



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy v4.2 with Avaya Aura® Session Manager R8.0.1 and Avaya Aura® Communication Manager R8.0.1 Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy v4.2 to interoperate with Avaya Aura® Session Manager R8.0.1 and Avaya Aura® Communication Manager R8.0.1 using SIP trunks.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy used SIP trunks to Avaya Aura® Session Manager. Using the SIP trunks, Unigy users on IPC turrets were able to reach users on Avaya Aura® Communication Manager and on the PSTN.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 v4.2 (Unigy) to interoperate with Avaya Aura® Session Manager R8.0.1 (Session Manager) and Avaya Aura® Communication Manager R8.0.1 (Communication Manager). Unigy integrates with Session Manager via SIP Trunks (TCP and UDP).

The Unigy Platform is a unified trading communications system designed specifically to make the entire trading ecosystem more productive, intelligent and efficient. Based on a 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 Unigy.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Unigy did not include use of any specific encryption features as requested by IPC.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, display, G.711MU, G.711A, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, blinded/attended conference, barge-in, and long duration calls.

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

2.2. Test Results

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

- Even when IPC Unigy is configured with UDP, the TCP protocol must be configured to be allowed on Session Manager as Unigy switches over to use TCP for diversions.
- During the compliance test media shuffling was disabled, as shown in **Section 5.2**. (IPC requested)

2.3. Support

Technical support on IPC Unigy v4.2 can be obtained through the following:

- **Phone:** +1-(800)-NEED-IPC, +1-(203) 339-7800
- **Email:** systems.support@ipc.com

3. Reference Configuration

As shown in the test configuration below, Unigy consists of the Media Manager (MM), Converged Communication Manager (CCM), and Turrets. The Media Manager and Converged Communication Manager are typically deployed on separate servers. In the compliance testing, the same server hosted the MM and CCM.

SIP trunks are used from Unigy to Session Manager, to reach users (SIP and H.323) and on the PSTN.

A five-digit dial plan was used to facilitate dialing between the Avaya and Unigy. Unique extension ranges were associated with Communication Manager users (5xxxx for H.323 and SIP), and IPC turret users (7205x).

