



Avaya Solution & Interoperability Test Lab

Application Notes for Amtelco Genesis Intelligent Series Version 5.3 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager Release 8.0 – Issue 1.0

Abstract

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

The Genesis solution consists of the Genesis Telephony Server, Intelligent Series Server, Intelligent Series Supervisor, and Intelligent Series Soft Agent. Operators have desktops running the Intelligent Series Soft Agent application, with dedicated audio connections via SIP with the Genesis Telephony Server.

In the compliance testing, calls from internal and external callers were routed over SIP trunks via Session Manager to Genesis 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.

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

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 Avaya systems and the Amtelco Genesis did not include use of any specific encryption features as requested by Amtelco.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

The serviceability testing focused on verifying the ability of Genesis 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. The following were observations on Genesis from the compliance testing.

- Genesis returned 404 Not Found for OPTIONS messages from Session Manager, and it was displayed on the SIP Entity connection status screen on Session Manager. This did not appear to have any other negative impact.
- The outgoing call from Amtelco Genesis does not display called name and number on the Soft Agent.

2.3. Support

Technical support on Amtelco Genesis can be obtained through the following:

- **Phone:** (800) 553-7679
- **Email:** service@amtelco.com
- **Web:** www.amtelco.com/Welcome.htm

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 Telephony Server as part of login. The Intelligent Series Supervisor was running on the supervisor desktop.

SIP trunks were used between the Genesis Telephony Server and Session Manager. A 4digit Uniform Dial Plan was used to facilitate dialing with Genesis. Calls to extensions 51xx were routed over the SIP trunks to Genesis. In particular, internal users on Communication Manager will dial 5100 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.

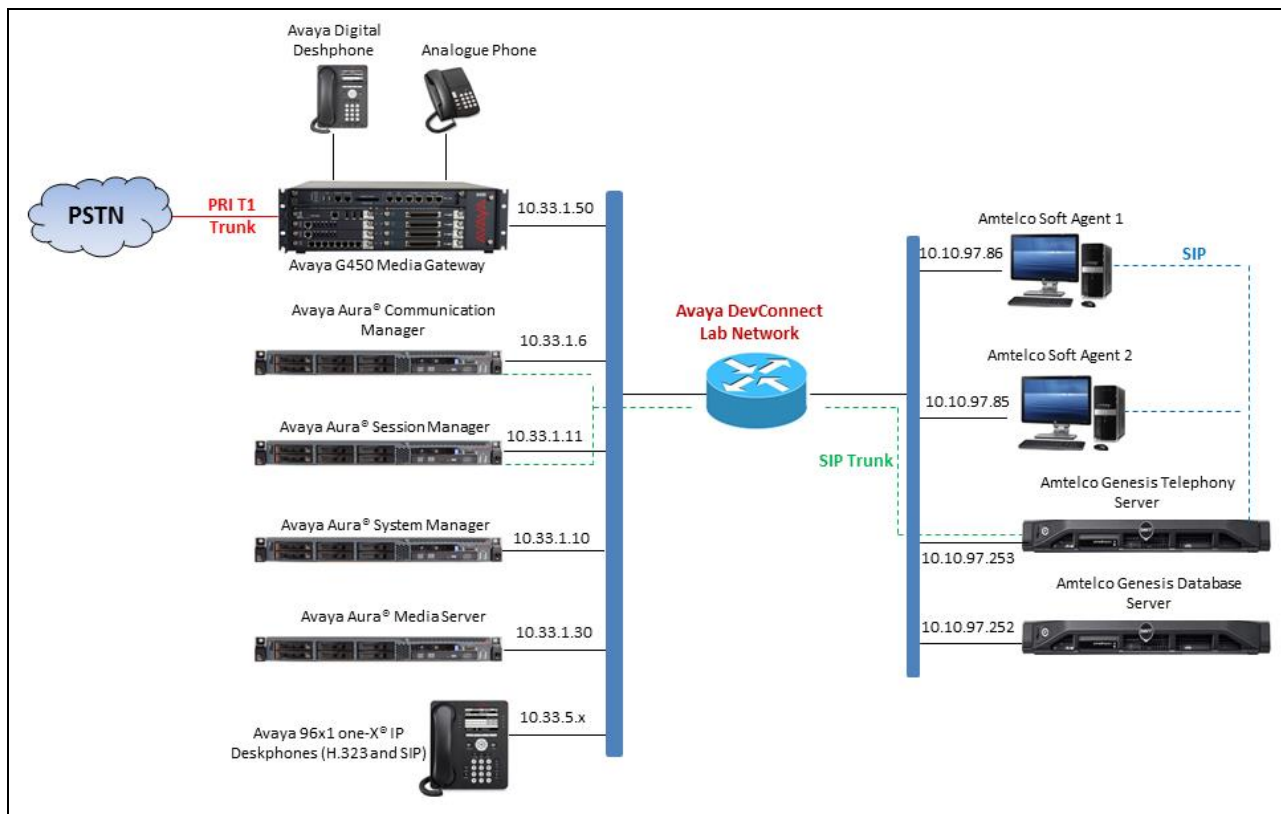


Figure 1: Compliance Testing Configuration

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 in Virtual Environment	8.0.1.0.0-FP1 (8.0.1.0.0.822.25031)
Avaya G450 Media Gateway	40.20.0
Avaya Aura® Media Server in Virtual Environment	8.0.0.173
Avaya Aura® Session Manager in Virtual Environment	8.0.1.0 (8.0.1.0.801007)
Avaya Aura® System Manager in Virtual Environment	8.0.1.0 (8.0.1.0.038826)
Avaya 9611GIP Deskphones (H.323)	6.7104
Avaya 9621G IP Deskphone (SIP)	7.1.4.0.11
Amtelco Genesis Telephony Server on Ubuntu <ul style="list-style-type: none">• Asterisk	Linux ubuntu 4.4.0 Asterisk PBX Version 13.20.0
Amtelco Server Intelligent Series	5.3.6774.20655
Amtelco Intelligent Series Soft Agent on Microsoft Windows 10 Pro	5.3.6774.24

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

In the 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 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	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
                                                UI Treatment: shared
                                                Maximum Size of UI Contents: 128
                                                Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

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

  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	

5.5. Administer SIP Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number from **Section 5.3**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.4**.
- **Number of Members:** The desired number of members, in this case “14”.

```
change 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
```

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:						
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 51xx 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 51xx, 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	
51	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 51xx. In the example shown below, calls with digits 51xx will be routed as an AAR call using route pattern “51” from **Section 5.8**.

change aar analysis 0						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
51		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 step of **administration of Session Manager Routing Policies** 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.

