



Avaya Solution & Interoperability Test Lab

Application Notes for Amtelco Intelligent Soft Agent 5.4 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Amtelco Intelligent Soft Agent 5.4 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

Amtelco Intelligent Soft Agent is call center solution that uses the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor call center agents on Avaya Aura® Communication Manager to provide screen pop, agent state change, and call control capabilities from the agent desktops.

Readers should pay attention to 2, in particular the scope of testing as outlined in Section 2.1, as well as any observations noted in 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 Intelligent Soft Agent (Soft Agent) 5.4 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

The Device, Media, and Call Control (DMCC) .NET integration with Application Enablement Services is from each agent desktop running the Intelligent Series Soft Agent application. The DMCC .NET interface is used to monitor the VDNs and the applicable agent station, to provide screen pop, agent state change, and call control capabilities. The total number of queued calls across the monitored VDNs are also tracked by Soft Agent and displayed on the agent desktop.

In addition, to support the Perfect Answer Greeting feature on Soft Agent, a virtual DMCC station is created on Communication Manager for each agent, for play back of pre-recorded greetings associated with the called client numbers. The Soft Agent registers the associated virtual DMCC station as part of application start up. When an incoming ACD call is delivered to an available agent, the called client number is checked to see if there is a pre-recorded greeting. When there is a match, then after the agent answers the call, the Single Step Conference feature is used by Soft Agent to add the associated virtual DMCC station to the connected call for playback of the applicable greeting.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Soft Agent application, the application automatically requests monitoring of VDNs and agent station, registers the virtual DMCC station, and logs the agent in to Communication Manager.

For the manual part of the testing, incoming ACD calls were placed with available agents. All necessary call actions were initiated from the agent desktops and/or telephones.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Soft Agent.

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 Soft Agent 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 focused on verifying the following on Soft Agent:

- Use of DMCC registration services to register and un-register virtual DMCC station.
- Use of DMCC logical device services to set agent states, including log in, log out, and work mode changes with support for pending aux work.
- Use of DMCC monitoring services to monitor VDNs and agent station.
- Use of DMCC call control services to support call controls, including Single Step Conference to playback Perfect Answer Greeting.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, perfect announcement, queue count, multiple calls, multiple agents, conference, transfer, long duration, and send DTMF.

The serviceability testing focused on verifying the ability of Soft Agent to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the server and/or client components of Soft Agent.

2.2. Test Results

All test cases were executed and verified. The following were observations on Soft Agent from the compliance testing.

- When the desktop running the Soft Agent application experiences a network disruption while on an active call, the Soft Agent application may disappear from the screen. A user can recover the application when the network connection is restored by using Windows task manager to manually end the Soft Agent process and then re-launch the application. For additional help reach out to Amtelco support.
- Outbound calls placed from the agent telephones were not reflected in Soft Agent, and there were screen pop anomalies with respect to transfer and conference performed using the agent telephones. In general, agents are advised to use the Soft Agent for all call actions.
- Outbound calls placed from Soft Agent reflected the agent's own station extension as called number in the call line and call information areas.
- In the attended transfer scenario, the transfer-to agent desktop did not reflect the original calling number (ANI) or the original called number (DNIS).

- Failure from VDN monitor request was not displayed on Soft Agent. The recommendation is to manually check the Soft Agent logs for verification of successful monitors as part of initial configuration.
- When a work mode change request to aux is in the “pending” state with agent on an active call, the reflection in Soft Agent is as if the agent is already in the aux state. The recommendation is for agents to be conscious of this behavior, as the state change request will succeed after the agent drops from the active call.

2.3. Support

Technical support on Amtelco Intelligent Soft Agent can be obtained through the following:

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

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center resources are not the focus of these Application Notes and will not be described.

The Soft Agent solution is an integral component of the Intelligent Series call center system. The solution consists of the Intelligent Series Server, the Intelligent Series Supervisor, and the Intelligent Series Soft Agent. In the compliance testing, Intelligent Series Supervisor was running on the supervisor desktop, and Intelligent Series Soft Agent was running on each agent desktop.

In the compliance testing, the Soft Agent on each agent desktop monitored the VDNs and the applicable agent station shown in the table below.

Device Type	Extension
VDN	3340
Hunt Group/Skill	3320
Agents	1000, 1001

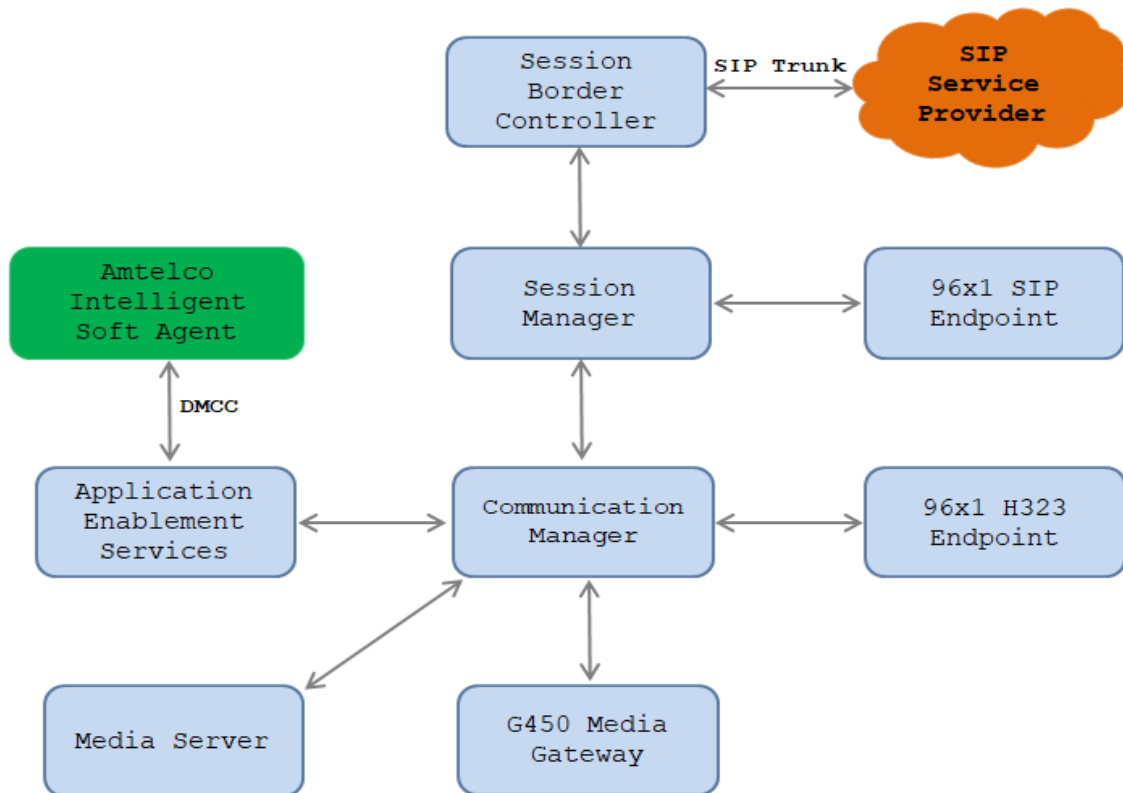


Figure 1: Compliance Testing Configuration.