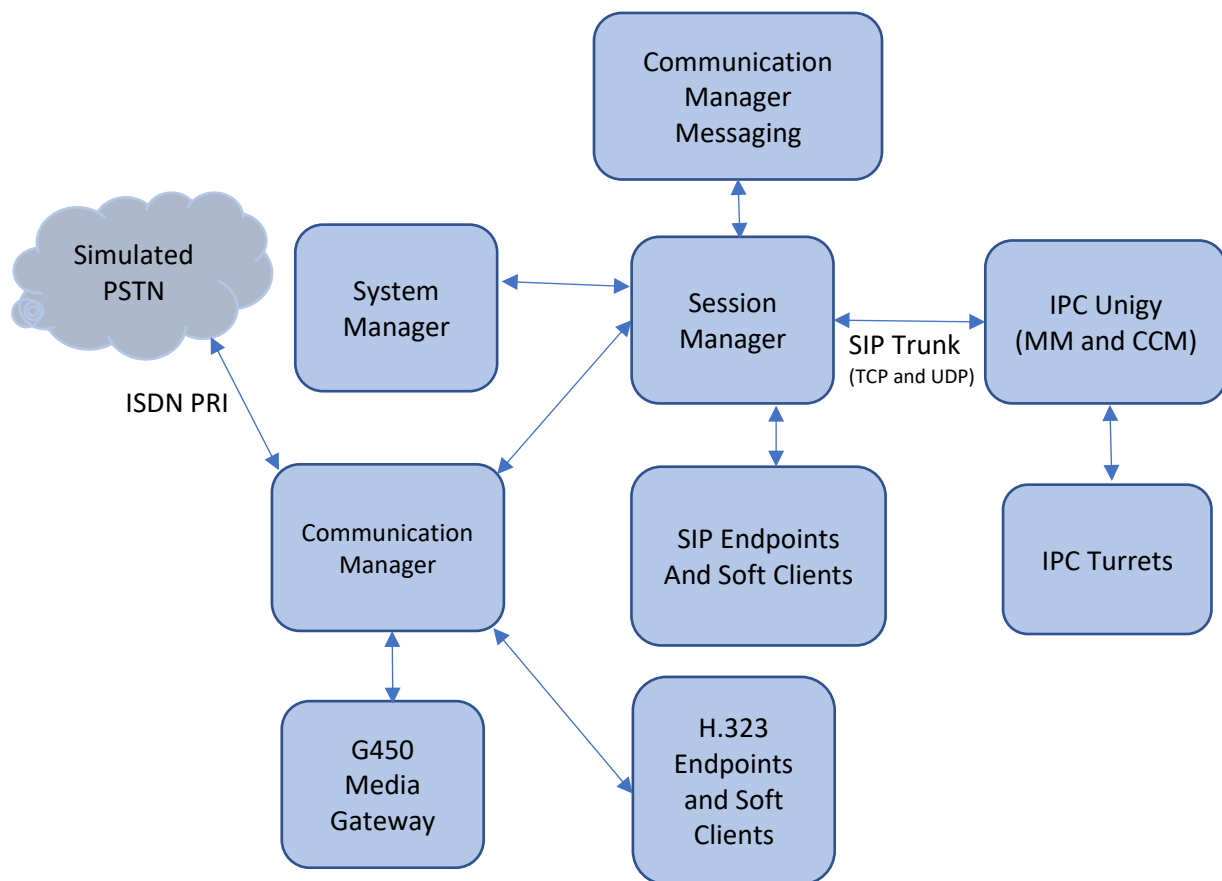


Figure 1: Test Configuration of IPC Unigy

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager running on Virtualized Environment	R8.0.1.0.0-FP1 (R018x.00.0.822.0-25031)
Avaya G450 Media Gateway	40.20.0
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.137
Avaya Aura® Session Manager running on Virtualized Environment	8.0.1.0
Avaya Aura® System Manager running on Virtualized Environment	8.0.1.0
Avaya Aura® Communication Manager Messaging on Virtualized Environment	7.0.0.0.441
Avaya 96xx IP Deskphone <ul style="list-style-type: none">• SIP• H.323	<ul style="list-style-type: none">• 7.1.4.0.11• 6.7104
IPC Unigy <ul style="list-style-type: none">• Media Manager• Converged Communication Manager• Turret	04.02.00.00.0200 04.02.00.00.0200 04.02.00.00.0200

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 SIP signaling group
- Administer SIP trunk group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer AAR analysis
- Administer ISDN/PRI trunk group
- Administer tandem calling party number

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

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

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		2400	1
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		36000	0
Maximum Video Capable IP Softphones:		2400	0
Maximum Administered SIP Trunks:		12000	10
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0
Maximum Number of DS1 Boards with Echo Cancellation:		688	0

5.2. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “1”. 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:** Set to “1”
- **Direct IP-IP Audio Connection:** “n”

```
add signaling-group 1                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
  Q-SIP? n
  IP Video? n                      Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y Peer Server: SM                      Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
  Near-end Node Name: procr                      Far-end Node Name: sm8
  Near-end Listen Port: 5061                      Far-end Listen Port: 5061
                                           Far-end Network Region: 1

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate                      Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                      RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 120                      Direct IP-IP Audio Connections? n
  Enable Layer 3 Test? y                      IP Audio Hairpinning? n
                                           Alternate Route Timer(sec): 6
```

5.3. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “1”. 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”
- **Signaling Group:** Number of signaling group configured in previous section.
- **Number of Members:** As required in the environment.

```
add trunk-group 1                                     Page 1 of 5
                                     TRUNK GROUP
Group Number: 1                                     Group Type: sip          CDR Reports: y
  Group Name: sm8                                     COR: 1          TN: 1          TAC: 101
  Direction: two-way                               Outgoing Display? n
  Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 1
                                                Number of Members: 10
```

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

```
add trunk-group 1                                     Page 3 of 5
TRUNK FEATURES
  ACA Assignment? n                               Measured: none
                                                Maintenance Tests? y

Suppress # Outpulsing? n  Numbering Format: private
                                                UI Treatment: shared
                                                Maximum Size of UI Contents: 128
                                                Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                Hold/Unhold Notifications? y
Send UCID? y                               Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```


Navigate to **Page 5** and disable **Network Call Redirection** (REFER) since REFER is not supported on Unigy.

add trunk-group 1	Page 5 of 5
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type:	
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	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.4. 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 5.3**.

For **Authoritative Domain**, set to “avaya.com”. 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 Unigy.

