



Avaya Solution & Interoperability Test Lab

Application Notes for IPC UnigyV2 with Avaya Aura® Communication Manager 6.0.1 using QSIG Trunks, and a direct SIP trunk between Avaya Aura® Communication Manager and Avaya Aura® Messaging – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC UnigyV2 to interoperate with Avaya Aura® Communication Manager 6.0.1 using QSIG trunks, and a direct SIP trunk between Avaya Aura® Communication Manager and Avaya Aura® Messaging.

IPC UnigyV2 is a trading communication solution. In the compliance testing, IPC UnigyV2 used E1 QSIG trunks to Avaya Aura® Communication Manager for turrent users on IPC to reach users on Avaya Aura® Communication Manager and PSTN.

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

1. Introduction

These Application Notes describe the configuration steps required for IPC UnigyV2 to interoperate with Avaya Aura® Communication Manager 6.0.1 using QSIG trunks, and a direct SIP trunk between Avaya Aura® Communication Manager and Avaya Aura® Messaging.

IPC UnigyV2 is a trading communication solution. In the compliance testing, IPC UnigyV2 used E1 QSIG trunks to Avaya Aura® Communication Manager for turret users on IPC to reach users on Avaya Aura® Communication Manager and PSTN.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established from IPC turret users to Avaya SIP, Avaya H.323, and/or PSTN users and vice-a-versa. Call controls were performed from various users to verify the call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the E1 connection to IPC UnigyV2.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, basic display, DTMF, hold/reconnect, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, calling number block from/to PSTN, and conference.

The serviceability testing focused on verifying the ability of IPC UnigyV2 to recover from adverse conditions, such as disconnecting/reconnecting the E1 connection to IPC UnigyV2.

2.2. Test Results

All test cases were executed.

2.3. Support

Technical support on IPC UnigyV2 can be obtained through the following:

- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** systems.support@ipc.com

3. Reference Configuration

As shown in the test configuration below, IPC UnigyV2 at the Remote Site consists of the Media Manager, Converged Communication Manager, Media Gateway, and Turrets. The Media Manager and Converged Communication Manager are typically deployed on separate servers. In the compliance testing, the same server hosted the Media Manager and Converged Communication Manager.

There is a physical connection between the DS1 circuit pack on Avaya Aura® Communication Manager with the IPC Media Gateway. E1 QSIG trunks are used from IPC UnigyV2 to Avaya Aura® Communication Manager, to reach users on Avaya Aura® Communication Manager and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges were associated with Avaya Aura® Communication Manager users at the Central site (4200x), and IPC turret users at the Remote site (7205x).

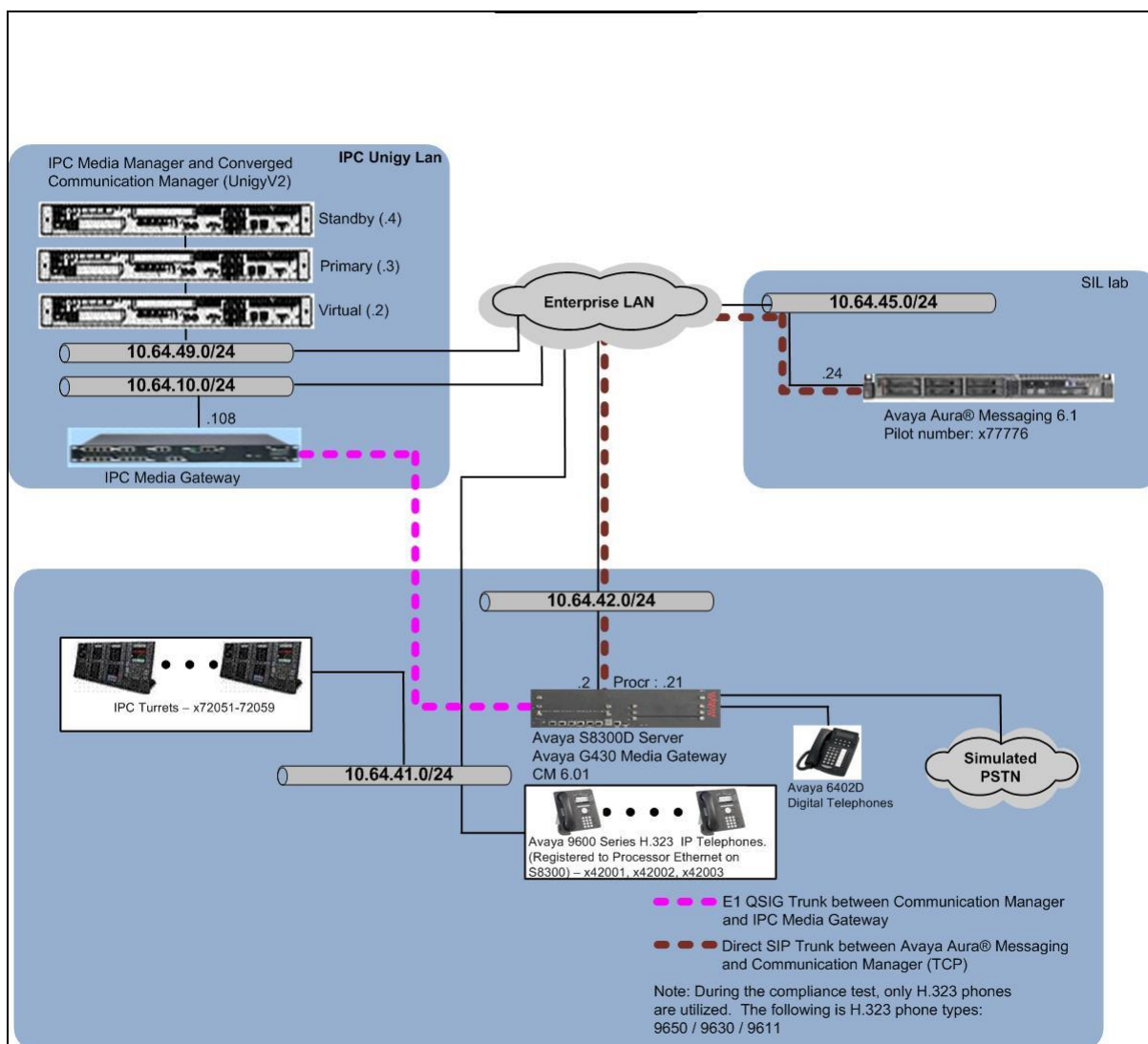


Figure 1: Test Configuration of IPC UnigyV2

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8300D Server	R016x.00.1.510.1-19940
Avaya G430 Media Gateway <ul style="list-style-type: none">TN464HP DS1 Interface	31.26 HW02 FW024
Avaya 9650C Series IP Telephone (H.323)	3.22
Avaya 9630 Series IP Telephone (H.323)	3.22
Avaya 9611 Series IP Telephone (H.323)	6.23
IPC UnigyV2 <ul style="list-style-type: none">Media ManagerConverged Communication ManageMedia GatewayTurrets	02.00.00.07.0025 02.00.00.07.0025 6.40A.073.004 02.00.00.07.0025

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Avaya Aura® Communication Manager.

The procedures include the following areas:

- Verify Communication Manager license
- Administer system parameters special applications
- Administer system parameters features
- Administer system parameters coverage forwarding
- Administer DS1 circuit pack
- Administer ISDN trunk group
- Administer ISDN signaling group
- Administer trunk group members
- Administer route pattern
- Administer public unknown numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer PSTN trunk group
- Administer tandem calling party number
- Administer SIP trunk for Avaya Aura® Messaging
- Administer Signal group for Avaya Aura® Messaging

These steps are performed from the Communication Manager System Access Terminal (SAT) interface.

5.1. Verify Communication Manager License

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 4**, and verify that **ISDN-PRI** is enabled, as shown below.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y		IP Stations? y
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? y
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		

Navigate to **Page 8**, and verify the highlighted QSIG features are enabled, as shown below.

```
display system-parameters customer-options                               Page 8 of 11
                               QSIG OPTIONAL FEATURES

                               Basic Call Setup? y
                               Basic Supplementary Services? y
                               Centralized Attendant? y
                               Interworking with DCS? y
                               Supplementary Services with Rerouting? y
                               Transfer into QSIG Voice Mail? y
                               Value-Added (VALU)? y
```

5.2. Administer System Parameters Special Applications

Use the “change system-parameters special-applications” command, and navigate to **Page 3** to enable **(SA8440) – Unmodified QSIG Reroute Number**.

Under the QSIG call forwarding feature, when a call comes into Communication Manager over the ISDN trunk administered for supplementary service option B and terminates to a station with call forwarding activated to an off-net number, Communication Manager sends an ISDN facility message back to the originating switch with the complete forward-to number that can include dial plan prefixes and route pattern digit manipulation, etc.

The **Unmodified QSIG ReRoute Number** special application allows the option of bypassing the number manipulation for the forwarded-to party.

```
display system-parameters special-applications                         Page 3 of 10
                               SPECIAL APPLICATIONS

                               (SA8141) - LDN Attendant Queue Priority? n
                               (SA8143) - Omit Designated Extensions From Displays? n
                               (SA8146) - Display Update for Redirected Calls? n
                               (SA8156) - Attendant Priority Queuing by COR? n
                               (SA8157) - Toll Free Vectoring until Answer? n
                               (SA8201) - Start Time and 4-Digit Year CDR Custom Fields? n
                               (SA8202) - Intra-switch CDR by COS? n
                               (SA8211) - Prime Appearance Preference? n
                               (SA8240) - Station User Admin of FBI? n
                               (SA8312) - Meet-Me Paging? n
                               (SA8323) - Idle Call Preference Display? n
                               (SA8339) - PHS X-Station Mobility? n
                               (SA8348) - Map NCID to Universal Call ID? n
                               (SA8428) - Station User Button Ring Control? n
                               (SA8434) - Delay PSTN Connect on Agent Answer? n
                               (SA8439) - Forward Held-Call CPN? n
                               (SA8440) - Unmodified QSIG Reroute Number? y
                               (SA8475) - SOSM? n
```

5.3. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers and chained call forwarding.