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)

Step 4: Create "Adaptations"

KP; Reviewed:
SPOC 2/19/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

15 of 45
Amtelco-SM80

AVAYA

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

Search

Help ?

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Location Details

Commit

Cancel

General

* Name:

Genesis

Notes:

Genesis Location

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

* Latency before Overall Alarm Trigger:

5

Minutes

* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

1 Item

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.97.251	

Select : All, None

Commit

Cancel

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.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing

SIP Entity Details Commit Cancel

General

* Name: Genesis

* FQDN or IP Address: 10.10.97.251

Type: Other ▾

Notes: Amtelco Genesis software

Adaptation: ▾

Location: Genesis ▾

Time Zone: America/New_York ▾

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: none ▾

CommProfile Type Preference: ▾

Loop Detection

Loop Detection Mode: On ▾

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▾

CRLF Keep Alive Monitoring: Use Session Manager Configuration ▾

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, and the compliance testing used the UDP protocol.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* ASM70A_SR140_5060_	ASM70A ▼	UDP ▼	* 5060	Genesis ▼	* 5060	trusted ▼	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

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.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search [] admin

Home Routing

SIP Entity Details [Commit] [Cancel] Help ?

General

* Name: ACM-Trunk1-Private

* FQDN or IP Address: 10.33.1.6

Type: CM ▾

Notes: Private SIP trunk for SIP phone

Adaptation: ▾

Location: CM71 ▾

Time Zone: America/Toronto ▾

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name: []

Securable: ☐

Call Detail Recording: both ▾

Loop Detection

Loop Detection Mode: On ▾

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▾

CRLF Keep Alive Monitoring: Use Session Manager Configuration ▾

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association: ▾

Backup Session Manager Bandwidth Association: ▾

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”

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* ASM70_ACM_Trunk1_5	ASM70A	TLS	* 5061	ACM-Trunk1-Private	* 5061	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

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.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Genesis	10.10.97.251	Other	Amtelco Genesis software

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

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.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM-Trunk1-Private	10.33.1.6	CM	Private SIP trunk for SIP phone

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

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 “51”.
- **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 “bvwddev.com”.

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

The screenshot displays the Avaya Aura System Manager 8.0 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Pattern:** 51
- Min:** 4
- Max:** 4
- Emergency Call:** ☐
- SIP Domain:** bvwddev.com
- Notes:** (empty text box)

The 'Originating Locations and Routing Policies' section features an 'Add' button and a table with one item. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-	To-Genesis		0	<input type="checkbox"/>	Genesis	Routing to Genesis fax software

At the bottom of the table, there is a 'Select' dropdown menu with options 'All' and 'None'.

6.5.2. Dial Pattern for Communication Manager

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 Communication Manager. 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 “33”.
- **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 “bvwddev.com”.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Manager. In the compliance testing, the entry allowed for call originations from Communication Manager endpoint in locations “All”. The Communication Manager routing policy from **Section 6.4.2** was selected as shown below.

AVAYA
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ≡ admin

Home Routing

Locations
Conditions
Adaptations ▾
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns ▾
Regular Expressions
Defaults

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 33

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: bvwddev.com ▾

Notes: Dial pattern to CM71 from all locations

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	To-CM-Trunk1		0	<input type="checkbox"/>	ACM-Trunk1-Private	

Select : All, None

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.

The screenshot shows the Genesis web interface. The top navigation bar includes 'Administration' (selected), 'Diagnostics', 'Licenses', 'MRCP', and 'About'. The left sidebar lists various configuration options: Applications, Agents, Emergency Agents, SIP Options, Trunks, Routes, Call Types, Class Of Service, and Music On Hold. The main content area is titled 'Applications' and features a 'Create New' button. Below this is a table with two columns: 'Name' and 'Description'. The 'Name' column header is circled in red. The table contains one entry: 'IS' under the 'Name' column and 'Intelligent Series Server' under the 'Description' column. At the bottom of the table, there are links for 'Edit' and 'Delete'. The page footer indicates 'Page 1 of 1' and provides navigation links: 'First', 'Previous', 'Next', and 'Last'.

Name	Description
IS	Intelligent Series Server

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.

The screenshot shows the 'Genesis' application window with the 'Administration' tab selected. The left sidebar lists various configuration areas, with 'Trunks' highlighted. The main panel is titled 'Trunk Information' and contains several sections:

- Trunk Information:** Includes fields for 'Name' (Avaya), 'Application' (IS), 'Maximum Inbound Channels' (24), and 'Maximum Outbound Channels' (24).
- SIP Service Provider Settings:** Includes fields for 'Extension' (10.33.1.12), 'Direction' (In/Out), 'Host' (10.33.1.12), 'Port' (5060), 'Register' (checkbox), 'UserName' (5000), 'Secret' (text field), 'DtmfMode' (RFC2833), 'Nat' (checkbox), and 'Qualify' (checkbox).
- CustomSettings:** A text area containing the following text:

```
deny=0.0.0.0/0.0.0.0
permit=135.10.97.0/24
permit=10.33.1.0/24
```
- Transfer:** Includes fields for 'Destination IP' (10.33.1.12), 'Hangup After Blind Transfer' (checkbox), and 'Hangup After Blind Transfer Delay (Seconds)' (0).

At the bottom right, there are 'Save' and 'Cancel' buttons.

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.

Genesis

Administration | Diagnostics | Licenses | MRCP | About

Applications
Agents
Emergency Agents
SIP Options
Trunks
Routes
Call Types
Class Of Service
Music On Hold

Route Information

Number

Name

Hunt ☐

Route Trunks

Available

Selected

Avaya

Save Cancel

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 screenshot shows the 'Genesis' application interface. The 'Administration' tab is selected in the top navigation bar. On the left sidebar, 'Agents' is highlighted. The main content area is titled 'Agents' and contains a 'Create New' button and a 'Modify Range' button. Below these buttons is a table with the header 'Application Agent Number'. The table contains one row with the value '1' in the 'Agent Number' column. At the bottom of the table, there are links for 'Edit', 'Delete', and 'IS'. The page number 'Page 1 of 1' and navigation links 'First Previous Next Last' are also visible.

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”

The screenshot shows the 'Genesis' application interface with the 'Create a new agent' screen displayed. The 'Administration' tab is selected in the top navigation bar. On the left sidebar, 'Agents' is highlighted. The main content area is titled 'Create a new agent' and contains the following fields: 'Agent Number' (set to 2), 'Password' (masked with dots), 'Application' (set to IS), 'Custom Settings' (a large text area), and 'Transport' (set to udp). Below these fields is the 'Access Control Lists' section, which contains two lists: 'Available' and 'Selected'. The 'Selected' list contains the item 'Primary'. At the bottom of the screen, there are 'Save' and 'Cancel' buttons.

