Avaya Solution & Interoperability Test Lab

Application Notes for Interactive Intelligence Customer Interaction Center (CIC) with Avaya Aura® Telephony Infrastructure – Issue 1.0

Abstract

These Application Notes describe the steps for configuring a SIP entity link between Interactive Intelligence CIC server and Avaya Aura® Telephony Infrastructure. The integration can then be leveraged for delivery of calls from one solution to the other, using Avaya endpoints as remote dial voice paths for CIC applications. This is typically provisioned for agents using Avaya hardware to receive CIC routed ACD calls and applications.

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

1. Introduction

These Application Notes describe the steps for configuring a SIP entity link between Interactive Intelligence CIC server and Avaya Aura® Telephony Infrastructure including Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya G450 Media Gateway. Various Avaya and CIC endpoints were used to validate the solution. The integration between systems was leveraged for delivery of calls from one solution to the other, using Avaya endpoints as remote dial voice paths for CIC applications. This is typically provisioned so agents using Avaya hardware can receive CIC routed ACD calls and applications.

2. General Test Approach and Test Results

The general test approach was to verify interoperability of Interactive Intelligence CIC with an Avaya Aura® Telephony Infrastructure. All test cases were executed manually.

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 testing included the following:

All test cases were performed manually.

- Calls delivered via CIC Server to Avaya Aura® Telephony Infrastructure
- Calls sent via Avaya Aura® Telephony Infrastructure to CIC Server
- Calling with Avaya H.323 and SIP telephones
- DTMF Tone Support per RFC 2833
- G.711MU, G.711A and G.729A support and Codec negotiation
- Dial plan processing to deliver calls appropriately between CIC Call Center and Avaya Aura® Telephony Infrastructure
- Telephony supplementary features, such as Hold, Call transfer, Conference Calling and Call Forwarding, powered by CIC Interaction Client
- Always-In Media audio between Avaya phones and Interaction Media Server
- Serviceability Testing
    - Restart CIC Server process
    - Basic Network Failure and Recovery

Compliance testing focused on proper call handling and verification of functionality between the two systems. Specifically, compliance testing verified that when the calls were placed from either system or calls arrived at either system the expected behavior results were met.

2.2. Test Results

The Interactive Intelligence CIC successfully achieved the above objectives. All test cases passed.

The following observation was made during testing:

"Always-In" audio on the Interactive Intelligence CIC server was required for proper audio for conference and transfer. This parameter forces the Interactive Media Server to be used in the audio-path. Without this parameter enabled a one-way audio talk-path was observed. The configuration can be found in **Section 7.1.2**.

2.3. Support

For technical support on Interactive Intelligence products, contact Interactive Intelligence at 1-800-267-1367, or refer to http://www.inin.com/Support

3. Reference Configuration

Figure 1 illustrates the setup used for compliance testing. The configuration enabled Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Interactive Intelligence Customer Interaction Center (CIC), and Interactive Intelligence Media Server to interoperate via SIP. The solution allowed calls between Interactive Intelligence CIC and Avaya Aura® Session Manager via a SIP entity link. Call types that were carried across the SIP entity link, included, intercom calls, delivery of calls into the CIC powered call center, and delivery of call center calls to the agent using the Avaya telephone as the voice path.

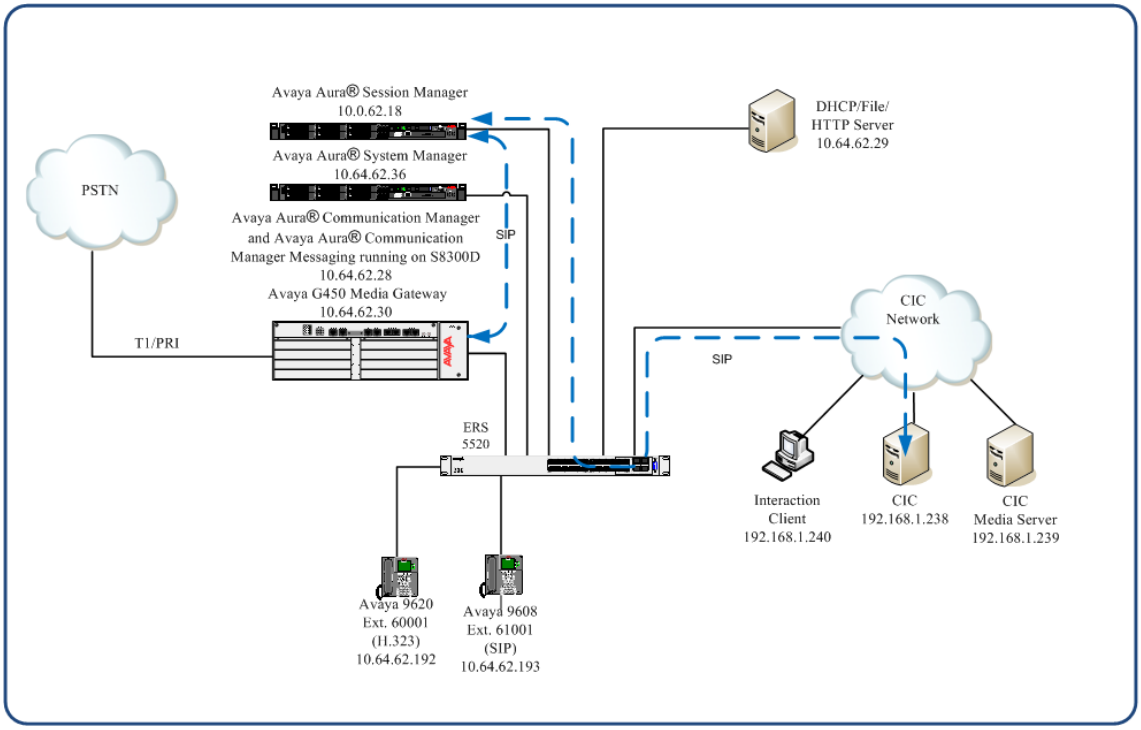


Figure 1: Interactive Intelligence CIC

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300D Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.2 Service Pack 5
Avaya G450 Media Gateway	HW 2 FW 31.20.0
Avaya Aura® Session Manager	
Avaya Aura® Session Manager HP Proliant DL360 G7	6.3.0 Service Pack 1
Avaya Aura® System Manager HP Proliant DL360 G7	6.3.0 Service Pack 1
Avaya Endpoints	
Avaya 96xx Series IP Telephones	H.323 3.1SP2 SIP 2.6.6.0
Avaya 96x1 Series IP Telephones	H.323 6.2 SIP 6.2
Interactive Intelligence Products	
CIC	3.0 SU16
CIC Media Server	4.0 SU2
Interaction Client	3.0 SU16

5. Configure Avaya Aura® Communication Manager

This section describes the steps required for Communication Manager to support the configuration in **Figure 1**. The following pages provide step-by-step instructions on how to administer parameters specific to the Interactive Intelligence CIC solution only. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available and that the reader has a basic understanding of the administration of Communication Manager and Session Manager. It is assumed that all other connections, e.g., to PSTN, to LAN, are configured and will not be covered in this document. The reader will need access to the System Administration Terminal screen (SAT). For detailed information on the installation, maintenance, and configuration of Communication Manager, please refer to **[1]**.

5.1. Configure Node-Names IP

In the **IP Node Names** form, assign the name and IP address of Session Manager. This is used to terminate the SIP Entity Link with Session Manager. The names will be used in the signaling group configuration configured later.

Enter the **change node-names ip** command. Specify node names and signaling IP address for Session Manager.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
default                0.0.0.0
procr                  10.0.62.28
procr6                 ::
sm                     10.0.62.18









( 8  of 8    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.2. IP Codec Set and IP Network Region

Enter the **change ip-codec-set g** command, where "g" is a number between 1 and 7, inclusive, and enter legal values for each **"Audio Codec"**. Compliance testing used G.711MU, G.711A, and G.729A. This IP codec set will be selected later in the IP Network Region form to define which codecs may be used within an IP network region.

```
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: G.711A            n         2        20
 3: G.729A            n         2        20
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for desk phone calls. This IP codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling groups.

Enter the **change ip-network-region h** command, where "h" is a number between 1 and 250, inclusive. On page 1 of the **ip-network-region** form, set **Codec Set** to the number of the IP codec set configured on the previous step. Accept the default values for the other fields.

```
change ip-network-region 1                                     Page   1 of  20
                            IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: SM_Public
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
```

5.3. Configure Signaling and Trunk Groups

Add a signaling group for calls that need to be routed to Interactive Intelligence CIC via Session Manager. Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as shown below:

- Set the **Group Type** field to **sip**.
- Specify the Communication Manager (**procr**) and the Session Manager as the two end-points of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were configured in the **IP Node Names** form shown in **Section 5.1**.
- Compliance testing used TCP and port value of **5060** in the **Near-end Listen Port** and the **Far-end Listen Port** fields. If the **Far-end Network Region** field is configured, the codec for the call will be selected from the IP codec set assigned to that network region.
- Enter the domain name in the **Far-end Domain** field. In this configuration, the domain name is **avaya.com**.
- The **DTMF over IP** field is set to the default value of **rtp-payload**. Avaya Communication Manager supports DTMF transmission using RFC 2833.
- The default values for the other fields may be used.

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

 Group Number: 100             Group Type: sip
  IMS Enabled? n         Transport Method: tcp
       Q-SIP? n
    IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                 Far-end Node Name: sm
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
                                  Far-end Secondary Node Name:
Far-end Domain: avaya.com
                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate              RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                 IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

Use the **add trunk-group** command to configure the Trunk Group form shown below for outgoing calls to be routed to Interactive Intelligence via Session Manager.

- Set the **Group Type** field to **sip**.
- Enter a meaningful name/description for **Group Name.**
- Enter a **Trunk Access Code (TAC)** that is valid under the provisioned dial plan
- Set the **Service Type** field to **tie**.
- Specify the **Signaling Group** associated with this trunk group.
- Specify the **Number of Members** supported by this SIP trunk group
- The default values for the other fields may be used.

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: To Session Manager          COR: 1        TN: 1        TAC: *001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                                Member Assignment Method: auto
                                                          Signaling Group: 1
                                                        Number of Members: 10
```

5.4. Dial Plan and Access Codes

The dial plan defines what digit strings are defined as extensions and access codes. Feature access codes (fac) can be used to invoke specific PBX features.

