Avaya Solution & Interoperability Test Lab

Application Notes for Amtelco 1Call Web Agent Release 5.5 with Avaya Aura® Session Manager Release 8.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Amtelco 1Call Web agent to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunks. Amtelco 1Call Web agent is a SIP-based solution that provides operator users with phone and call controls.

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 Amtelco 1Call Web Agent (Web Agent) to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunks. Amtelco 1Call Web Agent is a SIP-based solution that provides operator users with phone and call controls.

The 1Call Web solution consists of the Genesis Telephony Server, Intelligent Series Server, 1Call Web server, and 1Call Web Agent. Operators have desktops running the 1Call Web Agent in the internet browser application, with dedicated audio connections via SIP with the Genesis Telephony Server.

For compliance testing, calls from internal and external callers were routed over SIP trunks via Session Manager to 1Call Web Agent for operator functions. Genesis tracked the operator states and routed calls to available operators, and populated answering operator desktops with pertinent call information such as calling and called numbers. All call controls were performed from the operator desktops.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were placed manually with necessary operator actions such as hold and transfer, performed from the operator desktops.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Genesis servers and/or clients.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between the Avaya system and Amtelco Genesis did not use secure encryption feature as requested by Amtelco.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included inbound, outbound, internal, external, G.711MU, outbound DTMF, hold/resume, drop, display, transfer, supervised conference, multiple calls, and multiple operators.

The serviceability testing focused on verifying the ability of 1Call Web Agent to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Genesis servers and/or clients.

2.2. Test Results

All test cases were executed and verified. There is one observation below.

- The unsupervised transfer feature was accomplished by 1Call Web Agent via use of SIP REFER, and the supervised transfer and supervised conference features were accomplished by 1Call Web Agent via merge/unmerge of respective audio connections.

2.3. Support

Technical support on Amtelco 1Call Web Agent can be obtained through the following:

- **Phone:** +1 (800) 553-7679
- **Email:** service@amtelco.com
- **Web:** https://www.amtelco.com/customer-support

3. Reference Configuration

As shown in **Figure 1**, operators have desktops running the Intelligent Series Soft Agent application, and dedicated SIP connections with the Genesis Server as part of log in. The Intelligent Series Supervisor was running on the supervisor desktop.

SIP trunks were used between the 1Call Web Telephony Server and Session Manager. A 4 digit Uniform Dial Plan was used to facilitate dialing with the 1Call Web. Calls to extensions 52xx were routed over the SIP trunks to Genesis. In particular, internal users on Communication Manager will dial 5200 to reach Genesis.

The detailed administration of connectivity between Communication Manager and Session Manager are not the focus of these Application Notes and will not be described.

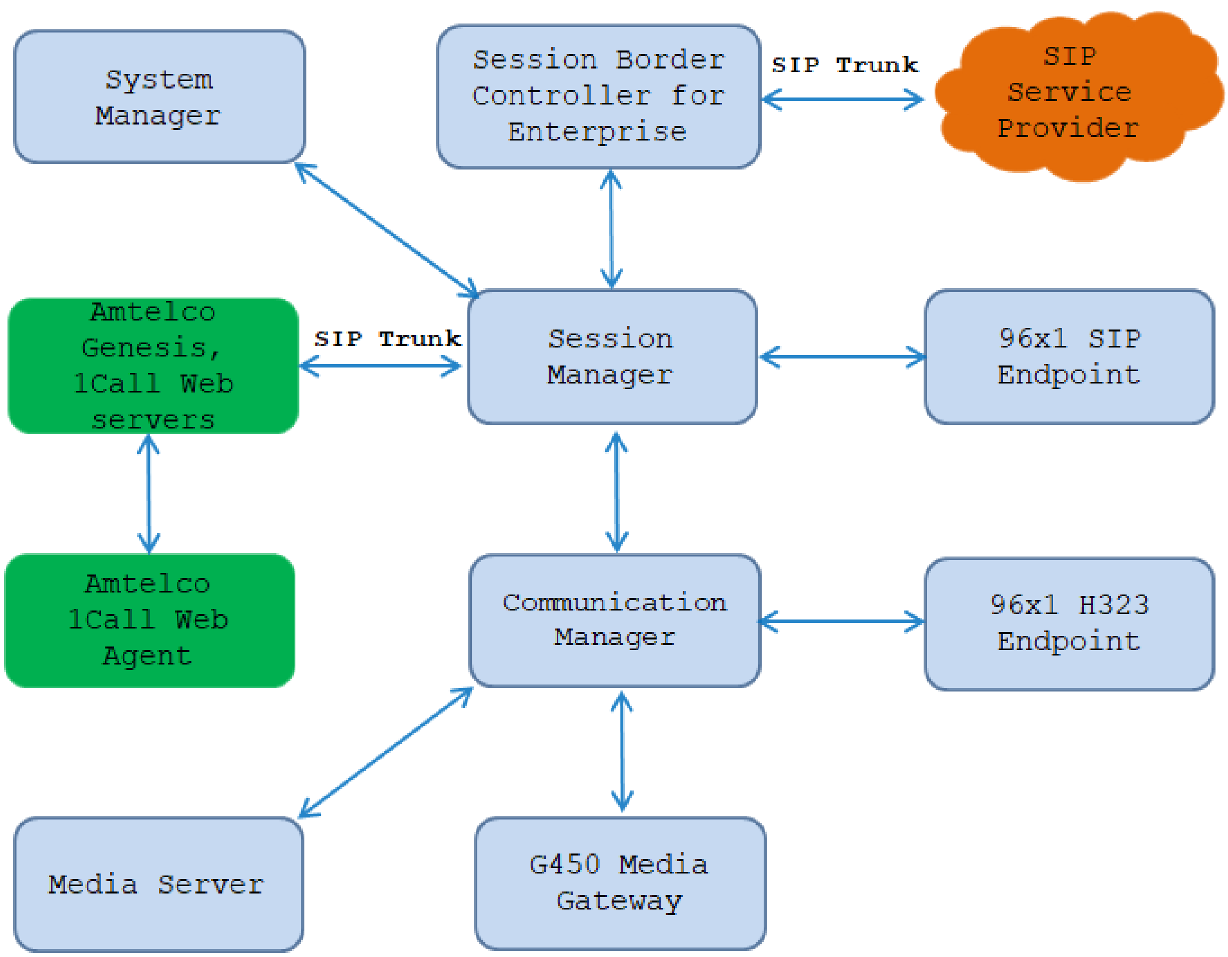


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Environment	8.1.3 8.1.3.2.0.890.26989
Avaya G450 Media Gateway	41.34.0
Avaya Aura® Media Server running on Virtual Environment	8.0 8.0.2.163
Avaya Aura® System Manager running on Virtualized Environment	8.1.3 8.1.3.0.1011784
Avaya Aura® Session Manager running on Virtualized Environment	8.1.3 8.1.3.0.813014
Avaya Session Border Controller for Enterprise	8.1.2 8.1.2.0-37-21065
Avaya 9611G IP Deskphone (SIP)	7.1.9.0.8
Avaya 9641G IP Deskphone (H.323)	6.8304
Amtelco Genesis Telephony Server running on Linux Ubuntu Amtelco Web Server running on Linux Ubuntu Amtelco IS Server running on Windows 2016	Asterisk PBX 16.23.0 Web Agent 5.5.7605.26

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis

For compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for integration with Genesis.

5.1. Verify License

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

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

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 10
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 30
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

5.2. Administer System Parameters Features

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

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/Tone on Hold: music Type: ext   1104
              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
```

5.3. Administer SIP Trunk Group

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

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

```
add trunk-group 1                                                Page   1 of  22
                                TRUNK GROUP

Group Number: 1                    Group Type: sip            CDR Reports: y
  Group Name: Private Trunk               COR: 1        TN: 1        TAC: #01
   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: 14
```

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

```
change trunk-group 1                                                Page   3 of  22

TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y
```

5.4. Administer SIP Signaling Group

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

- **Group Type:** "sip"
- **Transport Method:** "tls"
- **Near-end Node Name:** An existing C-LAN node name or "procr" in this case.
- **Far-end Node Name:** The existing Session Manager node name.
- **Near-end Listen Port:** An available port for integration with Genesis.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with Genesis.
- **Far-end Domain:** The applicable domain name for the network.
- **Direct IP-IP Audio Connections**: enter "y".

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

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? n  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: interopASM
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: bvwdev.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
```

5.6. 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**, enter the applicable domain for the network. 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 Genesis.

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

Navigate to **Page 4**, and specify this codec set to be used for calls with the network region used by the Avaya endpoints and with the PSTN. In the compliance testing, network region "1" was used by the Avaya endpoints and trunk to the PSTN.

```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I     S M
                                                                     G  A  y t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G  n c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L  c e
 1    1                                                                all
 2    2      y    NoLimit                                            n     y t
 3    1      y    NoLimit                                            n     y t
 4
 5
 6    6      y    NoLimit                                            n     y t
 7    7      y    NoLimit                                            n     y t
 8
```

5.7. Administer IP Codec Set

Use the "change ip-codec-set n" command, where "n" is the codec set number from **Section 5.6**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that Genesis supports the G.711 and G.729 codec variants, with G.729 requiring special license on Genesis. The compliance testing only covered the G.711 codec.

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

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.729            n          2        20
 3: G.722-64K                   2        20
 4:
 5:
 6:
 7:
```

5.8. Administer Route Pattern

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

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

```
change route-pattern 1                                          Page   1 of   3
                      Pattern Number: 1      Pattern Name: SIP-TLS-To-SM
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp  FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No           Mrk Lmt List Del  Digits                              QSIG
                              Dgts                                     Intw
 1: 1    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               lev0-pvt  next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
```

5.9. Administer Private Numbering

Use the "change private-numbering 0" command, to define the calling party number to send to Genesis. Add an entry for the trunk group defined in **Section 5.3**. In the example shown below, all calls originating from a 4-digit extension beginning with 33 and 34 routed to trunk group 1 will result in a 4-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
 4  33               1                             4
 4  34               1                              4
```

5.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 52xx to Genesis. Note that other routing methods may be used. Use the "change uniform-dialplan 0" command and add an entry to specify the use of AAR for routing of digits 52xx, as shown below.

```
change uniform-dialplan 5                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                            Percent Full: 0

  Matching                   Insert              Node
  Pattern       Len Del      Digits     Net Conv Num
  52              4   0                  aar  n
```

5.11. Administer AAR Analysis

Use the "change aar analysis 0" command and add an entry to specify how to route calls to 52xx. In the example shown below, calls with digits 51xx will be routed as an AAR call using route pattern "52" from **Section 5.8**.

```
change aar analysis 5                                         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
    52                   4    4      1        aar          n
```