```
change ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

  Region: 1          NR Group: 1
Location:          Authoritative Domain: avaya.com
  Name:                               Stub Network Region: n
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
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

5.5. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.4**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that Unigy supports G.711 and G.729. For G.729, IPC needs to install a license.

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

                                IP MEDIA PARAMETERS

  Codec Set: 1

  Audio      Silence      Frames      Packet
  Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU   n            2         20
2: G.711A   n            2         20
3: G.729    n            2         20
```

5.6. 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 “1”. 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 1											Page 1 of 4			
Pattern Number: 1											Pattern Name: sm8			
SCCAN? n		Secure SIP? n		Used for SIP stations? n										
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/	IXC		
No				Mrk	Lmt	List	Del	Digits			QSIG			
							Dgts				Intw			
1: 1		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	Sub	Numbering	LAR
0 1 2 M 4 W				Request								Dgts	Format	
1: y y y y y n		n				rest								
2: y y y y y n		n				rest								

5.7. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to IPC. In the example shown below, all calls originating from a 5-digit extension beginning with 5 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	2			5	Total Administered: 2
5	5			5	Maximum Entries: 540

5.8. Administer AAR Analysis

Use the “change aar analysis 7” command and add an entry to specify how to route calls to 7xxxx. In the highlighted example shown below, calls with digits 7xxxx will be routed using route pattern “1” from **Section 5.6**.

change aar analysis 7							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
7		5	5	1	aar		n	

5.9. 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 “97”.

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 97		Page 3 of 22	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Wideband Support? n	
	Internal Alert? n	Maintenance Tests? y	
	Data Restriction? n	NCA-TSC Trunk Member:	
	Send Name: y	Send Calling Number: y	
Used for DCS? n		Send EMU Visitor CPN? n	
Suppress # Outpulsing? n	Format: private		
Outgoing Channel ID Encoding: preferred	UII IE Treatment: shared		
	Maximum Size of UII IE Contents: 128		
	Replace Restricted Numbers? n		
	Replace Unavailable Numbers? n		
	Send Connected Number: y		
Network Call Redirection: none	Hold/Unhold Notifications? n		
Send UII IE? y	Modify Tandem Calling Number: tandem-cpn-form		
Send UCID? y	BSR Reply-best DISC Cause Value: 31		
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	Invoke ID for USNI Calling Name: variable		
	Network (Japan) Needs Connect Before Disconnect? n		

5.10. 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 **720** and routed to trunk group **97** 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 9
CALLING PARTY NUMBER CONVERSION FOR TANDEM CALLS						
		Incoming	Outgoing	Outgoing		
	CPN	Number	Trunk	Number		
Len	Prefix	Format	Group(s)	Delete	Insert	Format
5	720		97		303xxxyyyy	pub-unk

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. It is assumed that the basic configuration is already in place. This Section discusses the following areas:

- Launch System Manager
