Avaya Solution & Interoperability Test Lab

Application Notes for IPC UnigyV3P2 with Avaya Aura® Session Manager 7.0 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC UnigyV3P2 to interoperate with Avaya Aura® Session Manager 7.0 using SIP trunks.

IPC UnigyV3P2 is a trading communication solution. In the compliance testing, IPC UnigyV3P2 used SIP trunks to Avaya Aura® Session Manager. Using the SIP trunks, UnigyV3P2 users on IPC were able to reach users on Avaya Aura® Communication Manager and on the PSTN.

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

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

1. Introduction

These Application Notes describe the configuration steps required for IPC UnigyV3P2 to interoperate with Avaya Aura® Session Manager, and Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

The Unigy Platform is a unified trading communications system designed specifically to make the entire trading ecosystem more productive, intelligent and efficient. Based on an SIP-enabled, open and distributed architecture, Unigy utilizes the latest, standards-based technology to create a groundbreaking, innovative Unified Trading Communications (UTC) solution.

Unigy offers a portfolio of devices and applications that serve the entire trading workflow, across the front, middle and back offices.

2. General Test Approach and Test Results

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

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to IPC UnigyV3P2.

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, display, G.711MU, G.711A, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, blinded/attended conference, barge-in, and long duration calls.

The serviceability testing focused on verifying the ability of IPC UnigyV3P2 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to IPC UnigyV3P2.

2.2. Test Results

All test cases were executed and verified. The following were the observations on IPC UnigyV3P2 from the compliance testing:

- Even when IPC UnigyV3P2 is configured with UDP, the TCP protocol must be configured to be allowed on Session Manager as UnigyV3P2 switches over to use TCP for diversions.
- During the compliance test, Network Call Redirection (shuffling) was disabled, as shown in **Section 5.3**. (IPC requested)
- A blind conference initiated by an IPC turret with 96x1 Avaya SIP Deskphones did not work. This issue is being investigated by Avaya. A supervised conference from IPC turret with Avaya 96x1 SIP Deskphones worked properly. Also with 96x0 Avaya SIP Deskphones blind and supervised conferences worked as expected.

2.3. Support

Technical support on IPC UnigyV3P2 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 UnigyV3P2 consists of the Media Manager (MM), Converged Communication Manager (CCM), and Turrets. The Media Manager and Converged Communication Manager are typically deployed on separate servers. In the compliance testing, the same server hosted the Media Manager and Converged Communication Manager.

SIP trunks are used from IPC UnigyV3P2 to Session Manager, to reach users (SIP and H.323) and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Avaya and IPC. Unique extension ranges were associated with Communication Manager users (7200x for H.323 and 7202x for SIP), and IPC turret users (7205x).

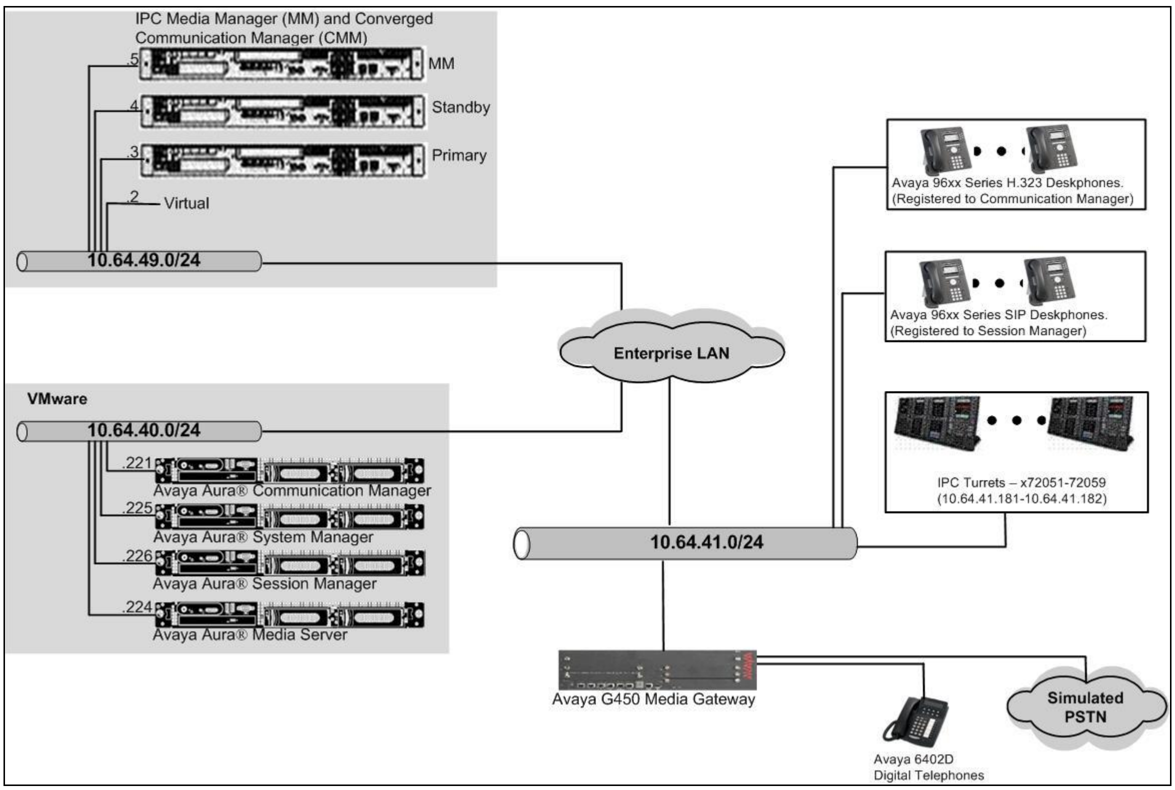


Figure 1: Test Configuration of IPC UnigyV3P2

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	R017x.00.0.441.0-22477
Avaya G450 Media Gateway	37.19
Avaya Aura® Media Server	7.7.0.226
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0.3929
Avaya 96xx IP Deskphone (H.323) 9621G 9650C	 6.6 3.25
Avaya 96x1 IP Deskphone (SIP)	7.0.0.39
IPC UnigyV3P2 • Media Manager • Converged Communication Manage • Turret	 03.00.00.02.0006 03.00.00.02.0006 03.00.00.02.0006

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer ISDN trunk group
- Administer tandem calling party number

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for the IPC turret users.

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  27
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  2
                   Maximum Video Capable IP Softphones: 2400  2
                       Maximum Administered SIP Trunks: 4000  70
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

5.2. 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 call to IPC (outgoing trunk to outgoing trunk). For ease of interoperability 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
```

5.3. Administer SIP Signaling Group

Use the "add signaling-group n" command, where "n" is an available signaling group number, in this case "92". Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** "sip"
- **Transport Method:** "tls"
- **Near-end Node Name:** An existing C-LAN node name or procr.
- **Far-end Node Name:** The existing Session Manager node name.
- **Near-end Listen Port:** An available port for integration on Communication Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** Set to "1".
- **Direct IP-IP Audio Connection:** Enable or Disable the field by entering "y" or "n".

```
add signaling-group 92                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 92             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                  Far-end Node Name: SM-1
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1
                                   Far-end Secondary Node Name:
Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                  Alternate Route Timer(sec): 6
```

5.4. Administer SIP Trunk Group

Use the "add trunk-group n" command, where "n" is an available trunk group number, in this case "92". Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** "sip"
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** "tie"

```
add trunk-group 92                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 92                   Group Type: sip          CDR Reports: y
  Group Name: SM_41_42                    COR: 1        TN: 1        TAC: 1092
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 92
                                                     Number of Members: 10
```

Navigate to Page 3, and enter "private" for Numbering Format.

```
add trunk-group 92                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n



                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Navigate to Page 4, and disable Network Call Redirection (REFER) since REFER did not work with Unigy V2. Enter “101” for Telephone Event Payload Type.

```
add trunk-group 92                                                Page   4 of  21
                             PROTOCOL VARIATIONS

                                      Mark Users as Phone? y
repend '+' to Calling/Alerting/Diverting/Connected Number? n
                      Send Transferring Party Information? y
                                 Network Call Redirection? n

                                    Send Diversion Header? n
                                  Support Request History? y
                             Telephone Event Payload Type: 101


                       Convert 180 to 183 for Early Media? n
                 Always Use re-INVITE for Display Updates? n
                       Identity for Calling Party Display: P-Asserted-Identity
           Block Sending Calling Party Location in INVITE? n
                Accept Redirect to Blank User Destination? n
                                             Enable Q-SIP? n
```

5.5. Administer IP Network Region

Use the "change ip-network-region n" command, where "n" is the existing far-end network region number used by the SIP signaling group from **Section 5.4**.

For **Authoritative Domain**, set to "avaya.com". Enter a descriptive **Name**. Enter "yes" for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with IPC UnigyV3P2.

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name:                         Stub Network Region: n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16390                       IP Audio Hairpinning? n
   UDP Port Max: 16999
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```

5.6. Administer IP Codec Set

Use the "change ip-codec-set n" command, where "n" is the codec set number from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that IPC UnigyV3P2 supports G.711 and G.729. For G.729, IPC needs to install a license.

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence       Frames   Packet
    Codec        Suppression   Per Pkt  Size(ms)
 1: G.711MU           n           2        20
 2:
 3:
 4:
 5:
 6:
 7:
```

5.7. Administer Route Pattern

Use the "change route-pattern n" command, where "n" is an existing route pattern number to be used to reach IPC, in this case "92". Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

```
change route-pattern 92                                         Page   1 of   3
                   Pattern Number: 92  Pattern Name: no IMS SIP trk
                            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: 92   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  n            rest                                        none
2: y y y y y n  n            rest                                        none
```

5.8. Administer Private Numbering

Use the "change private-numbering 0" command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 5.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 720 and routed to trunk group 92 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  720              92                          5      Total Administered: 10
 5  720              93                          5         Maximum Entries: 540
```

5.9. 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
 141044          11   0                   ars   n
 2               5    0                   aar   n
 20004           5    0                   aar   n
 50000           5    0                   aar   n
 53005           5    0                   aar   n
 7050            4    0                   aar   n
 7202            5    0                   aar   n
 7203            5    0                   aar   n
 7204            5    0                   aar   n
 7205            5    0                   aar   n
```

5.10. Administer AAR Analysis

Use the "change aar analysis 7" command, and add an entry to specify how to route calls to 7205x. In the highlighted example shown below, calls with digits 7205x will be routed using route pattern "92" from **Section 5.7**.

```
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       92        unku           n
    7206                   5    5       92        unku           n
    7301                   5    5       92        unku           n
    770                    5    5       26        aar            n
    7777                   4    4       92        unku           n
    780                    5    5       92        unku           n
    79000                  5    5       99        aar            n
                                                                 n
                                                                 n
                                                                 n
```

5.11. 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.

