



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Amtelco Genesis Intelligent Series with Avaya Aura® Session Manager 8.1 – 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 a SIP trunk. 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 a SIP trunk. 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 a SIP trunk 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 blind 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 system and Amtelco Genesis did not use secure encryption feature as requested Amtelco.

## **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.

## **2.3. Support**

Technical support on Genesis can be obtained through the following:

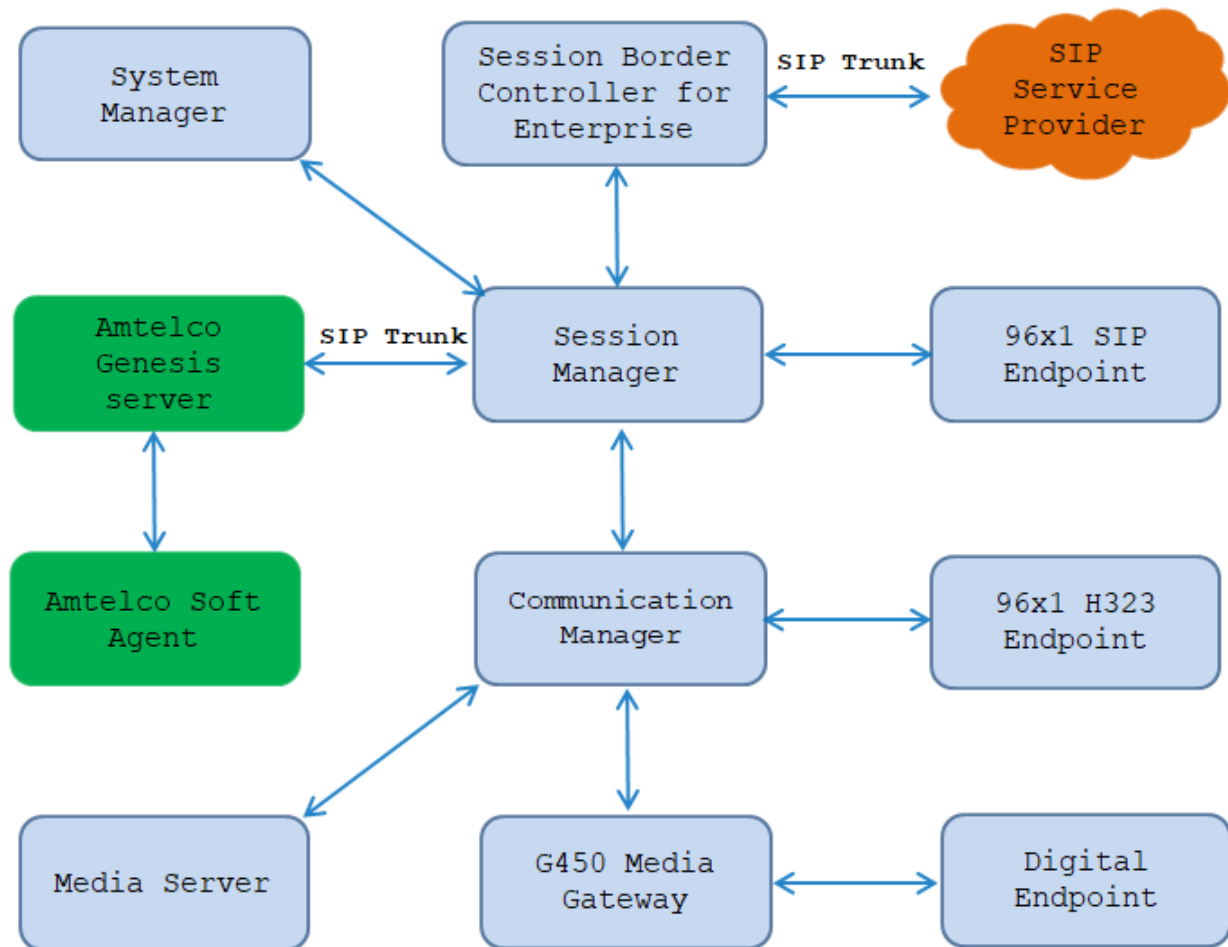
- **Phone:** (800) 553-7679
- **Email:** [service@amtelco.com](mailto:service@amtelco.com)
- **Web:** <https://www.amtelco.com/customer-support>

### 3. Reference Configuration

As shown in **Figure 1**, operators have desktops running the Amtelco 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 Amtelco Genesis Server and Session Manager. A 4-digit Uniform Dial Plan was used to facilitate dialing with Genesis. Calls to extensions 52xx were routed over the SIP trunk to Genesis. In particular, internal users on Communication Manager will dial 52000 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 (8.1.3.0.0.890.26568)
Avaya G450 Media Gateway	41.34.0
Avaya Aura® Media Server running on Virtual Environment	8.0.1
Avaya Aura® Session Manager running on Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager running on Virtual Environment	8.1.3 (8.1.3.0.1011784)
Avaya Aura® Session Border Controller for Enterprise running on Virtual Environment	8.1.1 (8.1.1.0-26-19214)
Avaya 9611G IP Deskphones (H.323)	6.8304
Avaya 9621G IP Deskphone (SIP)	7.1.9.0.8
Amtelco Genesis T Server on Ubuntu <ul style="list-style-type: none"><li>• Asterisk</li></ul>	Linux ubuntu 4.4.0 Asterisk PBX 16.9.0
Amtelco Intelligent Series Supervisor on Microsoft Windows 10 Pro	5.4.7065

## 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		
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>30</b>		
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 should 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 “52”. 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	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: Private Trunk</b>	COR: 1	TN: 1	<b>TAC: #01</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n	Member Assignment Method: auto	
		<b>Signaling Group: 1</b>	
		<b>Number of Members: 14</b>	

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 <b>Format: private</b>		
		UI Treatment: shared	
		Maximum Size of UI 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 “52”. 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
rgn set WAN Units	Total Norm	Prio Shr	Regions
1 1			
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

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet 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 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 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
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 52xx will be routed as an AAR call using route pattern “52” from **Section 5.8**.

change aar analysis 51							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.

