Application Notes for IPC Unigy v4.3 with Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication R8.1 Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy v4.3 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. IPC Unigy uses SIP trunks to Avaya Aura® Session Manager. Using the SIP trunks, Unigy users on IPC turrets are able to reach users on Avaya Aura® Communication Manager and the PSTN.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1 Introduction

These Application Notes describe the configuration steps required for IPC Unigy v4.3 (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).

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 IPC 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 IPC Unigy is configured with UDP, the TCP protocol must be configured to be allowed on Session Manager as Unigy switches over to use TCP for diversions.
- During the compliance test media shuffling was disabled, as shown in **Section 5.2**. (IPC requested)
- The caller/called display varied on the MAX and TOUCH endpoints as name versus number respectively with H.323 calls. The variation was specific to the endpoints, not the user.
- DTMF tones sent to turrets were not heard on their handset. Tones sent from turrets were heard on Avaya handsets and messaging.
- During media shuffling tests, transfers were noted to fail when the codec set was configured for only the G.729 codec set. Adding G.711 to the codec set eliminated the problem. The Unigy MM handles the transfer and may be configured for G.729.

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. In the compliance testing, the same server hosted the MM and CCM.

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

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

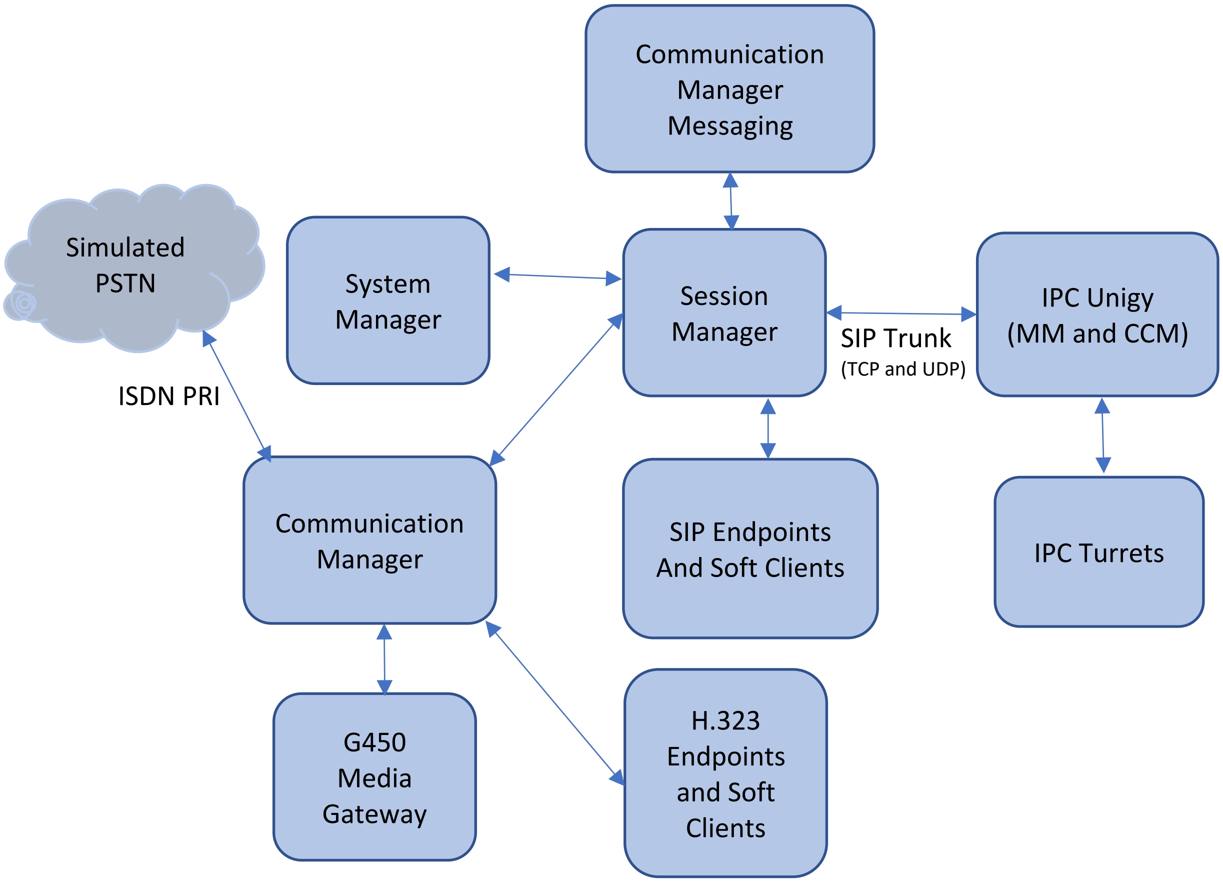


Figure 1: Test Configuration of IPC Unigy

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	R8.1.0.0-FP1 (R018x.01.0.890.0)
Avaya G450 Media Gateway	40.20.0
Avaya Aura® Media Server running on Virtualized Environment	8.0.2.61
Avaya Aura® Session Manager running on Virtualized Environment	8.1.1.0
Avaya Aura® System Manager running on Virtualized Environment	8.1.1.0
Avaya Aura® Communication Manager Messaging on Virtualized Environnent	7.0.0.0.441
Avaya 96xx IP Deskphones • SIP • H.323 • Avaya J100 Series SIP Deskphones	• 7.1.9.04.0.5.0.10 • 6.83044 • 4.0.5.0.10
IPC Unigy • Media Manager • Converged Communication Manager • Turret	04.03.00.04.0045 04.03.00.04.0045 04.03.00.04.0045

5 Configure Avaya Aura® Communication Manager

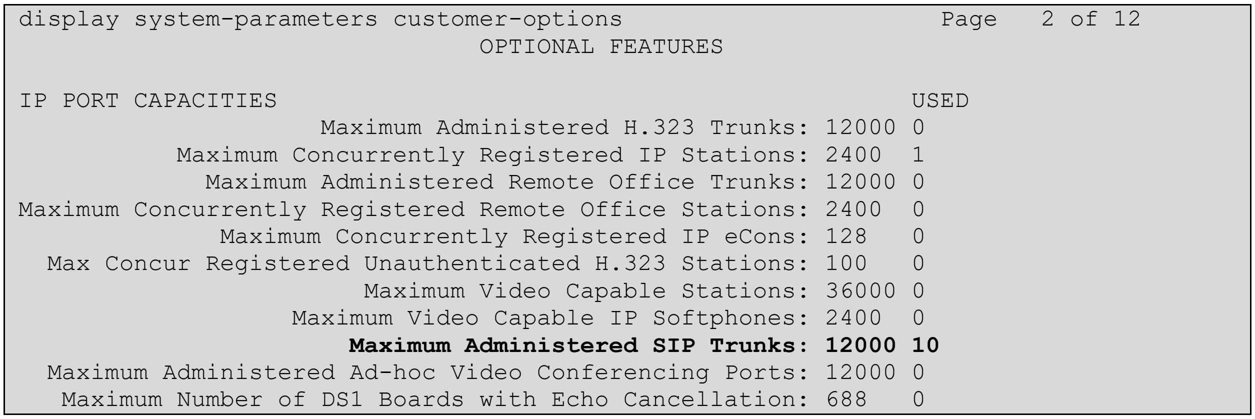
This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- 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.

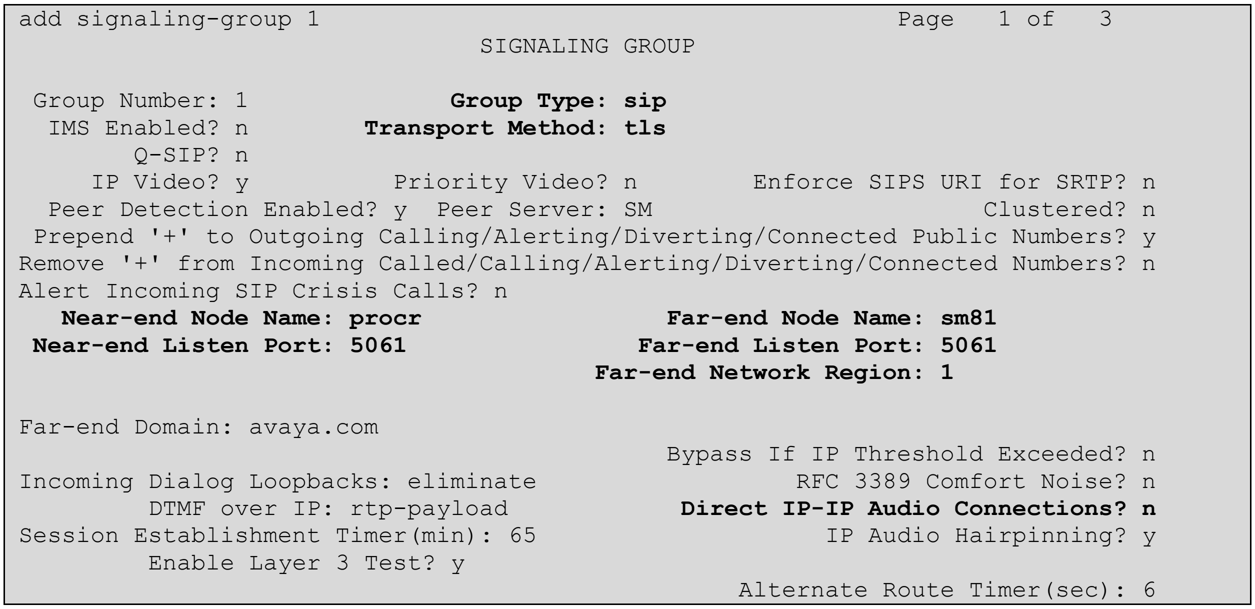


```
display system-parameters customer-options                      Page   2 of 12
                                OPTIONAL FEATURES

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”

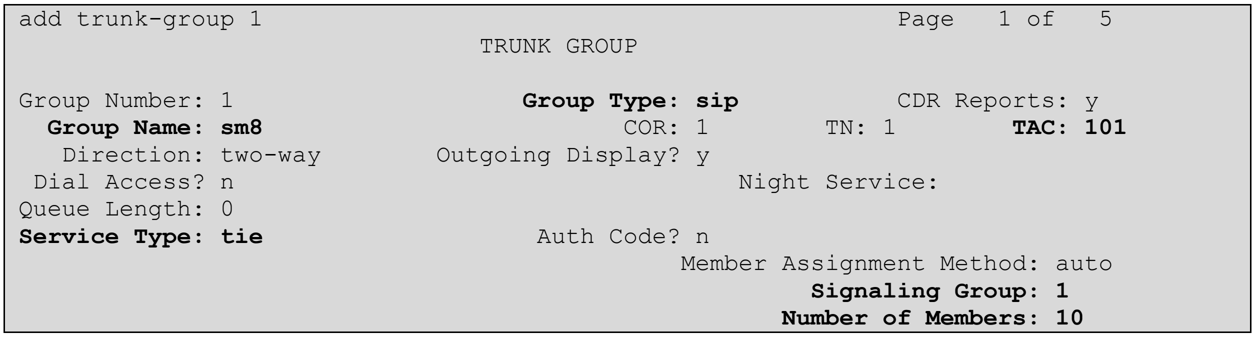


```
add signaling-group 1                                        Page   1 of   3
                                SIGNALING GROUP