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	R018x.01.0.890.0 8.1.2.0.0.890.26095
Avaya G450 Media Gateway	41.16.0
Avaya Aura® Media Server in Virtual Environment	8.0.0.173
Avaya Aura® Session Manager in Virtual Environment	8.1.2.0.812039
Avaya Aura® System Manager in Virtual Environment	8.1.2.0 Software Update Revision No: 8.1.2.0.0611097
Avaya Aura® Application Enablement Services	8.1.2.1.1
Avaya 9611GIP Deskphones (H.323)	6.8304
Avaya 9621G IP Deskphone (SIP)	7.1.9
Amtelco Server Intelligent Series	5.4.7065
Amtelco Intelligent Series Soft Agent 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 CTI Link.
- Administer AE Services.
- Administer IP Codec Set.
- Administer DMCC Station.

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for integration with Amtelco Soft Agent.

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has the appropriate permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 4**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Computer Telephony Adjunct Links** field set to “y”.

If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	Computer Telephony Adjunct Links?	y
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n		
Async. Transfer Mode (ATM) Trunking?	n	Digital Loss Plan Modification?	y
ATM WAN Spare Processor?	n	DS1 MSP?	y
ATMS?	y	DS1 Echo Cancellation?	y
Attendant Vectoring?	y		
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page	1 of 3
CTI LINK			
CTI Link: 1			
Extension: 3331			
Type: ADJ-IP			
COR: 1			
Name: AES8			
Unicode Name? n			

5.3. Administer AE Services

To administer the transport link to AES, use the command “**change ip-services**”. On Page 1, add an entry with the following values. Service Type should be selected as **AESVCS**, enter “y” in the **Enabled**, “procr” in the **Local Node** and 8765 in the **Local Port**.

change ip-services					Page	1 of	4
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				

Go to **Page 4**, enter the following values. **AE Services Server** should be the AES host name, enter a password in the **Password** field and select “y” in the **Enabled** field.

Note: The password entered for **Password** field must match the password on the AES server in the Switch Connection in **Section 6.3**. The **AE Services Server** should match the host name of the AES server. To obtain the host name of AES server, use the command “**uname -n**” in the AES server Linux command prompt.

change ip-services				Page	4 of	4
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes8	*	y	in use		
2:	aes81	*	y	in use		

5.4. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Soft Agent.

For **Audio Codec**, make certain a variant for **G.711MU** is included, which is the only codec supported by Soft Agent.

For **Media Encryption**, make certain “none” is included, as required for Soft Agent.
For compliance testing, this IP codec set was assigned to the agents and to the virtual DMCC stations used by Soft Agent.

```
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:

Media Encryption                                Encrypted SRTP: enforce-unenc-srtp
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
```

5.5. Administer DMCC Stations

Add a DMCC station using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “9640”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”.

change station 3371		Page	1 of	5
STATION				
Extension: 3371	Lock Messages? n	BCC:	0	
Type: 9640	Security Code: *	TN:	1	
Port: S000043	Coverage Path 1:	COR:	1	
Name: Amtelco DMCC 1	Coverage Path 2:	COS:	1	
Unicode Name? n	Hunt-to Station:	Tests?	y	
STATION OPTIONS				
Loss Group: 19		Time of Day Lock Table:		
Speakerphone: 2-way		Personalized Ringing Pattern: 1		
Display Language: english		Message Lamp Ext: 3371		
Survivable GK Node Name:		Mute Button Enabled? y		
Survivable COR: internal		Button Modules: 0		
Survivable Trunk Dest? y		Media Complex Ext:		
		IP SoftPhone? y		
		IP Video Softphone? n		
		Short/Prefixed Registration Allowed: default		
		Customizable Labels? y		

Repeat this section to administer a DMCC station for each agent station from **Section 3**. One DMCC station is required by Soft Agent for each agent station to support the Perfect Announcement feature. In the compliance testing, two DMCC stations were administered as shown below.

list station								Page	4
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Cable	Jack	Cv1/ Cv2	COR/ COS		
3371	S000043	Amtelco DMCC 1					1		
	9640		no				1		
3372	S000044	Amtelco DMCC 2					1		
	9640		no				1		

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch AE Web Interface.
- Verify License.
- Administer Switch Connection.
- Administer TSAPI link.
- Administer CTI user.
- Administer Security Database.
- Administer Ports.
- Restart Services.

6.1. Launch AE Web Interface

Access the AE web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a label "Username" and a text input field. Below the input field is a "Continue" button. Another thick red horizontal bar is located below the login box. At the bottom center of the page, the copyright notice "Copyright © 2009-2019 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A user information box in the top right corner displays: "Welcome: User cust", "Last login: Mon Aug 24 16:10:29 2020 from 10.33.1.200", "Number of prior failed login attempts: 0", "HostName/IP: aes8/10.33.1.4", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.2.1.1.6-0", "Server Date and Time: Wed Aug 26 13:35:50 IST 2020", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. The main content area is divided into a left sidebar and a central pane. The sidebar contains a list of menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The central pane is titled "Welcome to OAM" and contains the following text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their functions. At the bottom of the central pane, it states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."

Welcome: User cust
Last login: Mon Aug 24 16:10:29 2020 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Wed Aug 26 13:35:50 IST 2020
HA Status: Not Configured

Home Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

The screenshot shows the "Licensing" page of the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A user information box in the top right corner displays: "Welcome: User cust", "Last login: Mon Aug 24 16:10:29 2020 from 10.33.1.200", "Number of prior failed login attempts: 0", "HostName/IP: aes8/10.33.1.4", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.2.1.1.6-0", "Server Date and Time: Wed Aug 26 13:35:50 IST 2020", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. The main content area is divided into a left sidebar and a central pane. The sidebar contains a list of menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The central pane is titled "Licensing" and contains the following text: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bulleted list of items. Below this, it states: "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bulleted list of items. At the bottom of the central pane, it states: "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bulleted list of items. A red note at the bottom of the central pane states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page."

