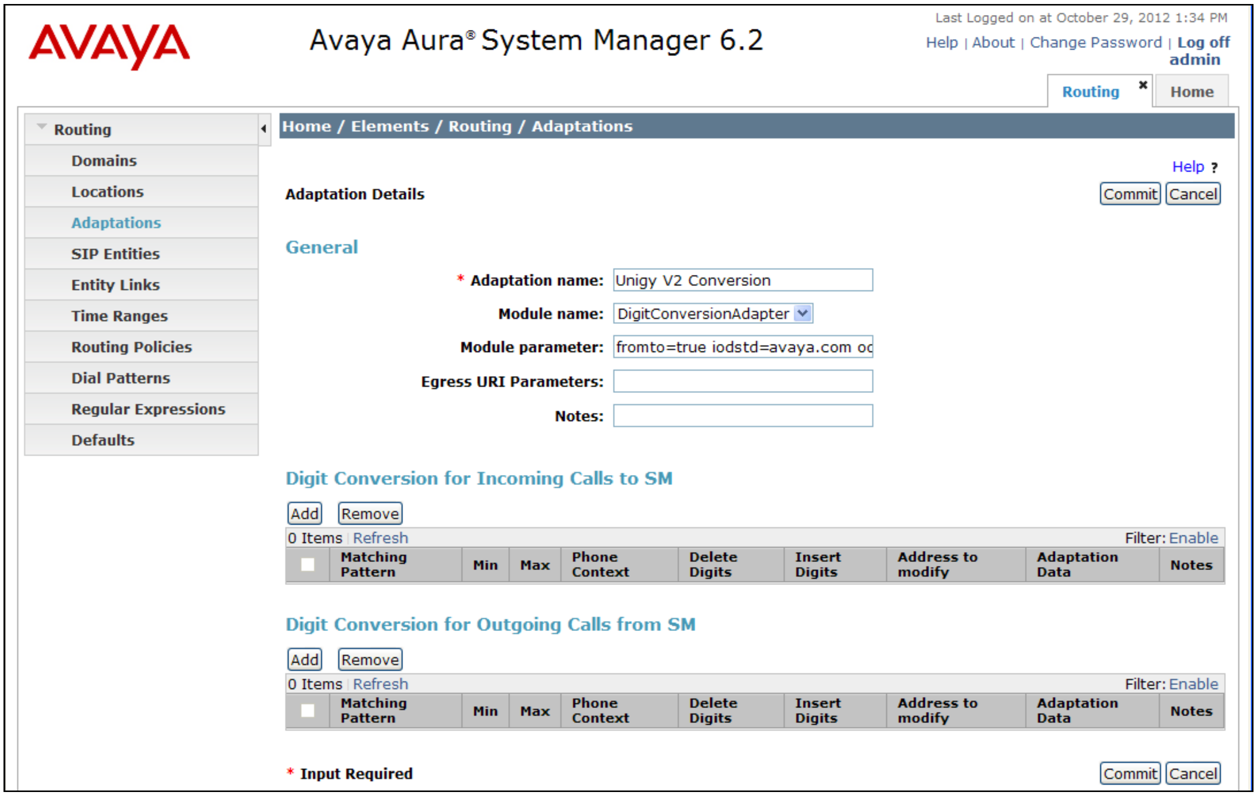
□	IP Address Pattern	Notes
□	* 10.64.10.*	IPC system

6.3. Administer Adaptations

Select **Routing → Adaptations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new adaptation for IPC.

The **Adaptation Details** screen is displayed. In the **General** sub-section, enter a descriptive **Adaptation name**. For **Module name**, select "DigitConversionAdapter".

For **Module parameter**, enter "iodstd=avaya.com odstd=ipc.com" where "avaya.com" and "ipc.com" are the applicable domain. This will set the source and destination domains for all incoming and outgoing calls for IPC.



Adaptation Details

General

* Adaptation name:	Unigy V2 Conversion
Module name:	DigitConversionAdapter
Module parameter:	fromto=true iodstd=avaya.com od
Egress URI Parameters:	
Notes:	

Digit Conversion for Incoming Calls to SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

* Input Required

6.4. Administer SIP Entities

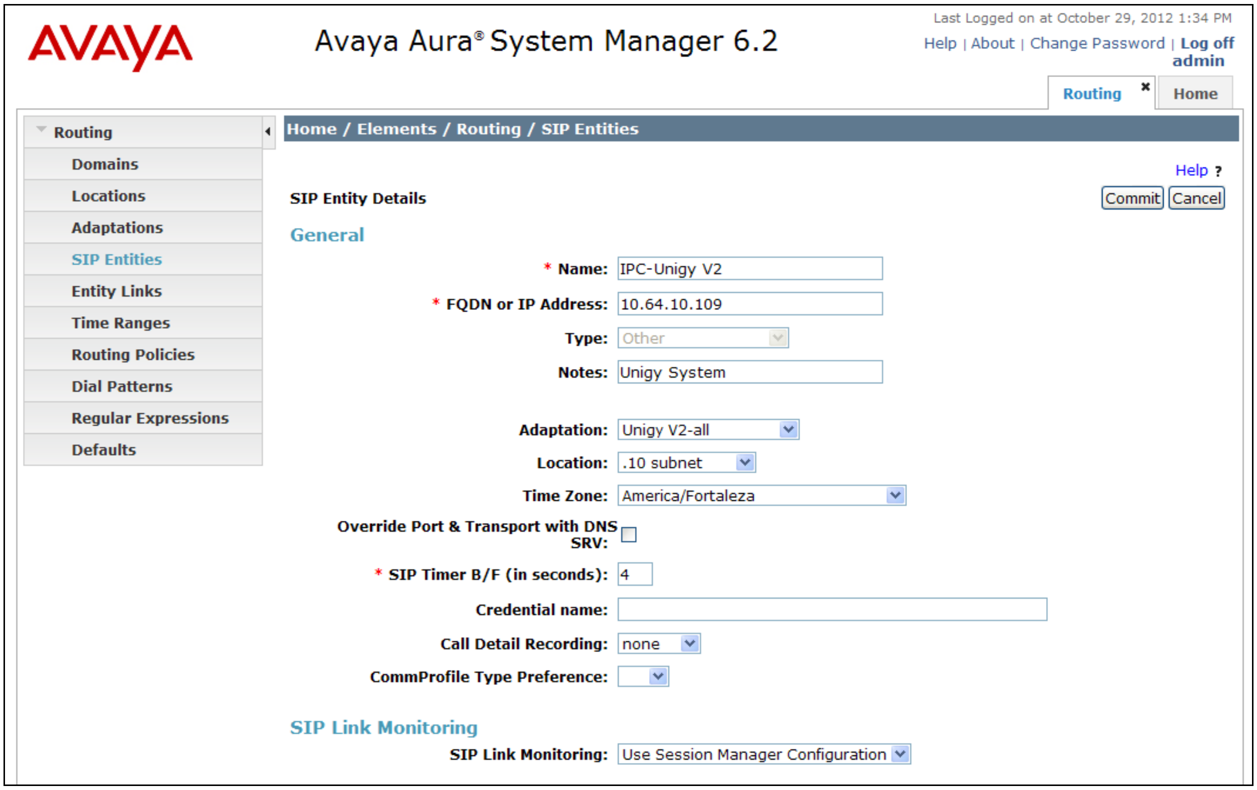
Add two new SIP entities, one for IPC, and another for the new SIP trunks for Communication Manager.

6.4.1. IPC SIP Entity

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for IPC.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

• **Name:**	A descriptive name.
• **FQDN or IP Address:**	The IP address of the IPC Media Manager server.
• **Type:**	"Other"
• **Adaptation:**	Select the IPC adaptation name from **Section 6.3**.
• **Location:**	Select the IPC location name from **Section 6.2**.
• **Time Zone:**	Select the applicable time zone.