Trunk-to-Trunk Transfer feature is needed to be able to transfer an incoming call from IPC back out to IPC (incoming trunk to outgoing trunk), and to transfer an outgoing call to IPC to another outgoing trunk to IPC (outgoing trunk to outgoing trunk). For ease of compliance testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis.

Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n
```

Navigate to **Page 16. Enable Chained Call Forwarding**, to allow changes to the maximum number of call forwarding hops parameter in **Section 5.4**.

```
change system-parameters features                               Page 16 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

      SPECIAL TONE
      Special Dial Tone? n
      Special Dial Tone for Digital/IP Stations: none

      REDIRECTION NOTIFICATION
      Display Notification for Do Not Disturb? n
      Display Notification for Send All Calls? n
      Display Notification for Call Forward? n
      Display Notification for Enhanced Call Forward? n
      Display Notification for a locked Station? n
      Display Notification for Limit Number of Concurrent Calls? n
      Display Notification for Posted Messages? n
      Scroll Status messages Timer(sec.):

      Chained Call Forwarding? Y
```

5.4. Administer System Parameters Coverage Forwarding

Use the “change system-parameters coverage-forwarding” command. Set **Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls** to a desired value. In the compliance testing, the threshold was disabled so that there will be no blocking on the number of calls being redirected off-net within the Call Forward timer.

```
change system-parameters coverage-forwarding                               Page 1 of 2
      SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING
CALL COVERAGE/FORWARDING PARAMETERS
      Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
      Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
      Coverage - Caller Response Interval (seconds): 4
      Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls: n
      Location for Covered and Forwarded Calls: called
      PGN/TN/COR for Covered and Forwarded Calls: caller
      COR/FRL check for Covered and Forwarded Calls? n
      QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path? y
COVERAGE
```

Navigate to **Page 2**, and set **Maximum Number Of Call Forwarding Hops** to a value mutually agreed with IPC.

```
change system-parameters coverage-forwarding                               Page 2 of 2
      SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING
COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)
      Coverage Of Calls Redirected Off-Net Enabled? n

CHAINED CALL FORWARDING
      Maximum Number Of Call Forwarding Hops: 6
      Station Coverage Path For Coverage After Forwarding: principal
```

5.5. Administer DS1 Circuit Pack

Use the “add ds1 x” command, where “x” is the slot number of the DS1 circuit pack with physical connectivity to IPC. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **Bit Rate:** “2.048”
- **Line Coding:** “hdb3”
- **Signaling Mode:** “isdn-pri”
- **Connect:** “pbx”
- **Interface:** “peer-master”
- **Peer Protocol:** “Q-SIG”
- **Side:** “b”
- **Interface Companding:** “alaw”
- **CRC:** “y”
- **Channel Numbering:** “timeslot”

```
change ds1 1v2                                     Page 1 of 1
DS1 CIRCUIT PACK

Location: 001V2                                     Name: QSIG to Unigy
Bit Rate: 2.048                                     Line Coding: hdb3
Signaling Mode: isdn-pri
Connect: pbx                                         Interface: peer-master
TN-C7 Long Timers? n                               Peer Protocol: Q-SIG
Interworking Message: PROGRESS                     Side: b
Interface Companding: alaw                         CRC? y
Idle Code: 11111111                               Channel Numbering: timeslot
DCP/Analog Bearer Capability: 3.1kHz

T303 Timer(sec): 4
Disable Restarts? n

Slip Detection? n                                  Near-end CSU Type: other

Echo Cancellation? N
```

5.6. Administer ISDN Trunk Group

Administer an ISDN trunk group to interface with IPC. Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “isdn”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Direction:** “two-way”
- **Carrier Medium:** “PRI/BRI”
- **Service Type:** “tie”

```
change trunk-group 71                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 71                                     Group Type: isdn                                     CDR Reports: n
Group Name: ElQSIG-Unigy                               COR: 1                                     TN: 1                                     TAC: 1071
Direction: two-way                                     Outgoing Display? n                               Carrier Medium: PRI/BRI
Dial Access? n                                         Busy Threshold: 255   Night Service:
Queue Length: 0
Service Type: tie                                     Auth Code? n                                     TestCall ITC: rest
Far End Test Line No:
TestCall BCC: 4
```

Navigate to **Page 2**. For **Supplementary Service Protocol**, enter “b” for QSIG. For **Digit Handling (in/out)**, enter “enbloc/enbloc”. For **Format**, enter “unk-unk”. Retain the default values for the remaining fields.

```
change trunk-group 71                                     Page 2 of 21
  Group Type: isdn

TRUNK PARAMETERS
  Codeset to Send Display: 6                               Codeset to Send National IEs: 6
  Max Message Size to Send: 260
  Supplementary Service Protocol: b                       Digit Handling (in/out): enbloc/enbloc

  Trunk Hunt: cyclical                                     Digital Loss Group: 13
Incoming Calling Number - Delete:                         Insert:                                     Format: unk-unk
  Bit Rate: 1200                                           Synchronization: async                     Duplex: full
Disconnect Supervision - In? y   Out? n
Answer Supervision Timeout: 0
  Administer Timers? n                                     CONNECT Reliable When Call Leaves ISDN? n
  XOIP Treatment: auto                                     Delay Call Setup When Accessed Via IGAR? n
CPN to Send for Redirected Calls: calling
```

Navigate to Page 3. Enable **Send Name**, **Send Calling Number**, and **Send Called/Busy/Connected Number**. For **Format**, select “unknown”. Disable **Modify Reroute Number**, as shown below.

```

change trunk-group 71                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                                     Measured: none                                     Wideband Support? n
                                                         Internal Alert? n                                     Maintenance Tests? y
                                                         Data Restriction? n                                   NCA-TSC Trunk Member: 30
                                                         Send Name: y                                           Send Calling Number: y
    Used for DCS? n                                       Hop Dgt? n                                           Send EMU Visitor CPN? n
    Suppress # Outpulsing? n                             Format: unknown
    Outgoing Channel ID Encoding: preferred              UI IE Treatment: service-provider

                                                         Replace Restricted Numbers? n
                                                         Replace Unavailable Numbers? n
                                                         Send Called/Busy/Connected Number: y
                                                         Hold/Unhold Notifications? y
    Send UI IE? y                                         Modify Tandem Calling Number: no
    Send UCID? n
    Send Codeset 6/7 LAI IE? y                           Dsl Echo Cancellation? n
                                                         Modify Reroute Number? n

    Apply Local Ringback? n
    Show ANSWERED BY on Display? y
                                                         Network (Japan) Needs Connect Before Disconnect? n
  
```

5.7. Administer ISDN Signaling Group

Administer an ISDN signaling group for the new trunk group to use for signaling. Use the “add signaling-group n” command, where “n” is an available signaling group number. For **Primary D-Channel**, enter the slot number for the DS1 circuit pack from **Section 5.5** and port “16”. Set desired values for **Max number of NCA TSC** and **Max number of CA TSC**.

For **Trunk Group for NCA TSC** and **Trunk Group for Channel Selection**, enter the ISDN trunk group number from **Section 5.6**. For **TSC Supplementary Service Protocol**, enter “b” for QSIG. Retain the default values for the remaining fields.

```

change signaling-group 71                                   Page 1 of 1
SIGNALING GROUP

Group Number: 71                                         Group Type: isdn-pri
Associated Signaling? y                                  Max number of NCA TSC: 30
Primary D-Channel: 001V216                              Max number of CA TSC: 30
                                                         Trunk Group for NCA TSC: 71
Trunk Group for Channel Selection: 71                   X-Mobility/Wireless Type: NONE
TSC Supplementary Service Protocol: b                    Network Call Transfer? n
  
```

5.8. Administer Trunk Group Members

Use the “change trunk-group n” command, where “n” is the ISDN trunk group number added in **Section 5.6**. Navigate to **Page 3**. For **NCA-TSA Trunk Member**, enter the highest trunk group member number to use for routing of tandem QSIG call independent signaling connections.

```
change trunk-group 71                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n          Measured: none          Wideband Support? n
                             Internal Alert? n        Maintenance Tests? y
                             Data Restriction? n      NCA-TSC Trunk Member: 30
                             Send Name: y            Send Calling Number: y
                             Hop Dgt? n              Send EMU Visitor CPN? n
  Used for DCS? n
  Suppress # Outpulsing? n  Format: natl-pub
  Outgoing Channel ID Encoding: preferred  UII IE Treatment: service-provider

                             Replace Restricted Numbers? n
                             Replace Unavailable Numbers? n
                             Send Called/Busy/Connected Number: y
                             Hold/Unhold Notifications? y
  Send UII IE? y            Modify Tandem Calling Number: no
  Send UCID? n
  Send Codeset 6/7 LAI IE? y          Dsl Echo Cancellation? n
                                     Modify Reroute Number? n
  Apply Local Ringback? n
  Show ANSWERED BY on Display? y
                                     Network (Japan) Needs Connect Before Disconnect? n
```

Navigate to **Page 5** and **6**. Enter all 30 ports of the DS1 circuit pack into the **Port** fields, and the corresponding **Code** and **Sfx** fields will be populated automatically. Enter the ISDN signaling group number from **Section 5.7** into the **Sig Grp** fields as shown below.