```
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: y
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
```

5.12. 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
                      Incoming                                      Outgoing
     CPN              Number    Trk                                 Number
 Len Prefix           Format    Grp(s)      Delete  Insert          Format
5   7205                       80                  303xxxyyyy      pub-unk
```

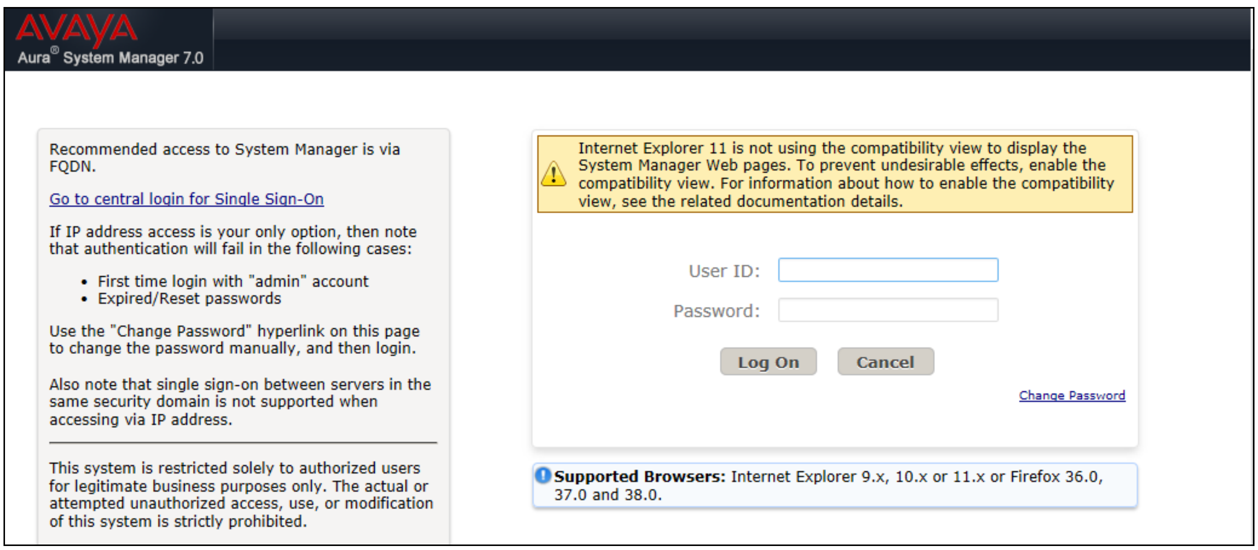
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. It is assumed that the basic configuration is already in place. This Section discusses the following area:

- Administer locations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

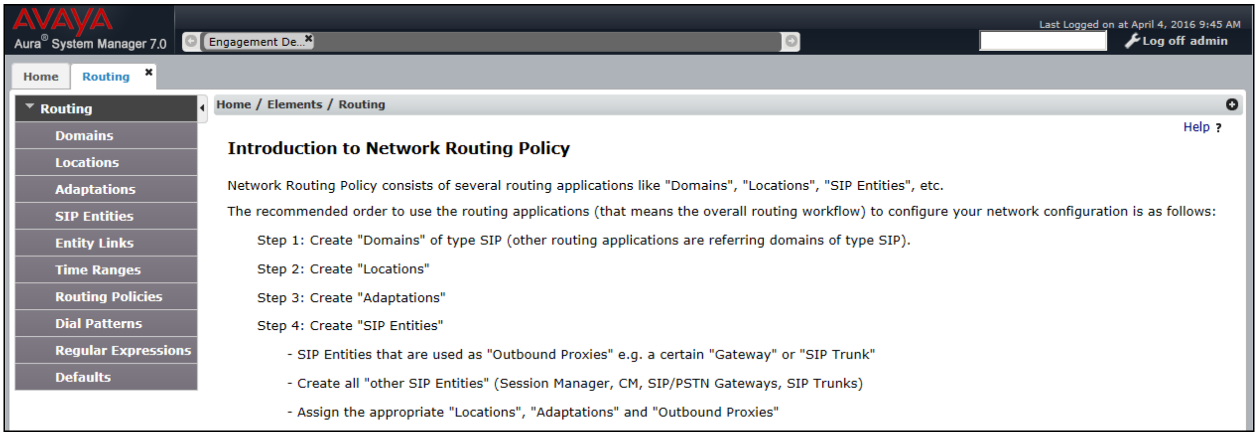
6.1. Launch System Manager

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

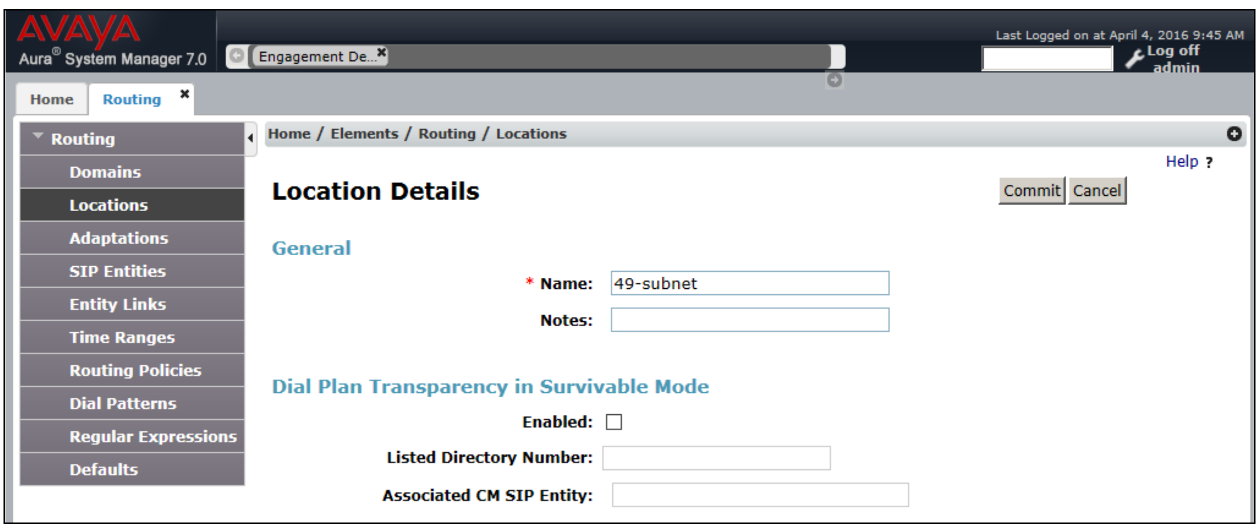


6.2. Administer Locations

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



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



6.3. Administer SIP Entities

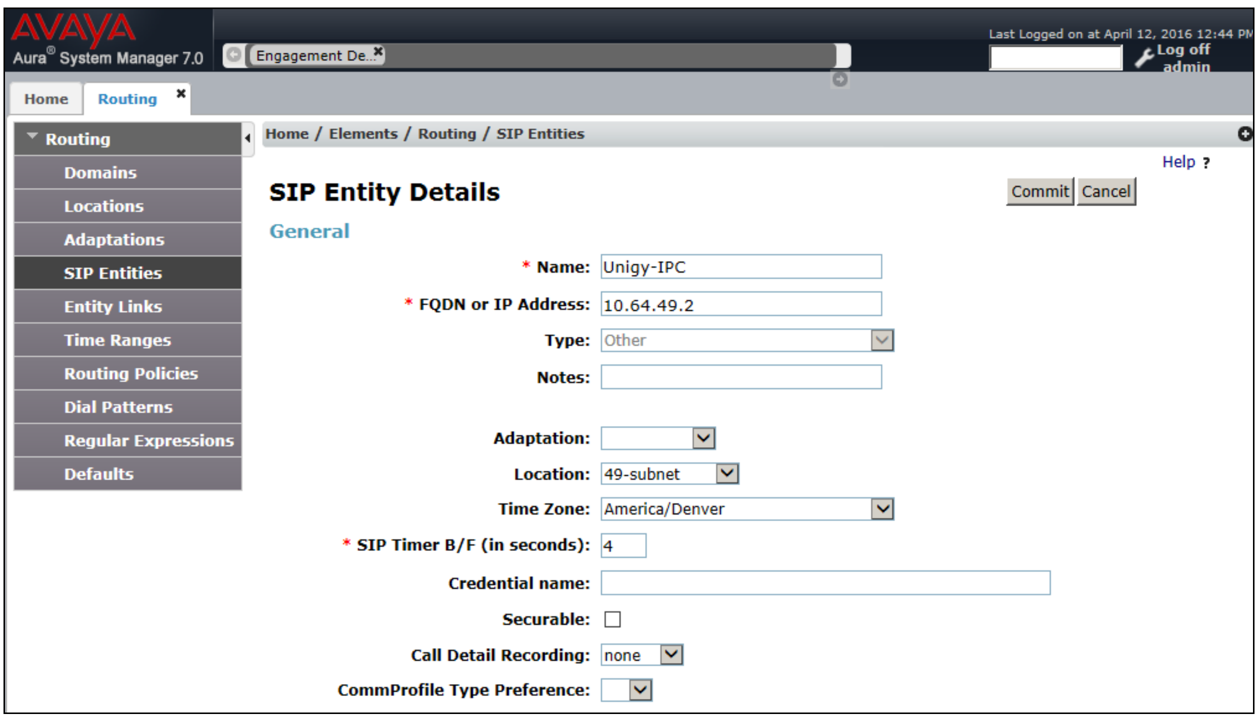
Add two new SIP entities, one for IPC, and another for the new SIP trunks for Communication Manager.

6.3.1. IPC SIP Entity

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for IPC.

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

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the IPC Media Manager server.
- **Type:** "Other"
- **Location:** Select the IPC location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