AVAYA

Aura® System Manager 8.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Session Manager

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Location Details

Commit

Cancel

General

\* Name:

Genesis

Notes:

Genesis Location

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Home

Session Manager

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

### Alarm Threshold

Overall Alarm Threshold:  %

Multimedia Alarm Threshold:  %

\* Latency before Overall Alarm Trigger:  Minutes

\* Latency before Multimedia Alarm Trigger:  Minutes

### Location Pattern

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.100.50	IP address of Genesis server

Select : All, None

Commit

Cancel

## 6.3. Administer SIP Entities

Add two new SIP entities, one for Genesis and one for the new SIP trunk to 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.

The screenshot shows the 'SIP Entity Details' screen in the Avaya Communication Manager interface. The left sidebar contains a navigation menu with the following items: Home, Session Manager, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main area displays the 'SIP Entity Details' form with the 'General' tab active. The form contains the following fields and values:

- Name:** Genesis
- FQDN or IP Address:** 10.33.100.50
- Type:** Other
- Notes:** Amtelco Genesis
- Adaptation:** (empty)
- Location:** Genesis
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty)

The 'Loop Detection' section is partially visible at the bottom of the form.



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. 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
<input type="checkbox"/>	* ASM_Genesis	ASM70A	UDP	* 5060	Genesis	* 5060	trusted

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.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a tree view of the system configuration, with 'SIP Entities' selected under the 'Routing' section. The main content area displays the 'SIP Entity Details' form. The 'General' tab is active, showing fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, SIP Timer B/F, Minimum TLS Version, Credential name, Securable, and Call Detail Recording. The values entered in the form are: Name: ACM-Trunk1-Private, FQDN or IP Address: 10.33.1.6, Type: CM, Notes: Private SIP trunk, Adaptation: (empty), Location: InteropCM, Time Zone: America/Toronto, SIP Timer B/F: 4, Minimum TLS Version: Use Global Setting, Credential name: (empty), Securable: (unchecked), and Call Detail Recording: both.

Field	Value
Name	ACM-Trunk1-Private
FQDN or IP Address	10.33.1.6
Type	CM
Notes	Private SIP trunk
Adaptation	(empty)
Location	InteropCM
Time Zone	America/Toronto
SIP Timer B/F (in seconds)	4
Minimum TLS Version	Use Global Setting
Credential name	(empty)
Securable	<input type="checkbox"/>
Call Detail Recording	both

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
<input type="checkbox"/>	* ASM70_ACM_Trunk1_Si	ASM70A	TLS	* 5061	ACM-Trunk1-Private	* 5061	trusted

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 trunk to 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 8.1

Users v Elements v Services v Widgets v Shortcuts v Search admin

Home Session Manager Routing

Routing Policies

### Routing Policy Details

Commit Cancel

**General**

\* Name: To-Genesis

Disabled: ☐

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
Genesis	10.33.100.50	Other	Amtelco Genesis

**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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

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.

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 “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 endpoints 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 8.1 interface. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and contains two sections: 'General' and 'Originating Locations and Routing Policies'.

**General Section:**

- \* Pattern: 52
- \* Min: 4
- \* Max: 4
- Emergency Call: ☐
- SIP Domain: bvwddev.com
- Notes:

**Originating Locations and Routing Policies Section:**

1 Item

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

Select : All, None

## 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. A similar dial pattern for “34” was configured.

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).

The screenshot displays the Avaya Aura System Manager 8.1 interface. The left navigation pane shows the 'Routing' section expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields:

- \* Pattern: 33
- \* Min: 4
- \* Max: 4
- Emergency Call: ☐
- SIP Domain: bvwddev.com
- Notes: Dial pattern to CM from all locations

The 'Originating Locations and Routing Policies' section shows a table with 2 items. 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
<input type="checkbox"/>	-ALL-		To-CM-Trunk1	0	<input type="checkbox"/>	ACM-Trunk1-Private	
<input type="checkbox"/>	-ALL-		To-LSP-Trunk1	1	<input type="checkbox"/>	LSP-Trunk1-Private	

## 7. Configure Amtelco Genesis Intelligent Series

This section provides the procedures for configuring Genesis. 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 displays the Genesis web interface. At the top, there is a navigation bar with tabs: Administration, Diagnostics, Licenses, MRCP, and About. The Administration tab is selected. On the left, a 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 contains a 'Create New' button. Below this is a table with two columns: 'Name' and 'Description'. The table contains one entry with the name 'IS' and the description 'Intelligent Series Server'. The 'Name' column header and the 'IS' entry are circled in red. At the bottom of the table, there are links for 'Edit' and 'Delete'. Below the table, there is a pagination bar showing 'Page 1 of 1' and links for '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 0**.
- **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 interface. On the left is a navigation pane with a tree view containing: Applications, Agents, Emergency Agents, SIP Options, Trunks (selected), Routes, Call Types, Class Of Service, and Music On Hold. The main area 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, DtmfMode (RFC2833), Nat (checkbox), and Qualify (checkbox).
- CustomSettings:** A text area containing: deny=0.0.0.0/0.0.0.0, permit=135.10.97.0/24, and 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 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** section, select the trunk from **Section 7.3** under **Available** and move to **Selected**, as shown below.

The screenshot displays the 'Genesis' application 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 'Route Information' and contains the following fields:

- Number:** A text box containing the value '0'.
- Name:** A text box containing the value 'Avaya'.
- Hunt:** A checkbox that is currently unchecked.

Below these fields is the 'Route Trunks' section, which is divided into two columns: 'Available' and 'Selected'. The 'Available' column is currently empty. The 'Selected' column contains a single entry, 'Avaya', which is highlighted in blue. Between the two columns are two buttons: a right-pointing arrow (→) and a left-pointing arrow (←). At the bottom of the 'Route Trunks' section are 'Save' and 'Cancel' buttons.