 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
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 65                    IP Audio Hairpinning? y
         Enable Layer 3 Test? y
                                                  Alternate Route Timer(sec): 6
```

5.3 Administer SIP Trunk Group

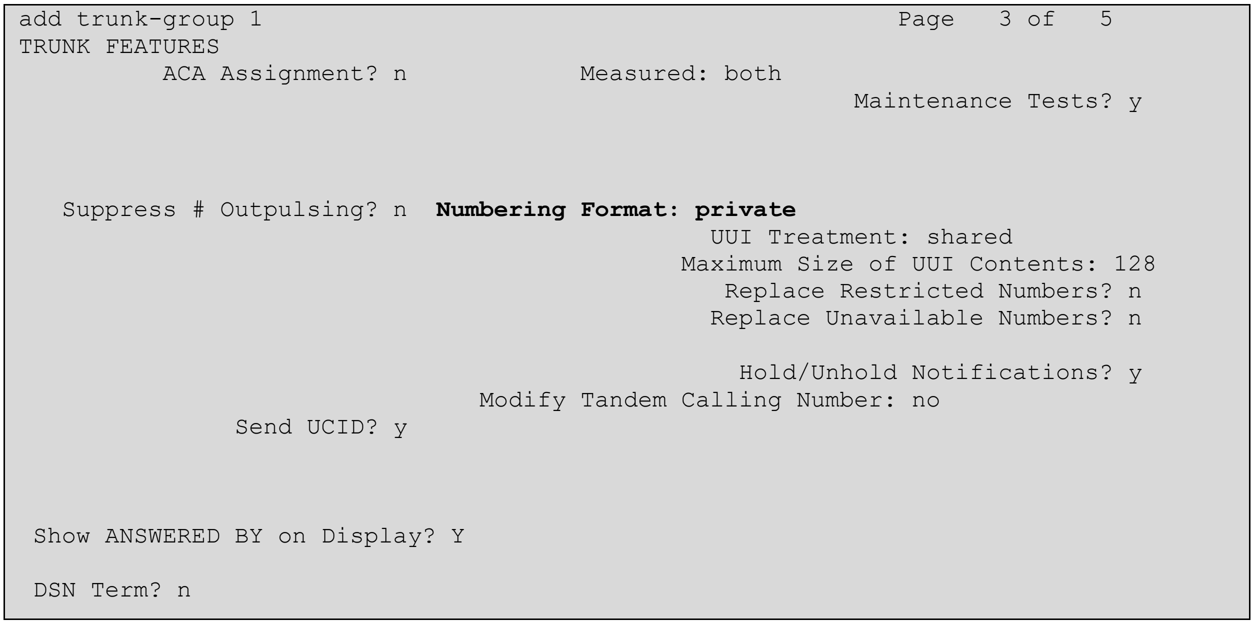
Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “1”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **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.



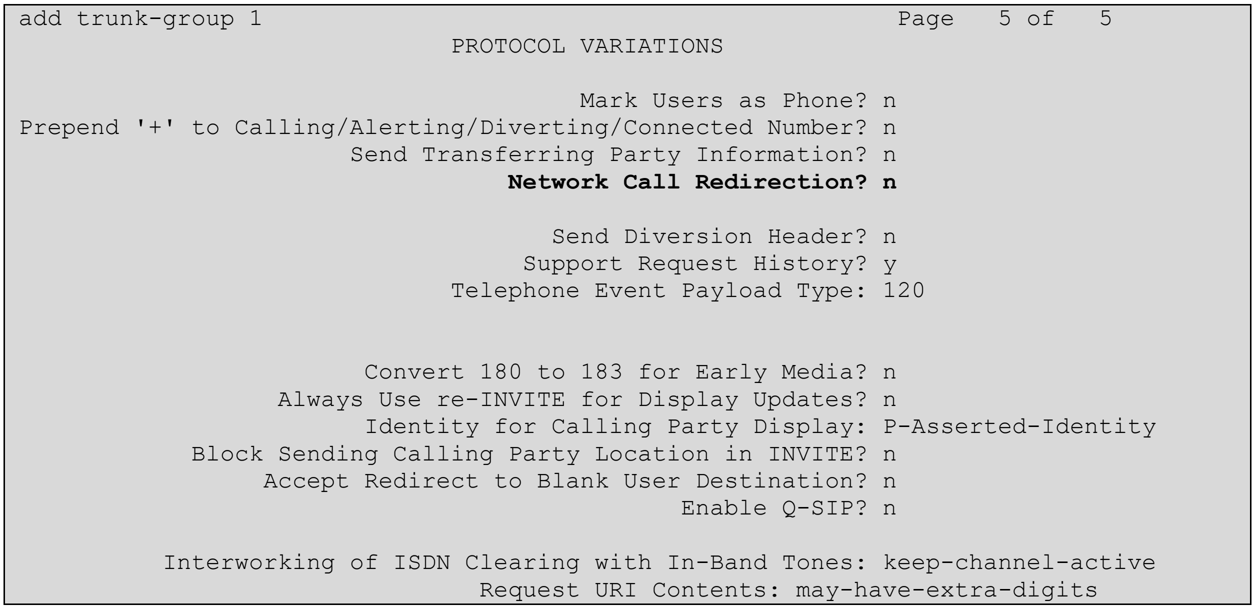
```
add trunk-group 1                                            Page   1 of   5
                                TRUNK GROUP

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.

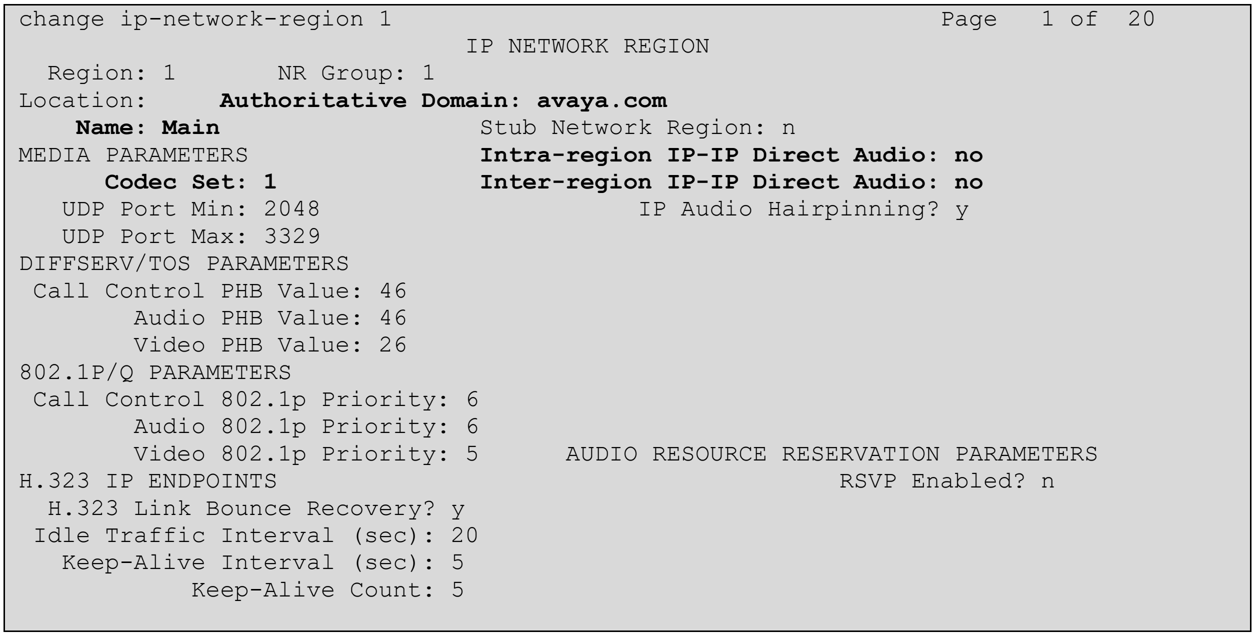


```
add trunk-group 1                                            Page   5 of   5
                              PROTOCOL VARIATIONS

                                       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? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                      Request URI Contents: may-have-extra-digits
```

5.4 Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.3**.

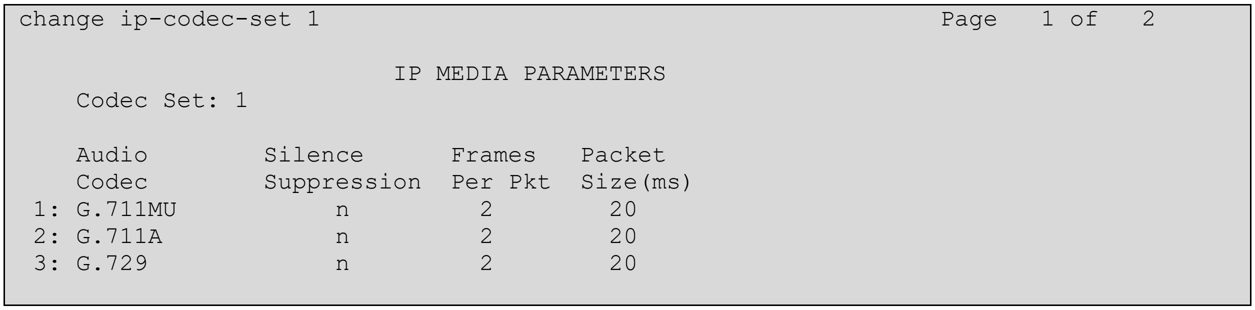
For **Authoritative Domain**, set to “avaya.com”. Enter a descriptive **Name**. Enter “no” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with Unigy.



```
change ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location:     Authoritative Domain: avaya.com
    Name: 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.

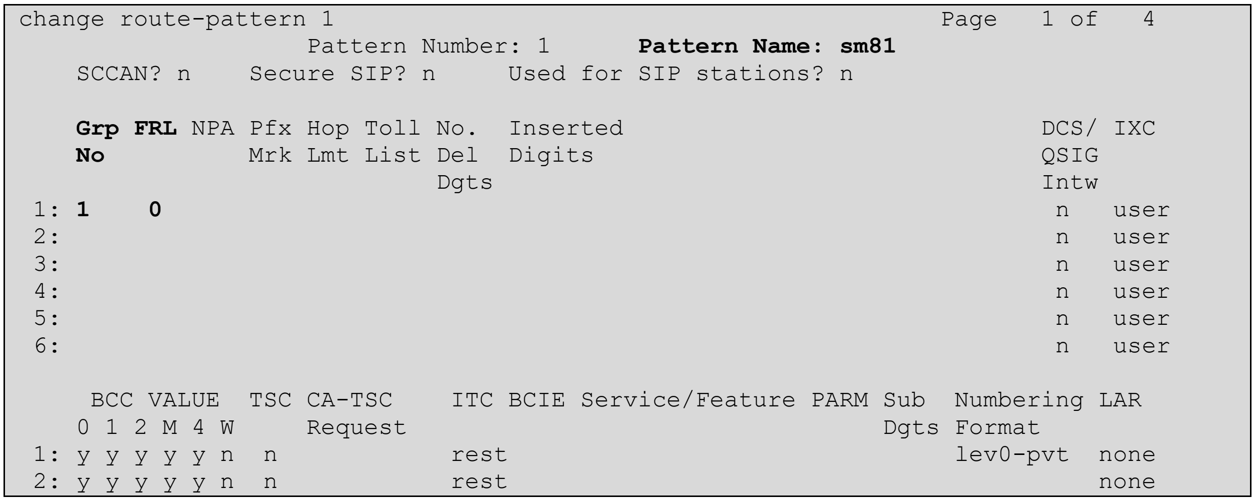


```
change ip-codec-set 1                                         Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 1

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

5.6 Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach IPC, in this case “1”. Enter the following values for the specified fields and retain the default values for the remaining fields.

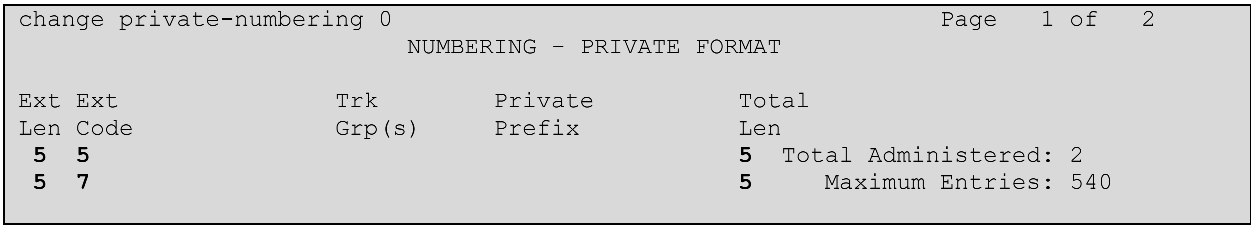
- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.3**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.



```
change route-pattern 1                                          Page   1 of   4
                    Pattern Number: 1      Pattern Name: 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 y n  n            rest                               lev0-pvt  none
 2: y y y y y n  n            rest                                         none
```

5.7 Administer Private Numbering

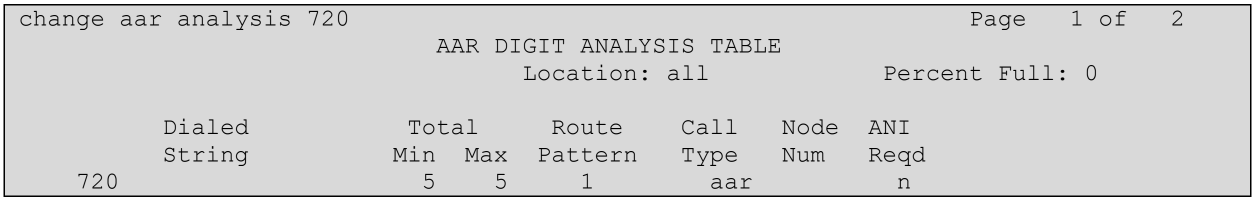
Use the “change private-numbering 0” command, to define the calling party number to send to IPC. In the example shown below, all calls originating from a 5-digit extension beginning with 5 or 7 will result in a 5 digits calling number. The calling party number will be in the SIP “From” header.



```
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
```