Welcome: User cust
Last login: Mon Aug 24 16:10:29 2020 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Wed Aug 26 13:35:50 IST 2020
HA Status: Not Configured

Home Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

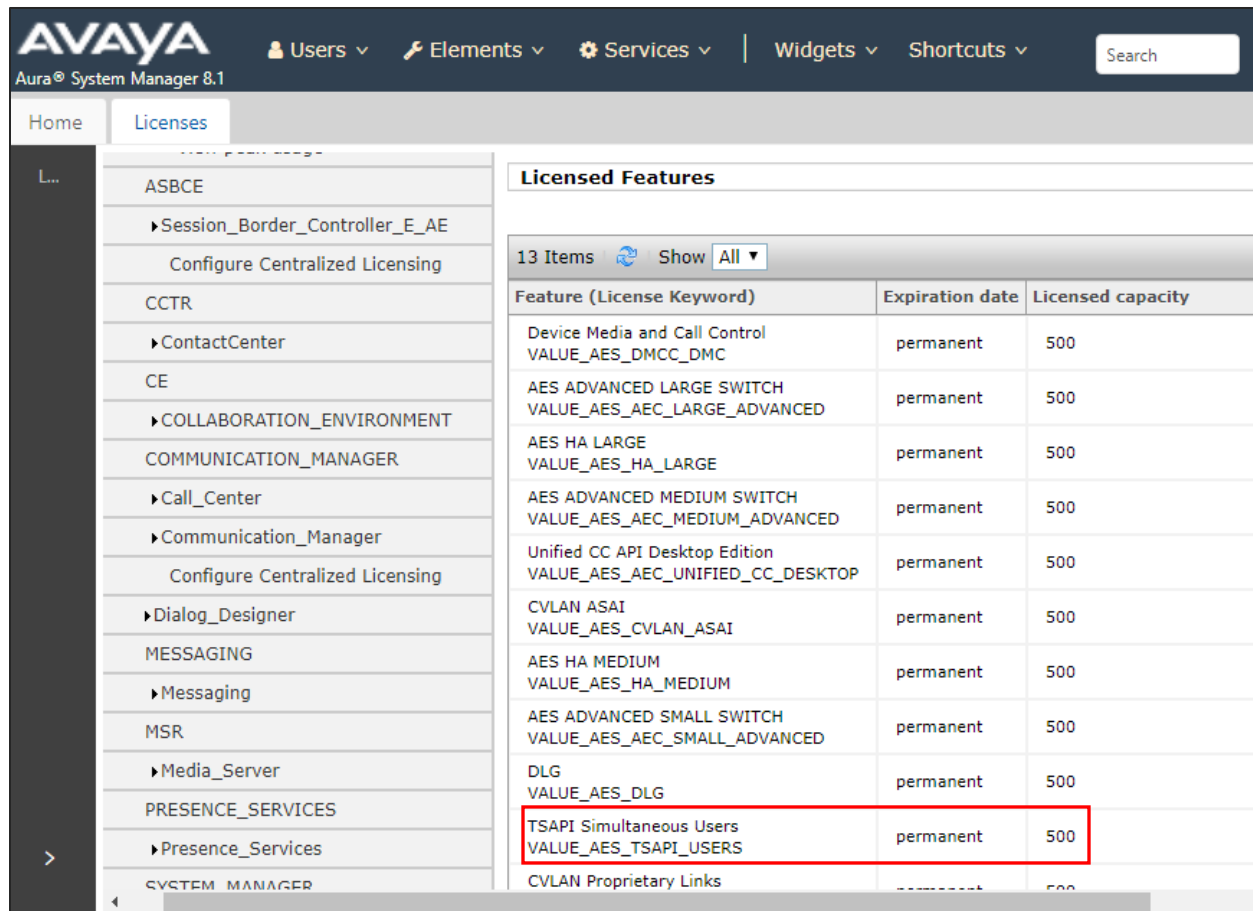
If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.



The screenshot displays the Avaya Aura System Manager 8.1 interface. The left pane shows a tree view with 'L...' expanded, listing various components like ASBCE, Session_Border_Controller_E_AE, CCTR, CE, COMMUNICATION_MANAGER, and SYSTEM_MANAGER. The right pane shows the 'Licensed Features' table, which contains 13 items. The table has three columns: 'Feature (License Keyword)', 'Expiration date', and 'Licensed capacity'. The 'TSAPI Simultaneous Users' feature is highlighted with a red box, showing a permanent license with a capacity of 500.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	500
AES HA LARGE VALUE_AES_HA_LARGE	permanent	500
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	500
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	500
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	500
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	500
DLG VALUE_AES_DLG	permanent	500
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	500
CVLAN Proprietary Links	permanent	500

6.3. Administer Switch Connection

Select **Communication Manager Interface** → **Switch Connection** from the left pane of the **Management Console**, enter a name in **Switch Connection** box and click **Add** button (not shown). Enter the password as configured in **Section 5.3** in the **Switch Password** and **Confirm Switch Password** and check on **Processor Ethernet** field if the Processor Ethernet is used in Communication Manager. Click **Apply** button to save the configuration.

The screenshot shows the 'Communication Manager Interface | Switch Connections' page. On the left is a navigation pane with 'Communication Manager Interface' expanded and 'Switch Connections' selected. The main area displays the 'Connection Details - interopcm' form. The form includes fields for 'Switch Password' and 'Confirm Switch Password' (both masked with dots), a 'Msg Period' of 30 minutes, and checkboxes for 'Provide AE Services certificate to switch' (checked), 'Secure H323 Connection' (unchecked), and 'Processor Ethernet' (checked). 'Apply' and 'Cancel' buttons are at the bottom.

Connection Details - interopcm	
Switch Password
Confirm Switch Password
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	<input checked="" type="checkbox"/>
Secure H323 Connection	<input type="checkbox"/>
Processor Ethernet	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Select the **interopCM** switch connection has been added above and selects **Edit PE/CLAN IPs** to add IP address of switch connection.

The screenshot shows the 'Communication Manager Interface | Switch Connections' page. On the left is the same navigation pane. The main area displays the 'Switch Connections' section. It includes an 'Add Connection' button and a table with one entry, 'interopcm'. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Switch Connections			
<input type="text"/>	<input type="button" value="Add Connection"/>		
Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> interopcm	Yes	30	1
<input type="button" value="Edit Connection"/> <input type="button" value="Edit PE/CLAN IPs"/> <input type="button" value="Edit H.323 Gatekeeper"/> <input type="button" value="Delete Connection"/> <input type="button" value="Survivability Hierarchy"/>			

Enter IP address of Processor Ethernet of Communication Manager in the box and click **Add/Edit Name of IP** button to add the IP.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit Processor Ethernet IP - interopcm

10.33.1.6

Name or IP Address	Status
10.33.1.6	In Use

Select **Edit H.323 Gatekeeper** button to add an IP address of gate keeper, the Gatekeeper IP address in this case is also the Processor Ethernet.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit H.323 Gatekeeper - interopcm

Name or IP Address

☒ 10.33.1.6

6.4. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the 'TSAPI Links' management console. The left sidebar contains a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TWS', 'Communication Manager Interface', 'High Availability', and 'Licensing'. Under 'TSAPI', 'TSAPI Links' is selected. The main content area has a red header bar with 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. Below this is a table with columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is displayed in the right side. The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “**interopcm**” which is added in the step above. For **Switch CTI Link Number**, select the CTI link number 1 from **Section 5.2**, select **Both** in the **Security** dropdown menu to support both unencrypted and encrypted TSAPI link. Retain the default values in the remaining fields.