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 **Active SIP Type** is set to “SIP”, as shown below.

Select **Access Control Lists**.

Genesis

Administration | Diagnostics | Licenses | MRCP | About

Applications
Agents
Emergency Agents
SIP Options
Trunks
Routes
Call Types
Class Of Service
Music On Hold

SIP Settings

- General
- **Access Control Lists**

PJSIP Settings

- [Address of Record List](#)
- [Authentication Records](#)
- [Domain Aliases](#)
- [Global](#)
- [Registrations](#)
- [System](#)
- [Transports](#)

Active SIP Type

SIP SIP Changing type requires a restart

Save Cancel

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. On the completion, click **Save** to complete.

Genesis

Administration | Diagnostics | Licenses | MRCP | About

Applications
Agents
Emergency Agents
SIP Options
Trunks
Routes
Call Types
Class Of Service
Music On Hold

Access Control List Information

Name Primary

Custom Settings

```
deny=0.0.0.0/0.0.0.0
permit=135.10.97.0/24
permit=10.33.1.0/24
```

Save Cancel

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.

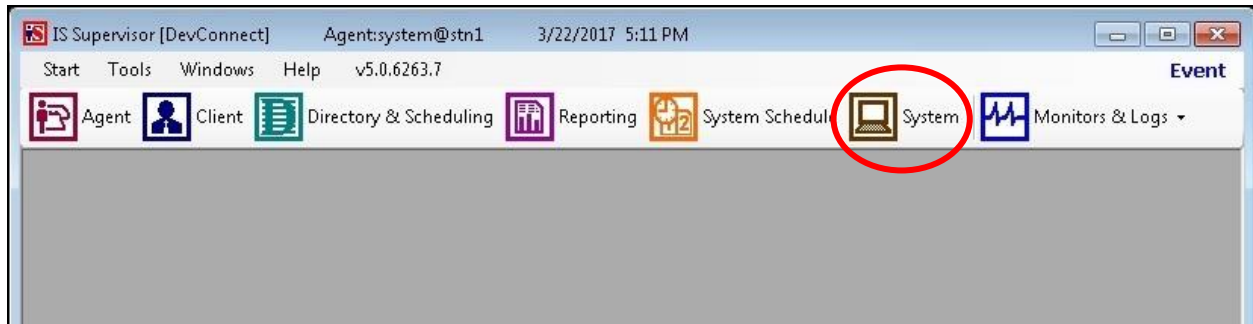


The **Supervisor Login** screen is displayed. Log in using the appropriate credentials.



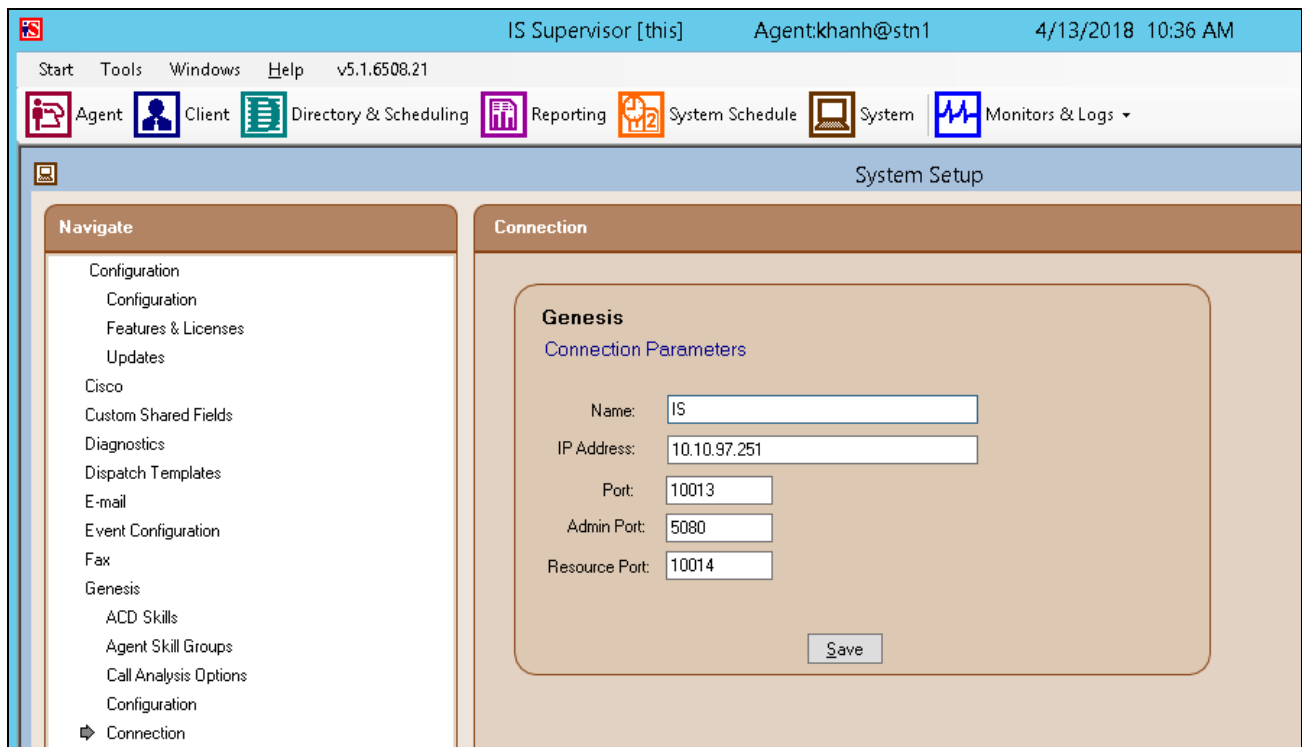
7.8. Administer IS System

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.