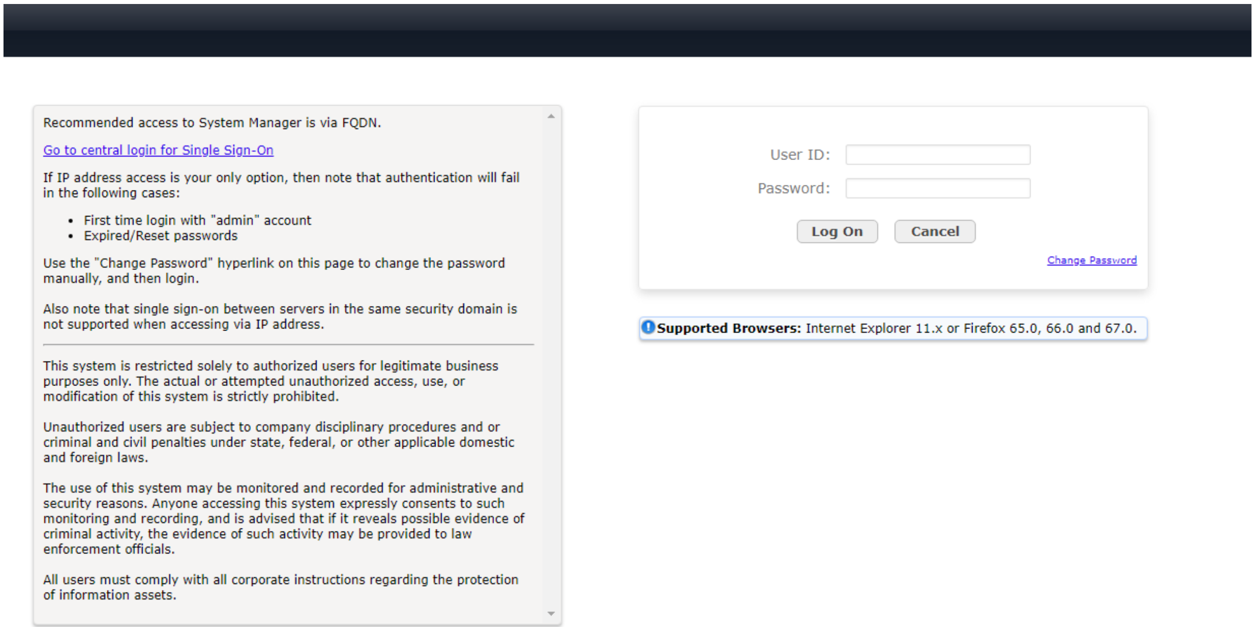
6 Configure Avaya Aura® Session Manager

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:

- 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.

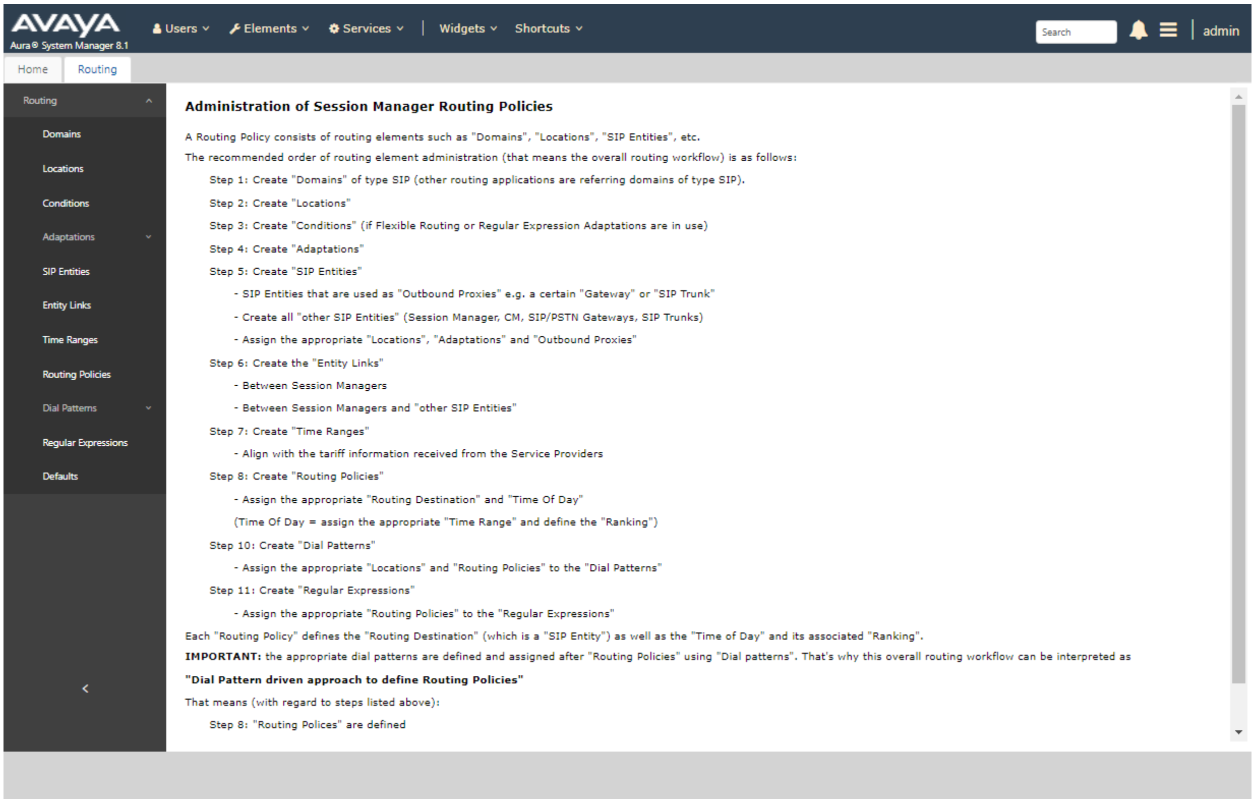
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law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

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

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



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"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 11: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

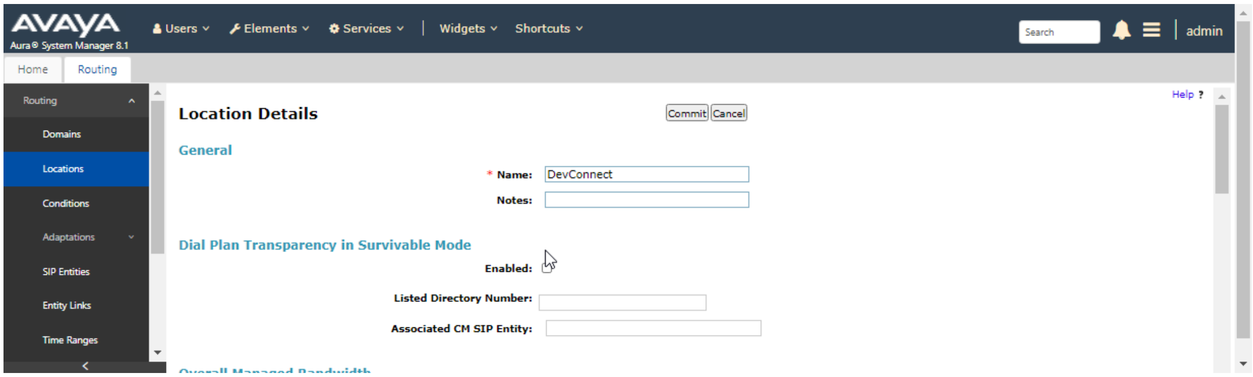
IMPORTANT: the appropriate dial patterns are defined and assigned after "Routing Policies" using "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 8: "Routing Polices" are defined

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. In the **Location Pattern** sub-section, click **Add** and enter the applicable **IP Address Pattern** (not shown). Retain the default values in the remaining fields.



Location Details

General

* Name: DevConnect

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

6.3 Adaptations

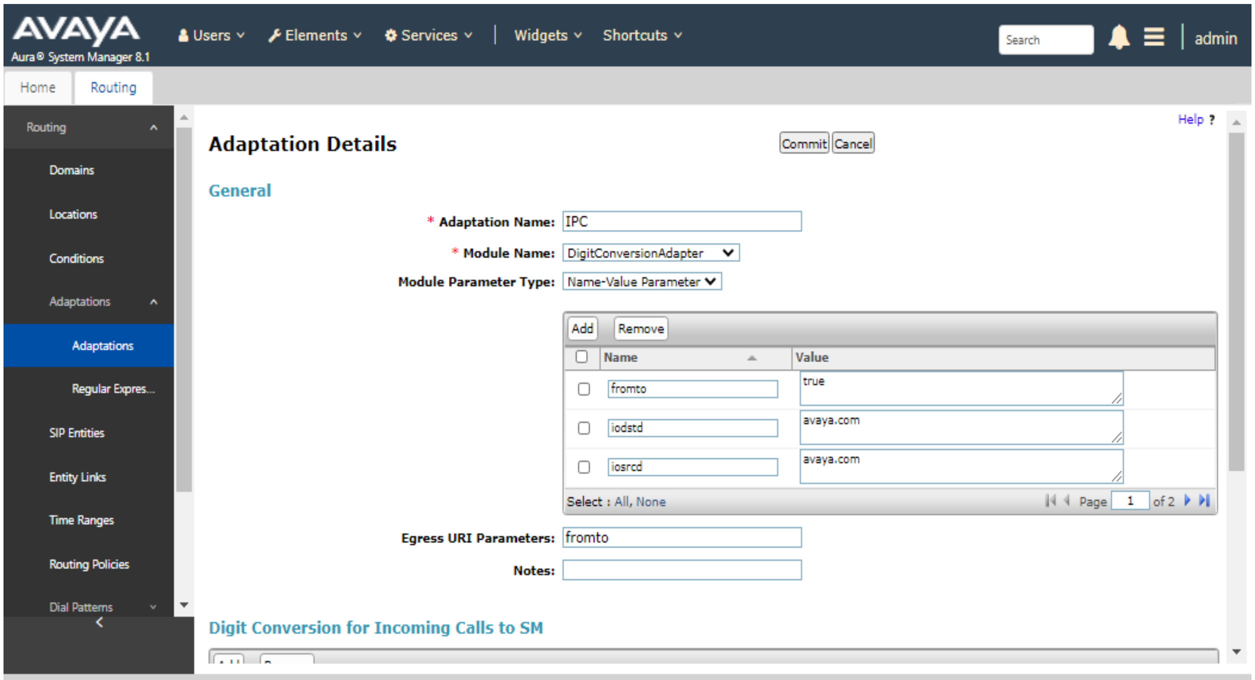
Add an adaptation to translate incoming/outgoing SIP headers. Select **Adaptations →** **Adaptations** from the left pane and click **New** (not shown) to add a new adaptation for IPC.

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”
- **Egress URI Parameters:** fromto

Click Add to add the adaption name value pairs as specified

- **fromto** true
- **iodstd** avaya.com
- **iosrcd** avaya.com
- **odstd:** ipc.com
- **osrcd:** 10.64.110.212 (the session manager IP address)



Adaptation Details

General

* Adaptation Name: IPC

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

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

Egress URI Parameters: fromto

Notes:

Digit Conversion for Incoming Calls to SM

6.4 Administer SIP Entities

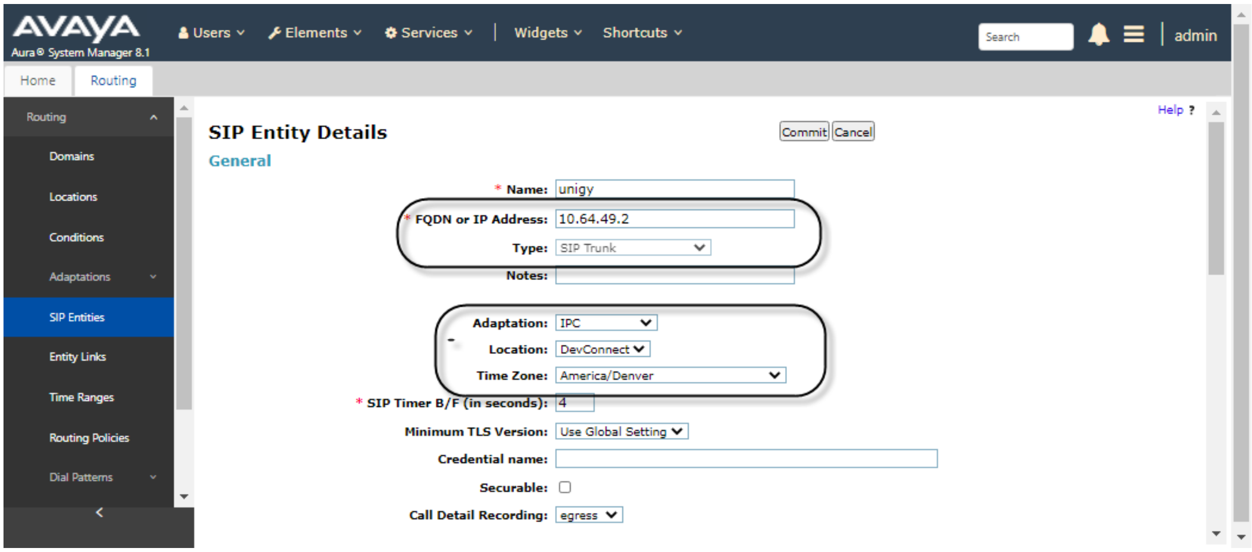
Add two new SIP entities, one for IPC, and another for the new SIP trunks for Communication Manager.