The screenshot shows the 'Add TSAPI Links' configuration screen. The left sidebar is the same as the previous screenshot. The main content area has a red header bar with 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. Below this is a form titled 'Add TSAPI Links'. The form contains the following fields: 'Link' (dropdown with value '1'), 'Switch Connection' (dropdown with value 'interopcm'), 'Switch CTI Link Number' (dropdown with value '1'), 'ASAI Link Version' (dropdown with value '8'), and 'Security' (dropdown with value 'Both'). Below the form are buttons for 'Apply Changes' and 'Cancel Changes'. In the top right corner, there is a welcome message: 'Welcome: User cust', 'Last login: Sat Apr 18 03:32:50 2020 from 10.33.1.200', 'Number of prior failed login attempts: 0', 'HostName/IP: aes8/10.33.1.4', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.1.1.0.2.8-0', 'Server Date and Time: Sun Apr 19 03:44:20 IST 2020', and 'HA Status: Not Configured'.

6.5. Administer CTI User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

User Management | User Admin | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Edit User

* User Id

test

* Common Name

test

* Surname

test

User Password

Confirm Password

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Home Phone

Home Postal Address

6.6. Configure Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Leave it as default as checked on **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services**.

The screenshot shows the 'Security | Security Database | Control' page. The left navigation pane lists various services, with 'Security Database' expanded to show 'Control'. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' (unchecked) and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services' (checked). Below the checkboxes is an 'Apply Changes' button.

Select **Security → Security Database → CTI Users → List All Users** and select the “test” CTI user which is created in **Section 6.5** and select **Edit** button (not shown). In the **Edit CTI User**, select the check box **Unrestricted Access** and click **Apply Changes** to save the configuration.

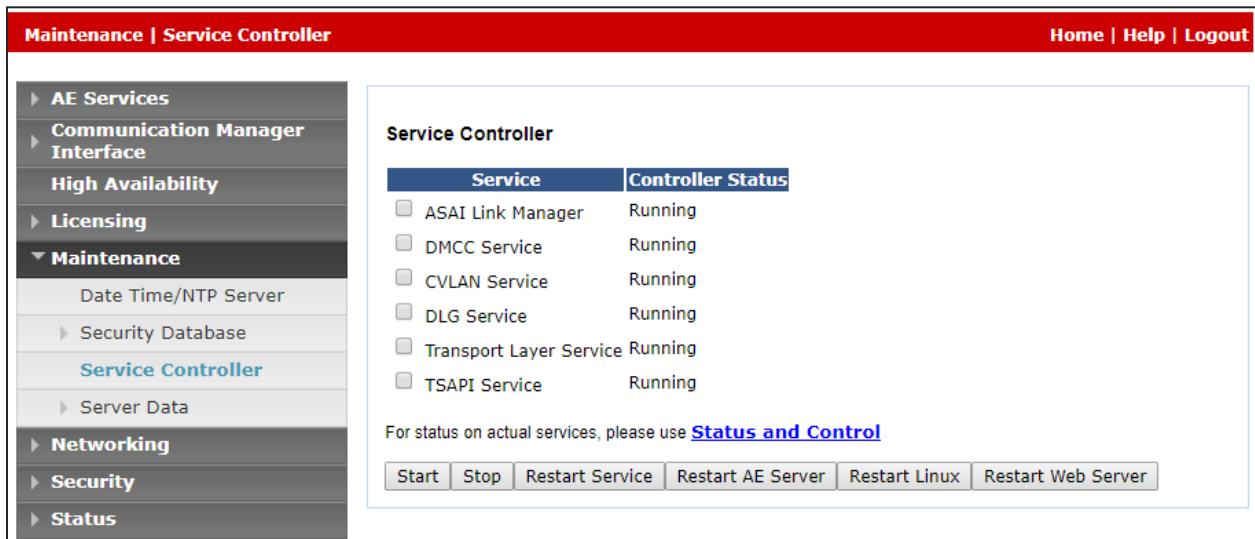
The screenshot shows the 'Security | Security Database | CTI Users | List All Users' page. The left navigation pane shows 'CTI Users' expanded to 'List All Users'. The main content area is titled 'Edit CTI User'. It displays the configuration for a user named 'test'. The 'User Profile' section includes fields for 'User ID' (test), 'Common Name' (test), 'Worktop Name' (NONE), and 'Unrestricted Access' (checked). The 'Call and Device Control' section has a dropdown for 'Call Origination/Termination and Device Status' set to 'None'. The 'Call and Device Monitoring' section has dropdowns for 'Device Monitoring' (None), 'Calls On A Device Monitoring' (None), and a checkbox for 'Call Monitoring' (unchecked). The 'Routing Control' section has a dropdown for 'Allow Routing on Listed Devices' set to 'None'. At the bottom are 'Apply Changes' and 'Cancel Changes' buttons.

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane. In the **DMCC Server Ports** section, select the radio button for **Unencrypted TLINK Port 4721** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

KP; Reviewed: Solution & Interoperability Test Lab Application Notes 19 of 37
SPOC 9/16/2020 ©2020 Avaya Inc. All Rights Reserved. Amtelco-AES81

6.8. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Click **Restart AE Service**.



The screenshot shows a web interface for the Service Controller. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists six services, all of which are 'Running'. Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. At the bottom of the main content area, there is a row of buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

7. Administer Amtelco Intelligent Soft Agent

This section provides the procedures for configuring Amtelco Soft Agent. The procedures include the following areas:

- Launch Intelligent Series Supervisor.
- Administer IS System.
- Administer IS Client.
- Administer IS Agents.
- Launch Intelligent Series Soft Agent.
- Administer Setup.

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

7.1. 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.

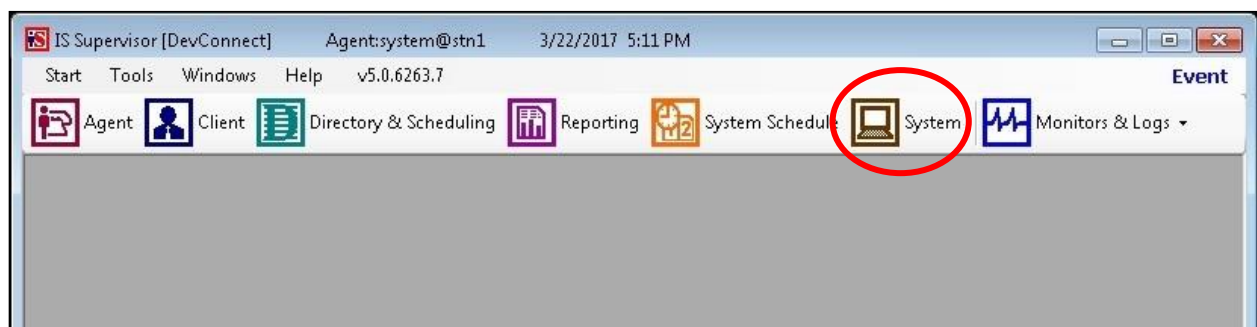


The **Supervisor Login** screen is displayed. Log in using the appropriate credentials.