Use the **display dialplan analysis** command to display the dial plan. Verify the dial strings that represent extensions and which are configured as a fac or dac. This information will be used in subsequent steps and sections. Extensions beginning with 54 were used for the Avaya endpoints and Dialed Strings beginning with 6 were used to reach Interactive Intelligence CIC.

```
display dialplan analysis                                    Page   1 of  12
                           DIAL PLAN ANALYSIS TABLE
                                 Location: all            Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   2           5   ext
   4           5   ext
   54          5   ext
   55          5   ext
   6           5   aar
   7           5   aar
   8           1   fac
   9           1   fac
   *           4   dac
```

Use the **change feature-access-codes** command to assign feature access codes for **AAR** and **ARS** (if not already assigned) that is consistent with the existing dial plan. .

```
change feature-access-codes                                   Page   1 of  10
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

5.5. Configure Route Pattern

A route pattern is configured to use the trunk defined in **Section 5.3**. The route pattern can also be configured to perform digit manipulation on outgoing calls if necessary. Calls destined for Interactive Intelligence CIC will be routed via the Session Manager using the route pattern defined below.

When configuring a route pattern, use the **change route-pattern x** command, where **x** is an available route pattern number. For the compliance test, route pattern 1 was selected. Set the parameters as shown below.

- For the **Pattern Name**, enter a descriptive name.
- Set the **Grp No** to the trunk group number created in **Section 5.3**.
- Set the **FRL** (Facility Restriction Level) to a value that allows all users access to the trunk that need to use it. The value of **0** is the least restrictive. This is the value used for the compliance test.
- Set **Numbering Format** to **lev0-pvt**.
- Default values may be used for all other fields.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: SM_62_18
                              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: 1    0                                                           n   user
 2:                                                                  n   user
 3:                                                                  n   user
 4:                                                                  n   user
 5:                                                                  n   user
 6:                                                                  n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n           rest                                lev0-pvt  none
 2: y y y y y n  n           rest                                          none
 3: y y y y y n  n           rest                                          none
 4: y y y y y n  n           rest                                          none
 5: y y y y y n  n           rest                                          none
 6: y y y y y n  n           rest                                          none
```

5.6. Configure Automatic Alternate Routing

Automatic Alternate Routing (AAR) is used to route the calls to Interactive Intelligence CIC via the Session Manager.

When creating entries in the AAR Digit Analysis Table, use the **change aar analysis x** command, where **x** is the first digit in the dialed string to be entered. Create an entry to reach the CIC user extensions supported by the configuration in **Figure 1**. The extensions are reached using the aar table entry "**6**". When creating the entries, enter the parameters as defined below.