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.



SIP Entity Details

General

* 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: □

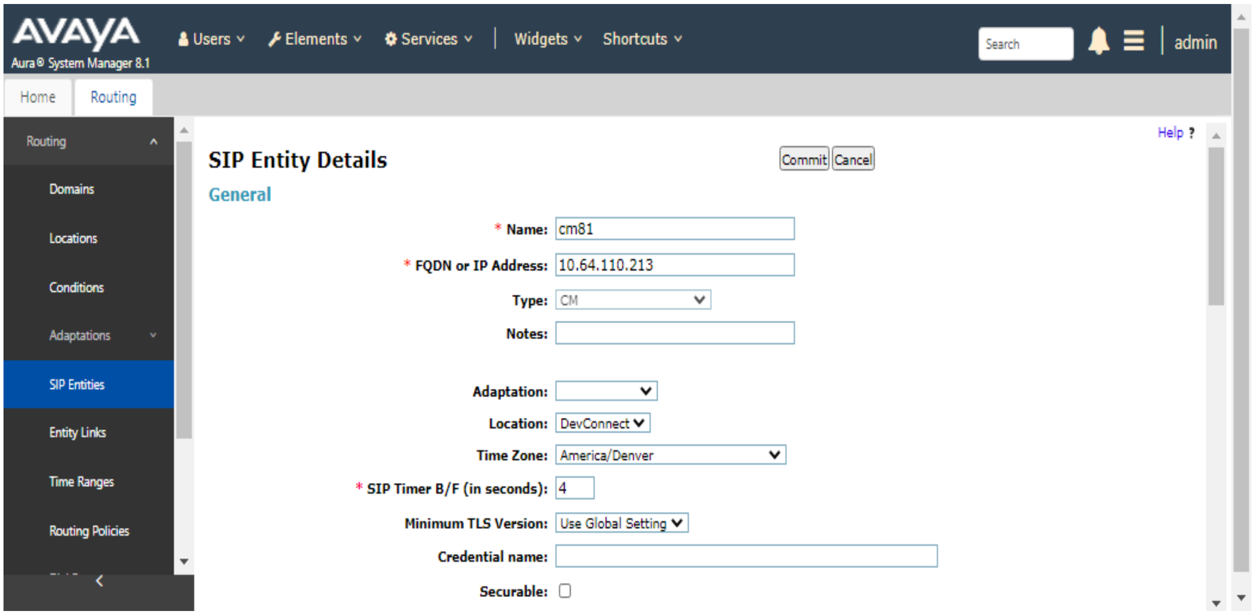
Call Detail Recording: egress

6.4.2 Communication Manager SIP Entity

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

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

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



SIP Entity Details

General

* Name: cm81

* FQDN or IP Address: 10.64.110.213

Type: CM

Notes:

Adaptation:

Location: DevConnect

Time Zone: America/Denver

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: □

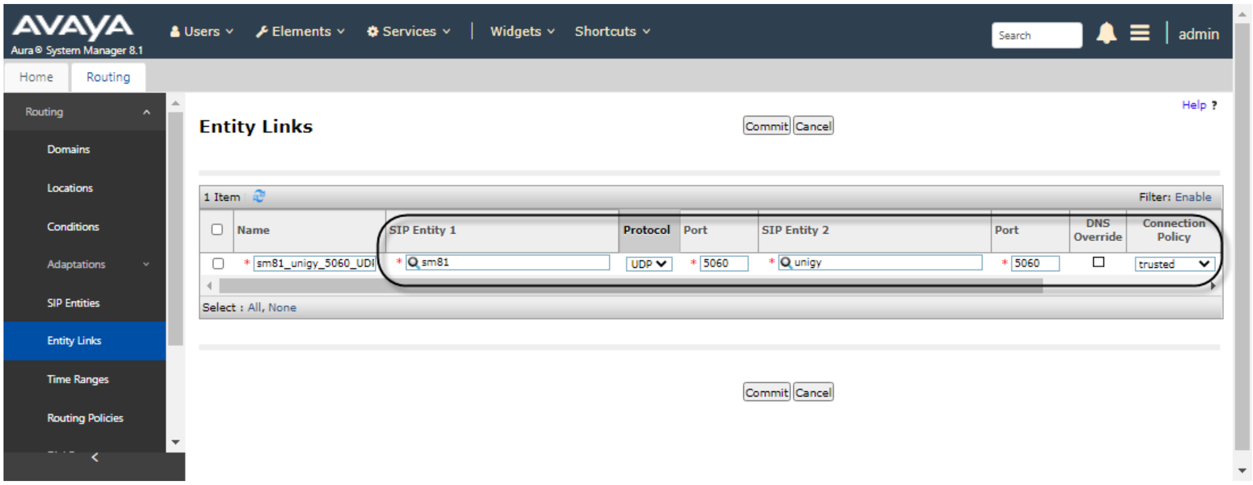
6.5 Administer Entity Links

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.

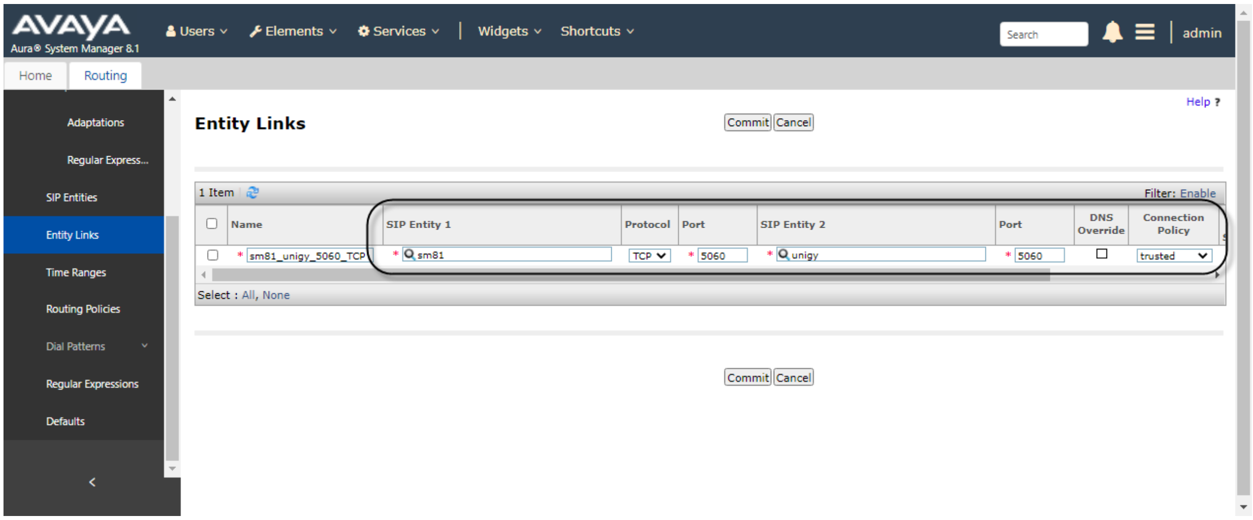
- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name
- **Protocol:** "UDP"
- **Port:** "5060"
- **SIP Entity 2:** The IPC entity name from **Section 6.4.1**.
- **Port:** "5060"
- **Connection Policy:** "Trusted"



Entity Links

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
☐	* sm81_unigy_5060_UDI	* sm81	UDP	* 5060	* unigy	* 5060	☐	trusted

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



Entity Links

1 Item   Filter: Enable

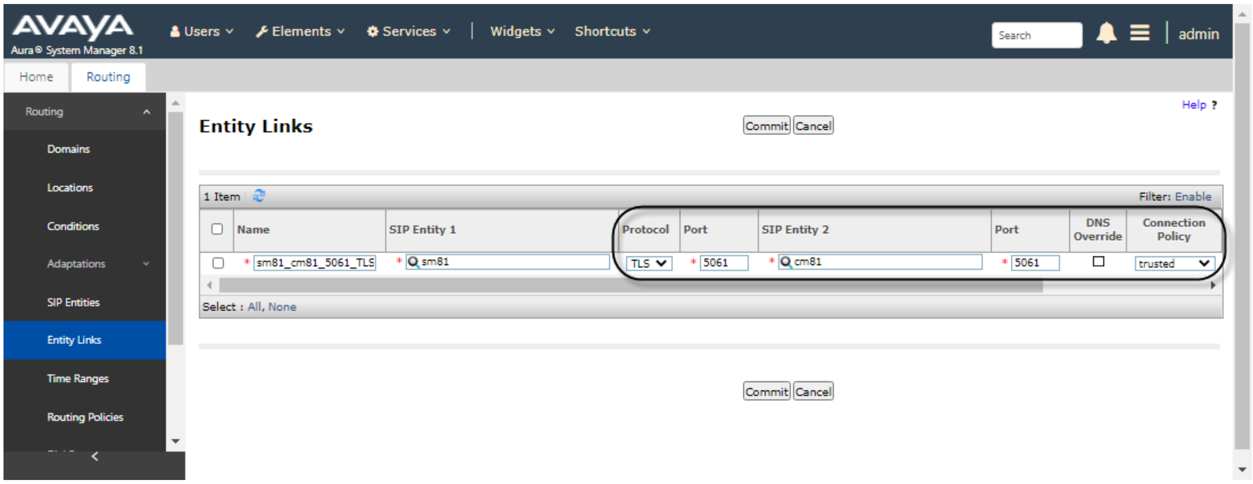
□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
□	* sm81_unigy_5060_TCP	* sm81	TCP	* 5060	* unigy	* 5060	□	trusted

Select : All, None

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



Entity Links

1 Item | Filter: Enable

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
☐	* sm81_cm81_5061_TLS	* sm81	TLS	* 5061	* cm81	* 5061	☐	trusted

Select : All, None

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.

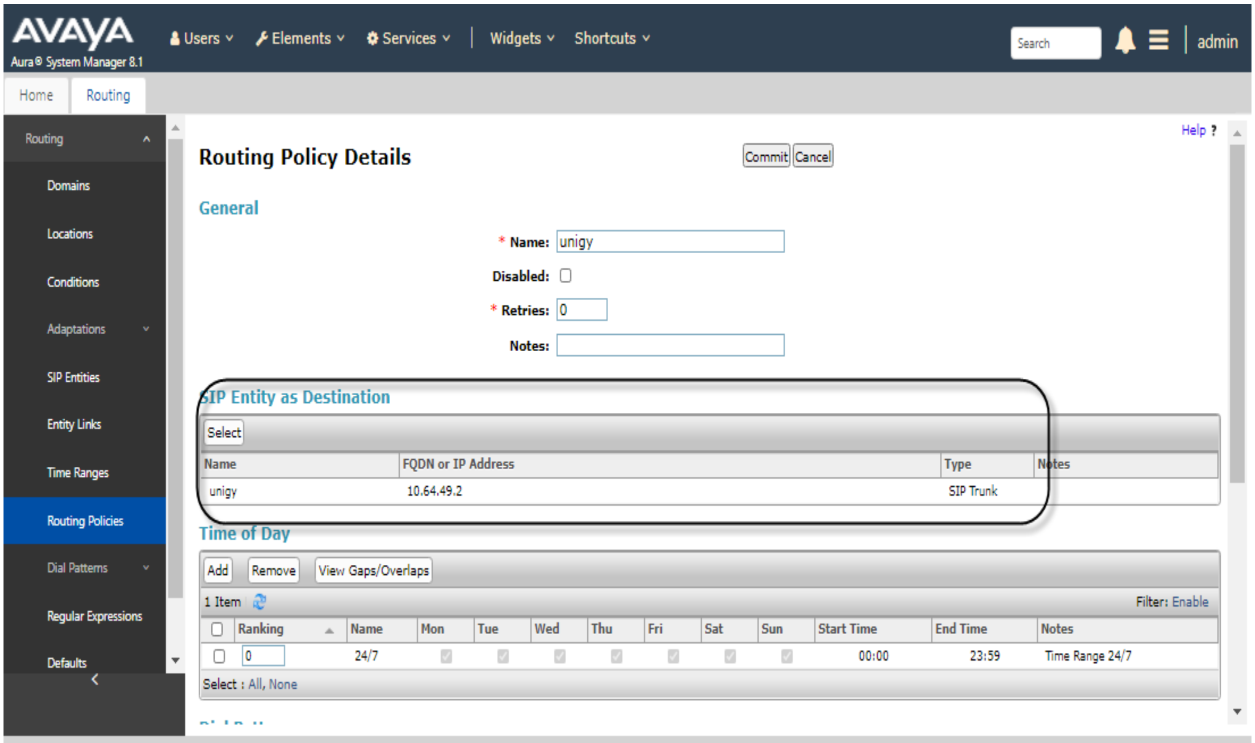
6.6.1 IPC Routing Policy

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. In the **General** sub-section, enter a descriptive **Name**.