SIP Entity Details

General

* Name: IPC-Unigy V2

* FQDN or IP Address: 10.64.10.109

Type: Other

Notes: Unigy System

Adaptation: Unigy V2-all

Location: .10 subnet

Time Zone: America/Fortaleza

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

SIP Link Monitoring

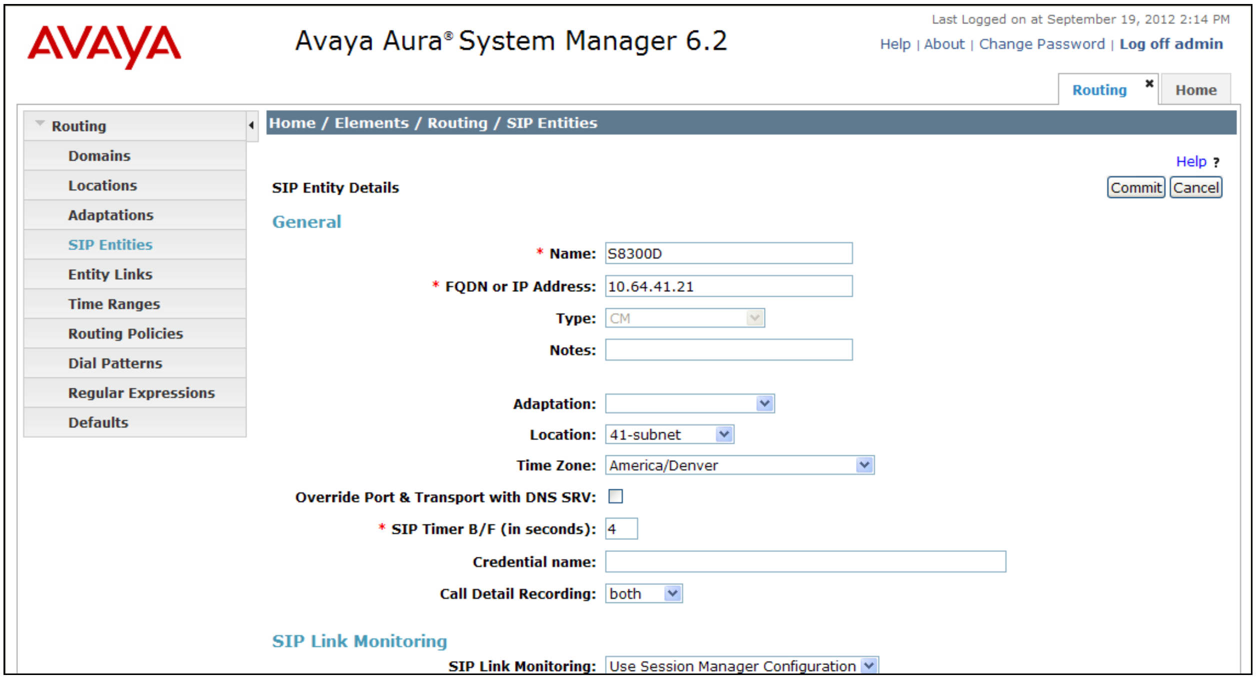
SIP Link Monitoring: Use Session Manager Configuration

6.4.2. Communication Manager SIP Entity

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with IPC.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or procr.
- **Type:** “CM”
- **Notes:** Any descriptive notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at September 19, 2012 2:14 PM
Help | About | Change Password | Log off admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / SIP Entities
Help ?
Commit
Cancel

SIP Entity Details

General

* Name:	S8300D
* FQDN or IP Address:	10.64.41.21
Type:	CM
Notes:	
Adaptation:	
Location:	41-subnet
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	both

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

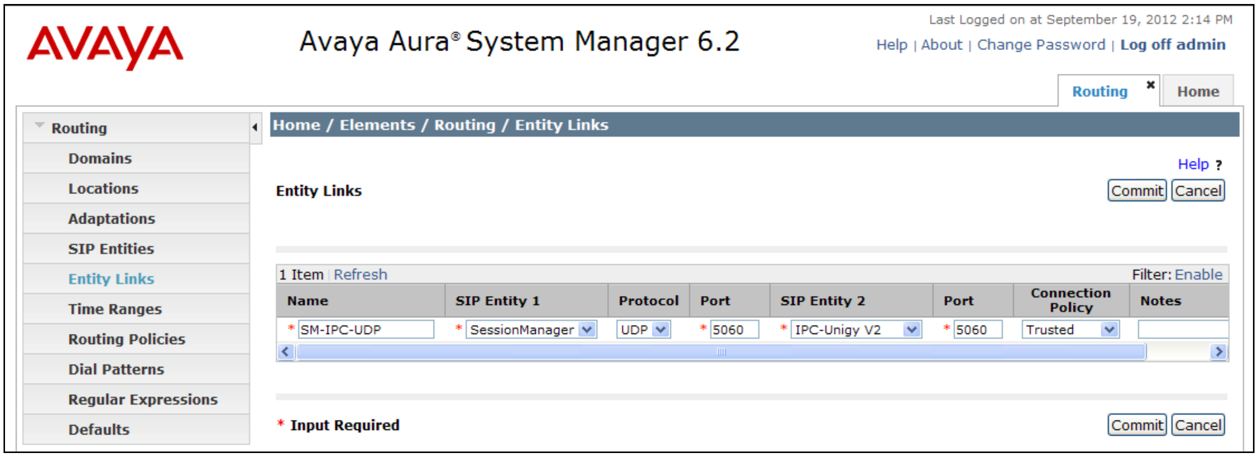
6.5. Administer Entity Links

Add three new entity links, two for IPC, and another for Communication Manager.

6.5.1. IPC Entity Links

Select **Routing → Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for IPC. The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "BR110-SM".
- **Protocol:** "UDP"
- **Port:** "5060"
- **SIP Entity 2:** The IPC entity name from **Section 6.4.1**.
- **Port:** "5060"
- **Trusted:** Retain the check.

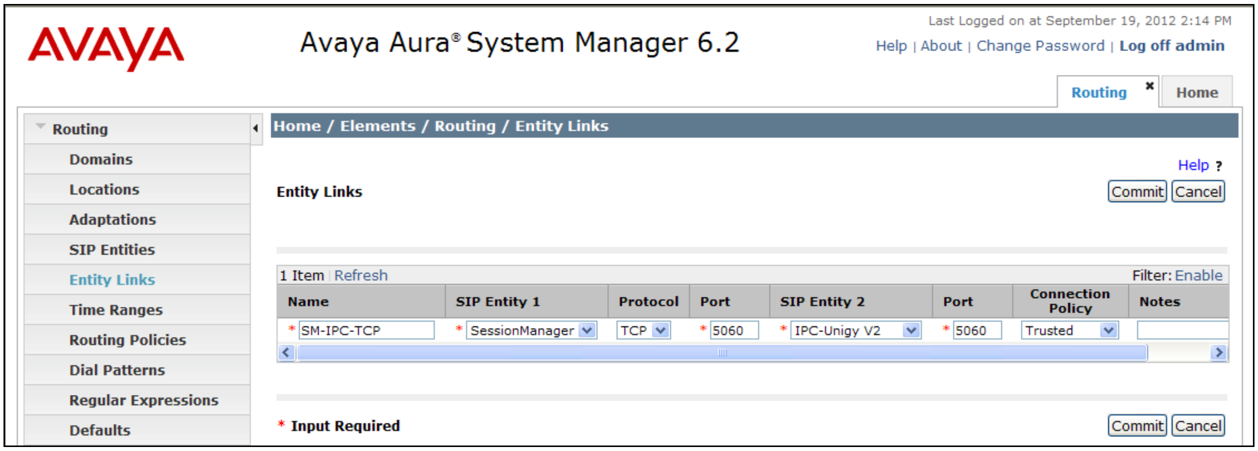


Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM-IPC-UDP	* SessionManager	UDP	* 5060	* IPC-Unigy V2	* 5060	Trusted	

* Input Required

Repeat and add another entity link for IPC with "TCP" as Protocol, as shown below.



Entity Links

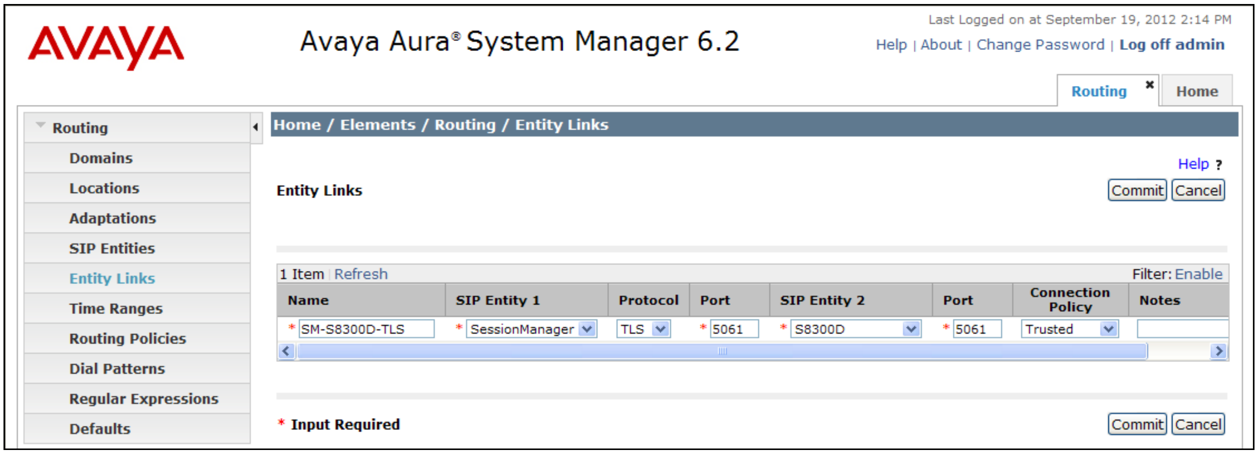
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM-IPC-TCP	* SessionManager	TCP	* 5060	* IPC-Unigy V2	* 5060	Trusted	

* Input Required

6.5.2. Communication Manager Entity Links

Select **Routing → Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for Communication Manager. The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "BR110-SM".
- **Protocol:** The signaling group transport method from **Section 0**.
- **Port:** The signaling group listen port number from **Section 0**.
- **SIP Entity 2:** The Communication Manager entity name from **Section 6.4.2**.
- **Port:** The signaling group listen port number from **Section 0**.
- **Trusted:** Retain the check.