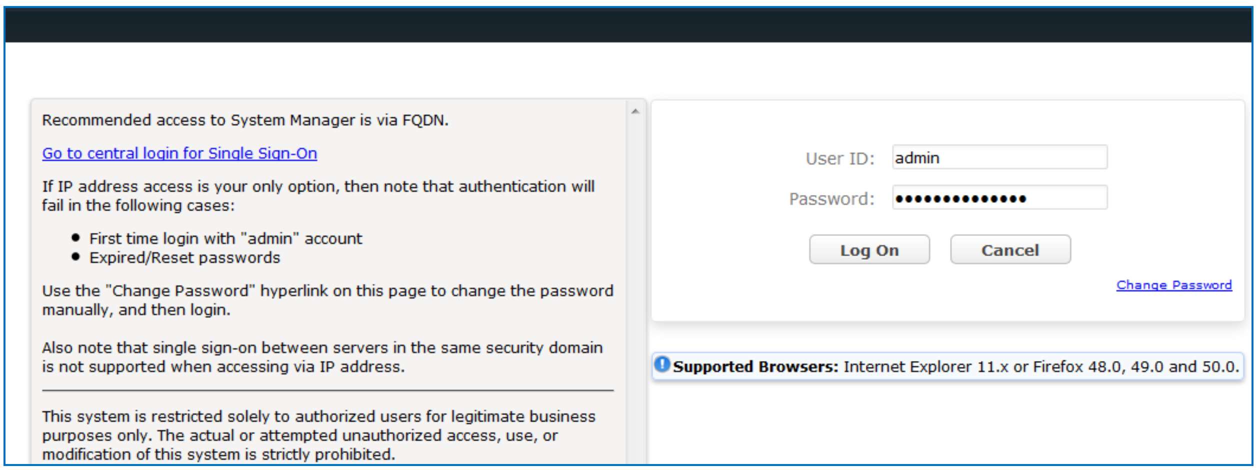
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer locations
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

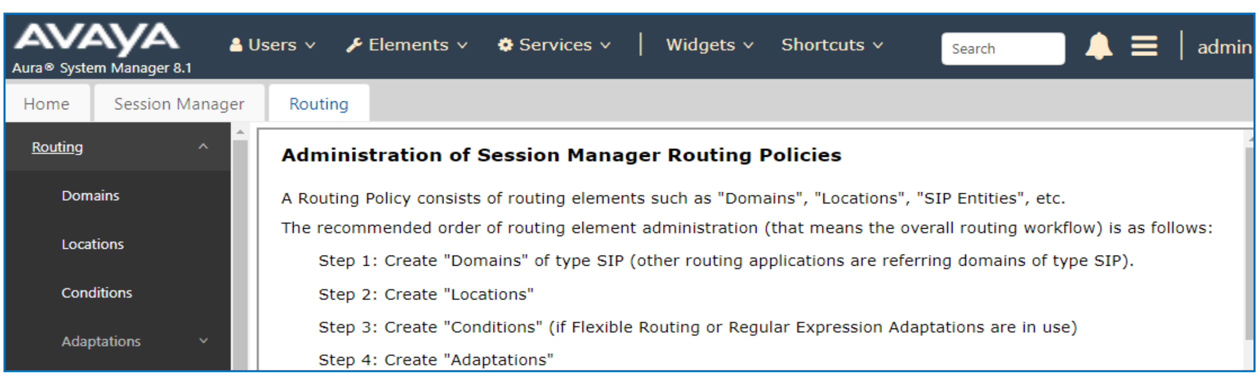
6.1. Launch System Manager

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 System Manager. Log in using the appropriate credentials.

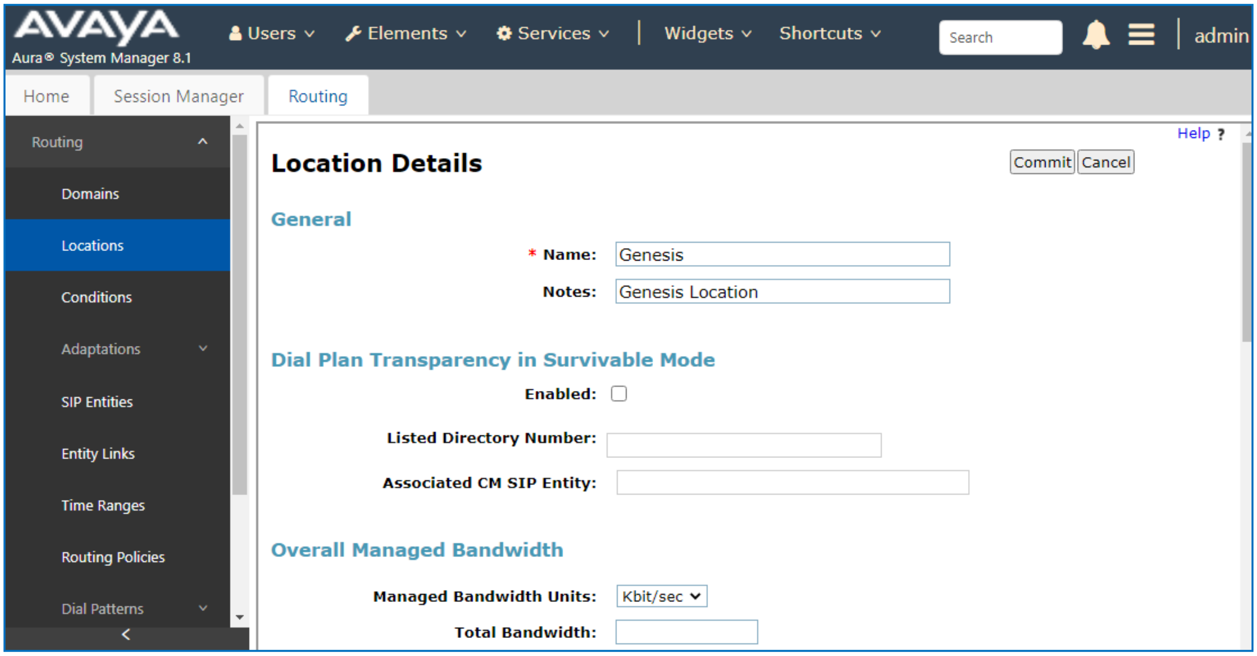


6.2. Administer Locations

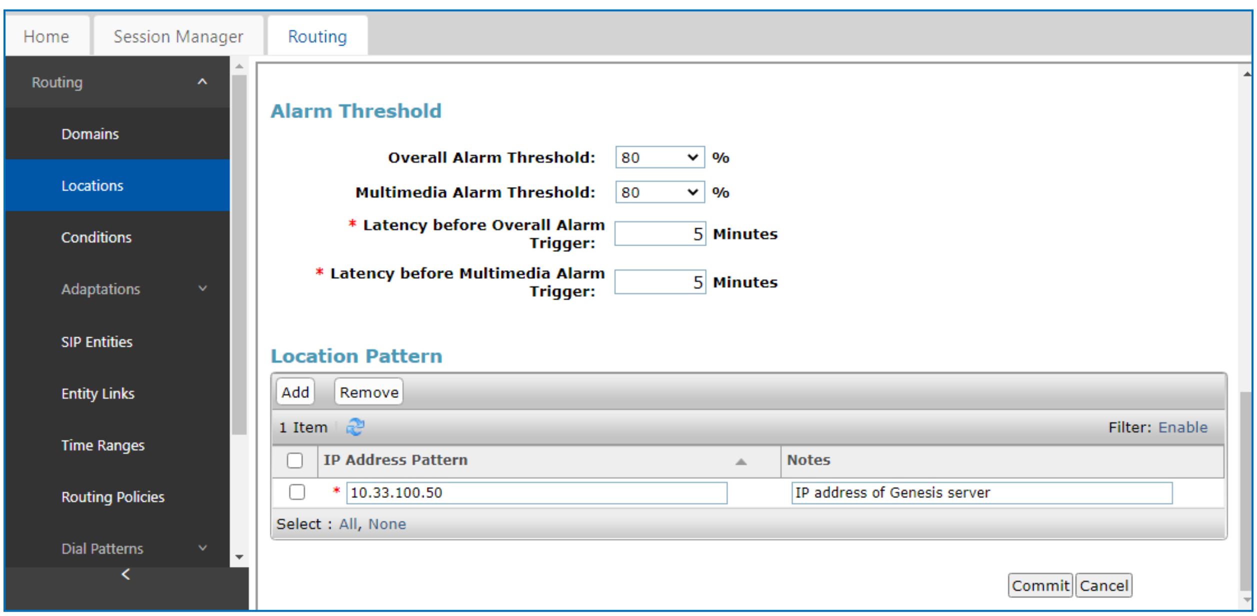
In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing → Locations** from the left pane and click **New** in the subsequent screen (not shown) to add a new location for Genesis.



The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.



Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of the Genesis Telephony Server in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.



6.3. Administer SIP Entities

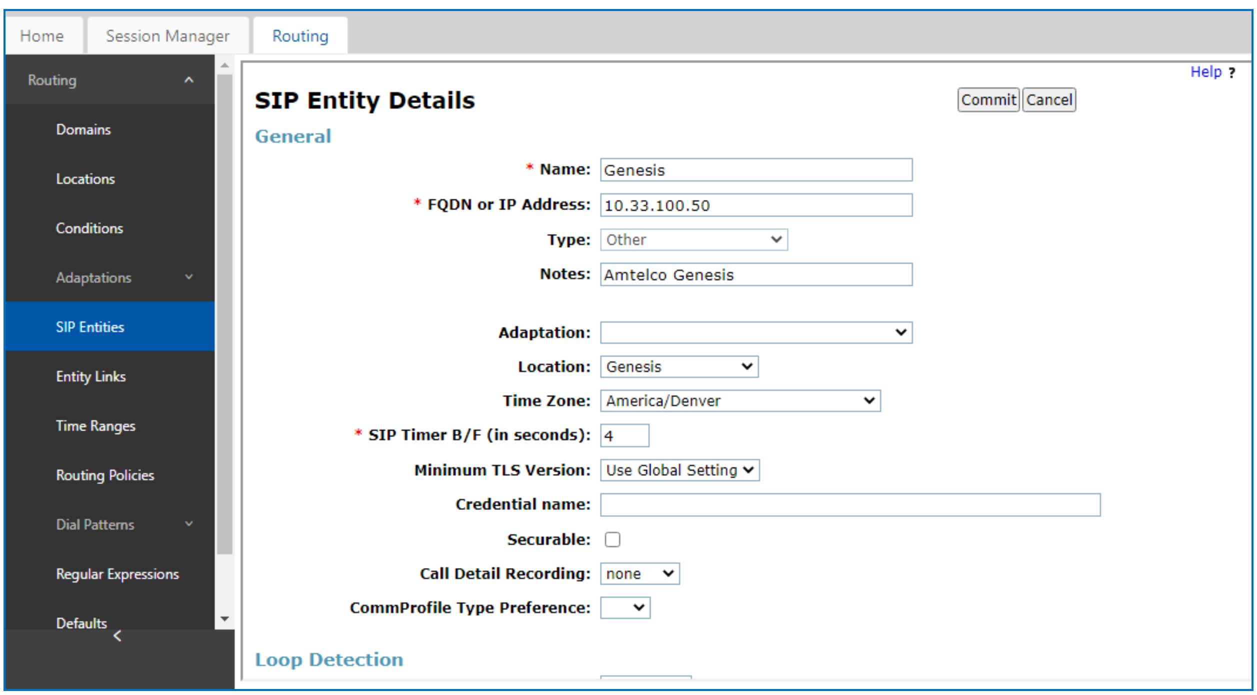
Add two new SIP entities, one for Genesis and one for the new SIP trunks with Communication Manager.

