Avaya Solution & Interoperability Test lab

Application Notes for IPC Unigy 2.0.1 with Avaya Aura® Messaging 6.3, Avaya Aura® Session Manager 6.3 and Avaya Aura® Communication Manager 6.3 in a Centralized Messaging Environment using QSIG Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy 2.0.1 to interoperate with Avaya Aura® Messaging 6.3, Avaya Aura® Session Manager 6.3 and Avaya Aura® Communication Manager 6.3 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 6.3.

IPC Unigy system is a trading communication solution. In the compliance testing, IPC Unigy Media Gateway used E1 QSIG trunks to Avaya Aura® Communication Manager, for IPC turret users to obtain voice messaging services from Avaya Aura® Messaging. E1 QSIG trunks were used from IPC Unigy Media Gateway to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Aura® Messaging. The Avaya Aura® Messaging system in the Central site supported local subscribers from Avaya Aura® Communication Manager at the Central site, and from IPC turret users at the Remote site.

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 2.0.1 to interoperate with Avaya Aura® Messaging 6.3, Avaya Aura® Session Manager 6.3 and Avaya Aura® Communication Manager 6.3 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 6.3.

IPC Unigy system is a trading communication solution. In the compliance testing, IPC Unigy Media Gateway used E1 QSIG trunks to Avaya Aura® Communication Manager, for IPC turret users to obtain voice messaging services from Avaya Aura® Messaging. E1 QSIG trunks were used from IPC Unigy Media Gateway to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Aura® Messaging. The Avaya Aura® Messaging system in the Central site supported local subscribers from Avaya Aura® Communication Manager at the Central site, and from IPC turret users at the Remote site.

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, PSTN users, and/or the Avaya Aura® Messaging voicemail pilot to verify various call scenarios. The Avaya Aura® Messaging Web Subscriber Options web-based interface was used to configure subscriber features such as Call Me.

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

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 following items were covered during the test.

- Login
- Ring No Answer Greeting
- Calling Party
- MWI
- Call Forwarding All calls
- Multiple Call Forward
- Receptionist/Personal Operator
- Live Attendant

- Reach Me (Find Me in MM)
- Notify Me (Call me in MM)
- Call Sender
- Transfer
- Vector
- Serviceability

The serviceability testing focused on verifying the ability of IPC Unigy 2.0.1 to recover from adverse conditions, such as disconnecting/reconnecting the E1 connection to IPC Unigy 2.0.1.

2.2. Test Results

All test cases were executed and passed. The following were the observations from the compliance testing.

- IPC does not offer the Coverage feature, therefore coverage to voicemail for the turret users were accomplished by setting the Aura® Messaging pilot number as the Call Forwarding destination for the users.

2.3. Support

Technical support on IPC Unigy 2.0.1 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 Unigy 2.0.1 at the Remote Site consisted of the Unigy 2.0.1 System Center, Media Gateway, and Turrets. E1 QSIG trunks were used from IPC Unigy Media Gateway to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Aura® Messaging. In the test configuration, QSIG allowed IPC turret users at the Remote Site to "cover" to Avaya Aura® Messaging at the Central site for voice messaging services.

The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® System Manager. The detailed administration of basic connectivity among Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® Messaging is not the focus of these Application Notes and will not be described. These Application Notes will focus on the additional configuration required to support IPC turret users as local subscribers on Avaya Aura® Messaging.

The detailed administration of E1 QSIG trunks between Avaya Aura® Communication Manager and IPC Unigy 2.0.1, to enable IPC turret users to reach users on Avaya Aura® Communication Manager and on the PSTN, is assumed to be in place. However, E1 QSIG configuration on both sides is included in these Application Notes, and it is only for informational only. 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 (7200x -7202x), and IPC turret users at the Remote site (7205x). The Avaya Aura® Messaging pilot number was 7777.

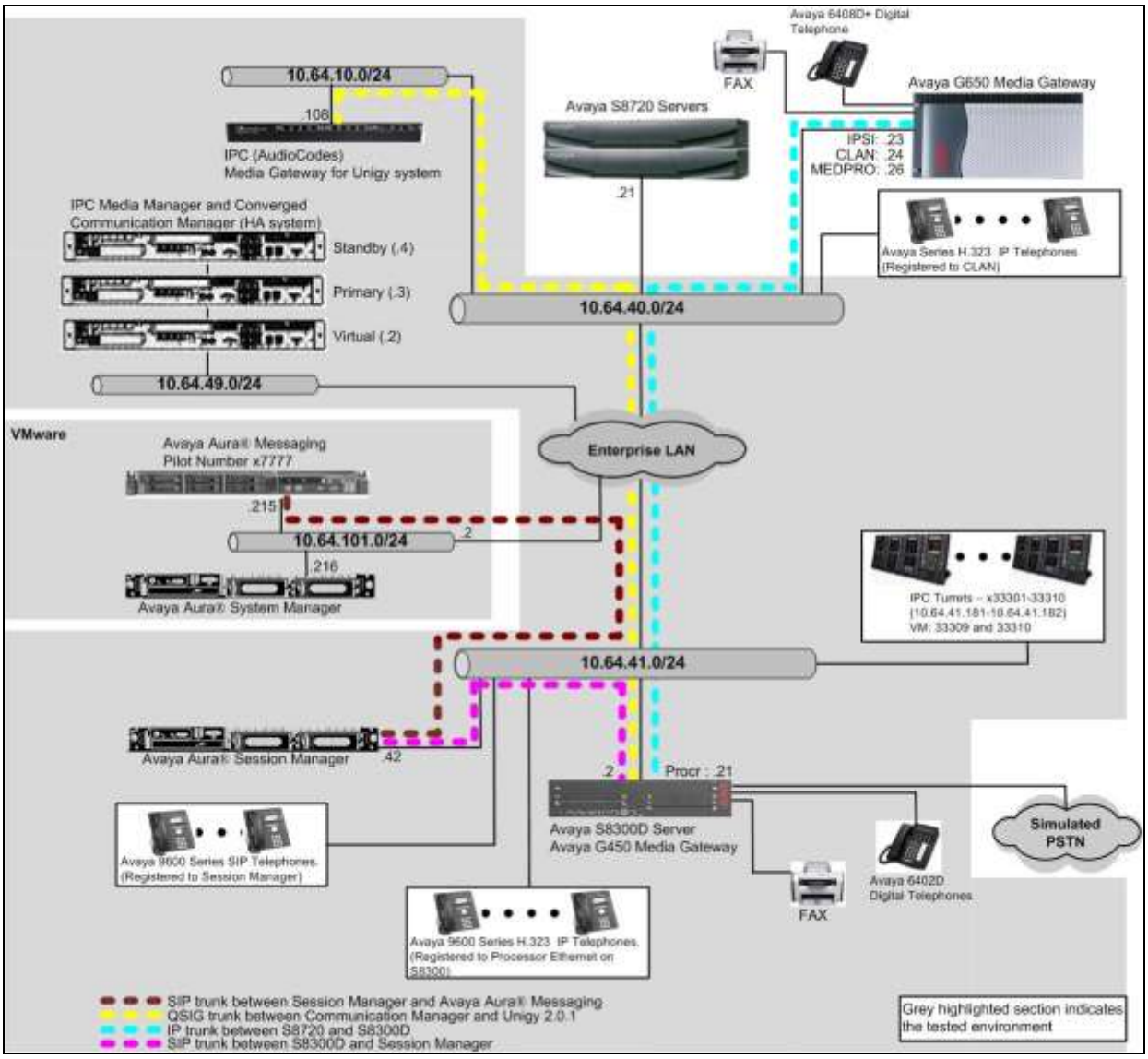


Figure 1: Test Configuration of IPC Unigy 2.0.1 with Avaya Aura® Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Messaging	MSG-03.0.124.0-321_0103
Avaya Aura® Communication Manager on Avaya S8800 Server	6.3 (R016x.03.0.124.0-21754
Avaya G450 Media Gateway	36.9
Avaya Aura® Session Manager	6.3.9.0.639011
Avaya Aura® System Manager	6.3.9
Avaya 9600 Series IP Telephone (H.323)	3.2.2
Avaya 96x1 Series IP Telephone (H.323)	6.2.3
Avaya 9600 Series IP Telephone (SIP)	2.6.12
Avaya 96x1 Series IP Telephone (SIP)	6.4.1
IPC Unigy 2.0.1 • Converged Communication Manager • Turrets	 02.00.01.02.0045 02.00.01.02.0045

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 ISDN trunk group
- Administer tandem calling party number
- Administer Coverage forwarding

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 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
        (NOTE: You must logoff & login to effect the permission changes.)
```

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.

```
change 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. This 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  20
                            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


            Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? 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  20
                         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 the 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? n

COVERAGE
                                Criteria for Logged Off/PSA/TTI Stations? n
                                        Keep Held SBA at Coverage Point? y
       External Coverage Treatment for Transferred Incoming Trunk Calls? n
        Immediate Redirection on Receipt of PROGRESS Inband Information? n
                                           Maintain SBA At Principal? y
            QSIG VALU Coverage Overrides QSIG Diversion with Rerouting? n
                                         Station Hunt Before Coverage? n
FORWARDING
Call Forward Override? n                      Coverage After Forwarding? y
```

Navigate to **Page 2**, and set **Maximum Number Of Call Forwarding Hops** to a value mutually agreeable 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"[This means IPC side is set to "peer-slave"]
- **Peer Protocol:** "Q-SIG"
- **Side:** "b"
- **Interface Companding:** "alaw"
- **CRC:** "y"
- **Channel Numbering:** "timeslot"

```
change ds1 1v7                                                Page   1 of   1
                              DS1 CIRCUIT PACK

            Location: 001V7                          Name: To IPC
            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.
- **Carrier Medium:** "PRI/BRI"
- **Service Type:** "tie"

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

Group Number: 71                    Group Type: isdn          CDR Reports: n
  Group Name: E1QSIG-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.

```
add 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**, enter "private". Disable **Modify Reroute Number**, as shown below.