Home / Elements / Routing / Entity Links

Entity Links

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM-S8300D-TLS	* SessionManager	TLS	* 5061	* S8300D	* 5061	Trusted	

* Input Required

6.6. Administer Routing Policies

Add two new routing policies, one for IPC, and another for Communication Manager.

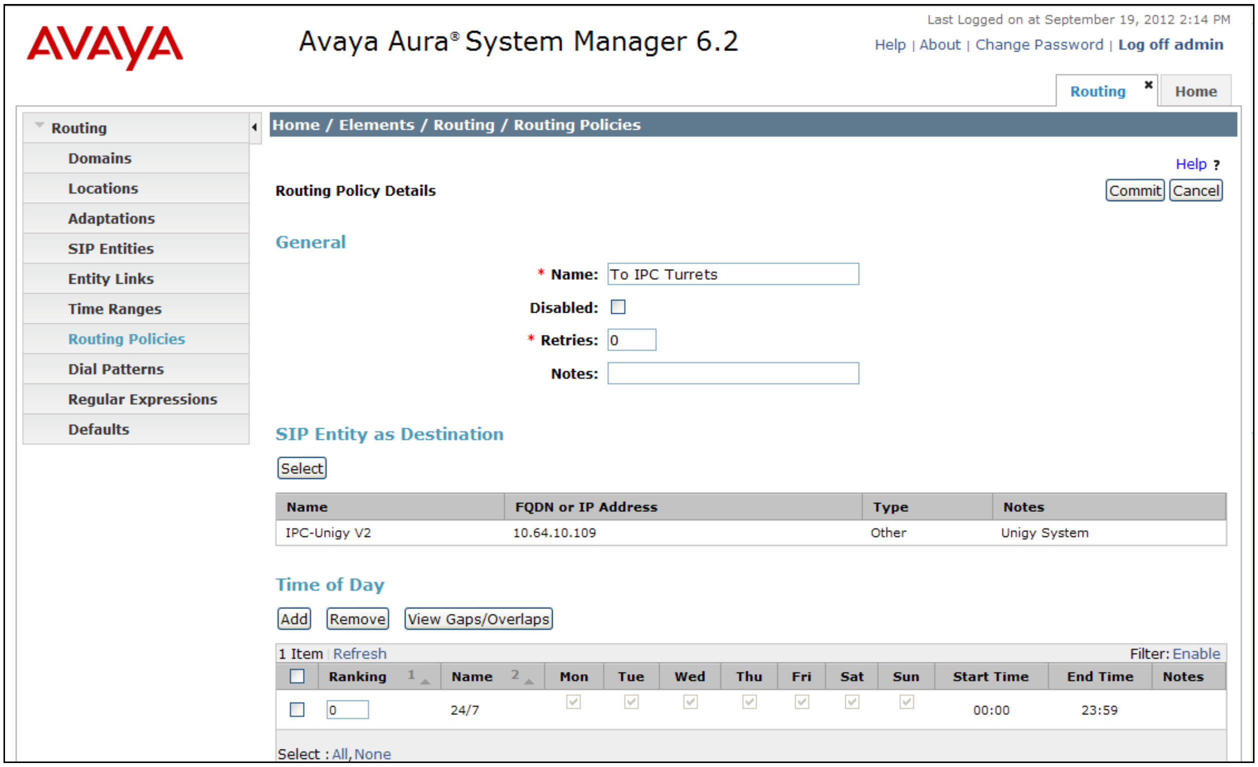
6.6.1. IPC Routing Policy

Select **Routing → Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for IPC.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**.

In the **SIP Entity as Destination** sub-section, click **Select** and select the IPC entity name from **Section 6.4.1** in the listing (not shown).

Retain the default values in the remaining fields.



Routing Policy Details

General

* Name: To IPC Turrets

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
IPC-Unigy V2	10.64.10.109	Other	Unigy System

Time of Day

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

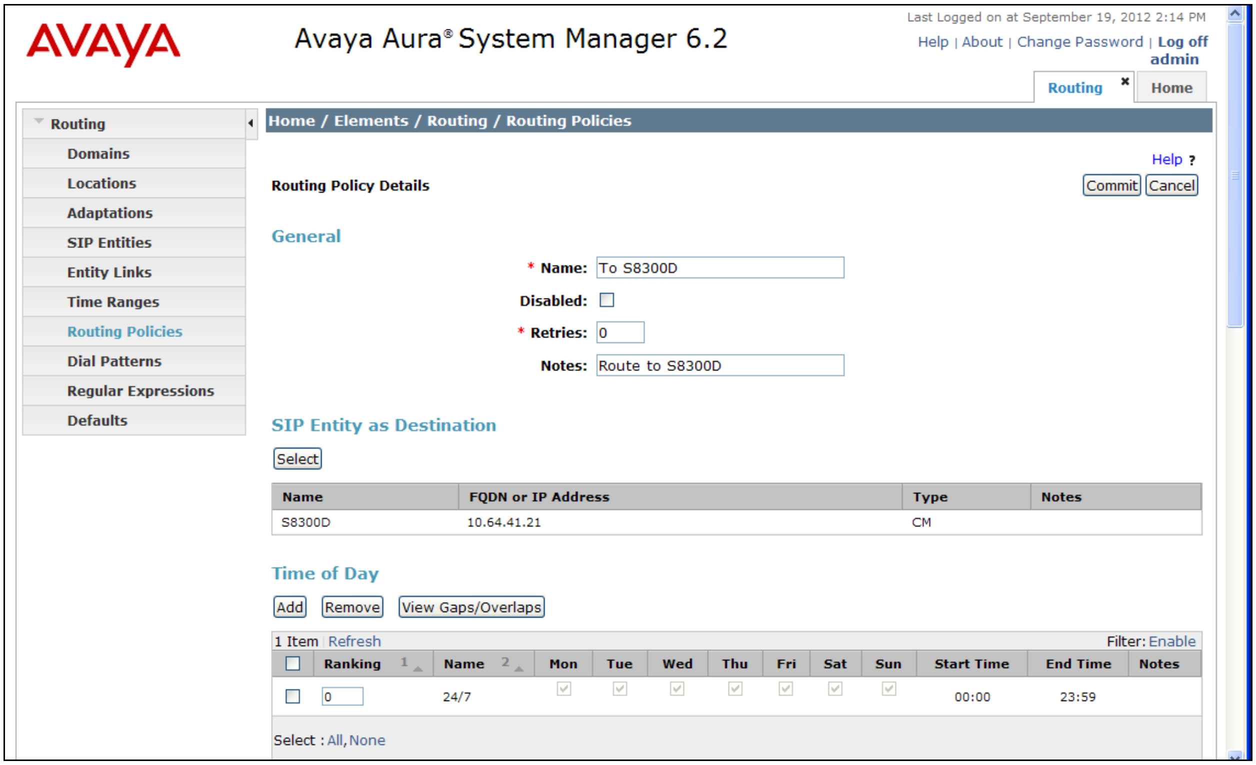
6.6.2. Communication Manager Routing Policy

Select **Routing → Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.4.2** in the listing (not shown).

Retain the default values in the remaining fields.