```
change trunk-group 71                                     Page 5 of 21
TRUNK GROUP
  Administered Members (min/max): 1/30
GROUP MEMBER ASSIGNMENTS
  Total Administered Members: 30

  Port   Code Sfx Name      Night      Sig Grp
1: 001V201 MM710
2: 001V202 MM710
3: 001V203 MM710
4: 001V204 MM710
5: 001V205 MM710
6: 001V206 MM710
7: 001V207 MM710
8: 001V208 MM710
9: 001V209 MM710
10: 001V210 MM710
11: 001V211 MM710
12: 001V212 MM710
13: 001V213 MM710
14: 001V214 MM710
15: 001V215 MM710
```

change trunk-group 71					Page 6 of 21	
TRUNK GROUP						
					Administered Members (min/max):	1/30
GROUP MEMBER ASSIGNMENTS					Total Administered Members:	30
	Port	Code Sfx	Name	Night	Sig Grp	
16:	001V217	MM710			71	
17:	001V218	MM710			71	
18:	001V219	MM710			71	
19:	001V220	MM710			71	
20:	001V221	MM710			71	
21:	001V222	MM710			71	
22:	001V223	MM710			71	
23:	001V224	MM710			71	
24:	001V225	MM710			71	
25:	001V226	MM710			71	
26:	001V227	MM710			71	
27:	001V228	MM710			71	
28:	001V229	MM710			71	
29:	001V230	MM710			71	
30:	001V231	MM710			71	

5.9. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is the existing route pattern number to reach IPC, in this case “71”. 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 ISDN trunk group number from **Section 5.6**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **TSC:** “y”
- **CA-TSC Request:** “as-needed”
- **Numbering Format:** “unk-unk”

change route-pattern 71										Page	1 of	3							
Pattern Number: 71										Pattern Name: Qsig to Unigy									
SCCAN? n										Secure SIP? n									
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC										
No			Mrk	Lmt	List	Del	Digits	QSIG											
Dgts										Intw									
1:	71	0							n	user									
2:									n	user									
3:									n	user									
4:									n	user									
5:									n	user									
6:									n	user									
BCC VALUE										TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR	
0 1 2 M 4 W										Request						Dgts	Format		
																Subaddress			
1:	y	y	y	y	y	n	y	as-needed	rest			unk-unk	none						
2:	y	y	y	y	y	n	n		rest				none						
3:	v	v	v	v	v	n	n		rest				none						

5.10. Administer Public Unknown Numbering

Use the “change public-unknown-numbering 0” command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 5.6**. In the example shown below, all calls originating from a 5-digit extension beginning with 4200, and routed to trunk group 71 will result in a 5-digit calling number.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	4200			5	Total Administered: 2
5	7205	60		5	Maximum Entries: 9999
					Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.

5.11. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 7205x to IPC. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 7205x, as shown below.

change uniform-dialplan 7					Page 1 of 2
UNIFORM DIAL PLAN TABLE					
					Percent Full: 0
Matching			Insert	Node	
Pattern	Len	Del	Digits	Net Conv	Num
7202	5	0		aar n	
7203	5	0		aar n	
7204	5	0		aar n	
7205	5	0		aar n	

5.12. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to specify how to route calls to 7205x. In the example shown below, calls with digits 7205x will be routed as an AAR call using route pattern “71” from **Section 5.9**.

change aar analysis 0					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					
Location: all					Percent Full: 3
Dialed	Total	Route	Call	Node	ANI
String	Min Max	Pattern	Type	Num	Reqd
7202	5 5	92	unku		n
7205	5 5	71	aar		n

5.13. Administer PSTN Trunk Group

Use the “change trunk-group n” command, where “n” is the existing ISDN trunk group number used to reach the PSTN, in this case “80”.

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

```
change trunk-group 80                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                                     Measured: none      Wideband Support? n
                                                           Internal Alert? n    Maintenance Tests? y
                                                           Data Restriction? n  NCA-TSC Trunk Member:
                                                           Send Name: y         Send Calling Number: y
                                                           Send EMU Visitor CPN? y
    Used for DCS? n
    Suppress # Outpulsing? n    Format: natl-pub
    Outgoing Channel ID Encoding: preferred    UII IE Treatment: service-provider

                                                           Replace Restricted Numbers? n
                                                           Replace Unavailable Numbers? n
                                                           Send Connected Number: n
    Network Call Redirection: none                Hold/Unhold Notifications? n
        Send UII IE? y    Modify Tandem Calling Number: tandem-cpn-form
        Send UCID? n
    Send Codeset 6/7 LAI IE? y                    Dsl Echo Cancellation? n

    Apply Local Ringback? n                        US NI Delayed Calling Name Update? n
    Show ANSWERED BY on Display? y
                                                           Network (Japan) Needs Connect Before Disconnect? n
```

5.14. 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 7205 and routed to trunk group 80, will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case “pub-unk”.

```
change tandem-calling-party-num                           Page 1 of 8
CALLING PARTY NUMBER CONVERSION
FOR TANDEM CALLS

    CPN          Incoming          Outgoing
    Len Prefix   Number   Trk      Number
    5  7205      Format    Grp(s)   Delete  Insert  Format
    5  7205      Format    80      Delete  Insert  pub-unk
```

5.15. Administer SIP trunk for Avaya Aura® Messaging

Administer a sip trunk group to interface with Avaya Aura® Messaging. Use the “add trunk-group n” command, where “n” is an available trunk group number. 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.
- **Direction:** “two-way”
- **Service Type:** “tie”

```
add trunk-group 94                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 94                                     Group Type: sip          CDR Reports: y
Group Name: DirectSIP2AAM61                         COR: 1                 TN: 1                TAC: 1094
Direction: two-way                                Outgoing Display? n
Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 94
                                                Number of Members: 10
```

On **Page 4**, enable the Network Call Redirection field.

```
add trunk-group 94                                     Page 4 of 21
                                     PROTOCOL VARIATIONS
                                     Mark Users as Phone? n
Prepend '+' to Calling Number? n
Send Transferring Party Information? n
Network Call Redirection? y
Send Diversion Header? n
Support Request History? y
Telephone Event Payload Type:

Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? n
Identity for Calling Party Display: P-Asserted-Identity
Enable Q-SIP? n
```

5.16. Administer Signal group for Avaya Aura® Messaging

Administer a signaling group for the new trunk group to use for signaling. Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “94”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tcp”
- **Near-end Node Name:** An existing C-LAN node name or procr.
- **Far-end Node Name:** The existing AAM 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:** “1” (During the compliance test, only one network region was used).
- **Direct IP-IP Audio Connection:** Disable the field by entering “n” (Unigy V2 does not fully support shuffling).

```
add signaling-group 94                                     Page 1 of 1
                                     SIGNALING GROUP

Group Number: 94
IMS Enabled? n
Q-SIP? n
IP Video? n
Peer Detection Enabled? y  Peer Server: Others

Group Type: sip
Transport Method: tcp

SIP Enabled LSP? n
Enforce SIPS URI for SRTP? y

Near-end Node Name: procr
Near-end Listen Port: 5060

Far-end Node Name: AAM61
Far-end Listen Port: 5060
Far-end Network Region: 1

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
Enable Layer 3 Test? y
H.323 Station Outgoing Direct Media? n

Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? n
IP Audio Hairpinning? n
Alternate Route Timer(sec): 6
```

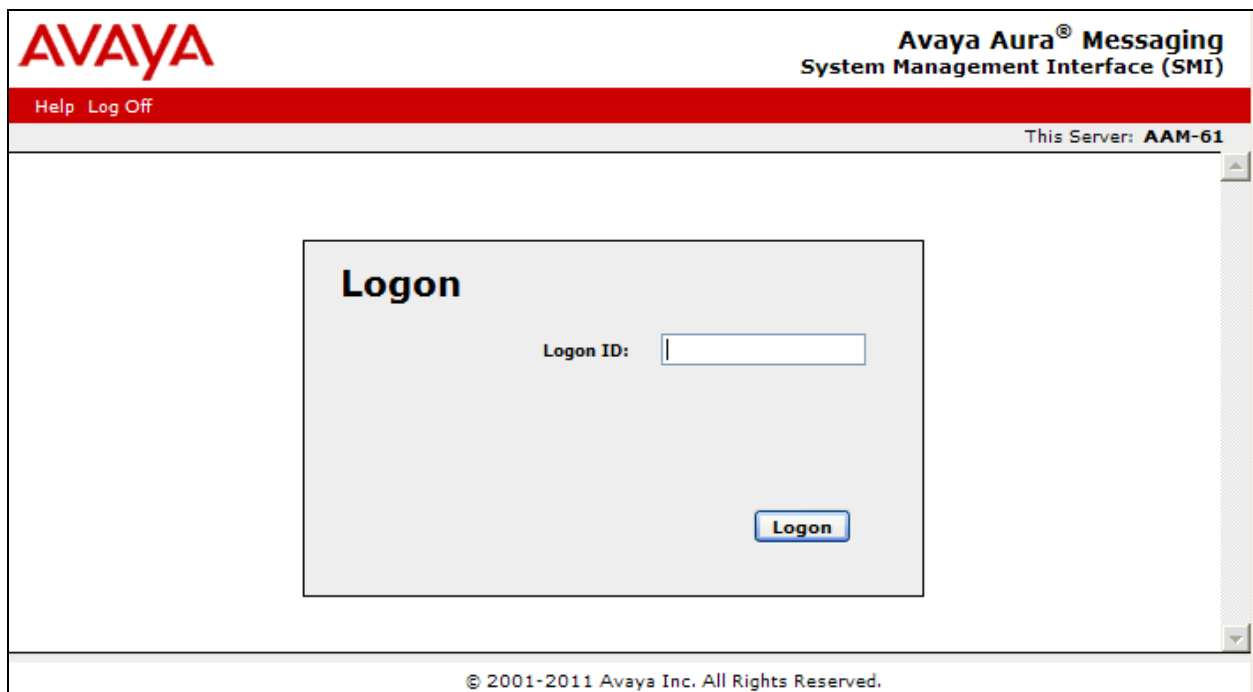
6. Configure Avaya Aura® Messaging

This section provides the procedures for configuring users as local subscribers on Avaya Aura® Messaging. The configuration procedures include the following areas:

- Launch messaging administration
- Administer telephony integration
- Administer subscribers

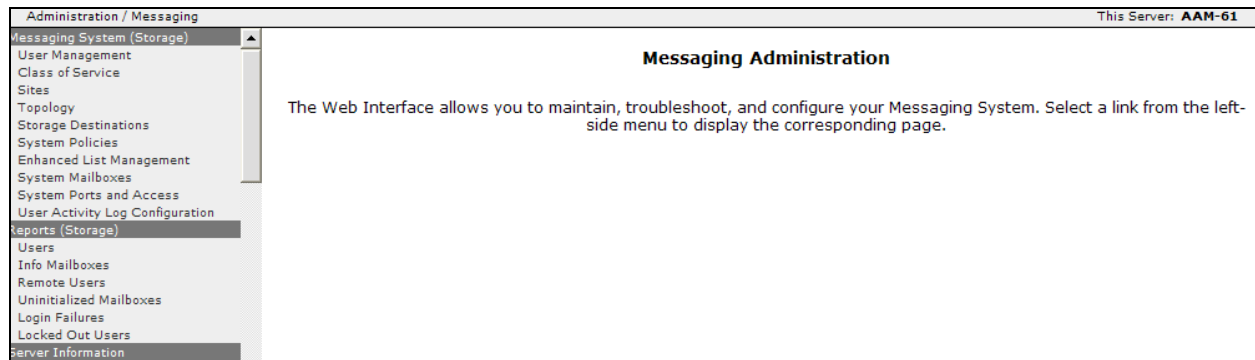
6.1. Launch Messaging Administration

Access the Avaya Aura® Messaging web interface by using the URL <http://ip-address> in an Internet browser window, where “ip-address” is the IP address of the Avaya Aura® Messaging server. The **Logon** screen is displayed. Log in using a valid user name and password. The **Password** field will appear after a value is entered into the **Username** field.



The screenshot displays the Avaya Aura® Messaging System Management Interface (SMI) web application. At the top left is the AVAYA logo. At the top right, it says "Avaya Aura® Messaging System Management Interface (SMI)". Below the logo, there are links for "Help" and "Log Off". On the right side, it indicates "This Server: AAM-61". The main content area features a "Logon" box with a "Logon ID:" label and a text input field. Below the input field is a "Logon" button. At the bottom of the page, there is a copyright notice: "© 2001-2011 Avaya Inc. All Rights Reserved."

After selecting **Administration** → **Messaging** from the top menu, the following screen is displayed.

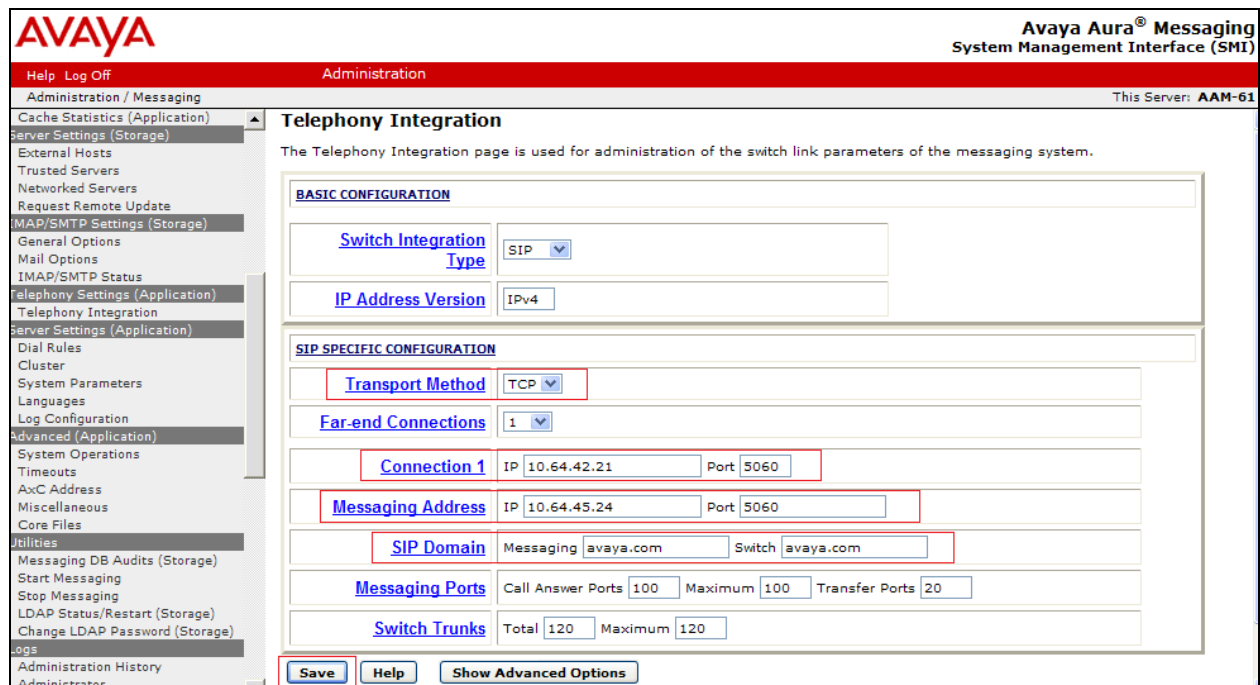


6.2. Administer Telephony Integration

Select the Telephony Integration from the left pane to access the telephony integration screen. Under the SIP SPECIFIC CONFIGURATION section, provide the following information:

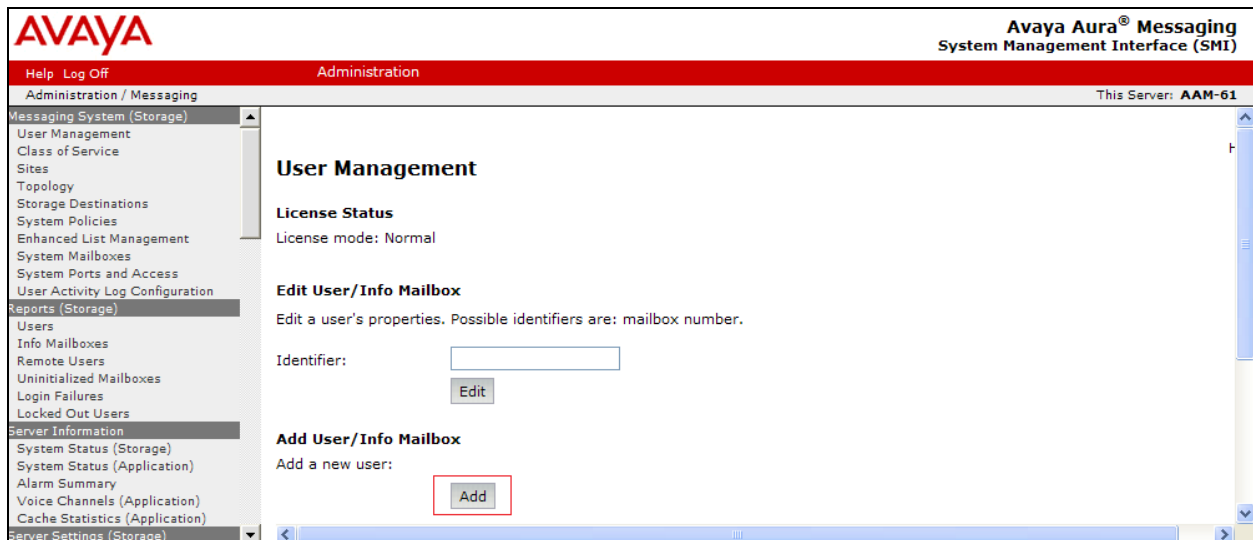
- Transport Method Select “TCP”
- Connection 1 IP address of Communication Manager and port, 5060.
- Messaging Address IP address of the Avaya Aura® Messaging and port, 5060.
- SIP Domain Enter an appropriate domain.

Click the **Save** button.



6.3. Administer Subscribers

Select **User Management** from the left pane. Click **Add** for the **Add a new user:** field.



The **User Management → Properties for New User** screen is displayed. Provide **First name**, **Last name**, **Mailbox number**, **Extension**. Enable MWI by selecting “yes” on **MWI enabled** field. Provide New and Confirm password for the user.

Click **Save** (not shown).

AVAYA Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration This Server: AAM-61

Administration / Messaging

User Management > Properties for New User

User Properties

First name: 42001
Last name: 42001
Display name:
ASCII name:

Site: Default

Mailbox number: 42001
Extension: 42001
☒ Include in Auto Attendant directory
Additional extensions:

Class of Service: Standard
Pronounceable name:

MWI enabled: Yes
Miscellaneous 1:
Miscellaneous 2:

New password:
Confirm password:

© 2001-2011 Avaya Inc. All Rights Reserved.

The following screen shows the created and utilized users during the compliance test

AVAYA

Avaya Aura® Messaging
System Management Interface (SMI)

Help Log Off

Administration

Administration / Messaging

This Server: AAM-61

Messaging System (Storage)

User Management

Class of Service

Sites

Topology

Storage Destinations

System Policies

Enhanced List Management

System Mailboxes

System Ports and Access

User Activity Log Configuration

Reports (Storage)

Users

Info Mailboxes

Remote Users

Uninitialized Mailboxes

Login Failures

Locked Out Users

Server Information

System Status (Storage)

System Status (Application)

Alarm Summary

Voice Channels (Application)

Cache Statistics (Application)

Server Settings (Storage)

Reports

Users (Local) Display: 25 items

First Name	Last Name	Site	Mailbox	Extension	Storage	In AA	Class of Service	Actions
		Choose One			Choose One	Choose One	Choose One	Filter Reset
42001	42001	Default	42001	42001	Avaya	Yes	Standard	
42002	42002	Default	42002	42002	Avaya	Yes	Standard	
42003	42003	Default	42003	42003	Avaya	Yes	Standard	
72051	72051	Default	72051	72051	Avaya	Yes	Standard	
72052	72052	Default	72052	72052	Avaya	Yes	Standard	

7. Configure IPC Converged Communications Server

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

- Launch Unigy Management System
- Administer media gateway
- Administer trunk groups
- Administer route lists
- Administer dial patterns
- Administer route plans
- Administer Codecs

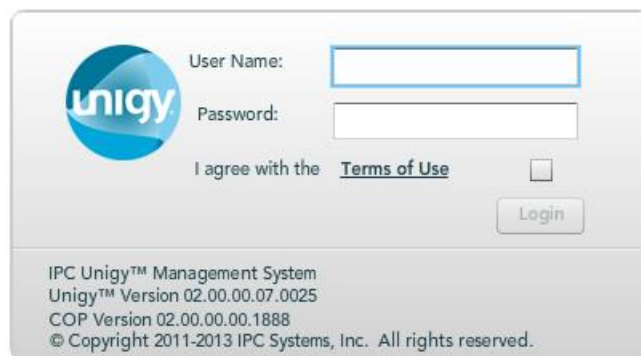
The configuration of Media Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy Management System

Access the Unigy Management System web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Media Manager. Log in using the appropriate credentials.

The screen below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use**, and click **Login**.

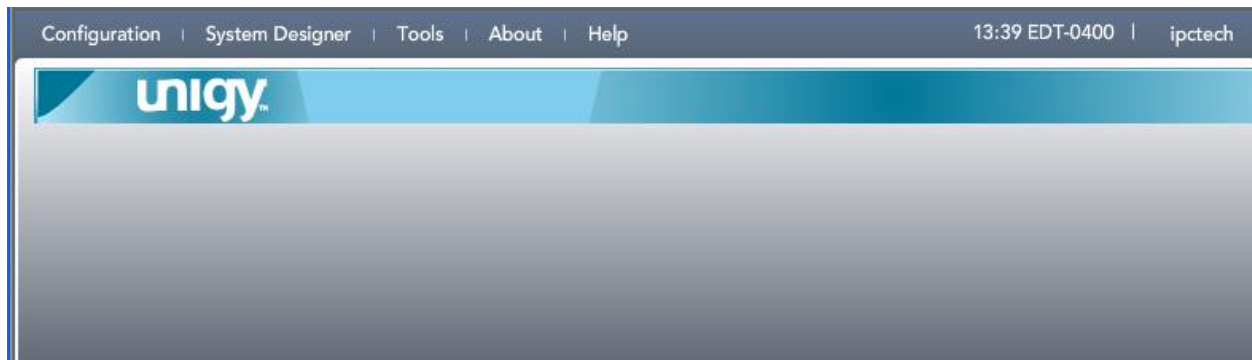
In the subsequent screen (not shown), click **Continue**.



The image shows a web-based login interface for the 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 are two input fields: 'User Name:' and 'Password:'. Below these fields is a checkbox labeled 'I agree with the' followed by a blue underlined link 'Terms of Use'. To the right of the checkbox is a small square icon. Below the checkbox and link is a 'Login' button. At the bottom of the form, there is a block of text: 'IPC Unigy™ Management System', 'Unigy™ Version 02.00.00.07.0025', 'COP Version 02.00.00.00.1888', and '© Copyright 2011-2013 IPC Systems, Inc. All rights reserved.'

7.2. Administer Media Gateway

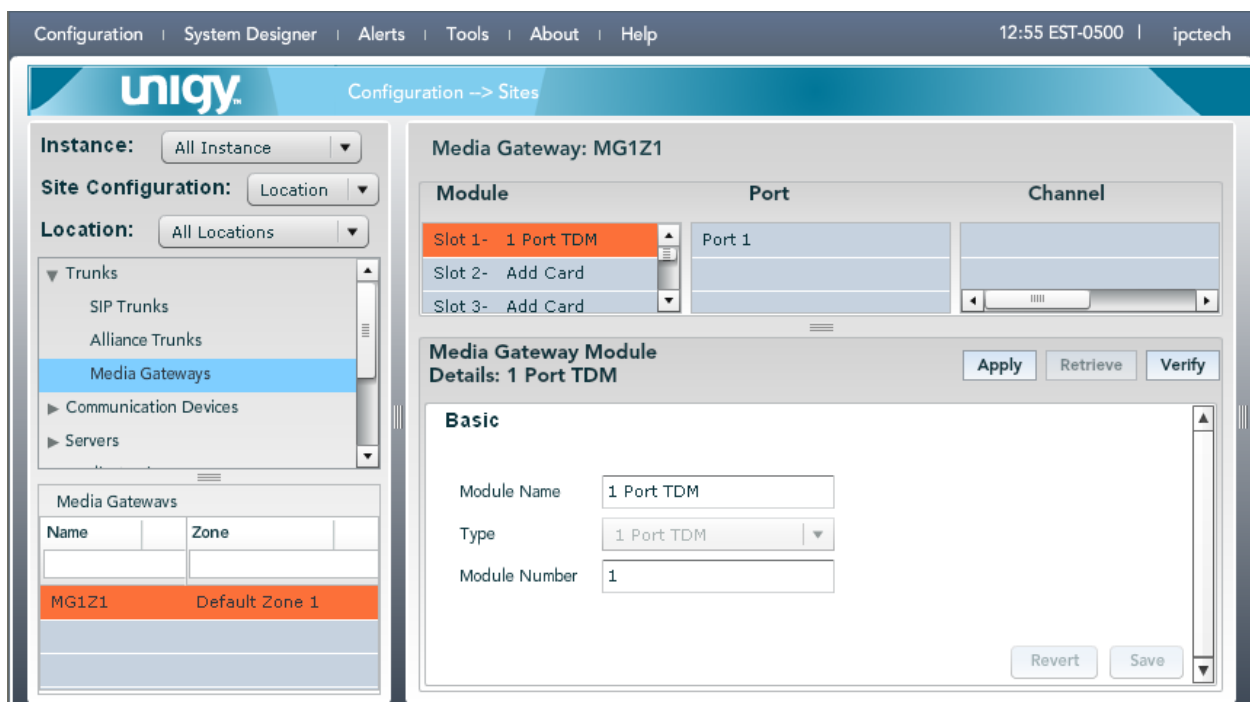
The screen below is displayed next. Select **Configuration → Sites** from the top menu.



The **Sites** information is displayed in the left pane. Select **Trunks → Media Gateways**, to display a list of media gateway in the lower left pane. Select the applicable media gateway from the listing, in this case “MG1Z1”.