## 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**.

Genesis	
Administration	Diagnostics Licenses About
Applications Agents Emergency Agents SIP Options Trunks Routes Call Types Class Of Service Music On Hold	<div><b>Agents</b></div> <div>Create New Modify Range</div> <div>Application Agent Number</div> <div>Edit Delete IS 1</div> <div>Page 1 of 1</div> <div>First Previous Next Last</div>

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 0**.
- **Transport:** “udp”

**Genesis**

**Administration** | Diagnostics | Licenses | MRCP | About

**Create a new agent**

Agent Number: 2

Password: ●●●

Application: IS

Custom Settings: [Empty text area]

Transport: udp

**Access Control Lists**

**Available**

**Selected**

Primary

Save Cancel

## 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 screenshot displays the Genesis Administration web interface. The top navigation bar includes tabs for Administration, Diagnostics, Licenses, MRCP, and About. The left sidebar lists various configuration categories: Applications, Agents, Emergency Agents, SIP Options, Trunks, Routes, Call Types, Class Of Service, and Music On Hold. The main content area is titled 'SIP Settings' and contains two sections: 'SIP Settings' and 'PJSIP Settings'. Under 'SIP Settings', there are links for 'General' and 'Access Control Lists', with the latter highlighted by a red rectangle. The 'PJSIP Settings' section lists links for 'Address of Record List', 'Authentication Records', 'Domain Aliases', 'Global', 'Registrations', 'System', and 'Transports'. Below these settings, the 'Active SIP Type' section features a dropdown menu currently set to 'SIP', also highlighted by a red rectangle. To the right of the dropdown, a message states 'Changing type requires a restart'. At the bottom of this section are 'Save' and 'Cancel' buttons.

**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.

# Genesis

**Administration**DiagnosticsLicensesMRCPAbout

ApplicationsAgentsEmergency AgentsSIP OptionsTrunksRoutesCall TypesClass Of ServiceMusic 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

SaveCancel

## 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.

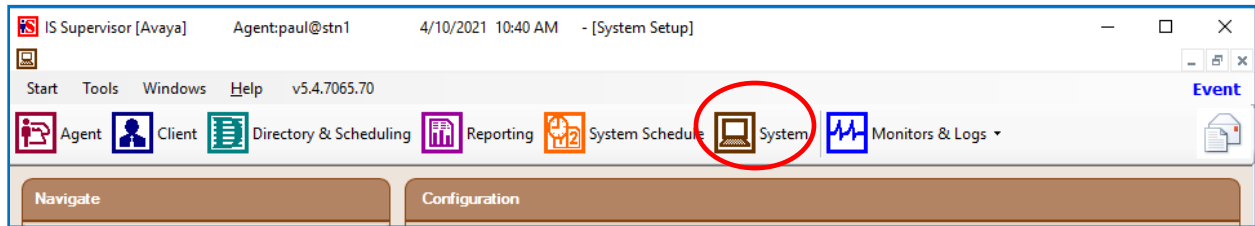


The **Supervisor Login** screen is displayed. Log in using the appropriate credentials.



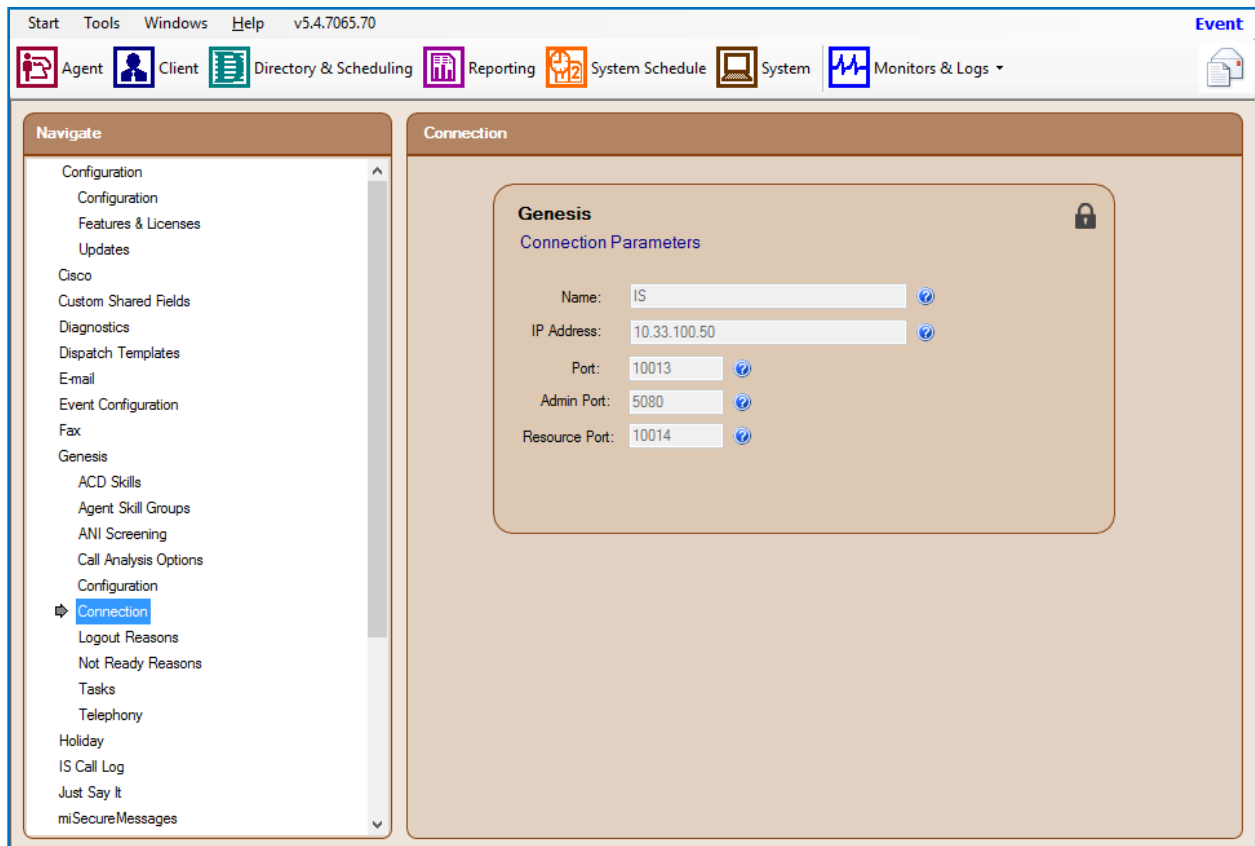
## 7.8. Administer IS System

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 0**.
- **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.