Routing Policy Details

General

* Name: To S8300D

Disabled: □

* Retries: 0

Notes: Route to S8300D

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
S8300D	10.64.41.21	CM	

Time of Day

1 Item

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

6.7. Administer Dial Patterns

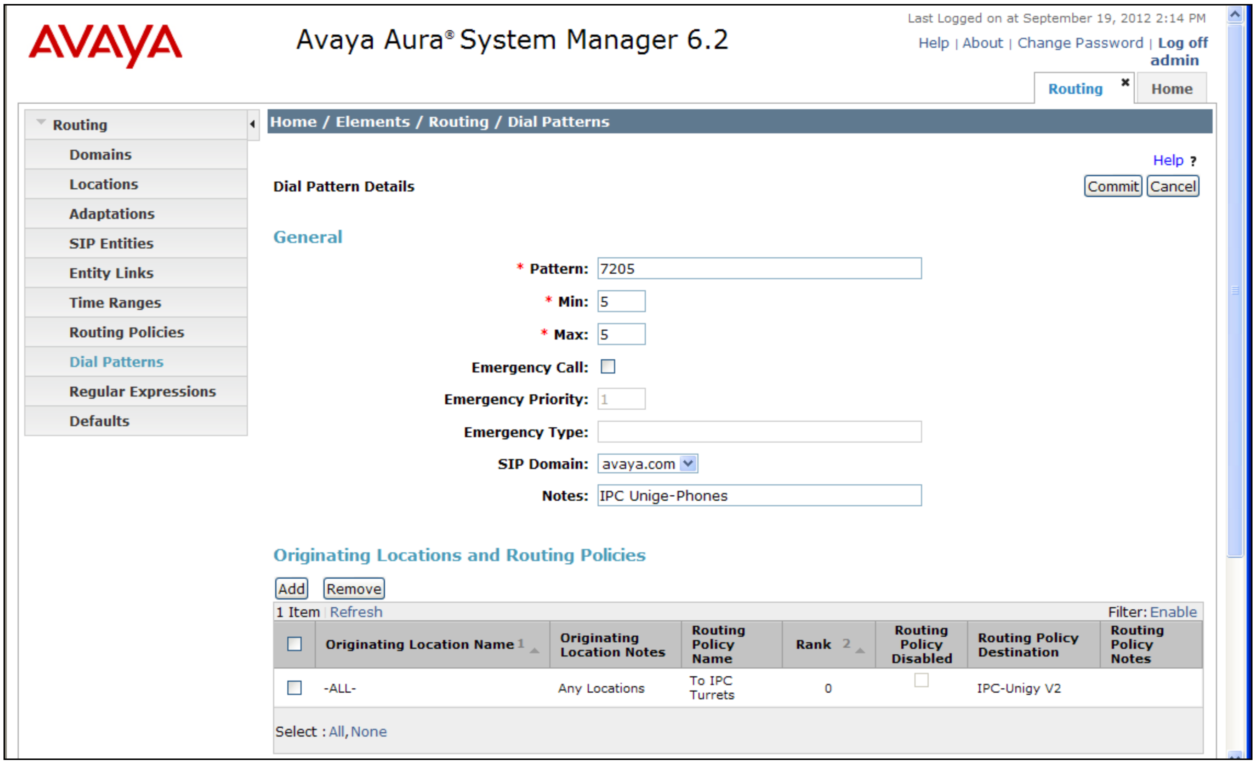
Add a new dial pattern for IPC, and update the existing dial pattern for Communication Manager.

6.7.1. IPC Dial Pattern

Select **Routing → Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach IPC turret users. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** The Communication Manager domain name from **Section 3**.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IPC turret users. In the compliance testing, the policy allowed for call origination from all locations, and the IPC routing policy from **Section 6.6.1** was selected as shown below.


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at September 19, 2012 2:14 PM
Help | About | Change Password | Log off admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / Dial Patterns
Help ?
Commit
Cancel

Dial Pattern Details

General

* Pattern:	7205
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	avaya.com
Notes:	IPC Unige-Phones

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

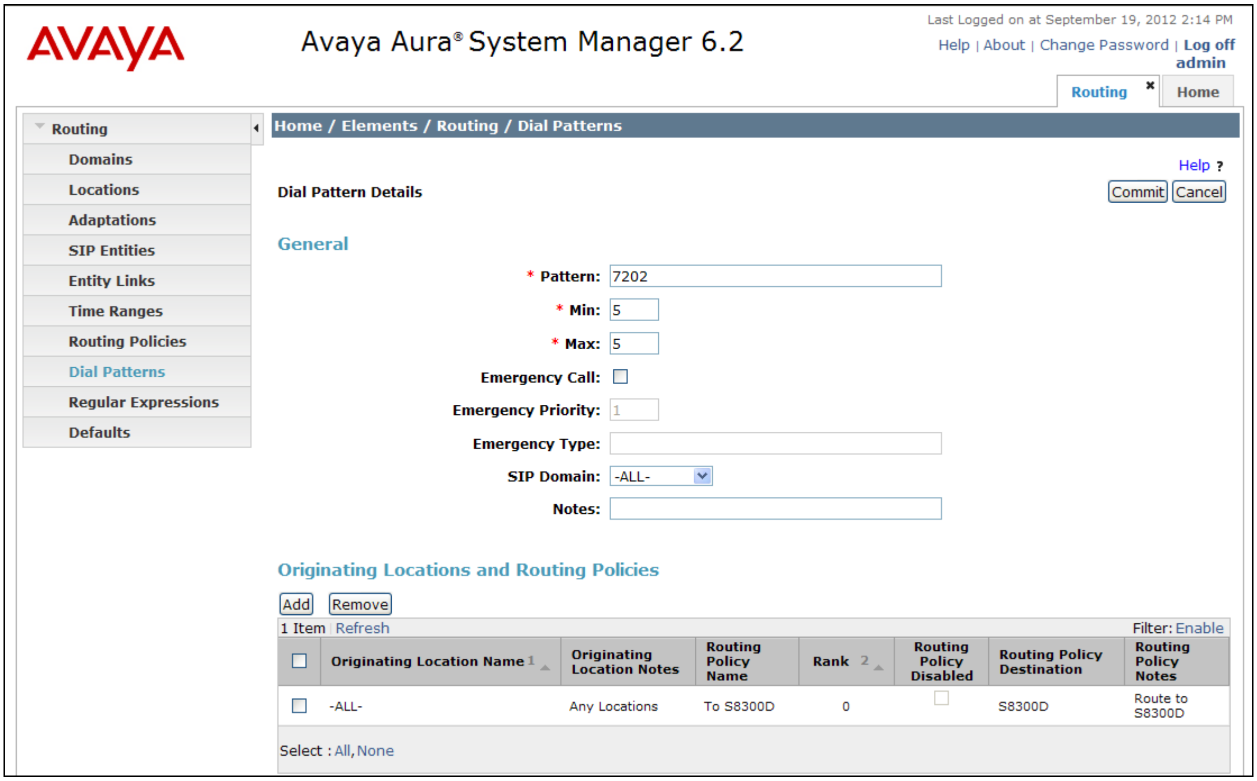
□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	To IPC Turrets	0	□	IPC-Unigy V2	

Select : All, None

6.7.2. Communication Manager Dial Pattern

Select **Routing → Dial Patterns** from the left pane, and click on the existing dial pattern for Communication Manager in the subsequent screen, in this case dial pattern “7202” (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy as necessary for calls from IPC turret users. In the compliance testing, the policy allowed for call origination from the IPC location from **Section 6.2**, and the Communication Manager routing policy from **Section 6.6.2** was selected as shown below. Retain the default values in the remaining fields.



Dial Pattern Details

General

* Pattern: 7202

* Min: 5

* Max: 5

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	To S8300D	0	□	S8300D	Route to S8300D

7. Configure IPC Converged Communication Manager

This section provides the procedures for configuring IPC Converged Communication 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

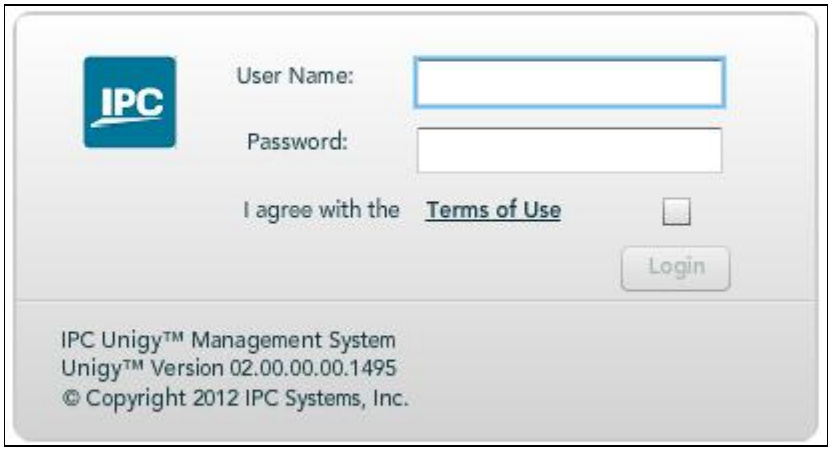
The configuration of Media Manager and/or Converged Communication Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy 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**.