- Administer locations
- 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/SMGR>” 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

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

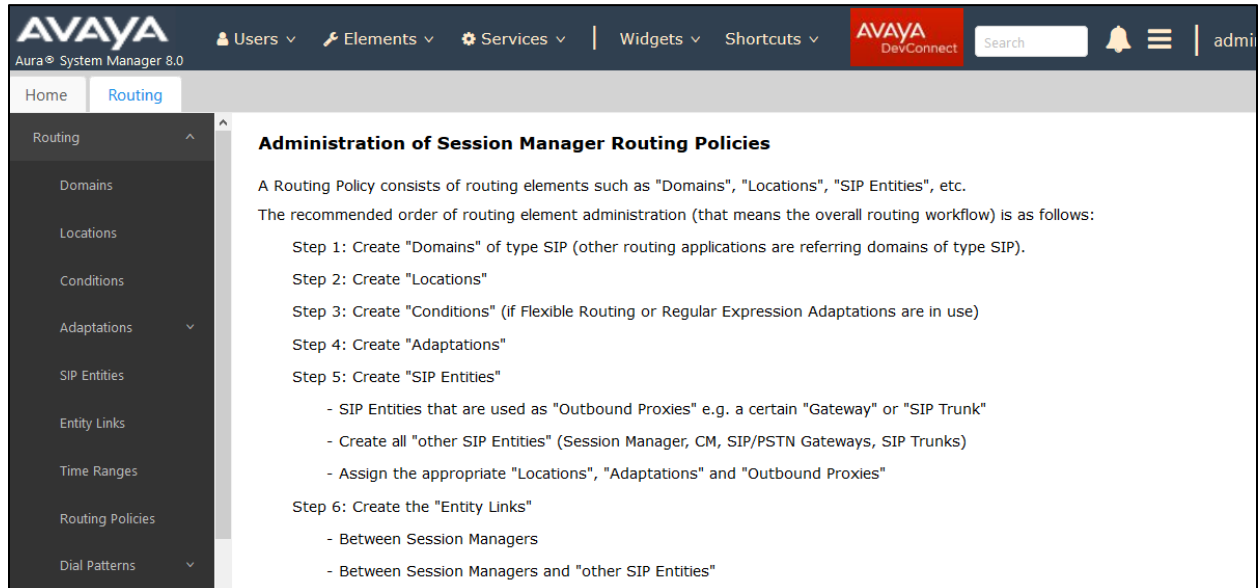
Password:

[Change Password](#)

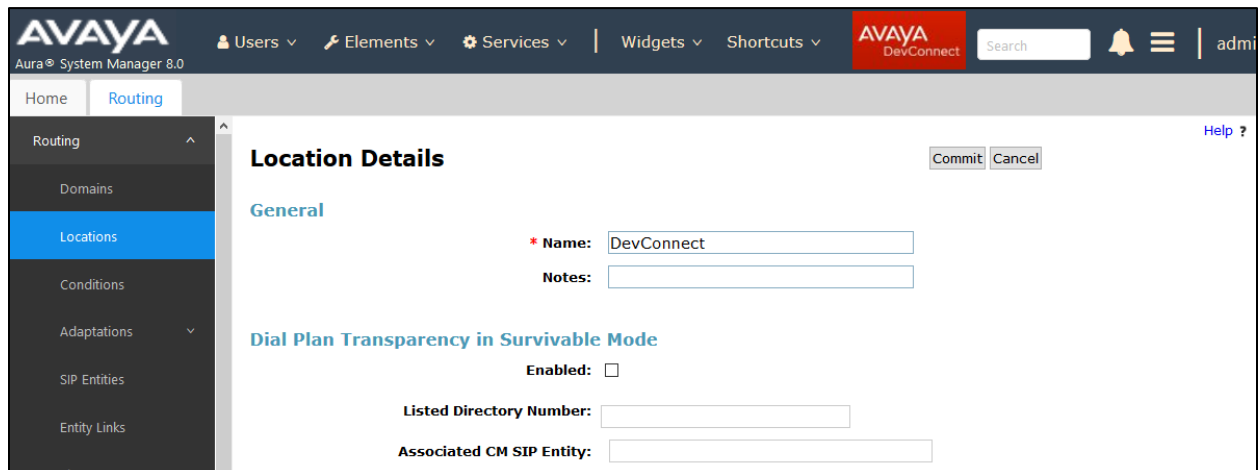
Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

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.



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** (not shown). Retain the default values in the remaining fields.



6.3. Administer SIP Entities

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

6.3.1. 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:** “SIP Trunk”.
- **Location:** Select the IPC location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.0', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', 'Shortcuts', and a search bar. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and has a 'General' tab. The form contains the following fields:

- Name:** unigy
- FQDN or IP Address:** 10.64.49.2
- Type:** SIP Trunk
- Notes:**
- Adaptation:** Unigy
- Location:** DevConnect
- Time Zone:** America/Fortaleza
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:**

Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area.

6.3.2. 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.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile icon are also present. The left-hand navigation pane shows a tree structure with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The form contains the following fields and values:

- Name:** cm8
- * FQDN or IP Address:** 10.64.110.131
- Type:** CM
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** DevConnect
- Time Zone:** America/Denver
- * SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area. A 'Help ?' link is also visible in the top right corner of the main content area.

6.4. Administer Entity Links

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

6.4.1. 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.
- **Protocol:** “UDP”.
- **Port:** “5060”.
- **SIP Entity 2:** The IPC entity name from **Section 6.3.1**.
- **Port:** “5060”.
- **Connection Policy:** “Trusted”.

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
* sm8	UDP	* 5060	* unigy	* 5060	<input type="checkbox"/>	trusted

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

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
sm8	TCP	5060	unigy	5060	<input type="checkbox"/>	trusted

6.4.2. 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 “sm8”.
- **Protocol:** The protocol used between Communication Manager and Session Manager is “TLS”.
- **Port:** Enter an appropriate port used, in this case “5061”.
- **SIP Entity 2:** The Communication Manager entity name from **Section 6.3.2**.
- **Port:** Enter an appropriate port used, in this case “5061”.
- **Connection Policy:** **Trusted**.

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
sm8	TLS	5061	cm8	5061	<input type="checkbox"/>	trusted

6.5. Administer Routing Policies

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

6.5.1. 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 6.3.1** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ AVAYA DevConnect Search 🔍 admin

Home Routing

Routing Policy Details Commit Cancel Help ?

General

* Name: unigy

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
unigy	10.64.49.2	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
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