The **Media Gateway** information is displayed in the upper right pane. Select the applicable physical card, in this case “Slot 1”.

The **Media Gateway Module Details** information is displayed in the lower right pane. Select “1 Port TDM” for **Type**, and click **Save**.



In the updated screen, click on a desired **Port** in the upper right pane, in this case “Port 1”.

The **Media Gateway Port Details** information is displayed in the lower right pane. For **Protocol Type**, select “E1 QSIG”. Retain the default values for the remaining fields.

Click **Save** (not shown), followed by **Apply**.

The screenshot displays the UniGY Configuration interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with the time 12:58 EST-0500 and the user ipctech. The main header shows 'unigy Configuration -> Sites'.

On the left, the 'Instance' dropdown is set to 'All Instance'. Under 'Site Configuration', the 'Location' dropdown is set to 'All Locations'. A tree view on the left lists various configuration categories, with 'Media Gateways' selected and highlighted in blue.


The main content area is titled 'Media Gateway: MG1Z1'. It features a table with three columns: 'Module', 'Port', and 'Channel'. The first row is highlighted in orange, showing 'Slot 1- 1 Port TDM' in the Module column, 'Port 1' in the Port column, and an empty Channel column.

Below this table, the 'Media Gateway Port Details: Port 1' section is visible. It has tabs for 'Port Properties' (selected) and 'ISDN'. The 'Basic' tab is active, showing various configuration fields:

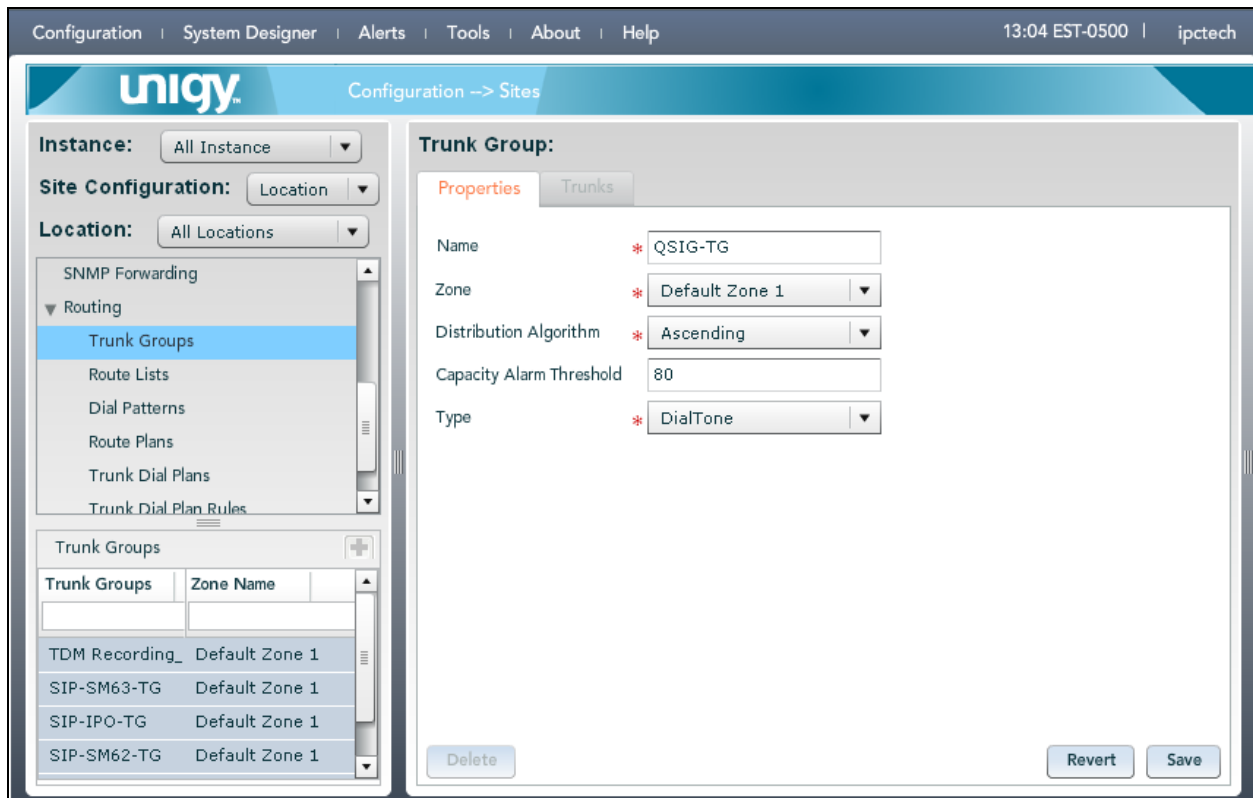
- Protocol Type: * E1 QSIG (dropdown)
- Partial Channel Config: ☐
- Number of Channels: 30 (text input)
- Alliance ICM Trunk: ☐
- Trunk: * ISDN (dropdown)
- Alliance Site: (dropdown)
- Alliance Site IP Address: (text input)
- Clock Master: * CLOCK-MASTER-OFF (dropdown)
- Line Code: * HDB3 (dropdown)
- Far End Connection: PBX (dropdown)
- Framing Method: * E1-FRAMING-MFF-CR (dropdown)

Buttons for 'Apply', 'Retrieve', and 'Verify' are located at the top right of the details section. A vertical scrollbar is visible on the right side of the details pane.

7.3. Administer Trunk Groups

Select **Routing → Trunk Groups** (not shown) in the left pane, and click the **Add** icon, , in the lower left pane to add a new trunk group.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, and click **Save**. Select the **Trunks** tab in the right pane.



The screenshot shows the UniGY Configuration interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with the time 13:04 EST-0500 and the user ipctech. The main header displays the UniGY logo and the path Configuration → Sites.

On the left side, there is a sidebar with the following sections:

- Instance:** All Instance
- Site Configuration:** Location
- Location:** All Locations
- Routing:** Trunk Groups (selected), Route Lists, Dial Patterns, Route Plans, Trunk Dial Plans, Trunk Dial Plan Rules
- Trunk Groups:** A table with columns Trunk Groups and Zone Name.

The Trunk Groups table contains the following entries:

Trunk Groups	Zone Name
TDM Recording_	Default Zone 1
SIP-SM63-TG	Default Zone 1
SIP-IPO-TG	Default Zone 1
SIP-SM62-TG	Default Zone 1

The main configuration area on the right is titled **Trunk Group:** and has two tabs: **Properties** (selected) and **Trunks**. The Properties tab contains the following fields:

- Name:** * QSIG-TG
- Zone:** * Default Zone 1
- Distribution Algorithm:** * Ascending
- Capacity Alarm Threshold:** 80
- Type:** * DialTone

At the bottom of the configuration area, there are three buttons: **Delete**, **Revert**, and **Save**.

The screen is updated with three panes. In the right pane, select the **MG Trunks** tab. In the **Media Gateway** listing, select and expand the applicable media gateway slot and port from **Section 7.2**, and drag the selection to the **Name** column in the middle pane as shown below. Click **Save**.

The screenshot displays the UniGy Configuration -> Sites interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with the time 13:12 EST-0500 and the user ipctech.

The main interface is divided into three panes:

- Left Pane:** Contains configuration options for Instance (All Instance), Site Configuration (Location), and Location (All Locations). A tree view on the left shows the configuration hierarchy, with Trunk Groups selected. Below this, a table lists Trunk Groups and their associated Zone Names.
- Middle Pane:** Displays the configuration for the selected Trunk Group, QSIG-TG. It has tabs for Properties and Trunks. The Trunks tab shows a table with columns for Name and Channels. The first row contains the text "MG1Z1>1 Port TDM>Port 1>QSIG/IS" and the value "30".
- Right Pane:** Titled "Available to Assign", it contains a table with a single row and multiple columns, likely for selecting media gateway slots and ports.

At the bottom of the middle pane, there are buttons for Remove, Revert, and Save.

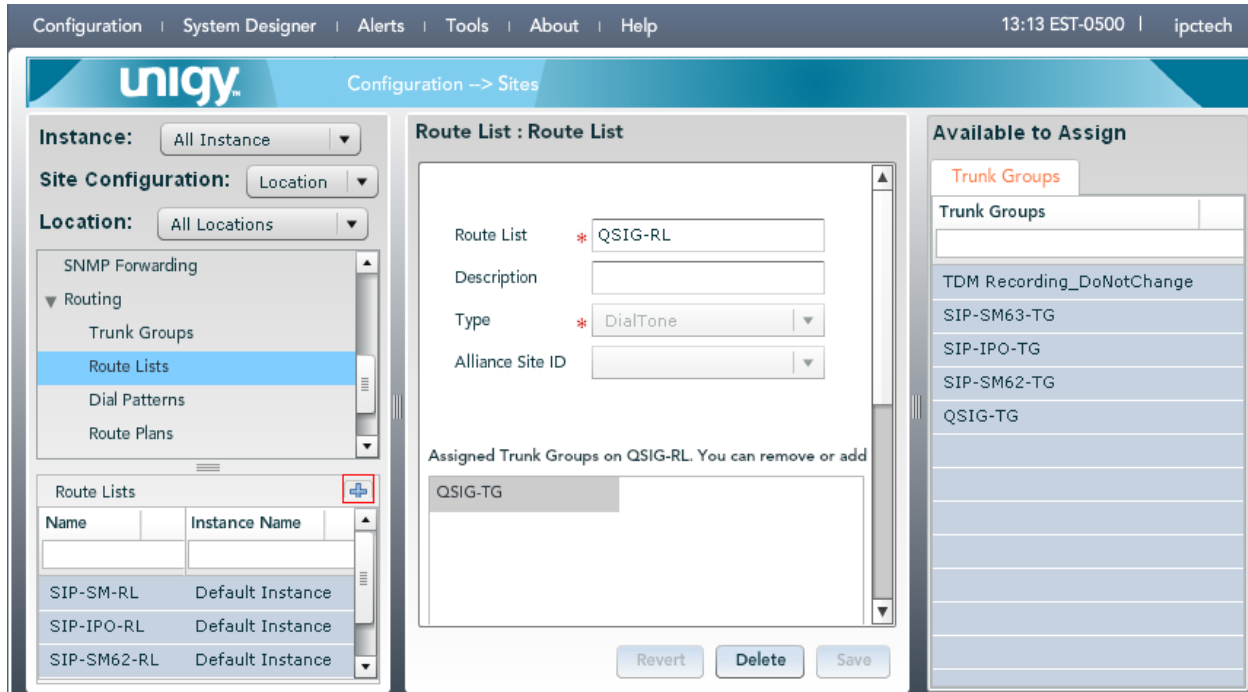
Trunk Groups	Zone Name
SIP-SM63-TG	Default Zone 1
SIP-IPO-TG	Default Zone 1
SIP-SM62-TG	Default Zone 1
QSIG-TG	Default Zone 1

Name	Channels
MG1Z1>1 Port TDM>Port 1>QSIG/IS	30

7.4. Administer Route Lists

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

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



7.5. Administer Dial Patterns

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

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya endpoints, in this case “*”, meaning any digit. For **Zone**, select “Default Zone 1”. Click **Save**.

The screenshot displays the Uni2CM601AAM61 configuration interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with the time 13:19 EST-0500 and the user ipctech. The main header shows the Uni2CM601AAM61 logo and the path Configuration → Sites.