6.3.1. SIP Entity for Genesis

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

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

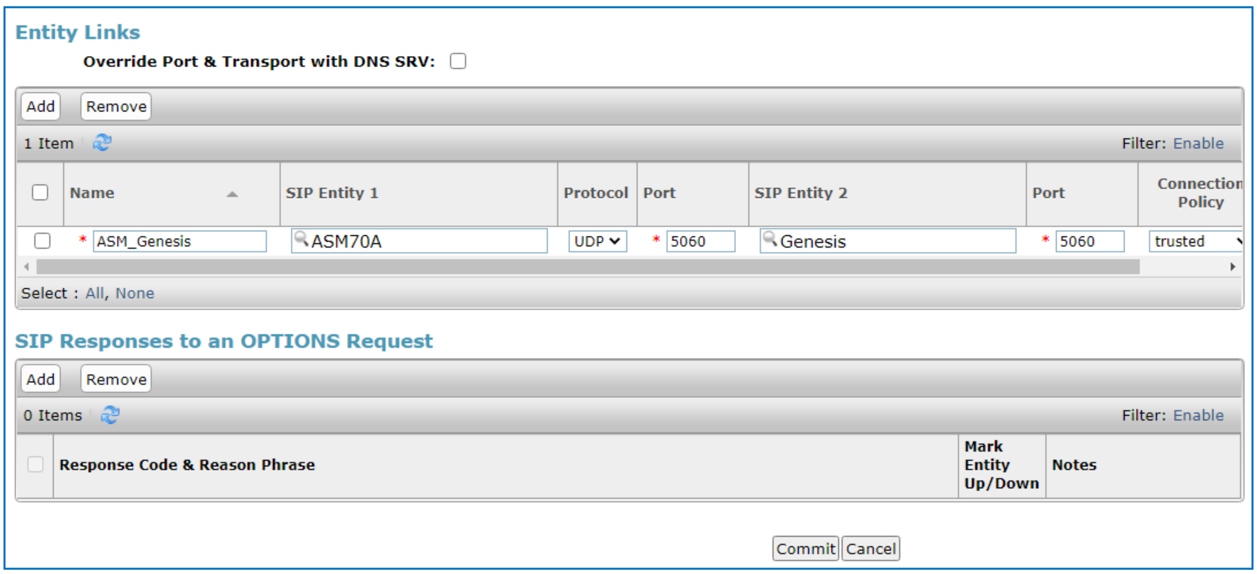
- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Genesis Telephony Server.
- **Type:** "Other"
- **Notes:** Any desired notes.
- **Location:** Select the Genesis location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.



Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. 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 “ASM70A”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The Genesis entity name from this section.
- **Port:** “5060”
- **Connection Policy:** “trusted”

Note that Genesis can support UDP and TCP. For compliance testing,the UDP protocol was used.

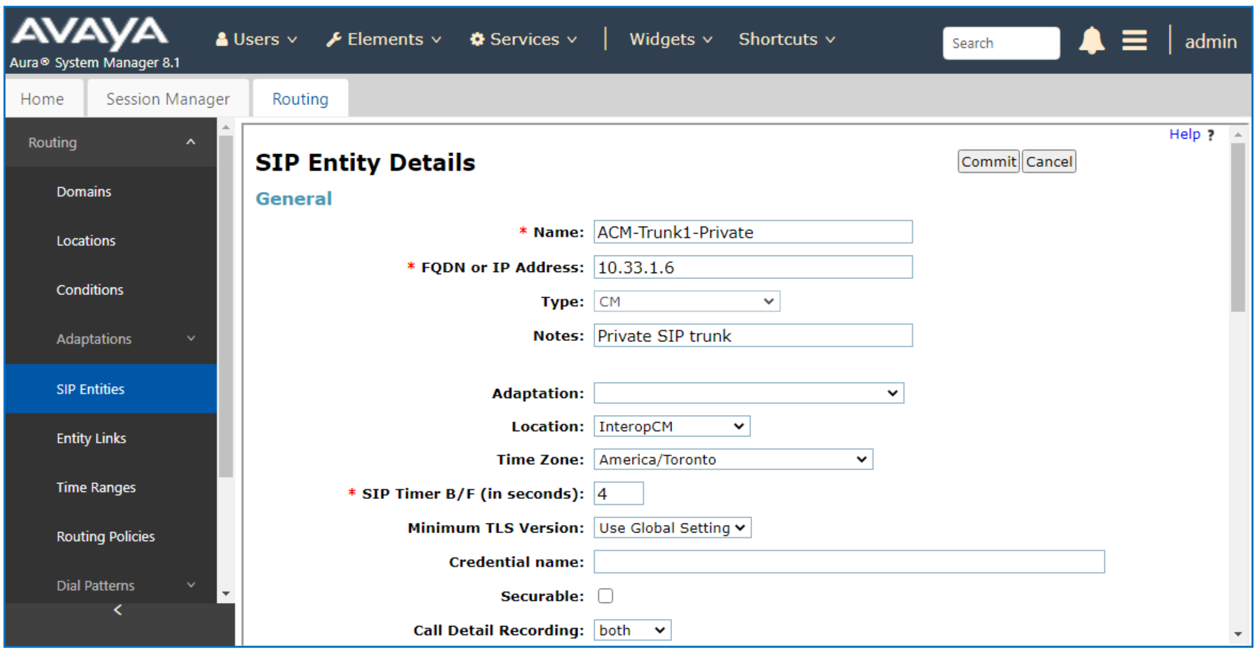


6.3.2. SIP Entity for Communication Manager

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 Genesis.

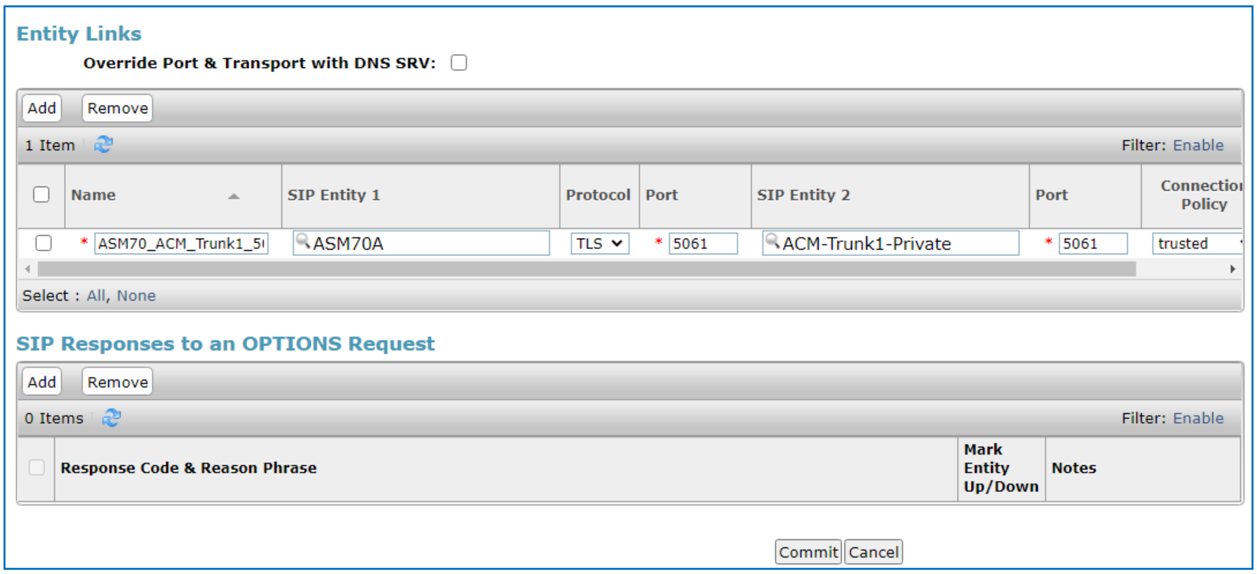
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

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



Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. 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 “ASM70”
- **Protocol:** The signaling group transport method from **Section 5.4**.
- **Port:** The signaling group far-end listen port number from **Section 5.4**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group near-end listen port number from **Section 5.4**.
- **Connection Policy:** “trusted”



6.4. Administer Routing Policies

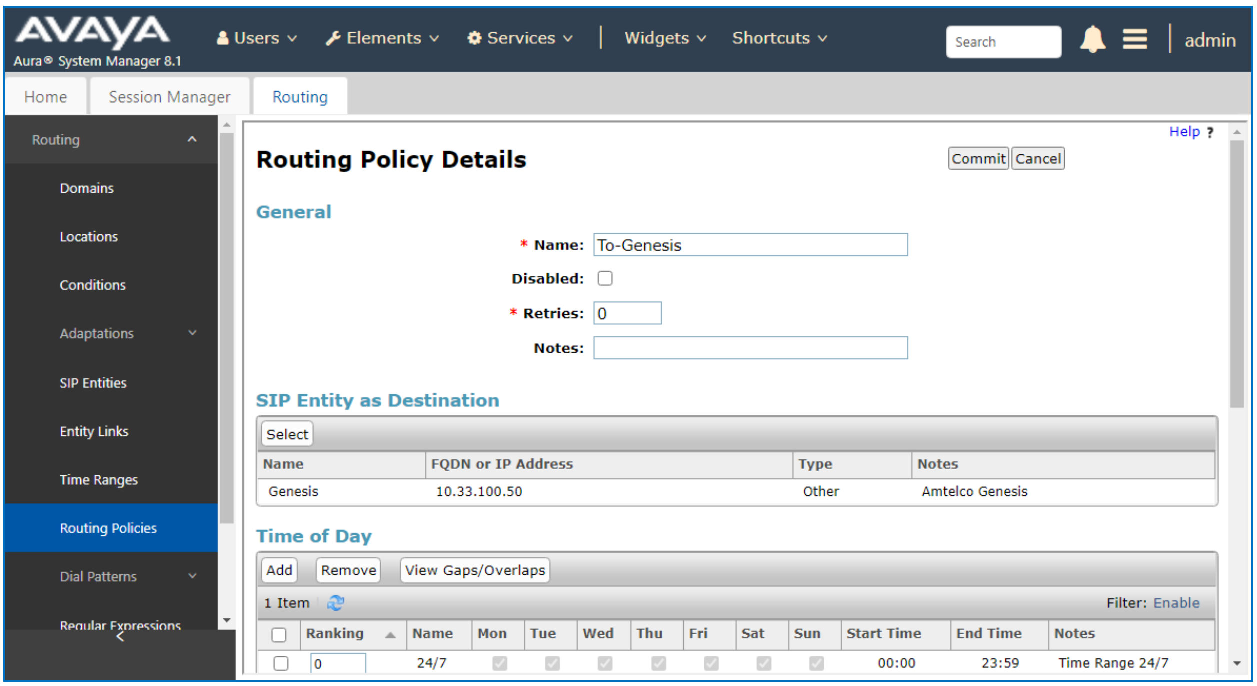
Add two new routing policies, one for Genesis and one for the new SIP trunks with Communication Manager.