```
add 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: private
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                              Replace Restricted Numbers? n
                                             Replace Unavailable Numbers? n
                                   Send Called/Busy/Connected Number: y
                                              Hold/Unhold Notifications? y
             Send UUI IE? y     Modify Tandem Calling Number: no
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                          Ds1 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.

```
add 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: 001V716     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
            Used for DCS? n             Hop Dgt? n     Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: private
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                          Send Called/Busy/Connected Number: y
                                                  Hold/Unhold Notifications? y
             Send UUI IE? y     Modify Tandem Calling Number: no
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                          Ds1 Echo Cancellation? n
                                                       Modify Reroute Number? y
    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** field 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: 001V701  MM710                                    71
  2: 001V702  MM710                                    71
  3: 001V703  MM710                                    71
  4: 001V704  MM710                                    71
  5: 001V705  MM710                                    71
  6: 001V706  MM710                                    71
  7: 001V707  MM710                                    71
  8: 001V708  MM710                                    71
  9: 001V709  MM710                                    71
 10: 001V710  MM710                                    71
 11: 001V711  MM710                                    71
 12: 001V712  MM710                                    71
 13: 001V713  MM710                                    71
 14: 001V714  MM710                                    71
 15: 001V715  MM710                                    71
```

```
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: 001V717  MM710                                    71
 17: 001V718  MM710                                    71
 18: 001V719  MM710                                    71
 19: 001V720  MM710                                    71
 20: 001V721  MM710                                    71
 21: 001V722  MM710                                    71
 22: 001V723  MM710                                    71
 23: 001V724  MM710                                    71
 24: 001V725  MM710                                    71
 25: 001V726  MM710                                    71
 26: 001V727  MM710                                    71
 27: 001V728  MM710                                    71
 28: 001V729  MM710                                    71
 29: 001V730  MM710                                    71
 30: 001V731  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

     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: y y y y y 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 720 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
                                          Total
Ext Ext           Trk       CPN            CPN
Len Code          Grp(s)    Prefix         Len
                                                 Total Administered: 3
 5  332                                    5        Maximum Entries: 240
 5  720                                    5
 4  777                                    4     Note: If an entry applies to
                                                 a SIP connection to Avaya
                                                 Aura(R) Session Manager,
```

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 0                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 0

  Matching                    Insert                Node
  Pattern        Len Del      Digits      Net Conv Num
 7205             5   0                    aar  n
```

5.12. Administer AAR Analysis

Use the "change aar analysis 7" command, and add an entry to specify how to route calls to 7205x. In the example shown below, calls with digits 7205 will be routed as an AAR call using route pattern "71" from **Section 5.9**.

```
change aar analysis 7                                          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
    7203                  5    5      92        unku          n
    7204                  5    5      92        unku          n
    7205                  5    5      71        aar           n
    7206                  5    5      92        unku          n
```

5.13. Administer ISDN Trunk Group

Use the "change trunk-group n" command, where "n" is the existing ISDN trunk group number used to reach the PSTN, in this case "80". Navigate to **Page 3**.

For **Modify Tandem Calling Number**, enter "tandem-cpn-form" to allow for the calling party number from IPC to be modified. By enabling this feature, the calling party number will be sent to PSTN when call is coming from IPC side via a SIP trunk.

```
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
            Used for DCS? n                             Send EMU Visitor CPN? y
   Suppress # Outpulsing? n    Format: natl-pub
 Outgoing Channel ID Encoding: preferred     UUI 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 UUI IE? y     Modify Tandem Calling Number: tandem-cpn-form
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                          Ds1 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 72 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
                     Incoming                                    Outgoing
     CPN             Number   Trk                                Number
 Len Prefix          Format   Grp(s)     Delete  Insert          Format
 5   72                       80                 3035383547      pub-unk
```

5.15. Administer Coverage Forwarding

Use the "change system-parameters coverage-forwarding" command. Enable **QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path**, as shown below. The **Diverted Party Identification** field set to "Principal".