6.5.2. 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 6.3.2** in the listing (not shown).

Retain the default values in the remaining fields.

Routing Policy Details [Commit] [Cancel] [Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm8	10.64.110.131	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item [Filter: Enable](#)

	Ranking	Name	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. Administer Dial Patterns

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

6.6.1. 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:** Select “ALL”.
- **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 6.5.1** was selected as shown below.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.0', and various menu items like Users, Elements, Services, Widgets, Shortcuts, and a search bar. The left sidebar shows a navigation tree with 'Routing' selected, and 'Dial Patterns' highlighted. The main content area is titled 'Dial Pattern Details' and contains two sections: 'General' and 'Originating Locations and Routing Policies'. The 'General' section has input fields for 'Pattern' (720), 'Min' (5), 'Max' (5), 'Emergency Call' (unchecked), 'SIP Domain' (-ALL-), and 'Notes'. The 'Originating Locations and Routing Policies' section has an 'Add' button and a table with one item: 'DevConnect', 'unigy', '0', 'unigy'. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The bottom of the table has a 'Select : All, None' option.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
DevConnect		unigy	0		unigy	

6.6.2. 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 “5xxxx” (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 all locations, and the Communication Manager routing policy from **Section 6.5.2** was selected as shown below. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ AVAYA DevConnect Search 🔍 🔔 ≡ | admin

Home Routing

Routing
Domains
Locations
Conditions
Adaptations ▾
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns ▾
Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 5

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: -ALL- ▾

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item 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"/>	DevConnect	cm8		0	<input type="checkbox"/>	cm8	

Select : All, None

7. Configure IPC Unigy

This section provides the procedures for configuring Unigy. 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 installation/configuration of Media Manager (MM) and/or CCM is typically performed by IPC installation engineers. 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 CCM. Log in using 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 image shows a web-based login interface for the Unigy Management System. It features a light gray background with a white login box. Inside the box, there is a blue circular logo with the word "unigy" in white. To the right of the logo is a text label "User Name:" followed by a text input field. Below the input field is a checkbox labeled "I agree with the" and a blue hyperlink "Terms of Use". To the right of the checkbox is a small square icon. Below these elements is a button with a right-pointing arrow. At the bottom of the login box, there is a block of small text providing version and copyright information.

IPC Unigy™ Management System
Unigy™ Version 04.02.00.00.0200
COP Version 03.00.00.00.1272
OS Patch Version 06.00.00.08.0015
© Copyright 2011-2016 IPC Systems, Inc. All rights reserved.

