



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy v5.0 with Avaya Aura[®] Session Manager R8.1 and Avaya Aura[®] Communication Manager R8.1 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy v5.0 to interoperate with Avaya Aura[®] Session Manager R8.1 and Avaya Aura[®] Communication Manager R8.1 using SIP trunks.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy uses SIP trunks to Avaya Aura[®] Session Manager. Using the SIP trunks, Unigy users with IPC MAX/TOUCH endpoints (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 v5.0 (Unigy) to interoperate with Avaya Aura® Session Manager R8.1 (Session Manager) and Avaya Aura® Communication Manager R8.1 (Communication Manager). Unigy integrates with Session Manager via SIP Trunks (TCP and UDP). IPC MAX/TOUCH endpoints provide calling functionality.

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 disabling and reenabling the entity links 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.729, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and conference. Messaging interoperability is not verified except for sending DTMF tones to the server.

The serviceability testing focused on verifying the ability of Unigy to recover from adverse conditions, simulated by disabling/reenabling the entity links 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 Unigy is configured with UDP, the TCP protocol must also 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)
- The caller/called display varied on the MAX and TOUCH endpoints as name versus number respectively with calls using Avaya H.323 endpoints. The variation was specific to the turret configuration.
- DTMF tones sent to turrets were not heard on their handset. Tones sent from turrets were heard on Avaya handsets and messaging.
- The G.729 codec was not supported unless a license was enabled on Unigy.
- Call forwarding was configured for turret endpoints via button assignments.

2.3 Support

Technical support on IPC Unigy 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.

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

A five-digit dial plan was used to facilitate dialing between Communication Manager and Unigy. Unique extension ranges were associated with Communication Manager users (70xxx for H.323 and SIP), and IPC turret users (7205x).