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

Retain the default values in the remaining fields.



Routing Policy Details

General

* Name: 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	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

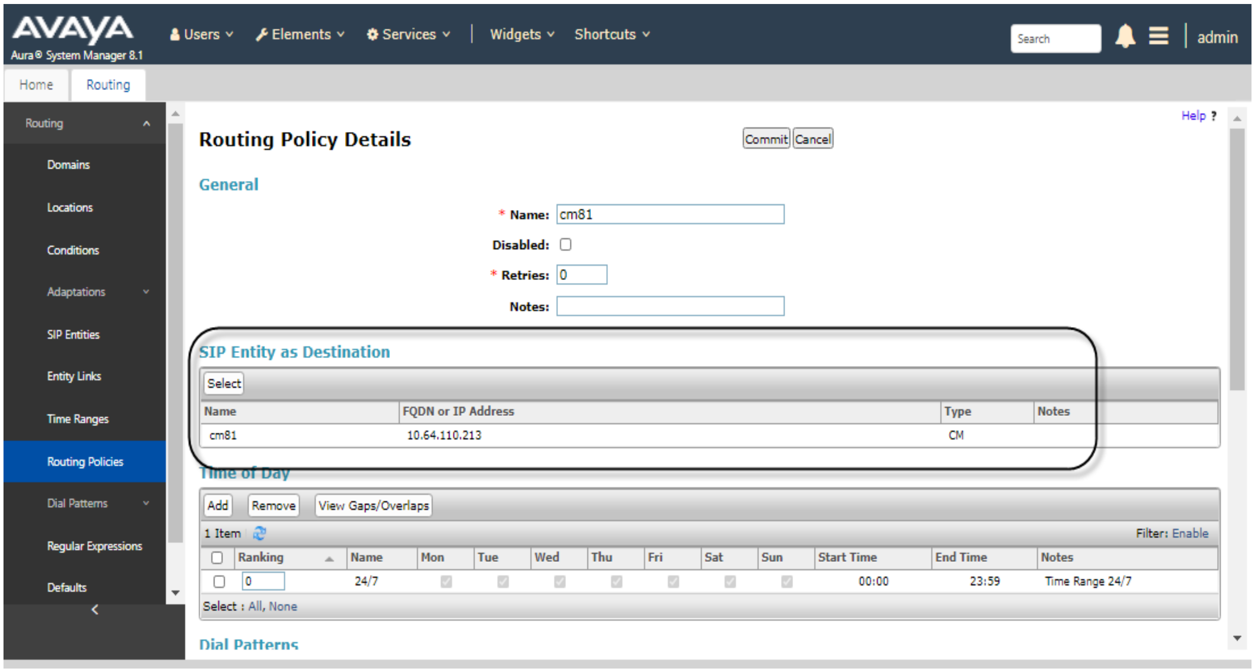
6.6.2 Communication Manager Routing Policy

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

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

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

Retain the default values in the remaining fields.



Routing Policy Details

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

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	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

6.7 Administer Dial Patterns

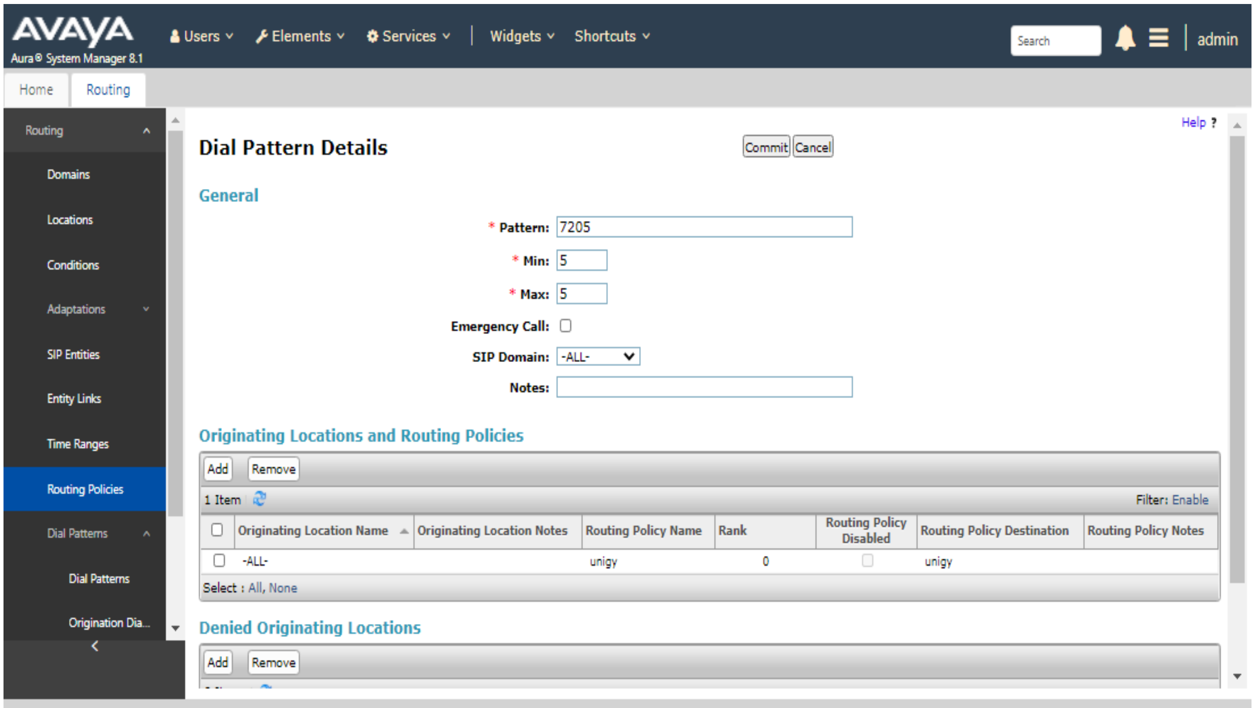
Add a new dial pattern for IPC and update the existing dial pattern for Communication Manager.

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:** Select "ALL".
- **Notes:** Any desired description.

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



Dial Pattern Details

General

* Pattern: 7205

* Min: 5

* Max: 5

Emergency Call: □

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

1 Item

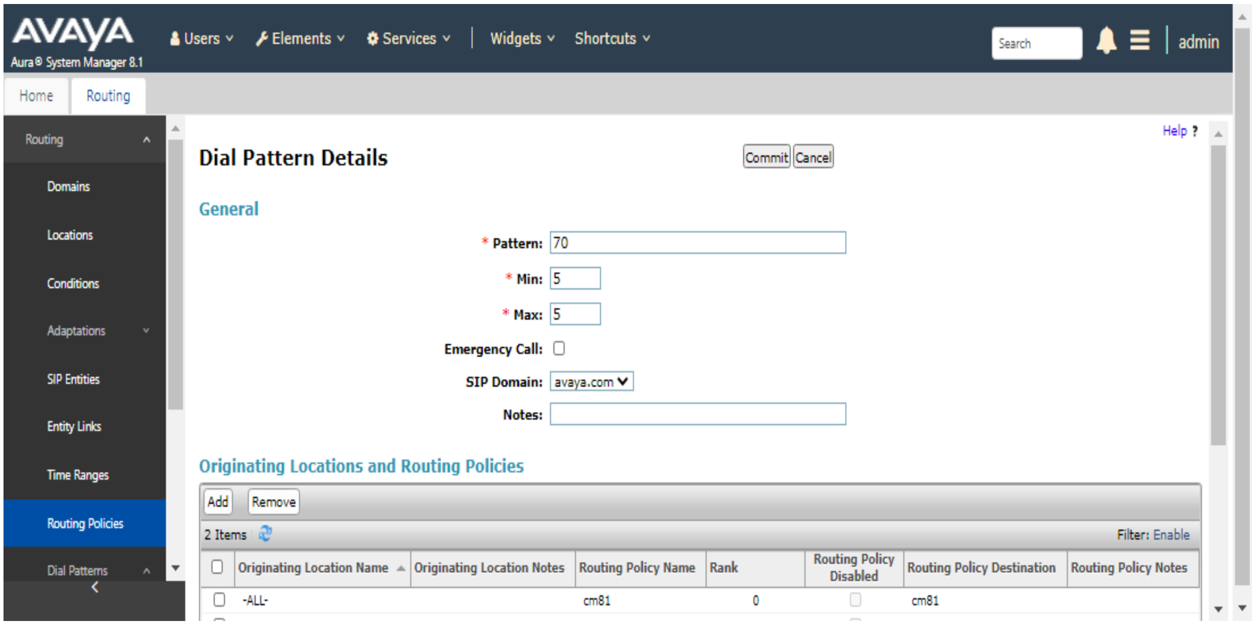
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		unigy	0	□	unigy	

Denied Originating Locations

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.



Dial Pattern Details

Commit Cancel

General

* Pattern: 70

* Min: 5

* Max: 5

Emergency Call: □

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items

Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		cm81	0	□	cm81	

7 Configure IPC Unigy V4.3 Converged Communication Manager

This section provides the procedures for configuring IPC Unigy V4.3 Converged Communication Manager. The procedures include the following areas:

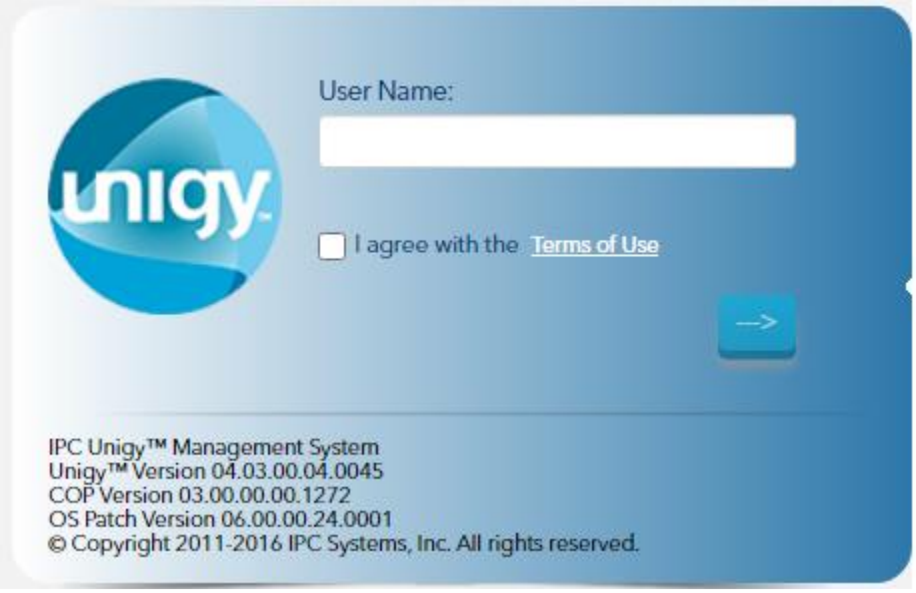
- Launch Unigy Management System
- Administer SIP trunks
- Administer trunk groups
- Administer route lists
- Administer zone dial patterns
- Administer route plans