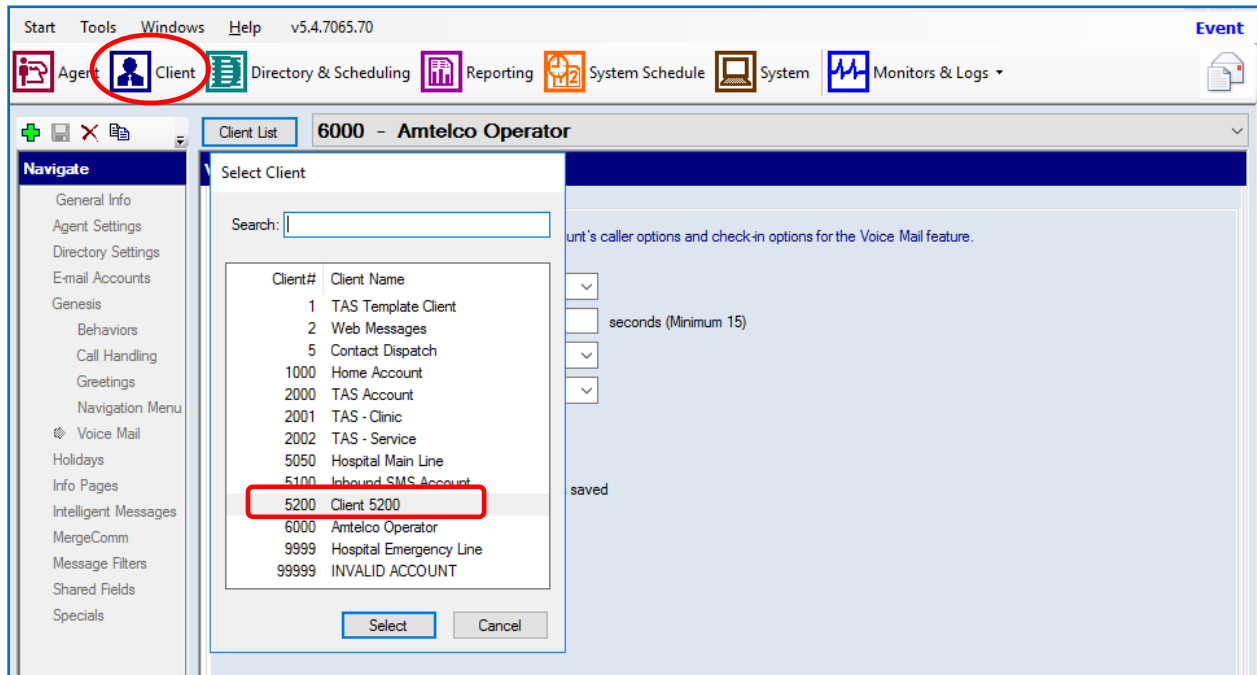
- **Caller ID:** The desired calling party extension to use for outbound calls.
- **Caller Name:** The desired calling party name to use for outbound calls.

The screenshot shows the Avaya System Manager interface. The top navigation bar includes 'Start', 'Tools', 'Windows', 'Help', and 'v5.4.7065.70'. Below this is a toolbar with icons for Agent, Client, Directory & Scheduling, Reporting, System Schedule, System, and Monitors & Logs. The left pane, titled 'Navigate', contains a tree view with categories like Configuration, Cisco, Custom Shared Fields, Diagnostics, Dispatch Templates, E-mail, Event Configuration, Fax, Genesis, Tasks, Holiday, IS Call Log, Just Say It, and miSecureMessages. The 'Telephony' option under 'Genesis' is selected. The right pane, titled 'Telephony', displays the 'Genesis Telephony Settings' form. The form includes fields for 'Auto Answer Repeat Interval' (0 seconds), 'Calls for ATTA' (0), 'Waits List Refresh Rate' (0 seconds), 'Caller ID' (999999999), 'Caller Name' (Amtelco), 'Patch Time' (99 minutes), 'Blind Transfer Timeout' (20 seconds), 'Comma Time' (2 seconds), 'Initial Digit Timeout' (3 seconds), 'Time Between Digits Timeout' (3 seconds), and a 'Set Invalid Source Client' dropdown (1000 - Home Account). There are also checkboxes for 'Hangup Patch After Patch Time Elapses', 'Play Busy When No Ops On Duty', and 'Single Call Hold Park'. A 'Save' button is at the bottom right.

## 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 5200 to Genesis, and calls from internal users on Communication Manager will be routed with digits 5 to Genesis. Therefore, two clients were created, as shown below.

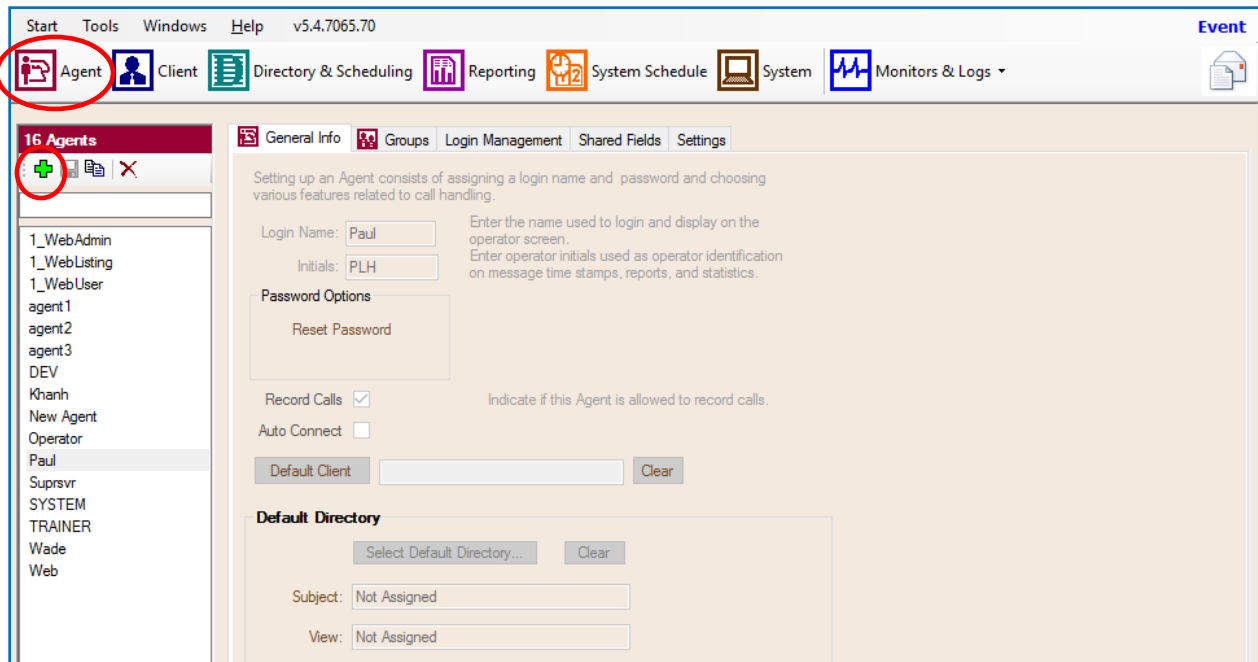


## 7.10. Administer IS Agent

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.