- For the **Dialed String**, enter the extensions reachable at Interactive Intelligence CIC.
- Set the **Total Min** and **Total Max** fields to the number length.
- Set the **Route Pattern** to the route pattern defined in **Section 5.5** that directs calls to the trunk connected to the Avaya Aura® Session Manager.
- Set the **Call Type** to **aar**.

```
change aar analysis 6                                        Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                 Location: all            Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    6                     5    5     1        aar           n
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Adaptations to support handling Caller-ID information.
- SIP Entities corresponding to Session Manager, Communication Manager, and Interactive Intelligence CIC
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed

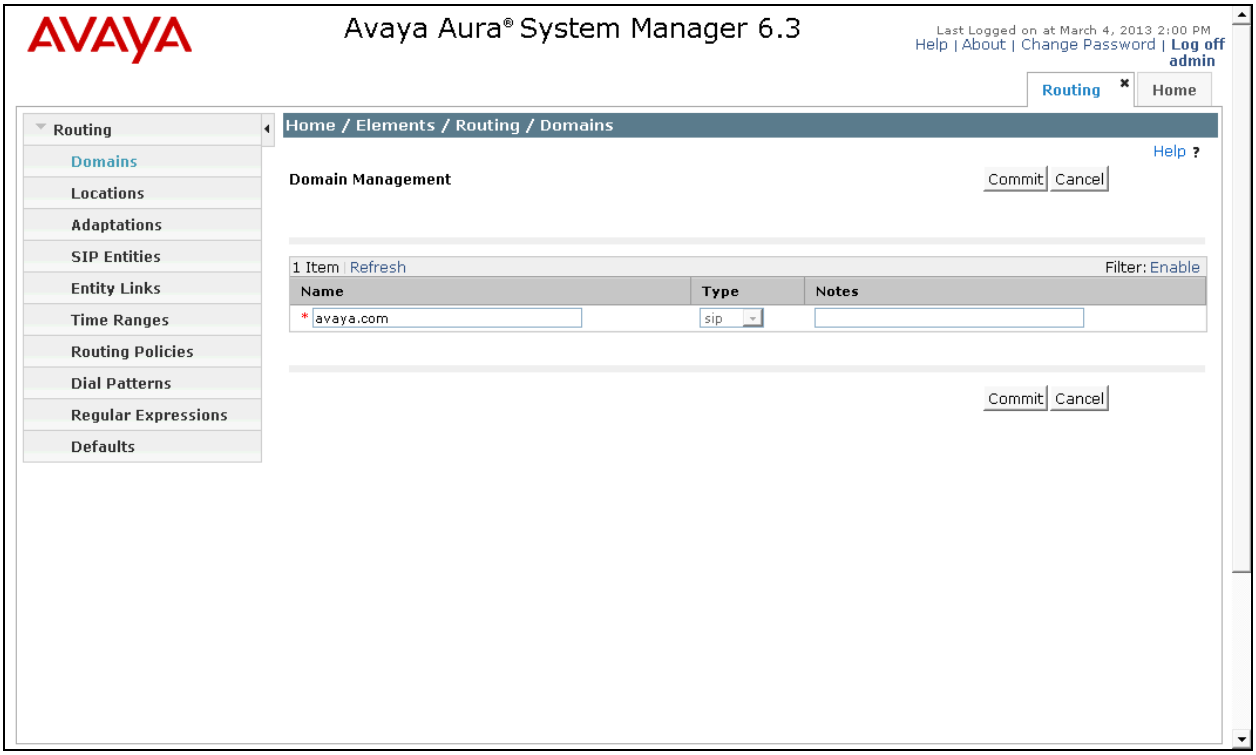
Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials.

6.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. From the System Manager Home screen, navigate to **Elements → Routing** (not shown). Select **Domains** on the left and click the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., **avaya.com**).
- **Type:** Select sip.
- **Notes:** Descriptive text (optional).

Click **Commit**.



6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

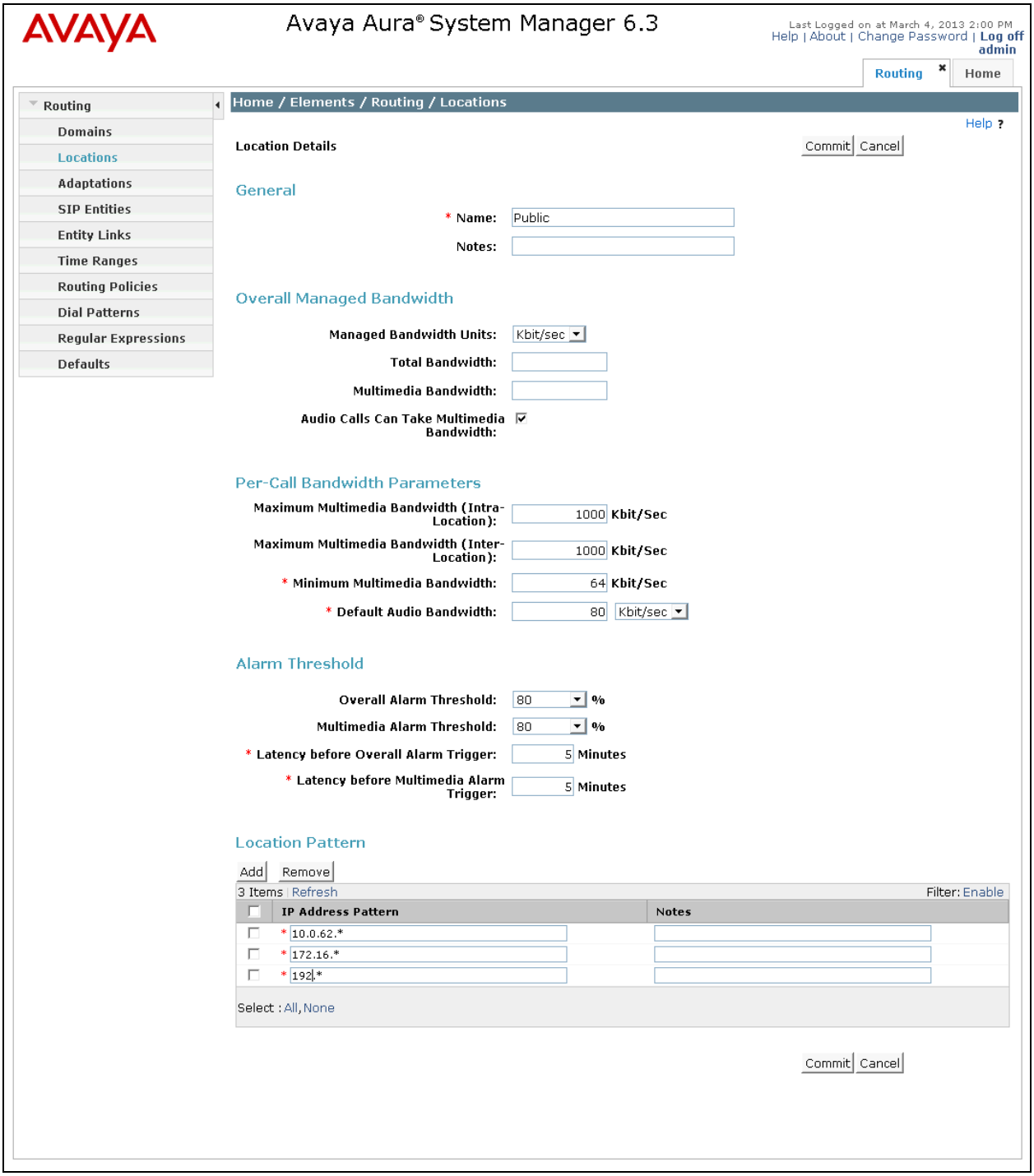
Under **General**:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows the addition of the Public location, where Communication Manager, Session Manager and CIC reside. Click **Commit** to save the Location definition.



6.3. Add Adaptations