On the left side, there is a sidebar with a tree view. The 'Routing' section is expanded, and 'Dial Patterns' is selected. Other options in the tree include Trunks (SIP Trunks, Alliance Trunks, Media Gateways), Communication Devices, Servers, Media Service, Prototype Devices, SNMP Forwarding, Trunk Groups, Route Lists, Route Plans, Trunk Dial Plans, and Trunk Dial Plan Rules.

The main content area is divided into two sections. The top section, titled 'Dial Patterns', contains a table with four columns: Name, Pattern String, Description, and Zone Name. Below the table are 'Add New' and 'Delete' buttons. The bottom section, titled 'Dial pattern Details', has a 'Properties' tab. It contains four fields: Name (set to 'All Dial Pattern'), Zone (set to 'Default Zone 1'), Description (set to 'all'), and Pattern String (set to '*'). At the bottom right of this section are 'Revert' and 'Save' buttons.

7.6. Administer Route Plans

Select **Routing** → **Route Plans** in the left pane, and click **Add New** in the right pane to create a new route plan.

Unigy Management System (Enterprise/Default Zone 1) - Windows Internet Explorer

https://10.64.49.2/ums/UMSClient.htm Certificate Error Conduit Search

File Edit View Favorites Tools Help

Related Links: International Phone Cards Medicare Advantage Plans Upgrade My Phone Black Friday Deals Anti Aging Skin Care Products

Unigy Management System (Enterprise/Default Zone 1)

Configuration | System Designer | Alerts | Tools | About | Help 13:23 EST-0500 | ipctech

unigy Configuration --> Sites

Instance: All Instance Site Configuration: Location Location: All Locations

- Trunks
- Communication Devices
- Servers
- Media Service
- Prototype Devices
- SNMP Forwarding
- Routing
 - Trunk Groups
 - Route Lists
 - Dial Patterns
 - Route Plans
 - Trunk Dial Plans
 - Trunk Dial Plan Rules

Route Plan

List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
Route2SM62	*	*	FORWARD	Default Instance
QSIG2CM601	*	*	FORWARD	Default Instance
Route2SM63	*	*	FORWARD	Default Instance
Route-2-IPO	*	*	FORWARD	Default Instance

Delete Add New Revert Save Sequence Change

The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter “*” to denote any calling party from UnigyV2. For **Destination**, enter “*” to denote any called party from UnigyV2. Select “Forward” for **Action**. Select “Default Instance” for **Instance**, and click **Save**.

The screenshot displays the Unigy Configuration web interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with the time 13:26 EST-0500 and the user ipctech. The main header shows the Unigy logo and the path Configuration -> Sites.

The interface is divided into three main panes:

- Left Pane (Site Configuration):** Contains dropdown menus for Instance (All Instance), Site Configuration (Location), and Location (All Locations). A tree view on the left lists various configuration categories, with 'Route Plans' highlighted under the 'Routing' section.
- Middle Pane (Route Plan):** Titled 'Create New Route Plan', it contains a form with the following fields:
 - UI Name: * QSIG2CM601
 - Description: (empty)
 - Calling Party: * *
 - Destination: * *
 - Action: * Forward (dropdown)
 - Instance: * Default Instance (dropdown)Below the form is a 'Route List' table (currently empty) and a 'Remove' button. At the bottom of the pane are 'Back', 'Revert', and 'Save' buttons.
- Right Pane (Available to Assign):** Titled 'Route Lists', it shows a list of available route lists. The 'QSIG-RL' entry is highlighted in orange.

Configuration | System Designer | Alerts | Tools | About | Help

13:27 EST-0500 | ipctech

unigy Configuration -> Sites

Instance: All Instance ▼

Site Configuration: Location ▼

Location: All Locations ▼

- ▶ Trunks
- ▶ Communication Devices
- ▶ Servers
- ▶ Media Service
- ▶ Prototype Devices
 - SNMP Forwarding
- ▼ Routing
 - Trunk Groups
 - Route Lists
 - Dial Patterns
 - Route Plans**
 - Trunk Dial Plans
 - Trunk Dial Plan Rules

Route Plan

List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
Route2SM62	*	*	FORWARD	Default Instance
QSIG2CM601	*	*	FORWARD	Default Instance
Route2SM63	*	*	FORWARD	Default Instance
Route-2-IPO	*	*	FORWARD	Default Instance

[Delete](#)
[Add New](#)
[Revert](#)
[Save Sequence Change](#)

The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 7.4** and drag into the **Route List** sub-section in the middle pane, as shown below. Click **Save**.

The screenshot displays the UniQy Configuration -> Sites interface. The left pane shows the navigation tree with 'Route Plans' selected. The middle pane, titled 'Route Plan', contains a 'Create New Route Plan' form with fields for UI Name (QSIG2CM601), Description, Calling Party (*), Destination (*), and Action (Forward). Below these fields is a 'Route List' section where 'QSIG-RL' is highlighted. The right pane, titled 'Available to Assign', shows a list of route lists including 'TDM Recording_DoNot', 'SIP-SM-RL', 'SIP-IPO-RL', 'SIP-SM62-RL', and 'QSIG-RL'. The 'Save' button at the bottom right of the middle pane is highlighted with a red box.

Configuration | System Designer | Alerts | Tools | About | Help 13:31 EST-0500 | ipctech

Configuration -> Sites

Instance: All Instance

Site Configuration: Location

Location: All Locations

Trunks

Communication Devices

Servers

Media Service

Prototype Devices

SNMP Forwarding

Routing

Trunk Groups

Route Lists

Dial Patterns

Route Plans

Trunk Dial Plans

Trunk Dial Plan Rules

Route Plan

Create New Route Plan

UI Name * QSIG2CM601

Description

Calling Party * *

Destination * *

Action * Forward

Route List:

QSIG-RL

Remove

Back Revert Save

Available to Assign

Route Lists

Name

TDM Recording_DoNot

SIP-SM-RL

SIP-IPO-RL

SIP-SM62-RL

QSIG-RL

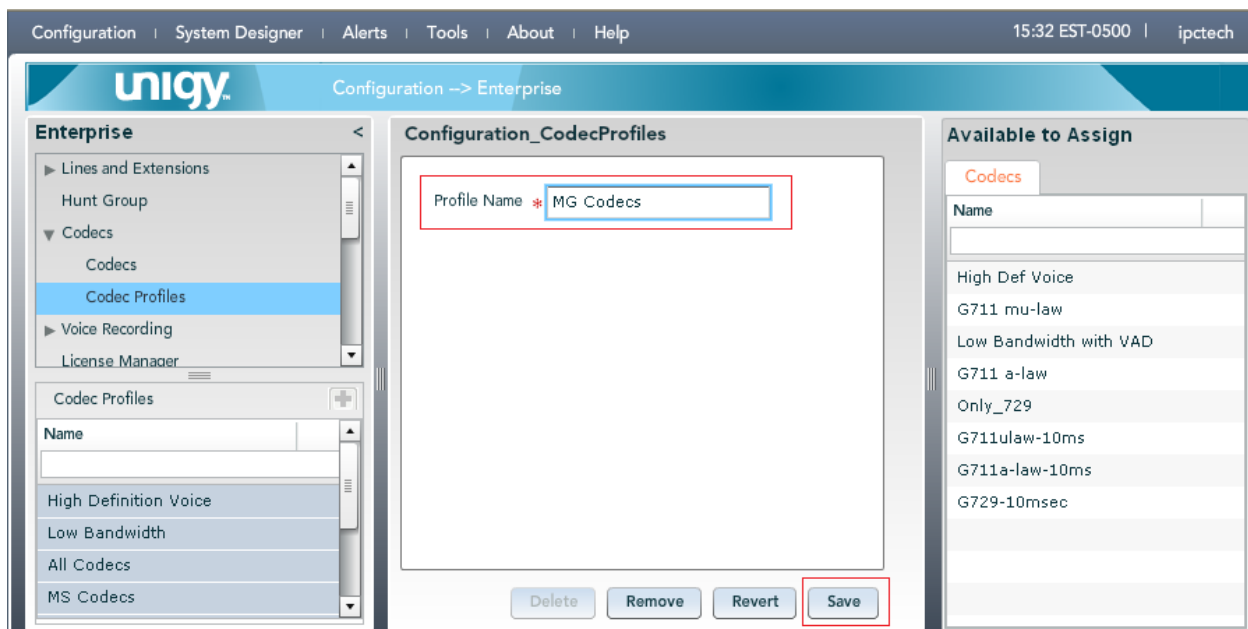
7.7. Administer Codecs

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

- Administer codec profile
- Assign codec profile to user
- Assign codec profile to turret

7.7.1. Administer Codec Profile