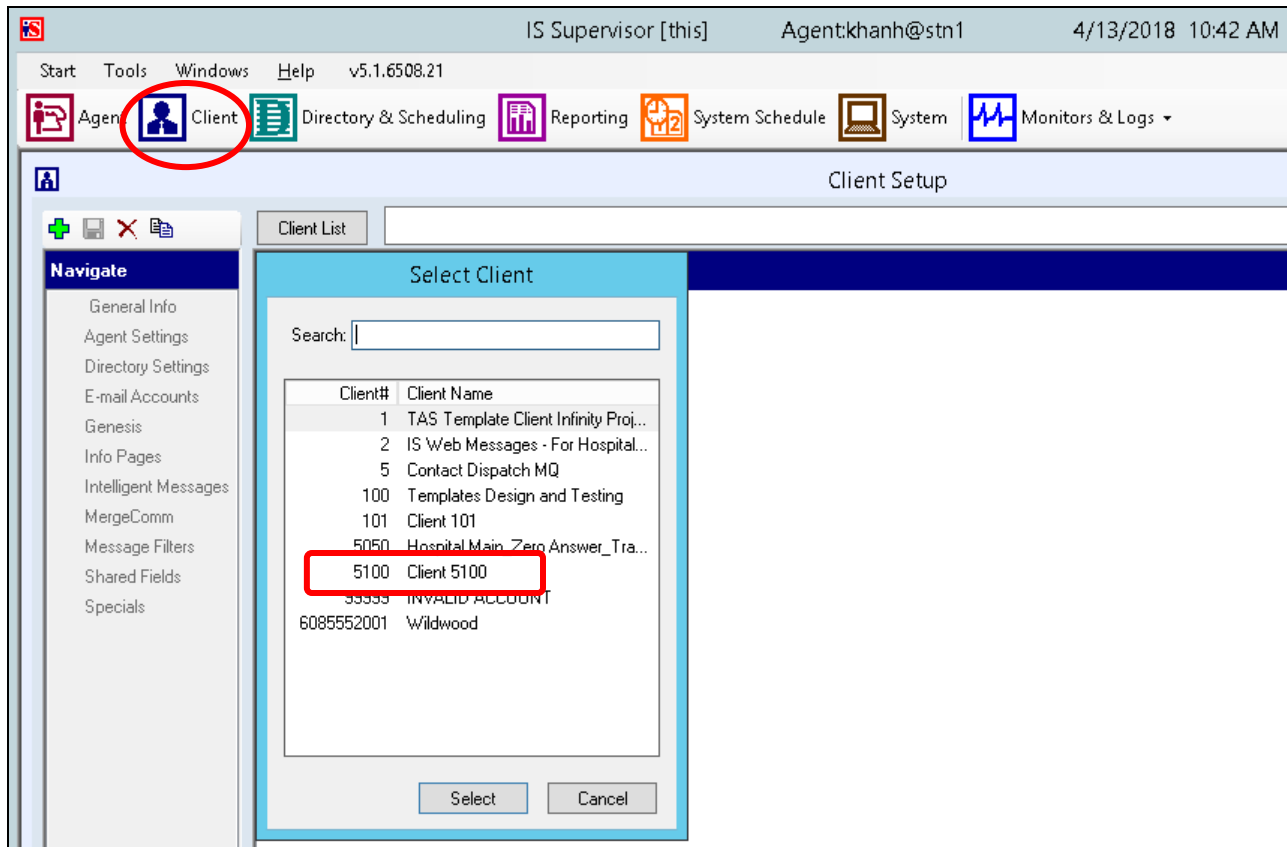
The screenshot shows the IS Supervisor application interface. The top status bar displays 'IS Supervisor [this]', 'Agent: kxanh@stn1', and the date/time '4/13/2018 10:39 AM'. Below this is a menu bar with 'Start', 'Tools', 'Windows', and 'Help'. A toolbar contains icons for 'Agent', 'Client', 'Directory & Scheduling', 'Reporting', 'System Schedule', 'System', and 'Monitors & Logs'. The main area is titled 'System Setup' and is split into two panes. The left pane, 'Navigate', lists various configuration categories, with 'Telephony' selected and highlighted in blue. The right pane, 'Telephony', displays the 'Genesis' configuration page. Under the 'Telephony Settings' heading, several fields are visible: 'Auto Answer Repeat Interval' (20 seconds), 'Calls for ATTA' (0), 'Waits List Refresh Rate' (0 seconds (0 -100)), 'Caller ID' (6088384194), 'Caller Name' (Amtelco), 'Patch Time' (15 seconds) with an unchecked checkbox for 'Hangup Patch After Patch Time Elapses', 'Blind Transfer Timeout' (20 seconds), and 'Comma Time' (2 seconds). A 'Save' button is located at the bottom of the settings area.

Field	Value	Unit/Notes
Auto Answer Repeat Interval	20	seconds
Calls for ATTA	0	
Waits List Refresh Rate	0	seconds (0 -100)
Caller ID	6088384194	
Caller Name	Amtelco	
Patch Time	15	seconds
Hangup Patch After Patch Time Elapses	<input type="checkbox"/>	
Blind Transfer Timeout	20	seconds
Comma Time	2	seconds

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

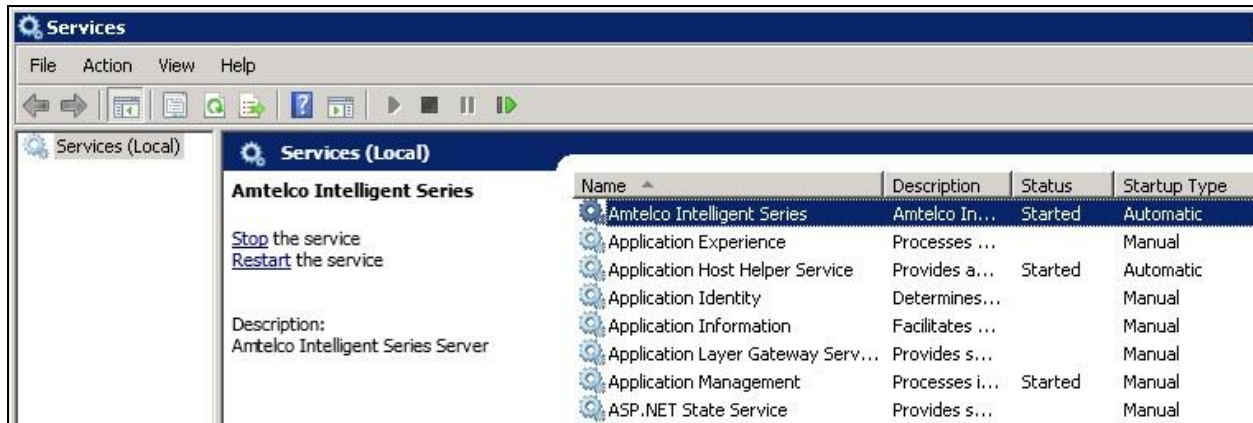
Select **Agent** from the top of the screen. The screen is updated with **Agent Setup** displayed in the lower pane. Click on the **New Agent** icon in the left pane to create a new agent entry.

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 in the 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.