6.4.1. Routing Policy for Genesis

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

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes** and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Genesis entity name from **Section 6.3.1**. The screen below shows the result of the selection.

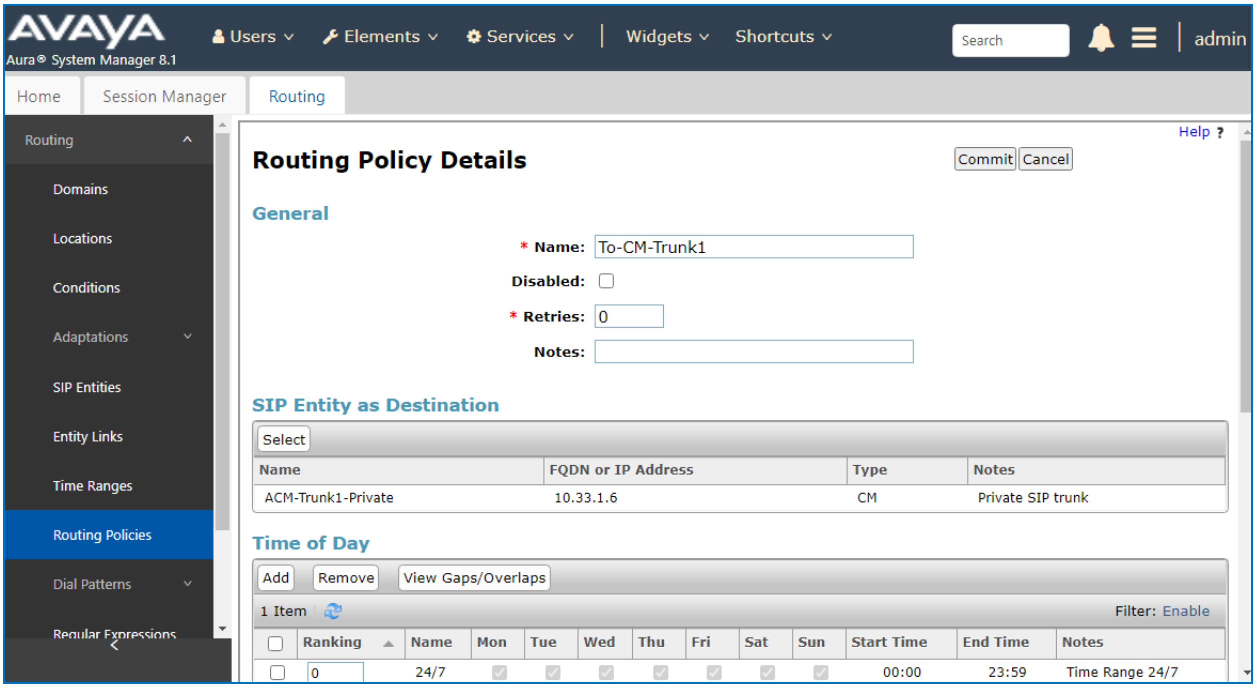


6.4.2. Routing Policy for Communication Manager

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**. Enter optional **Notes** and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.3.2**. The screen below shows the result of the selection.



6.5. Administer Dial Patterns

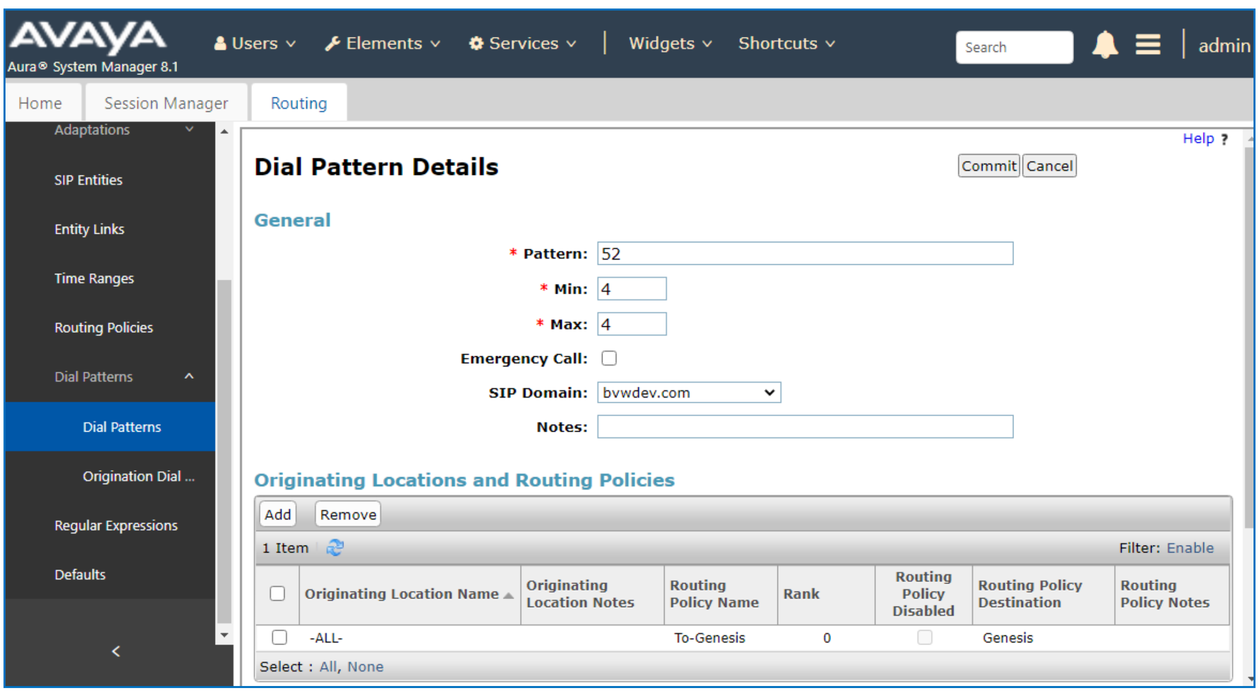
Add a new dial pattern for Genesis and update existing dial patterns for Communication Manager.

6.5.1. Dial Pattern for Genesis

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 Genesis. 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, in this case "52".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** Select the applicable domain, in this case "bvwdev.com".

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Genesis. For compliance testing, the entry allowed for call originations from Communication Manager endpoints in locations "All". The Genesis routing policy from **Section 6.4.1** was selected as shown below.

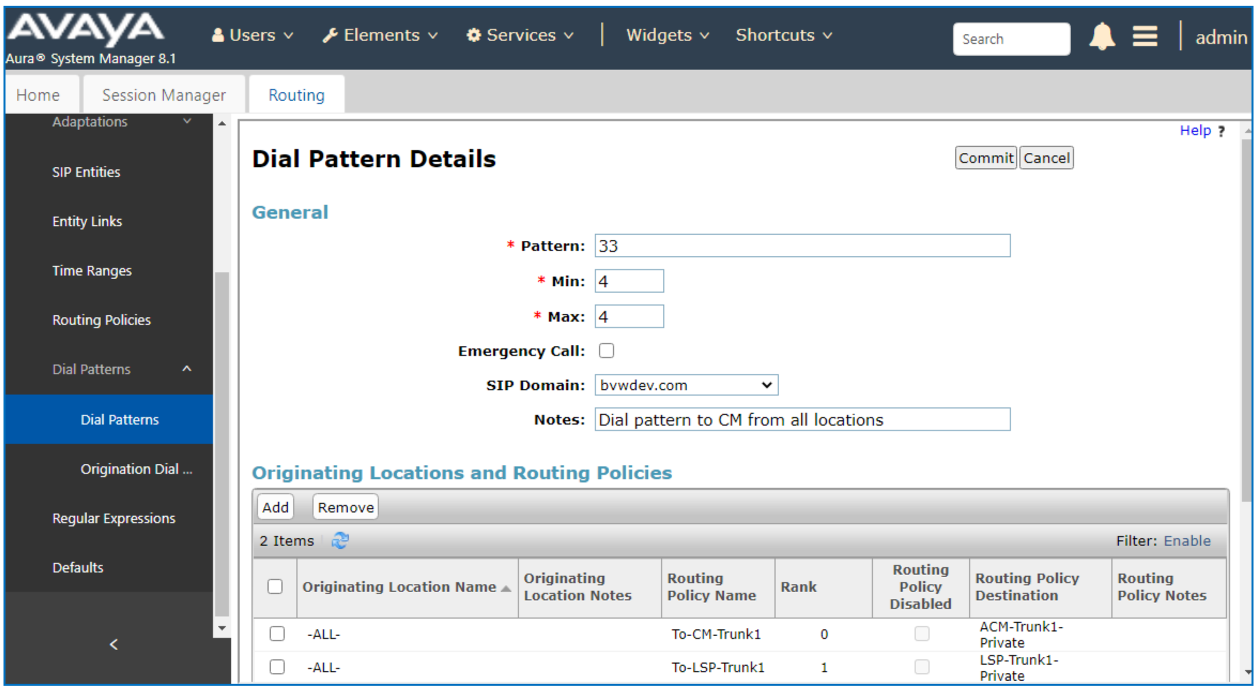


6.5.2. Dial Pattern for Communication Manager

Select **Routing → Dial Patterns** from the left pane and click on the first existing dial pattern for Communication Manager in the subsequent screen, in this case dial pattern "33". 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 Genesis. In the compliance testing, the new policy allowed for call origination from the Genesis location from **Section 6.2**, and the Communication Manager routing policy from **Section 6.4.2** was selected as shown below. Retain the default values in the remaining fields.

Follow the procedures in this section to make similar changes to the applicable Communication Manager dial pattern to reach the PSTN. In the compliance testing, operators on Genesis manually added the prefix "9" for outbound calls to the PSTN, and therefore the existing dial pattern for "9" was also changed (not shown below).



