



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for IPC Unigy with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Manager 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 6.0.1 and Avaya Aura® Session Manager using SIP trunks.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy 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 Unigy to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Session Manager.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy 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.

## 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 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 the 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.
- For blind transfer scenarios involving IPC turrets as the called party and Avaya SIP or PSTN as the calling and forward-to parties, there is no talk path for the resultant call with IPC returning 500 Internal Error. The workaround is to use attended transfer instead.
- Even when IPC Unigy is configured with UDP, the TCP protocol must be configured to be allowed on Avaya Session Manager as Unigy switches over to use TCP for diversions.

## 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](mailto:systems.support@ipc.com)

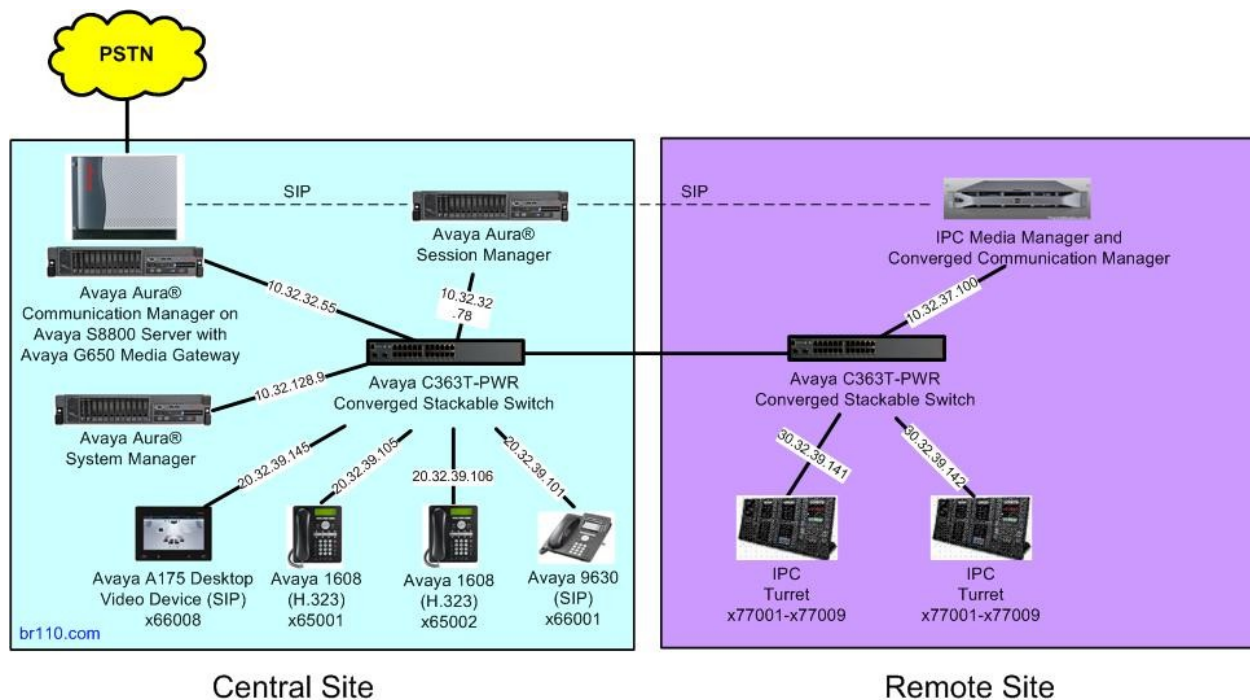
### 3. Reference Configuration

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® 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 (6xxxx), and IPC turret users at the Remote site (77xxx).

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.



## 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 S8800 Server	6.0.1 SP2 with special patch 18993 (R016x.00.1.510.1-18993)
Avaya G650 Media Gateway <ul style="list-style-type: none"><li>TN799DP C-LAN Circuit Pack</li><li>TN2302AP IP Media Processor</li><li>TN464HP DS1 Interface</li></ul>	HW01 FW038 HW20 FW122 HW02 FW024
Avaya Aura® Session Manager	6.1 SP2
Avaya Aura® System Manager	6.1 SP2
Avaya 1608 IP Telephone (H.323)	1.3
Avaya 9630 IP Telephone (SIP)	2.6.4
Avaya A175 Desktop Video Device (SIP)	1.0.2
IPC Unigy <ul style="list-style-type: none"><li>Media Manager</li><li>Converged Communication Manage</li><li>Turrets</li></ul>	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 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:		12000	6	
Maximum Concurrently Registered IP Stations:		18000	0	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		414	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		18000	1	
Maximum Video Capable IP Softphones:		18000	0	
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>10</b>	
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	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? 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 “add trunk-group n” command, where “n” is an available trunk group number, in this case “77”. 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 77		Page 1 of 21	
TRUNK GROUP			
Group Number: 77	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: IPC Unigy</b>	COR: 1	TN: 1	<b>TAC: 1077</b>
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group:	
		Number of Members: 0	