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

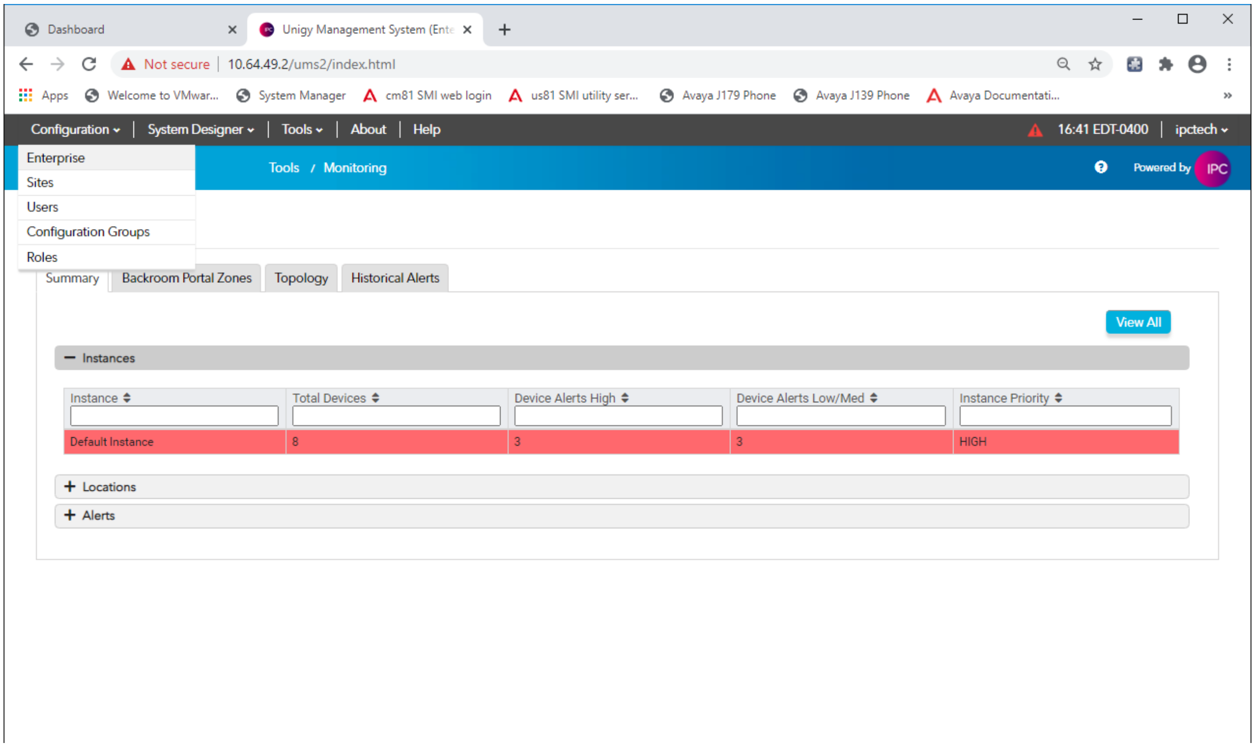
Access the Unigy Management System web interface by using the URL http://ip-address in an Internet browser window, where "ip-address" is the VIP of the Zone or in a standalone environment is the IP address of the CCM. Log in using appropriate credentials.

The screen below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use** and click **Login**.
In the subsequent screen (not shown), click **Continue**.



IPC Unigy™ Management System
Unigy™ Version 04.03.00.04.0045
COP Version 03.00.00.00.1272
OS Patch Version 06.00.00.24.0001
© Copyright 2011-2016 IPC Systems, Inc. All rights reserved.

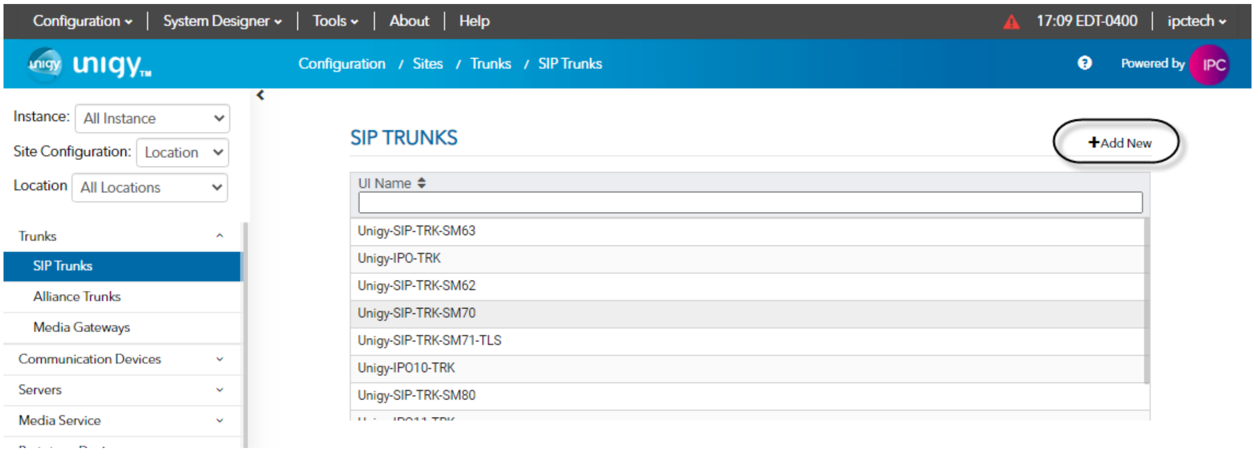
The following screen (Tools -> Monitoring) displays. Navigate to **Configuration → Sites** under the main menu.



Instance	Total Devices	Device Alerts High	Device Alerts Low/Med	Instance Priority
Default Instance	8	3	3	HIGH

7.2 Administer SIP Trunks

Select **Trunks → SIP Trunks** in the left pane and click the **Add New** icon in the upper right pane to add a new SIP trunk. Select "Dial Tone" from the **Select Connection Type** drop-down list.



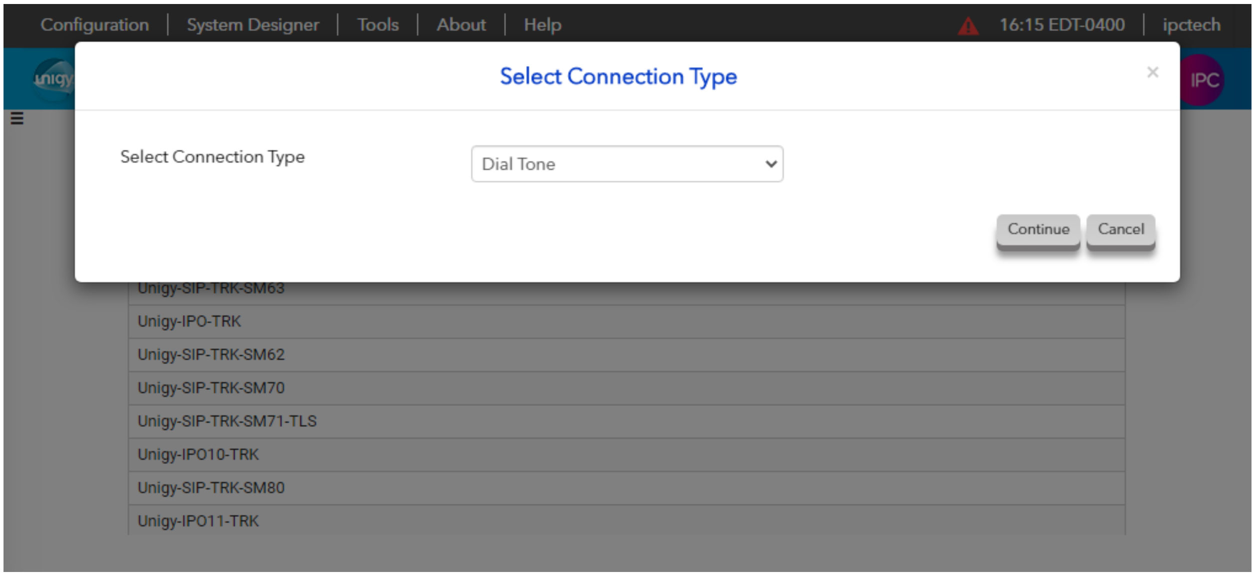
Instance: All Instance

Site Configuration: Location

Location: All Locations

SIP TRUNKS

UI Name
Unigy-SIP-TRK-SM63
Unigy-IPO-TRK
Unigy-SIP-TRK-SM62
Unigy-SIP-TRK-SM70
Unigy-SIP-TRK-SM71-TLS
Unigy-IPO10-TRK
Unigy-SIP-TRK-SM80



Select Connection Type

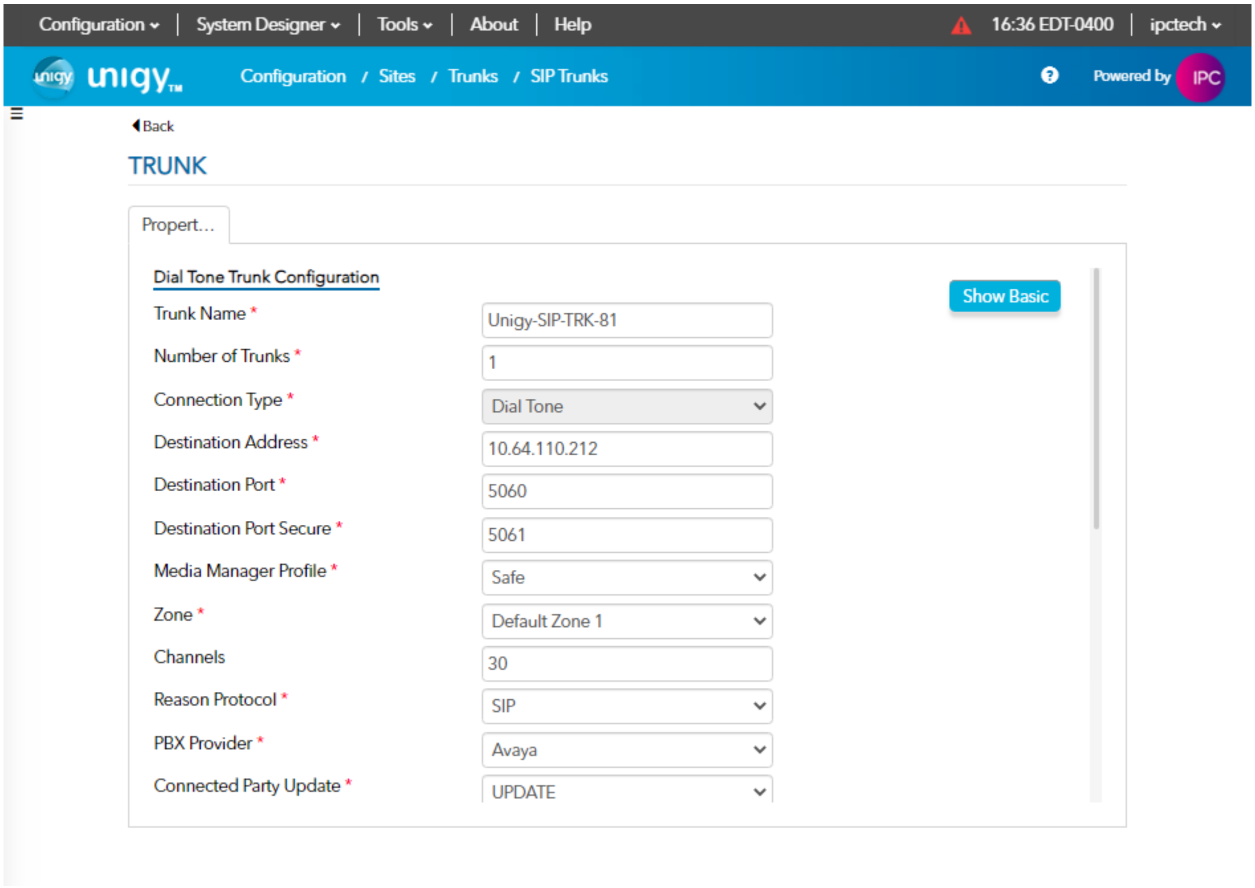
Select Connection Type: Dial Tone

Unigy-SIP-TRK-SM63
Unigy-IPO-TRK
Unigy-SIP-TRK-SM62
Unigy-SIP-TRK-SM70
Unigy-SIP-TRK-SM71-TLS
Unigy-IPO10-TRK
Unigy-SIP-TRK-SM80
Unigy-IPO11-TRK

The screen below is displayed next. Select “Advanced” on the top right, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Trunk Name:** A descriptive name.
- **Destination Address:** IP address of the Session Manager signaling interface.
- **Destination Port:** The port number from **Section 6.5.1**.
- **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.



