



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy v5.2 sp2 with Avaya Aura[®] Session Manager R10.1 and Avaya Aura[®] Communication Manager R10.1 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy v5.2 sp2 to interoperate with Avaya Aura[®] Session Manager R10.1 and Avaya Aura[®] Communication Manager R10.1 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, IPC 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 v5.2 sp2 (Unigy) to interoperate with Avaya Aura® Session Manager R10.1 (Session Manager) and Avaya Aura® Communication Manager R10.1 (Communication Manager). Unigy integrates with Session Manager via SIP Trunks (UDP). IPC MAX/TOUCH endpoints (turrets) 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. Calls were placed from various users to verify the call scenarios.

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:

- During the compliance test media shuffling was disabled, as shown in **Section 5.2** and **Section 5.4**. (IPC requested)
- 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 on turrets to Avaya endpoints, other IPC turrets, and PSTN are configured using Unigy features.

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 turret endpoints. 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 simulated PSTN via Avaya Session Border Controller for Enterprise.

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).

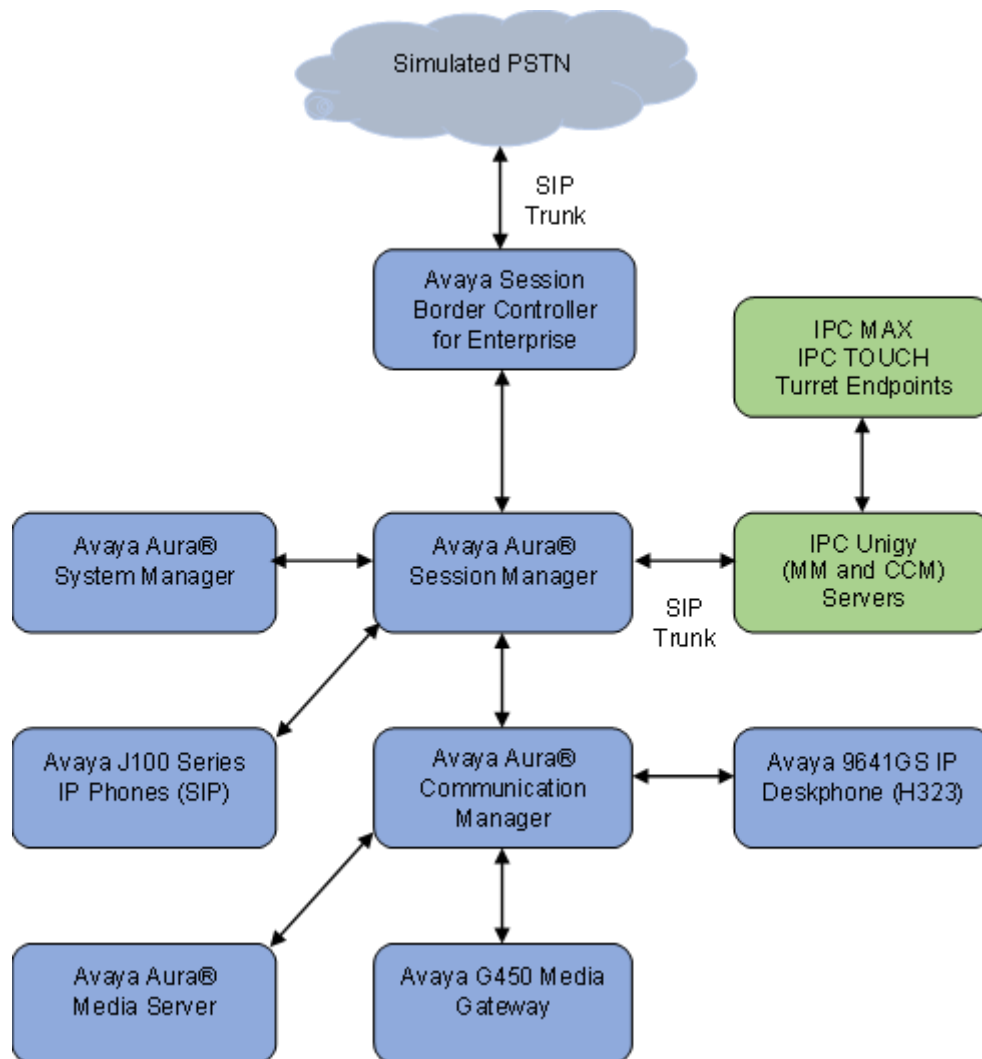


Figure 1: Test Configuration of IPC Unigy

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	10.1.0.2-SP2 01.0.974.0-27607
Avaya Aura® System Manager running on Virtualized Environment	10.1.0.2 Service Pack 2 10.1.0.2.0715160
Avaya Aura® Session Manager running on Virtualized Environment	10.1.0.2 Service Pack 2 10.1.0.02.1010215
Avaya Session Border Controller for Enterprise running on Virtualized Environment	10.1.1.0-35-218720
Avaya Aura® Media Server running on Virtualized Environment	10.1.0.101
Avaya G450 Media Gateway	42.7.0
Avaya 9641GS IP Deskphone (H.323)	6.8.5.3.2
Avaya J179/J189 IP Phones (SIP)	4.0.13.0.6
IPC Unigy <ul style="list-style-type: none">Media ManagerConverged Communication Manager	05.02.02.00.0033 05.02.02.00.0033 HF3: 05.02.02.00.9000303