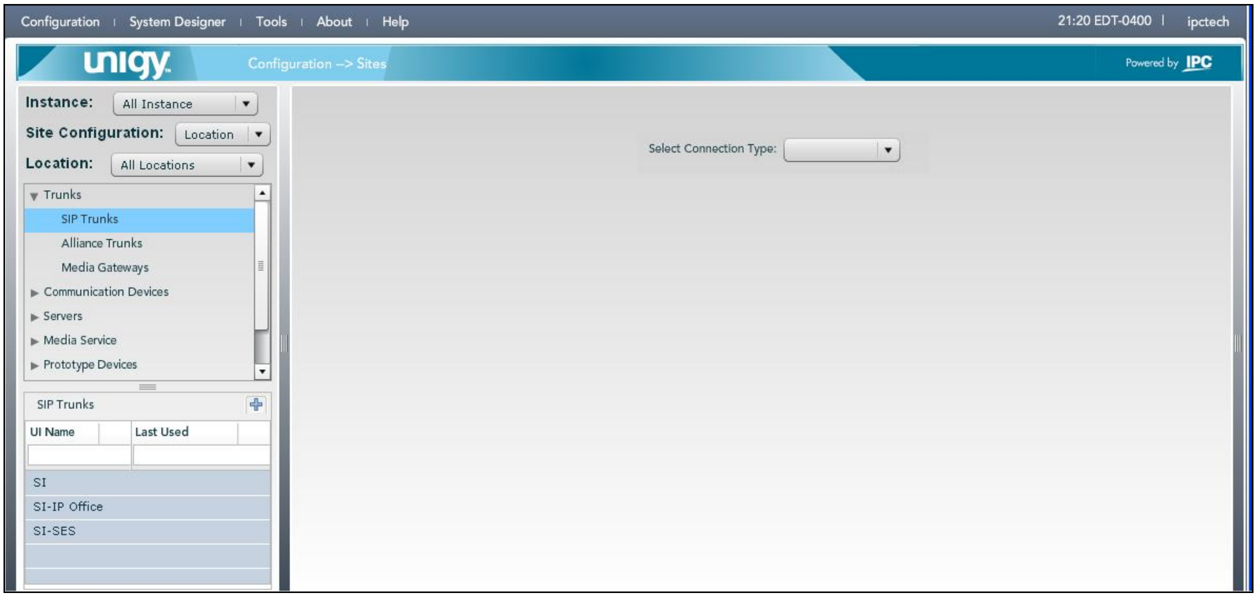
In the subsequent screen (not shown), click **Continue**.



IPC Unigy™ Management System
Unigy™ Version 02.00.00.00.1495
© Copyright 2012 IPC Systems, Inc.

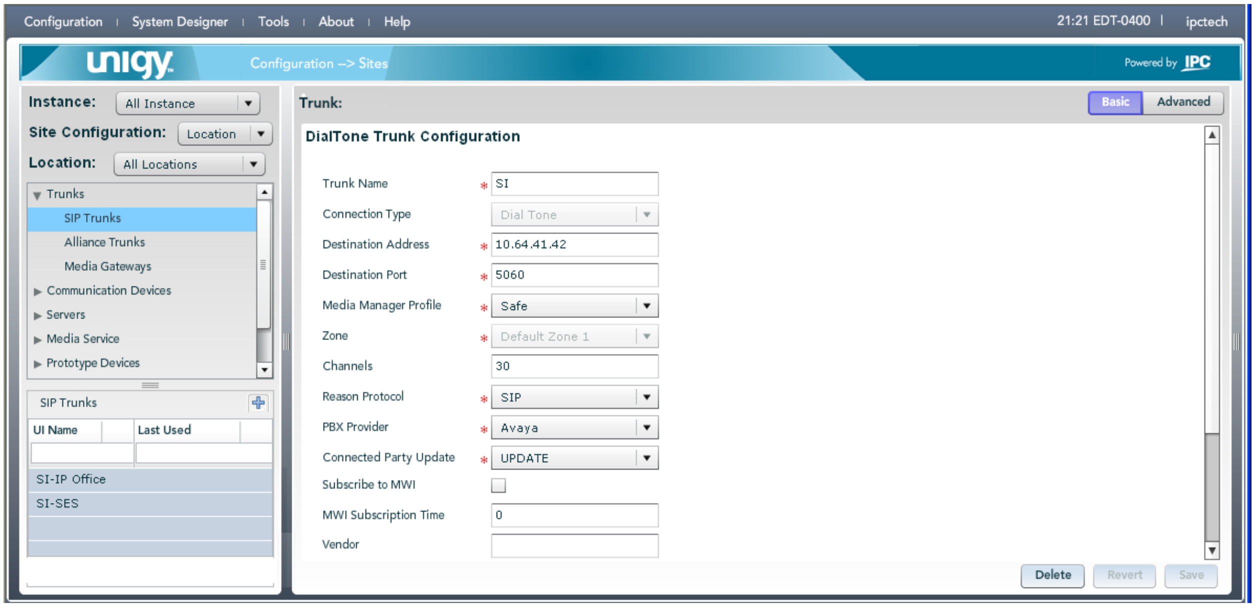
7.2. Administer SIP Trunks

Select **Trunks → SIP Trunks** in the left pane, and click the **Add** icon (✚) in the lower left pane to add a new SIP trunk. 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 the Session Manager signaling interface.
- **Destination Port:** The port number from **Section 6.5.1**.
- **Zone:** An available zone, in this case “Default Zone 1”.
- **Channels:** The number of SIP trunk group members from **Section 0**.
- **Reason Protocol** “SIP”
- **PBX Provider:** “Avaya”
- **Connected Party Update:** “UPDATE”



Instance: All Instance

Site Configuration: Location

Location: All Locations

SIP Trunks

UI Name	Last Used
SI-IP Office	
SI-SES	

Trunk:

DialTone Trunk Configuration

Trunk Name * SI

Connection Type Dial Tone

Destination Address * 10.64.41.42

Destination Port * 5060

Media Manager Profile * Safe

Zone * Default Zone 1

Channels 30

Reason Protocol * SIP

PBX Provider * Avaya

Connected Party Update * UPDATE

Subscribe to MWI □

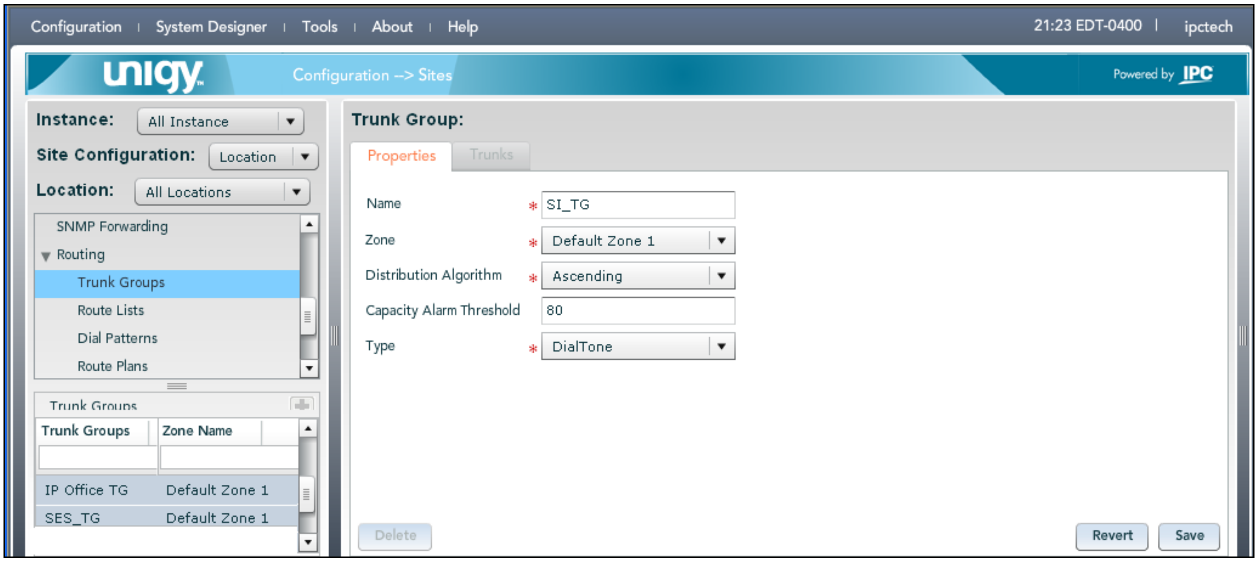
MWI Subscription Time 0

Vendor

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**, select "Default Zone 1" for the **Zone** field, select "Ascending" for the **Distribution Algorithm** field, and click **Save**. Select the **Trunks** tab in the right pane.