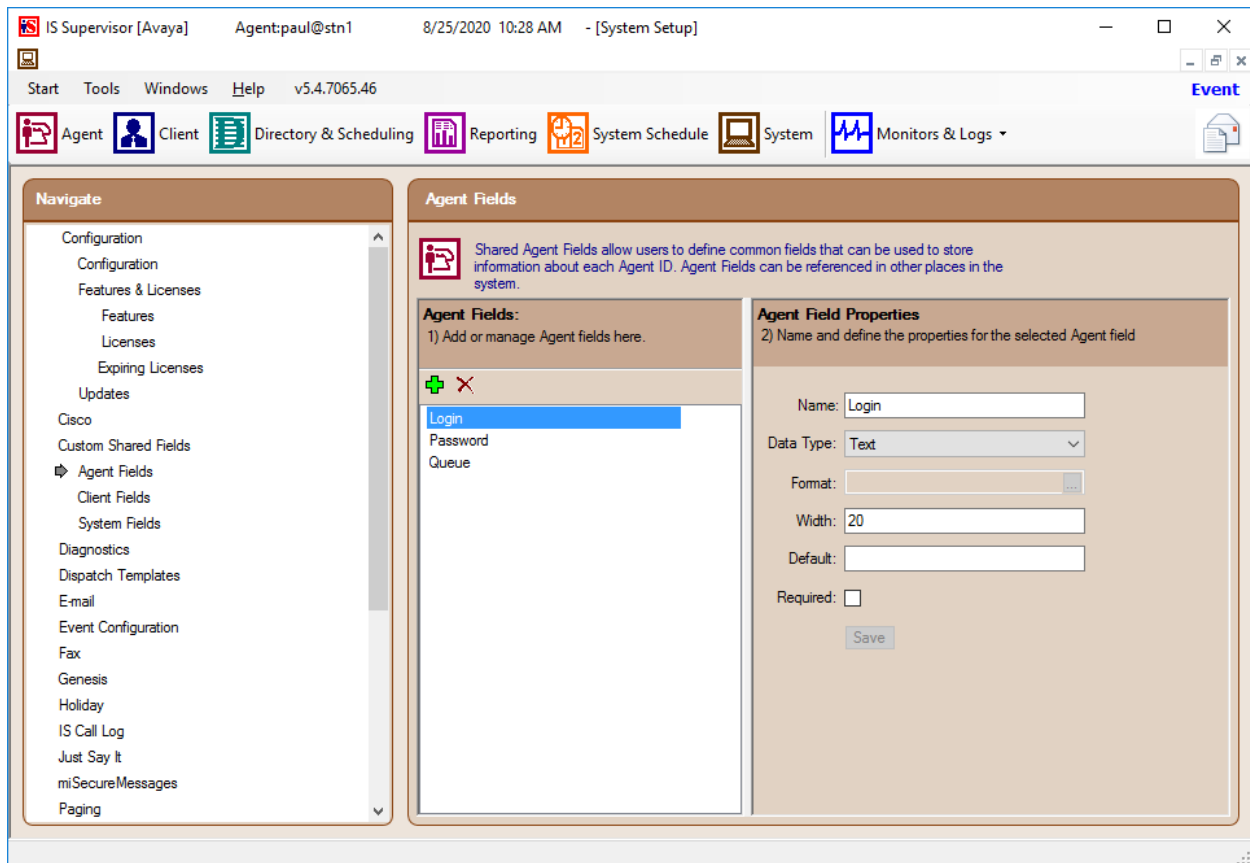
7.2. Administer IS System

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 **Custom Shared Fields → Agent Fields** from the left pane, to display **Agent Fields** in the right pane.

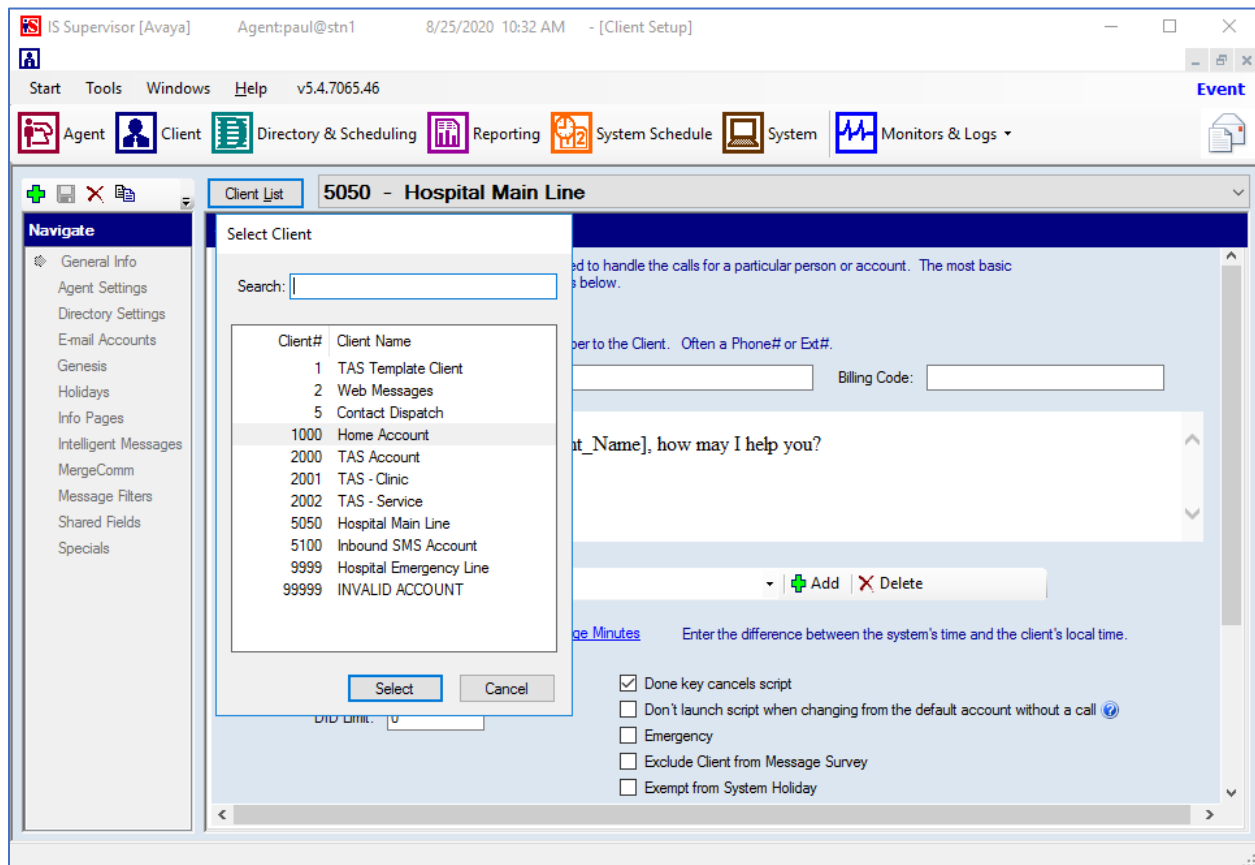
Follow reference [3] to create three agent fields for login, password, and queue, using descriptive values for Name and default values for the remaining parameters. In the compliance testing, field names of **Login**, **Password**, and **Queue** were created, as shown below.