7. Configure Amtelco Genesis Intelligent Series

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

- Launch web interface
- Obtain application name
- Administer trunks
- Administer routes
- Administer agents
- Administer access control lists
- Launch Intelligent Series Supervisor
- Administer IS system
- Administer IS client
- Administer IS agent
- Restart IS service
- Launch Intelligent Series Soft Agent
- Administer setup

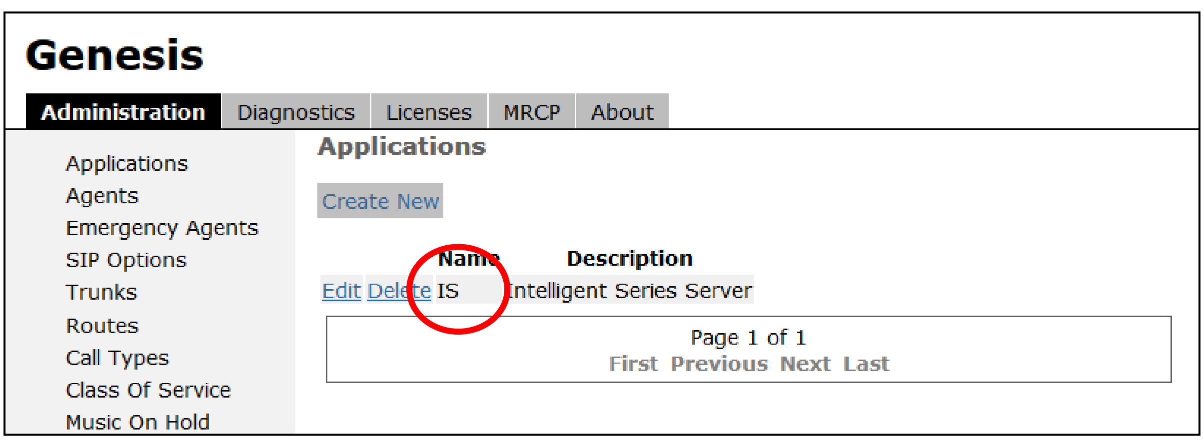
The configuration of Genesis is typically performed by Amtelco technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Web Interface

From a PC, launch an Internet browser window and access the Genesis web-based interface by using the URL "http://<ip-address:5080>/Admin/Application/Index", where "ip-address" is the IP address of the Genesis Telephony Server.

7.2. Obtain Application Name

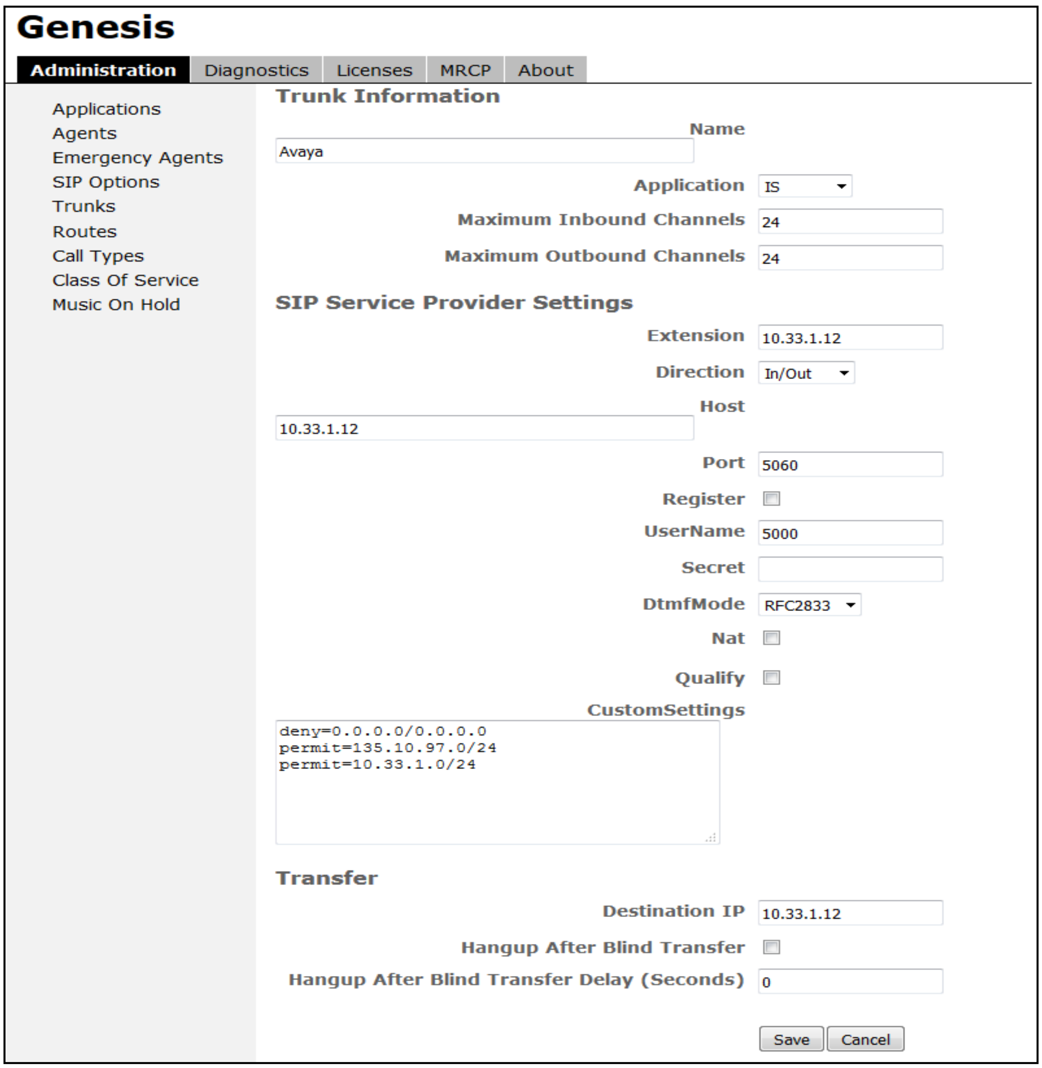
The **Applications** screen below is displayed in the right pane. Make a note of the application **Name**, in this case "IS", which is created as part of installation. The name will be used in later sections.



7.3. Administer Trunks

Select **Trunks** in the left pane, followed by **Create New SIP Trunk** (not shown) in the updated right pane, to display the **Trunk Information** screen below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **Application:** Select the application name from **Section 7.2**.
- **Maximum Channels:** Enter desired number of trunk members.
- **Extension:** The routing extension digits from **Section 3** for calls from PSTN.
- **Host:** IP address of the Session Manager signaling interface.
- **Port:** The Genesis SIP entity port number from **Section 6.3.1**.
- **UserName:** The routing extension digits from **Section 3** for calls from PSTN.
- **Destination IP:** IP address of the Session Manager signaling interface.

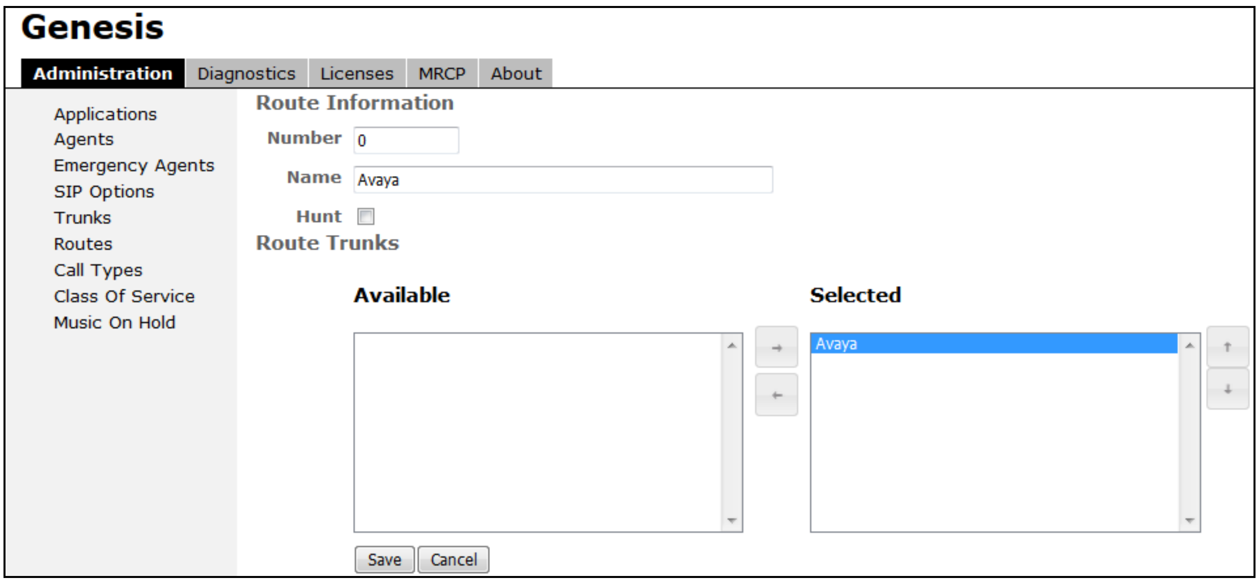


7.4. Administer Routes

Select **Routes** in the left pane, followed by **Create New Route** (not shown) in the updated right pane, to display the **Route Information** screen below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Number:** An available route number.
- **Name:** A descriptive name.

In the **Route Trunks** sub-section, select the trunk from **Section 7.3** under **Available** and move to **Selected**, as shown below.

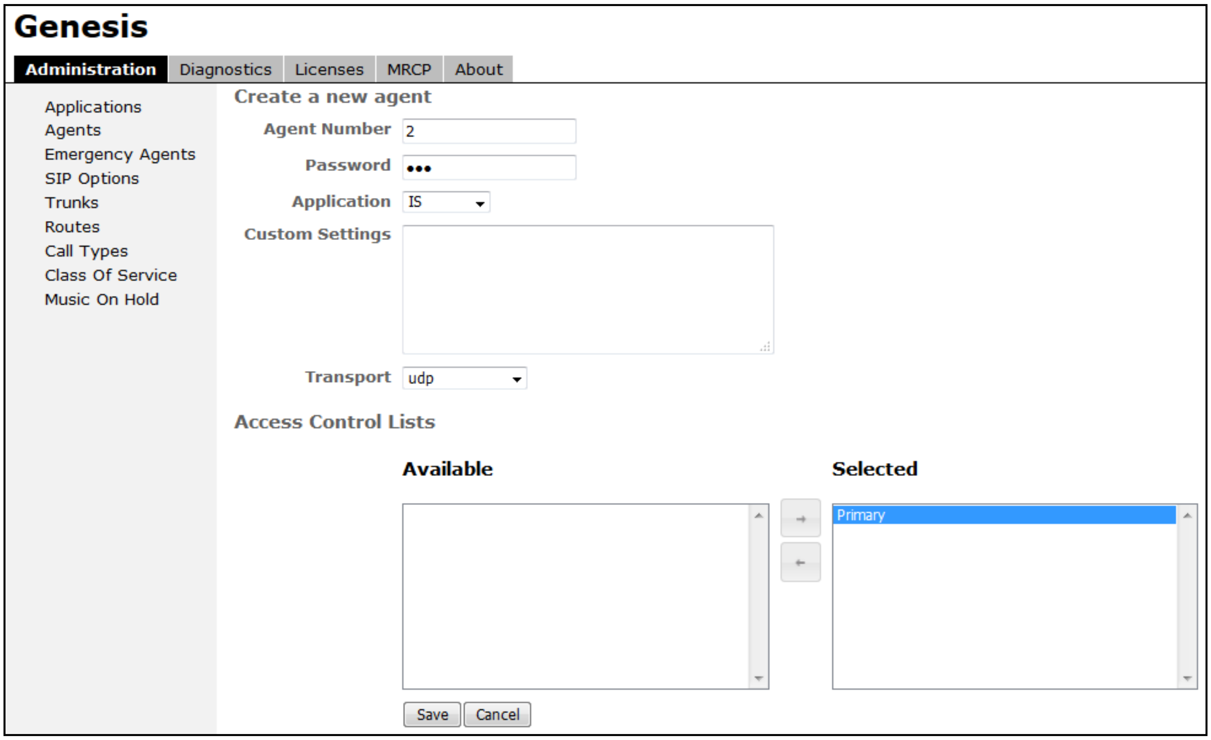


7.5. Administer Agents

Select **Agents** in the left pane, to display the **Agents** screen. One agent is needed for each operator user, and by default the first agent is automatically created, as shown below. To create additional agents, select **Create New**.