TRUNK

Dial Tone Trunk Configuration

Trunk Name * Unigy-SIP-TRK-81

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

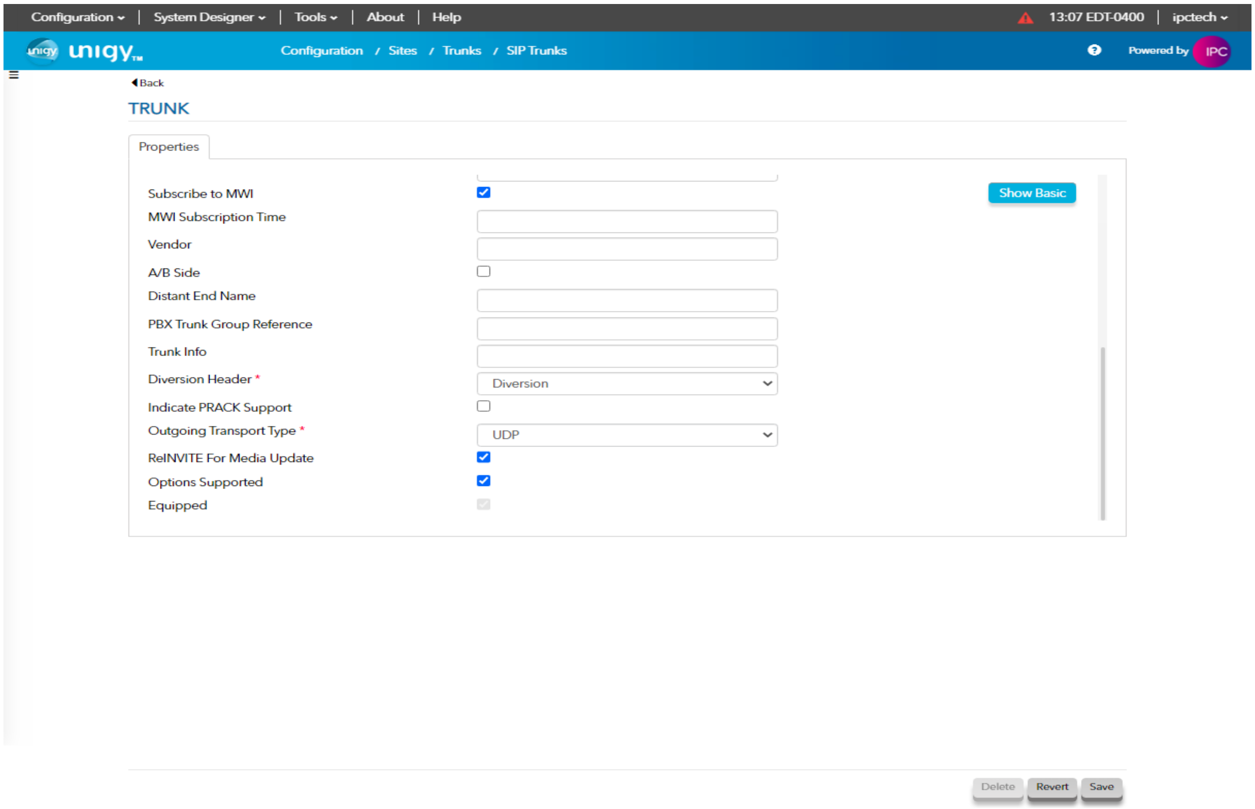
Zone * Default Zone 1

Channels 30

Reason Protocol * SIP

PBX Provider * Avaya

Connected Party Update * UPDATE



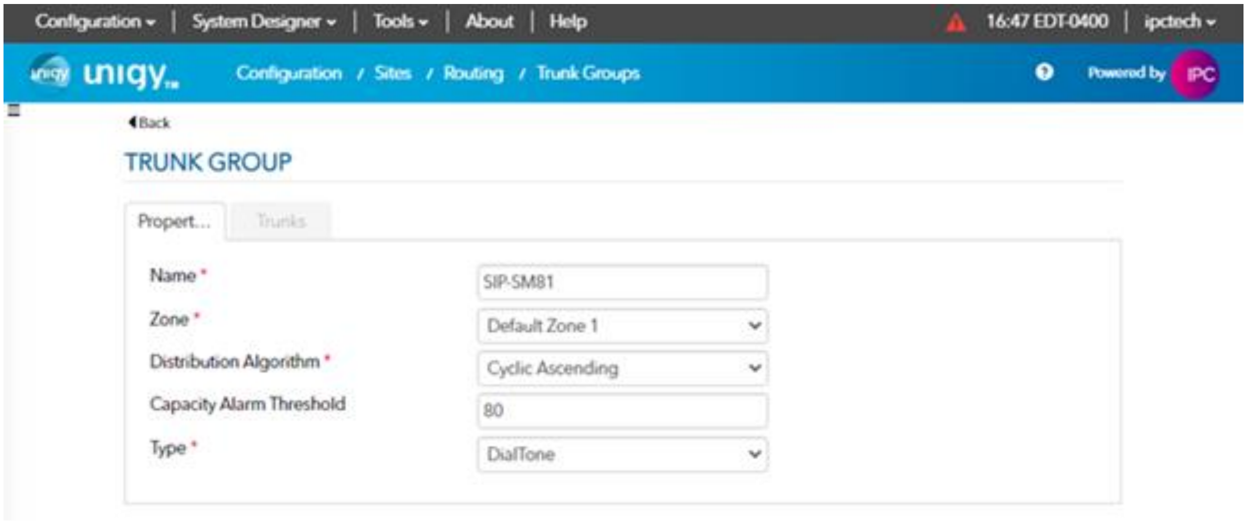
TRUNK

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	☑

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**.


Configuration ▾ | System Designer ▾ | Tools ▾ | About | Help
16:47 EDT-0400 | ipctech ▾
unigy
Configuration / Sites / Routing / Trunk Groups
Powered by IPC
Back
Propert...
Trunks

TRUNK GROUP

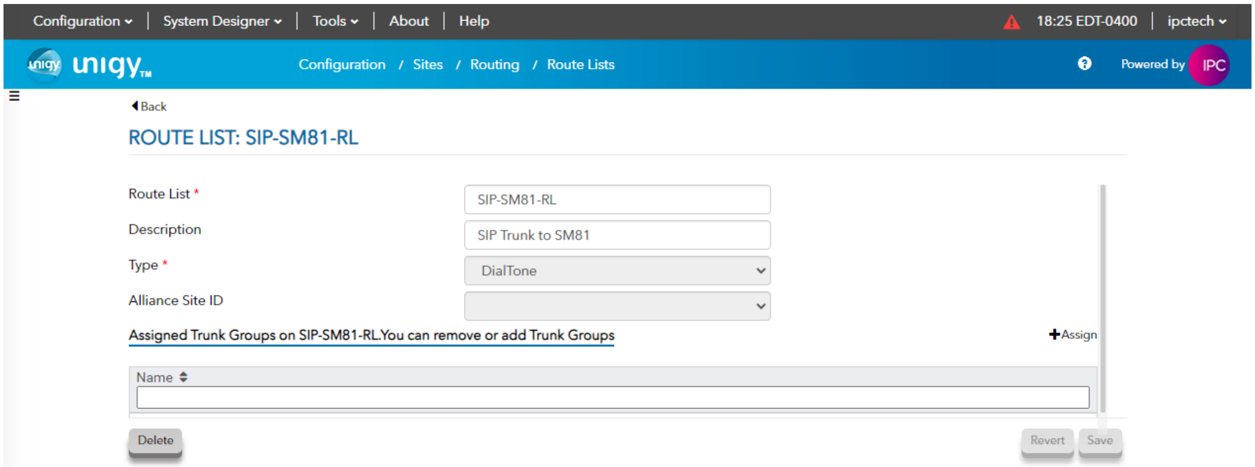
Name *	SIP-SM81
Zone *	Default Zone 1
Distribution Algorithm *	Cyclic Ascending
Capacity Alarm Threshold	80
Type *	DialTone

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 **+AddNew** icon in the upper right to add a new route list.

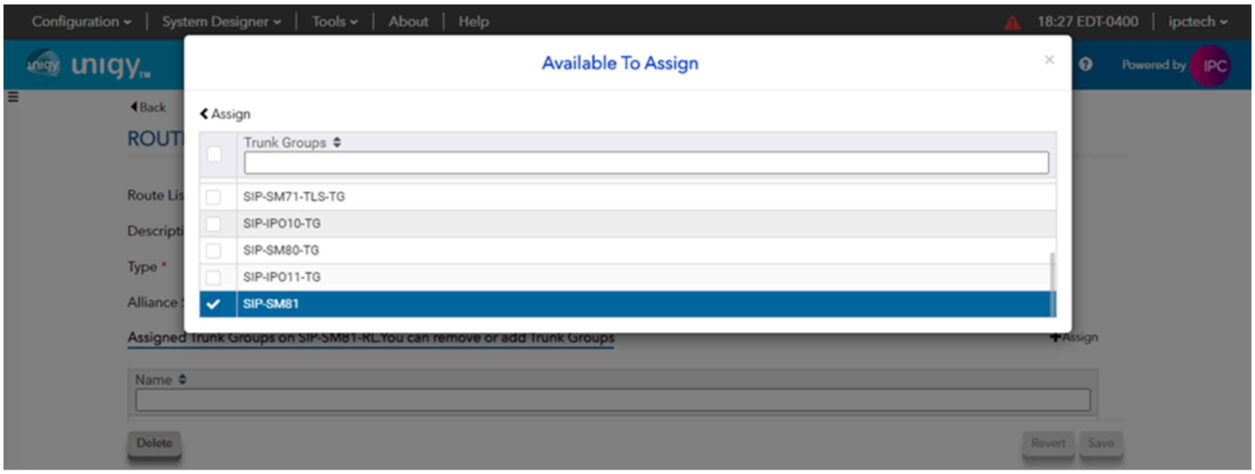
The **Route List** screen is displayed. For **Route List**, enter a descriptive name. Input a description in the **Description** field if desired.


Configuration
System Designer
Tools
About
Help
18:25 EDT-0400
ipctech
unigy
Configuration / Sites / Routing / Route Lists
Powered by IPC
Back
Assigned Trunk Groups on SIP-SM81-RL.You can remove or add Trunk Groups
+Assign
Name
Delete
Revert
Save

ROUTE LIST: SIP-SM81-RL

Route List *	SIP-SM81-RL
Description	SIP Trunk to SM81
Type *	DialTone
Alliance Site ID	

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**.



Available To Assign

<Assign

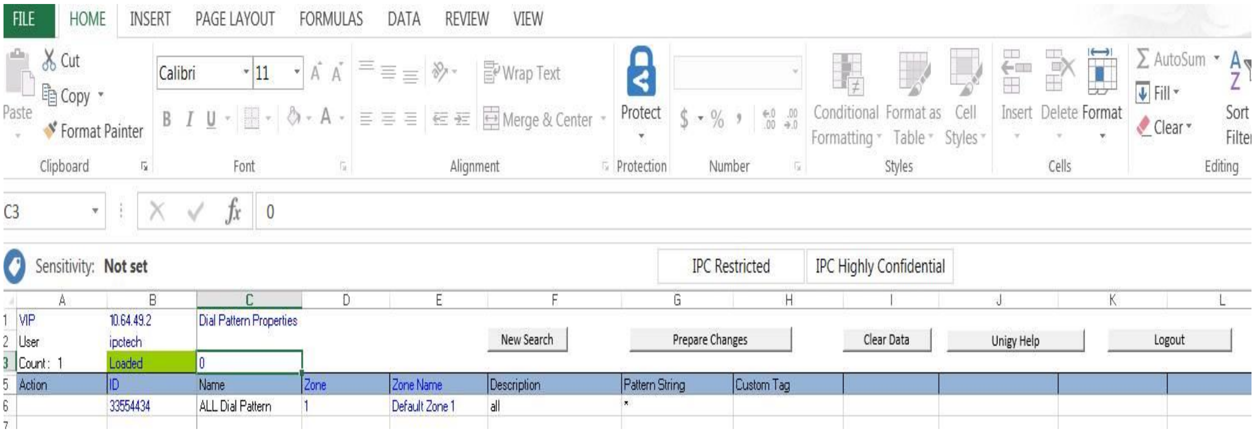
	Trunk Groups
□	SIP-SM71-TLS-TG
□	SIP-IPO10-TG
□	SIP-SM80-TG
□	SIP-IPO11-TG
☑	SIP-SM81

Assigned Trunk Groups on SIP-SM81-RL.You can remove or add Trunk Groups

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:** **Default** Zone 1
- **Description:** all
- **Pattern String:** *

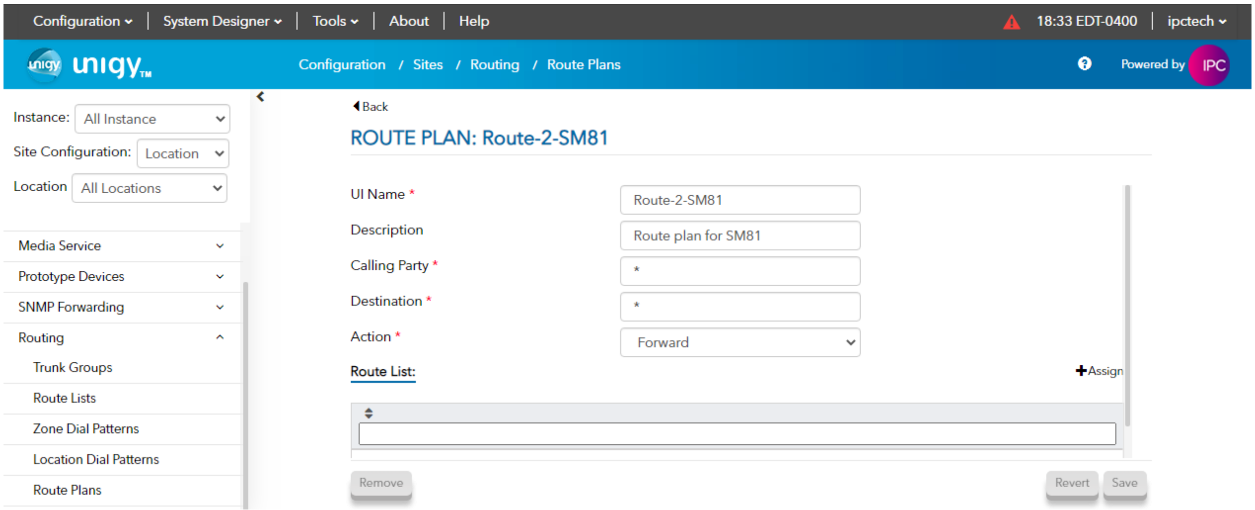


	A	B	C	D	E	F	G	H
1	VIP	10.64.49.2	Dial Pattern Properties					
2	User	ipctech						
3	Count : 1	Loaded	0					
5	Action	ID	Name	Zone	Zone Name	Description	Pattern String	Custom Tag
6		33554434	ALL Dial Pattern	1	Default Zone 1	all	*	

7.6 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" (not shown). Click **Save**.