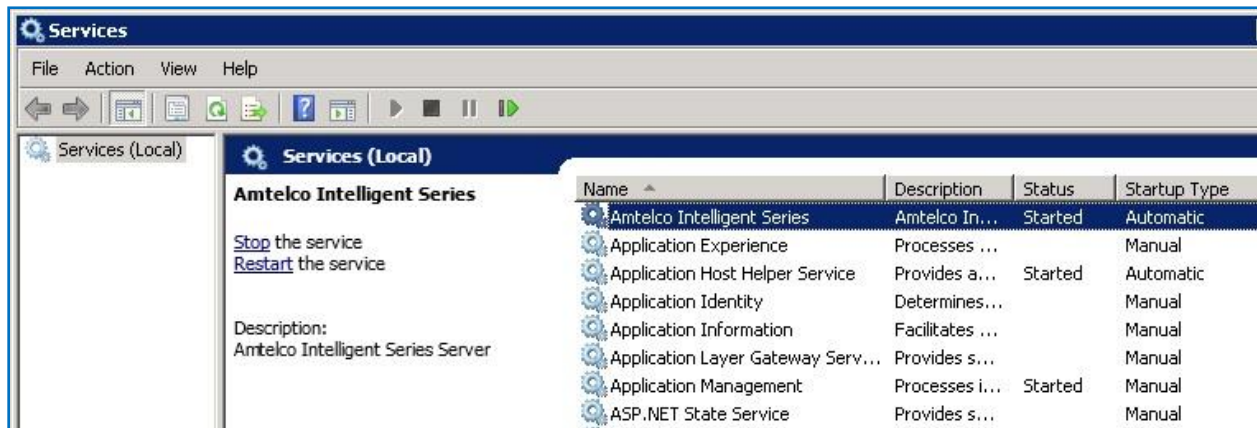
The **General Info** tab is displayed. For **Login Name**, **Password**, and **Confirm**, enter desired values. Retain the default values in the remaining fields.

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.

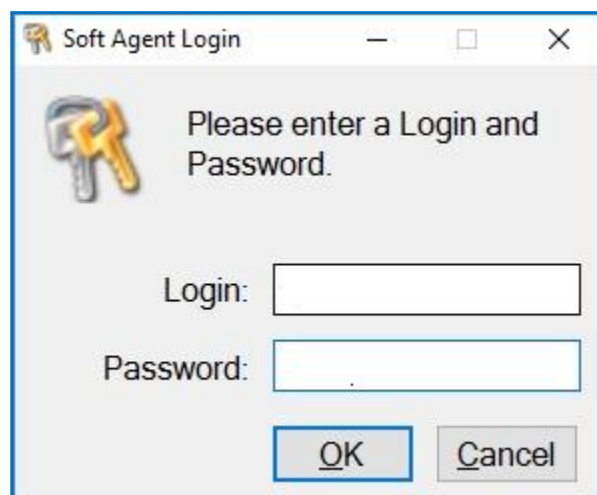


## 7.12. Launch Intelligent Series Soft Agent

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.



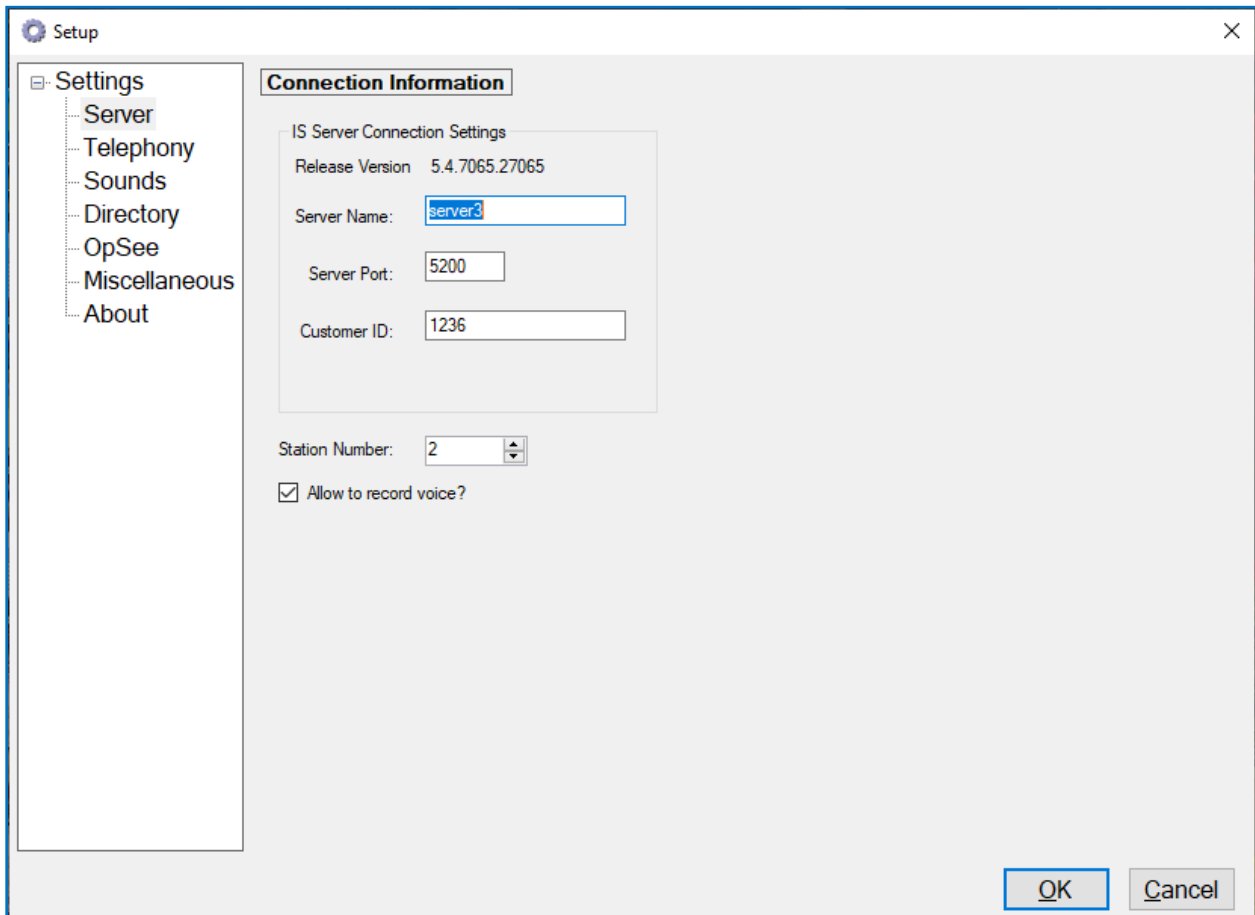
The **Soft Agent Login** screen is displayed. Press the **Ctrl** and **F12** keys together to enter setup.