Select **Configuration → Enterprise → Codecs → Codec Profiles**, and click **Add New** in the left pane to create a new codec profile. Provide a profile name, and click **Save**.



After saving the codec profile, the following screen is displayed. In the right pane, select the available codecs and drag into the **Codecs** sub-section in the middle pane, as shown below. Click **Save**.

The screenshot shows the UniQy Configuration -> Enterprise interface. The left pane shows the 'Enterprise' menu with 'Codecs' selected. The middle pane shows the 'MG Codecs' configuration with a 'Profile Name' field set to 'MG Codecs'. Below this is a table titled 'Codecs' with columns 'Name' and 'Type'. The table contains three rows: 'G711 mu-law' with type 'G_711u_law', 'G711 a-law' with type 'G_711a_law', and 'Low Bandwidth with VAD' with type 'G_729'. A red box highlights these three rows. Below the table is a note: 'Note: List the codec in the order you want the device to try to use them.' At the bottom of the middle pane are buttons for 'Delete', 'Remove', 'Revert', and 'Save'. The right pane shows 'Available to Assign' with a 'Codecs' tab selected, displaying a list of codecs: 'High Def Voice', 'G711 mu-law', 'Low Bandwidth with VAD', 'G711 a-law', 'Only_729', 'G711ulaw-10ms', 'G711a-law-10ms', and 'G729-10msec'.

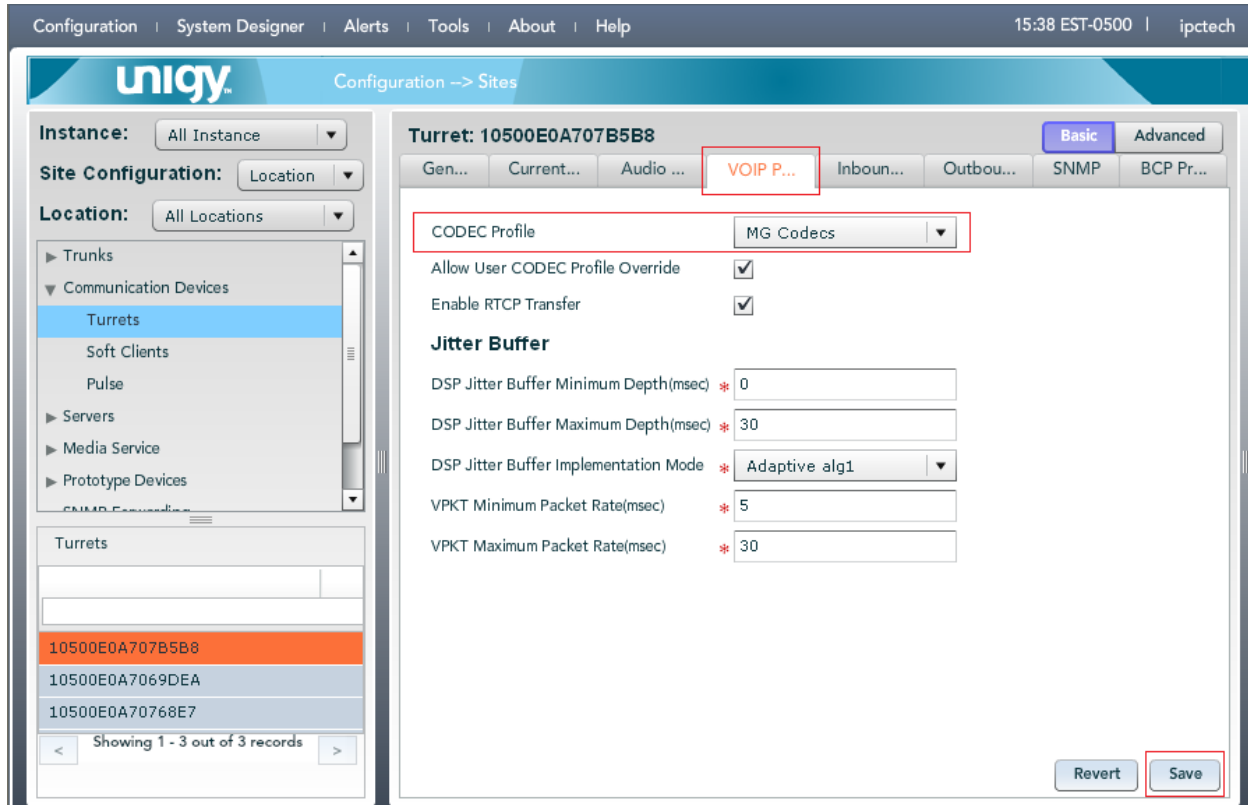
7.7.2. Assign Codec Profile to User

Select **System Designer**→ **End User Configuration**, and select a user to associate a codec profile with. Provide a profile name, and click **Save**.

The screenshot shows the UniQy System Designer -> End User Configuration interface. The left pane shows the 'End User Groups' and 'Users' sections. The 'Users' section shows a table with columns 'Name' and 'End User Group'. The table contains five rows: 'ipctech', 'user1', 'user2', 'user3', and 'user4', all associated with 'Untitled1'. The 'user1' row is highlighted. The right pane shows the 'User: user1' configuration. It has tabs for 'Tra...', 'Fa...', 'Sp...', 'Pri...', 'Au...', 'Dis...', 'Sof...', 'Pe...', 'O...', 'Pul...', and 'C...'. The 'Dis...' tab is selected. It contains several fields: 'Maximum digit for the divert to number' (26), 'Divert Intercom Calls To' (empty), 'Condition for Intercom Calls Diversion' (None), 'Ring No Answer Duration for Intercom Diversion (sec)' (6), 'Intercom Diversion Mode' (none), 'Maintain Intercom Divert Upon Log On?' (checkbox), 'Handset Button Press and Release Actions' (HANDSET_NONE), 'CODEC Profile' (MG Codecs), and 'Handset Select Mode' (left). A red box highlights the 'CODEC Profile' field. At the bottom right are buttons for 'Revert' and 'Save'.

7.7.3. Assign Codec Profile to Turret

Navigate to **Configuration** → **Sites** → **Communication Devices** → **Turrets** and select a turret to associate a codec profile with. Click the **VoIP Parameter** tab in the right pane. Select a codec on the **CODEC Profile** field, and click **Save**.



After codecs are configured, reboot the turret.

8. Configure IPC Media Gateway

This section provides the procedures for the following configuring:

- Administer codecs
- Administer the TDM Bus setting

The configuration of the Media Gateway is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Administer Codecs

Access the Media Gateway web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Media Gateway. Log in using the appropriate credentials.

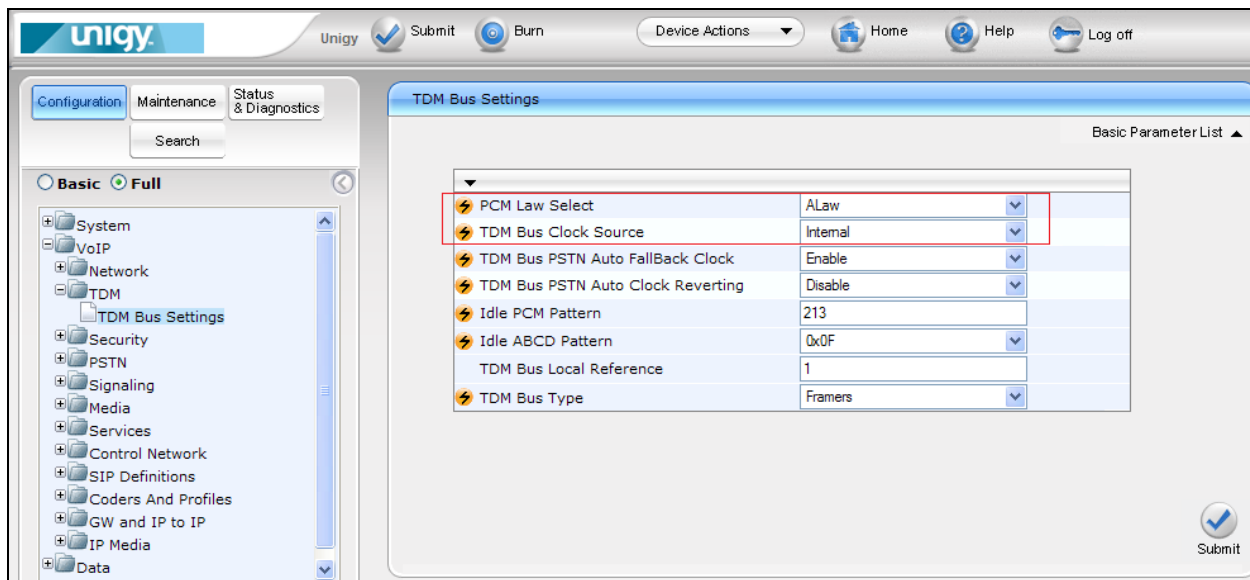
Navigate to **Configuration → VOIP → Coders And Profiles → Coders** in the left pane. Enter codecs that will be used.

The screenshot shows the UniQy web interface for configuring codecs. The left sidebar contains a tree view with categories like System, VoIP, Network, TDM, Security, PSTN, Signaling, Media, Services, Control Network, SIP Definitions, and Coders And Profiles. The 'Coders' option under 'Coders And Profiles' is selected. The main area displays the 'Coders Table' with the following data:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711U-I4W	20	64	0	Disabled
G.711A-I4W	20	64	8	Disabled
G.729	20	8	18	Disabled

8.2. Administer TDM Bus

Navigate to **Configuration → VOIP → TDM → TDM Bus Settings** in the left pane. Enter the Interface Companding codec that is being used in the Communication Manager DS1 card (**Section 5.5**). During the compliance test, Alaw was utilized. For the **TDM Bus Clock Source** field, set to “Internal”, meaning Avaya side is master and IPC side is slave. After the configuration changes, press the **Burn** button, and reset **Media Gateway**.



Note: Interface Compounding in Avaya side is set to Alaw (Refer to Section 5.5)

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager and IPC UnigyV2.

9.1. Verify Avaya Aura® Communication Manager

From the Communication Manager SAT interface, verify the status of the ISDN trunk group by using the “status trunk n” command, where “n” is the ISDN trunk group number administered in **Section 5.6**. Verify that all trunks are in the “in-service/idle” state as shown below.

status trunk 71				Page 1
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports	Busy
0071/001	001V201	in-service/idle	no	
0071/002	001V202	in-service/idle	no	
0071/003	001V203	in-service/idle	no	
0071/004	001V204	in-service/idle	no	
0071/005	001V205	in-service/idle	no	

0071/006	001V206	in-service/idle	no
0071/007	001V207	in-service/idle	no
0071/008	001V208	in-service/idle	no
0071/009	001V209	in-service/idle	no
0071/010	001V210	in-service/idle	no
0071/011	001V211	in-service/idle	no
0071/012	001V212	in-service/idle	no
0071/013	001V213	in-service/idle	no
0071/014	001V214	in-service/idle	no

Verify the status of the ISDN signaling groups by using the “status signaling-group n” command, where “n” is the ISDN signaling group number administered in **Section 5.7**. Verify that the signaling group is “in-service” as indicated in the **Group State** and **Level 3 State** fields shown below.