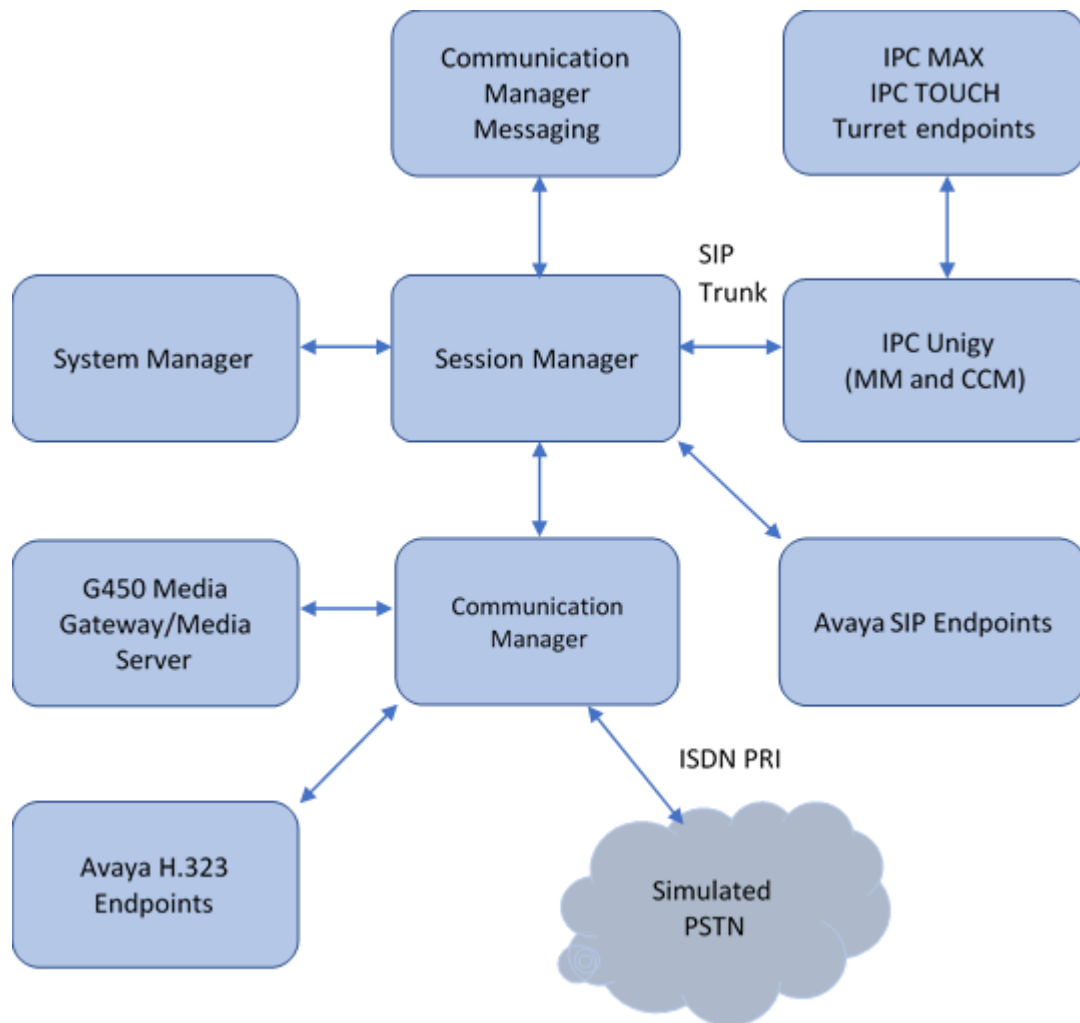


Figure 1: Test Configuration of IPC Unigy

4 Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	8.1.3.0.1.890.26685
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server running on Virtualized Environment	8.0.2.61
Avaya Aura® Session Manager running on Virtualized Environment	8.1.3.0.813014
Avaya Aura® System Manager running on Virtualized Environment	8.1.3.0.813014
Avaya Aura® Communication Manager Messaging on Virtualized Environment	7.0.0.0.441
Avaya IP Desktop phones <ul style="list-style-type: none">• Avaya 9641G SIP• Avaya 9641G H.323• Avaya J179/J189 SIP	7.1.11.0-092520 6.8.5.02-110720 4.0.7.1-121020
IPC Unigy <ul style="list-style-type: none">• Media Manager• Converged Communication Manager	05.00.00.00.0303 05.00.00.00.0303
IPC TOUCH turret	05.00.00.00.0303
IPC MAX turret	05.00.00.00.0303

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

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 3
                                     SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
Q-SIP? n
IP Video? y                      Priority 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: sm81
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): 65          Direct IP-IP Audio Connections? n
Enable Layer 3 Test? y                      IP Audio Hairpinning? y
                                           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? y
    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: both
                                Maintenance Tests? y