The **Create a new agent** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

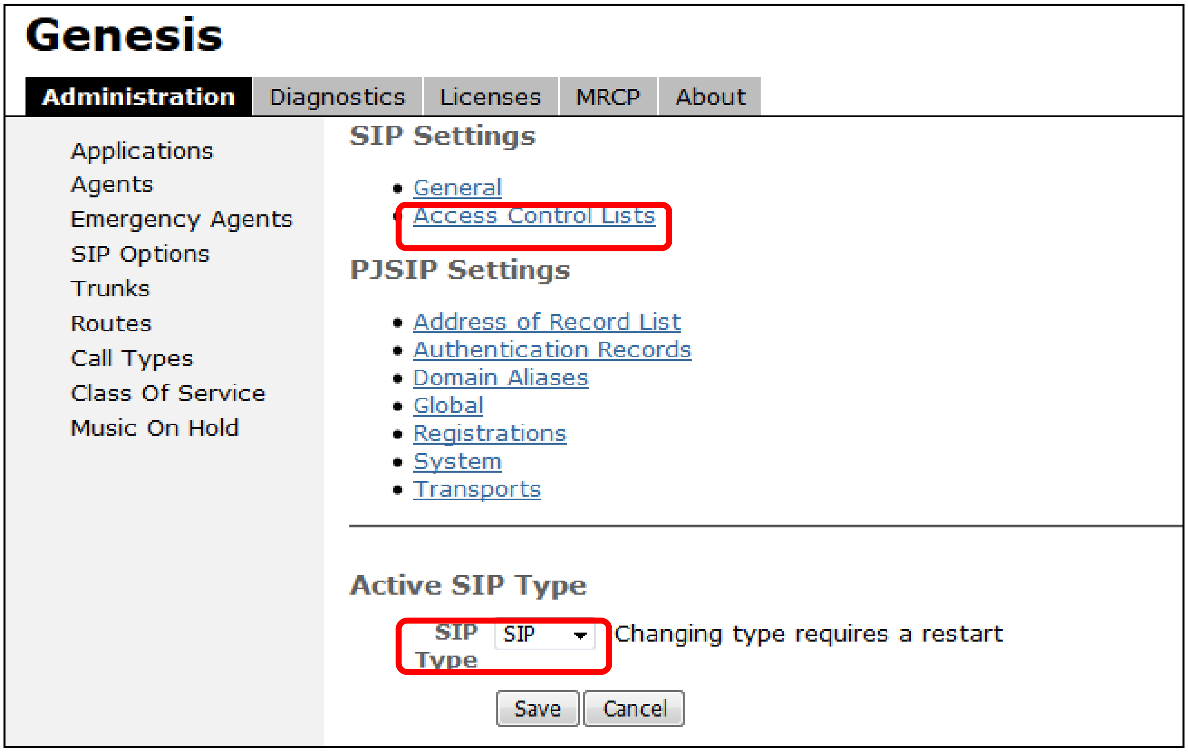
- **Agent Number:** An available agent number.
- **Password:** A desired password.
- **Application:** Select the application name from **Section 7.2**.
- **Transport:** "udp"



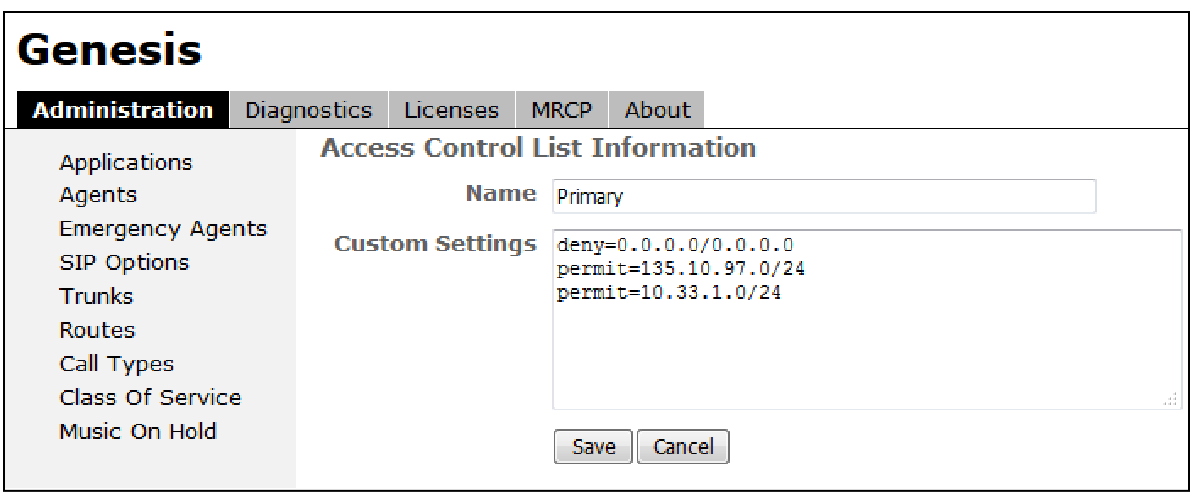
7.6. Administer Access Control Lists

Select **SIP Options** in the left pane, followed by **Access Control Lists** in the updated right pane, to display the screen below. Make certain **SIP Type** is set to "SIP", as shown below.

Select **Access Control Lists**.



The **Access Control List Information** screen is displayed. Enter a desired **Name** and create a **permit** entry for each network subnet from **Section 3**, and create a generic **deny** entry as shown below.



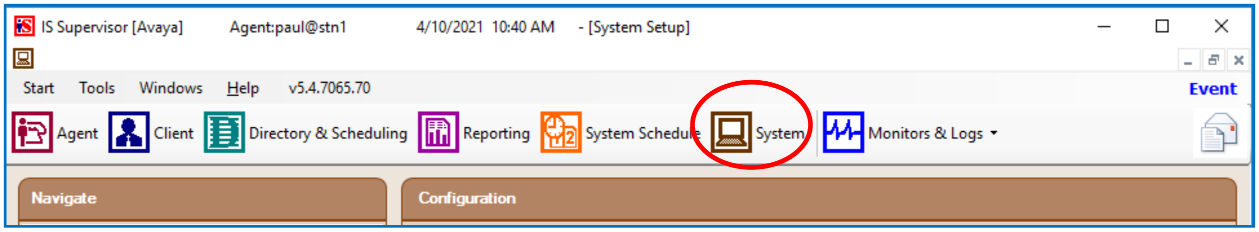
7.7. Launch Intelligent Series Supervisor

From the supervisor PC, double-click on the Intelligent Series Supervisor shortcut icon shown below, which was created as part of Intelligent Series Supervisor installation.

The **Supervisor Login** screen is displayed. Log in using the appropriate credentials.

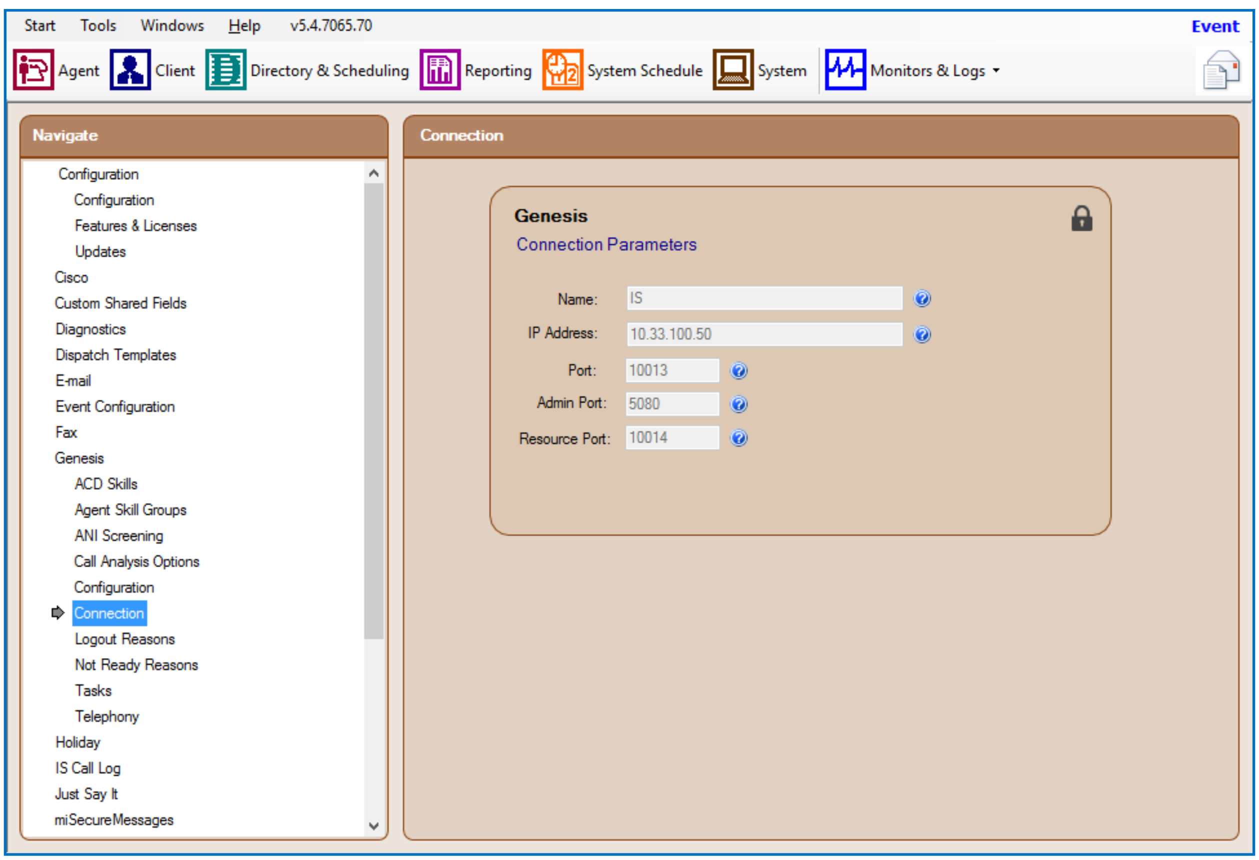
7.8. Administer IS System

The **IS Supervisor** screen is displayed. Select **System** from the top of the screen.