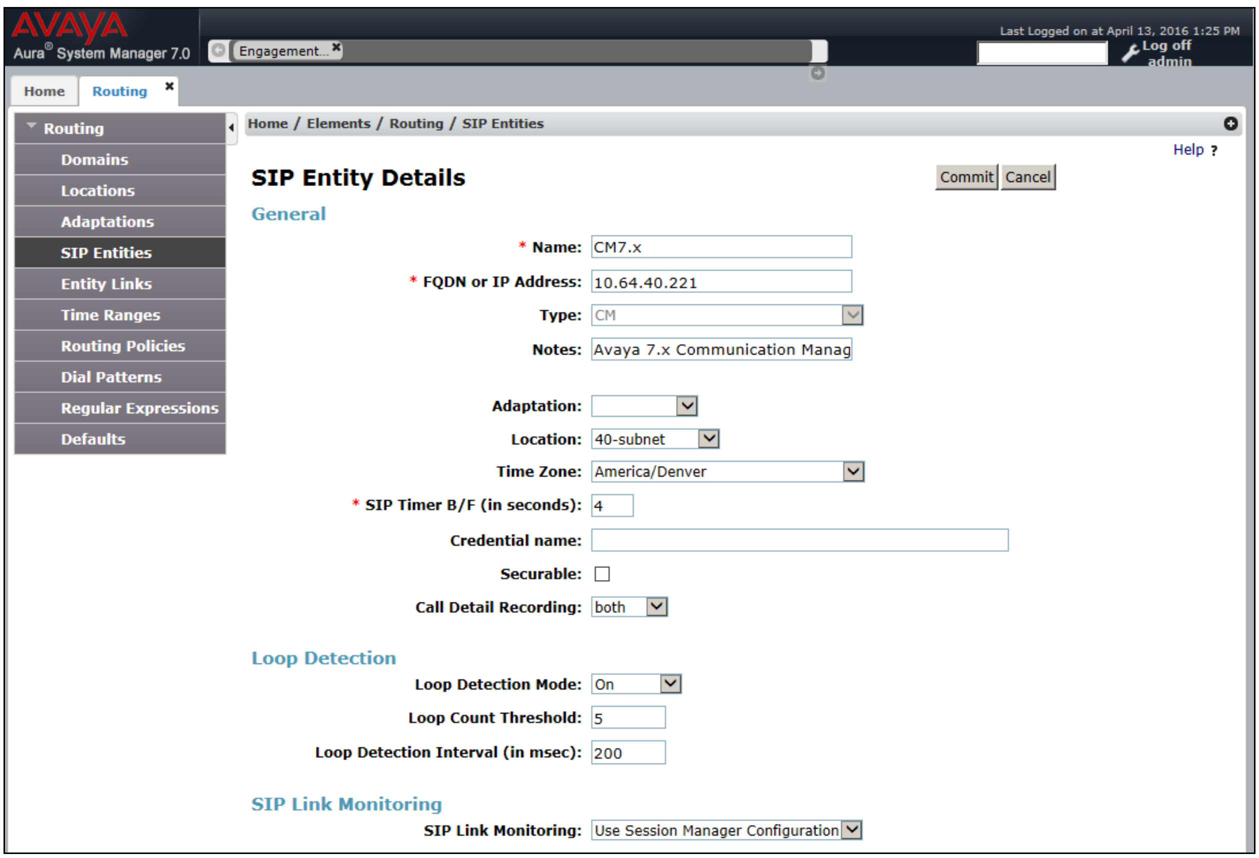


6.3.2. Communication Manager SIP Entity

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

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

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



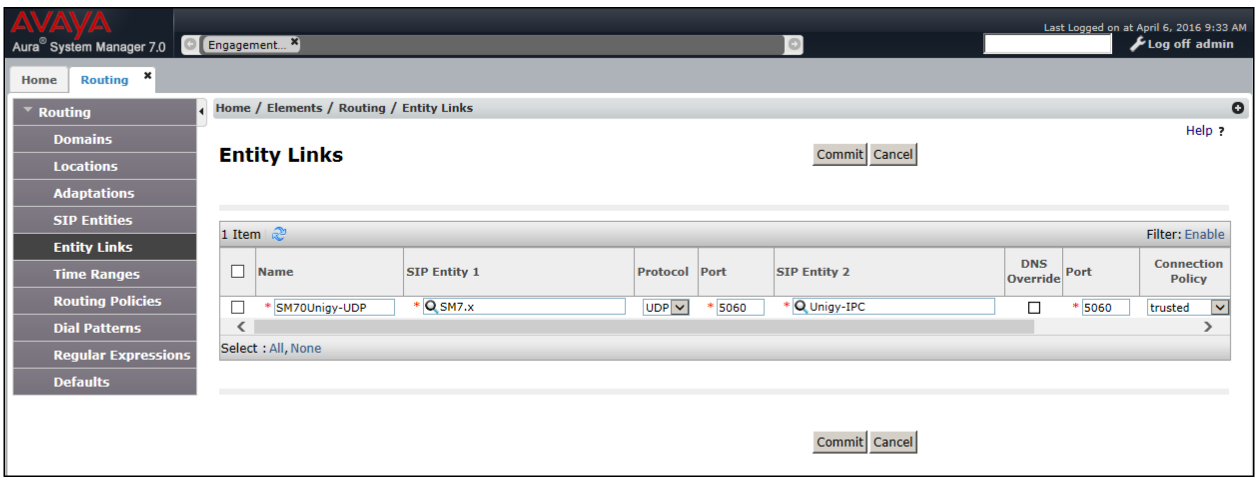
6.4. Administer Entity Links

Add three new entity links, two for IPC, and another for Communication Manager.

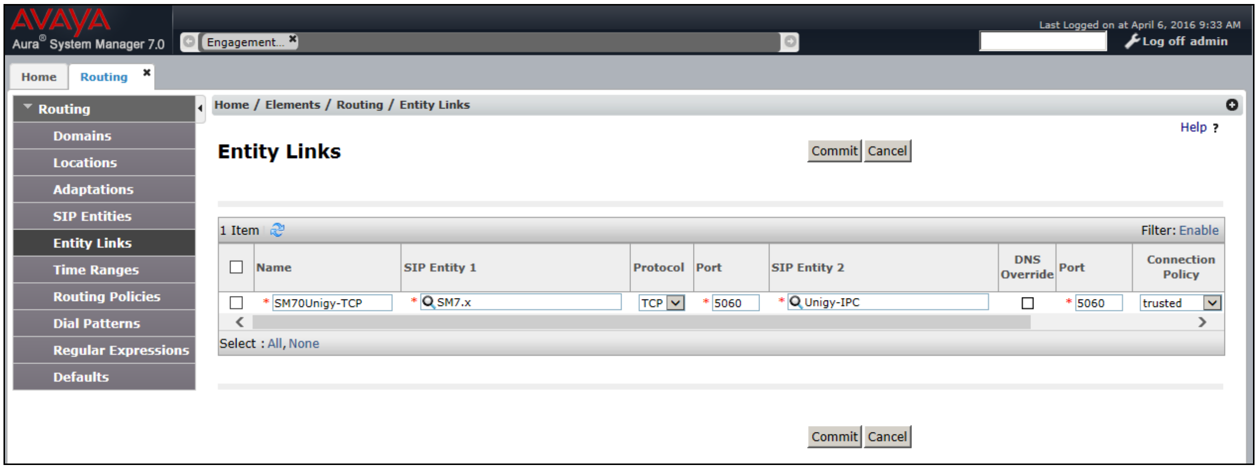
6.4.1. IPC Entity Links

Select **Routing → Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for IPC. The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name
- **Protocol:** "UDP"
- **Port:** "5060"
- **SIP Entity 2:** The IPC entity name from **Section 6.3.1**.
- **Port:** "5060"
- **Connection Policy:** "Trusted"



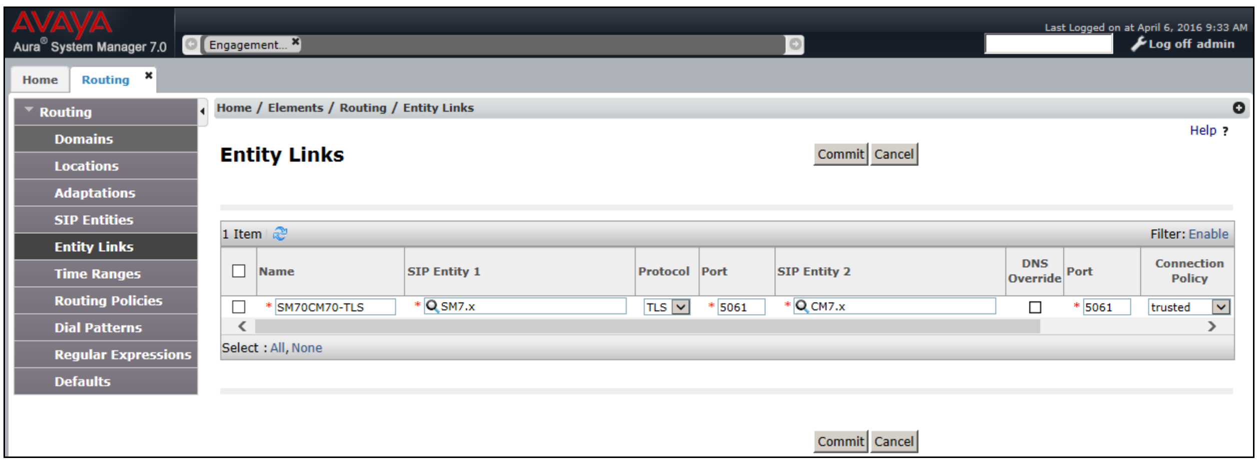
Repeat and add another entity link for IPC with “TCP” as Protocol, as shown below.



6.4.2. Communication Manager Entity Links

Select **Routing → Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for Communication Manager. The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "SM7.x".
- **Protocol:** The protocol used between Communication Manager and Session Manager is "TLS".
- **Port:** Enter an appropriate port used, in this case "5061".
- **SIP Entity 2:** The Communication Manager entity name from **Section 6.3.2**.
- **Port:** Enter an appropriate port used, in this case "5061".
- **Connection Policy:** **Trusted**



6.5. Administer Routing Policies

Add two new routing policies, one for IPC, and another for Communication Manager.

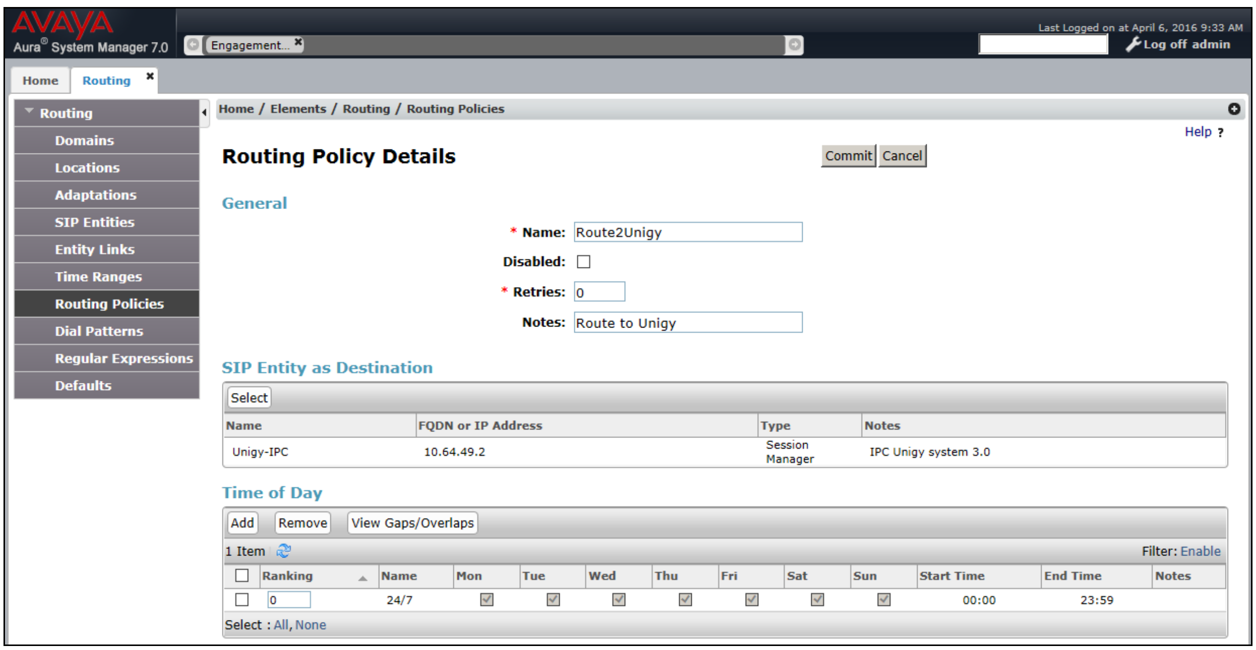
6.5.1. IPC Routing Policy

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

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the IPC entity name from **Section 6.3.1** in the listing (not shown).

Retain the default values in the remaining fields.