IPC TOUCH Turret Endpoints	05.02.02.00.0033
IPC MAX Turret Endpoints	05.02.02.00.0033

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 Trunk Group Calling Number
- 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	5	
Maximum Administered Remote Office Trunks: 12000	0	
Max Concurrently Registered Remote Office Stations: 2400	0	
Maximum Concurrently Registered IP eCons: 128	0	
Max Concur Reg Unauthenticated H.323 Stations: 100	0	
Maximum Video Capable Stations: 36000	1	
Maximum Video Capable IP Softphones: 150	21	
Maximum Administered SIP Trunks: 12000	20	
Max Administered Ad-hoc Video Conferencing Ports: 12000	0	
Max 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” to turn off Media Shuffling.

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: sm10
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? 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: SM Trunk 1                             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

    Send UCID? y                                   Modify Tandem Calling Number: no

    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.711MU 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 Unigy, 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						unk-unk	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 Unigy. 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	

5.9 Administer Trunk Group Calling Number

Use the “change trunk-group n” command, where “n” is the SIP trunk group from **Section 5.3**, in this case “1”.

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

change trunk-group 1		Page	3 of	5
TRUNK FEATURES				
ACA Assignment? n		Measured: both		Maintenance Tests? y
Suppress # Outpulsing? n		Numbering Format: private		

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 1 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 67	
CALLING PARTY NUMBER CONVERSION						
FOR TANDEM CALLS						
		Incoming	Outgoing	Outgoing		
		Number	Trunk	Number		
Len	CPN	Format	Group(s)	Delete	Insert	Format
5	720		1		303xxxxyyy	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 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:

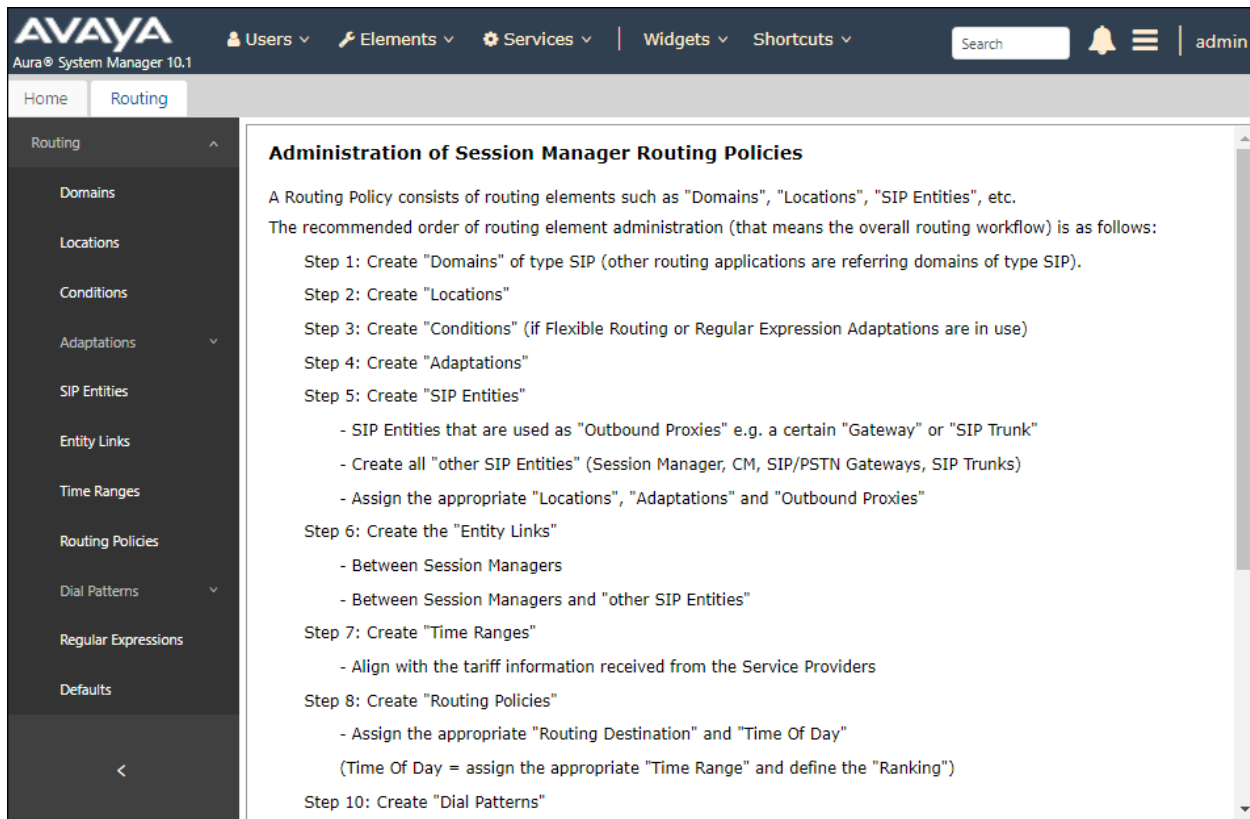
Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

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 location for Unigy.



AVAYA
Aura® System Manager 10.1

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

Home Routing

Routing ^

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

<

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 10.1 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**: Features '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 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, a search bar, and a user profile 'admin'. The left sidebar shows 'Home' and 'Routing' tabs, with 'Routing' selected. The 'Location Details' title is at the top of the main content area, with 'Commit' and 'Cancel' buttons to its right.

6.3 Administer Adaptations

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 Unigy.

The **Adaptation Details** screen is displayed. Enter the following values for the specified fields:

- **Adaptation Name:** A descriptive name.
- **Module Name:** “DigitConversionAdapter”
- **Module Parameter Type:** “Name-Value Parameter”

Click **Add** to add the adaptation name value pairs as specified:

- **fromto:** “true”
- **iodstd:** The pertinent domain name.
- **iosrcd:** The pertinent domain name.
- **odstd:** “ipc.com” (not shown).
- **osrcd:** The Session Manager signaling IP address (not shown).

The screenshot shows the 'Adaptation Details' screen in the Avaya Aura System Manager 10.1 interface. The 'General' tab is selected. The form contains the following fields and values:

- Adaptation Name:** IPC
- Notes:** (empty)
- Module Name:** DigitConversionAdapter (dropdown)
- Type:** digit
- State:** enabled (dropdown)
- Module Parameter Type:** Name-Value Parameter (dropdown)

Below these fields is a table with 'Add' and 'Remove' buttons. The table has columns for 'Name' and 'Value':

Name	Value
fromto	true
iodstd	avaya.com
iosrcd	avaya.com

At the bottom, there is a section for 'Egress URI Parameters' with an empty text box.