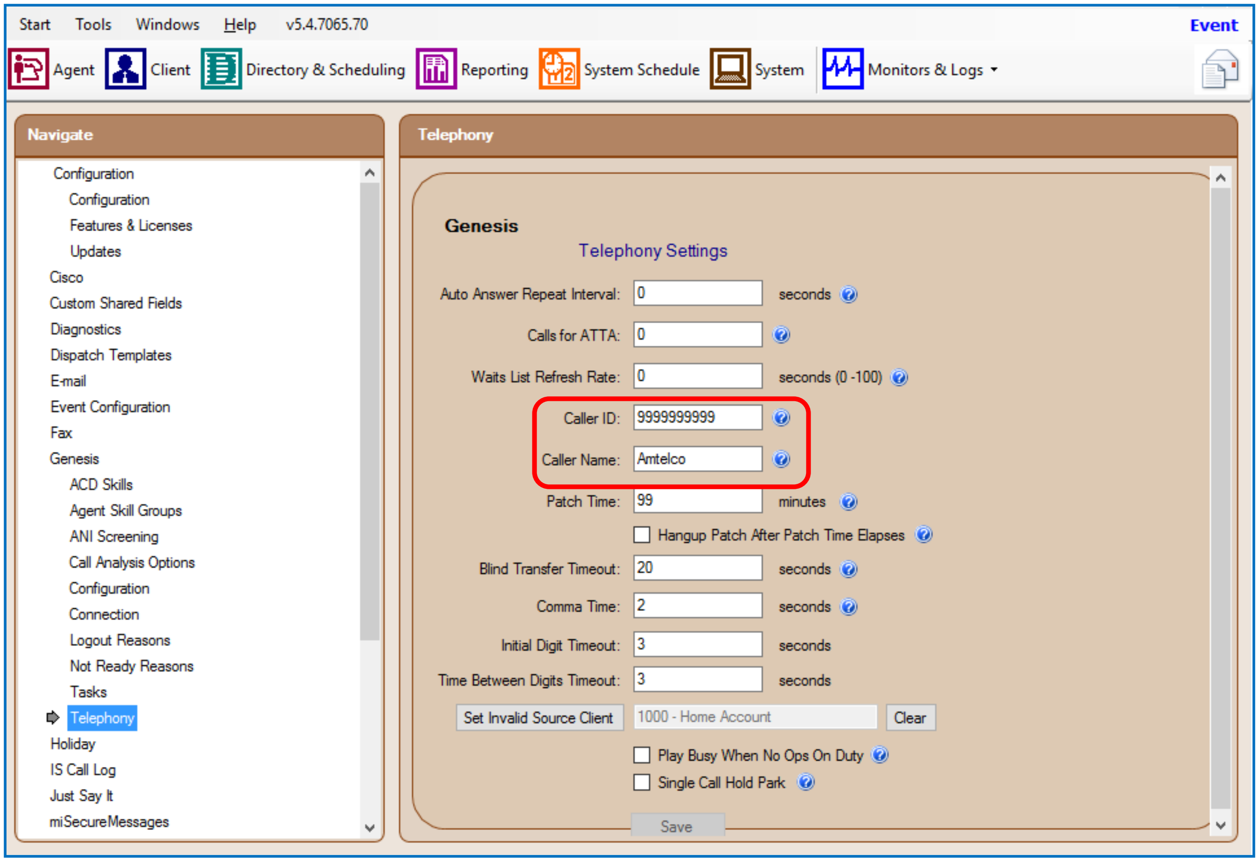
The screen is updated with **System Setup** displayed in the lower pane. Select **Genesis → Connection** from the left pane, to display the **Connection** screen in the right pane. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** Enter the application name from **Section 7.2**.
- **IP Address:** IP address of the Genesis Telephony Server.
- **Port:** "10013"
- **Admin Port:** "5080"
- **Resource Port:** "10014"



Select **Genesis → Telephony** from the left pane, to display the **Telephony** screen in the right pane. Enter the following values for the specified fields and retain the default values for the remaining fields.

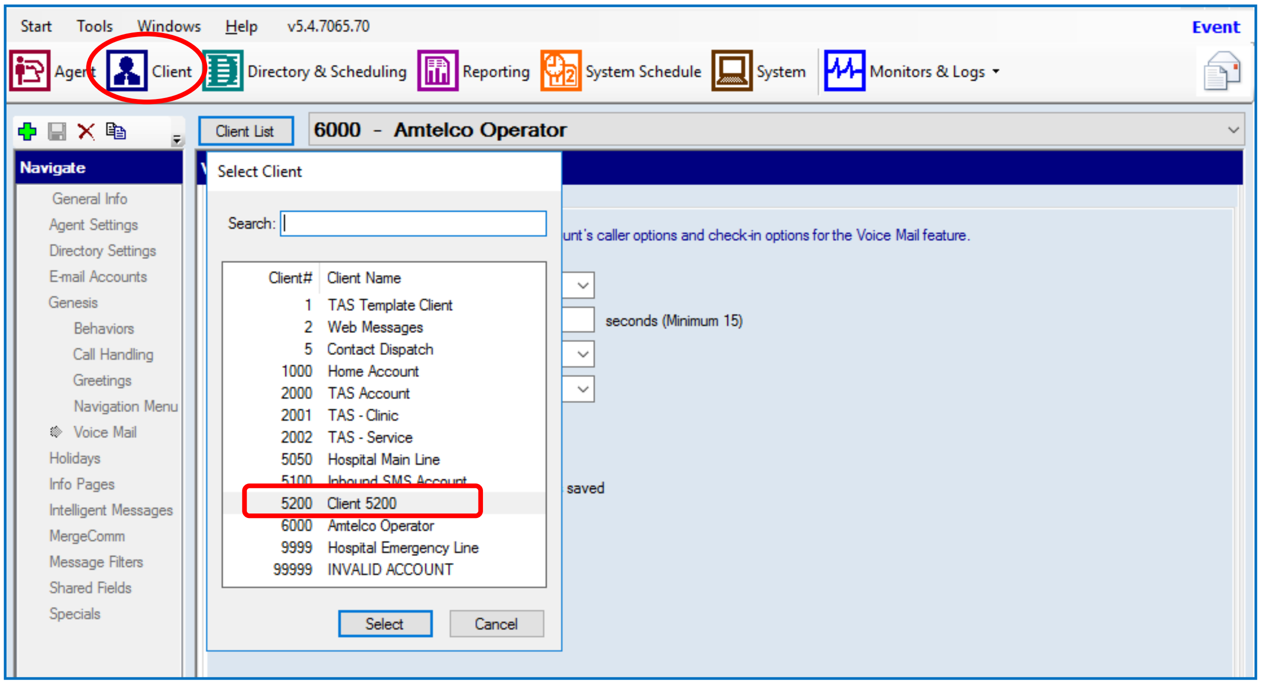
- **Caller ID:** The desired calling party extension to use for outbound calls.
- **Caller Name:** The desired calling party name to use for outbound calls.



7.9. Administer IS Client

Select **Client** from the top of the screen. The screen is updated with **Client Setup** displayed in the lower pane.

Follow reference [3] to create desired client entries to associate with called numbers for the customer network. In the compliance testing, calls from the PSTN will be routed with digits 52000 to Genesis, and calls from internal users on Communication Manager will be routed with digits 52222 to Genesis. Therefore, two clients were created, as shown below.

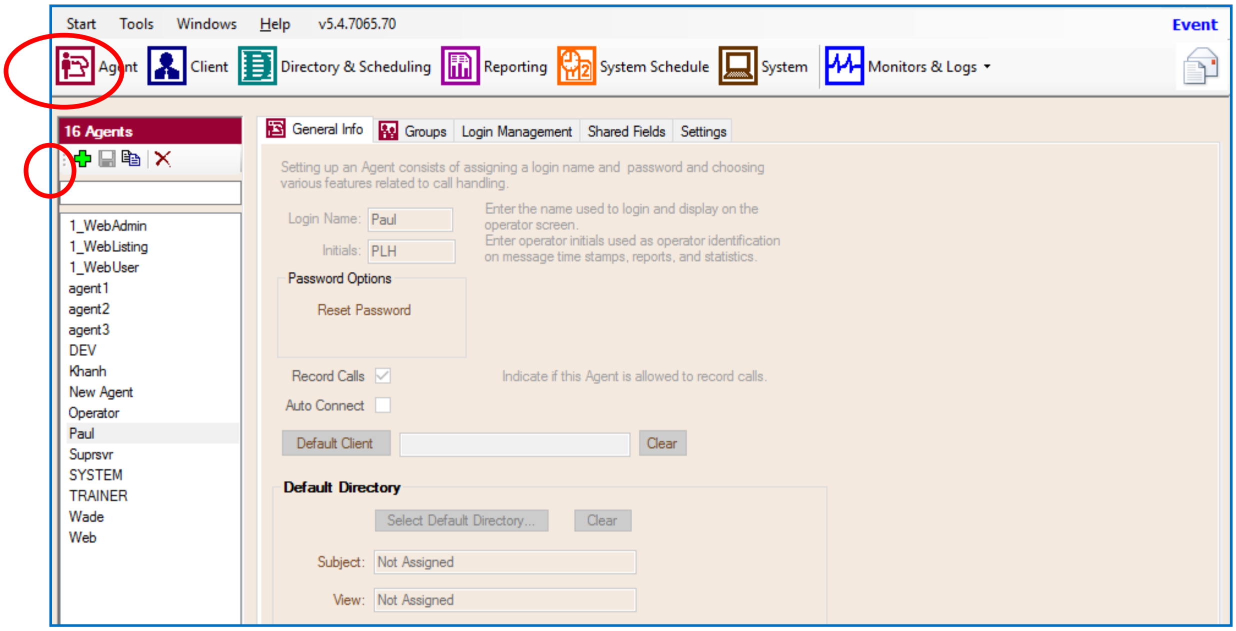


7.10. Administer IS Agent

Select **Agent** from the top of the screen. The screen is updated with **Agent Setup** displayed in the lower pane. Click on the **New Agent** icon in the left pane to create a new agent entry.

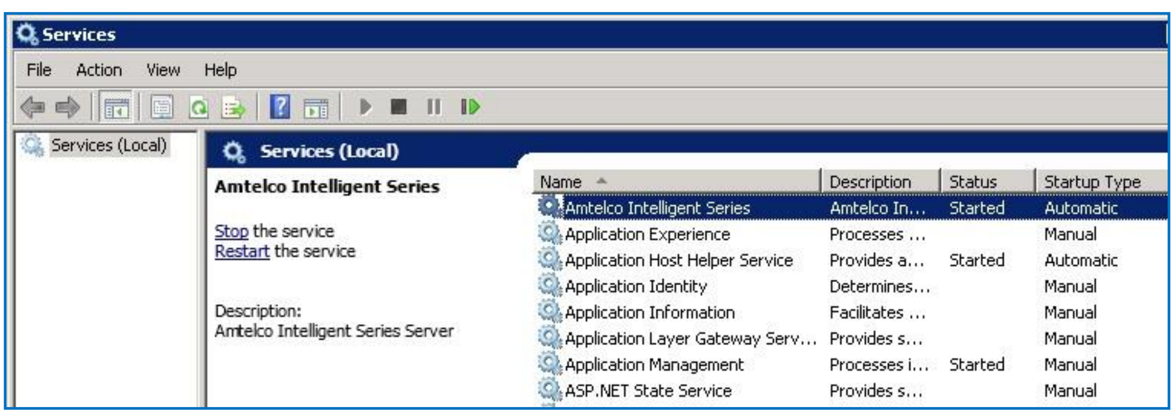
The **General Info** tab is displayed. For **Login Name**, **Password**, and **Confirm**, enter desired values. Retain the default values in the remaining fields.