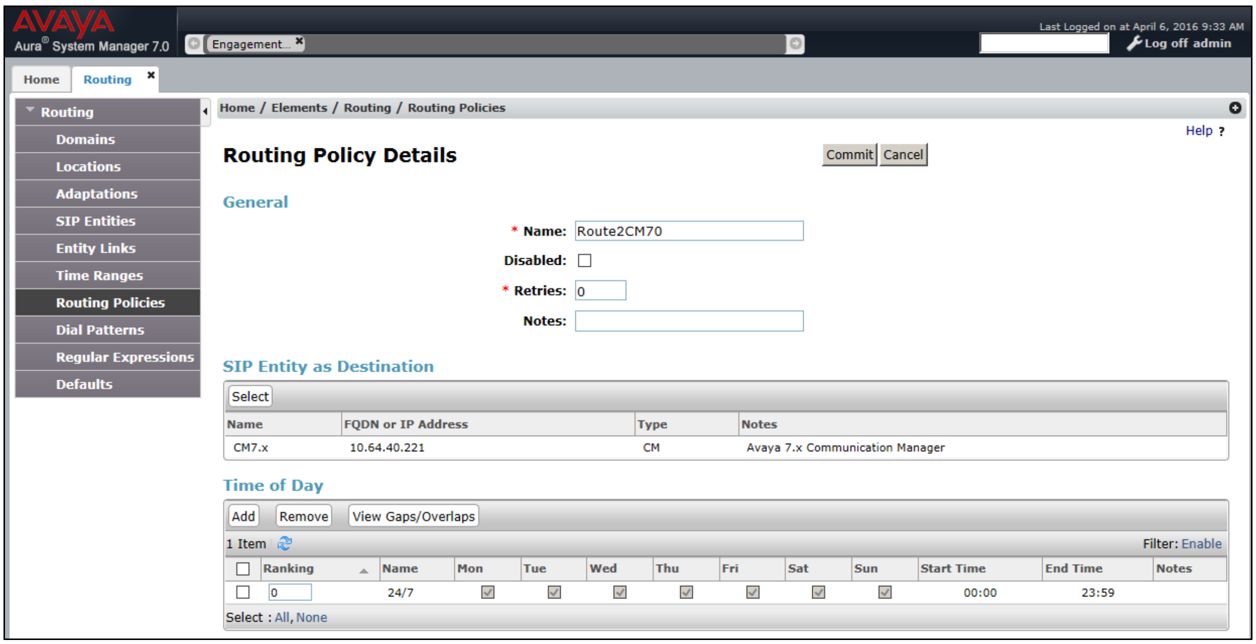
6.5.2. Communication Manager Routing Policy

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

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.3.2** in the listing (not shown).

Retain the default values in the remaining fields.



6.6. Administer Dial Patterns

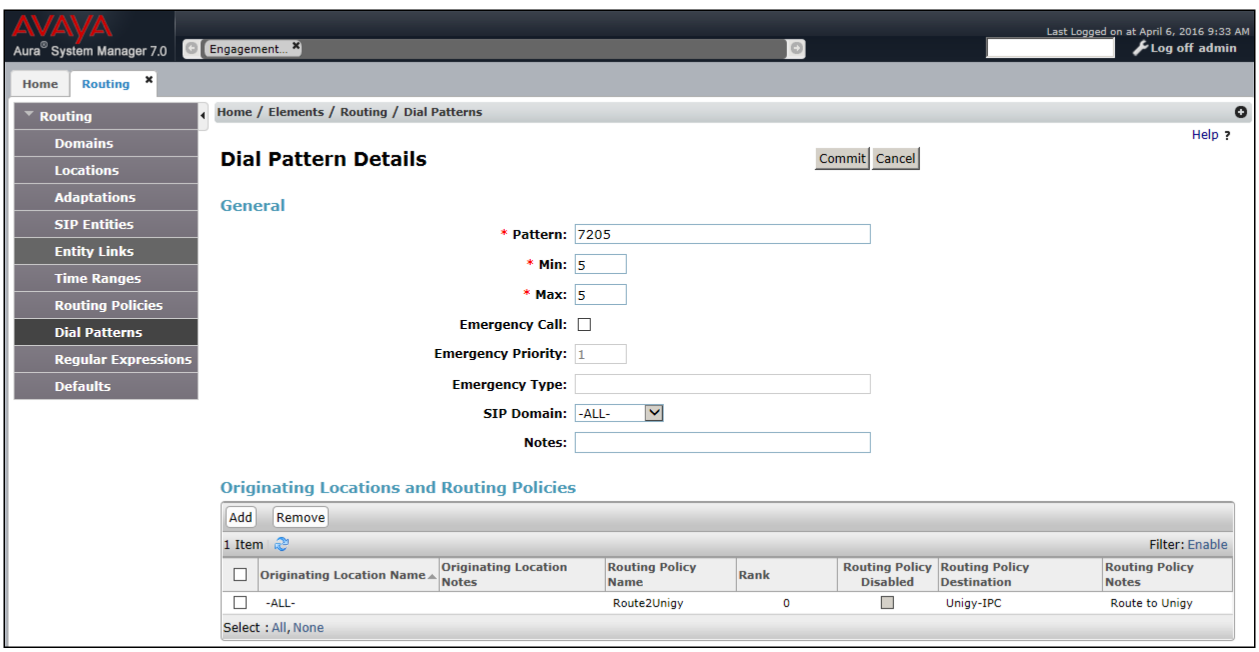
Add a new dial pattern for IPC, and update the existing dial pattern for Communication Manager.

6.6.1. IPC Dial Pattern

Select **Routing → Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach IPC turret users. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** Select "ALL".
- **Notes:** Any desired description.

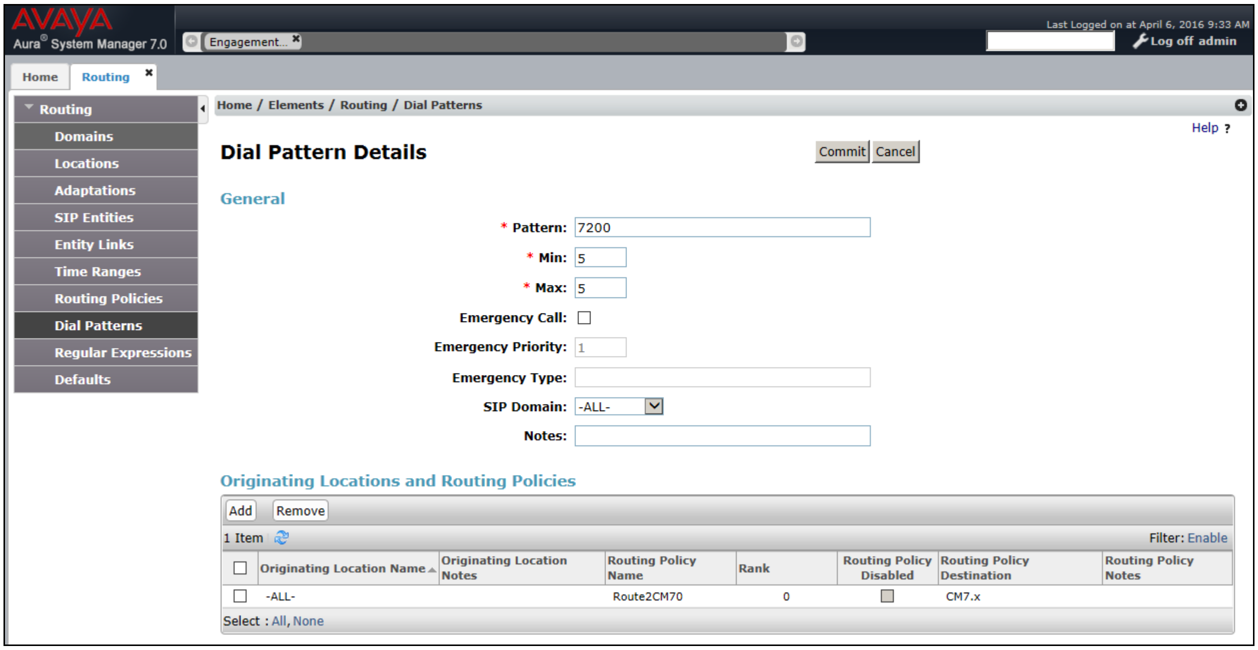
In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IPC turret users. In the compliance testing, the policy allowed for call origination from all locations, and the IPC routing policy from **Section 6.5.1** was selected as shown below.



6.6.2. Communication Manager Dial Pattern

Select **Routing → Dial Patterns** from the left pane, and click on the existing dial pattern for Communication Manager in the subsequent screen, in this case dial pattern "7200" (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy as necessary for calls from IPC turret users. In the compliance testing, the policy allowed for call origination from all locations, and the Communication Manager routing policy from **Section 6.5.2** was selected as shown below. Retain the default values in the remaining fields.



7. Configure IPC Converged Communication Manager

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

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

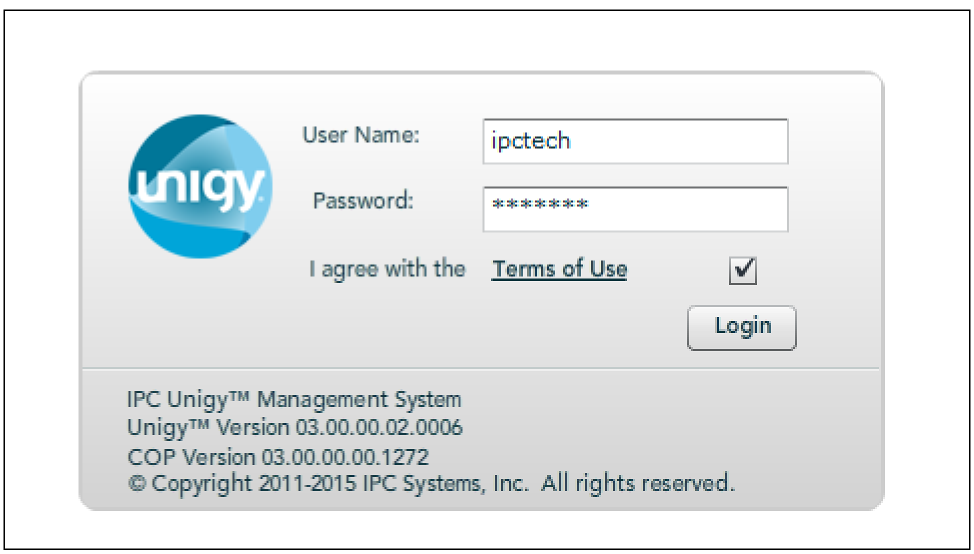
The installation/configuration of Media Manager and/or Converged Communication Manager is typically performed by IPC installation engineers. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy Management System