Instance: All Instance

Site Configuration: Location

Location: All Locations

Trunk Groups	Zone Name
IP Office TG	Default Zone 1
SES_TG	Default Zone 1

Trunk Group:

Name * SI_TG

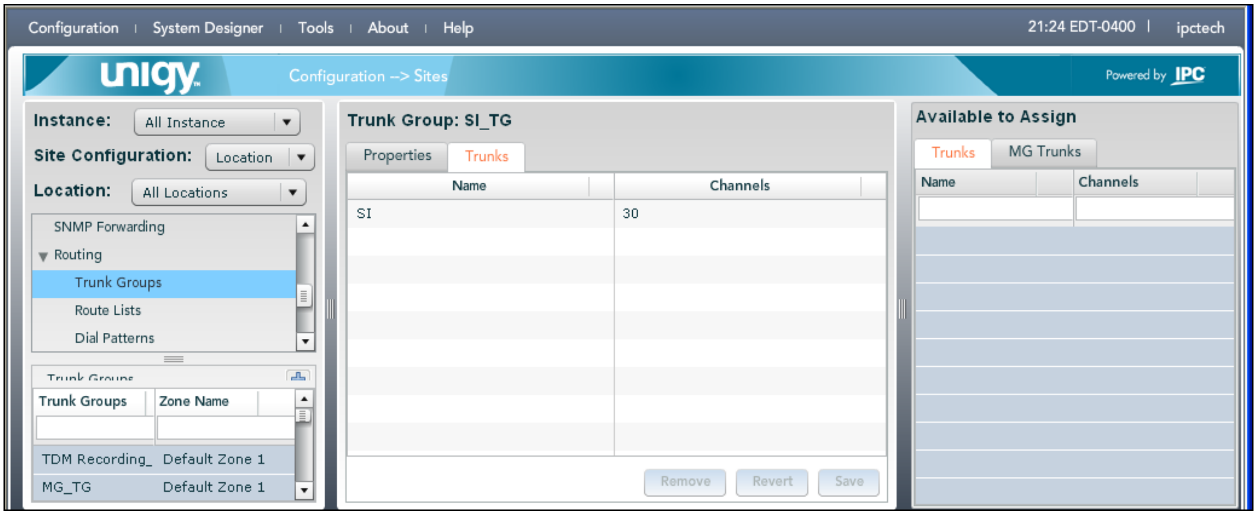
Zone * Default Zone 1

Distribution Algorithm * Ascending

Capacity Alarm Threshold 80

Type * DialTone

The screen is updated with three panes. In the rightmost pane, select the **Trunks** tab to display a list of trunks. Select the SIP trunk from **Section 7.2** in the rightmost pane and drag to the middle pane as shown below. Click **Save**.



Instance: All Instance

Site Configuration: Location

Location: All Locations

Trunk Groups	Zone Name
TDM Recording_	Default Zone 1
MG_TG	Default Zone 1

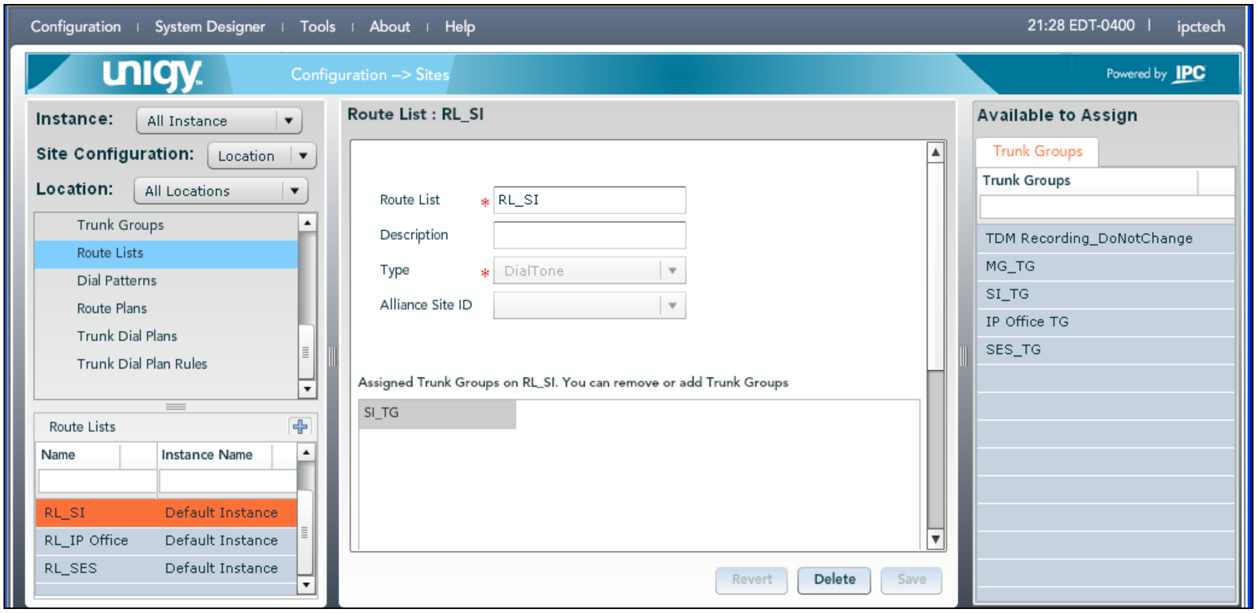
Trunk Group: SI_TG

Name	Channels
SI	30

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**.



Instance: All Instance

Site Configuration: Location

Location: All Locations

Route Lists

Name	Instance Name
RL_SI	Default Instance
RL_IP Office	Default Instance
RL_SES	Default Instance

Route List : RL_SI

Route List * RL_SI

Description

Type * DialTone

Alliance Site ID

Assigned Trunk Groups on RL_SI. You can remove or add Trunk Groups

SI_TG

Available to Assign

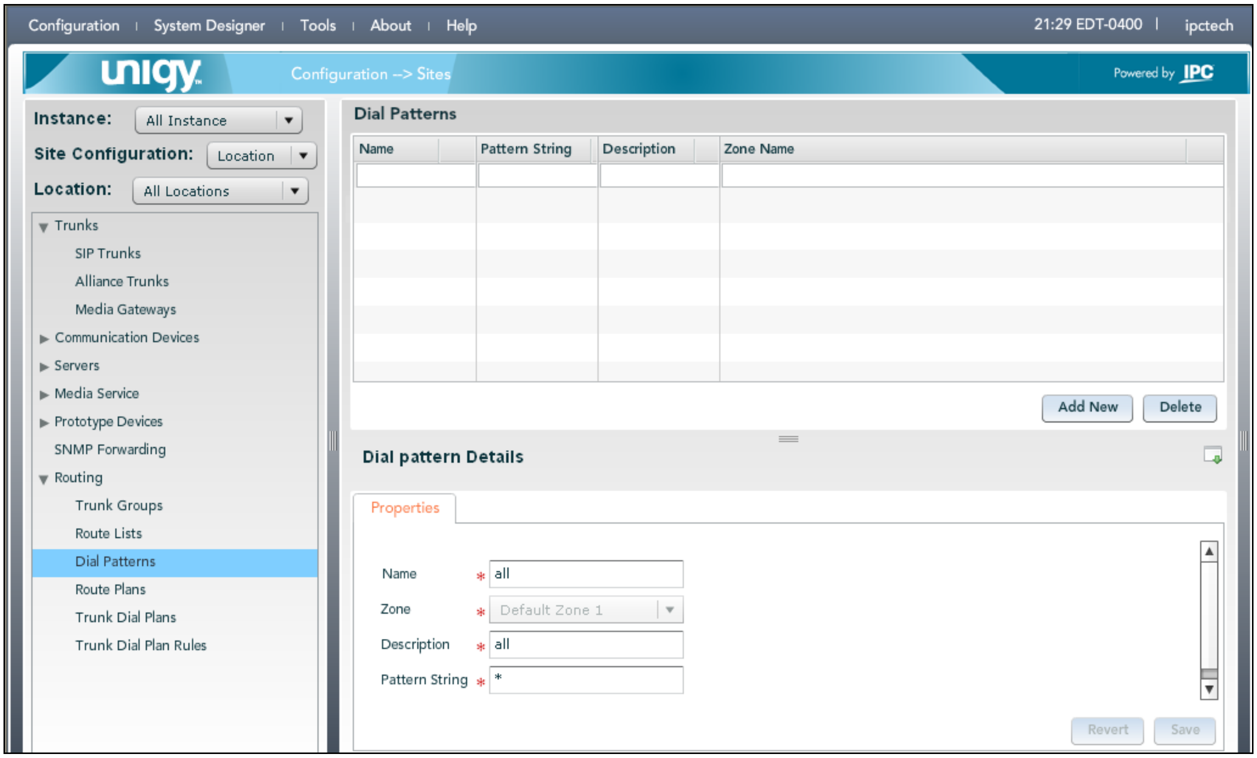
Trunk Groups

Trunk Groups
TDM Recording_DoNotChange
MG_TG
SI_TG
IP Office TG
SES_TG

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 "*" meaning any digits will be sent to Session Manager. Click **Save**.