One agent is needed for each operator user, and two agents were created for compliance testing.



7.11. Restart IS Service

From the Intelligent Series Server, select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Locate and restart the **Amtelco Intelligent Series** service, as shown below.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and Amtelco Web Agent.

8.1. Verify Avaya Aura® Communication Manager

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

```
status trunk 1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
0001/011 T00011   in-service/idle    no
0001/012 T00012   in-service/idle    no
0001/013 T00013   in-service/idle    no
0001/014 T00014   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 **Group State** is "in-service", as shown below.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

8.2. Verify Avaya Aura® Session Manager

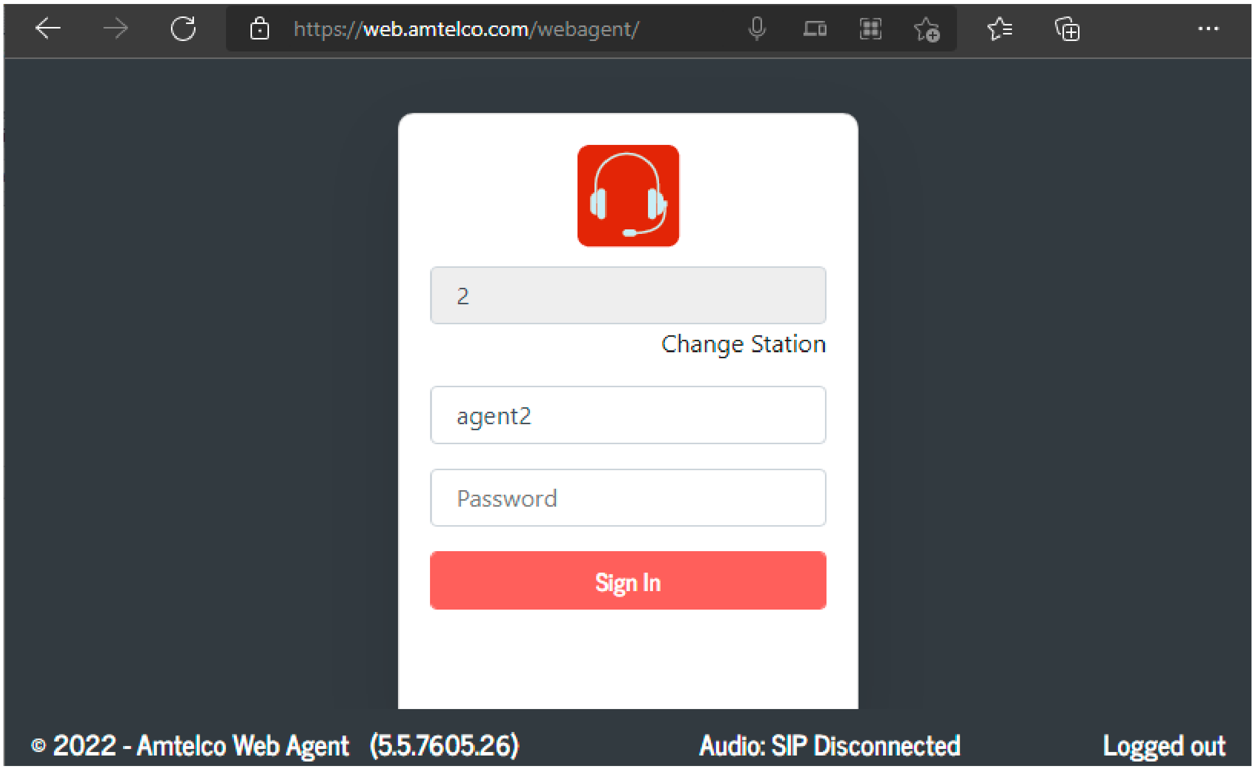
From the System Manager home page (not shown), select **Elements → Session Manager** to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click the Genesis entity name from **Section 6.3.1**.

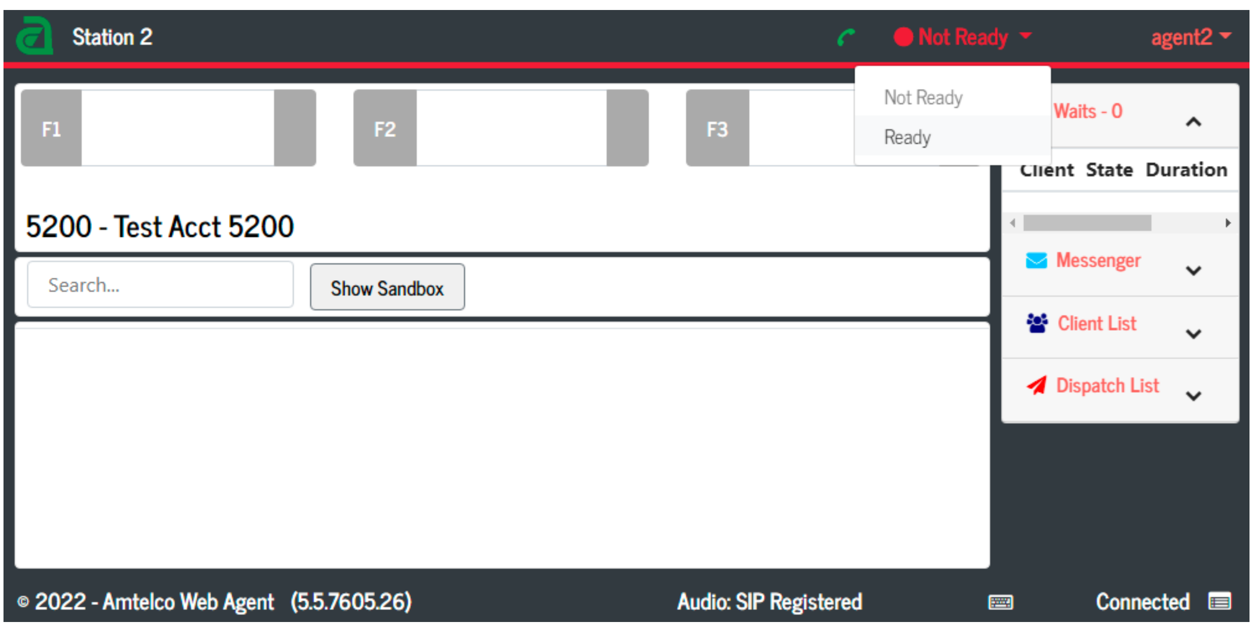
The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn Status** and **Link Status** are "UP", as shown below.

8.3. Verify Amtelco Web Agent

From the operator PC, launch the web agent page by entering the URL link https://web.amtelco.com/webagent/ in the internet browser. Enter the username and password and click on the **Sign In** button.

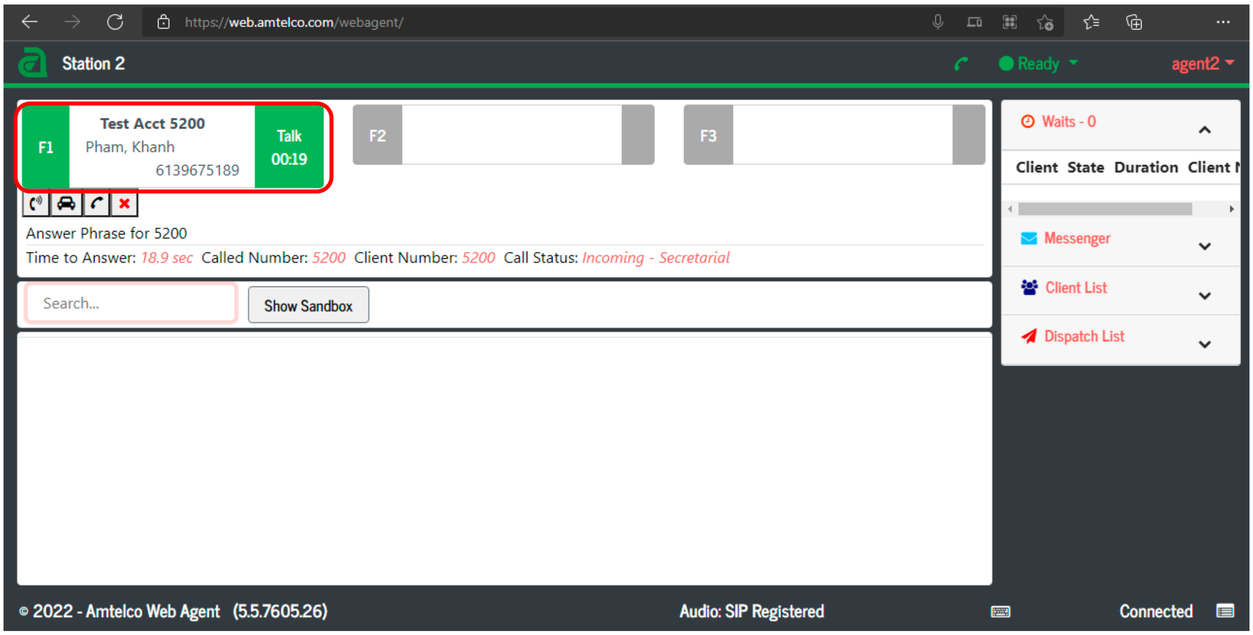


In the top right portion of the page, click on **Not Ready** and select **Ready**.



Make an incoming call from the PSTN to reach the Web Agent. Verify that the call is ringing at the available web agent, and that the web agent screen is updated to reflect a ringing call along with the calling party number and the called client name, as shown below. In this case, the calling party number is **6139675189**, and the called client name is **Test Acct 5200**. Press the **F1** key or click in the applicable call line area highlighted below to answer the call.

Verify that the web agent is connected to the PSTN with two-way talk paths. Also verify that the web agent is updated to reflect the **Talk** state, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Amtelco 1Call Web Agent to successfully interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication 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 (Release 8.1.3, Issue 5, February 2020)

[2] Administering Network Connectivity on Avaya Aura® Communication Manager (Release 8.1.3, Issue 4, August 2020), 555-233-504

[3] Avaya Aura® Communication Manager Feature Description and Implementation (Release 8.1.3, Issue 4, October 2020)

[4] Administering Avaya Aura® Session Manager (Release 8.1.3, Issue 5, December 2020)

[5] Soft Agent User Reference Guide, May 2020, available at https://service.amtelco.com/doclib/library.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.