```
status signaling-group 71
                        STATUS SIGNALING GROUP

      Group ID: 71                      Active NCA-TSC Count: 0
      Group Type: isdn-pri              Active CA-TSC Count: 0
      Signaling Type: facility associated signaling
      Group State: in-service

                        Primary D-Channel

      Port: 001V216          Level 3 State: in-service

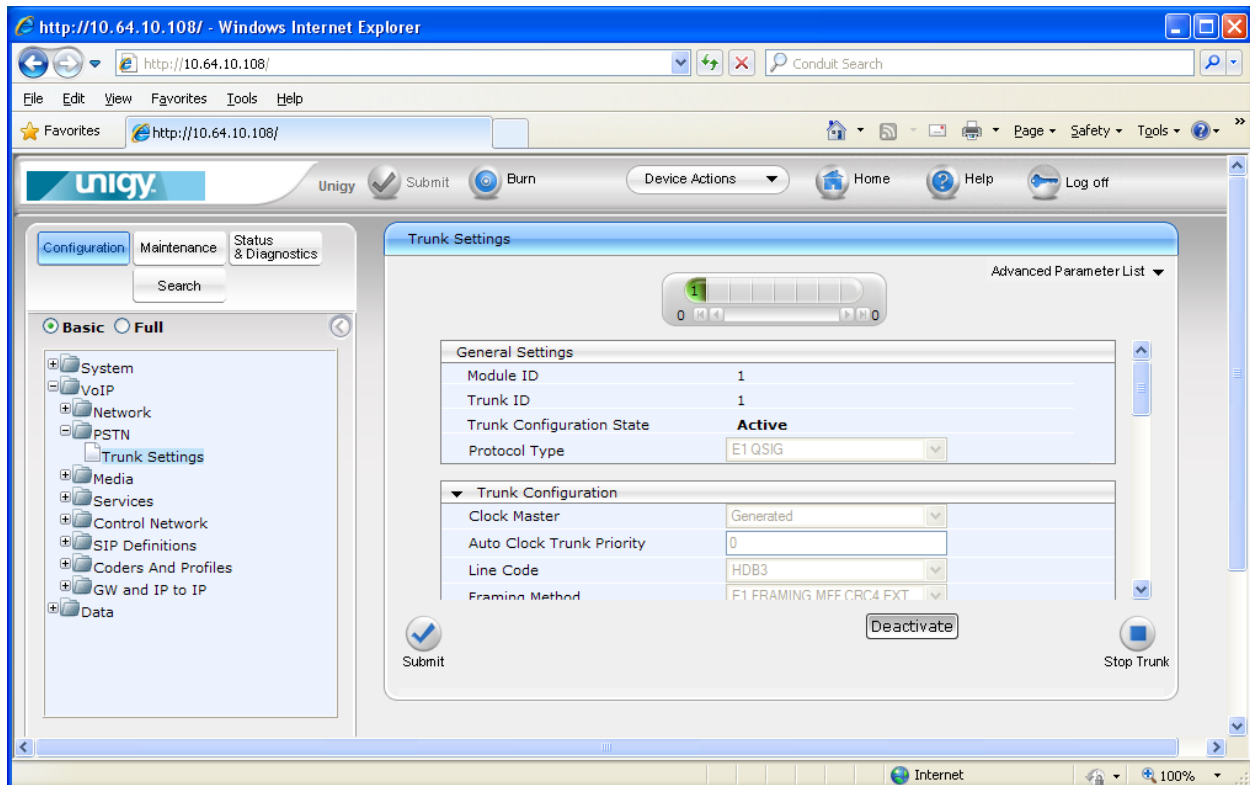
                        Secondary D-Channel

      Port:                  Level 3 State: no-link
```

9.2. Verify IPC UnigyV2

From the Media Gateway web interface, select **VoIP → PSTN Settings → Trunk Settings** to display the **Trunk Settings** screen.

Toward the top of the screen, click the applicable trunk port from **Section 7.2**, in this case “1”. Verify that the **Trunk Configuration State** is “Active”, as shown below.



10. Conclusion

These Application Notes describe the configuration steps required for IPC UnigyV2 to successfully interoperate with Avaya Aura® Communication Manager 6.0.1 using QSIG trunks, and a direct SIP trunk between Avaya Aura® Communication Manager and Avaya Aura® Messaging. All feature and serviceability test cases were completed.

11. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, July 2010, available at <http://support.avaya.com>.
2. *UnigyV2 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

©2014 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.