Adaptations are used to modify SIP messages that are leaving Session Manager (egress adaptation) and that are entering Session Manager (ingress adaptation). One reason to use an adaptation is to convert strings containing calling and called party numbers from the local dial plan of a SIP entity to the dial plan administered on the Session Manager, and vice versa. Another reason would be to convert the domain in a SIP INVITE URI to an IP address. The **DigitConversionAdapter** installed on Session Manager is used for this purpose.

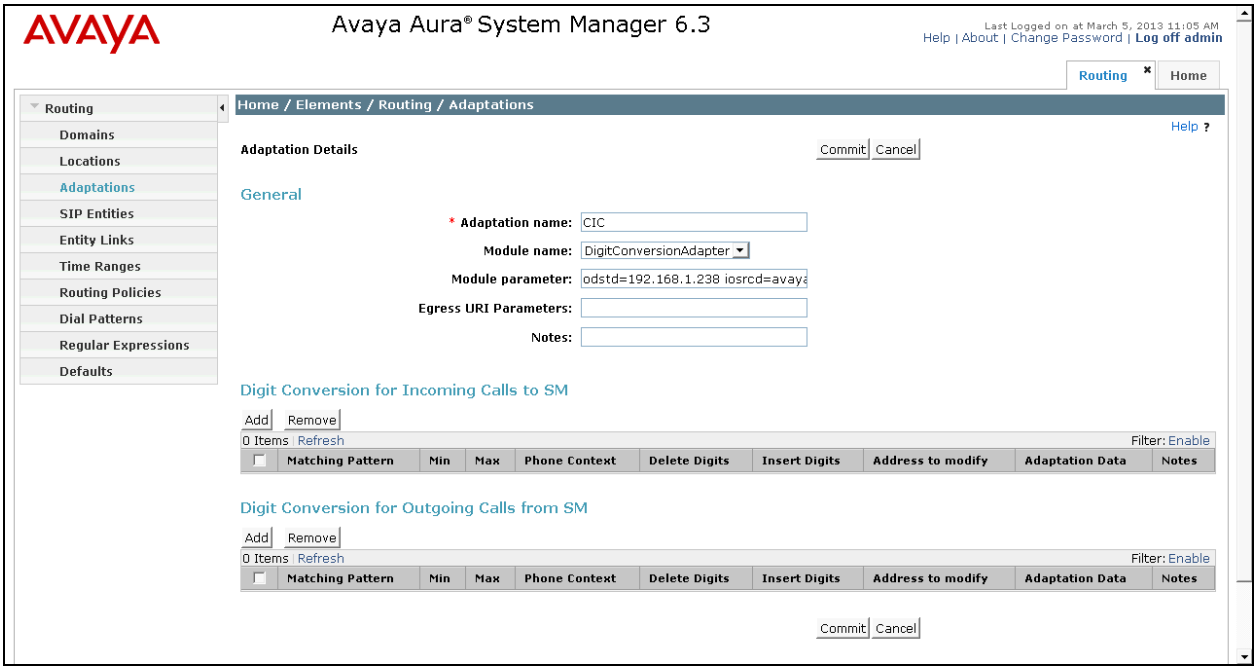
To add an Adaptation, select **Adaptations** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under **General**:

- **Name:** A descriptive name.
- **Module name:** **DigitConversionAdapter**
- **Module Parameter:** **odstd=192.168.1.238 iosrcd=avaya.com fromto=true**

Defaults can be used for the remaining fields. Click **Commit** to save the Adaptation definition.

The following adaptation will be used for calls routed from Interactive Intelligence to Communication Manager.



6.4. Add SIP Entities

In the sample configuration, SIP Entities are added for Session Manager, Communication Manager and Interactive Intelligence CIC.

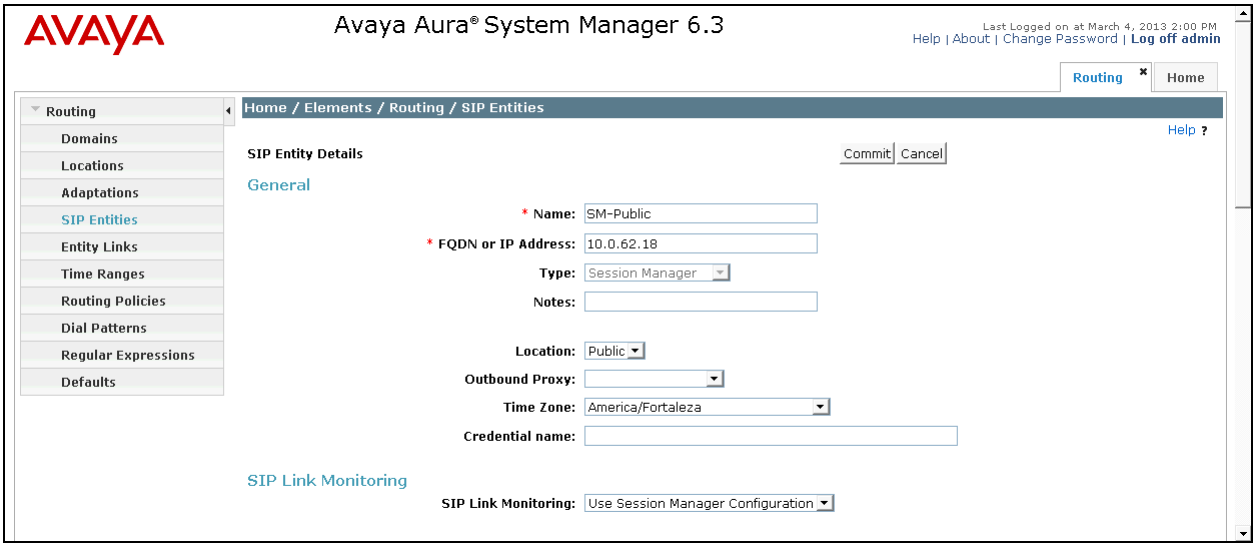
6.4.1. Avaya Aura® Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select **Session Manager**.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save the SIP Entity definition.



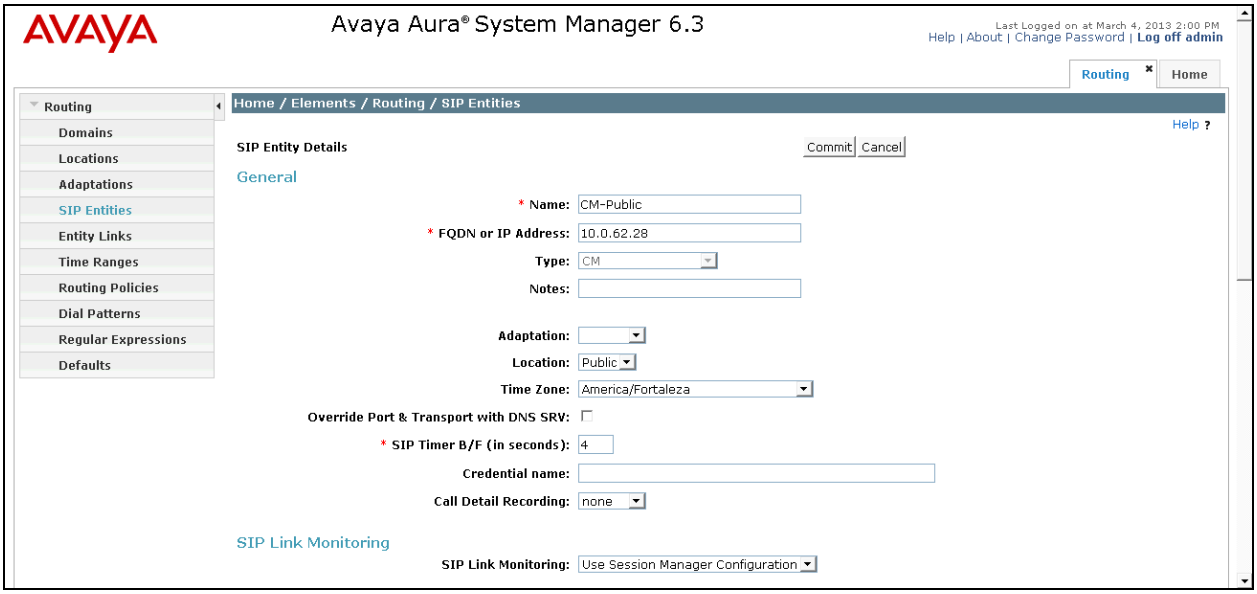
6.4.2. Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (**procr**) in Communication Manager, as seen in **Section 5.1**.
- **Type:** Select **CM**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save the SIP Entity definition.



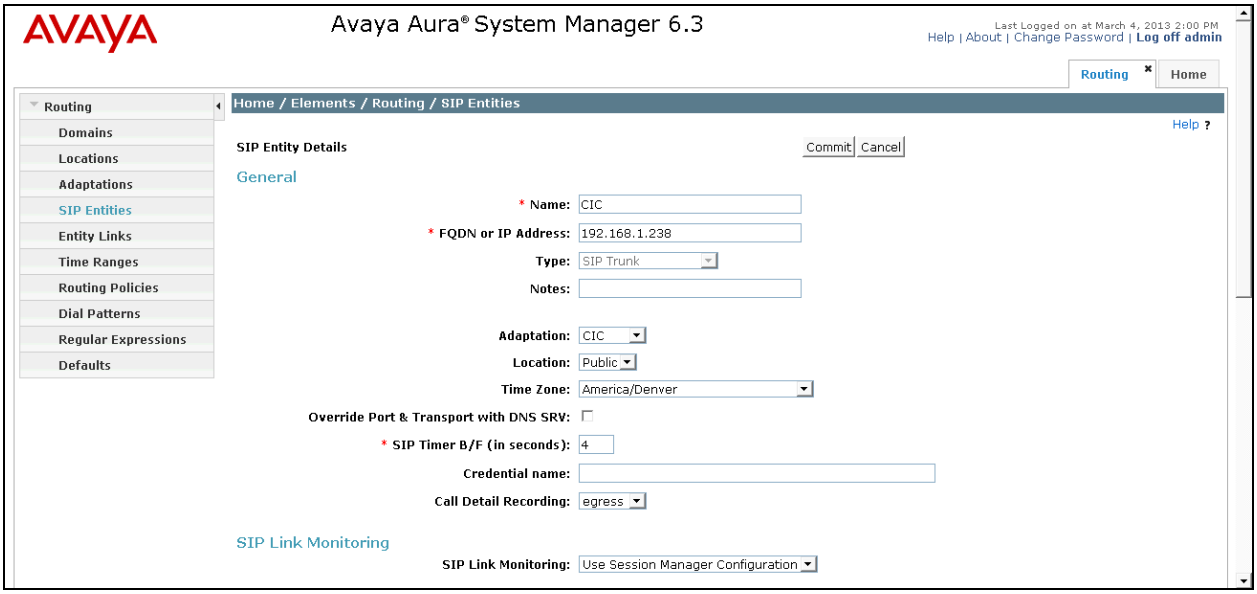
6.4.3. Interactive Intelligence CIC

A SIP Entity must be added for the Interactive Intelligence CIC. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** Interactive Intelligence CIC IP address.