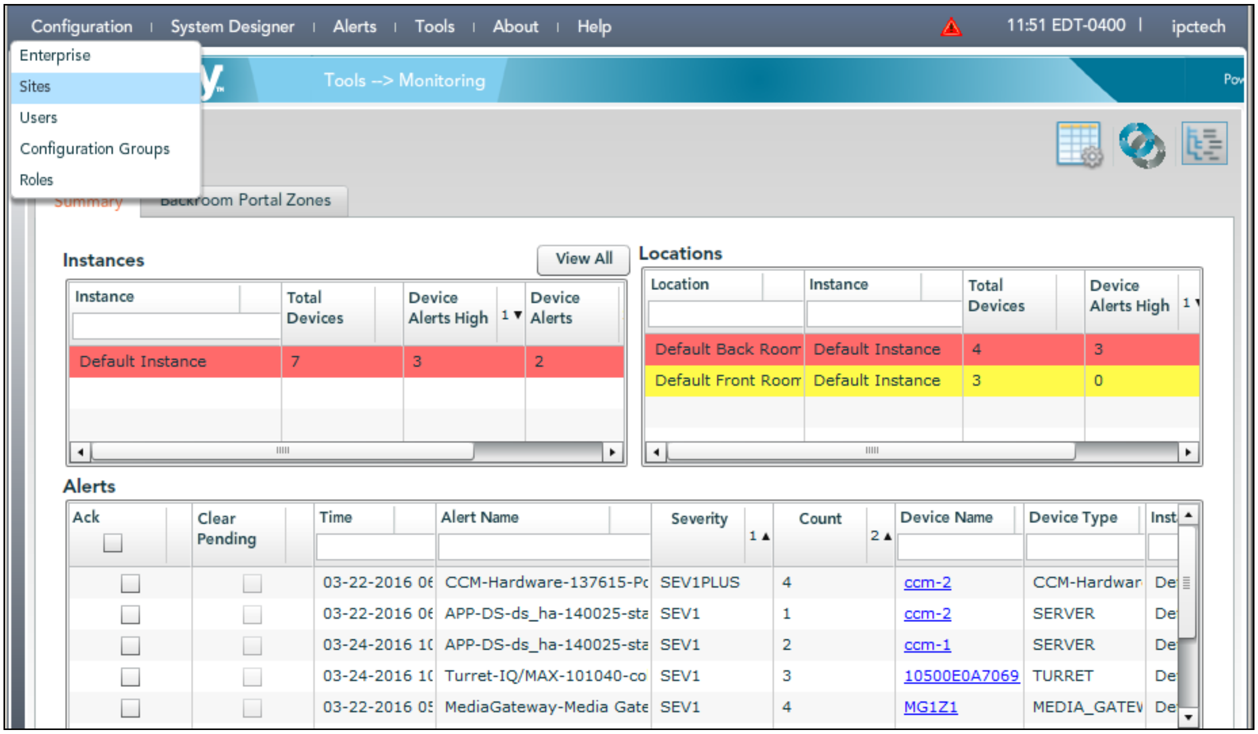
Access the UnigyV3P2 Management System web interface by using the URL http://ip-address in an Internet browser window, where "ip-address" is the IP address of the Media Manager. Log in using the appropriate credentials.

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**.

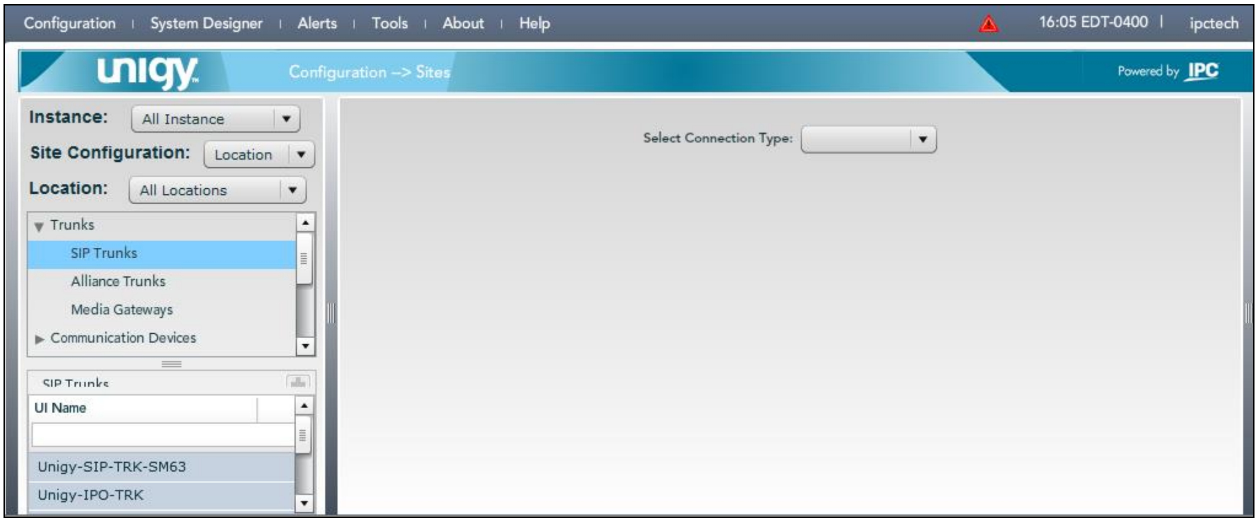


The following screen (Tools -> Monitoring) displays. Navigate to **Configuration → Site** under the main menu.



7.2. Administer SIP Trunks

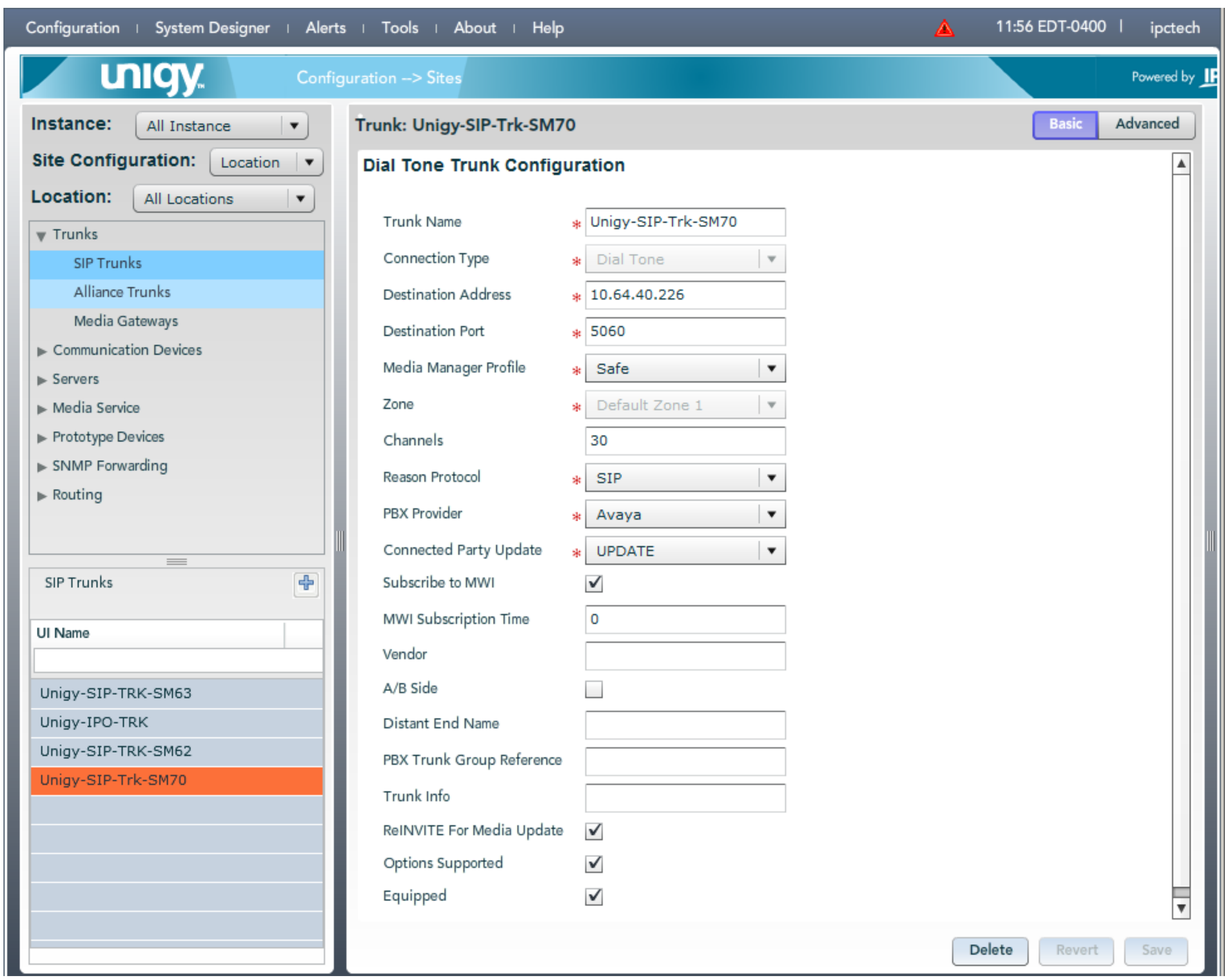
Select **Trunks → SIP Trunks** in the left pane, and click the **Add** icon ( ) in the lower left pane to add a new SIP trunk. Select "Dial Tone" from the **Select Connection Type** drop-down list.



The screen below is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

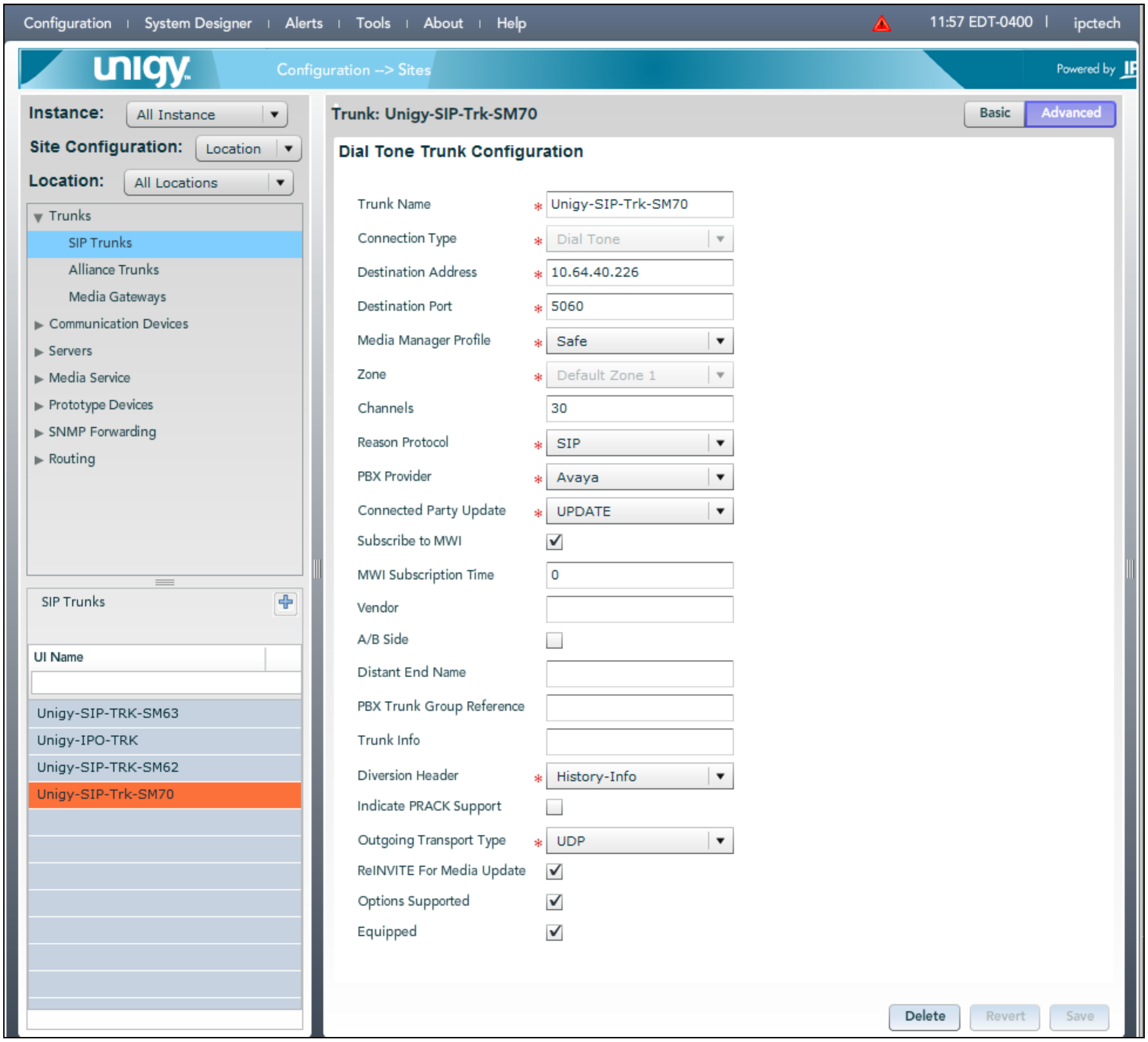
- **Trunk Name:** A descriptive name.
- **Destination Address:** IP address of the Session Manager signaling interface.
- **Destination Port:** The port number from **Section 6.4.1**.
- **Zone:** An available zone, in this case "Default Zone 1".
- **Channels:** The number of SIP trunk group members.
- **Reason Protocol** "SIP"
- **PBX Provider:** "Avaya"
- **Connected Party Update:** "UPDATE"

Retain the default values in the remaining fields.