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

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

    Show ANSWERED BY on Display? Y

    DSN Term? n
```


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: 120	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? y	
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 5.2**.

For **Authoritative Domain**, set to the pertinent domain, in this case “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: Main              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? y
      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.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: sm81			
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	n	n	rest						lev0-pvt	none
2:	y	y	y	y	n	n	rest							none

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 or 7 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	5									5	Total Administered: 2
5	7									5	Maximum Entries: 540

5.8 Administer AAR Analysis

Use the “change aar analysis 720” command, and add an entry to specify how to route calls to 720xx. In the highlighted example shown below, calls with digits 720xx will be routed using route pattern “1” from **Section 5.6**.

change aar analysis 720						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
720		5	5	1	aar		n

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 area:

- 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/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 65.0, 66.0 and 67.0.

6.2 Administer Locations

In the subsequent screen (not shown), select **Elements** → **Routing** to display the **Administration of Session Manager Routing Policies** 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
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

R...

Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)
- Step 4: Create "Adaptations"
- Step 5: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 6: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 7: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 8: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"
 - (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 10: Create "Dial Patterns"

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** of **10.64.*** (not shown). Retain the default values in the remaining fields.

The screenshot displays the 'Location Details' configuration page in the Avaya Aura System Manager 8.1 interface. The page is divided into several sections:

- General**: Contains fields for **Name** (set to 'DevConnect') and **Notes**.
- Dial Plan Transparency in Survivable Mode**: Includes an **Enabled** checkbox (unchecked), **Listed Directory Number**, and **Associated CM SIP Entity** fields.
- Overall Managed Bandwidth**: Includes **Managed Bandwidth Units** (set to 'Kbit/sec'), **Total Bandwidth**, **Multimedia Bandwidth**, and an **Audio Calls Can Take Multimedia Bandwidth** checkbox (checked).
- Per-Call Bandwidth Parameters**: Includes **Maximum Multimedia Bandwidth (Intra-Location)** and **Maximum Multimedia Bandwidth (Inter-Location)**, both set to '2000 Kbit/Sec'.

The interface includes a top navigation bar with the Avaya logo, 'Aura® System Manager 8.1', and various menu items (Users, Elements, Services, Widgets, Shortcuts). A search bar and user profile (admin) are also present. The left sidebar shows 'Home' and 'Routing' tabs, with 'Routing' selected. The right sidebar contains a 'Help ?' link.

Add an adaptation to translate incoming/outgoing SIP headers. Select **Adaptations** → **Adaptations** from the left pane and click **New** (not shown) to add a new adaptation for IPC.

• Adaptation Name:	A descriptive name.
• Module Name:	“DigitConversionAdapter”
• Module Parameter Type:	“Name-Value Parameter”
• Egress URI Parameters:	“fromto”