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

add trunk-group 77		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
<b>Numbering Format: private</b>			
		UUI Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	

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

change trunk-group 77		Page 4 of 21	
PROTOCOL VARIATIONS			
Mark Users as Phone? n			
Prepend '+' to Calling Number? n			
Send Transferring Party Information? n			
Network Call Redirection? n			
Send Diversion Header? n			
Support Request History? y			
<b>Telephone Event Payload Type: 101</b>			



## 5.4. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “77”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tcp”
- **Near-end Node Name:** An existing C-LAN node name.
- **Far-end Node Name:** The existing Session Manager node name.
- **Near-end Listen Port:** An available port for integration with IPC Unigy.
- **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 Unigy.

For **Far-end Domain**, leave the field blank since IPC Unigy does not support domain name. For **Direct IP-IP Audio Connections**, enter “n” since IPC Unigy does not support shuffling.

add signaling-group 77		Page 1 of 1
SIGNALING GROUP		
Group Number: 77	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y Peer Server: Others		
Near-end Node Name: Clan-1	Far-end Node Name: S8800-SM-SIG	
Near-end Listen Port: 5077	Far-end Listen Port: 5077	
Far-end Network Region: 7		
Far-end Secondary Node Name:		
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? n	
Enable Layer 3 Test? y	IP Audio Hairpinning? 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. 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 Unigy.

```
change ip-network-region 7                                     Page 1 of 20
                                                                IP NETWORK REGION
  Region: 7
Location: 1      Authoritative Domain:
  Name: IPC Unigy
MEDIA PARAMETERS                                     Intra-region IP-IP Direct Audio: no
  Codec Set: 7                                       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
```

Navigate to **Page 4**, and specify this codec set to be used for calls with the network region used by the Avaya endpoints. In the compliance testing, all Avaya endpoints are on network region “1”.

```
change ip-network-region 7                                     Page 4 of 20

Source Region: 7      Inter Network Region Connection Management      I      M
                                                                G  A  t
dst codec direct  WAN-BW-limits  Video      Intervening      Dyn  A  G  c
rgn  set  WAN  Units      Total Norm  Prio Shr Regions      CAC  R  L  e
1    7    y    NoLimit
2
3
4
5
6
7    7
8                                     all
```

## 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 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.

change ip-codec-set 7					Page	1 of	2
IP Codec Set							
Codec Set: 7							
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 an existing route pattern number to be used to reach IPC, in this case “77”. 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 5.3**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 77											Page	1 of 3	
Pattern Number: 77    Pattern Name: IPC Unigy													
SCCAN? n    Secure SIP? n													
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC
No			Mrk	Lmt	List	Del	Digits					QSIG	
											Intw		
1:	77	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 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 5.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 6 and routed to trunk group 77 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 Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	6	77		5	Total Administered: 2 Maximum Entries: 540

## 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 Pattern	Len	Del	Insert Digits	Node 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 “77” from **Section 5.7**.

change aar analysis 0					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					Percent Full: 2
Location: all					
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num ANI Req'd
77	5	5	77	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 “10”.

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 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		UII 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 UII IE? y		<b>Modify Tandem Calling Number: tandem-cpn-form</b>			
Send UCID? n					
Send Codeset 6/7 LAI IE? y		Dsl 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			
DSN Term? 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”.

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	6	10		90884	pub-unk		
<b>5</b>	<b>7</b>	<b>10</b>		<b>90884</b>	<b>pub-unk</b>		

## 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.

The screenshot shows the Avaya Aura® System Manager 6.1 login interface. At the top, the Avaya logo is on the left and the title 'Avaya Aura® System Manager 6.1' is on the right. Below the title bar is a red navigation bar with 'Home / Log On'. The main heading is 'Log On'. On the left, a box contains text: 'Recommended access to System Manager is via FQDN.' followed by a link 'Go to central login for Single Sign-On'. Below this, it says 'If IP address access is your only option, then note that authentication will fail in the following cases:' followed by a bulleted list: 'First time login with "admin" account' and 'Expired/Reset passwords'. On the right, there are input fields for 'User ID:' and 'Password:'. At the bottom right are 'Log On' and 'Cancel' buttons, and a link 'Change Password' at the very bottom right.