6.4 Administer SIP Entities

Add two new SIP entities, one for Unigy, and another for the SIP trunk for Communication Manager.

6.4.1 Unigy 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 Unigy. 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 Unigy Media Manager server.
- **Type:** “SIP Trunk”
- **Location:** Select the Unigy location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.
- **Adaptation:** Click Add, then select the Adaptation Name from **Section 6.3**.

AVAYA Aura® System Manager 10.1

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

Home Routing

R...

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:

Adaptations

Add Remove

<input type="checkbox"/>	Order	Name	Module Name	State	Type	Notes
<input type="checkbox"/>	1	IPC	DigitConversionAdapter	enabled	digit	

Select : All, None

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 Unigy.

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.

AVAYA Aura® System Manager 10.1

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

Home Routing

R...

SIP Entity Details Commit Cancel

General

* Name: cm10

* FQDN or IP Address: 10.64.110.213

Type: CM ▾

Notes:

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: none ▾

Adaptations

Add Remove

<input type="checkbox"/>	Order	Name	Module Name	State	Type	Notes
--------------------------	-------	------	-------------	-------	------	-------

6.5 Administer Entity Links

Add entity links for Unigy and for Communication Manager.

6.5.1 Unigy Entity Link

Select **Routing** → **Entity Links** from the left pane and click **New** in the subsequent screen (not shown) to add a new entity link for Unigy.

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 administered Session Manager SIP entity name, e.g., “sm10”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The administered Unigy SIP entity name from **Section 6.4.1**.
- **Port:** “5060”
- **Connection Policy:** “trusted” (not shown).

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 10.1', and several menu items: 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left pane shows 'Home' and 'Routing' tabs. The main area is titled 'Entity Links' and contains a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, and Port. The row contains the following values: 'sm10_Unigy_5060_UDP', 'sm10', 'UDP', '5060', 'Unigy', and '5060'. Above the table are 'Commit' and 'Cancel' buttons. Below the table is a 'Select : All, None' dropdown and another 'Commit' and 'Cancel' button pair.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
* sm10_Unigy_5060_UDP	* Q sm10	UDP	* 5060	* Q Unigy	* 5060

6.5.2 Communication Manager Entity Link

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 administered Session Manager SIP entity name, e.g., “sm10”.
- **Protocol:** “TLS”
- **Port:** “5061”
- **SIP Entity 2:** The administered Communication Manager SIP entity name from **Section 6.4.2**.
- **Port:** “5061”
- **Connection Policy:** “trusted” (not shown)

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top header shows the Avaya logo, navigation tabs (Users, Elements, Services, Widgets, Shortcuts), a search bar, and user information (admin). The left sidebar has a 'Routing' tab selected. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, and Port. The item is 'sm10_cm10_5061_TLS' with SIP Entity 1: sm10, Protocol: TLS, Port: 5061, SIP Entity 2: cm10, and Port: 5061. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
* sm10_cm10_5061_TLS	* sm10	TLS	* 5061	* cm10	* 5061

6.6 Administer Routing Policies

Add two new routing policies, one for Unigy, 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 Unigy 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 Unigy.

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 Unigy SIP entity administered in **Section 6.4.1**.

AVAYA Aura® System Manager 10.1

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

Home Routing

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

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
<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"/>	00:00	23:59	Time Range 24/7

Select : All, None

6.6.2 Communication Manager Routing Policy

Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Communication Manager. The **Routing Policy Details** screen is displayed. 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 Communication Manager entity administered in **Section 6.4.2**.

Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search [] Bell Icon Menu Icon admin

Home Routing

Routing Policy Details

[Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
cm10	10.64.110.213	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

6.7 Administer Dial Patterns

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

6.7.1 Unigy 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 Unigy 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 (optional).

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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled 'Dial Pattern Details' and is divided into two sections: 'General' and 'Originating Locations and Routing Policies'.

General Section:

- Pattern:** 7205
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- SIP Domain:** -ALL-
- Notes:** (empty field)

Originating Locations and Routing Policies Section:

Buttons: 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

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 7 (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 Unigy 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 10.1

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

Home Routing

R... **Dial Pattern Details** Commit Cancel Help ?