## 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.

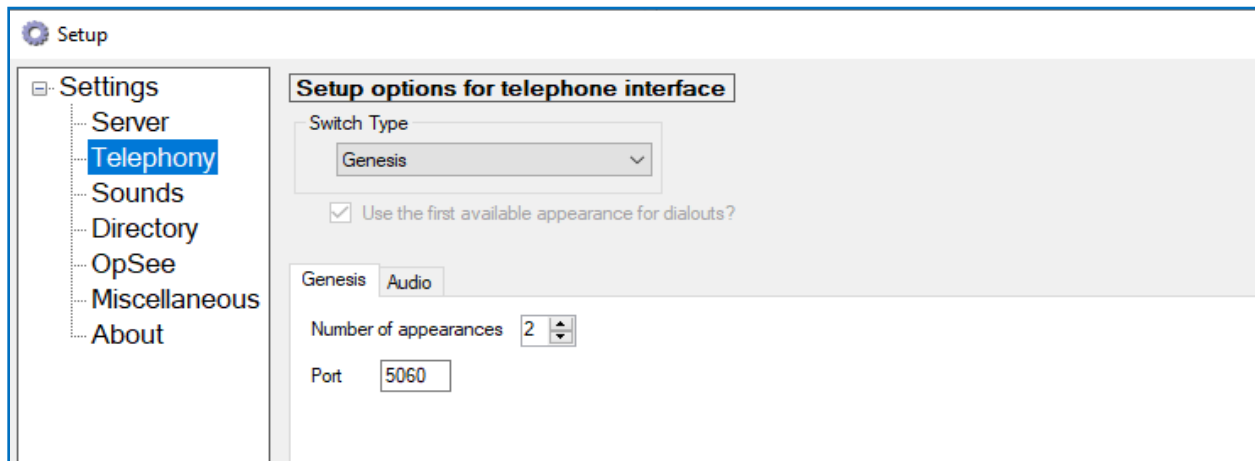
- **Server Name:** IP address or hostname of the Intelligent Series Server.
- **Server Port:** “5200”
- **Customer ID:** The unique customer ID assigned by Amtelco, in this case “1236”.
- **Station Number:** An available station number, in this case “2”.



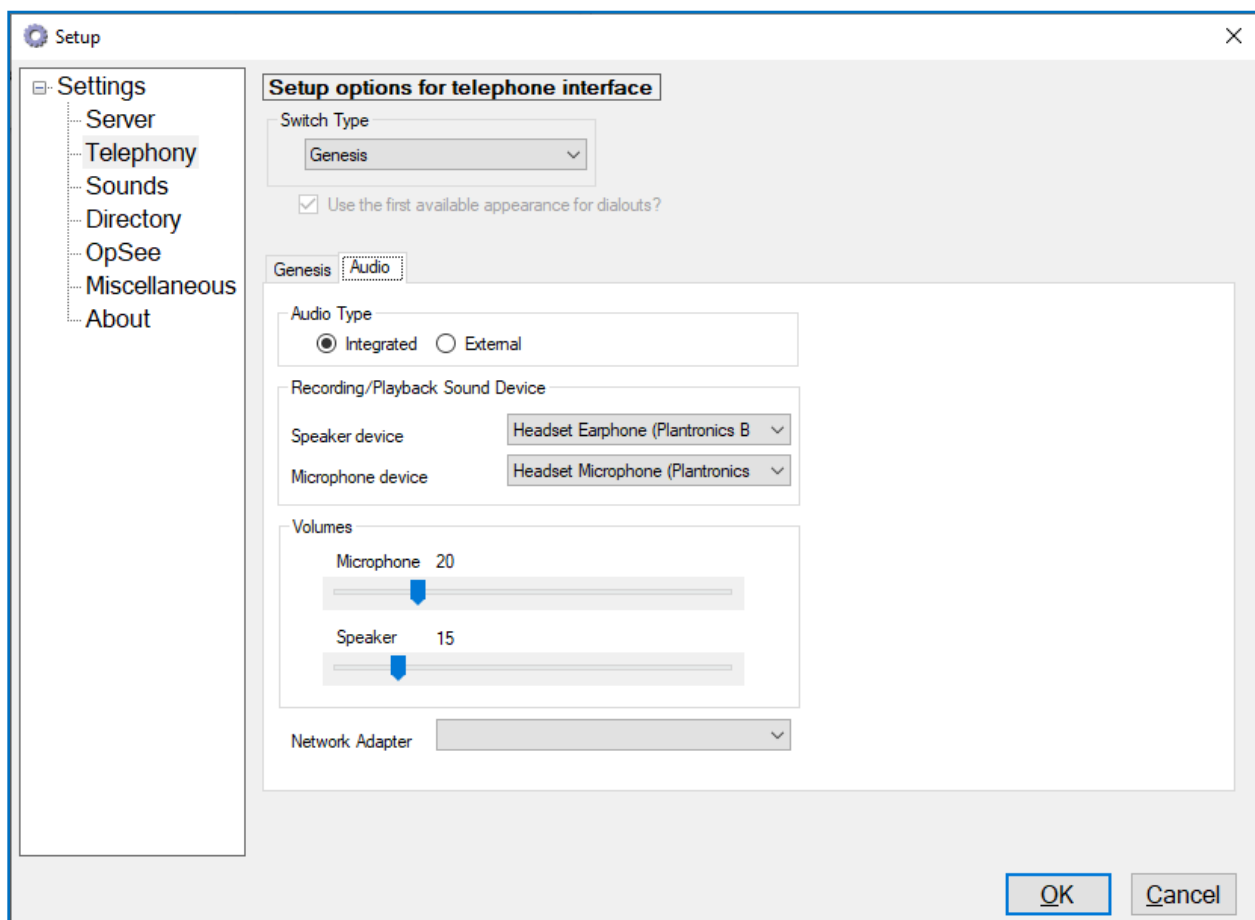
The screenshot shows a Windows-style dialog box titled "Setup" with a close button (X) in the top right corner. On the left is a vertical sidebar with a tree view containing the following items: Settings (expanded), Server (selected), Telephony, Sounds, Directory, OpSee, Miscellaneous, and About. The main area of the dialog is titled "Connection Information" and contains the following fields and controls:

- A sub-header "IS Server Connection Settings" is present.
- A "Release Version" label followed by the text "5.4.7065.27065".
- A "Server Name:" label followed by a text input field containing "server3".
- A "Server Port:" label followed by a text input field containing "5200".
- A "Customer ID:" label followed by a text input field containing "1236".
- A "Station Number:" label followed by a spinner box containing the value "2".
- A checked checkbox labeled "Allow to record voice?".
- At the bottom right are two buttons: "OK" and "Cancel".

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**.

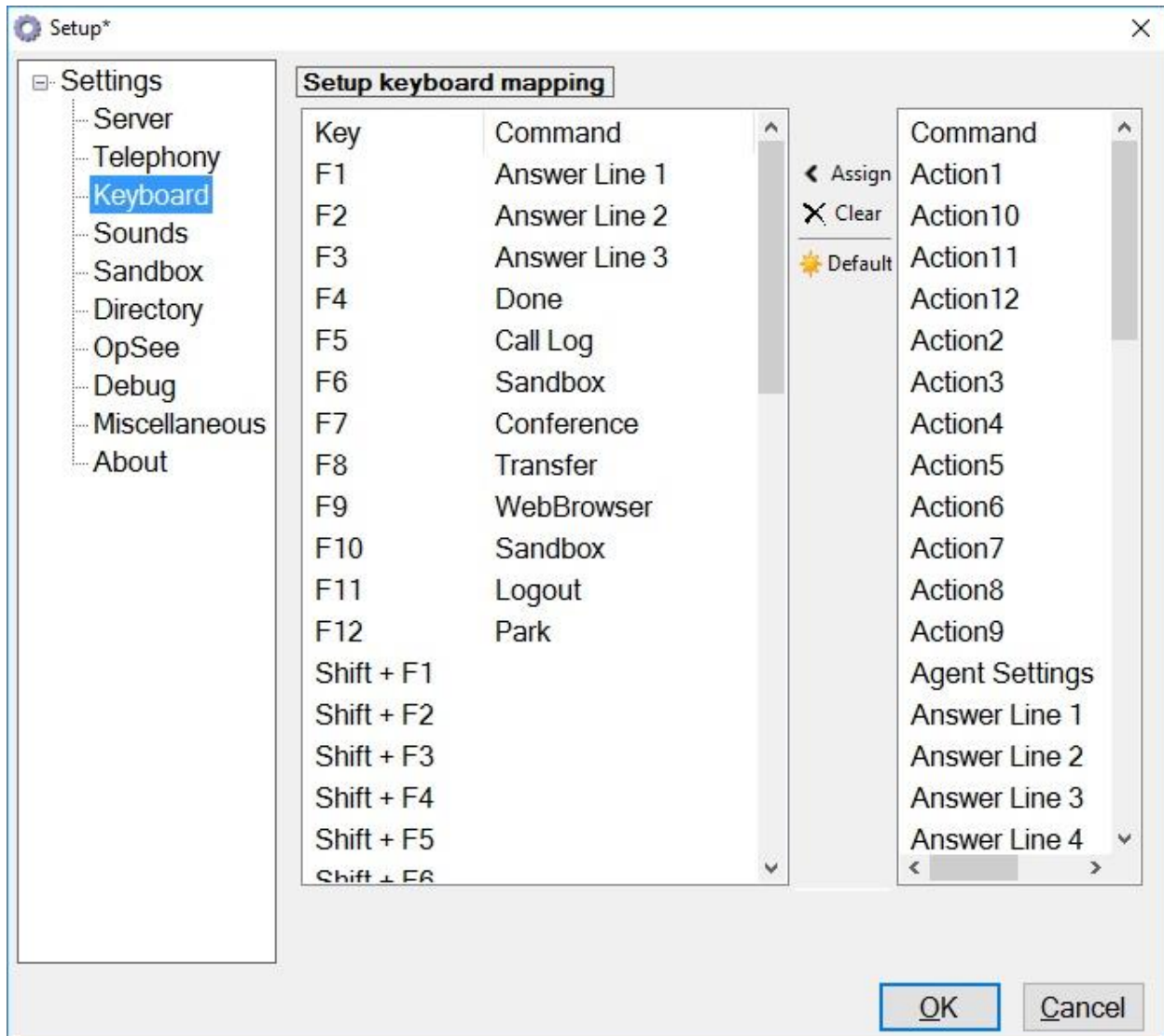


Select the **Audio** tab in the right pane, to display the screen below. For **Audio Type**, select **Integrated**. For **Speaker device** and **Microphone device**, select the applicable devices, as shown below.