```
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
                                      Diverted Party Identification: principal
COVERAGE
                                Criteria for Logged Off/PSA/TTI Stations? n
                                        Keep Held SBA at Coverage Point? y
       External Coverage Treatment for Transferred Incoming Trunk Calls? n
        Immediate Redirection on Receipt of PROGRESS Inband Information? n
                                            Maintain SBA At Principal? y
             QSIG VALU Coverage Overrides QSIG Diversion with Rerouting? n
                                          Station Hunt Before Coverage? n
FORWARDING
Call Forward Override? n                       Coverage After Forwarding? y
```

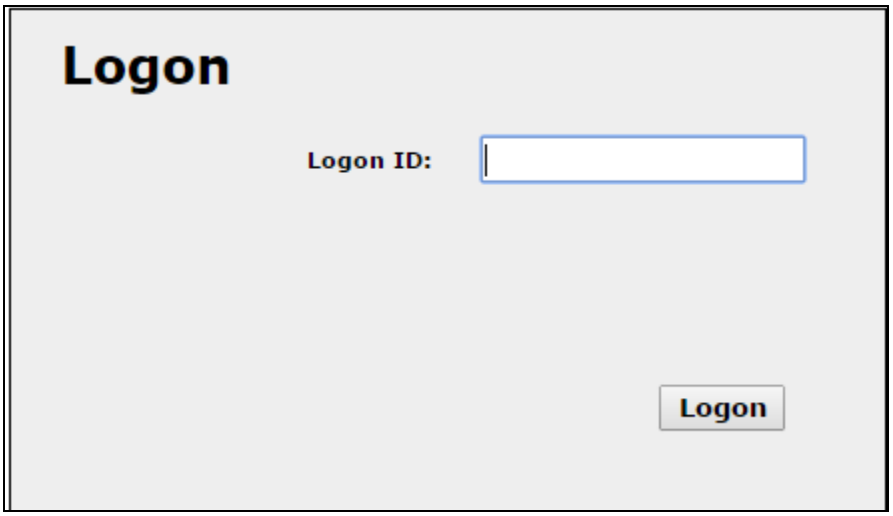
6. Configure Avaya Aura® Messaging

This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Aura® Messaging. Installation and Basic configuration on Avaya Aura® Messaging are assumed to be in place.
The configuration procedures include the following areas:

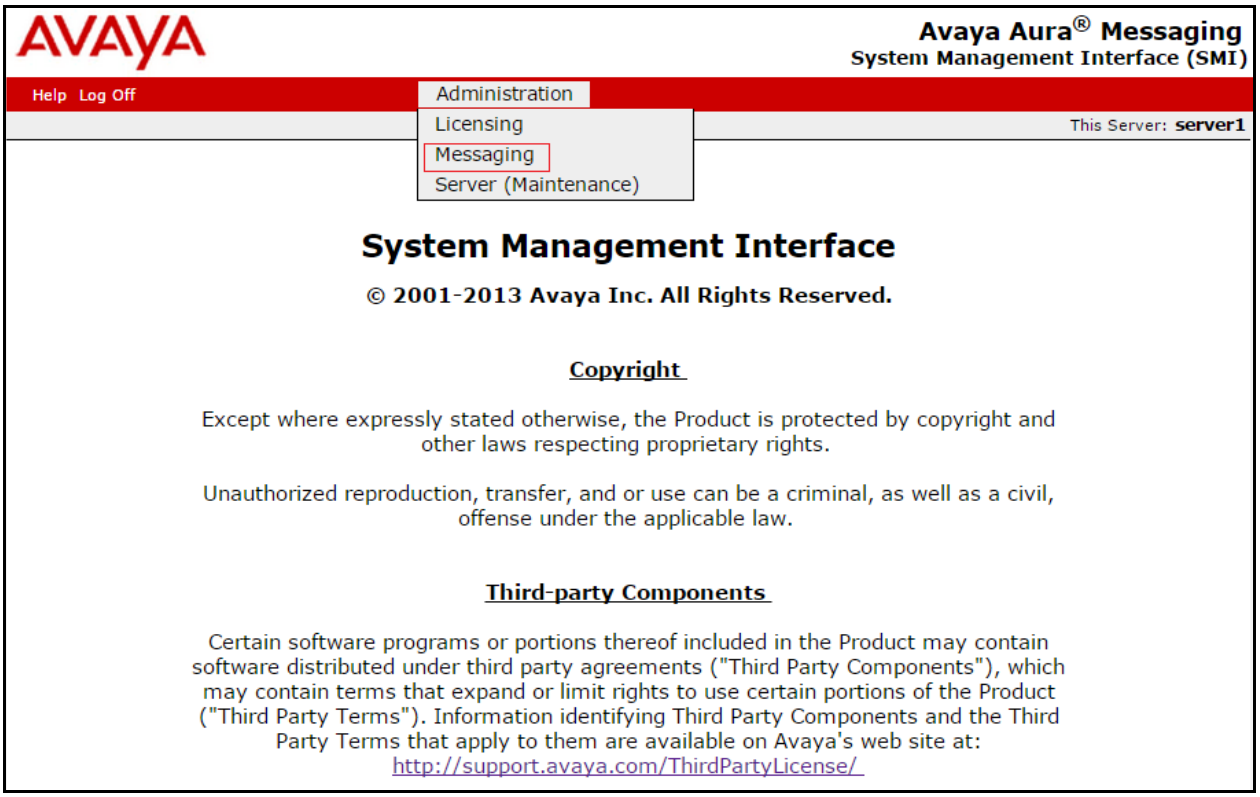
- Launch messaging administration
- Administer subscriber extension ranges
- Administer subscribers

6.1. Launch Messaging Administration

Access the AAM web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of the MSS 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.

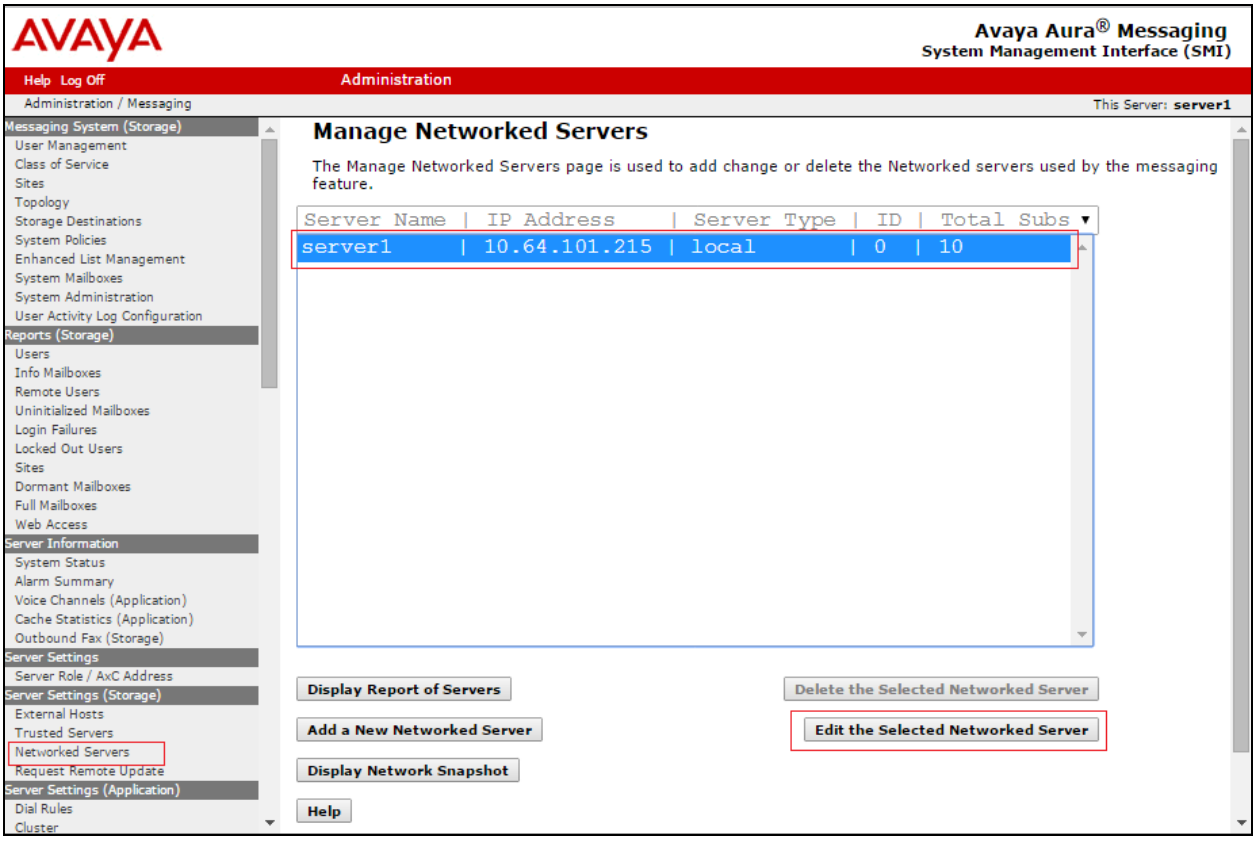


The **System Manager Interface** screen appears, as shown below. Navigate to **Administration → Messaging**.

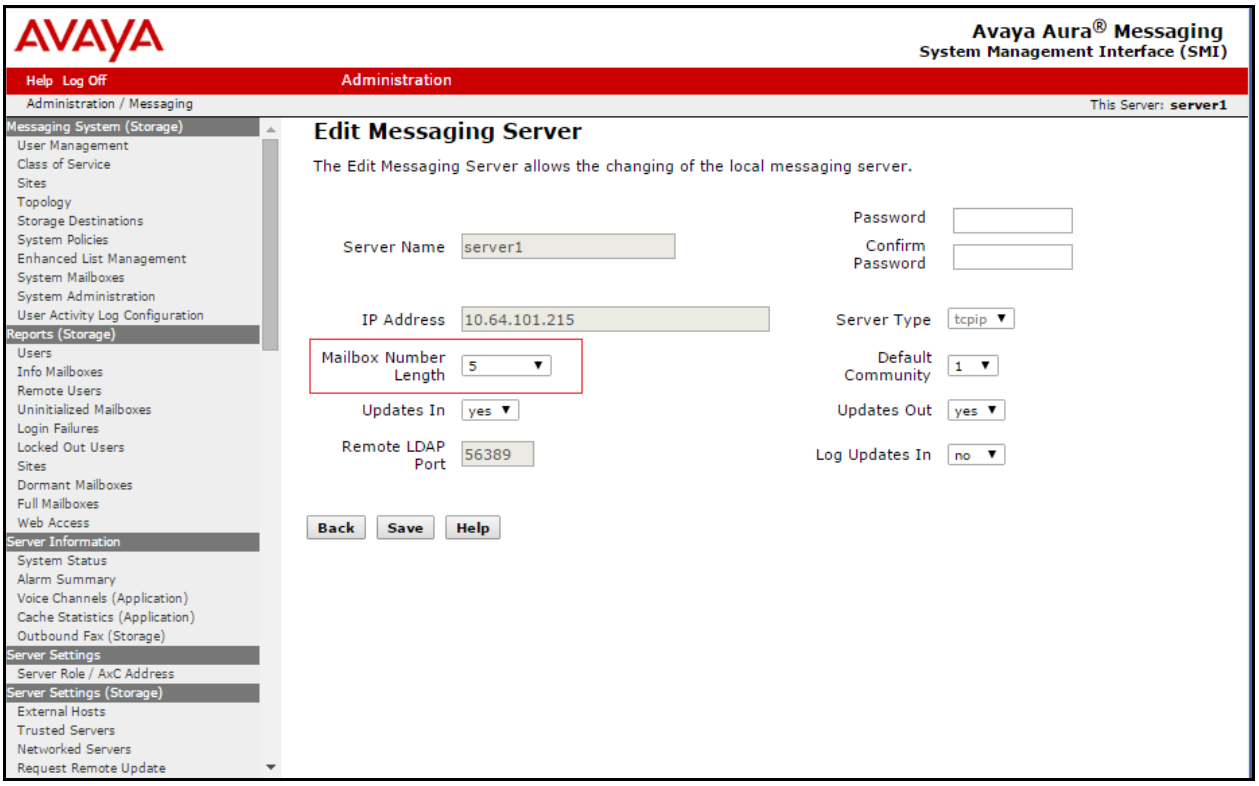


6.2. Administer Subscriber Extension Ranges

Select **Server Settings (Storage)** → **Networked Servers** from the left pane, to display the **Manage Networked Servers** screen. Select a server from the table listing, and click **Edit the Selected Networked Server**.

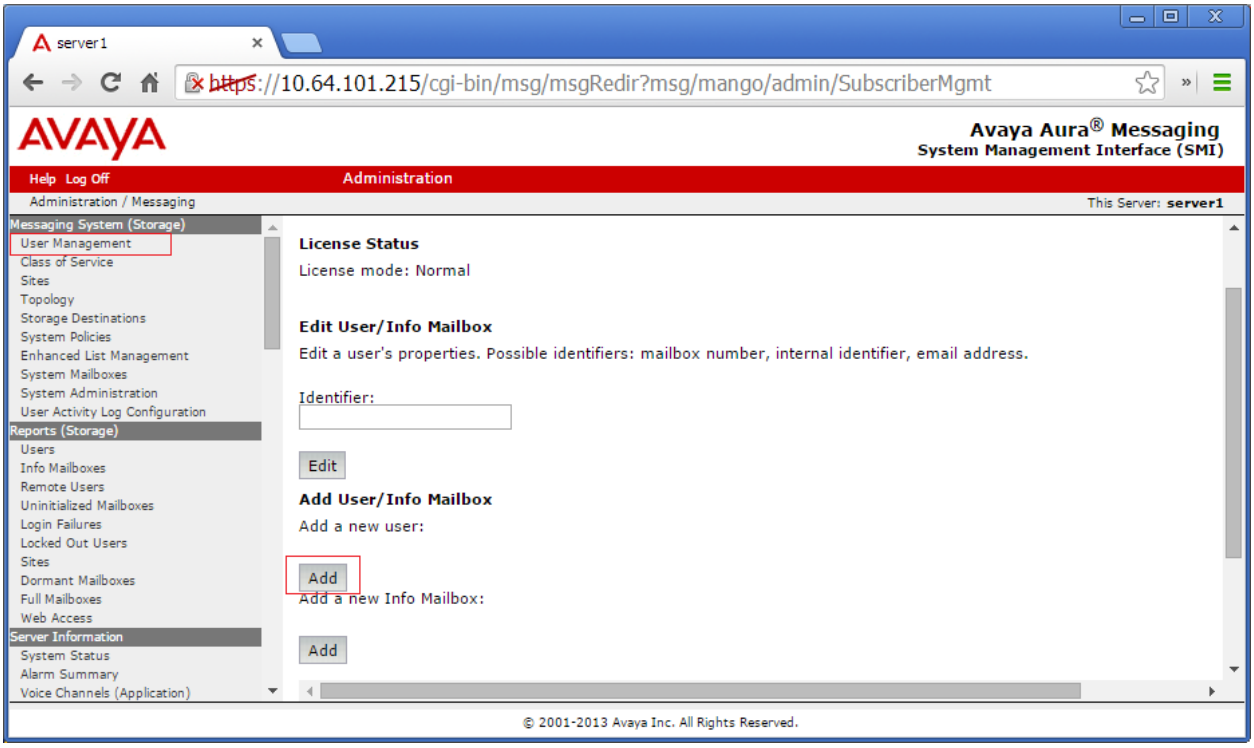