- **Type:** Select **SIP Trunk**.
- **Adaptation:** Select **CIC.**
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save the SIP Entity definition.



6.5. Add Entity Links

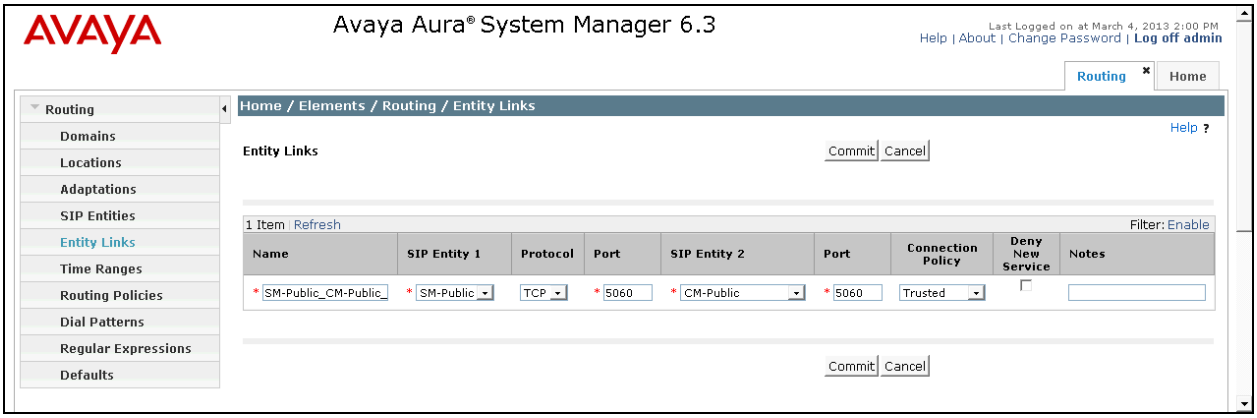
The SIP trunk from Session Manager to Communication Manager and Interactive Intelligence CIC are described by Entity Links. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol for the link.
- **Port:** Port number in which Session Manager will receive SIP requests from the far end.
- **SIP Entity 2:** Select the appropriate SIP entity.
- **Port:** Port number in which the other system will receive SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted**.

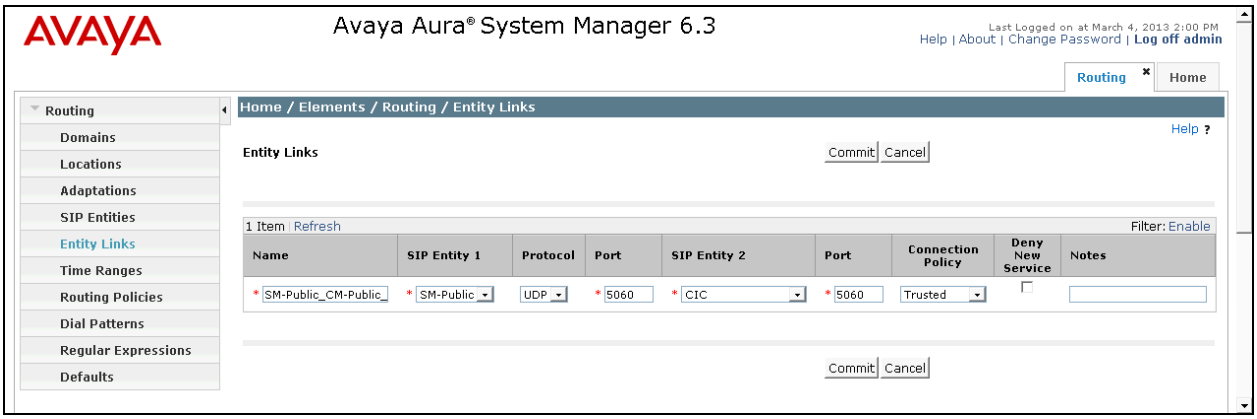
Click **Commit** to save the Entity Link definition.

The following screens display the configuration of each Entity Link. The first entity link is for the connection between Session Manager and Communication Manager and the second entity link is for the connection between Session Manager and Interactive Intelligence CIC.

Session Manager ←→ Communication Manager.
Note: *The Entity Link between Session Manager and Communication Manager uses TCP.*



Session Manager ←→ Interactive Intelligence CIC.
Note: *The Entity Link between Session Manager and Interactive Intelligence CIC uses UDP.*



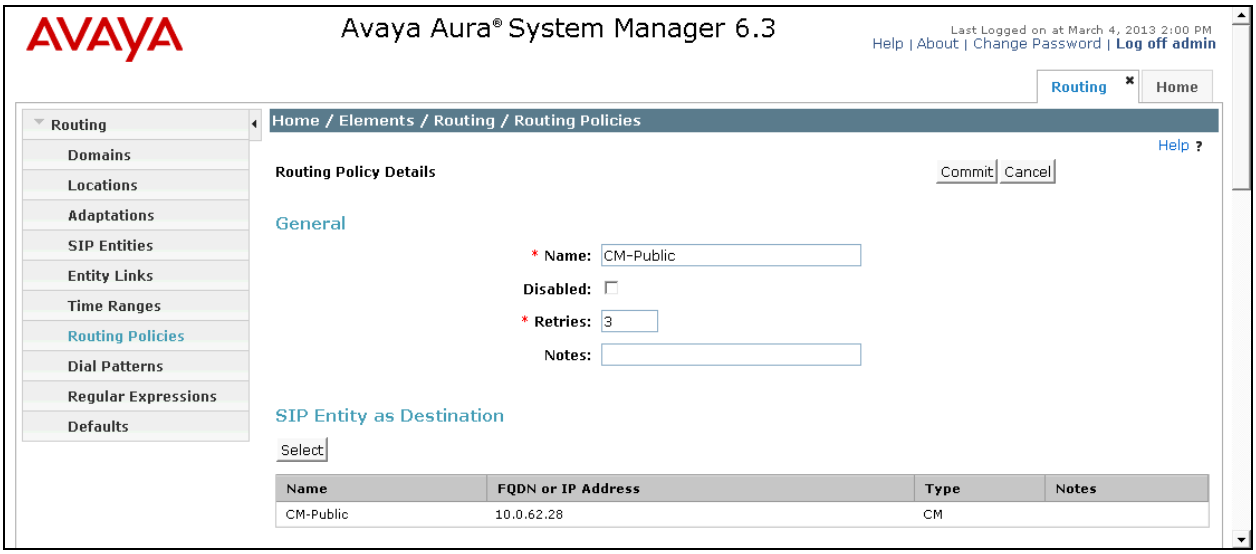
6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies were added – one for Communication Manager, one for Interactive Intelligence CIC. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

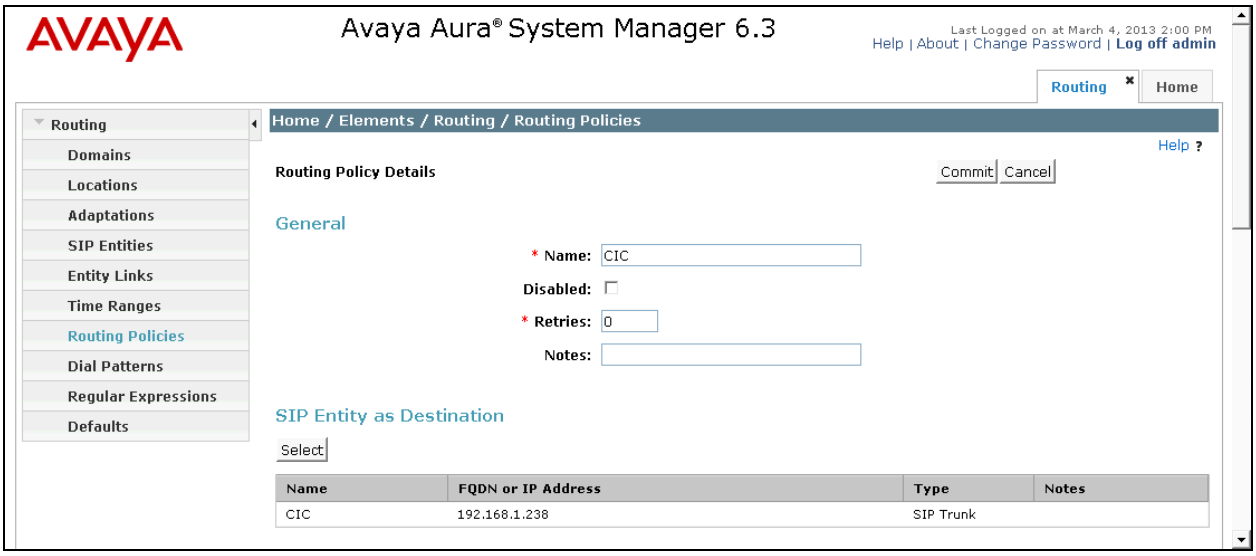
Under **General**:
Enter a descriptive name in **Name**.

Under **SIP Entity as Destination**:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Routing Policy for Communication Manager.



The following screen shows the Routing Policy for Interactive Intelligence CIC..