General

* Pattern: 7

* 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		cm10	0	<input type="checkbox"/>	cm10	

Select : All, None

7 Configure IPC Unigy Converged Communication Manager

This section provides the procedures for configuring 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 virtual IP address (VIP) of the Zone or in a standalone environment the IP address of the CCM.

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 image shows the login interface for the IPC Unigy Management System. On the left is the Unigy logo, a blue circle with the word 'unigy' in white. To the right of the logo is a 'User Name:' label above a white text input field. Below the input field is a checkbox followed by the text 'I agree with the [Terms of Use](#)'. To the right of this is a blue button with a white right-pointing arrow. At the bottom of the screen, there is a block of text providing version information and a copyright notice.

IPC Unigy™ Management System
Unigy™ Version 05.02.02.00.0033
COP Version 07.07.00.00.0020
OS Patch Version 07.00.00.24.0008
© Copyright 2011-2016 IPC Systems, Inc. All rights reserved.

The following screen (**Tools → Monitoring**) displays.

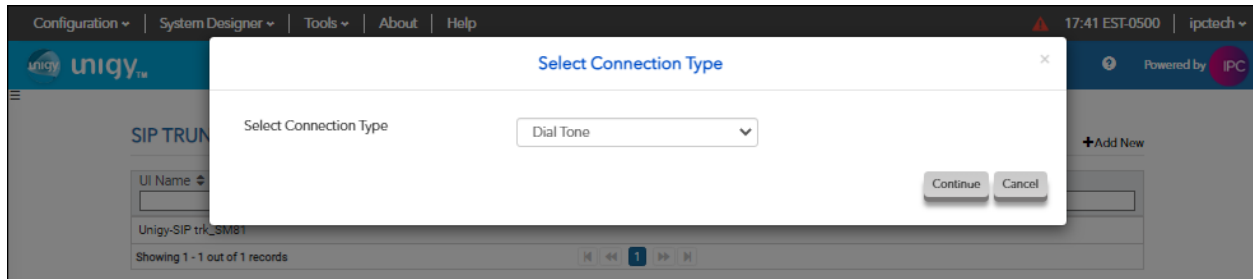
The screenshot shows the 'unigy™' interface with a navigation bar at the top containing 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The current page is 'Tools / Monitoring', and it is 'Powered by IPC'. The main heading is 'ENTERPRISE050000000303'. Below this, there are tabs for 'Summary', 'Backro...', 'Topology', and 'Historic...'. A 'View All' button is located in the top right corner of the main content area. The 'Instances' section is expanded, showing a table with the following data:

Instance	Total Devices	Device Alerts High	Device Alerts Low/Med	In:
Default Instance	6	5	1	HI

Below the table, it says 'Showing 1 - 1 out of 1 records' with pagination controls. At the bottom, there are expandable sections for '+ Locations' and '+ Alerts'.

7.2 Administer SIP Trunks

Navigate to **Configuration** → **Sites** from the top Main Toolbar. 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 **Show Advanced** (not shown) on the top right and enter the following values for the specified 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”
- **Diversion Header** “Diversion”
- **Outgoing Transport Type** “UDP”

Retain the default values in the remaining fields.

The screenshot displays the Unigy configuration interface for SIP Trunks. The top navigation bar includes links for Configuration, System Designer, Tools, About, and Help, along with a status bar showing the time (10:21 EST-0500) and the user (ipctech). The main header shows the Unigy logo and the current path: Configuration / Sites / Trunks / SIP Trunks. A 'Back' button is located at the top left of the configuration area. The 'TRUNK' title is centered above the configuration form. The form is titled 'Dial Tone Trunk Configuration' and contains the following fields:

Property	Value
Trunk Name *	SIP_Trk_SM10_1
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 form.

Configuration | System Designer | Tools | About | Help

10:23 EST-0500 | ipctech

unigy™

Configuration / Sites / Trunks / SIP Trunks

Powered by IPC

Back

TRUNK

Property...