The **Edit Messaging Server** screen is displayed. Verify **Mailbox Number Length** is set to an appropriate length. During the compliance test, a **5** digit length was utilized.



6.3. Administer Subscribers

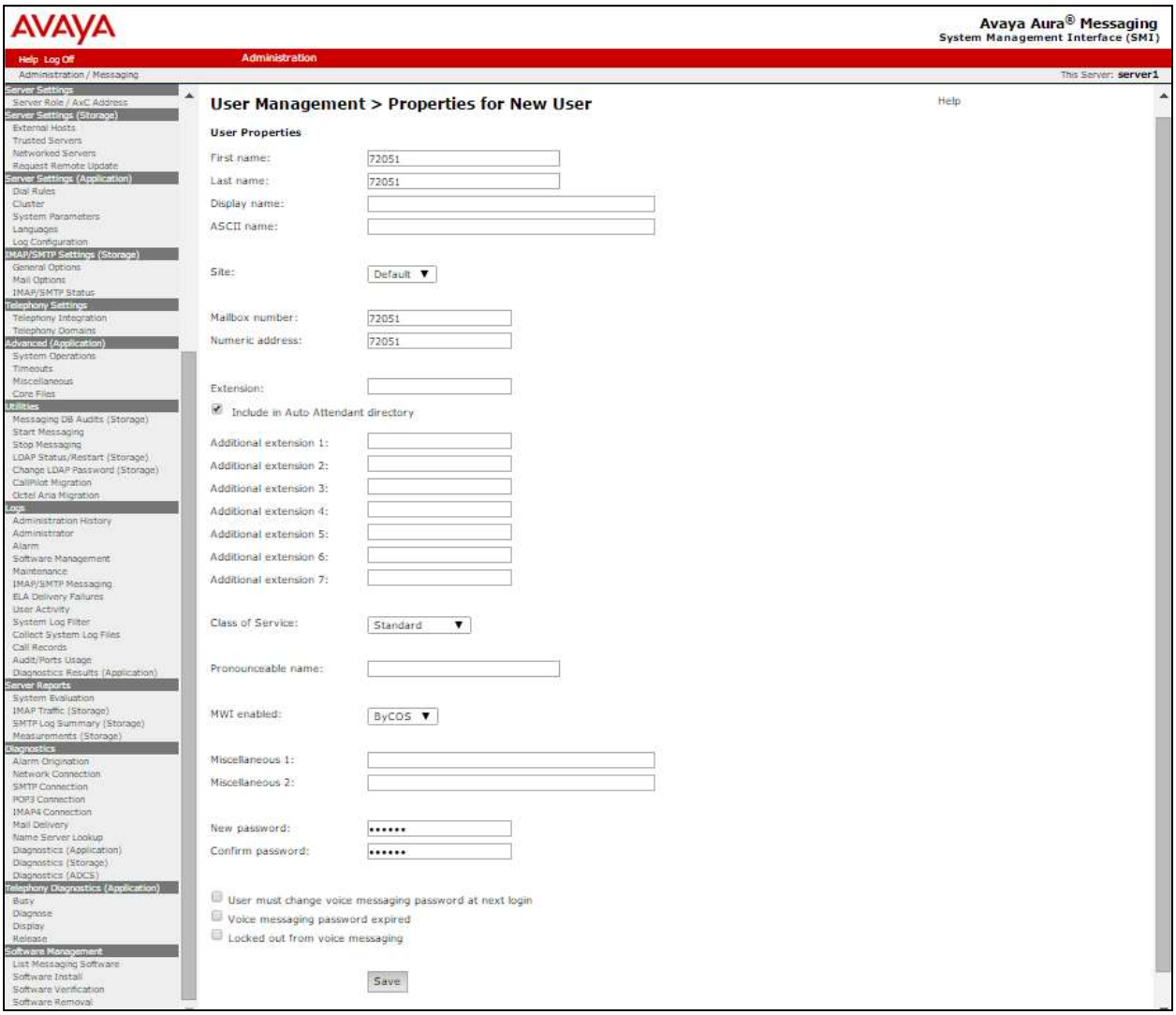
Navigate to **Messaging System (Storage)** → **User Management** from the left pane, to display the **User Management** screen. To add a new subscriber, select the **Add** button under the **Add a new user**: section.



The **User Management > Properties for New User** screen is displayed next. Enter the desired string into the **Last Name**, **First Name**, and **Password** fields.

In the compliance testing, the same telephone extensions for the IPC subscribers were used for the **Mailbox Number**, **Numeric Address**, and **Extension** fields. Select the appropriate **Class Of Service**. Enter a **New password** and **Confirm password**, and retain the default values in the remaining fields. Repeat this section to add all IPC subscribers.

Click the **Save** button.



7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Configuration changes on Session Manager were performed through System Manager. Installation and Basic configuration on Session Manager and System Manager are assumed to be in place.

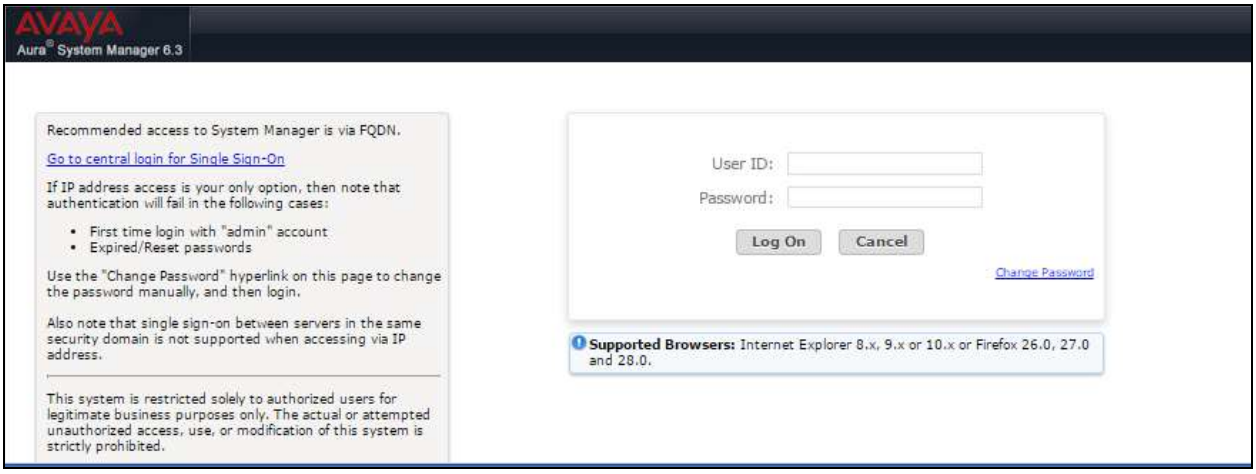
The procedures include the following areas:

- Launch System Manager
- Administer dial patterns

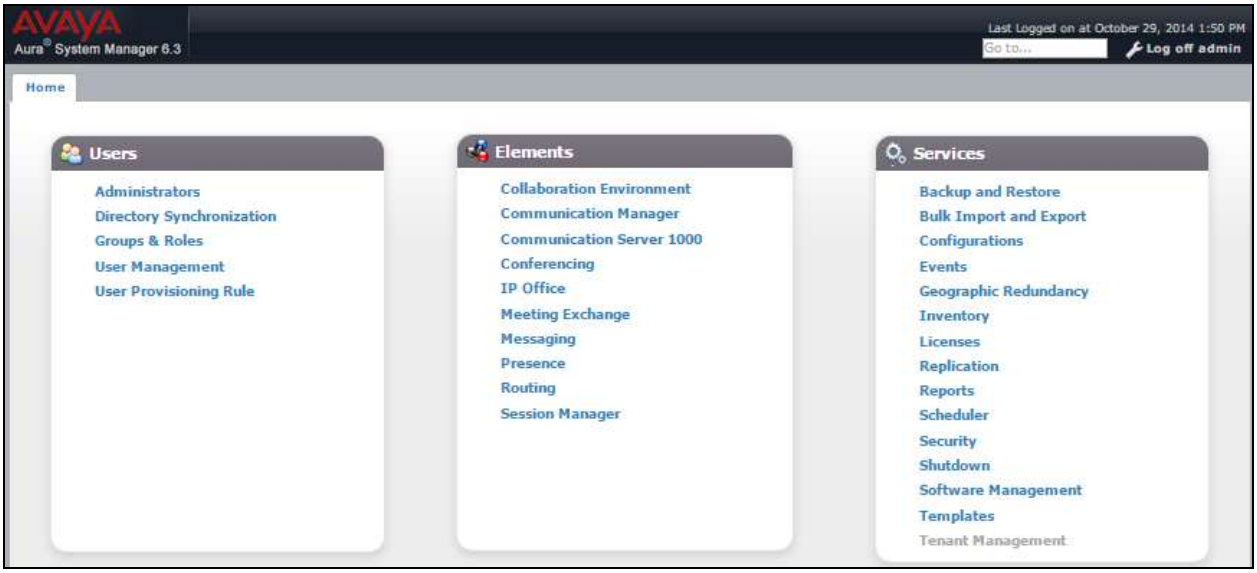
7.1. Launch System Manager

Access the System Manager Web interface by using the URL http://ip-address in an Internet browser window, where "ip-address" is the IP address of the System Manager server. Log in using the appropriate credentials.

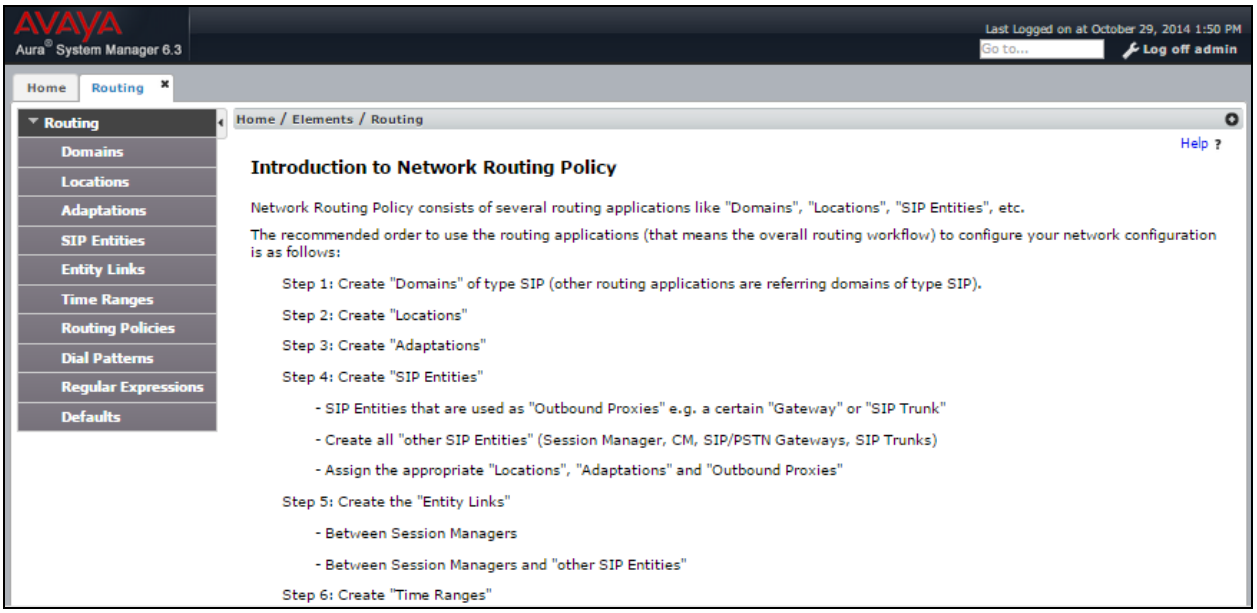
Note: During the compliance the System Manager was installed onto a VMware.



The **Main** screen is displayed. Navigate to **Elements → Routing**



The **Introduction to Network Routing Policy** screen is displayed next.