ROUTE PLAN: Route-2-SM81

UI Name * Route-2-SM81

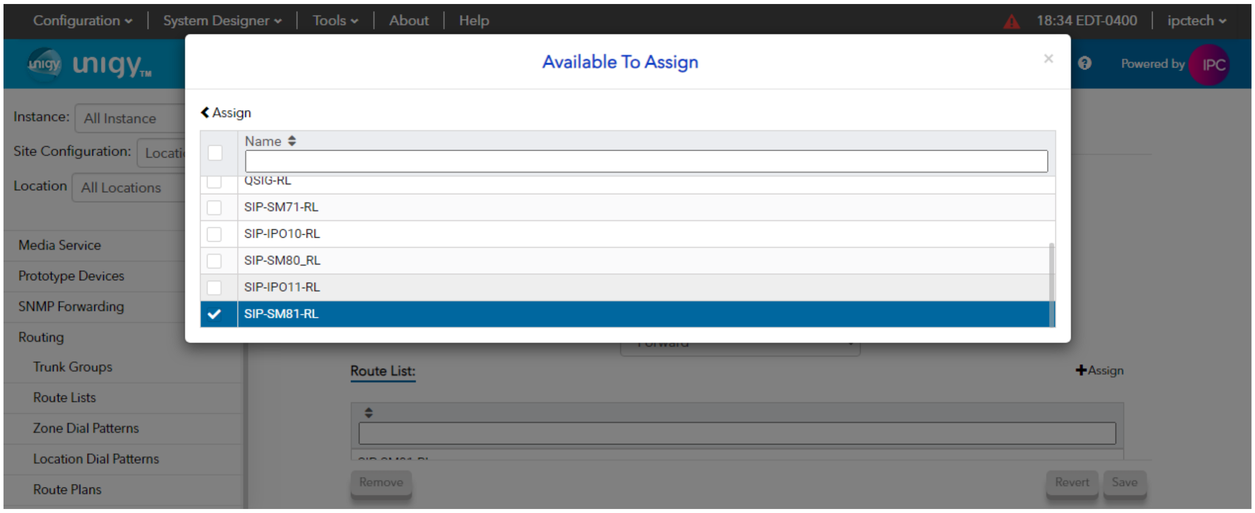
Description Route plan for SM81

Calling Party * *

Destination * *

Action * Forward

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**.



Available To Assign

< Assign

	Name
□	QSIG-RL
□	SIP-SM71-RL
□	SIP-IPO10-RL
□	SIP-SM80_RL
□	SIP-IPO11-RL
✓	SIP-SM81-RL

8 Verification Steps

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

8.1 Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.3**. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 1

                             TRUNK GROUP STATUS

Member    Port    Service State      Mtce Connected Ports
                                     Busy

0001/0001 T00001  in-service/idle    no
0001/0002 T00002  in-service/idle    no
0001/0003 T00003  in-service/idle    no
0001/0004 T00004  in-service/idle    no
0001/0005 T00005  in-service/idle    no
0001/0006 T00006  in-service/idle    no
0001/0007 T00007  in-service/idle    no
0001/0008 T00008  in-service/idle    no
0001/0009 T00009  in-service/idle    no
0001/0010 T00010  in-service/idle    no
```

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.2**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

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

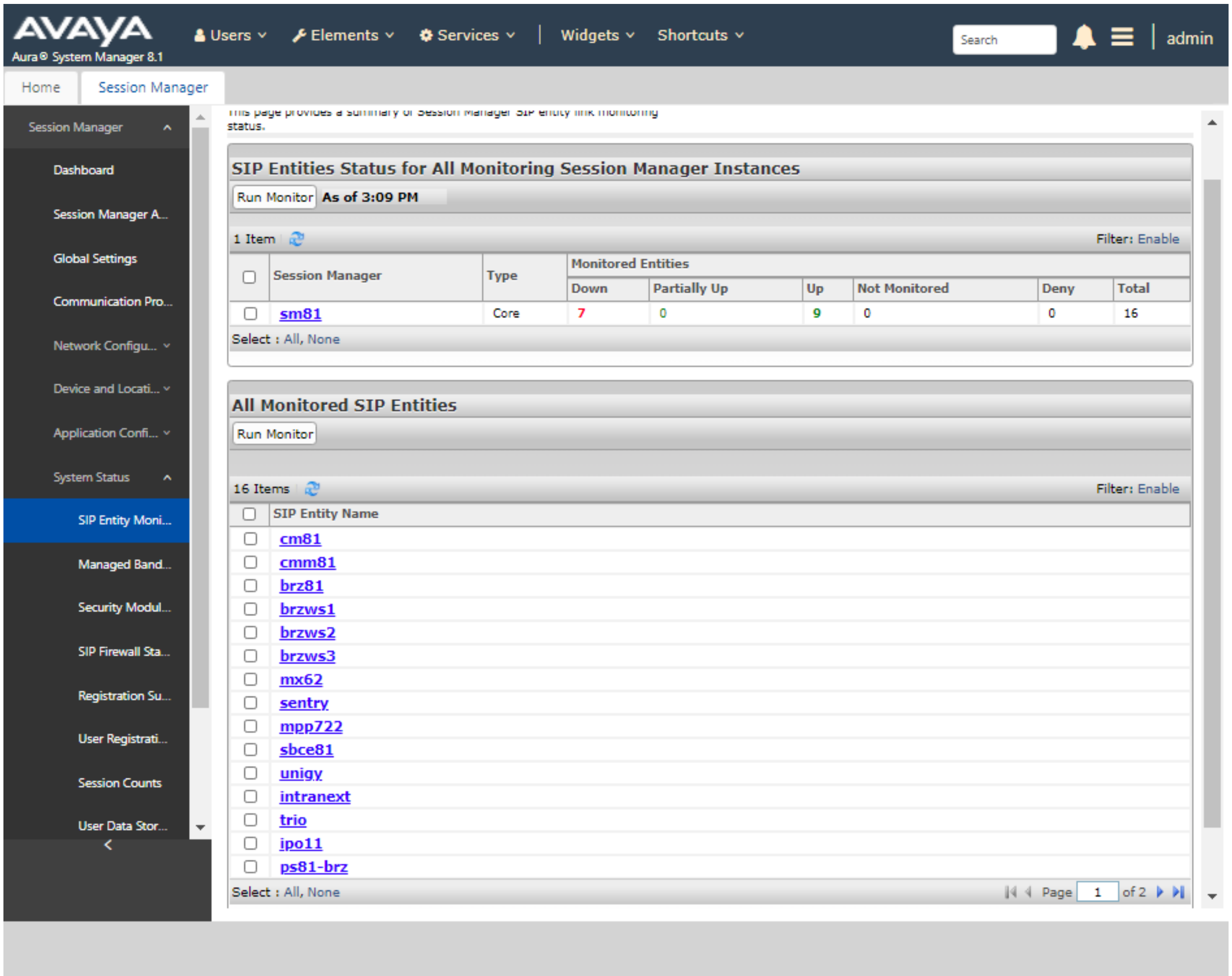
```
change ip-codec-set 1                                           Page   1 of   2

                          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**.



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 3:09 PM**

1 Item Filter: Enable

□	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
□	sm81	Core	7	0	9	0	0	16

Select : All, None

All Monitored SIP Entities

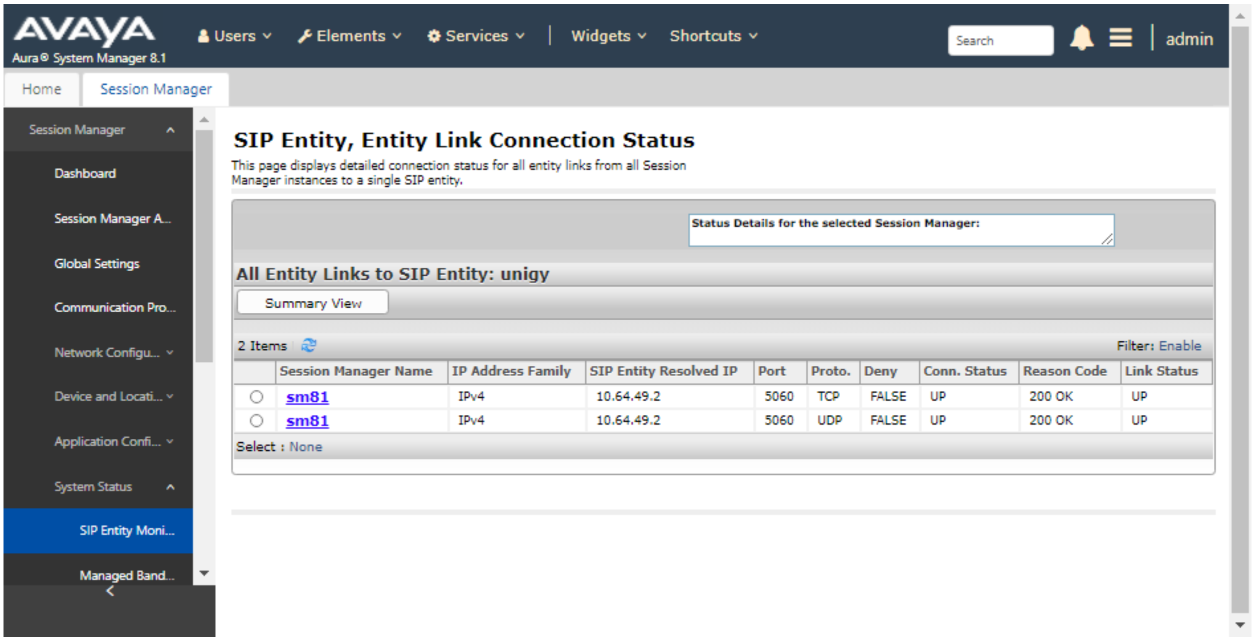
Run Monitor

16 Items Filter: Enable

□	SIP Entity Name
□	cm81
□	cmm81
□	brz81
□	brzws1
□	brzws2
□	brzws3
□	mx62
□	sentry
□	mpp722
□	sbce81
□	unigy
□	intranext
□	trio
□	ipo11
□	ps81-brz

Select : All, None Page 1 of 2

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



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

2 Items Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	sm81	IPv4	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
○	sm81	IPv4	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP

Select : None

8.3 Verify IPC Unigy

Make a call from an IPC turret user to an Avaya endpoint. Verify that the call can be connected with two-way talk paths.

9 Conclusion

These Application Notes describe the configuration steps required for IPC Unigy v4.3 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 6, Release 8.1.x, March 2020
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 9, Release 8.1.x, June 2020
3. *Administering Avaya Aura® Session Manager*, Issue 5, Release 8.1.x, July 2020
4. *Administering Avaya Aura® System Manager*, Issue 6, Release 8.1.x, April 2020
5. *Unigy 4.03 System Configuration*; available upon request to IPC Support.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.