The following screen (Tools -> Monitoring) displays. Navigate to **Configuration** → **Site** under the main menu.

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. Select “Advanced” on the top right, 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 6.4.1**.
- **Zone:** An available zone, in this case “Default Zone 1”.
- **Channels:** The number of SIP trunk group members.
- **Reason Protocol:** “SIP”.
- **PBX Provider:** “Avaya”.
- **Connected Party Update:** “UPDATE”.
- **Subscribe to MWI:** Check box.
- **Diversion Header:** “History-Info”.
- **Outgoing Transport Type:** “UDP.”

Retain the default values in the remaining fields.

The screenshot shows the Unigy configuration interface. The top navigation bar includes 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The main header displays 'unigy' and 'Configuration -> Sites'. On the right, it says 'Powered by IPC'. The left sidebar shows a tree view with 'Trunks' expanded, listing various SIP trunks, with 'Unigy-SIP-trk-SM80' selected. The main panel is titled 'Trunk: Unigy-SIP-trk-SM80' and has two tabs: 'Basic' and 'Advanced'. The 'Advanced' tab is active, showing a list of configuration fields with their current values and a 'Save' button at the bottom right.

Field	Value
Trunk Name	Unigy-SIP-TRK-SM80
Connection Type	Dial Tone
Destination Address	10.64.110.135
Destination Port	5060
Destination Port Secure	5061
Media Manager Profile	Safe
Zone	Default Zone 1
Channels	30
Reason Protocol	SIP
PBX Provider	Avaya
Connected Party Update	UPDATE
Subscribe to MWI	<input checked="" type="checkbox"/>
MWI Subscription Time	0
Vendor	
A/B Side	<input type="checkbox"/>
Distant End Name	
PBX Trunk Group Reference	
Trunk Info	
Diversion Header	History-Info
Indicate PRACK Support	<input type="checkbox"/>
Outgoing Transport Type	UDP
ReINVITE For Media Update	<input checked="" type="checkbox"/>

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**.



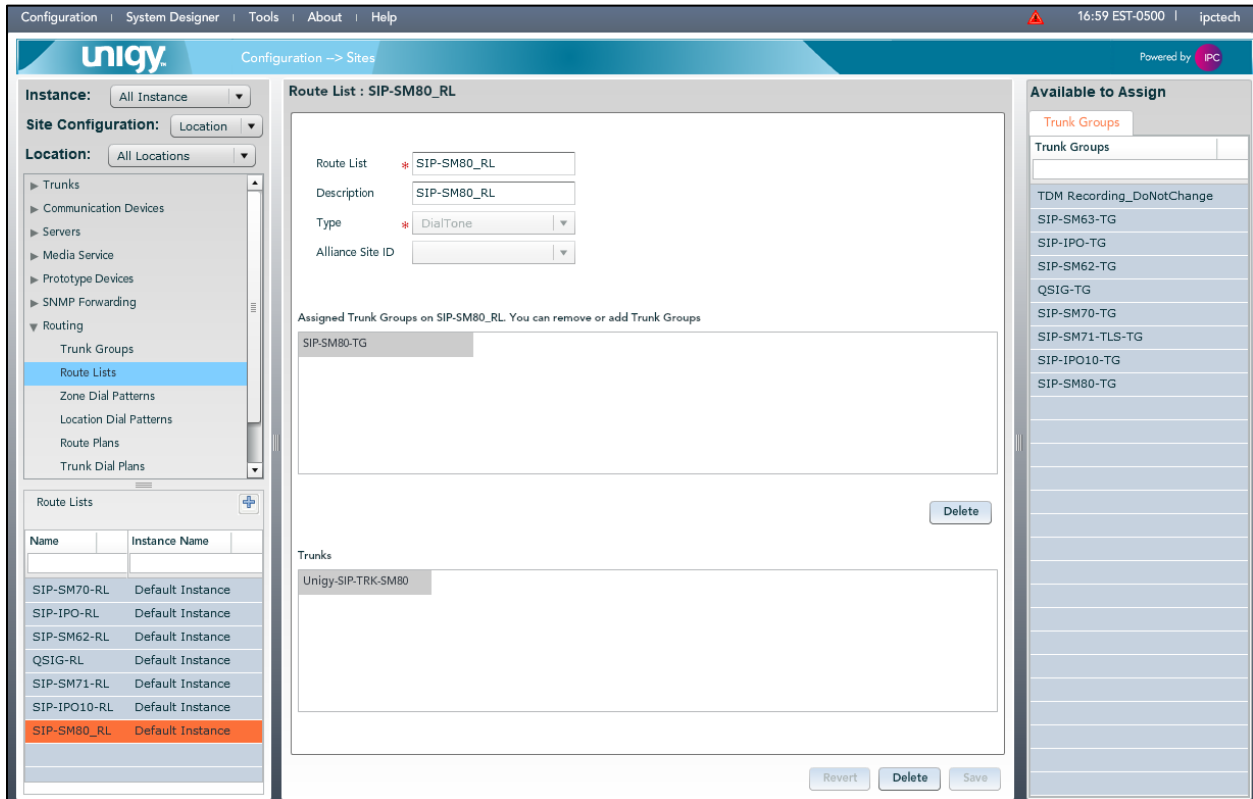
Select the **Trunks** tab in the right pane. The screen is updated with three panes. In the rightmost pane, select the **Trunks** tab to display a list of trunks. Select the SIP trunk from **Section 7.2** in the rightmost pane and drag to the middle pane as shown below. Click **Save**.



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 0** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below. Click **Save**.



The screenshot displays the Unigy configuration interface. The left pane shows the navigation tree with 'Route Lists' selected under 'Routing'. The middle pane shows the 'Route List : SIP-SM80_RL' configuration form. The right pane shows the 'Available to Assign' section with a list of trunk groups.

Route List : SIP-SM80_RL

Route List: * SIP-SM80_RL
Description: SIP-SM80_RL
Type: * DialTone
Alliance Site ID: [Dropdown]

Assigned Trunk Groups on SIP-SM80_RL. You can remove or add Trunk Groups

SIP-SM80-TG [Delete]

Trunks

Unigy-SIP-TRK-SM80

Available to Assign

Trunk Groups

- TDM Recording_DoNotChange
- SIP-SM63-TG
- SIP-IPO-TG
- SIP-SM62-TG
- QSIG-TG
- SIP-SM70-TG
- SIP-SM71-TLS-TG
- SIP-IPO10-TG
- SIP-SM80-TG

Route Lists Table:

Name	Instance Name
SIP-SM70-RL	Default Instance
SIP-IPO-RL	Default Instance
SIP-SM62-RL	Default Instance
QSIG-RL	Default Instance
SIP-SM71-RL	Default Instance
SIP-IPO10-RL	Default Instance
SIP-SM80_RL	Default Instance

Buttons: Revert, Delete, Save

7.5. Administer Zone Dial Patterns

Select **Routing** → **Zone 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**. Once the **Save** button is clicked, the newly created Dial pattern should be displayed under the **Dial Patterns** section.