Subscribe to MWI

☐

MWI Subscription Time

Vendor

A/B Side

☐

Distant End Name

PBX Trunk Group Reference

Trunk Info

Diversion Header *

Diversion

▼

Indicate PRACK Support

☐

Outgoing Transport Type *

UDP

▼

ReINVITE For Media Update

☒

Options Supported

☒

Equipped

☒

Secure SIP

Disabled

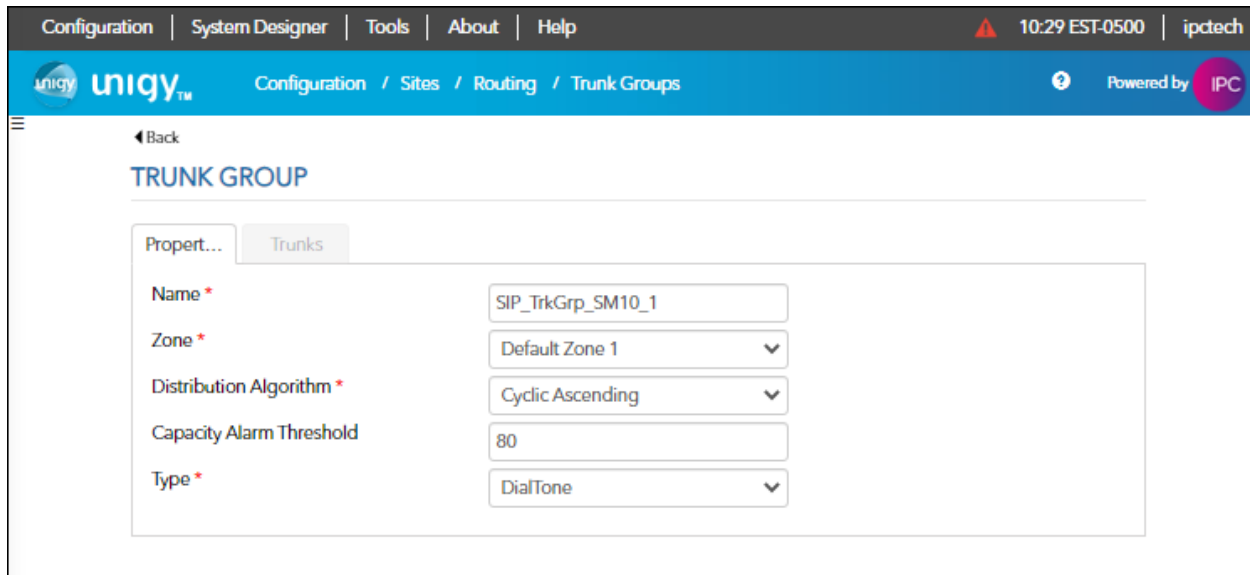
▼

Show Basic

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 unigy configuration interface. The top navigation bar includes links for Configuration, System Designer, Tools, About, and Help. The main header displays the unigy logo and the current path: Configuration / Sites / Routing / Trunk Groups. The page title is "TRUNK GROUP". Below the title, there are two tabs: "Properties" (selected) and "Trunks". The "Properties" tab contains the following fields:

Field	Value
Name *	SIP_TrkGrp_SM10_1
Zone *	Default Zone 1
Distribution Algorithm *	Cyclic Ascending
Capacity Alarm Threshold	80
Type *	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.