Navigate to **Routing → Dial Patterns** from the left pane.



7.2. Administer Dial Patterns

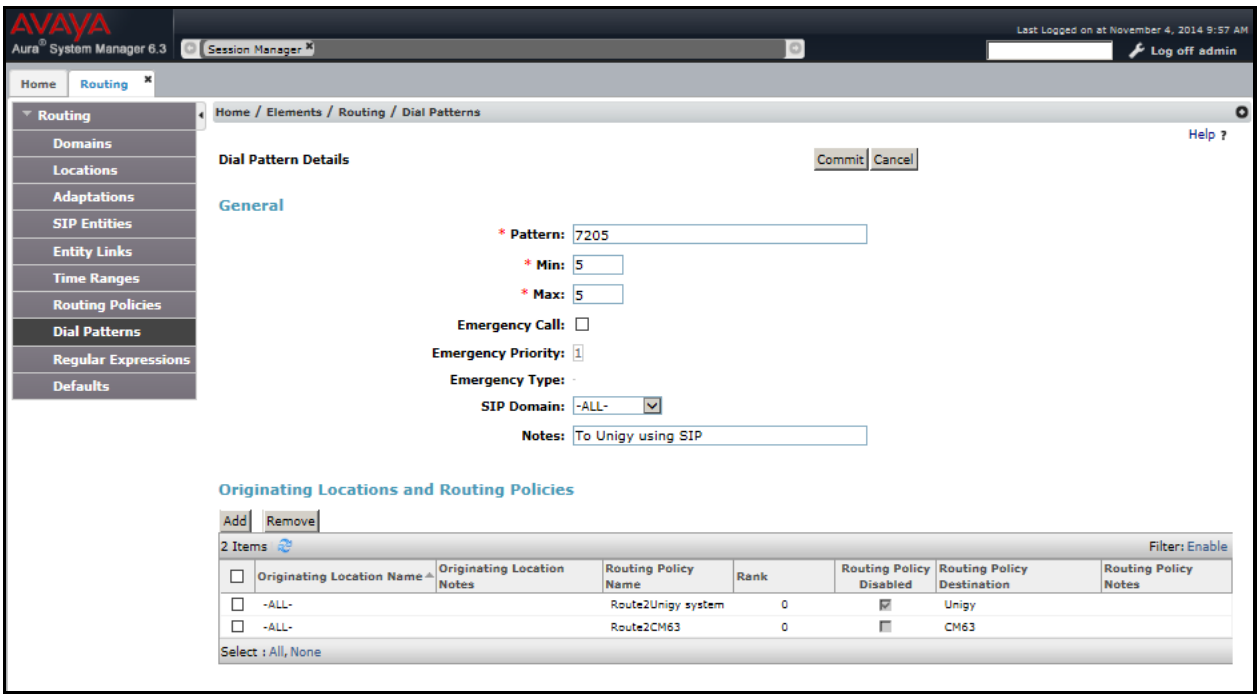
On the **Dial Pattern Details** screen, click **New** in the subsequent screen (not shown) to add a new dial pattern for Avaya Aura® Messaging to reach IPC turret users.

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.

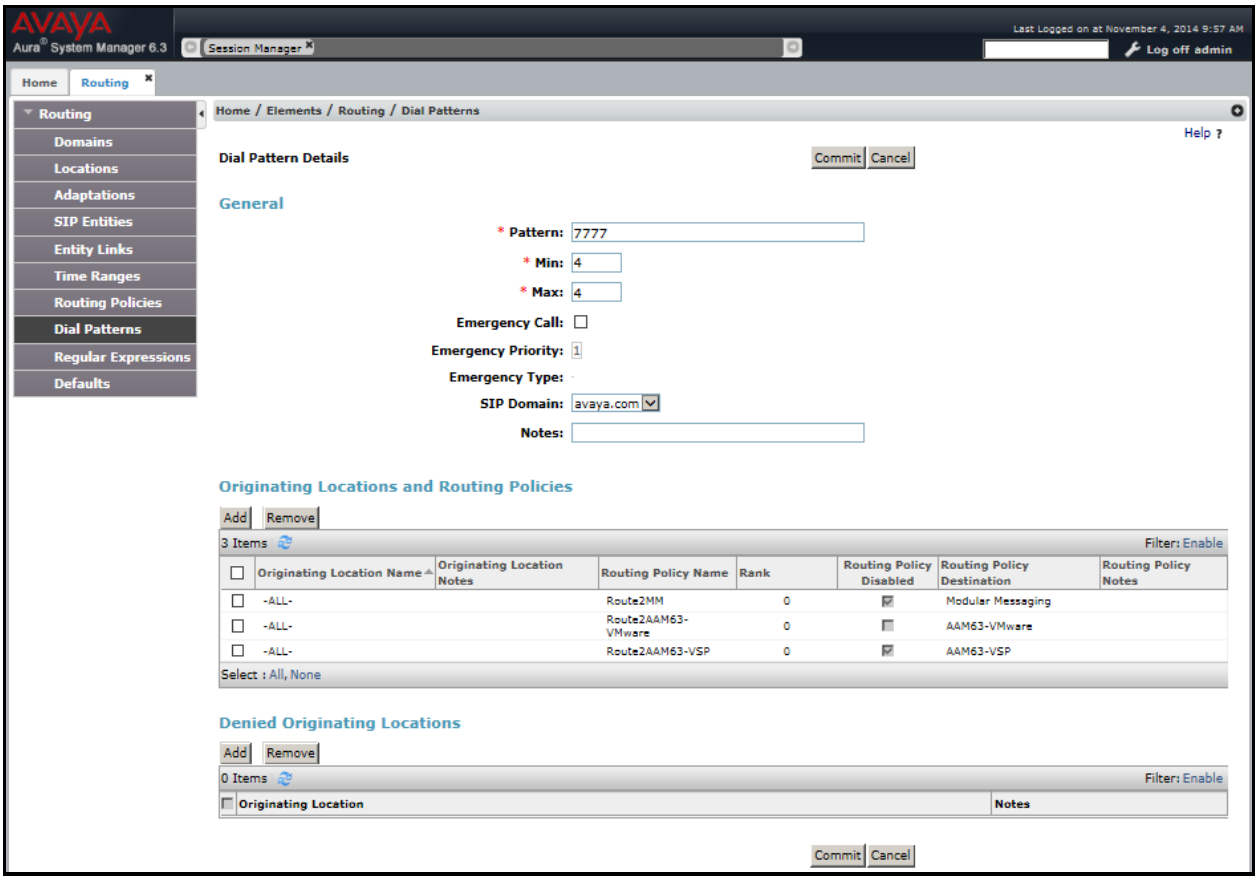
- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** Select the applicable domain for the relevant Communication Manager.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IPC turret users with extensions 7205x. In the compliance test, the policy allowed for call origination from location "Apply The Selected Routing Policies to All Originating Locations", and the destination is Communication Manager, as shown below. Retain the default values in the remaining fields. Avaya Aura® Messaging will dial out to IPC turret users for features such as Call Sender, and the call will be delivered as SIP from Avaya Aura® Messaging to Session Manager, and SIP from Session Manager to Communication Manager, and then QSIG from Communication Manager to Unigy 2.0.1.

After the completion, click **Commit**



The following screen shows the dial pattern for the pilot number, 7777, to Avaya Aura® Messaging.



8. Configure IPC Unigy V2.0.1 Converged Communication Manager

This section provides the procedures for configuring IPC Unigy V2.0.1 Converged Communication Manager. The procedures include the following areas:

- Launch Unigy V2.0.1 Management System
- Administer SIP trunks
- Administer trunk groups
- Administer route lists
- Administer 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.

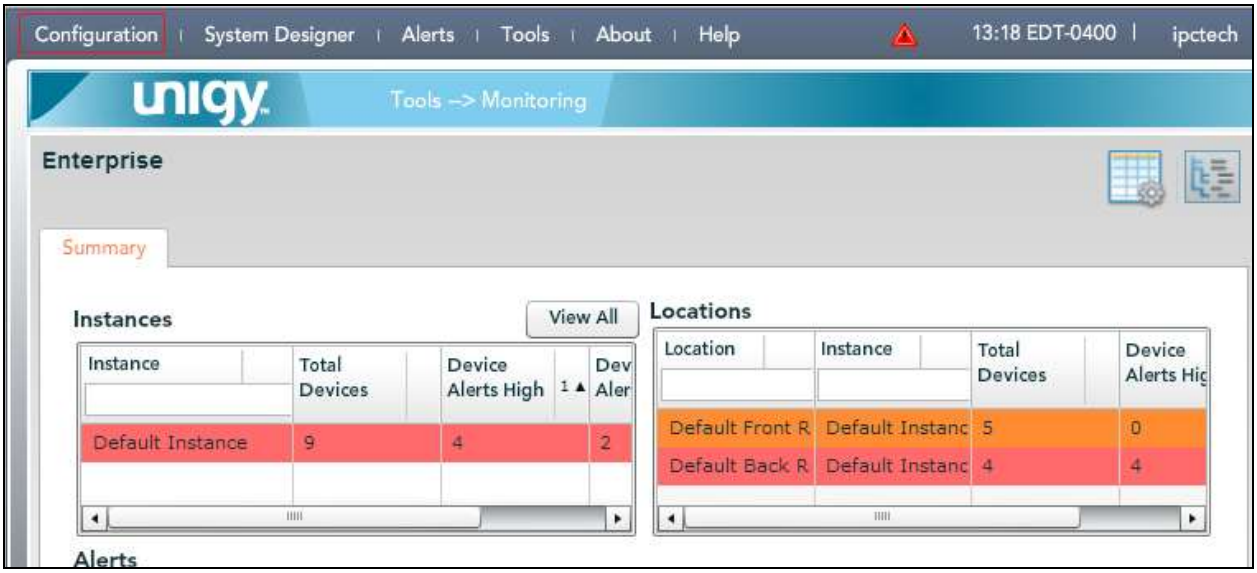
8.1. Launch Unigy V2.0.1 Management System

Access the UnigyV2.0.1 Management System web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of VIP. 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**.