**AVAYA** Avaya Aura® System Manager 6.1

Home / Log On

**Log On**

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

User ID:

Password:

[Change Password](#)

## 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 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home /Elements / Routing- Introduction to Network Routing Policy 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:

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.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home /Elements / Routing / Locations- Location Details Help ?

**Location Details** Commit Cancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

**General**

\* Name: IPC-Unigy-Loc

Notes: IPC Unigy

**Overall Managed Bandwidth**

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

**Per-Call Bandwidth Parameters**

\* Default Audio Bandwidth: 80 Kbit/sec

**Location Pattern**

Add Remove

1 Item | Refresh Filter: Enable

	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.37.100	

### 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 “osrcd=br110.com odstcd=br110.com iosrcd=br110.com iodstd=br110.com”, where “br110.com” is the applicable domain. This will set the source and destination domains for all incoming and outgoing calls for IPC.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

General

\* Adaptation name: IPC-Unigy-Adaptation

Module name: DigitConversionAdapter

Module parameter: osrcd=br110.com odstcd=br110.com iosrcd=br110.com iodstd=br110.com

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-------



## 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.

**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) \* [Home](#)

▼ Routing ◀ Home /Elements / Routing / SIP Entities- SIP Entity Details

Domains  
Locations  
Adaptations  
**SIP Entities**  
Entity Links  
Time Ranges  
Routing Policies  
Dial Patterns  
Regular Expressions  
Defaults

**SIP Entity Details** [Help ?](#)  
[Commit](#) [Cancel](#)

**General**

\* **Name:** IPC-Unigy

\* **FQDN or IP Address:** 10.32.37.100

**Type:** Other ▼

**Notes:**

**Adaptation:** IPC-Unigy-Adaptation ▼

**Location:** IPC-Unigy-Loc ▼

**Time Zone:** America/New\_York ▼

**Override Port & Transport with DNS SRV:** ☐

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

**Credential name:**

**Call Detail Recording:** none ▼

**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.
- **Type:** “CM”
- **Notes:** Any descriptive notes.
- **Adaptation:** Select the applicable adaptation for Communication Manager.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) \* [Home](#)

Home / Elements / Routing / SIP Entities- SIP Entity Details

**SIP Entity Details** [Help ?](#)

[Commit](#) [Cancel](#)

**General**

\* **Name:** BR110-CM-5077

\* **FQDN or IP Address:** 10.32.32.12

**Type:** CM

**Notes:** CM port 5077 for IPC Unigy

**Adaptation:** BR110-CM-Adaptation

**Location:** BR-1C110

**Time Zone:** America/New\_York

**Override Port & Transport with DNS** ☐

**SRV:**

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

**Credential name:**

**Call Detail Recording:** none

**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.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane has 'Entity Links' selected under the 'Routing' section. The main area displays the 'Entity Links' screen with a table containing one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The values in the table are: Name: \* BR110-SM\_IPC-Unig, SIP Entity 1: \* BR110-SM, Protocol: UDP, Port: \* 5060, SIP Entity 2: \* IPC-Unigy, Port: \* 5060, and Trusted: ☒.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* BR110-SM_IPC-Unig	* BR110-SM	UDP	* 5060	* IPC-Unigy	* 5060	<input checked="" type="checkbox"/>

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

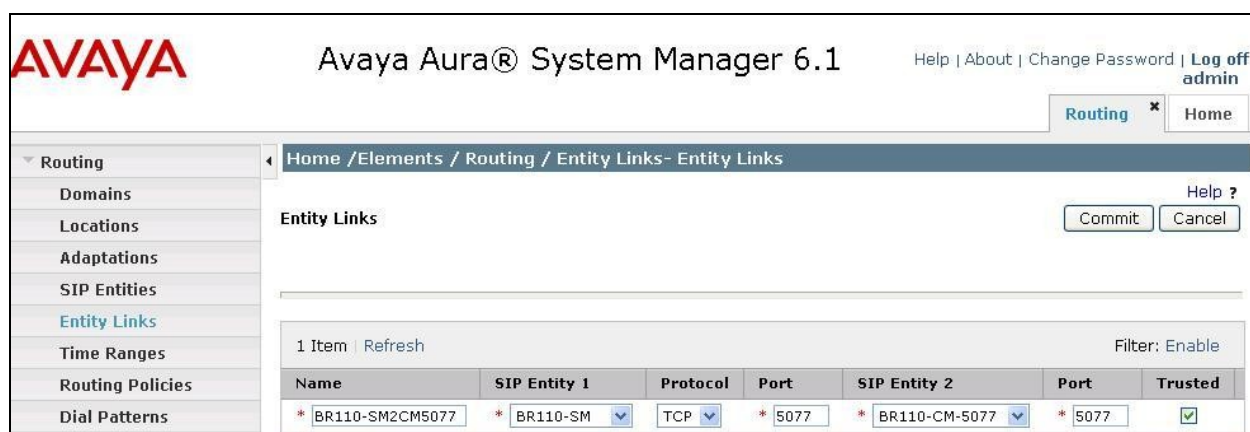
The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane has 'Entity Links' selected under the 'Routing' section. The main area displays the 'Entity Links' screen with a table containing two items. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The values in the table are: Name: \* BR110-SM\_IPC-Unig, SIP Entity 1: \* BR110-SM, Protocol: TCP, Port: \* 5060, SIP Entity 2: \* IPC-Unigy, Port: \* 5060, and Trusted: ☒.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* BR110-SM_IPC-Unig	* BR110-SM	TCP	* 5060	* IPC-Unigy	* 5060	<input checked="" type="checkbox"/>