Select the Advance tab in the upper right. .Enter the following values for the specified fields, and retain the default values for the remaining fields.

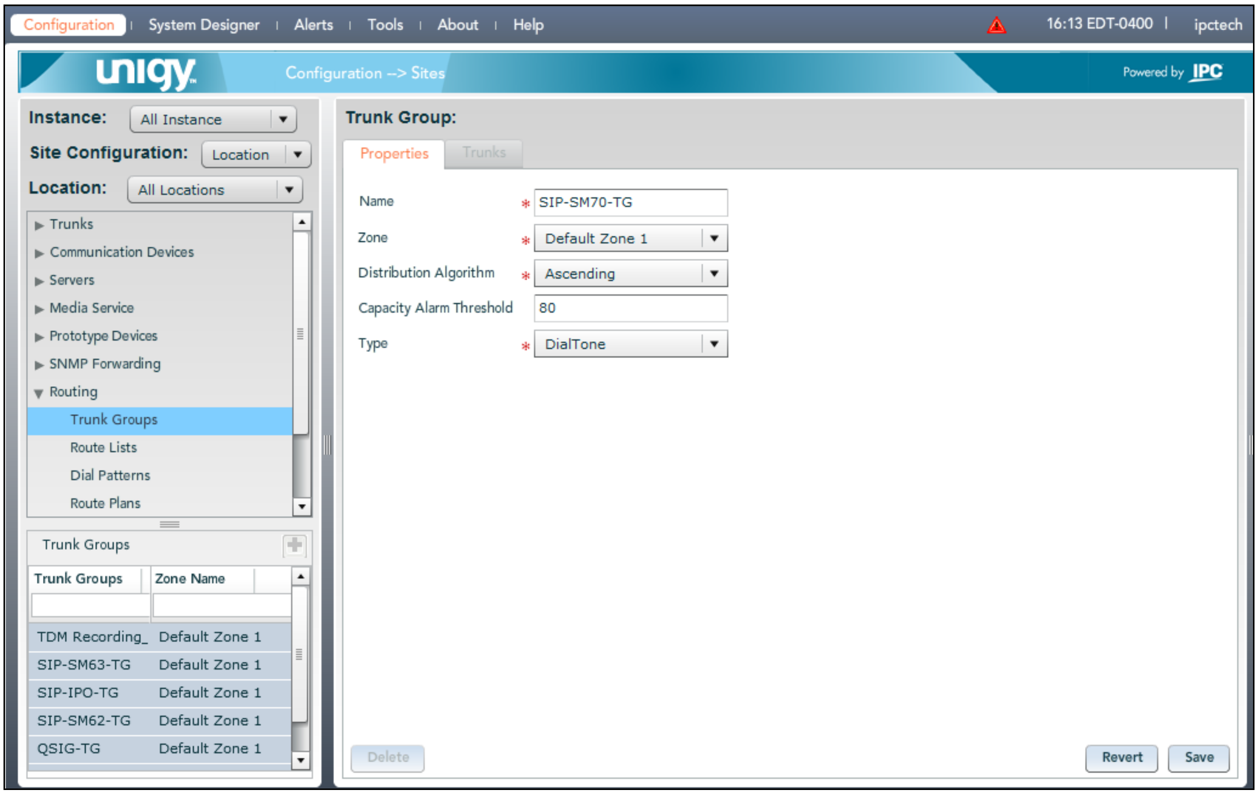
- **Diversion Header:** "History-Info.
- **Outgoing Transport Type:** "UDP".



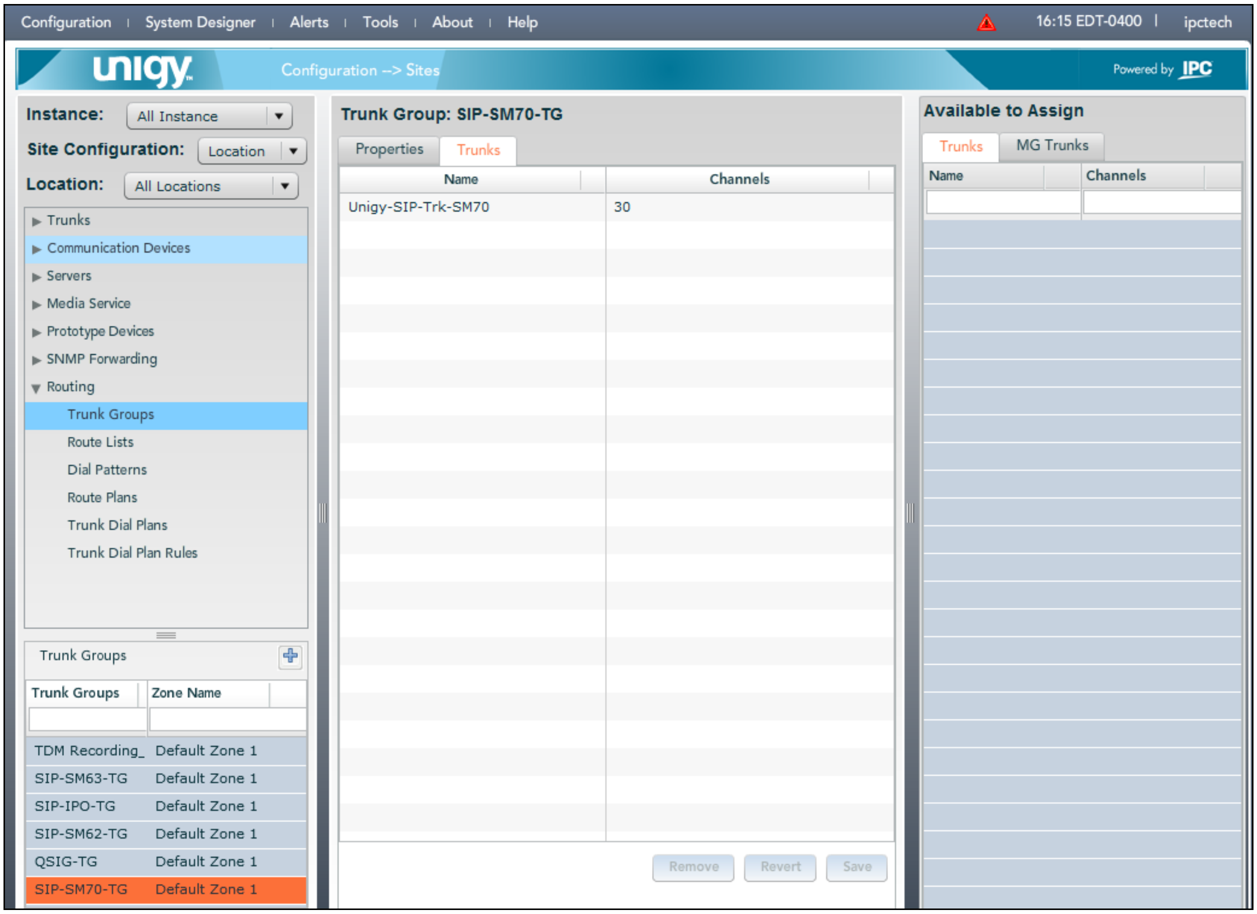
7.3. Administer Trunk Groups

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

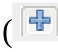
The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, select "Default Zone 1" for the **Zone** field, select "Ascending" for the **Distribution Algorithm** field, and click **Save**. Select the **Trunks** tab in the right pane.



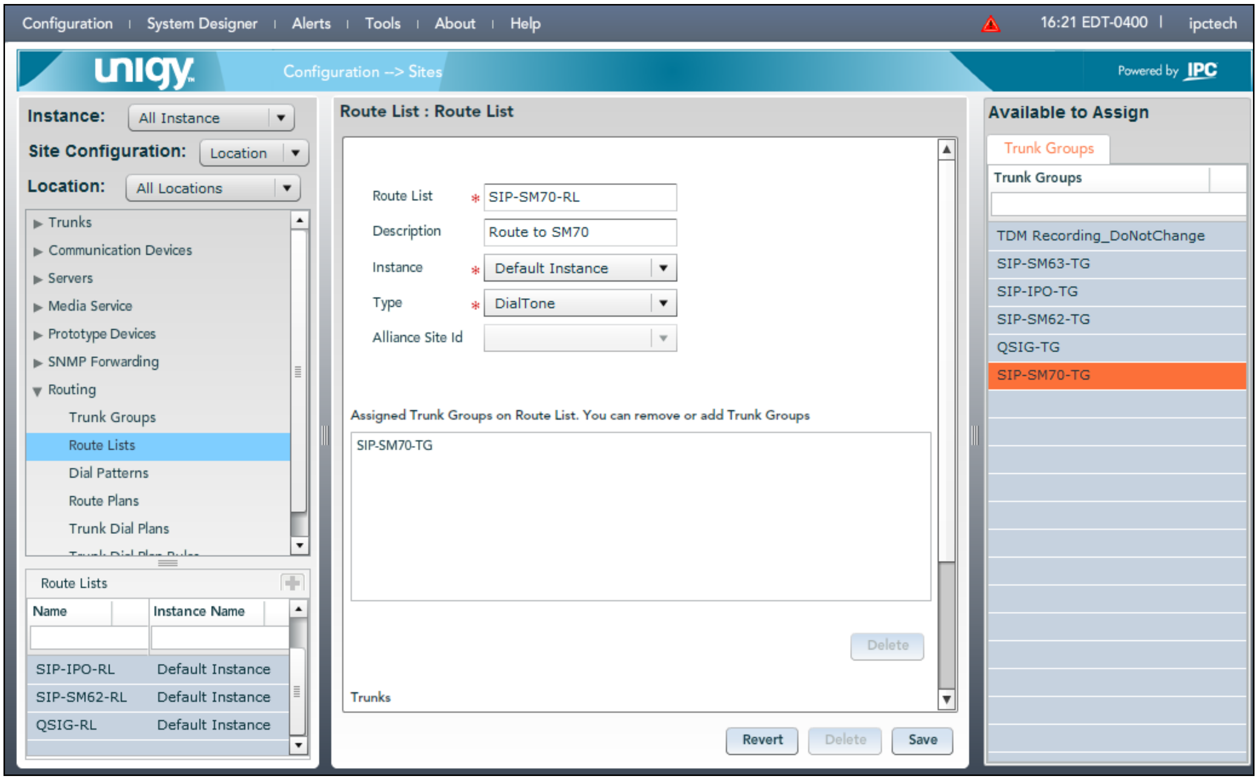
The screen is updated with three panes. In the rightmost pane, select the Trunks tab to display a list of trunks. Select the SIP trunk from **Section 7.2** in the rightmost pane and drag to the middle pane as shown below. Click **Save**.