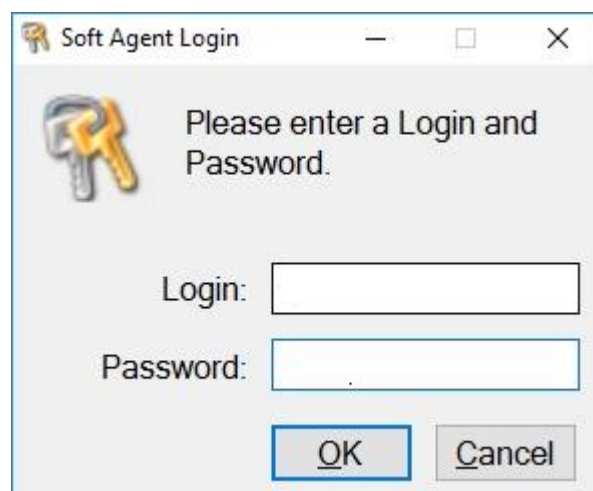


7.12. Launch Intelligent Series Soft Agent

From an operator PC, double-click on the **Soft Agent** shortcut icon shown below, which was created as part of the Intelligent Series Soft Agent installation.



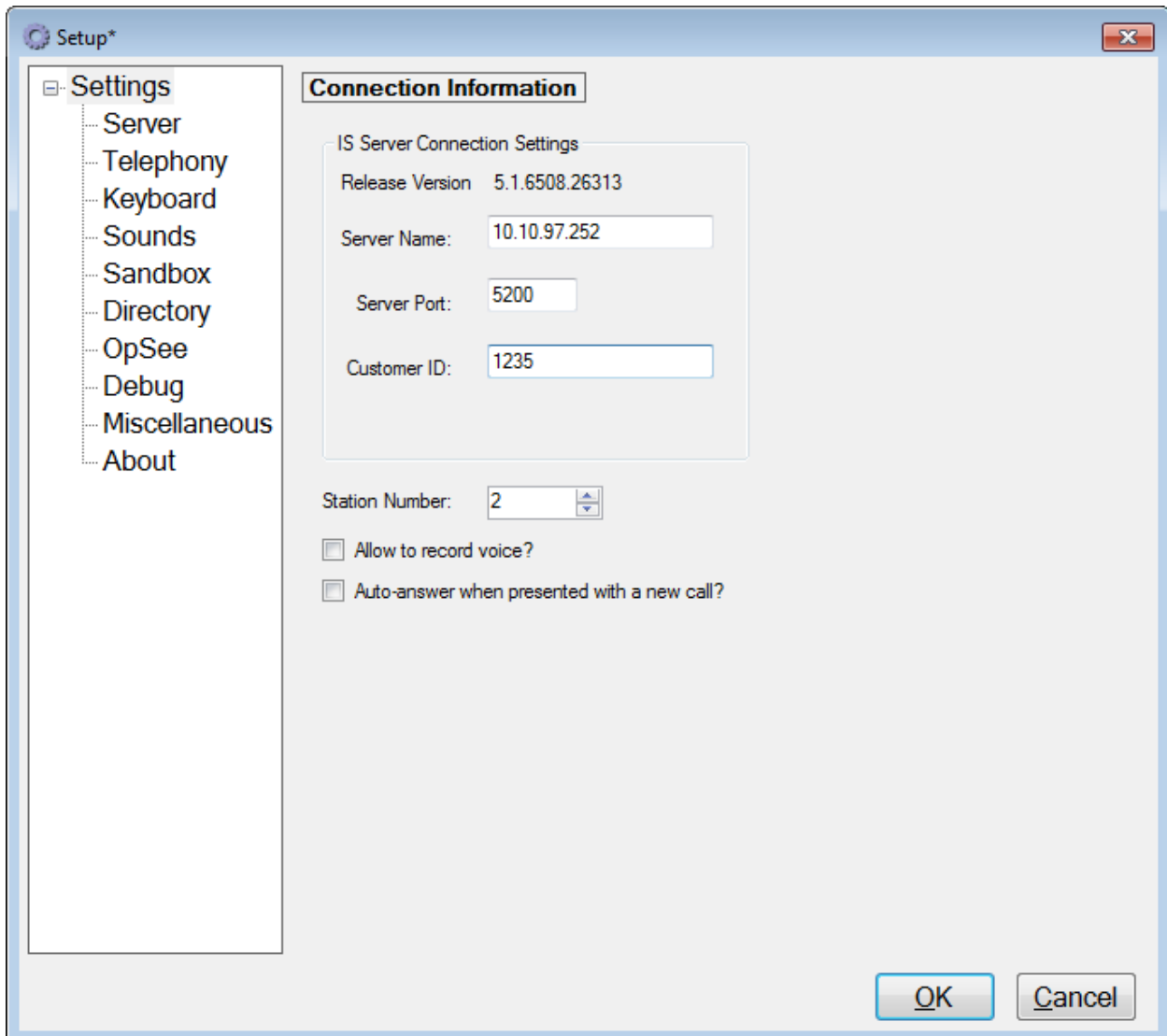
The **Soft Agent Login** screen is displayed. Press the **Ctrl** and **F12** keys together to enter setup.



7.13. Administer Setup

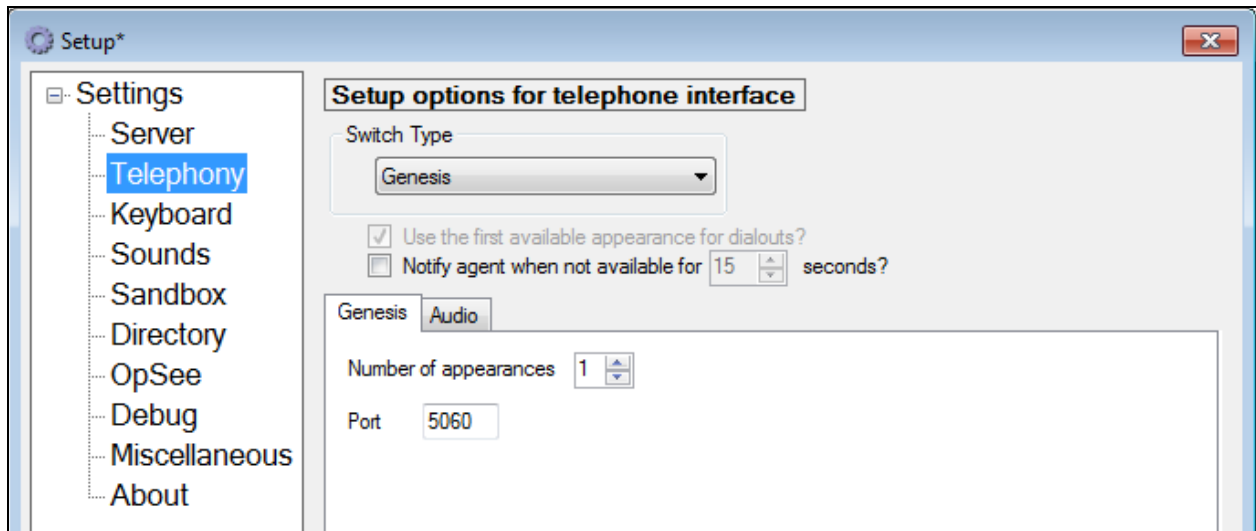
The **Setup** screen below is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Server Name:** IP address of the Intelligent Series Server.
- **Server Port:** “5200”
- **Customer ID:** The unique customer ID assigned by Amtelco, in this case “1235”.
- **Station Number:** An available station number, in this case “2”.