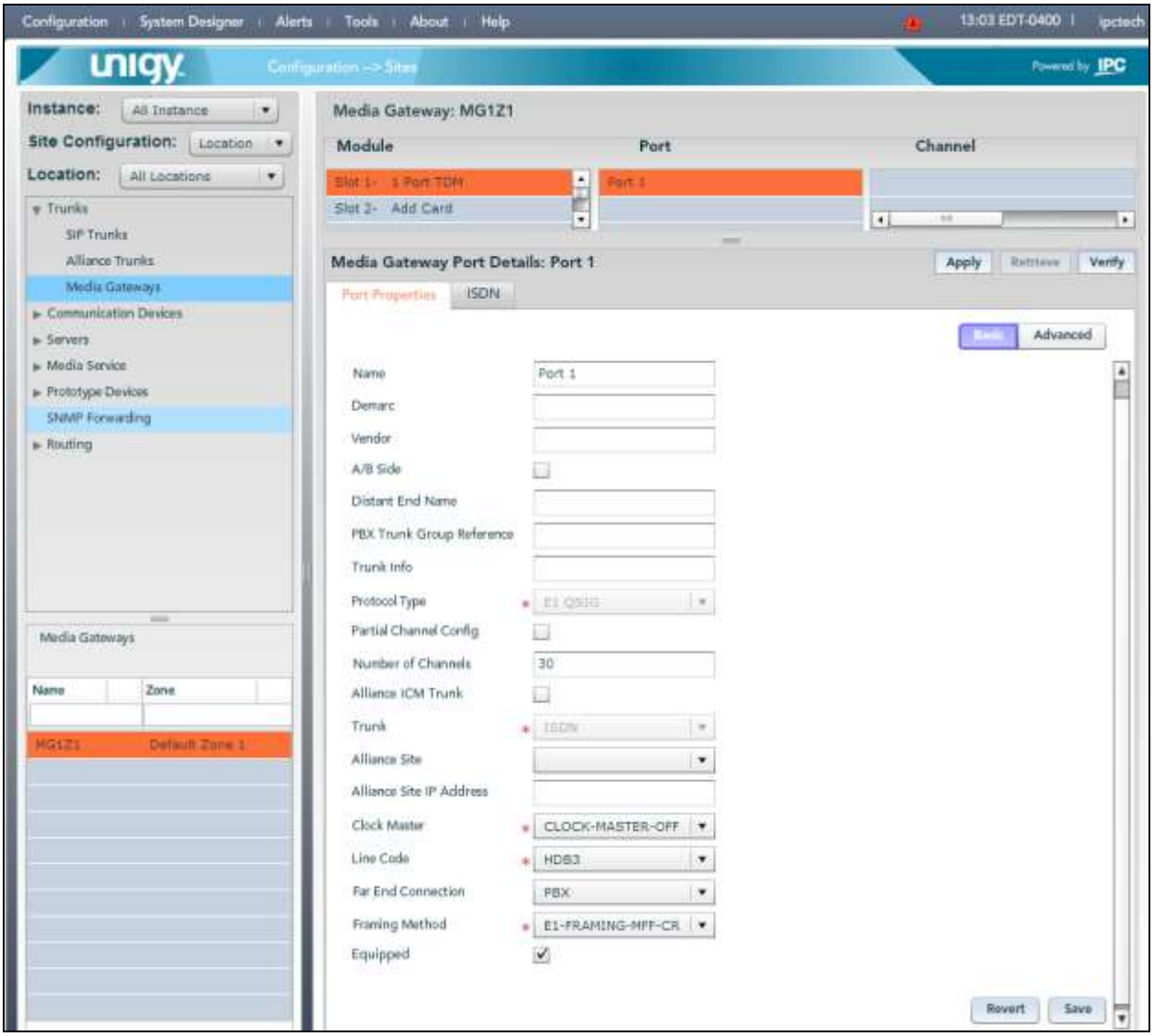
The following screen (Tools -> Monitoring) displays. Navigate to **Configuration → Site**.



8.2. Administer QSIG Trunks

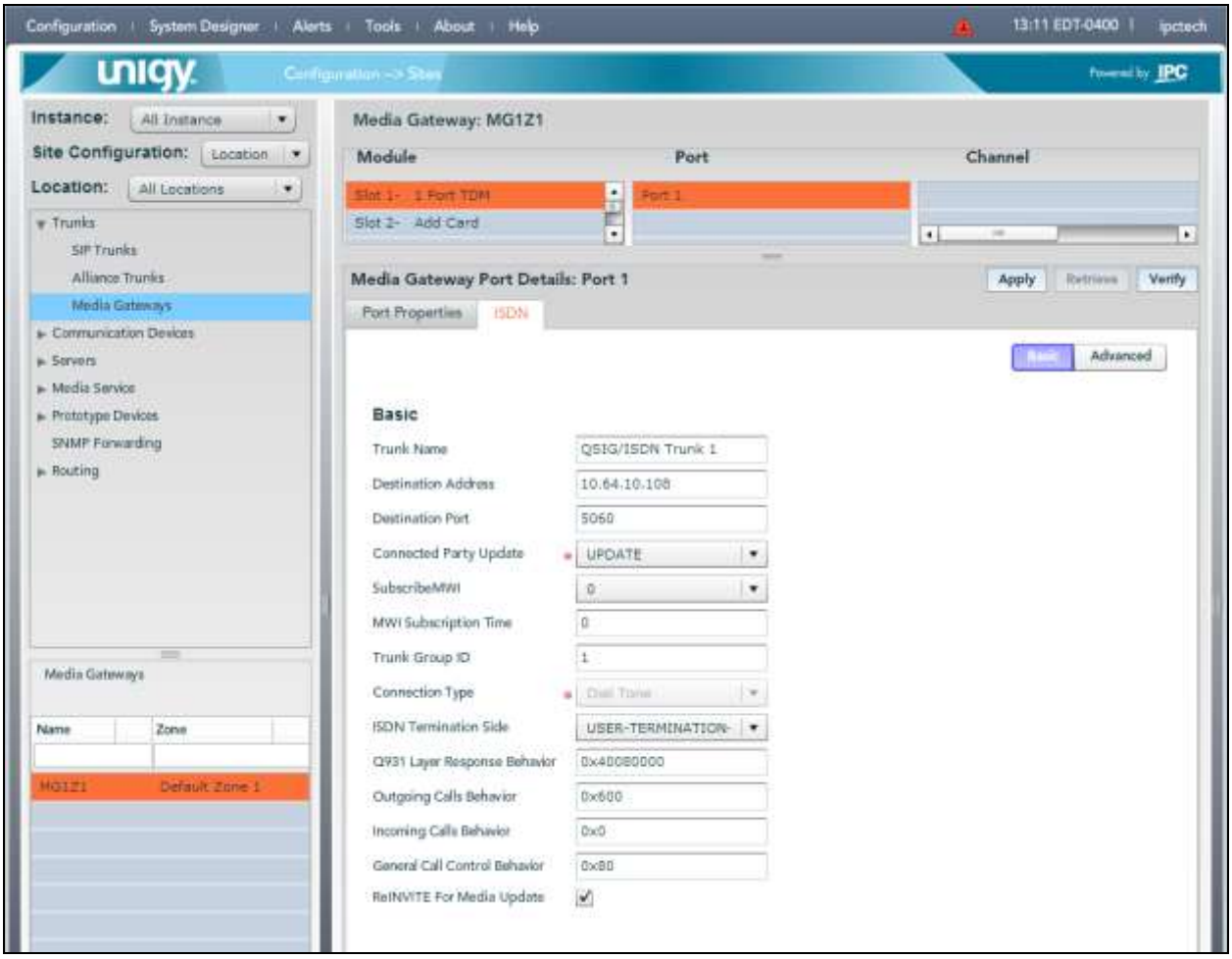
Select **Trunks → Media Gateways** in the left pane. The QSIG trunk is already configured prior to the DevConnect test. This section will only display what was configured.
Select **Slot 1- Port TDM** under **Module**, and **Port 1** under **Port** in the right pane. The **Media Gateway Port Details: Port 1** screen is displayed underneath.

The following screen shows the port properties



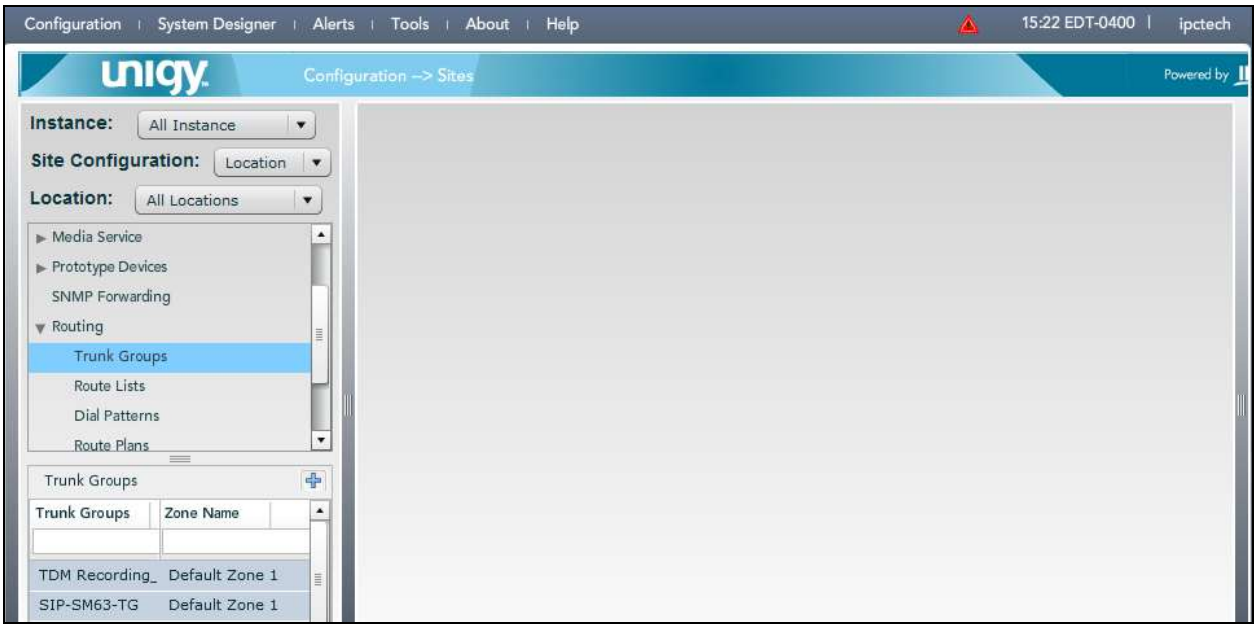
The following screen shows the ISDN configuration. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Trunk Name:** A descriptive name.
- **Destination Address:** Enter the IP address of the IPC Media Gateway
- **Destination Port:** Enter the port number.
- **Connected Party Update:** "UPDATE"
- **ISDN Termination Side** "USER TERMINATION"



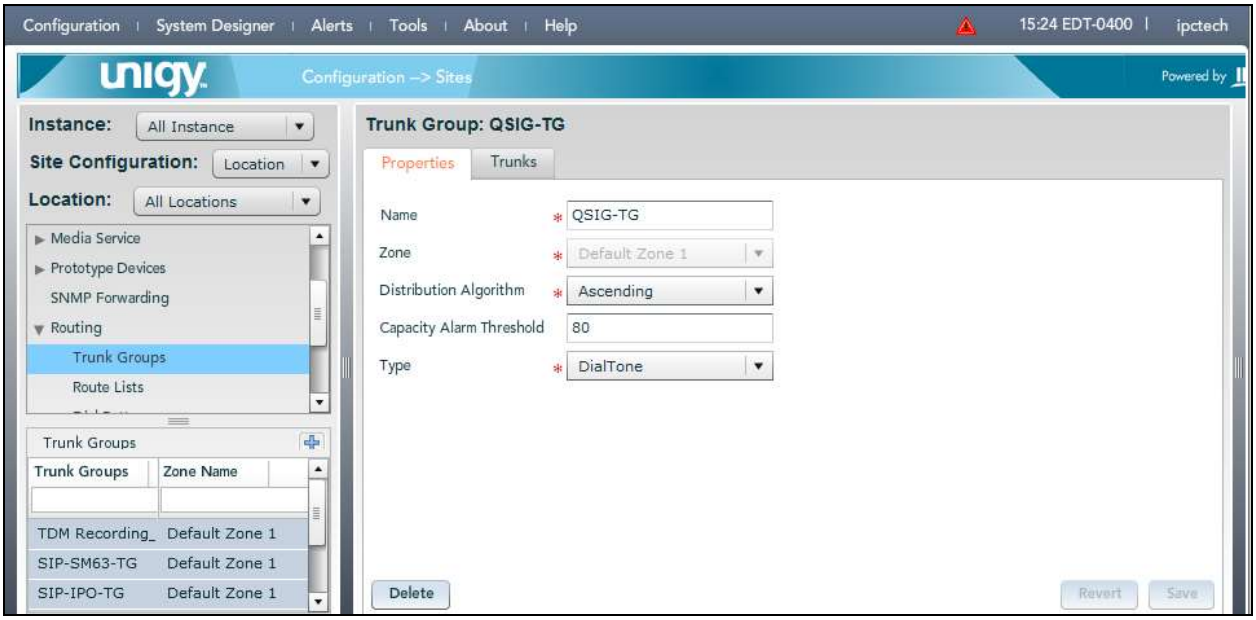
8.3. Administer Trunk Groups

Select **Routing → Trunk Groups** in the left pane, and click the **Add** icon ( ) in the lower left pane to add a new trunk group.



The **Trunk Group** screen is displayed in the right pane. In the **Properties** (default) tab, enter a descriptive **Name**, select "Default Zone 1" for the **Zone** field, and select "Ascending" for the **Distribution Algorithm** field.

Click **Save**.



Select the **Trunk Group** that was previously created in the left pane, and select the **Trunk** tab in the right pane. From the far right pane, select a trunk under **MG Trunks**., and drag it into the middle pane.

Click **Save**.

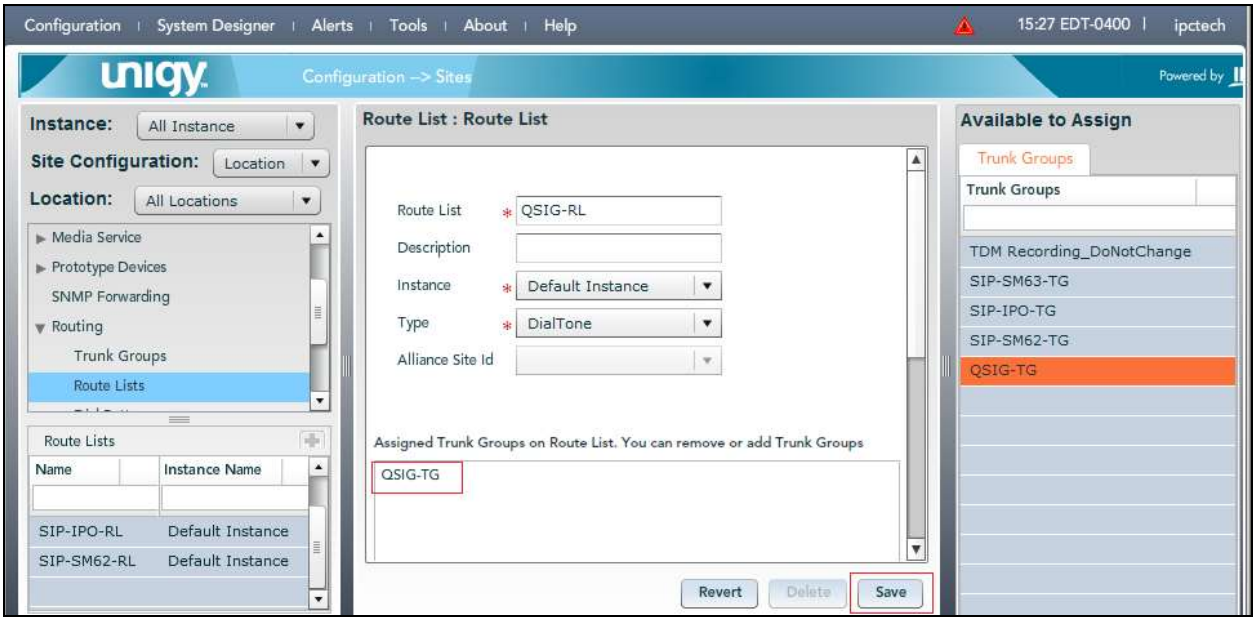
The following screen shows after the dragging of the trunk is completed.

8.4. 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 8.3** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below.

Click **Save**.