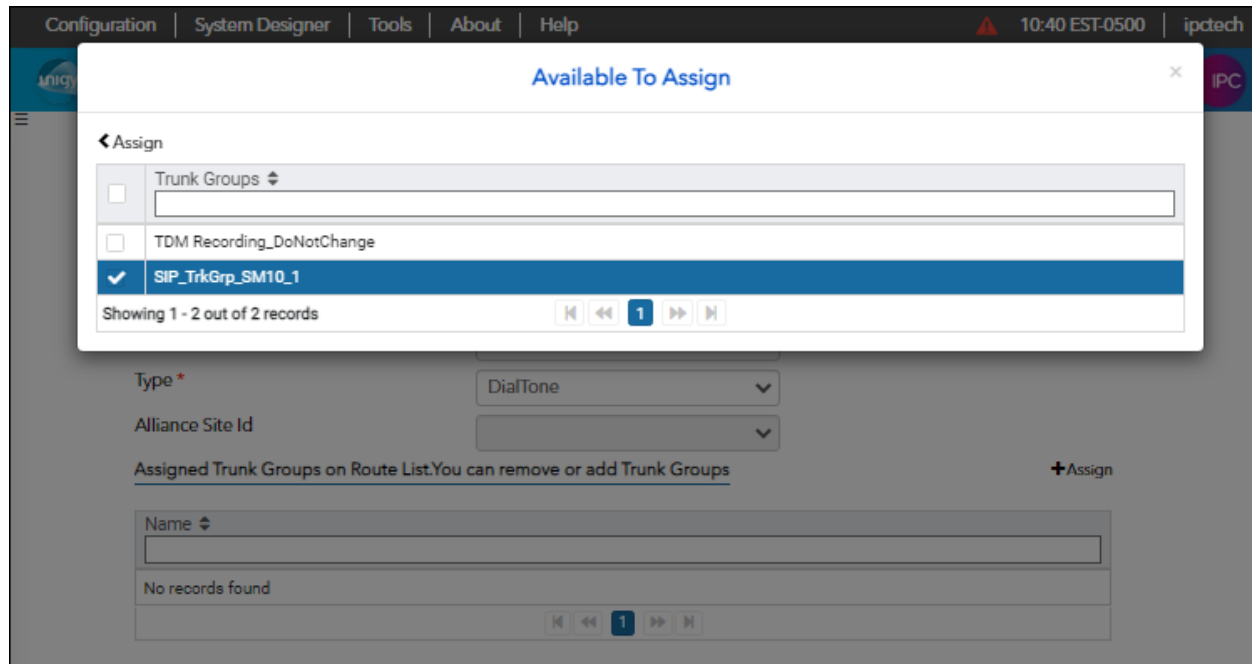
The **ROUTE LIST** screen is displayed. For **Route List**, enter a descriptive name. Input a description in the **Description** field if desired. Select “Default Instance” for **Instance**.

The screenshot shows the 'ROUTE LIST' configuration page in the unigy system. The top navigation bar includes 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The breadcrumb trail is 'Configuration / Sites / Routing / Route Lists'. The main form contains the following fields:

- Route List ***: Text input with value 'RouteList_SM10_1'
- Description**: Text input with value 'Route to SM10_1'
- Instance ***: Dropdown menu with 'Default Instance' selected
- Type ***: Dropdown menu with 'DialTone' selected
- Alliance Site Id**: Dropdown menu (empty)

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. A table with one column 'Name' is shown, containing the text 'No records found'. At the bottom of the table, there are pagination controls showing '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**.

7.6 Administer Zone Dial Patterns

Select **Routing** → **Zone Dial Pattern**. Click **Add New**. Enter an appropriate value for **Name**. Select **Default Zone 1** for **Zone**. Enter an appropriate value for **Description**. Input * for **Pattern String**. Click **Save**.

The screenshot shows the 'unigy' configuration interface. The top navigation bar includes 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The main header shows the 'unigy' logo and the breadcrumb 'Configuration / Sites / Routing / Zone Dial Patterns'. The page title is 'DIAL PATTERN DETAILS'. A 'Back' link is visible. The form contains four fields: 'Name' (text input with 'All Dial Pattern'), 'Zone' (dropdown menu with 'Default Zone 1'), 'Description' (text input with 'All'), and 'Pattern String' (text input with '*'). At the bottom right, there are 'Revert' and 'Save' buttons.

7.7 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 window. The top navigation bar includes 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The main header displays the Unigy logo and the path 'Configuration / Sites / Routing / Route Plans'. The window title is 'ROUTE PLAN'. Below the title, there is a 'Back' button. The form contains the following fields:

- UI Name ***: Text input with value 'Route_Plan_SM10_1'.
- Description**: Text input with value 'Route plan for SM10_1'.
- Calling Party ***: Text input with value '*'.
- Destination ***: Text input with value '*'.
- Action ***: Dropdown menu with 'Forward' selected.
- Instance ***: Dropdown menu with 'Default Instance' selected.