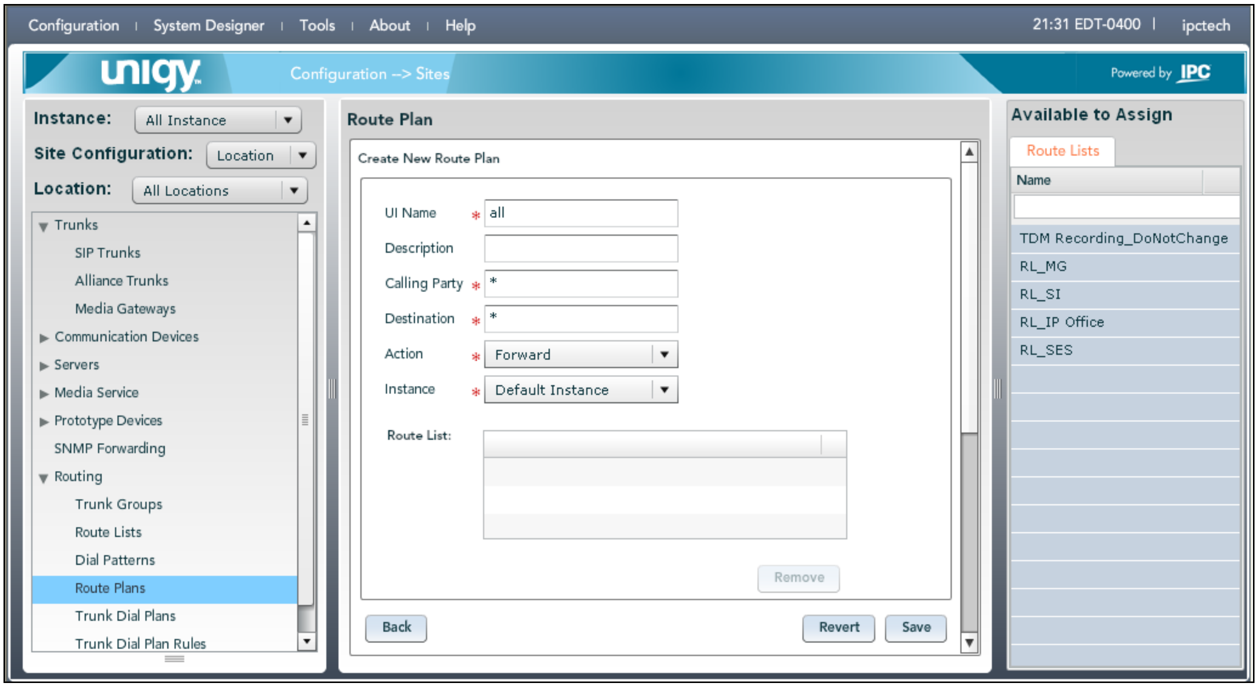
Name	*	all
Zone	*	Default Zone 1
Description	*	all
Pattern String	*	*

Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Avaya Aura® Communication Manager.

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 **Called Party**, select the dial pattern for Avaya endpoints from **Section 7.5**. Select "Forward" for **Action**, and click **Save**.



Instance: All Instance
Site Configuration: Location
Location: All Locations

Route Plan

Create New Route Plan

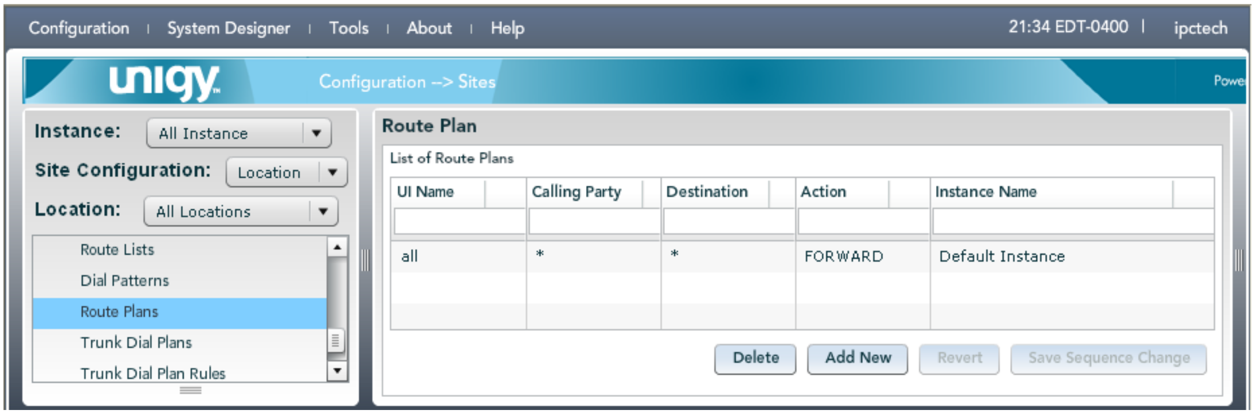
UI Name * all
Description
Calling Party * *
Destination * *
Action * Forward
Instance * Default Instance
Route List:

Available to Assign

Route Lists

Name
TDM Recording_DoNotChange
RL_MG
RL_SI
RL_IP Office
RL_SES

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).



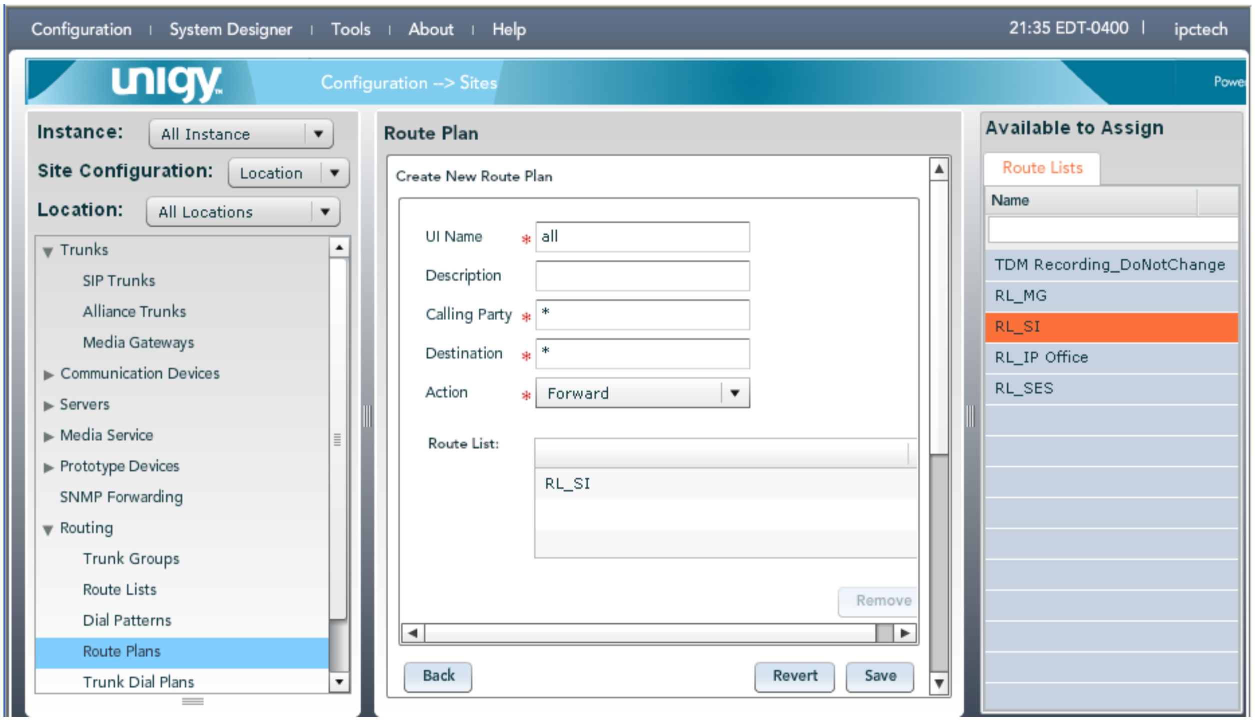
Instance: All Instance
Site Configuration: Location
Location: All Locations

Route Plan

List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
all	*	*	FORWARD	Default Instance

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**.