6.7. Add Dial Patterns

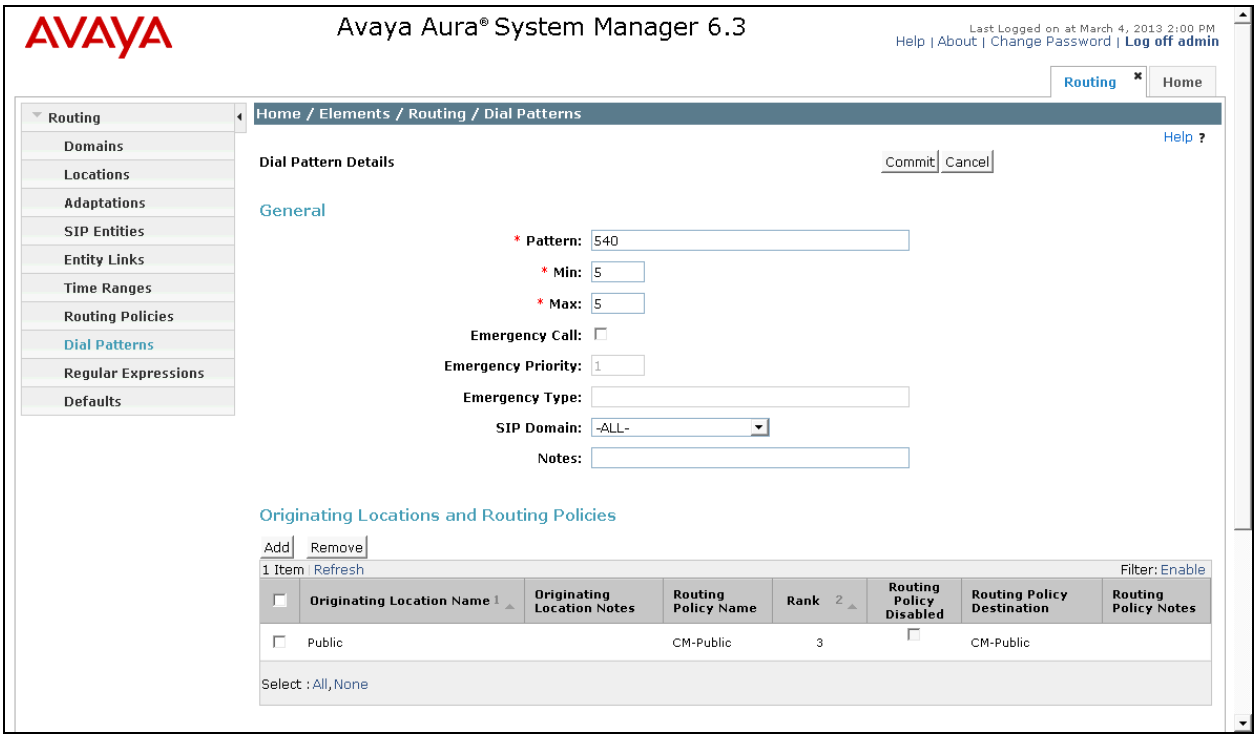
Dial patterns must be defined that will direct calls to the appropriate SIP entity. In the sample configuration, 5-digit numbers beginning with "540" will be routed to the Communication Manager and 5-digit numbers beginning with "6" to CIC. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under **General**:

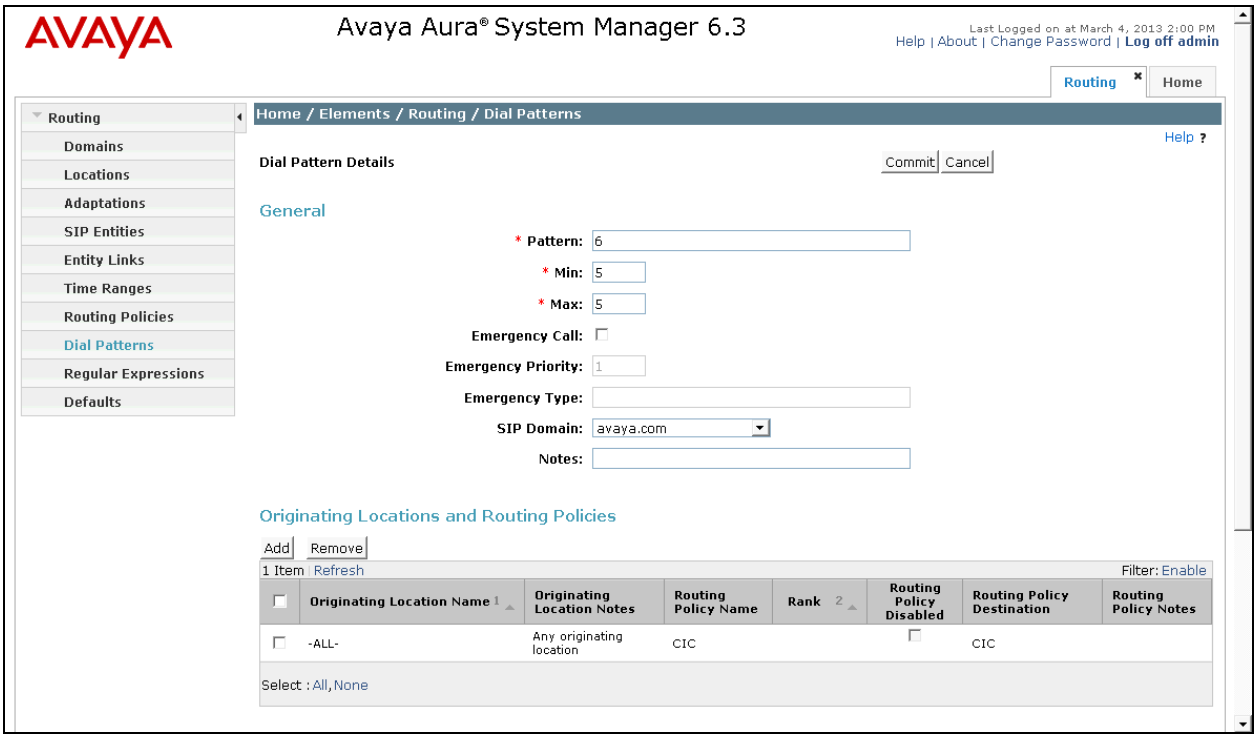
- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern.

Under **Originating Locations and Routing Policies**:
Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definitions for local extensions on Communication Manager.



The following screen shows the dial pattern definition for reaching endpoints and systems via Interactive Intelligence CIC.



7. Configuring Interactive Intelligence CIC

Customer Interaction Center is configured to connect to Session Manager using a SIP Line. The configuration below represents the requirements to communicate with Session Manager.

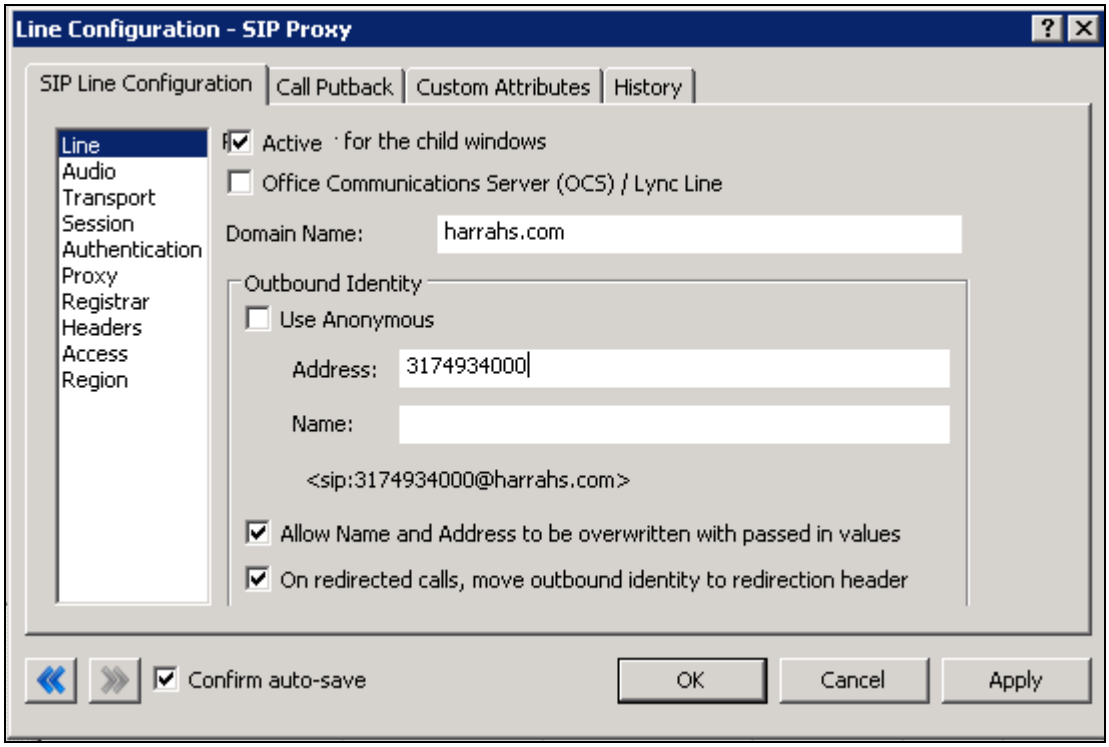
7.1. Configure SIP Line

7.1.1. Line

Configure CIC by launching the Interaction Administrator from the Windows Start Menu. Once opened select **System** and right-click **Lines** to configure a new Line. (Not shown).
Domain Name needs to match on both systems otherwise a manipulation on Session Manager is required for Caller ID.

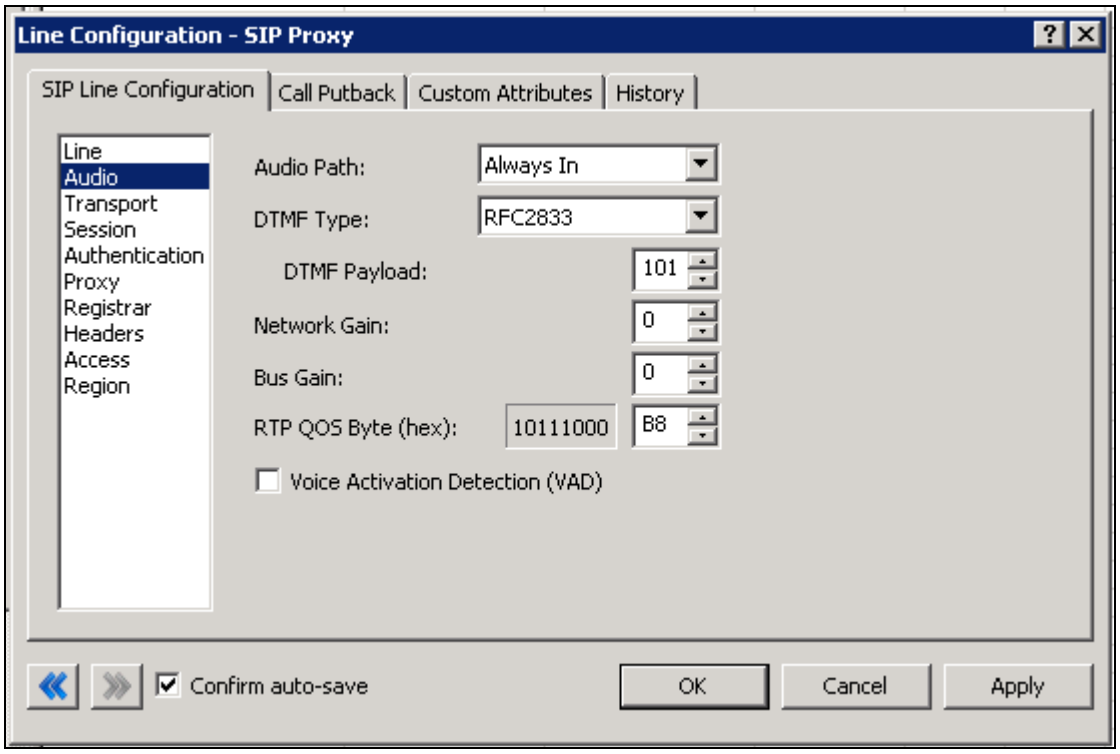
- Domain Name and Address/Name Need to filled in the below screen.

Note: *Compliance testing used a SIP Adaptation on Session Manager to support Caller-ID.*



7.1.2. Audio

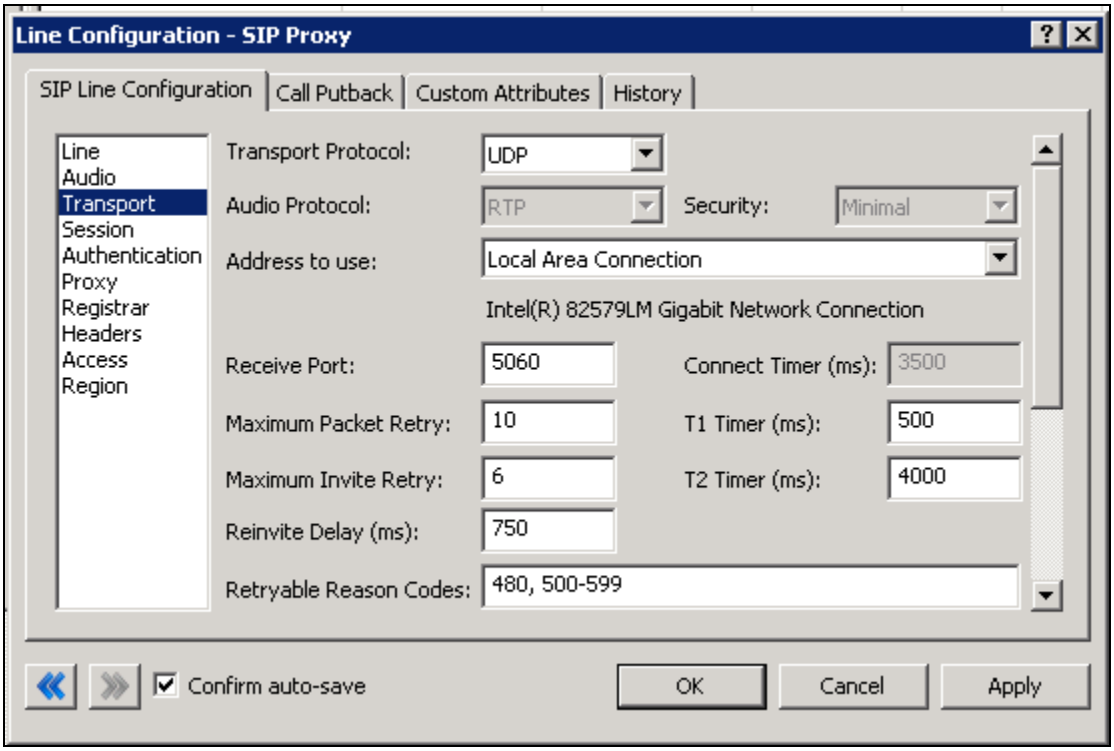
The Selected Audio Path needs to be set to **Always In**. This setting forces the Interactive Media Server to always be in the audio path.

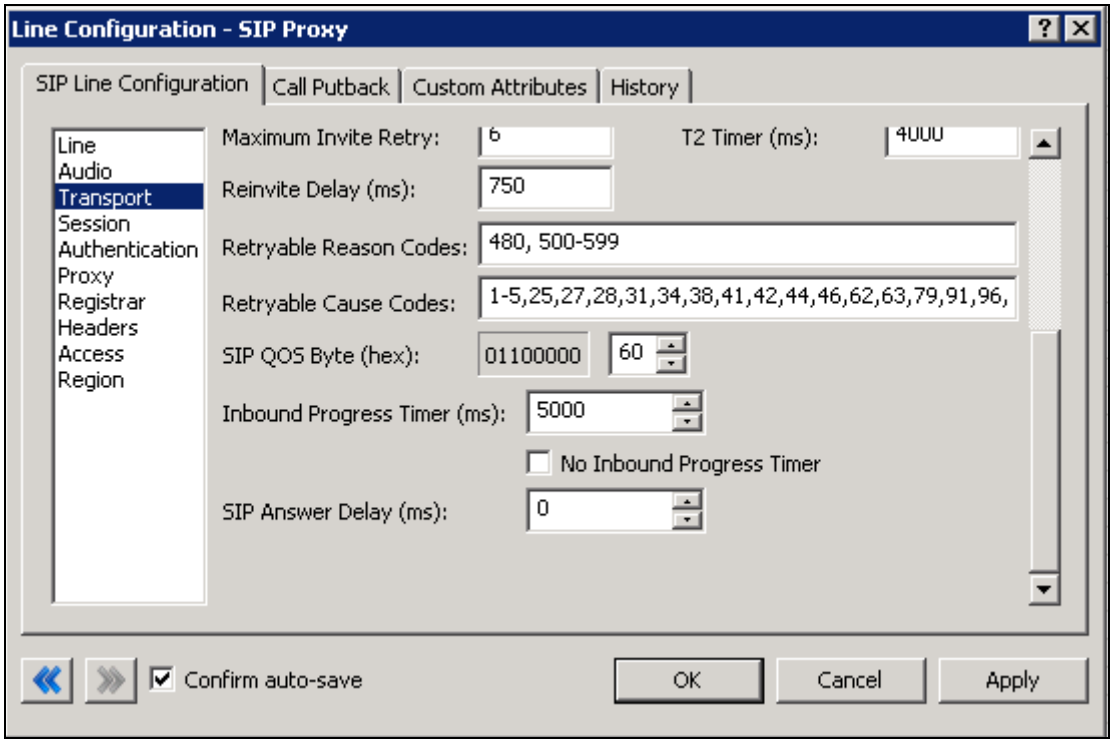