7.3. 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, two client entries were created to correspond to the numbers associated with the VDNs in **Section 3**.



7.4. Administer IS Agents

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 for the first agent user from **Section 3**. Retain the default values in the remaining fields.

IS Supervisor [Avaya] Agent:paul@stn1 8/25/2020 10:40 AM - [Agent Setup]

Start Tools Windows Help v5.4.7065.46 Event

Agent Client Directory & Scheduling Reporting System Schedule System Monitors & Logs

16 Agents

- 1_WebAdmin
- 1_WebListing
- 1_WebUser
- agent1
- agent2
- agent3
- DEV
- Khanh
- New Agent
- Operator
- Paul
- Suprsvr
- SYSTEM
- TRAINER
- Wade
- Web

General Info Groups Login Management Shared Fields Settings

Setting up an Agent consists of assigning a login name and password and choosing various features related to call handling.

Login Name: agent1 Enter the name used to login and display on the operator screen.

Initials: at1 Enter operator initials used as operator identification on message time stamps, reports, and statistics.

Password Options

[Reset Password](#)

Record Calls ☒ Indicate if this Agent is allowed to record calls.

Auto Connect ☐

Default Client Clear

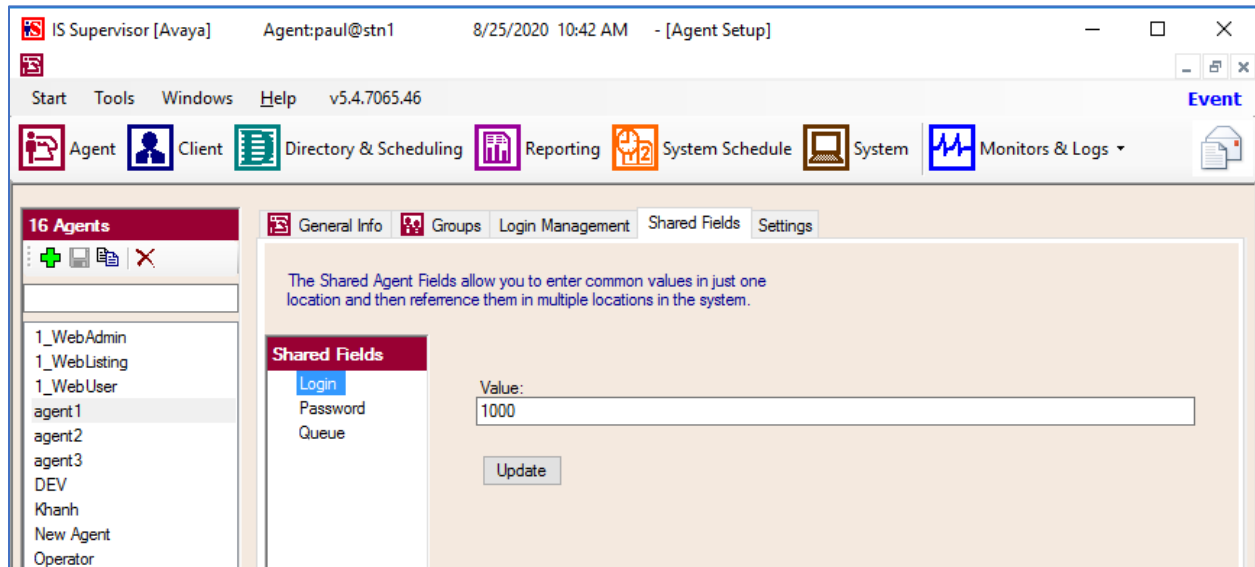
Default Directory

Select Default Directory... Clear

Subject: Not Assigned

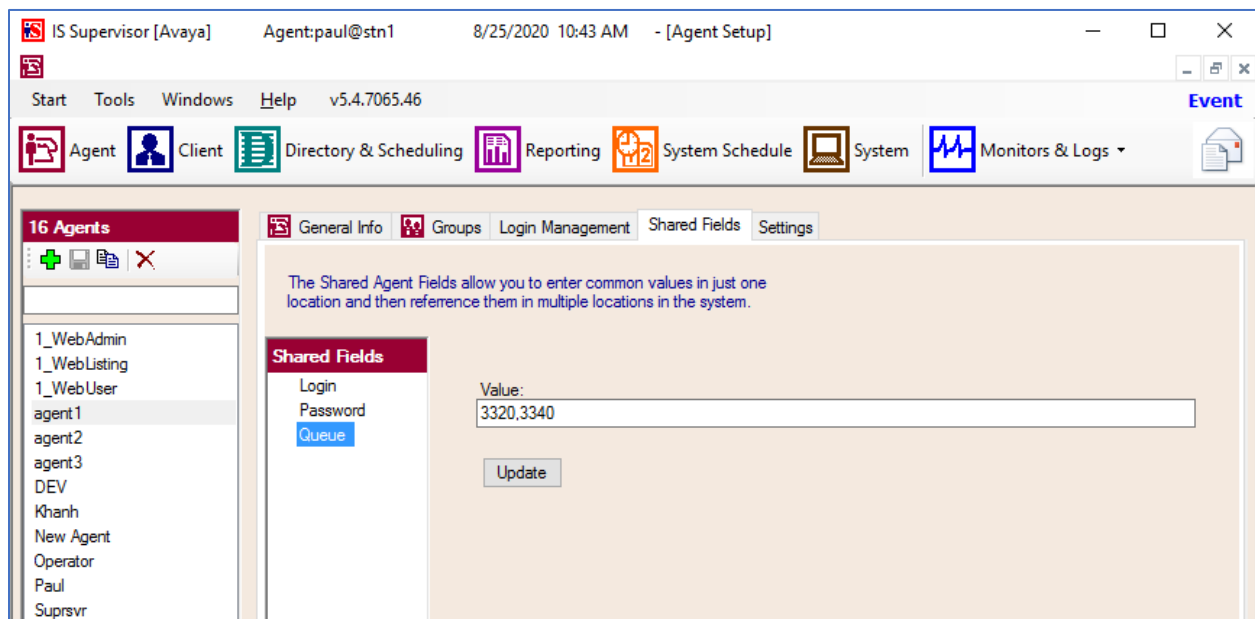
View: Not Assigned

Select the **Shared Fields** tab. For **Login** and **Password**, enter the agent ID and password respectively for the first agent from **Section 3**.



For **Queue**, enter the skill and VDN extensions from **Section 3**, separated by commas, in this case “3320,3340”.

Repeat this section to create an agent entry for each agent user in **Section 3**. In the compliance testing, two agent entries were created.