## 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 5.4**.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **SIP Entity 2:** The Communication Manager entity name from **Section 6.4.2**.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **Trusted:** Retain the check.



The screenshot displays the Avaya Aura System Manager 6.1 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Entity Links' selected. The main content area is titled 'Entity Links' and contains a table with one configuration item. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The configuration shown is for a link between BR110-SM2CM5077 and BR110-SM, using TCP protocol on port 5077, linked to BR110-CM-5077 on port 5077, and is marked as trusted.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* BR110-SM2CM5077	* BR110-SM	TCP	* 5077	* BR110-CM-5077	* 5077	<input checked="" type="checkbox"/>

## 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.

**AVAYA** Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Routing Policies - Routing Policy Details

**Routing Policy Details** Help ?

Commit Cancel

**General**

\* Name: To-IPC-Unigy

Disabled: ☐

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
IPC-Unigy	10.32.37.100	Other	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

## 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.

**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) \* [Home](#)

Home / Elements / Routing / Routing Policies - Routing Policy Details

**Routing Policy Details** [Help ?](#)

[Commit](#) [Cancel](#)

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

[Select](#)

Name	FQDN or IP Address	Type	Notes
BR110-CM-5077	10.32.32.12	CM	CM port 5077 for IPC Unigy

**Time of Day**

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

## 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 select as shown below.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for Help, About, Change Password, and Log off admin. A breadcrumb trail shows the path: Home / Elements / Routing / Dial Patterns - Dial Pattern Details. The left sidebar contains a tree view with the following items: Routing (selected), Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled "Dial Pattern Details" and includes a "General" sub-section. The fields in the General section are: Pattern (77), Min (5), Max (5), Emergency Call (unchecked), SIP Domain (br110.com), and Notes (IPC Unigy SIP). Below the General section is the "Originating Locations and Routing Policies" sub-section, which includes "Add" and "Remove" buttons. A table with 1 item is displayed, showing a list of policies. The table has columns for checkboxes, Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The single row shows a policy for "-ALL-" with "Any Locations" as the origin, "To-IPC-Unigy" as the destination, and a rank of 0.

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To-IPC-Unigy	0	<input type="checkbox"/>	IPC-Unigy	



## 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 “6” (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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Commit Cancel

General

\* Pattern: 6

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: br110.com

Notes:

Originating Locations and Routing Policies

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	BR-1C110	Test Room 1C110	To-BR110-CM	0	<input type="checkbox"/>	BR110-CM	
<input type="checkbox"/>	IPC-Unigy-Loc	IPC Unigy	To-BR110-CM-5077	0	<input type="checkbox"/>	BR110-CM-5077	for IPC Unigy