- **fromto:** “true”
- **iodstd:** The pertinent domain name.
- **iosrcd:** The pertinent domain name.
- **odstd:** “ipc.com”
- **osrcd:** The Session Manager signaling IP address.

RH; Reviewed:
SPOC 6/26/2021

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:** “SIP Trunk”
- **Adaptation:** Select the Adaptation Name from **Section 6.3**.
- **Location:** Select the IPC location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items: Users, Elements, Services, Widgets, Shortcuts, a search bar, a notification bell, and the user 'admin'. The left sidebar shows a tree view with 'Home' and 'Routing' selected. The main content area is titled 'SIP Entity Details' and contains a 'Commit' and 'Cancel' button. The 'General' tab is active, showing the following fields:

- Name:** unigy
- * FQDN or IP Address:** 10.64.49.2
- Type:** SIP Trunk
- Notes:**
- Adaptation:** IPC
- Location:** DevConnect
- Time Zone:** America/Denver
- * SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:**
- Securable:** ☐
- Call Detail Recording:** egress
- Loop Detection**
 - Loop Detection Mode:** On
 - Loop Count Threshold:** 5
 - Loop Detection Interval (in msec):** 200
- 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 Communication Manager.
- **Type:** “CM”
- **Notes:** Any descriptive notes.
- **Location:** Select the location administered in **Section 6.2**
- **Time Zone:** Select the applicable time zone.

The screenshot displays the 'SIP Entity Details' configuration page in the Avaya Aura System Manager 8.1 interface. The page is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: 'Name' (cm81), 'FQDN or IP Address' (10.64.110.213), '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' (unchecked), and 'Call Detail Recording' (none). The 'Loop Detection' section includes 'Loop Detection Mode' (On), 'Loop Count Threshold' (5), and 'Loop Detection Interval (in msec)' (200). The 'Monitoring' section shows 'SIP Link Monitoring' (Use Session Manager Configuration). The left sidebar shows the navigation menu with 'Routing' selected.

6.5 Administer Entity Links

Add entity links for IPC and 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
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The IPC entity name from **Section 6.4.1**.
- **Port:** “5060”
- **Connection Policy:** “trusted” (not shown)

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left sidebar shows 'Home' and 'Routing' tabs, with 'Routing' selected. The main content area is titled 'Entity Links' and contains a table with one item. The table has columns for 'Name', 'SIP Entity 1', 'Protocol', 'Port', and 'SIP Entity 2'. The values in the table are: 'sm81_unigy_5060_UDP_i', 'sm81', 'UDP', '5060', and 'unigy'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table area. A 'Filter: Enable' link is also visible.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2
* sm81_unigy_5060_UDP_i	* Q sm81	UDP	* 5060	* Q unigy

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

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing

R...

Entity Links Commit Cancel [Help ?](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2
<input type="checkbox"/>	* sm81_unigy_5060_TCP_I	* <input type="text" value="sm81"/>	TCP ▾	* <input type="text" value="5060"/>	* <input type="text" value="unigy"/>

Select : All, None

Commit Cancel

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 "sm81".
- **Protocol:** "TLS"
- **Port:** "5061"
- **SIP Entity 2:** The Communication Manager entity name from **Section 6.4.2**.
- **Port:** "5061"
- **Connection Policy:** "trusted" (not shown)