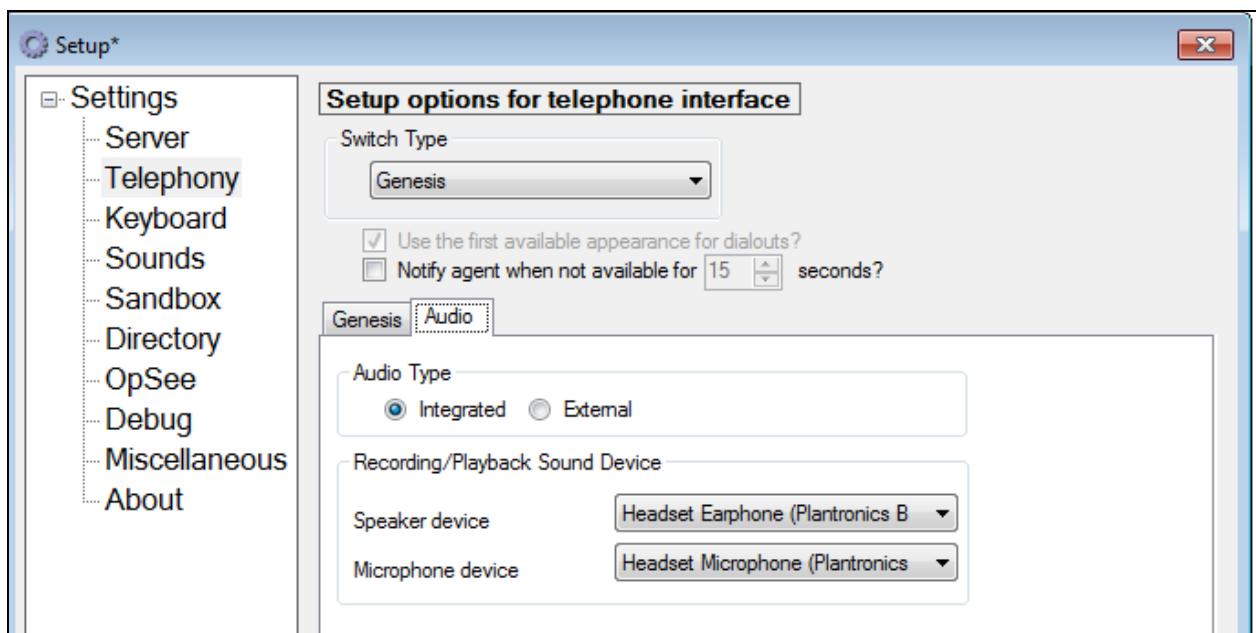


The screenshot shows a Windows-style dialog box titled "Setup*". On the left is a tree view with the following items: Settings (selected), Server, Telephony, Keyboard, Sounds, Sandbox, Directory, OpSee, Debug, Miscellaneous, and About. The main area of the dialog is titled "Connection Information". Inside this area, there is a sub-section titled "IS Server Connection Settings" which contains the following fields: "Release Version" (5.1.6508.26313), "Server Name:" (10.10.97.252), "Server Port:" (5200), and "Customer ID:" (1235). Below this sub-section, there is a "Station Number:" field with a spinner box set to 2. At the bottom of the "Connection Information" section, there are two unchecked checkboxes: "Allow to record voice?" and "Auto-answer when presented with a new call?". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Select **Settings** → **Telephony** from the left pane, to display the screen below. For **Switch Type**, select “Genesis”. Select the desired **Number of appearances**, and enter “5060” for **Port**.