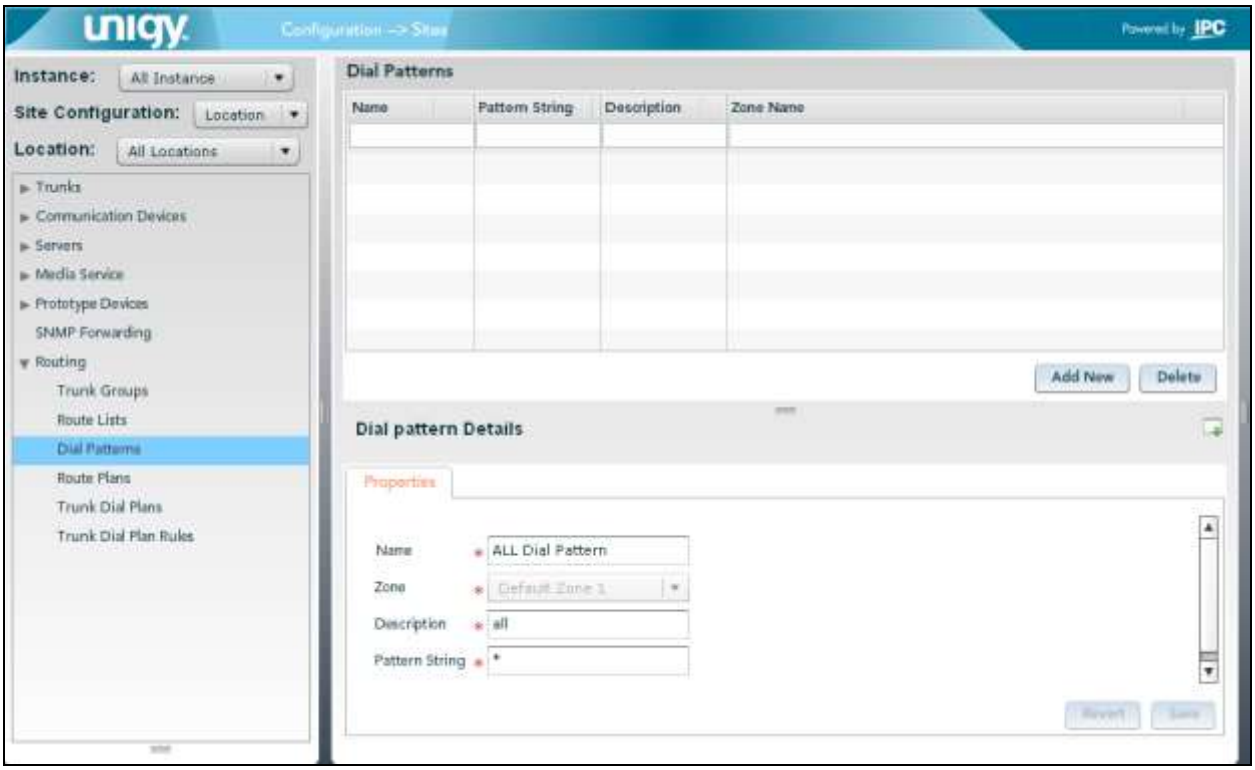
8.5. Administer Dial Patterns

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

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya endpoints, in this case "*" meaning any digits will be sent to QSIG trunk via IPC Media Gateway.

Click **Save**.

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

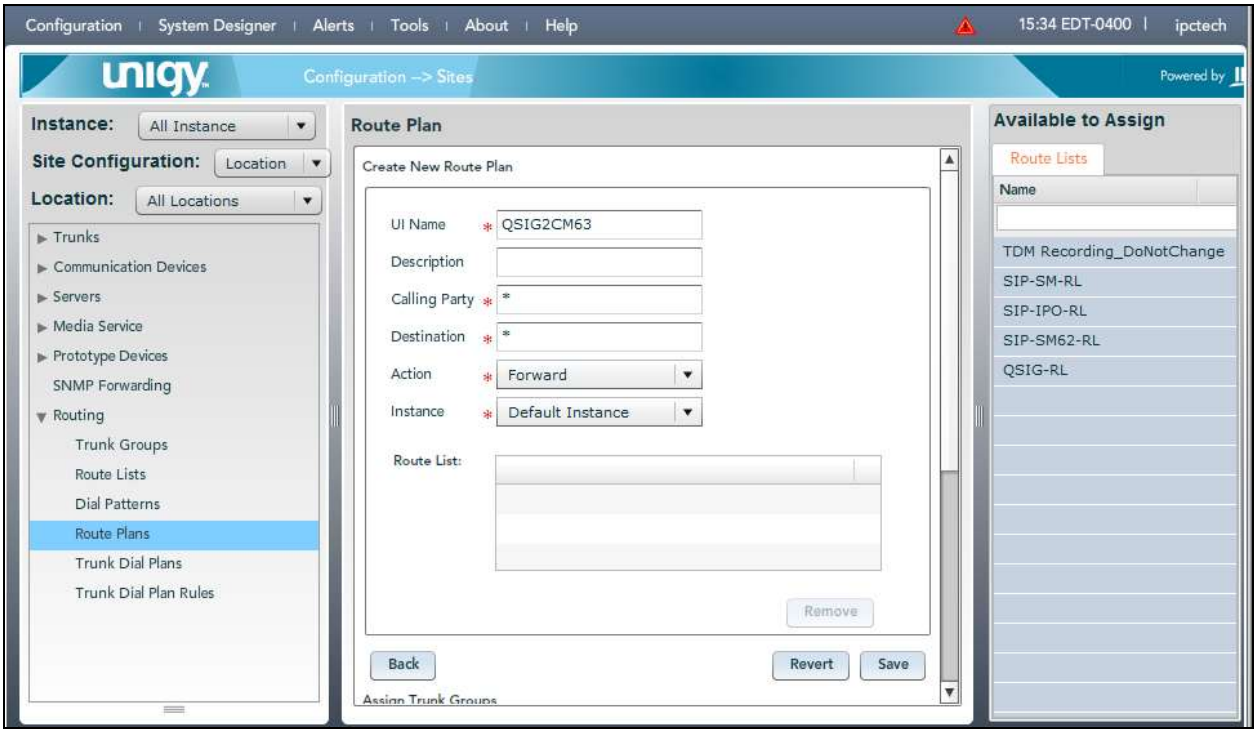


8.6. Administer Route Plans

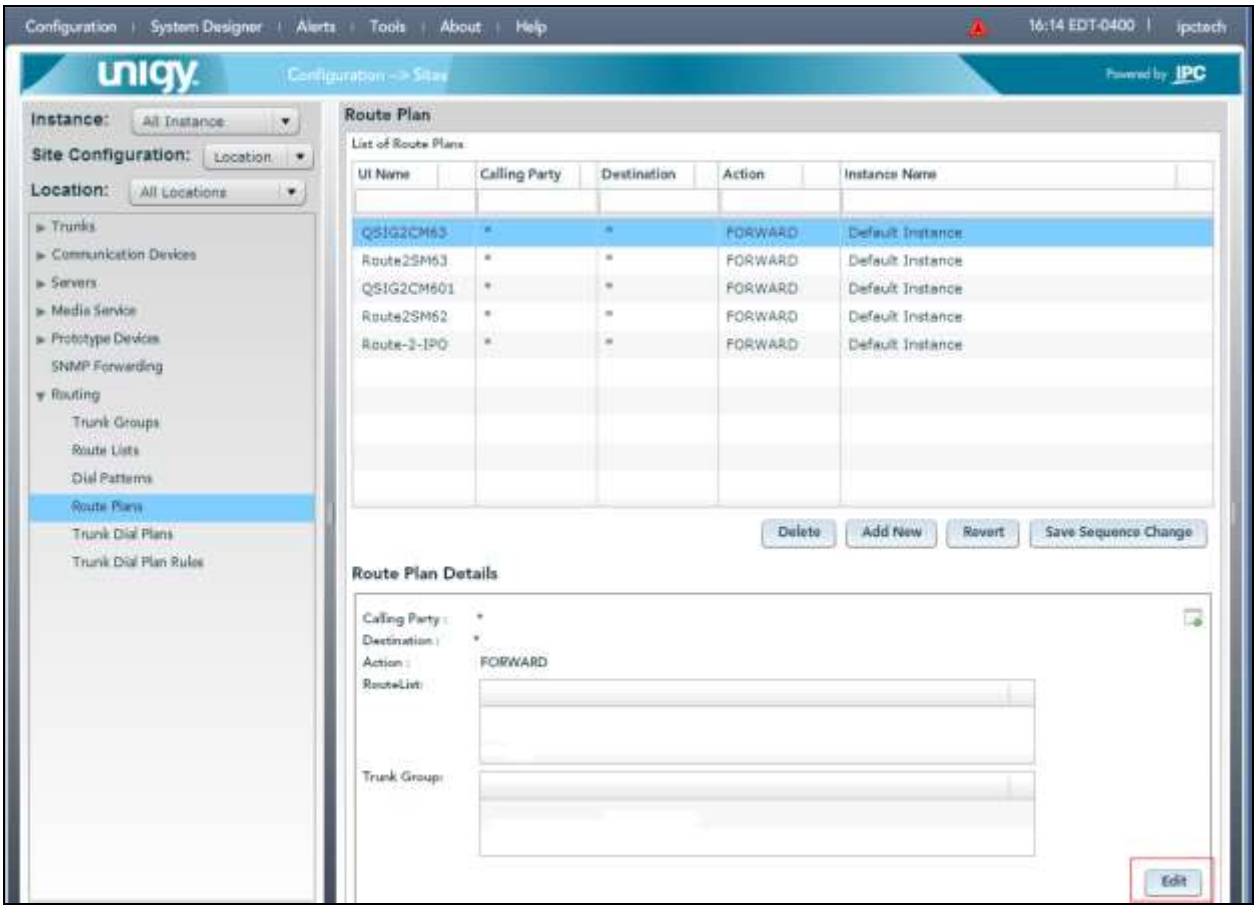
Select **Routing → Route Plans** in the left pane, and click **Add New** (not shown) in the right pane to create a new route plan.

The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter "*" to denote any calling party from UnigyV2.0.1. For **Destination**, select the dial pattern for Avaya endpoints from **Section 8.5**. During the compliance test "*" was used. Select "Forward" for **Action**.

Click **Save**.

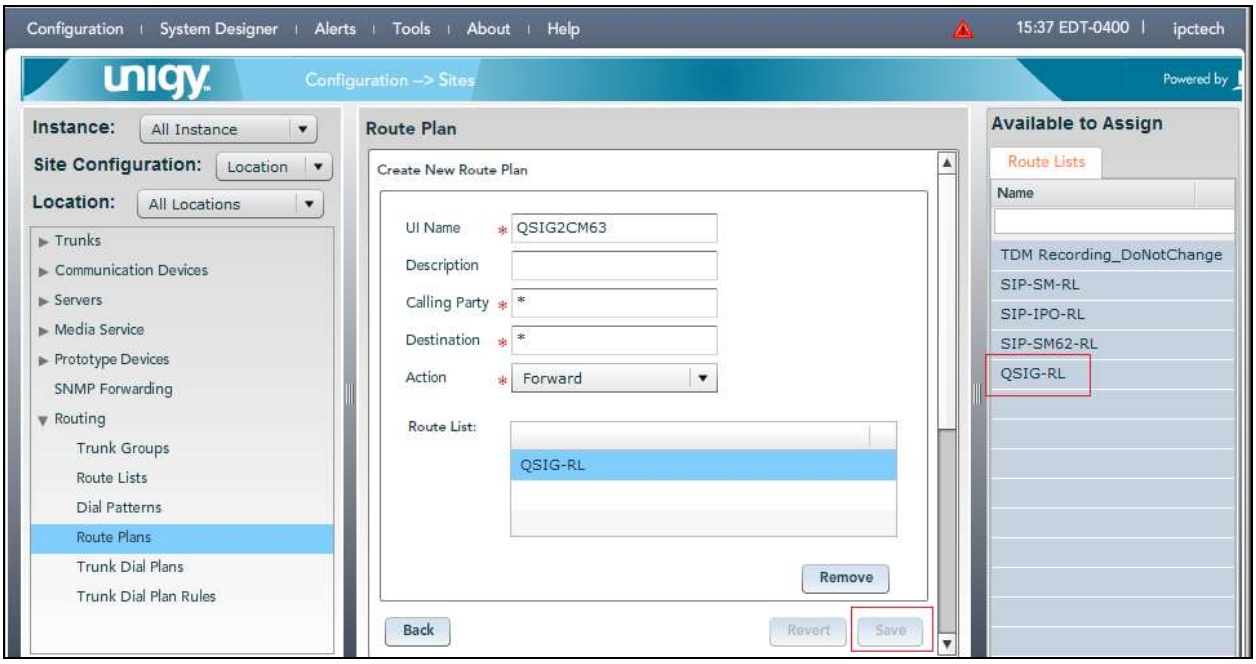


The screen is updated with the newly created route plan. Select the route plan, and click **Edit** toward the bottom of the screen.



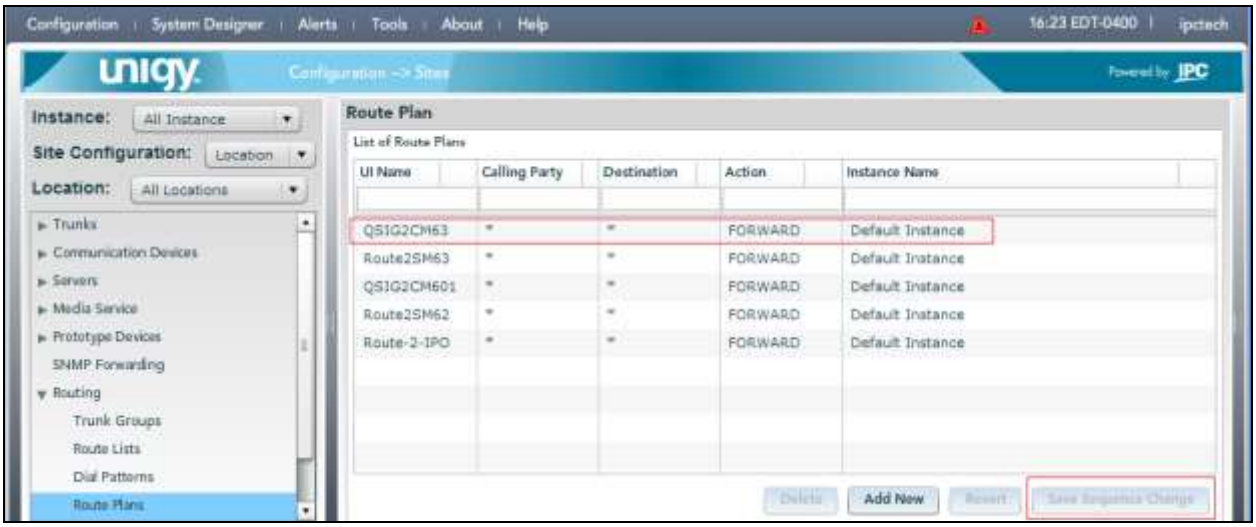
The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 8.4** and drag into the **Route List** sub-section in the middle pane, as shown below.

Click **Save**



Once the route plan configuration is completed, again select **Routing → Route Plans** in the left pane. List of route plans is displayed. Drag the latest route plan you've created, to the top.

Click the **Save Sequence Change** button to finish the Unigy V2.0.1 configuration.



9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Avaya Aura® Messaging, Session Manager, and IPC Unigy 2.0.1.

In Communication Manager, use the "status trunk" command to verify the trunk between Communication Manager and IPC Media Gateway. The following screen shows the status trunk between Communication Manager and and IPC Media Gateway. Verify all members are **in-service/idle**.