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The left sidebar shows the 'Routing' tab selected. The main content area is titled 'Entity Links' and contains a table with one item. The table has columns for Name, SIP Entity 1, Protocol, Port, and SIP Entity 2. The item 'sm81_cm81_5061_TLS' is listed with 'sm81' as SIP Entity 1, 'TLS' as Protocol, '5061' as Port, and 'cm81' as SIP Entity 2. The table also includes a checkbox for selection and a 'Filter: Enable' option. Below the table, there are 'Commit' and 'Cancel' buttons.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2
<input type="checkbox"/>	* sm81_cm81_5061_TLS	* Q sm81	TLS	* 5061	* Q cm81

6.6 Administer Routing Policies

Add two new routing policies, one for IPC, and another for Communication Manager. The routing policies are linked to matching digits in dial plans defined in **Section 6.7** below. Then digits matching that dial plan entry are routed to the proper destination.

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. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name
- **SIP Entity as Destination:** Click **Select** and choose the IPC entity name from **Section 6.4.1**.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ 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

Dial Patterns

Add Remove

1 Item Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
---------	-----	-----	----------------	------------	----------------------	-------

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. Enter the following values for the specified fields and retain the default values for the remaining fields.

- AVAYA

Aura® System Manager 8.1

Users ▾

Elements ▾

Services ▾

Widgets ▾

Shortcuts ▾

Search

admin

Home

Routing

Routing Policy Details

CommitCancel

Help ?

General

* Name: cm81

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm81	10.64.110.213	CM	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item

Filter: Enable

<input type="checkbox"/>	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

Dial Patterns

AddRemove

11 Items

Filter: Enable

<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	-----------	-----	-----	----------------	------------	----------------------	-------

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:** “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 6.6.1** was selected as shown below.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 7205

* 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"/>	-ALL-		unigy	0	<input type="checkbox"/>	unigy	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

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 **70** (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. 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 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

R...

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 70

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com ▾

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"/>	-ALL-		cm81	0	<input type="checkbox"/>	cm81	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

7 Configure IPC Unigy Converged Communication Manager

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

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

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

7.1 Launch Unigy Management System

Access the Unigy Management System web interface by using the URL `http://ip-address` in an Internet browser window, where “ip-address” is the VIP of the Zone or in a standalone environment 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** (not shown).

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

The following screen (**Tools → Monitoring**) is displayed. Navigate to **Configuration → Site** under the main menu.

Configuration ▾ | System Designer ▾ | Tools ▾ | About | Help

12:42 EST-0500 | ipctech ▾

 Tools / Monitoring  Powered by 

ENTERPRISE050000000303

Summary | Backro... | Topology | Historic...

View All

Instances