Instance: All Instance
Site Configuration: Location
Location: All Locations

UI Name * all
Description
Calling Party * *
Destination * *
Action * Forward
Route List: RL_SI

Name
TDM Recording_DoNotChange
RL_MG
RL_SI
RL_IP Office
RL_SES

8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, 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 0**. Verify that all trunks are in the “in-service/idle” state as shown below.

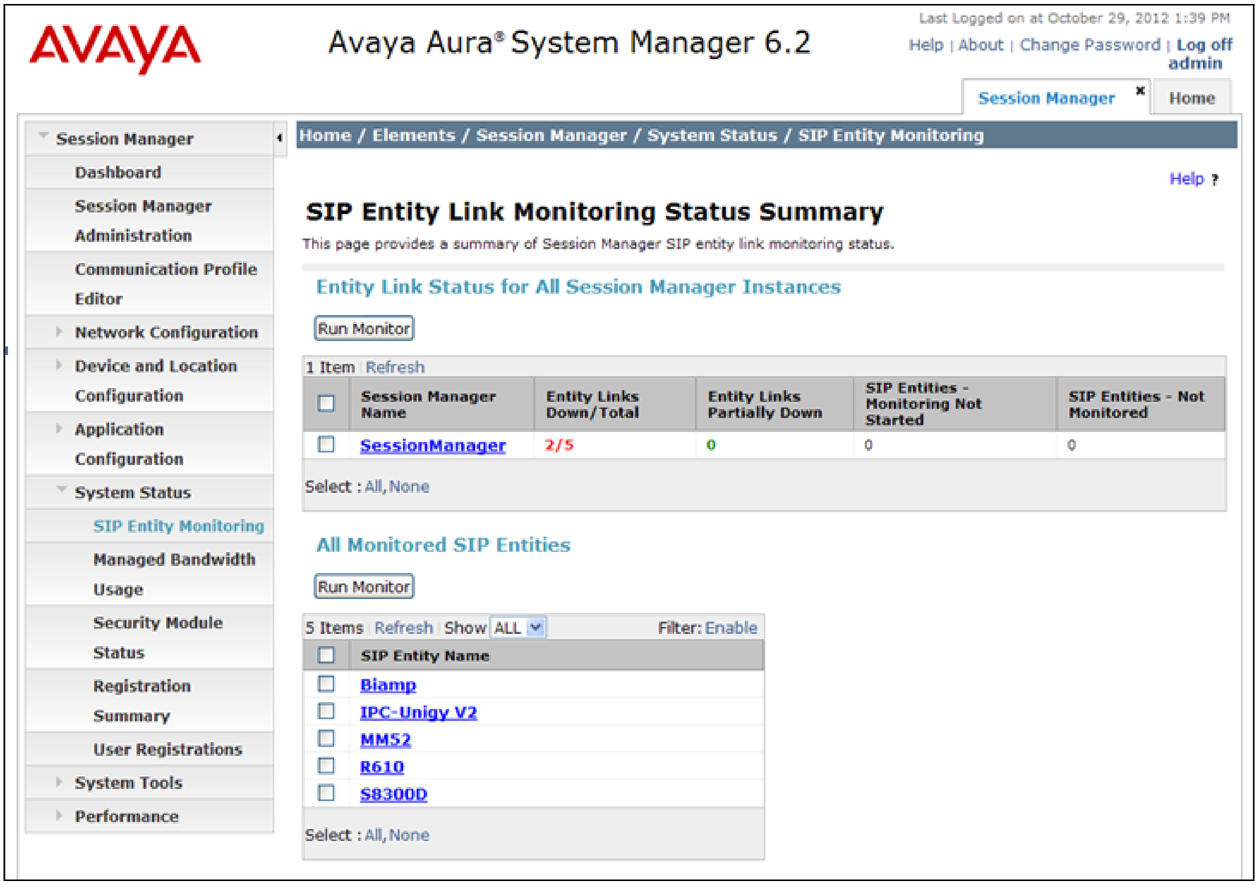
```
status trunk 92

                            TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0092/001 T00135   in-service/idle    no
0092/002 T00136   in-service/idle    no
0092/003 T00137   in-service/idle    no
0092/004 T00138   in-service/idle    no
0092/005 T00139   in-service/idle    no
0092/006 T00140   in-service/idle    no
0092/007 T00141   in-service/idle    no
0092/008 T00142   in-service/idle    no
0092/009 T00143   in-service/idle    no
0092/010 T00144   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 0**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 92
                        STATUS SIGNALING GROUP

        Group ID: 92
      Group Type: sip

     Group State: in-service
```

8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements → Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the IPC entity name from **Section 6.4.1**.


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at October 29, 2012 1:39 PM
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
Registration Summary
User Registrations
System Tools
Performance
Home / Elements / Session Manager / System Status / SIP Entity Monitoring
Help ?

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Run Monitor

1 Item | Refresh

□	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
□	SessionManager	2/5	0	0	0

Select : All, None

All Monitored SIP Entities

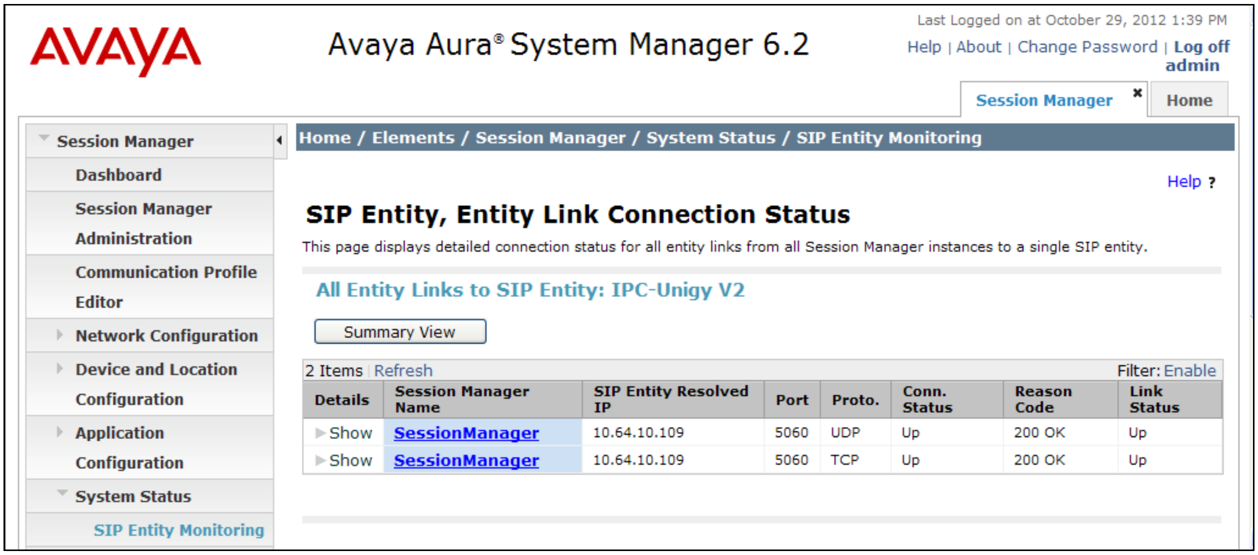
Run Monitor

5 Items | Refresh | Show ALL | Filter: Enable

□	SIP Entity Name
□	Biamp
□	IPC-Unigy V2
□	MM52
□	R610
□	S8300D

Select : All, None

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are "Up", as shown below.



AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at October 29, 2012 1:39 PM
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Home / Elements / Session Manager / System Status / SIP Entity Monitoring
Help ?
Summary View
2 Items | Refresh
Filter: Enable

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: IPC-Unigy V2

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	SessionManager	10.64.10.109	5060	UDP	Up	200 OK	Up
▶ Show	SessionManager	10.64.10.109	5060	TCP	Up	200 OK	Up

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 6.2→→ using Avaya Aura® Session Manager.   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. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 7.0, Release 6.2, July 2012, available at http://support.avaya.com.

2. *Administering Avaya Aura® Session Manager*, Document Number 03-603324, Release 6.2, July2012, 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.