The screenshot displays the Unigy Configuration web interface. The top navigation bar includes links for Configuration, System Designer, Tools, About, and Help, along with a status bar showing the time (17:00 EST-0500) and user (ipctech). The left sidebar contains a tree view of configuration categories: Trunks, Communication Devices, Servers, Media Service, Prototype Devices, SNMP Forwarding, and Routing. The Routing category is expanded, showing sub-items like Trunk Groups, Route Lists, Zone Dial Patterns (selected), Location Dial Patterns, Route Plans, Trunk Dial Plans, and Trunk Dial Plan Rules. The main content area is divided into two sections. The top section, titled 'Dial Patterns', contains a table with columns for Name, Pattern String, Description, and Zone Name. The table lists one entry: 'ALL Dial Pattern' with a pattern string of '*', description of 'all', and zone name of 'Default Zone 1'. Below the table are 'Add New' and 'Delete' buttons. The bottom section, titled 'Dial pattern Details', has a 'Properties' tab. It contains four labeled input fields: 'Name' (set to 'ALL Dial Pattern'), 'Zone' (set to 'Default Zone 1'), 'Description' (set to 'all'), and 'Pattern String' (set to '*'). 'Revert' and 'Save' buttons are located at the bottom right of this section.

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

Dial pattern Details

Properties

Name: ALL Dial Pattern

Zone: Default Zone 1

Description: all

Pattern String: *

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 **Destination** select the dial pattern for Avaya endpoints from **Section 7.5**. Select “Forward” for **Action** and click **Save**.

The screenshot displays the Unigy Configuration interface. The top navigation bar includes links for Configuration, System Designer, Tools, About, and Help, along with a status bar showing the time (17:02 EST-0500) and the user (ipctech). The main interface is divided into three panes:

- Left Pane:** A tree view showing the configuration hierarchy. The 'Routing' section is expanded, and 'Route Plans' is selected.
- Middle Pane:** The 'Route Plan' configuration screen. It includes a 'Create New Route Plan' section with fields for UI Name (Route-2-SM8), Description, Calling Party (*), Destination (*), and Action (Forward). Below these fields is a 'Route List' section with a table containing 'SIP-SM80_RL'. At the bottom of the middle pane, there are sections for 'Assign Trunk Groups' (containing 'SIP-SM80-TG') and 'Trunks' (containing 'Unigy-SIP-TRK-SM80').
- Right Pane:** The 'Available to Assign' section, which lists various route lists. The list includes 'TDM Recording_DoNotChange', 'SIP-SM70-RL', 'SIP-IPO-RL', 'SIP-SM62-RL', 'QSIG-RL', 'SIP-SM71-RL', 'SIP-IPO10-RL', and 'SIP-SM80-RL' (which is highlighted in orange).

8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, 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 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/0001	T00001	in-service/idle	no
0001/0002	T00002	in-service/idle	no
0001/0003	T00003	in-service/idle	no
0001/0004	T00004	in-service/idle	no
0001/0005	T00005	in-service/idle	no
0001/0006	T00006	in-service/idle	no
0001/0007	T00007	in-service/idle	no
0001/0008	T00008	in-service/idle	no
0001/0009	T00009	in-service/idle	no
0001/0010	T00010	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 5.2**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 1
```