Instance ▾	Total Devices ▾	Device Alerts High ▾	Device Alerts Low/Med ▾	Instance Priority ▾
Default Instance	6	4	2	HIGH

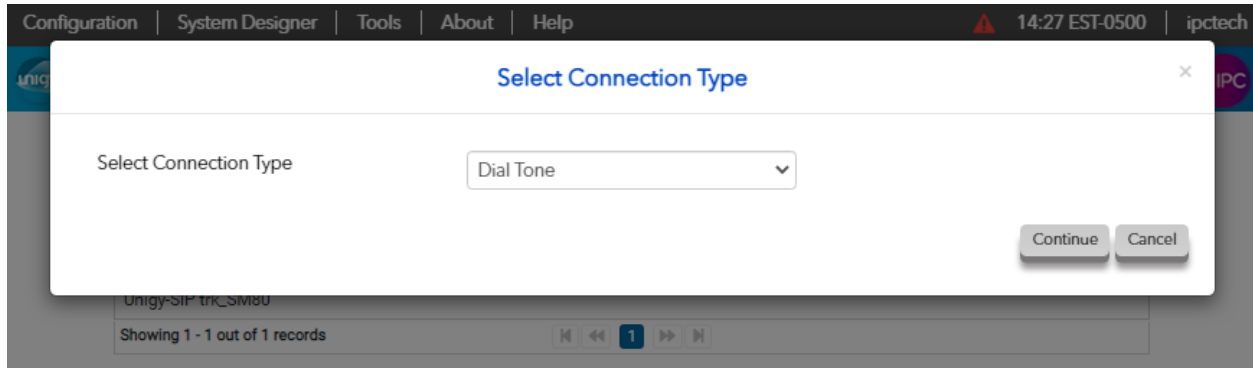
Showing 1 - 1 out of 1 records

+ Locations

+ Alerts

7.2 Administer SIP Trunks

Select **Trunks** → **SIP Trunks** (not shown) in the left pane and click the **Add New** icon (not shown) in the upper right pane to add a new SIP trunk. Select “Dial Tone” from the **Select Connection Type** drop-down list. Click **Continue**.



The screen below is displayed next. Select **Advanced** (not shown) 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 6.5.1**.
- **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** “Diversion”
- **Outgoing Transport Type** “UDP”

Retain the default values in the remaining fields.

The screenshot shows the Unigy web interface for configuring SIP trunks. The top navigation bar includes 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The breadcrumb trail is 'Configuration / Sites / Trunks / SIP Trunks'. The main content area is titled 'TRUNK' and shows the 'Dial Tone Trunk Configuration' tab. The configuration fields are as follows:

Field	Value
Trunk Name *	Unigy-SIP trk_SM81
Number of Trunks *	1
Connection Type *	Dial Tone
Destination Address *	10.64.110.212
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

A 'Show Basic' button is located in the top right corner of the configuration area.

◀ Back

TRUNK

Propert...

Subscribe to MWI	<input checked="" type="checkbox"/>	<div>Show Basic</div>
MWI Subscription Time	<input type="text"/>	
Vendor	<input type="text"/>	
A/B Side	<input type="checkbox"/>	
Distant End Name	<input type="text"/>	
PBX Trunk Group Reference	<input type="text"/>	
Trunk Info	<input type="text"/>	
Diversion Header *	<div>Diversion ▾</div>	
Indicate PRACK Support	<input type="checkbox"/>	
Outgoing Transport Type *	<div>UDP ▾</div>	
RelINVITE For Media Update	<input checked="" type="checkbox"/>	
Options Supported	<input checked="" type="checkbox"/>	
Equipped	<input checked="" type="checkbox"/>	

7.3 Administer Trunk Groups

Select **Routing** → **Trunk Groups** in the left pane and click the **Add New** icon in the upper right pane to add a new trunk group.

In the **Properties** tab, enter a descriptive **Name**, select “Default Zone 1” for the **Zone** field, select “Cyclic Ascending” for the **Distribution Algorithm** field, and click **Save**.

The screenshot shows the UniQy web interface for configuring a Trunk Group. The top navigation bar includes links for Configuration, System Designer, Tools, About, and Help. The main header displays the UniQy logo and the current path: Configuration / Sites / Routing / Trunk Groups. A 'Back' link is visible above the 'TRUNK GROUP' title. Below the title, there are two tabs: 'Propert...' (selected) and 'Trunks'. The 'Propert...' tab contains a form with the following fields: 'Name' (text input with value 'SIP-SM81'), 'Zone' (dropdown menu with value 'Default Zone 1'), 'Distribution Algorithm' (dropdown menu with value 'Cyclic Ascending'), 'Capacity Alarm Threshold' (text input with value '80'), and 'Type' (dropdown menu with value 'DialTone').

Select the **Trunks** tab. Click on the **+Assign** icon on the upper right to display available trunks. Select the SIP trunk from **Section 7.2** (not shown). Click **Save**.

7.4 Administer Route Lists

Select **Routing** → **Route Lists** in the left pane and click the **+Add New** icon in the upper right to add a new route list.

The **ROUTE LIST** screen is displayed. For **Route List**, enter a descriptive name. Input a description in the **Description** field if desired.