Select : All, None



## 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**.

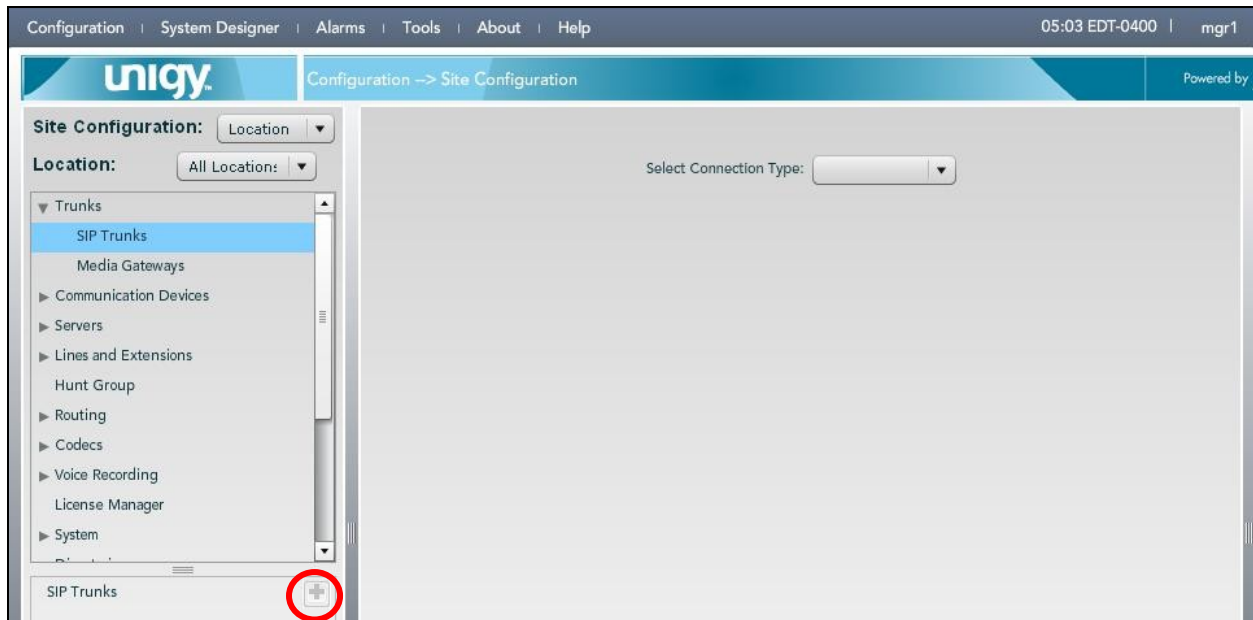


The screenshot shows the login interface for the IPC Unigy Management System. It features the IPC logo on the left. To the right of the logo are two input fields: 'User Name:' and 'Password:'. Below these fields is a checkbox labeled 'I agree with the' followed by a link to 'Terms of Use'. A 'Login' button is positioned to the right of the checkbox. At the bottom of the form, the following text is displayed: 'IPC Unigy™ Management System', 'Unigy™ Version 01.00.00.01.0003', and '© 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 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 5.3**.
- **PBX Provider:** “Avaya”
- **Connected Party Update:** “UPDATE”

The screenshot displays the UniQy configuration interface. The top navigation bar includes links for Configuration, System Designer, Alarms, Tools, About, and Help. The current page is titled "Configuration -> Site Configuration". On the left, a sidebar shows a tree view of configuration options, with "SIP Trunks" selected under the "Trunks" category. The main area is titled "Trunk:" and contains a "DialTone" section. The "Trunk Configuration" form has the following fields and values:

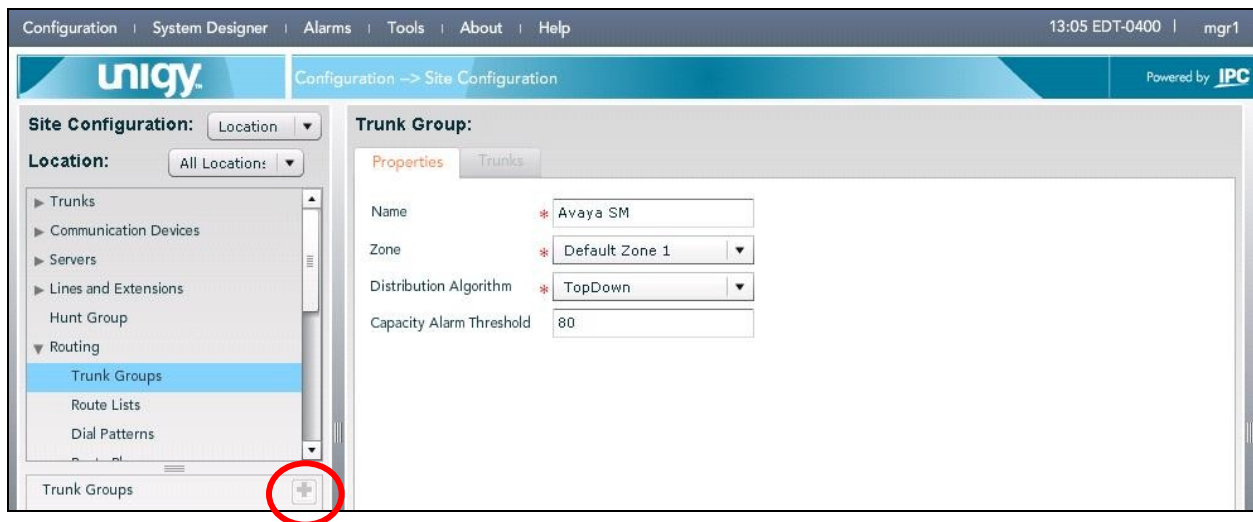
Field	Value
Trunk Name	SIP Trunk to SM
Number of Trunks	1
Connection Type	Dial Tone
Destination Address	10.32.32.78
Destination Port	5060
Media Manager Profile	Safe
Zone	Default Zone 1
Channels	10
Reason Protocol	SIP
PBX Provider	Avaya
Connected Party Update	UPDATE
Subscribe to MWI	<input type="checkbox"/>
MWI Subscription Time	