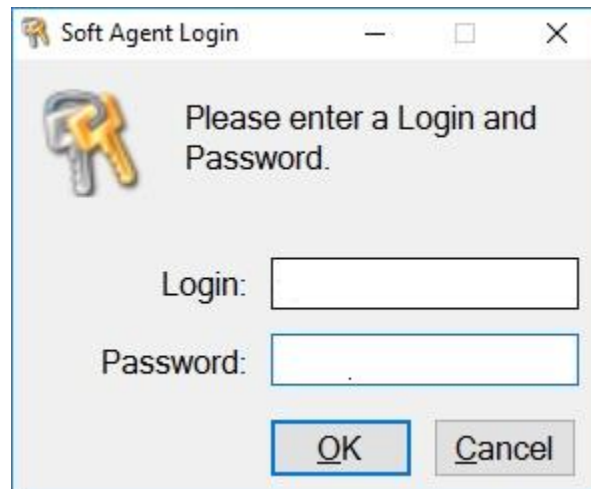


7.5. Launch Intelligent Series Soft Agent

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.



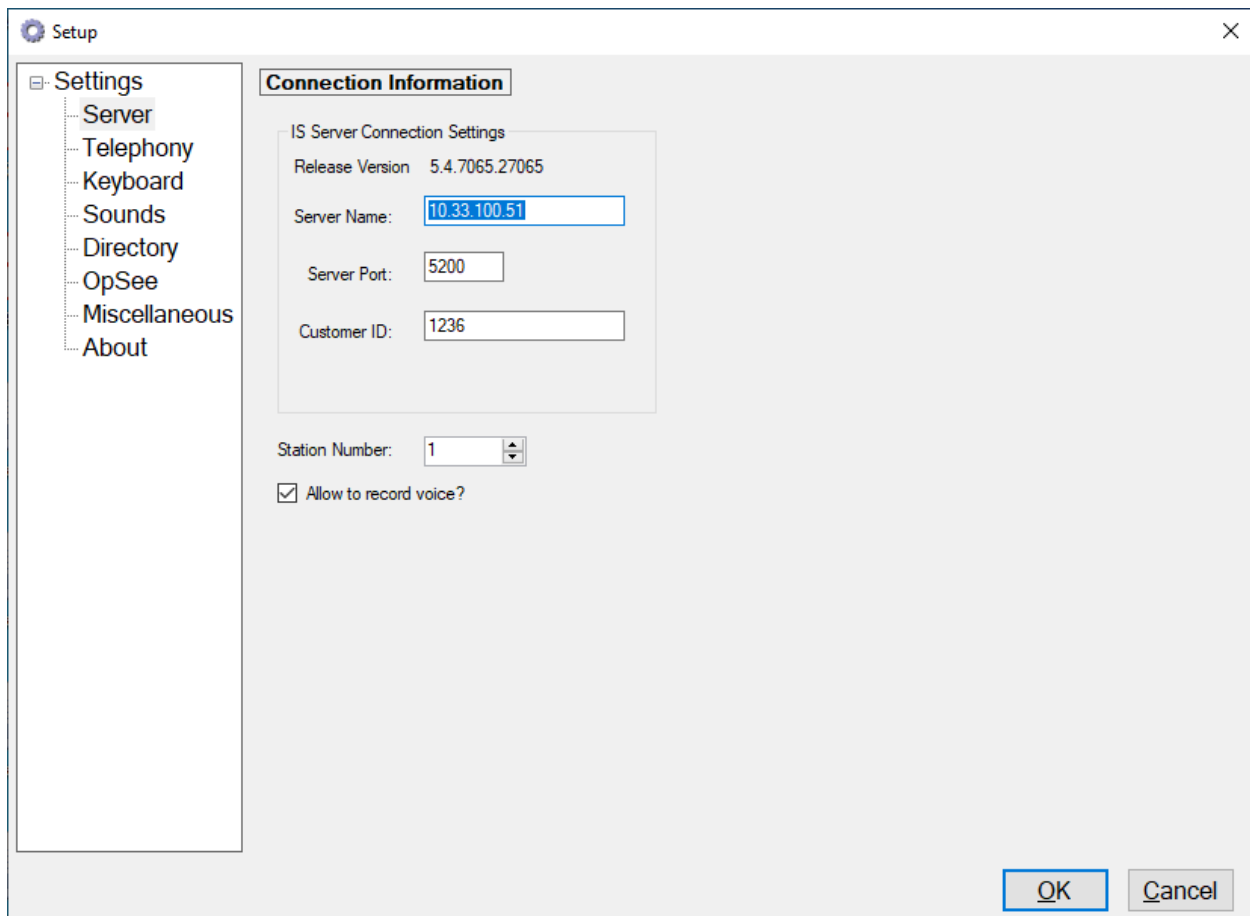
The **Soft Agent Login** screen is displayed. Press the **Ctrl** and **F12** keys together to enter setup.



7.6. 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 Soft Agent 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 “1”.
- **Allow to record voice:** Checked. To record the audio call.



The screenshot shows a Windows-style dialog box titled "Setup". On the left is a tree view with the following items: Settings (expanded), Server (selected), Telephony, Keyboard, Sounds, Directory, OpSee, 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" with the value "5.4.7065.27065", "Server Name" with the value "10.33.100.51", "Server Port" with the value "5200", and "Customer ID" with the value "1236". Below this sub-section, there is a "Station Number" field with a spinner control set to "1", and a checkbox labeled "Allow to record voice?" which is checked. At the bottom right of the dialog are "OK" and "Cancel" buttons.

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

- **Switch Type:** “Avaya DMCC – Phone”.
- **Number of appearances:** Desired number of agent appearances, in this case “2”.
- **AES Address:** IP address of Application Enablement Services server.
- **AES Port:** The DMCC unencrypted port from **Section 6.7**.
- **Switch Name:** The switch connection name from **Section 6.3**.
- **Switch Address:** IP address of the H.323 gatekeeper from **Section 6.3**.
- **User Name:** The Amtelco user credentials from **Section 6.5**.
- **Password:** The Amtelco user credentials from **Section 6.5**.

The screenshot shows the 'Setup' dialog box with the 'Telephony' tab selected in the left pane. The 'Setup options for telephone interface' section is active. The 'Switch Type' dropdown is set to 'Avaya DMCC - Phone'. The 'Use the first available appearance for dialouts?' checkbox is checked. The 'AE Server' tab is selected, showing fields for 'Number of appearances' (2), 'AES Address' (10.33.1.4), 'AES Port' (4721), 'Use SSL' (unchecked), 'Switch Name' (interopcm), 'Switch Address' (10.33.1.6), 'User Name' (test), 'Password' (test), 'Local Certificate' (empty), and 'Agent Login Fields' (Login: Login, Password: Password). The 'OK' button is highlighted.

Select the **Extension** tab, enter extension of agent and its password in the **Extension** and **Extension Password** fields.

The screenshot shows a 'Setup' window with a sidebar on the left containing a tree view with the following items: Settings, Server, Telephony (highlighted), Keyboard, Sounds, Directory, OpSee, Miscellaneous, and About. The main area is titled 'Setup options for telephone interface'. It contains a 'Switch Type' dropdown menu set to 'Avaya DMCC - Phone', a checked checkbox for 'Use the first available appearance for dialouts?', and a tabbed interface with tabs for 'AE Server', 'Extension' (selected), 'Media', 'Agent States', 'Reason Codes', and 'Features'. The 'Extension' tab contains three input fields: 'Extension' with the value '3301', 'Extension Password' with the value '1234', and 'Device Instance' with a spinner set to '1'. There is also an unchecked checkbox for 'Ignore calls not from ACD'. At the bottom right are 'OK' and 'Cancel' buttons.