STATUS SIGNALING GROUP	
Group ID:	1
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 6.3.1**.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, user information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows the navigation tree with 'SIP Entity Monitoring' selected under 'System Status'. The main content area is divided into two sections: 'Session Manager' and 'All Monitored SIP Entities'.

Session Manager

	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/>	sm8	Core	1	0	8	1	0	10

Select : All, None

All Monitored SIP Entities

Run Monitor

	SIP Entity Name
<input type="checkbox"/>	cm8
<input type="checkbox"/>	cmm8
<input type="checkbox"/>	brz8
<input type="checkbox"/>	m3k
<input type="checkbox"/>	ps8
<input type="checkbox"/>	m1k
<input type="checkbox"/>	mpp31
<input type="checkbox"/>	CTIntegrations
<input type="checkbox"/>	unigy

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
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ AVAYA DevConnect Search 🔔 admin

Home Routing **Session Manager**

Session Manager ^
Dashboard
Session Manager Ad...
Global Settings
Communication Profi...
Network Configur... ▾
Device and Locati... ▾
Application Config... ▾
System Status ^

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.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: unigy

Summary View

2 Items Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	sm8	IPv4	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	sm8	IPv4	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP

Select : None

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 v4.2 to successfully interoperate with Avaya Aura® Session Manager R8.0.1 and Avaya Aura® Communication Manager R8.0.1. All feature and serviceability test cases were completed with observations noted in **Section 2.22.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 8.0, August 2018
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 9.0, Release 8.0, August 2018
3. *Administering Avaya Aura® Session Manager*, Document 03-300509, Issue 10, Release 8.0, August 2018
4. *Administering Avaya Aura® System Manager*, Issue 9.0, Release 8.0, August 2018
5. *Unigy 4.2 System Configuration*; available upon request to IPC Support.

©2019 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.