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.

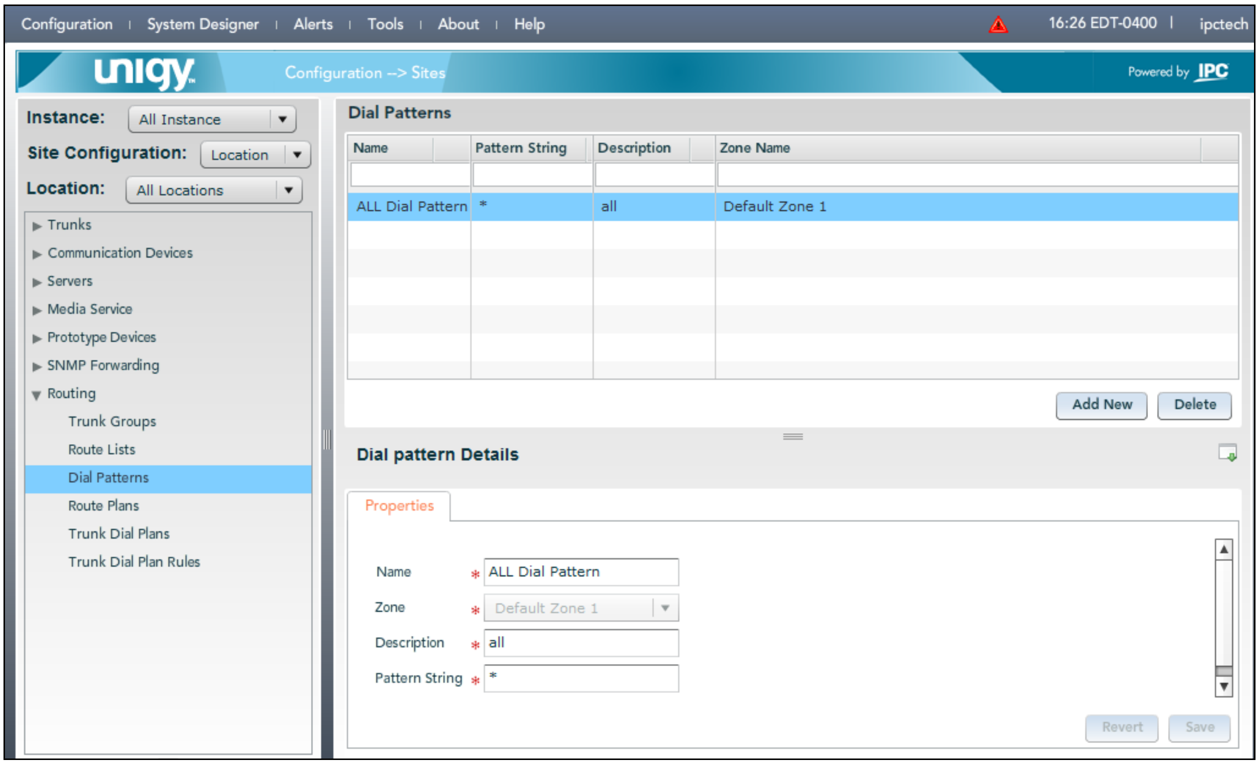
The **Route List** screen is displayed in the middle pane. For **Route List**, enter a descriptive name. In the right pane, select the trunk group from **Section 7.3** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below. Click **Save**.



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.

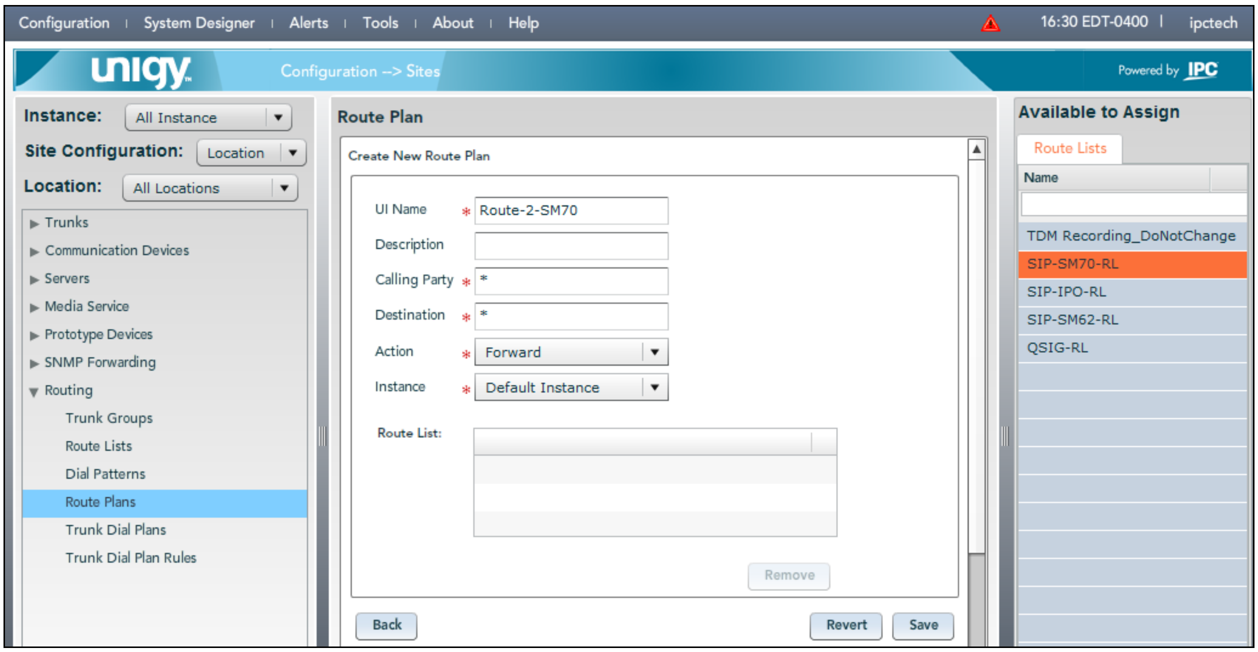
In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya endpoints, in this case "*" meaning any digits will be sent to Session Manager. Click **Save**. Once the **Save** button is clicked, the newly created Dial pattern should be displayed under the **Dial Patterns** section.