At the bottom right of the form are buttons for "Delete", "Revert", and "Save".

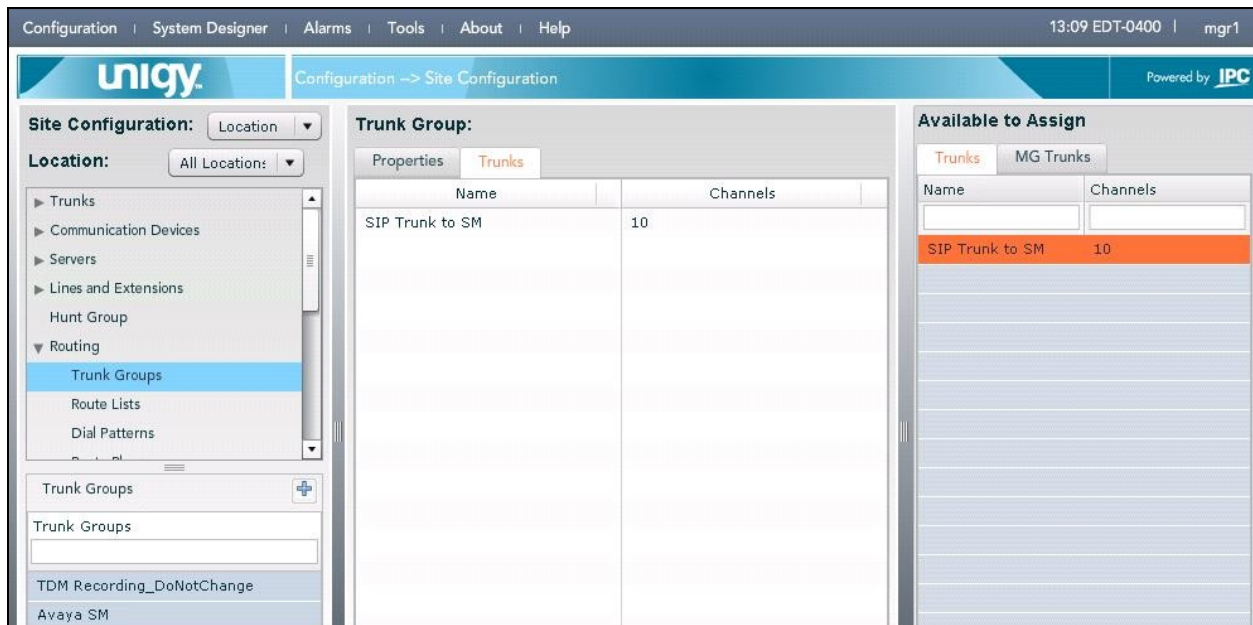
### 7.3. Administer Trunk Groups

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

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



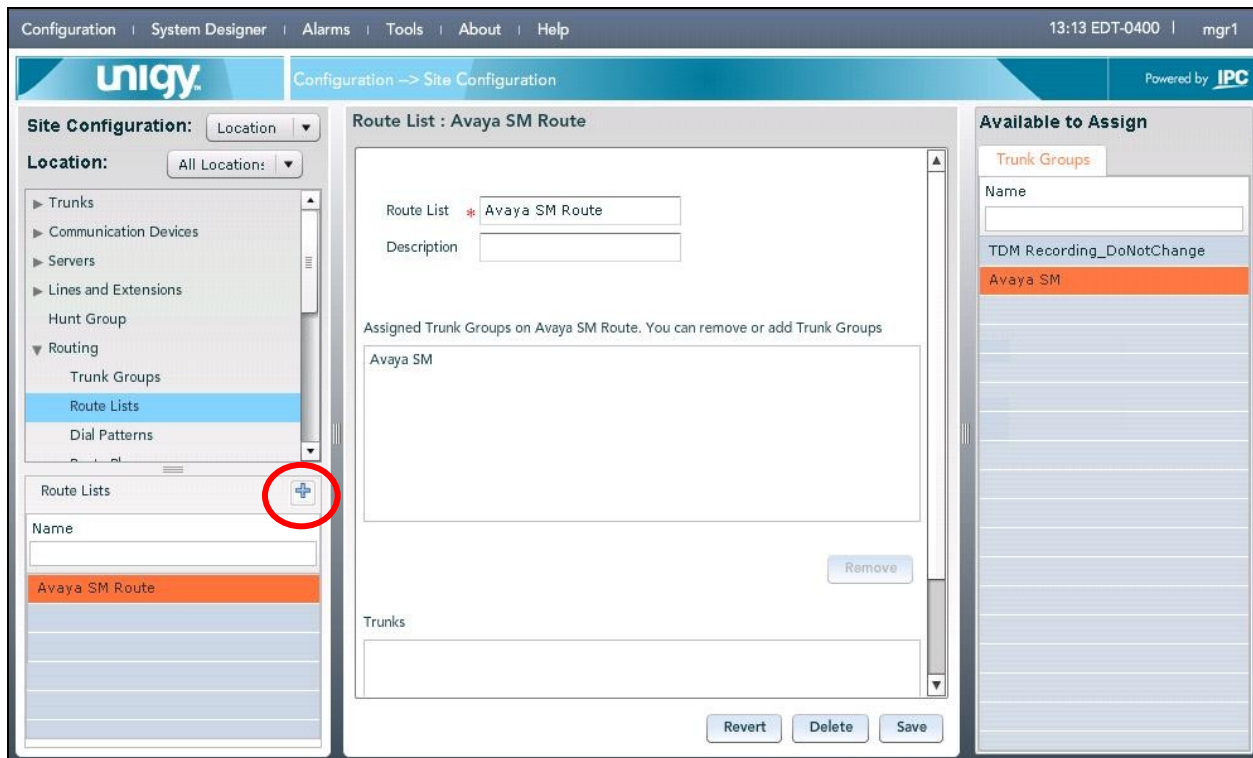
The screen is updated with three panes. In the rightmost pane, select the **Trunks** tab to display a list of trunks. Select the SIP trunk from **Section 7.2** in the rightmost pane and drag to the middle pane as shown below. Click **Save** (not shown).



## 7.4. Administer Route Lists

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

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



## 7.5. Administer Dial Patterns

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

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya endpoints, in this case “6\$\$\$\$” with “\$” matching to any digit. For **Call Classification**, select “External”. Click **Save** (not shown).

The screenshot shows the Unigy configuration interface. The left pane displays a tree view under 'Site Configuration' with 'Dial Patterns' selected. The right pane shows the 'Dial Patterns' table and the 'Dial pattern Details' form. The 'Add New' button in the 'Dial Patterns' table is circled in red.

Name	Pattern String	Outbound CLI	Call Classification	Prefix Digits	Description

**Dial pattern Details**

Properties

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 Avaya Aura® Communication Manager. In the compliance testing, two dial patterns were created as shown below.

The screenshot shows the Unigy configuration interface with two dial patterns added to the table.

Name	Pattern String	Outbound CLI	Call Classification	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).

The screenshot shows the Unigy configuration interface. The top navigation bar includes 'Configuration', 'System Designer', 'Alarms', 'Tools', 'About', and 'Help'. The user is logged in as 'mgr1' at '11:31 EDT-0400'. The main header shows 'unigy' and 'Configuration --> Site Configuration'. The left pane, 'Site Configuration', has a 'Location' dropdown set to 'All Location:' and a tree view with 'Routing' expanded to 'Route Plans'. The middle pane, 'Route Plan', contains a 'Create New Route Plan' form with the following fields: 'UI Name' (IPC2Avaya), 'Description' (empty), 'Calling Party' (\*), 'Called Party' (6xxxx), 'Action' (Forward), and 'Route List' (empty). The right pane, 'Available to Assign', shows a 'Route Lists' section with a 'Name' dropdown and a list containing 'Avaya SM Route'.