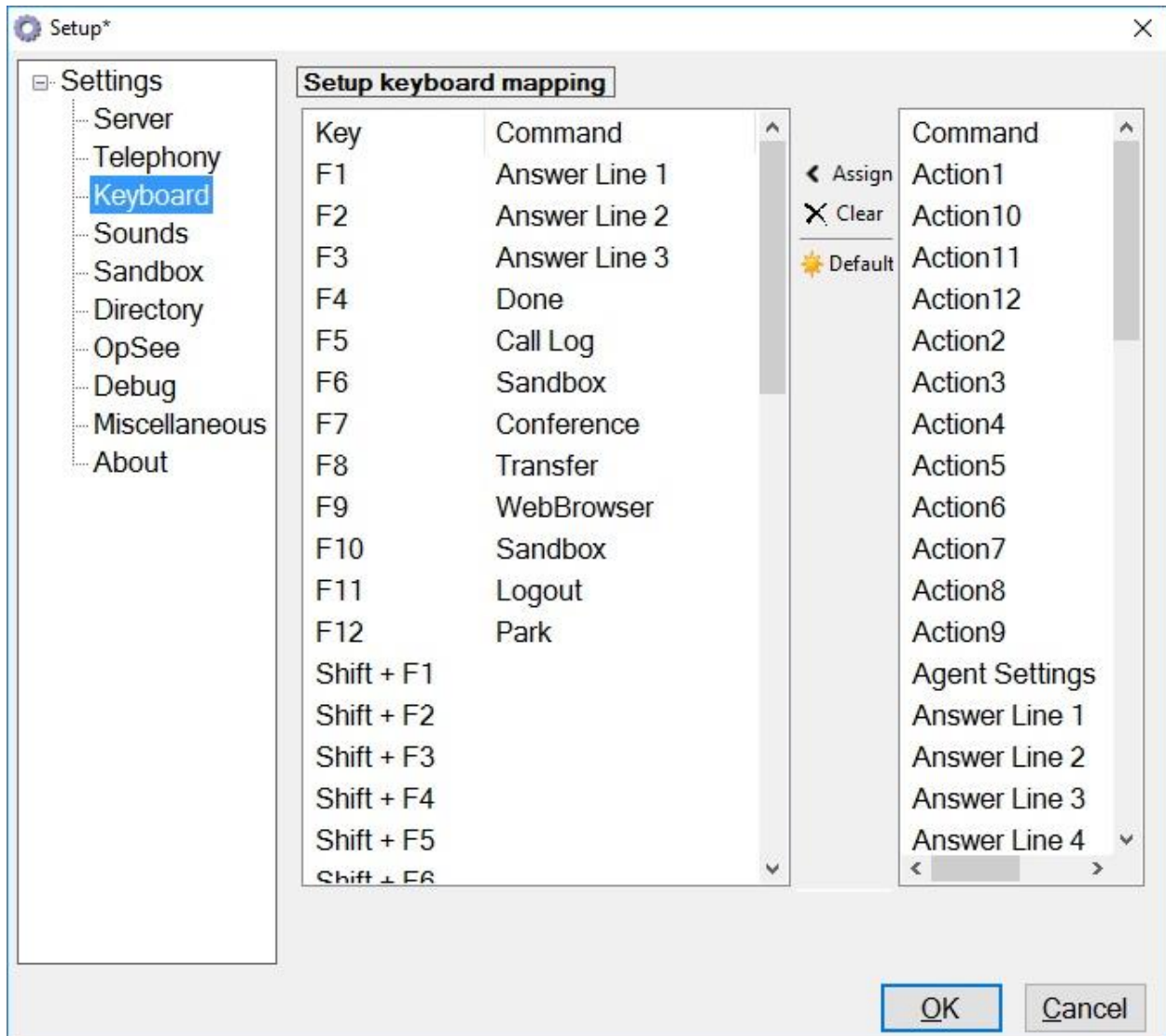


Select the **Audio** tab in the right pane, to display the screen below. For **Audio Type**, select **Integrated**. For **Speaker device** and **Microphone device**, select the applicable devices, as shown below.



Select **Settings** → **Keyboard** from the left pane, to display the screen below. Follow reference [3] to set the desired keyboard mapping for the agent. The setting used in the compliance testing is shown below.

Repeat **Section 7.12** and **Section 7.13** for each operator in **Section 3**. In the compliance testing, two operators were configured.



8. Verification Steps

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

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 screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'System Status' expanded, highlighting 'SIP Entity Monitoring'. The main content area is titled 'SIP Entity Link Monitoring Status Summary' and includes a description: 'This page provides a summary of Session Manager SIP entity link monitoring status.' Below this, there are two sections: 'SIP Entities Status for All Monitoring Session Manager Instances' and 'All Monitored SIP Entities'. The first section shows a table with 2 items, filtered to 'Enable'. The second section shows a list of 17 monitored SIP entities, also filtered to 'Enable'.

Session Manager	Type	Monitored Entities					Deny	Total
		Down	Partially Up	Up	Not Monitored			
ASM70A	Core	1	0	13	8	2	24	
ASM70B	Core	5	0	0	1	0	6	

SIP Entity Name
LSP-Trunk1-Private
Presence70
LSP-Trunk3-Public
AURACCSIP
Breeze2
IPOSE110
Genesis
Cisco862
Car2-cores
ACM-Trunk1-Private

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

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: Genesis

Summary View

1 Item Filter: Enable

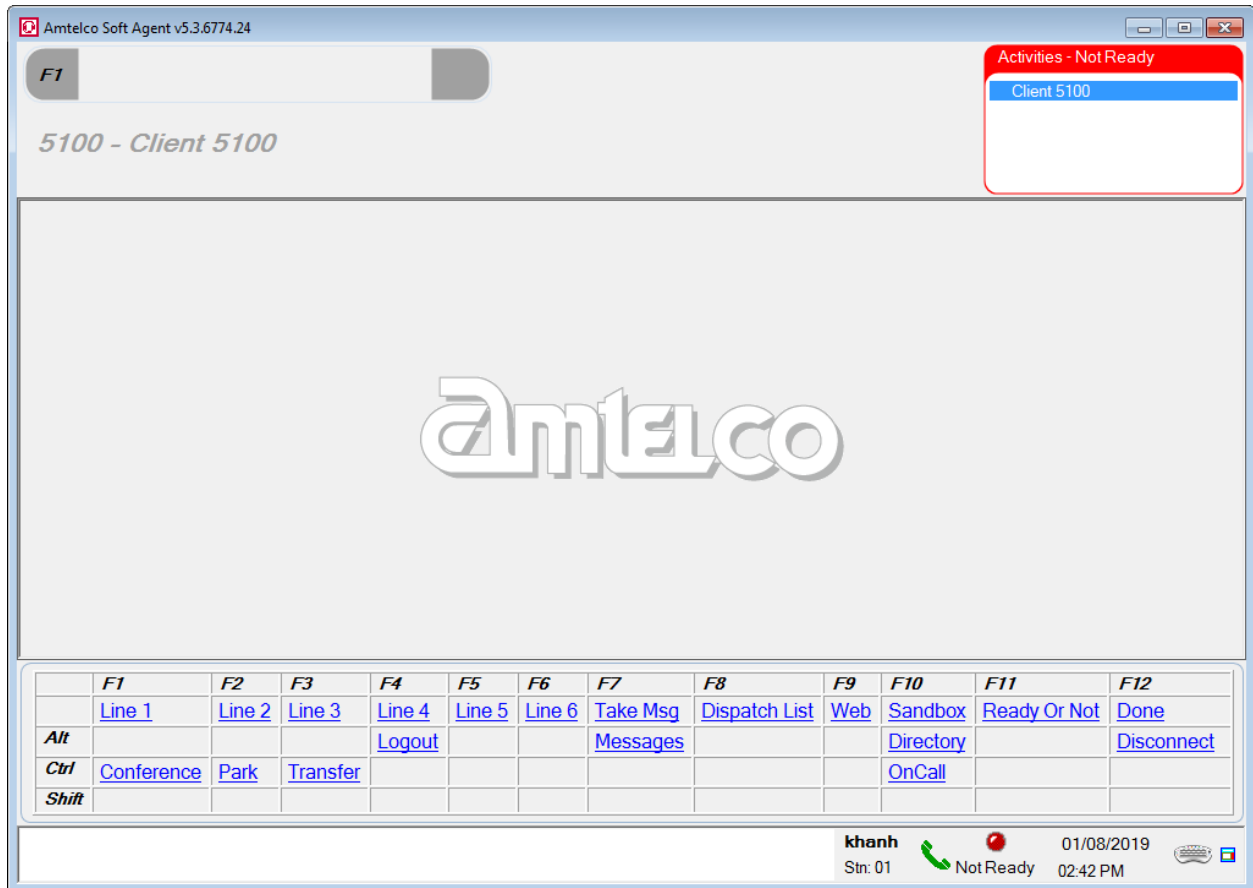
	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	ASM70A	IPv4	10.10.97.251	5060	UDP	FALSE	UP	404 Not Found	UP

Select : None

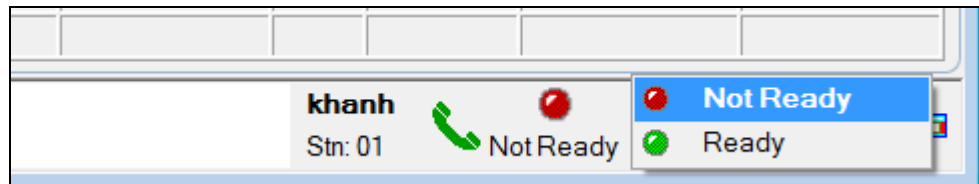
8.3. Verify Amtelco Genesis Intelligent Series

From the operator PC, follow the procedure in **Section 7.12** to launch the Intelligent Series Soft Agent and log in with the appropriate credentials from **Section 7.10**.