At the bottom of the form, there are three buttons: 'Remove', 'Revert', and 'Save'.

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. The title bar says 'Available To Assign'. Inside the dialog, there is a '< Assign' button. Below it is a table with the following rows:

	Name
<input type="checkbox"/>	TDM Recording_DoNotChange
<input checked="" type="checkbox"/>	RouteList_SM10_1

Below the table, it says 'Showing 1 - 2 out of 2 records'. At the bottom right of the dialog, there is a '+Assign' button. The background shows the same ROUTE PLAN configuration window as the previous screenshot, but it is dimmed.

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 group 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.

TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/0001	T000001	in-service/idle	no	
0001/0002	T000002	in-service/idle	no	
0001/0003	T000003	in-service/idle	no	
0001/0004	T000004	in-service/idle	no	
0001/0005	T000005	in-service/idle	no	
0001/0006	T000006	in-service/idle	no	
0001/0007	T000007	in-service/idle	no	
0001/0008	T000008	in-service/idle	no	
0001/0009	T000009	in-service/idle	no	
0001/0010	T000010	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	3 of	3
				SRC PORT TO DEST PORT TALKPATH		
src port: T000001						
T000001:TX:10.64.10.201:2048/g729/20ms						
AMS1:RX:10.64.110.214:6050/g729/20ms:TX:cnfID:0						
AMS1:RX:cnfID:0:TX:10.64.110.214:6052/g729/10ms						
T000009:RX:10.64.10.214:16426/g729/10ms						

8.2 Verify Avaya Aura® Session Manager

The SIP trunk status between Session Manager and Unigy is verified through System Manager. From the System Manager home page (not shown), select **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Under **All Monitored SIP Entities**, click on the Unigy SIP entity name, e.g., “Unigy”, from **Section 6.4.1**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). A search bar and a notification bell are also present. 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 10:13 AM". Below this, there is a table showing the status of monitored entities for a single item, "sm10". The table has columns for "Down", "Partially Up", "Up", "Not Monitored", "Deny", and "Total". The status for "sm10" is "Core" with 0 Down, 1 Partially Up, 6 Up, 0 Not Monitored, 0 Deny, and a Total of 7. Below the table, there is a section for "All Monitored SIP Entities" with a "Run Monitor" button and a list of 7 items. The list includes "Unigy", "sbce10", and "ipo11".

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 10:13 AM

1 Item Filter: Enable

Session Manager	Type	Monitored Entities					
		Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/> sm10	Core	0	1	6	0	0	7

Select : All, None

All Monitored SIP Entities

Run Monitor

7 Items Filter: Enable

SIP Entity Name
<input type="checkbox"/> Unigy
<input type="checkbox"/> sbce10
<input type="checkbox"/> ipo11

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

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, a search bar, and links for Users, Elements, Services, Widgets, and Shortcuts. The user is logged in as 'admin'. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a sub-header 'All Entity Links to SIP Entity: Unigy'. A table displays the connection status for the selected Session Manager 'sm10'.

Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
sm10	IPv4	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP

8.3 Verify IPC Unigy

Make calls in both directions from IPC MAX and TOUCH turret endpoints to Avaya endpoints. Verify calls connect with two-way talk paths.

9 Conclusion

These Application Notes describe the configuration steps required for IPC Unigy 5.2 sp2 to successfully interoperate with Avaya Aura® Session Manager R10.1 and Avaya Aura® Communication Manager R10.1. All feature and serviceability test cases were completed with observations as noted in **Section 2.2**.

10 Additional References

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

The following Avaya product documentation can be found at <http://support.avaya.com>.

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 2, September 2022.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 6, Release 10.1, September 2022.
3. *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 4, September 2022.
4. *Administering Avaya Aura® System Manager*, Issue 7, Release 10.1.x, September 2022.

©2023 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.