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

The screenshot shows the Unigy configuration interface after creating a route plan. The top navigation bar and user information are the same. The left pane shows 'Routing' expanded to 'Route Plans'. The middle pane, 'Route Plan', now displays a 'List of Route Plans' table. The table has four columns: 'UI Name', 'Calling Party', 'Called Party', and 'Action'. The first row is highlighted in blue and contains the values 'IPC2Avaya', '\*', '6xxxx', and 'FORWARD'. The right pane is not visible in this screenshot.

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**.

Configuration | System Designer | Alarms | Tools | About | Help 13:20 EDT-0400 | mgr1

Configuration -> Site Configuration Powered by IPC

**Site Configuration:** Location: [Location] All Location: [All Location]

**Location:** All Location: [All Location]

- Trunks
- Communication Devices
- Servers
- Lines and Extensions
- Hunt Group
- Routing
  - Trunk Groups
  - Route Lists
  - Dial Patterns
  - Route Plans**
- Codecs
- Voice Recording
- License Manager
- System
- Directories
- System Features

**Route Plan**

Create New Route Plan

UI Name: \* IPC2Avaya

Description: [ ]

Calling Party: \*

Called Party: \* 6xxxx

Action: \* Forward

Route List: Avaya SM Route

Remove

Back Revert Save

**Available to Assign**

Route Lists

Name

Avaya SM Route

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

Configuration | System Designer | Alarms | Tools | About | Help 17:43 EDT-0400 | mgr1

Configuration -> Site Configuration Powered by IPC

**Site Configuration:** Location: [Location] All Location: [All Location]

**Location:** All Location: [All Location]

- Trunks
- Communication Devices
- Servers
- Lines and Extensions
- Hunt Group
- Routing
  - Trunk Groups
  - Route Lists
  - Dial Patterns
  - Route Plans**
- Codecs
- Voice Recording
- License Manager
- System
- Directories
- System Features

**Route Plan**

List of Route Plans

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



## 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 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 77
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0077/001	T00135	in-service/idle	no
0077/002	T00136	in-service/idle	no
0077/003	T00137	in-service/idle	no
0077/004	T00138	in-service/idle	no
0077/005	T00139	in-service/idle	no
0077/006	T00140	in-service/idle	no
0077/007	T00141	in-service/idle	no
0077/008	T00142	in-service/idle	no
0077/009	T00143	in-service/idle	no
0077/010	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 5.4**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 77
```

STATUS SIGNALING GROUP	
Group ID:	77
Group Type:	sip
<b>Group State:</b>	<b>in-service</b>

## 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**.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left navigation pane includes sections like 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, SIP Performance, System Performance, and System Tools. The main content area is titled 'SIP Entity Link Monitoring Status Summary' and includes a 'Run Monitor' button. Below this is a table with 3 items, showing Session Manager Name, Entity Links Down/Total, Entity Links Partially Down, SIP Entities - Monitoring Not Started, and SIP Entities - Not Monitored. The table lists Dev4 SM, devcon-asm, and BR110-SM. Below the table is a 'Select : All, None' dropdown. Further down is the 'All Monitored SIP Entities' section, also with a 'Run Monitor' button. It shows 18 items with a 'Show 15' dropdown and a 'Filter: Enable' button. The list of SIP Entity Names includes BR110-CM, BR110-CM-5072, IPC-Uniqv (highlighted with a red circle), and mango.

<input type="checkbox"/>	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
<input type="checkbox"/>	<a href="#">Dev4 SM</a>	1/3	0	0	0
<input type="checkbox"/>	<a href="#">devcon-asm</a>	3/10	0	0	0
<input type="checkbox"/>	<a href="#">BR110-SM</a>	1/5	0	0	0

Select : All, None

All Monitored SIP Entities

Run Monitor

18 Items | Refresh | Show 15 | Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	<a href="#">BR110-CM</a>
<input type="checkbox"/>	<a href="#">BR110-CM-5072</a>
<input type="checkbox"/>	<a href="#">IPC-Uniqv</a>
<input type="checkbox"/>	<a href="#">mango</a>

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 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) [Home](#)

Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring [Help ?](#)

### 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](#)

[Summary View](#)

2 Items | [Refresh](#) Filter: [Enable](#)

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	<a href="#">BR110-SM</a>	10.32.37.100	5060	TCP	Up	200 OK	Up
▶ Show	<a href="#">BR110-SM</a>	10.32.37.100	5060	UDP	Up	200 OK	Up

[SIP Entity Monitoring](#)

### 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 6.0.1 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<sup>TM</sup> Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Administering Avaya Aura<sup>TM</sup> Session Manager*, Document Number 03-603324, Issue 3, Release 6.0, August 2010, available at <http://support.avaya.com>.
3. *Unigy 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

---

**©2012 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).