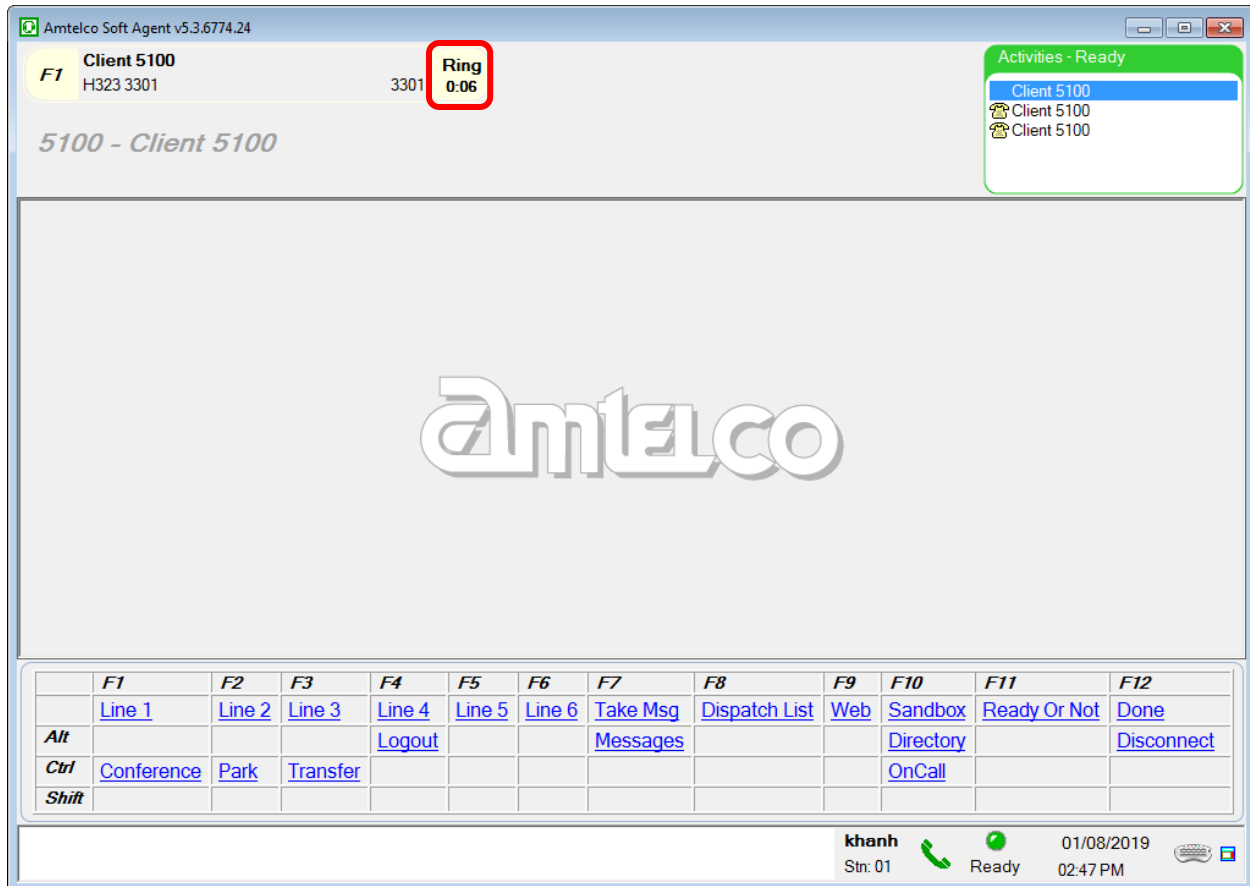
The **Amtelco Soft Agent** screen below is displayed.



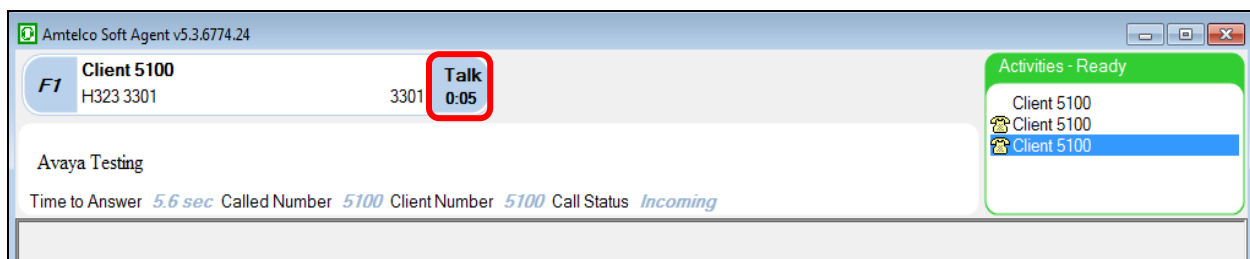
In the lower right portion of the screen, right click on **Not Ready** and select **Ready**.



Make an incoming call from an extension in Communication Manager to reach Genesis. Verify that the call is ringing at the available operator, and that the operator 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 **3301**, and the called number is **5100**. Press the **F1** key or click in the applicable call line area highlighted below to answer the call.



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



9. Conclusion

These Application Notes describe the configuration steps required for Amtelco Genesis Intelligent Series 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 Avaya documentation that are relevant to these Application Notes. Product documentation for Avaya Aura® Session Manager, including the following, is available at: <http://support.avaya.com/>

[1] *Administering Avaya Aura® Session Manager*, Document 03-300509, Issue 10, Release 8.0, August 2018

[2] *Administering Avaya Aura® System Manager*, Issue 9.0, Release 8.0, August 2018

[3] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 8.0, August 2018

[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 9.0, Release 8.0, August 2018

For the Amtelco Genesis document can be obtained by contact Amtelco.

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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