Note: *Always-In: The audio will flow through the Interaction Media Server (if one is available in the topology) or the CIC Server (if no Interaction Media Server is configured or available).* ***Used in this scenario to ensure proper audio.***

7.1.3. Transport

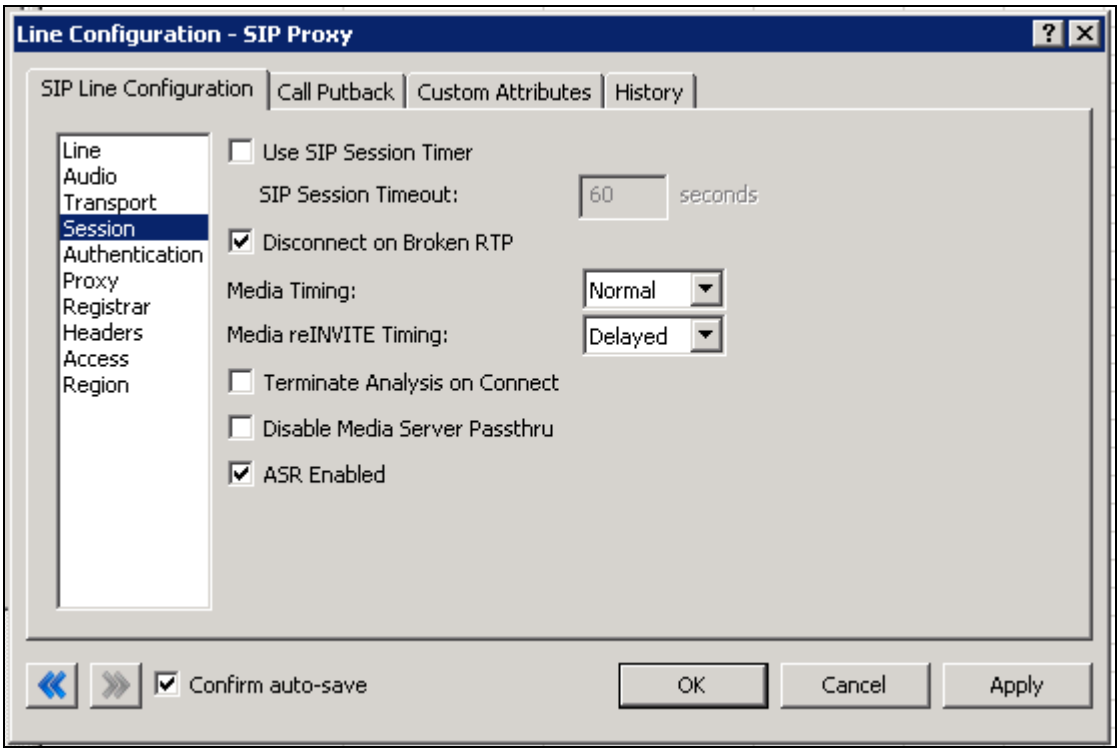
Transport Protocol should be set to UDP (Can also be set to TCP if required).





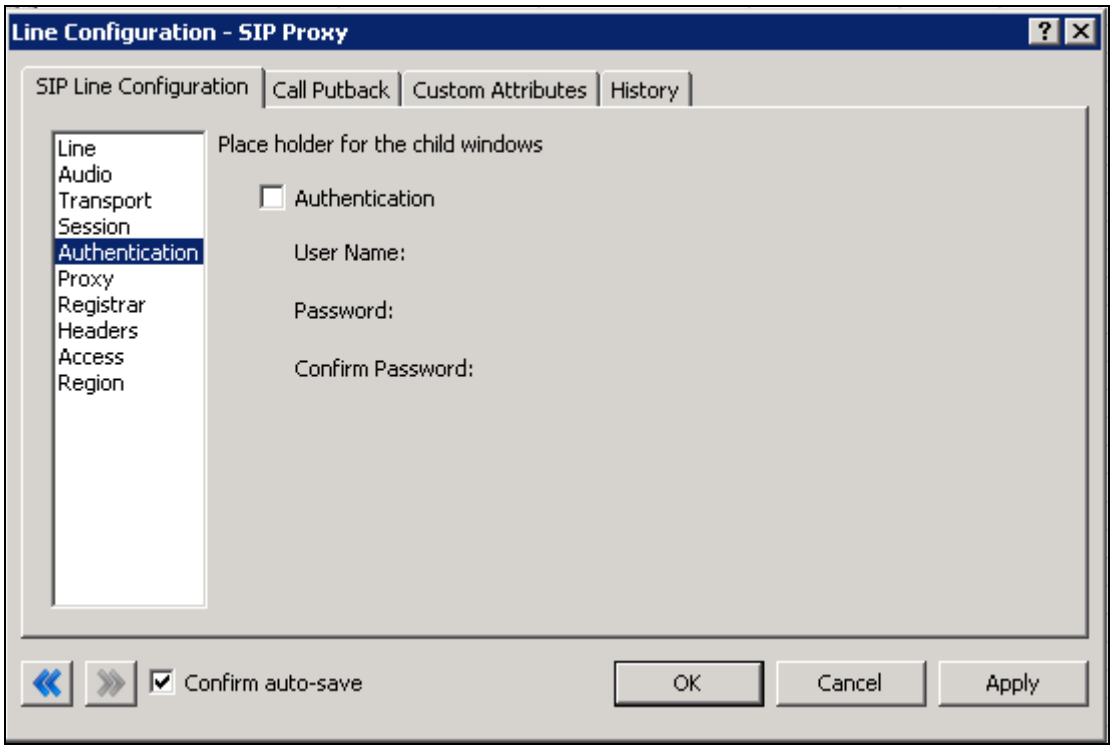
7.1.4. Session

Default values do not need to be adjusted.



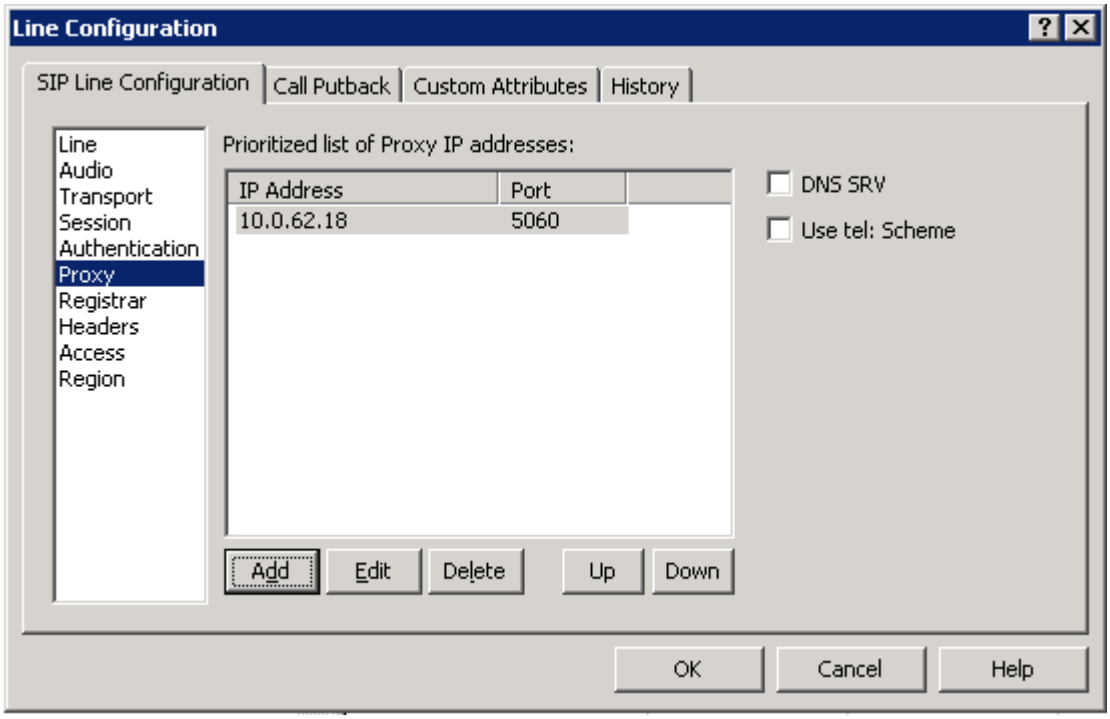
7.1.5. Authentication

Default values do not need to be adjusted.



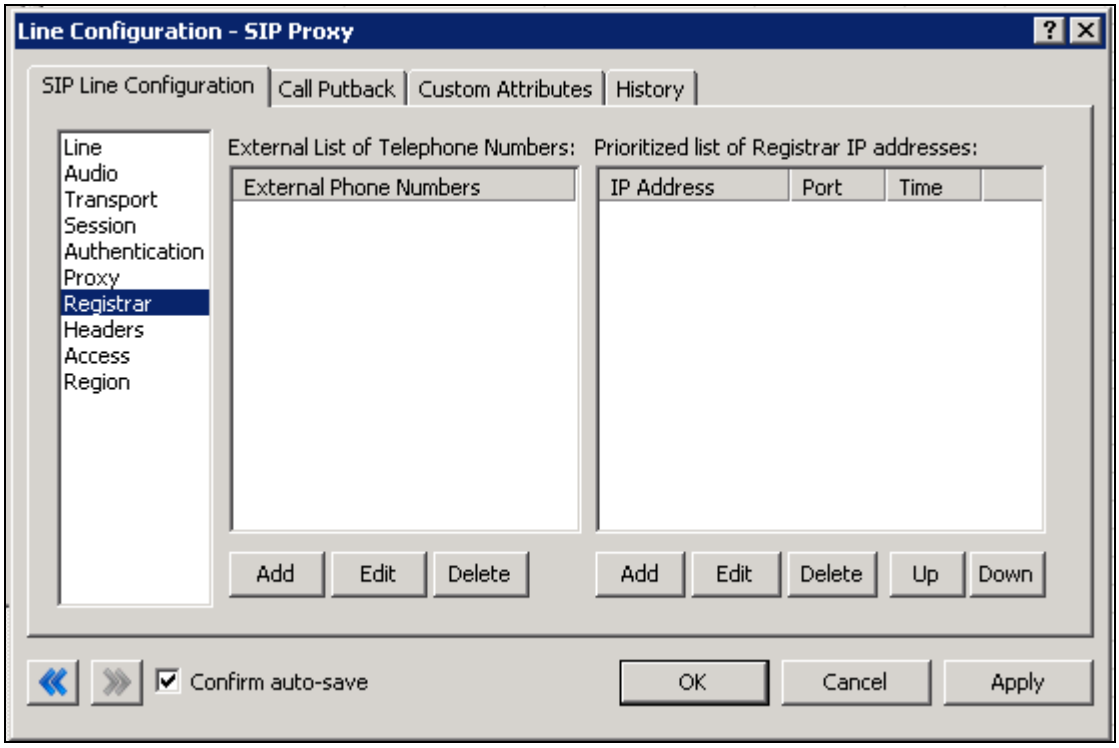
7.1.6. Proxy

IP Address of SIP Proxy or device of where traffic is sent is entered below. This should be the IP address of Session Manager.



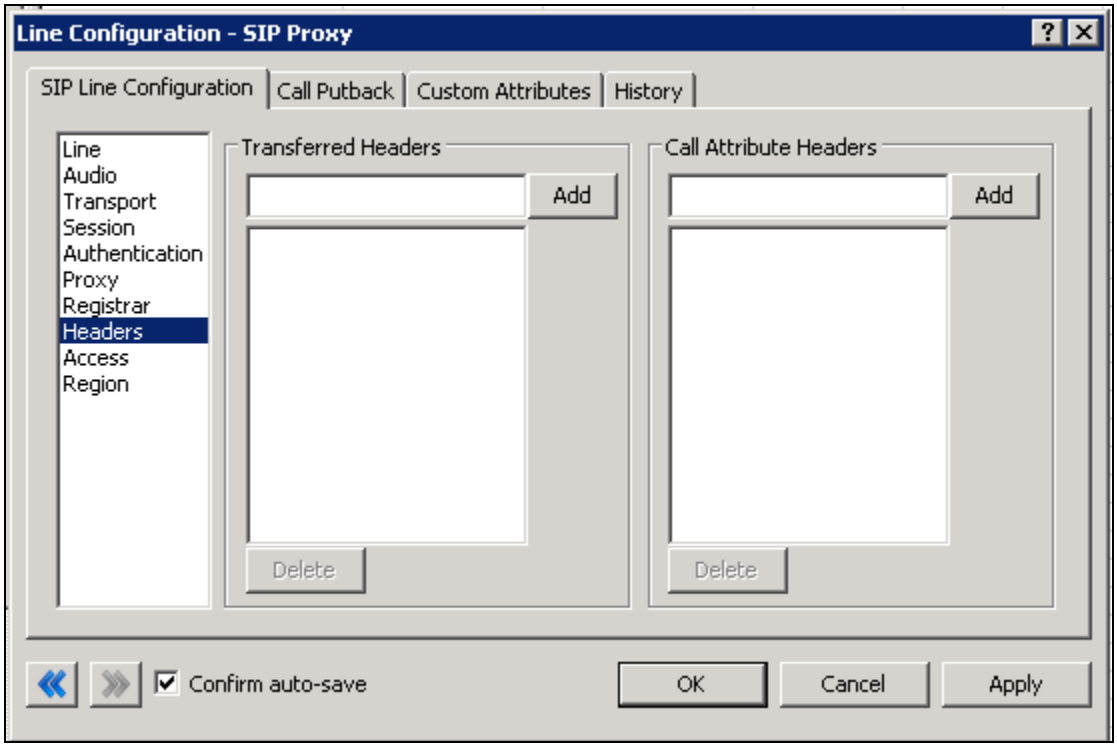
7.1.7. Registrar

Default values do not need to be adjusted.



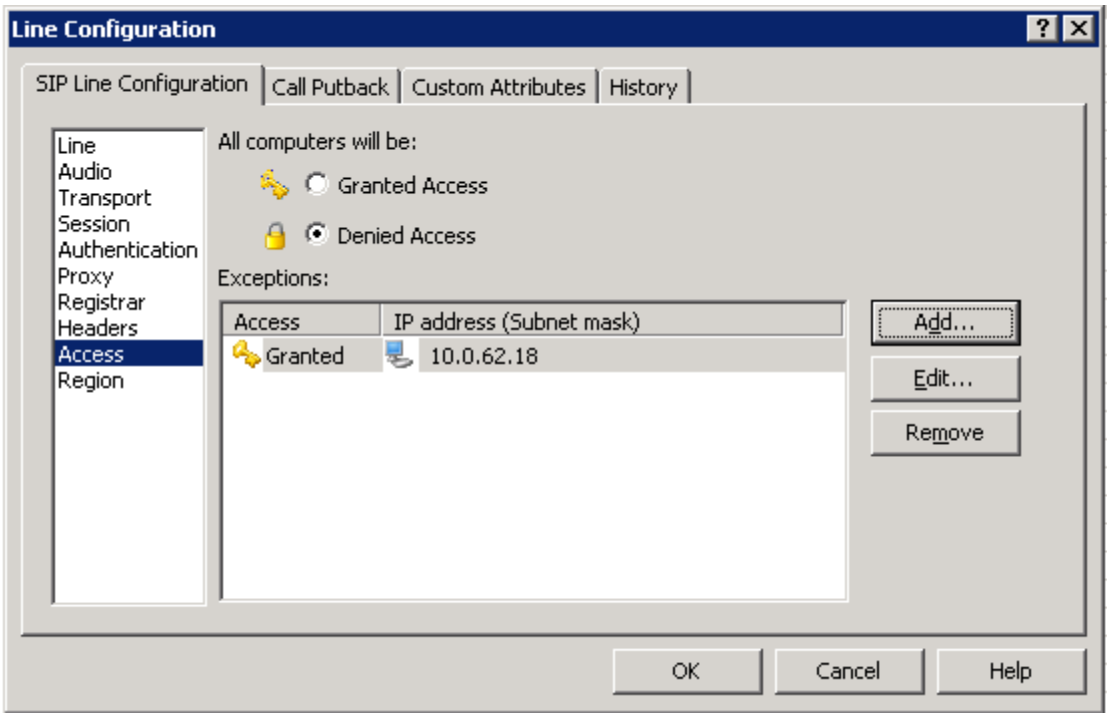
7.1.8. Headers

Default values do not need to be adjusted.



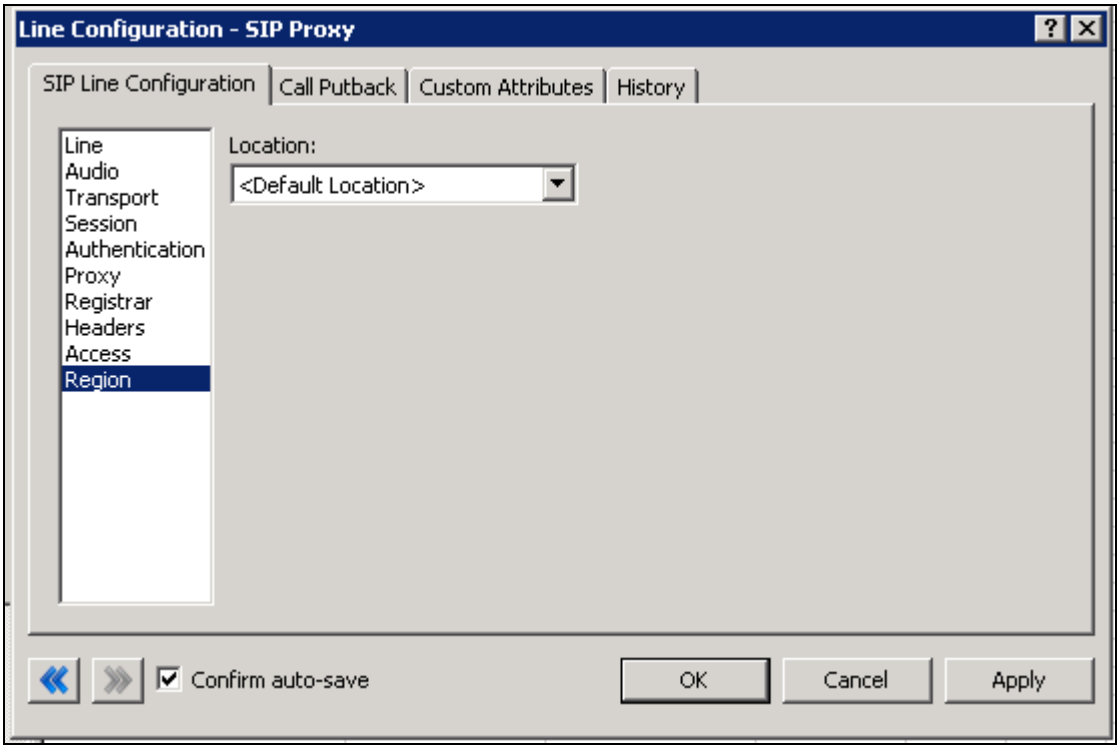
7.1.9. Access

IP Address of SIP Proxy or device of where traffic is being received from. This should be the IP address of Session Manager.
No other device is given access to the server.



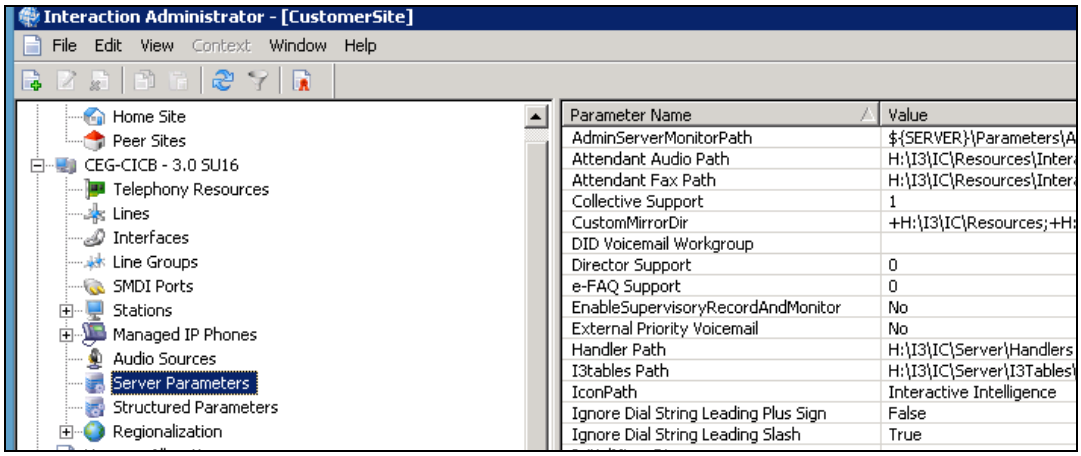
7.1.10. Region

Select Region below and specify the Line Location. Normally this is the Default Location. This will be based on Dial Plan needs.

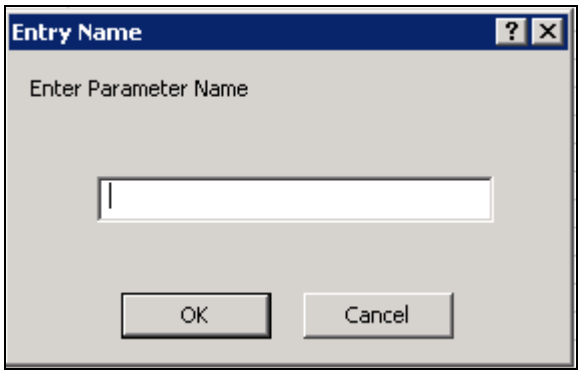


7.1.11. P-Asserted Identity

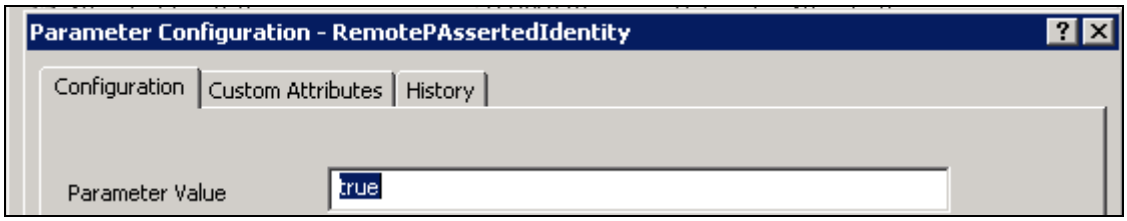
In support of Caller-ID for CIC the following parameters are required.
To add these parameters the Container Server Parameters must be selected in Interaction Administrator.

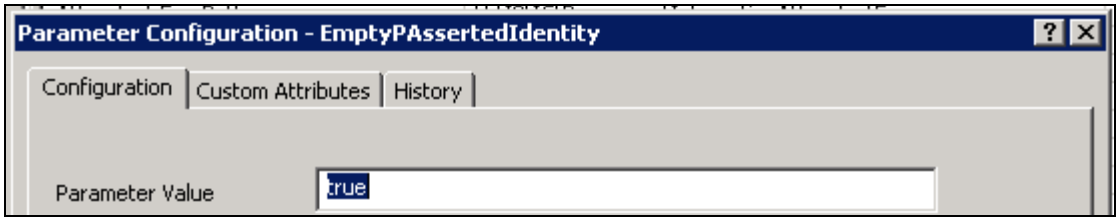


By Right-clicking and selecting New inside of the Server Parameters Container, a new Parameter can be entered with the appropriate values.