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

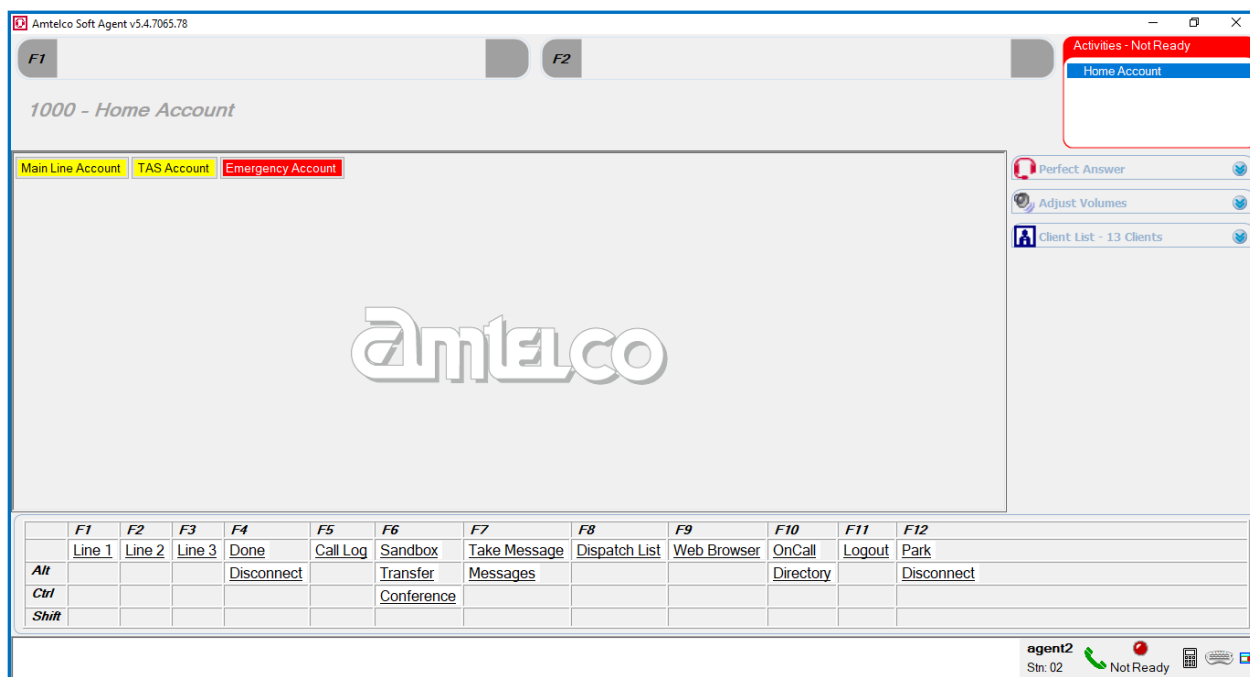
The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and user profile are also present. The left sidebar shows a navigation tree with options like Home, Session Manager, Routing, and various configuration sections. The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a description of the page's purpose. Below this, there is a section for "All Entity Links to SIP Entity: Genesis" with a "Summary View" button. A table lists the connection status for the selected entity, showing one item with details such as Session Manager Name, IP Address, Resolved IP, Port, Protocol, Deny status, Connection Status, Reason Code, and Link Status.

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	ASM70A	IPv4	10.33.100.50	5060	UDP	FALSE	UP	200 OK	UP

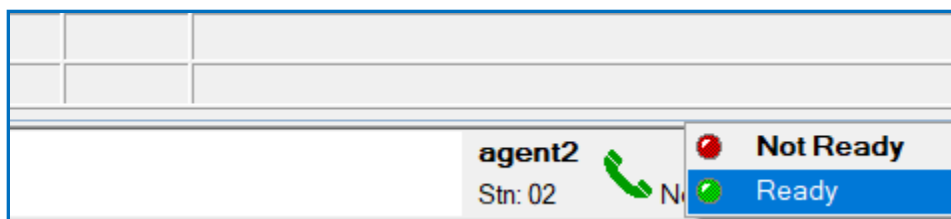
### 8.3. Verify Amtelco Genesis Intelligent Series

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 is displayed below.

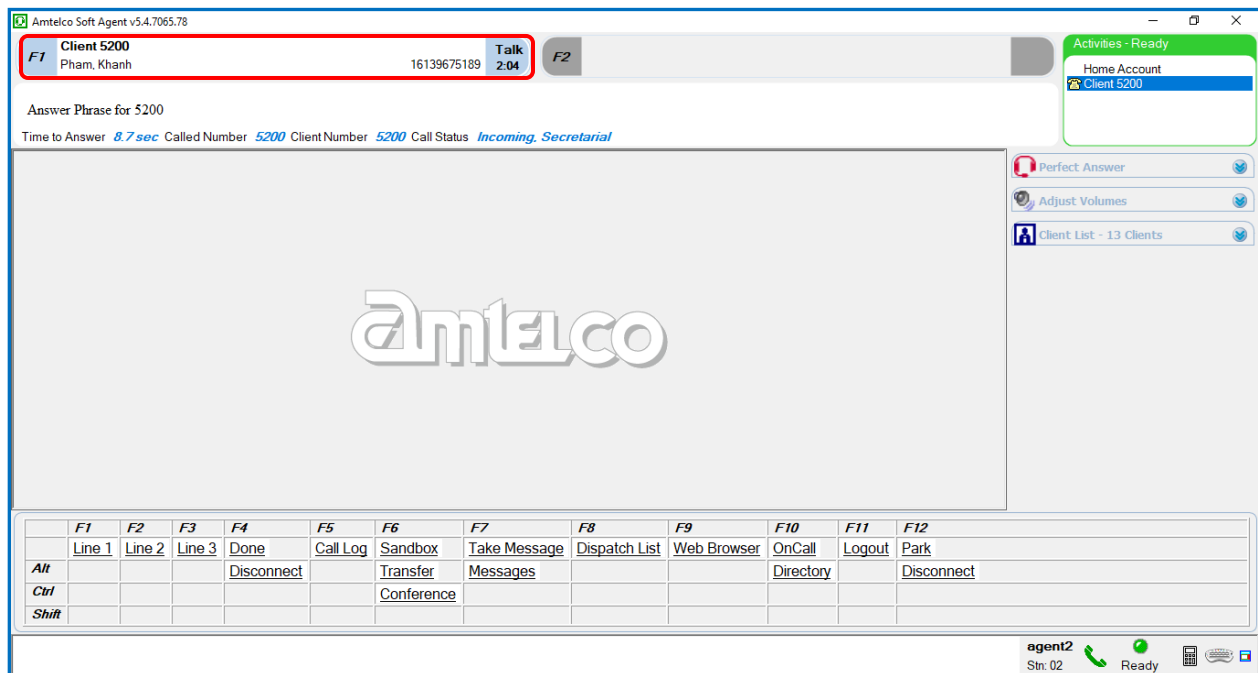


In the lower right portion of the screen, right click on **Not Ready** and select **Ready**.



Make an incoming call from PSTN 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 **16139675189**, and the called client name is **Client 5200**. 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 PSTN 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.

## 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>.

---

**©2021 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](mailto:devconnect@avaya.com).