```
status trunk 71                                                    Page   1

                              TRUNK GROUP STATUS

Member    Port      Service State       Mtce Connected Ports
                                        Busy

0071/001  001V701   in-service/idle     no
0071/002  001V702   in-service/idle     no
0071/003  001V703   in-service/idle     no
0071/004  001V704   in-service/idle     no
0071/005  001V705   in-service/idle     no
0071/006  001V706   in-service/idle     no
0071/007  001V707   in-service/idle     no
0071/008  001V708   in-service/idle     no
0071/009  001V709   in-service/idle     no
0071/010  001V710   in-service/idle     no
0071/011  001V711   in-service/idle     no
0071/012  001V712   in-service/idle     no
0071/013  001V713   in-service/idle     no
0071/014  001V714   in-service/idle     no
```

Place a call from an IPC turret user to the Aura® Messaging pilot number. Verify that Aura® Messaging recognizes the calling party as a local subscriber.

10. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy 2.0.1 to successfully interoperate with Avaya Aura® Messaging 6.3 and Avaya Aura® Session Manager 6.3 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 6.3. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Release 6.3, Issue 10, June 2014, available at http://support.avaya.com.

2. *Administering Avaya Aura® Messaging*, Release 6.3, Issue 3, August 2014, available at http://support.avaya.com.

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.