Below are the Parameter Values that were entered to add support for Caller-ID.





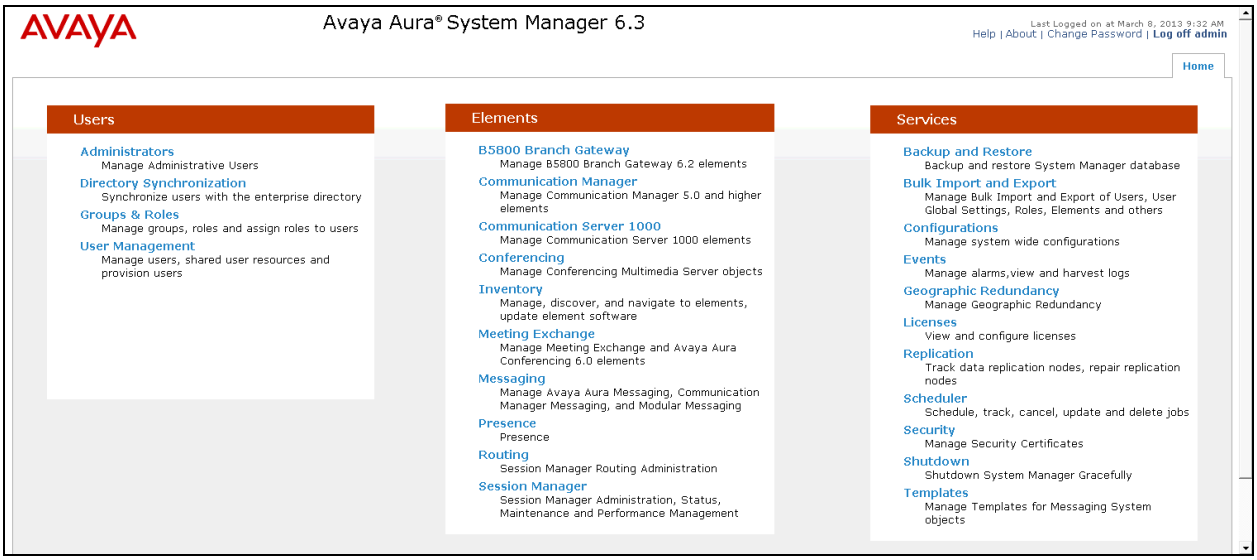
8. Verification Steps

The following steps may be used to verify the configuration.

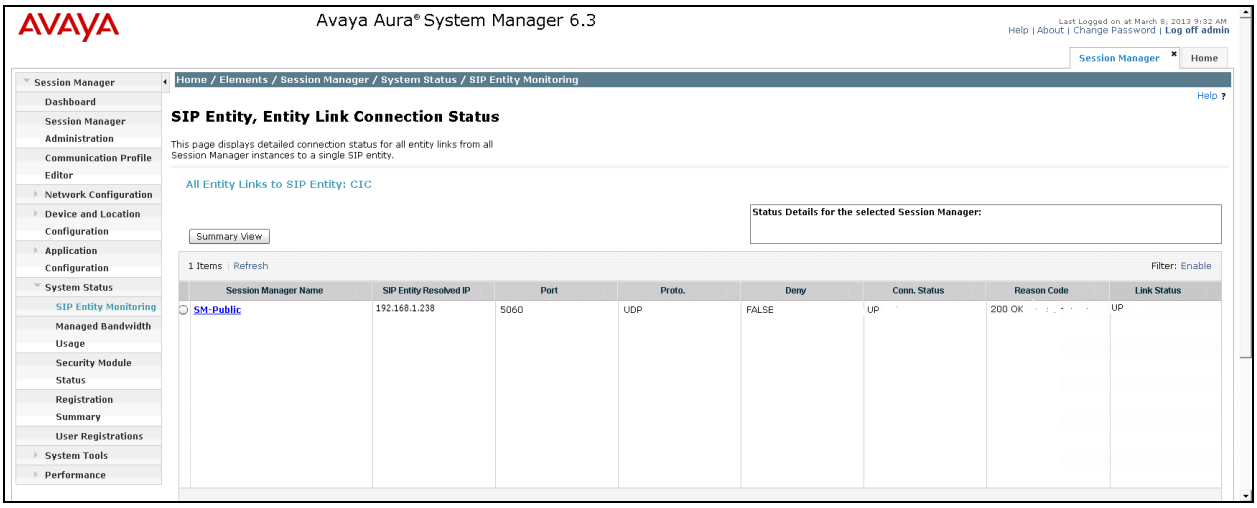
8.1. Verify SIP Entity Link Avaya Aura® Session Manager

Verification can be accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials.

From the **Home** tab select **Session Manager → System Status → SIP Entity Monitoring**.



From the SIP Entity Link Monitoring Status Summary page (not shown) click on the desired Session Manager then click on the desired **SIP Entity Name** to display the screen below. Verify that the **Conn. Status** and **Link Status** are both **UP**.



8.2. Verify Interactive Intelligence CIC

Verification can be accomplished by placing a call to the Avaya System and or receiving a call from the Avaya System.

9. Conclusion

These Application Notes have described the administration steps required to configure Interactive Intelligence CIC to integrate with an Avaya Aura® Telephony Infrastructure. The solution verified interoperability and proper call handling between the two systems as depicted in **Figure 1.**

10. Additional References

The documents referenced below were used for additional support and configuration information.

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Administering Avaya Aura® Communication Manager*, Doc # 03-300509
[2] *Administering Avaya Aura® Session Manager*, Doc # 03-603324

Product documentation for Interactive Intelligence products may be found at http://www.inin.com/support

[3] IC 3.0 Documentation Library
https://my.inin.com/support/products/ic30/Documentation/index.htm

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.