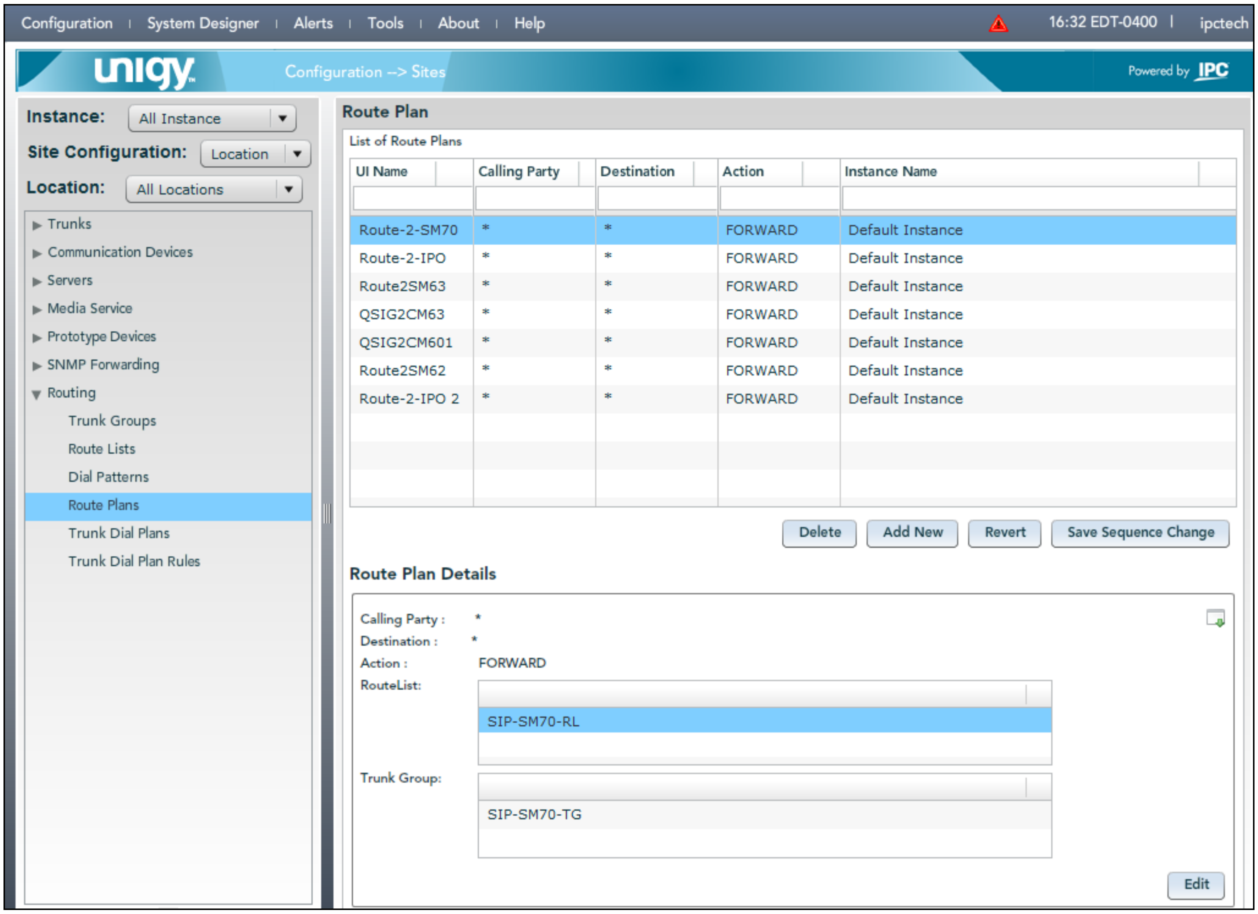
7.6. Administer Route Plans

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

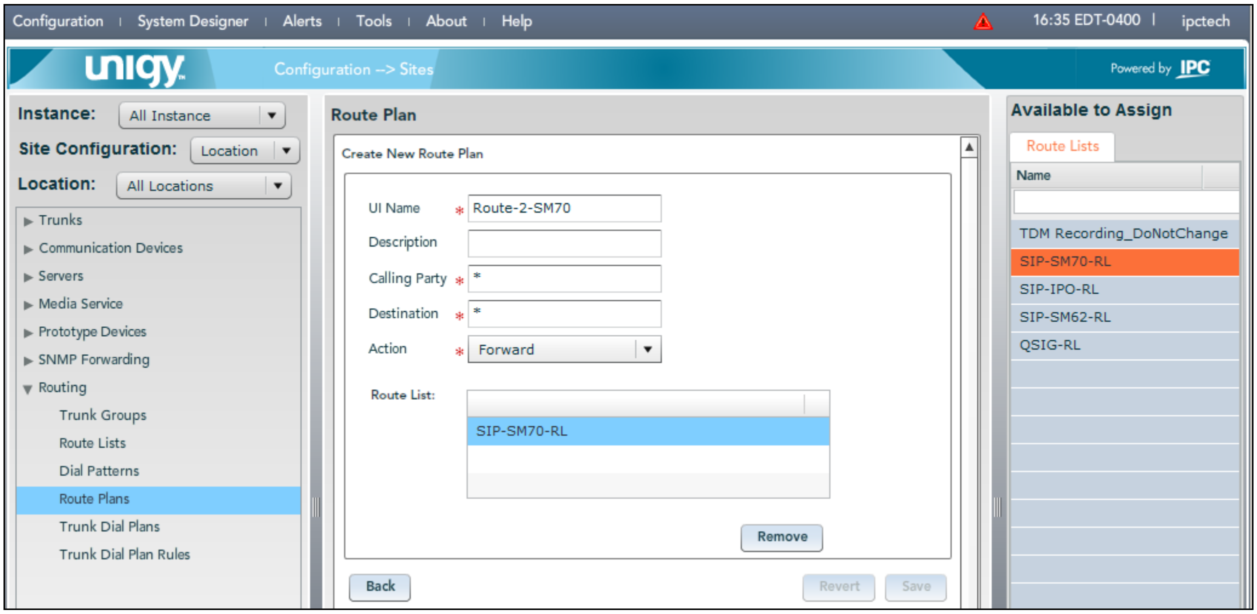
The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter "*" to denote any calling party from UnigyV3P2. For **Destination** select the dial pattern for Avaya endpoints from **Section 7.5**. Select "Forward" for **Action**, and click **Save**.



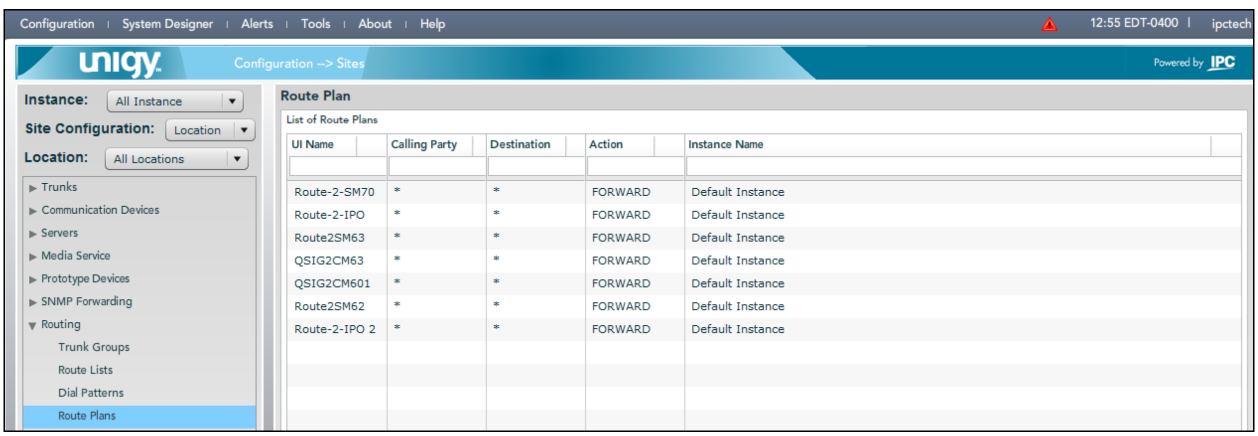
The screen is updated with the newly created route plan. Select the route plan, and click **Edit** toward the bottom of the screen.



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



In the Route Plan page, verify the route plan that utilizes during the compliance test is at the top of the route plan list.



8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and IPC UnigyV3P2.

8.1. Verify Avaya Aura® Communication Manager

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

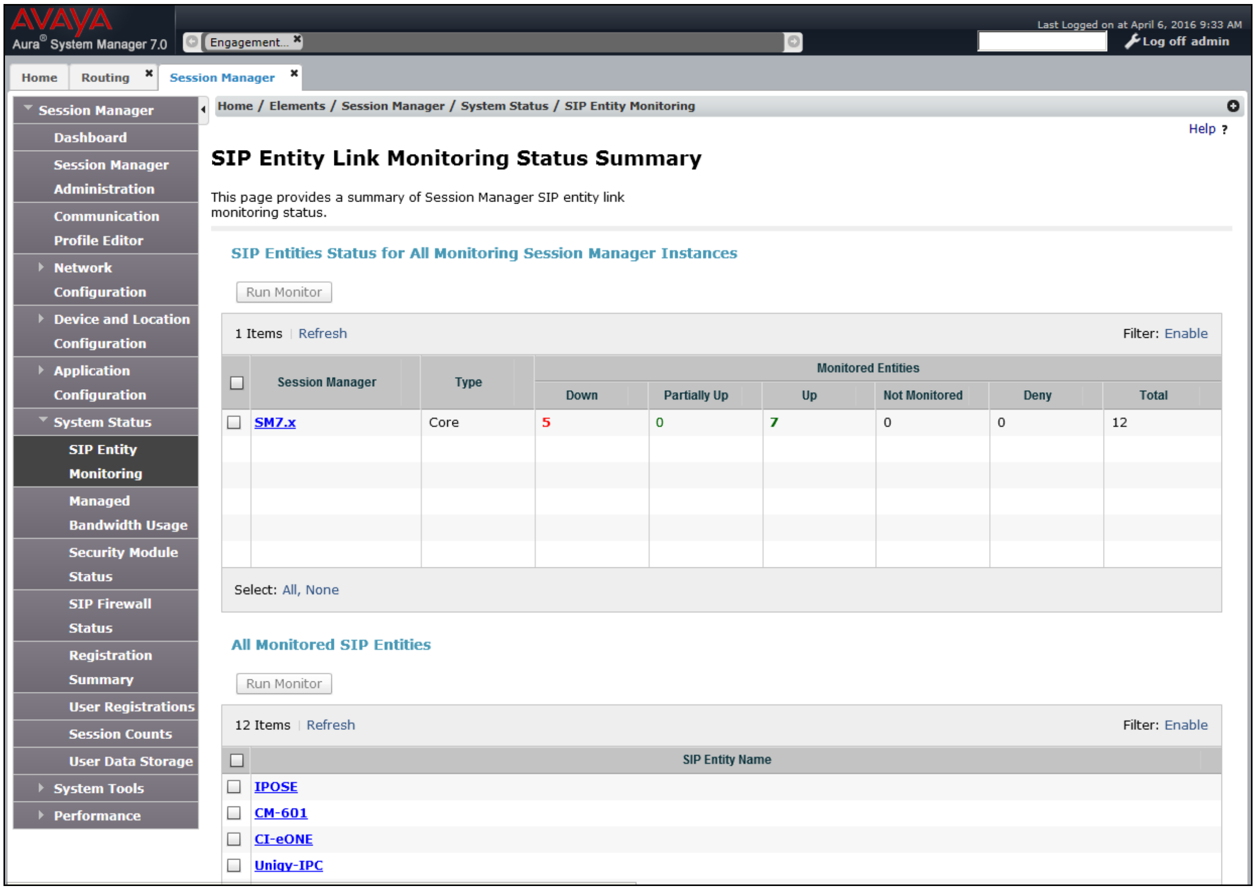
```
status trunk 92

                            TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0092/001 T00135   in-service/idle    no
0092/002 T00136   in-service/idle    no
0092/003 T00137   in-service/idle    no
0092/004 T00138   in-service/idle    no
0092/005 T00139   in-service/idle    no
0092/006 T00140   in-service/idle    no
0092/007 T00141   in-service/idle    no
0092/008 T00142   in-service/idle    no
0092/009 T00143   in-service/idle    no
0092/010 T00144   in-service/idle    no
```

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.4**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

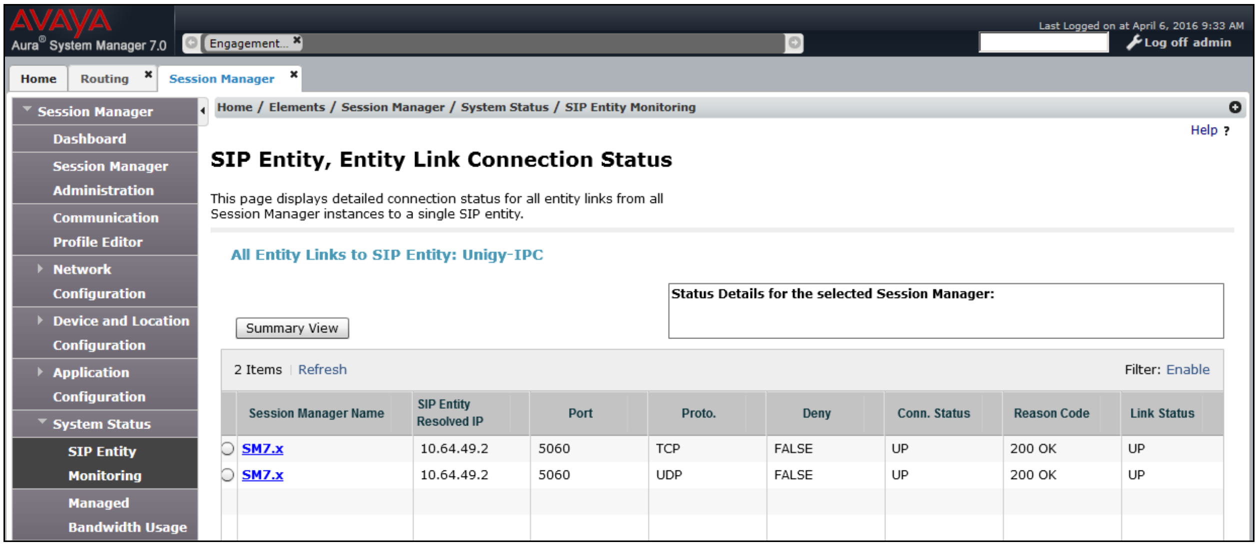
```
status signaling-group 92
                        STATUS SIGNALING GROUP

        Group ID: 92
      Group Type: sip

     Group State: in-service
```

8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements → Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the IPC entity name from **Section 6.3.1**.



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



8.3. Verify IPC UnigyV3P2

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

9. Conclusion

These Application Notes describe the configuration steps required for IPC UnigyV3P2 to successfully interoperate with Avaya Aura® Session Manager 7.0 and Avaya Aura® Communication Manager 7.0 via Avaya Aura® Session Manager. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Release 7.0, August 2015, available at http://support.avaya.com.

2. *Administering Avaya Aura® System Manage for Release 7.0,* , Issue 1, January 2016, available at http://support.avaya.com

3. *UnigyV3P2 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

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