The screenshot shows the unigy ROUTE LIST configuration interface. At the top, there is a navigation bar with links for Configuration, System Designer, Tools, About, and Help. The main header includes the unigy logo, the breadcrumb path Configuration / Sites / Routing / Route Lists, and a status bar showing the time 14:11 EST-0500 and the user ipctech. Below the header, there is a back button and the title ROUTE LIST. The form contains several fields: Route List (with the value SIP-SM81-RL), Description (with the value SIP trunk to SM81), Instance (with a dropdown menu showing Default Instance), Type (with a dropdown menu showing DialTone), and Alliance Site Id (with a dropdown menu). Below the form, there is a section titled Assigned Trunk Groups on Route List. You can remove or add Trunk Groups, with a +Assign button. The table below this section has a header row with a Name column and a body row indicating No records found. At the bottom of the table, there are pagination controls showing 1 record out of 1.

Configuration | System Designer | Tools | About | Help 14:11 EST-0500 | ipctech

unigy Configuration / Sites / Routing / Route Lists Powered by IPC

Back

ROUTE LIST

Route List * SIP-SM81-RL

Description SIP trunk to SM81

Instance * Default Instance

Type * DialTone

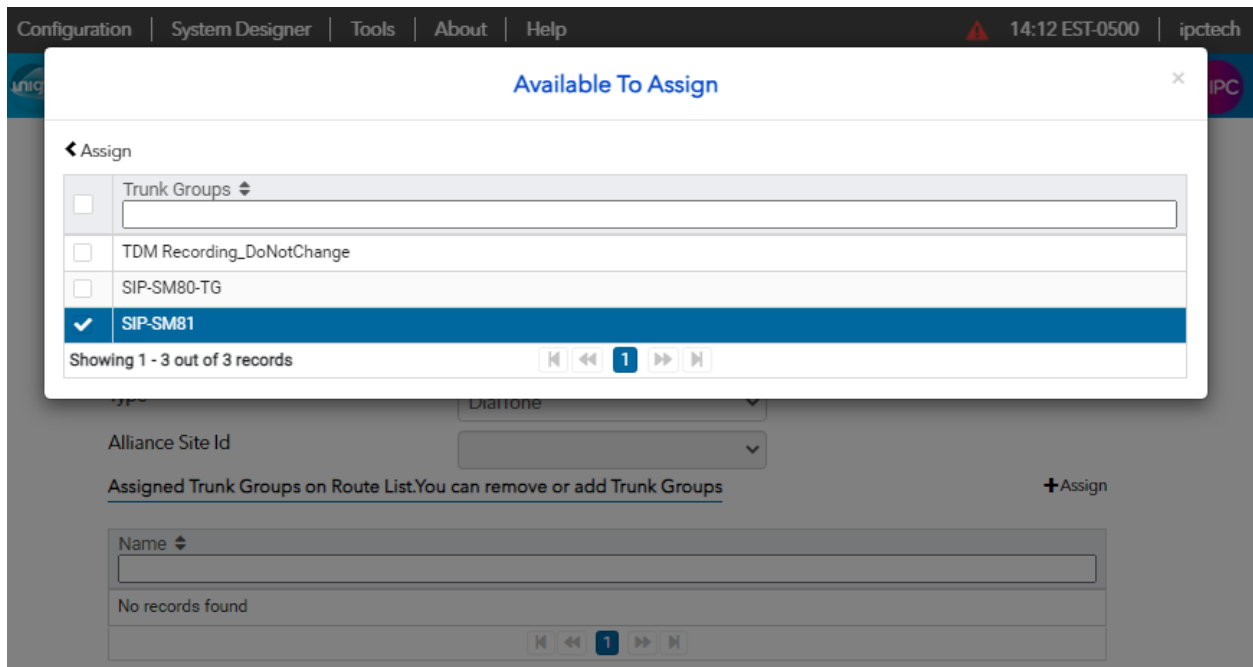
Alliance Site Id

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

Name
No records found

1

Click the **+Assign** icon and select the trunk group from **Section 7.3**. Click the **<Assign** icon to return to the route lists window. Click **Save**.



7.5 Administer Zone Dial Patterns

Select **Tools** → **Mass Edit Client** → **Zone Dial Pattern**. Follow the Zone Dial Pattern Mass Edit process as noted in the Unigy UMS guide. Input values as seen in the example below:

- **Name:** “ALL Dial Pattern”
- **Zone:** “1”
- **Zone Name:** “Default Zone 1”
- **Description:** “all”
- **Pattern String:** “*”

The screenshot shows the Microsoft Excel ribbon with tabs: FILE, HOME, INSERT, PAGE LAYOUT, FORMULAS, DATA, REVIEW, and VIEW. The ribbon groups include Clipboard, Font, Alignment, Protection, Number, Styles, Cells, and Editing. Below the ribbon is the formula bar showing 'C3' and a value of '0'. Below the formula bar is a sensitivity section with 'Sensitivity: Not set' and two buttons: 'IPC Restricted' and 'IPC Highly Confidential'. Below the sensitivity section is a table with columns A through L. The table contains data for a Zone Dial Pattern.

	A	B	C	D	E	F	G	H	I	J	K	L
1	VIP	10.64.49.2	Dial Pattern Properties									
2	User	ipclech										
3	Count: 1	Loaded	0									
5	Action	ID	Name	Zone	Zone Name	Description	Pattern String	Custom Tag				
6		33554434	ALL Dial Pattern	1	Default Zone 1	all	*					
7												

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.

In the **ROUTE PLAN** pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter “*” to denote any calling party from Unigy. For **Destination** enter “*”. For **Action** select “Forward”. For **Instance** select “Default Instance”. Click **Save**.

The screenshot shows the Unigy ROUTE PLAN configuration page. The top navigation bar includes links for Configuration, System Designer, Tools, About, and Help. The main header displays the Unigy logo and the breadcrumb path: Configuration / Sites / Routing / Route Plans. A 'Back' link is located above the 'ROUTE PLAN' title. The form contains the following fields:

UI Name *	Route-2 SM81
Description	Route plan for SM81
Calling Party *	*
Destination *	*
Action *	Forward
Instance *	Default Instance

Click **+Assign** to open the **Available To Assign** window. Select the Route List from **Section 7.4**. Click on the **<Assign** icon to return to the route plan window. Click **Save**.

The screenshot shows the 'Available To Assign' dialog box overlaid on the route plan configuration page. The dialog has a title bar with a close button. Inside, there is a search bar labeled 'Name' and a list of items:

<input type="checkbox"/>	Name
<input type="checkbox"/>	TDM Recording_DoNotChange
<input type="checkbox"/>	SIP-SM80-RL
<input checked="" type="checkbox"/>	SIP-SM81-RL

Below the list, it says 'Showing 1 - 3 out of 3 records' with navigation buttons. The background shows the 'ROUTE PLAN' form with the 'Action' dropdown set to 'Forward' and a '+Assign' button.

8 Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and 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 group 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

Verify the codec set specified is used in the calls made between Avaya sets and the turret sets.
For example, with the codec set to only G.729 as below:

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.729	n	2	20			

The trunk status on the call should show the codec used:

status trunk 1/1				Page	4 of	4
SRC PORT TO DEST PORT TALKPATH						
src port: T000001						
T000001:TX:10.64.49.5:36154/g729/10ms						
001V063:RX:10.64.50.54:2054/g729/10ms:TX:ctxID:155						
001V065:RX:ctxID:155:TX:10.64.50.54:2050/g729/20ms/1-srtp-aescm128-hmac80						
S000017:RX:10.64.10.202:2116/g729a/20ms/1-srtp-aescm128-hmac80						

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 displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The left sidebar shows the navigation menu with options like Home, Session Manager, and SIP Entity Monitoring. The main content area is titled "SIP Entity Link Monitoring Status Summary" and provides a summary of Session Manager SIP entity link monitoring status. It includes a "Run Monitor" button and a timestamp "As of 8:09 AM". Below this, there is a table showing the status of monitored entities for the "Session Manager" type. The table has columns for "Down", "Partially Up", "Up", "Not Monitored", "Deny", and "Total". The data row shows 8 Down, 2 Partially Up, 5 Up, 0 Not Monitored, 3 Deny, and a Total of 18. Below the table, there is a section for "All Monitored SIP Entities" with a "Run Monitor" button and a list of 18 items. The list includes SIP Entity Names such as "unigy", "trio", "sentry", "sbce81", "ps81-brz", "mx62", and "mpp722".

SIP Entity Link Monitoring Status Summary

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

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor As of 8:09 AM

1 Item Filter: Enable

	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/>	sm81	Core	8	2	5	0	3	18

Select : All, None

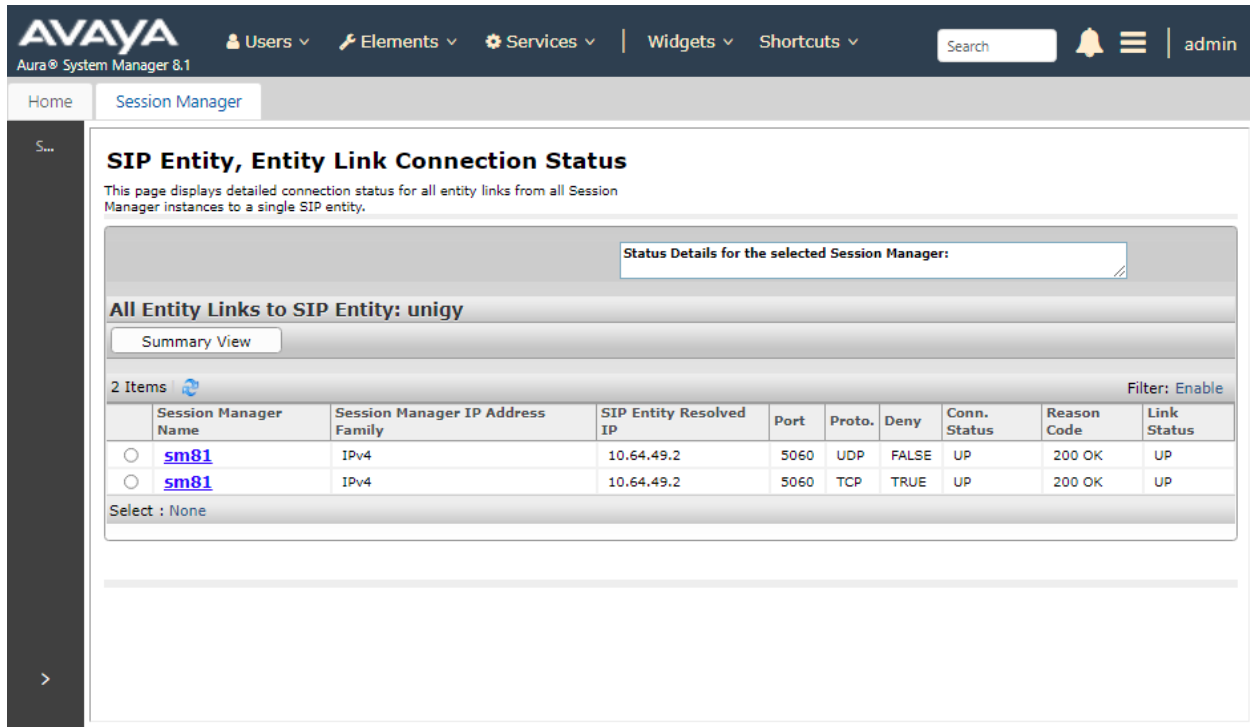
All Monitored SIP Entities

Run Monitor

18 Items Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	unigy
<input type="checkbox"/>	trio
<input type="checkbox"/>	sentry
<input type="checkbox"/>	sbce81
<input type="checkbox"/>	ps81-brz
<input type="checkbox"/>	mx62
<input type="checkbox"/>	mpp722

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 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search [] admin

Home Session Manager

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	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	sm81	IPv4	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	sm81	IPv4	10.64.49.2	5060	TCP	TRUE	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 5.0 to successfully interoperate with Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication Manager R8.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10 Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Issue 10, Release 8.1.x, March 2021.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 16, Release 8.1.x, March 2021.
3. *Administering Avaya Aura® Session Manager*, Issue 8, Release 8.1.x, February 2021.
4. *Administering Avaya Aura® System Manager*, Issue 11, Release 8.1.x, April 2021.
5. *Unigy 5.0 System Configuration*; available upon request to IPC Support.

©2021 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.