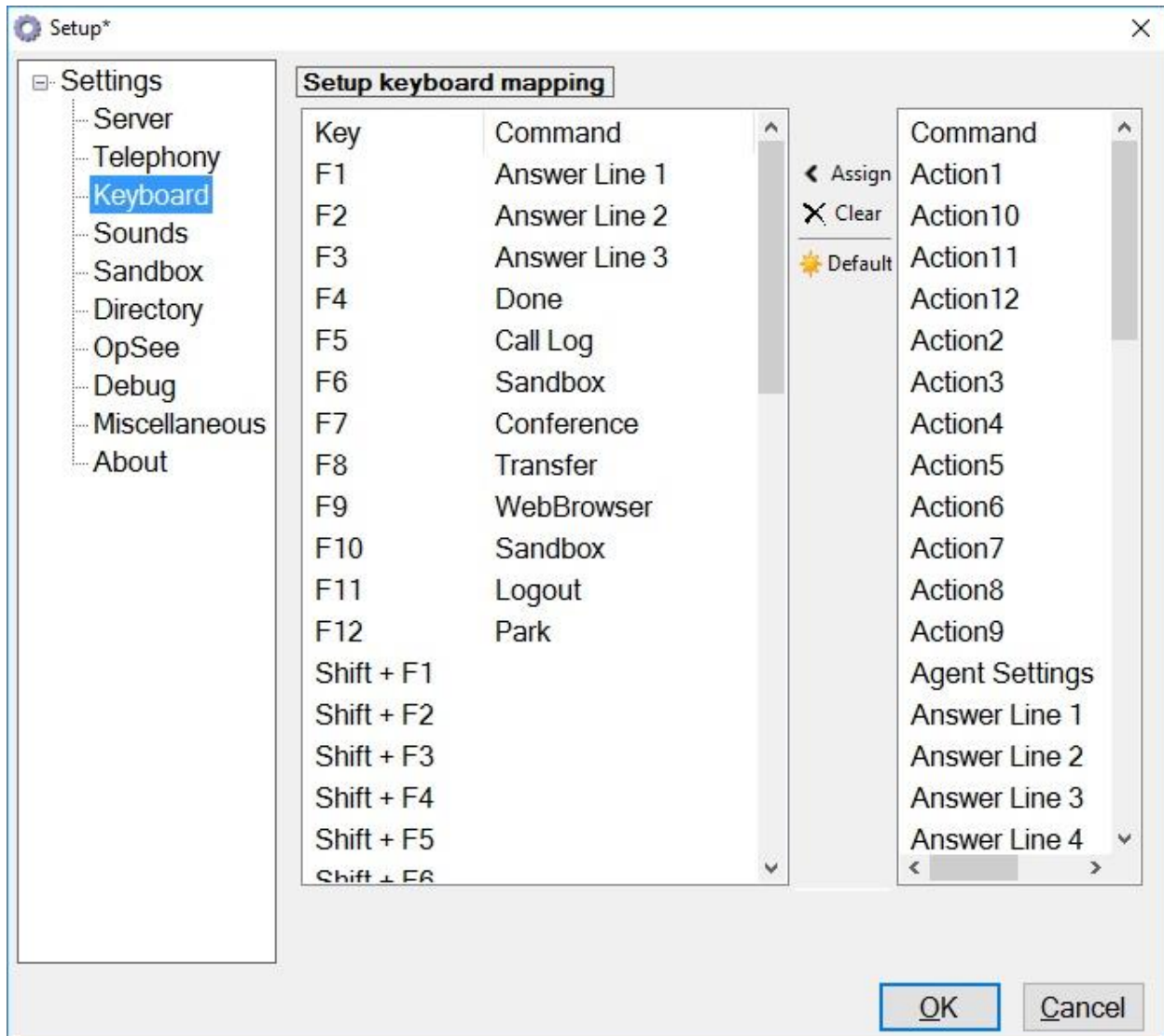
Select the **Media** tab in the right pane, to display the screen below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **RTP IP Address:** IP address of the agent PC, in this case “192.168.299.8”.
- **RTP Port:** “5000”.
- **Extension:** An available DMCC station extension from **Section 5.4**.
- **Password:** The available DMCC station security code from **Section 5.4**.

The screenshot shows a 'Setup' window with a sidebar on the left containing a tree view with the following items: Settings, Server, Telephony, Keyboard, Sounds, Directory, OpSee, Miscellaneous, and About. The 'Telephony' item is selected. The main area is titled 'Setup options for telephone interface'. It contains a 'Switch Type' dropdown menu set to 'Avaya DMCC - Phone' and a checked checkbox labeled 'Use the first available appearance for dialouts?'. Below this is a tabbed interface with tabs for 'AE Server', 'Extension', 'Media' (which is active), 'Agent States', 'Reason Codes', and 'Features'. The 'Media' tab contains several input fields: 'RTP IP Address' (192.168.199.8), 'RTP Port' (5000), a 'Perfect Answer Extension' section with 'Extension' (3372) and 'Security Code' (1234) fields, 'Speaker device' (Speakers (High Definition Audi...)), and 'Microphone device' (Microphone (High Definition Audi...)). There is also a 'Voice Assisted Transfer' section with 'Extension' and 'Security Code' fields. A note at the bottom of this section states: 'Voice Assisted Transfer also requires a RTP Address and Port to be setup above.' At the bottom right of the window are 'OK' and 'Cancel' buttons.

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 7.6** and **Section 7.7** for each agent. In the compliance testing, two agents were configured.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Soft Agent.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the registration status of DMCC stations by using the “list registered-ip-stations” command.

Verify that the DMCC stations from **Section 5.4** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS					
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address		
3371	9640	IP_API_A	10.33.1.4		
tcp	1	3.2040	10.33.1.60001/013	T00013	in-service/idle
3372	9640	IP_API_A	10.33.1.4		
tcp	1	3.2040	10.33.1.60001/013	T00013	in-service/idle

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify that the **Status** is “Talking” for the TSAPI link administered in **Section 6.4**.

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	interopcm	1	Talking	Fri Jun 19 12:50:07 2020	Online	18	3	15	15	30

Online Offline

For service-wide information, choose one of the following:

TSAPI Service Status TLink Status User Status

Verify the status of the DMCC connection by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify that there is an active session for each logged in agent to the Soft Agent application, with the corresponding **User** column reflecting the Amtelco user name from **Section 6.5**, and the corresponding **# of Associated Devices** column reflecting the number of VDNs from **Section 3**, plus the agent, plus the associated DMCC station from **Section 5.4**.

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
High Availability
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▼ Status
Alarm Viewer
▶ Logs
▶ Log Manager
▼ Status and Control
CVLAN Service Summary
DLG Services Summary
DMCC Service Summary
Switch Conn Summary
TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Sun Aug 23 14:18:28 IST 2020

Service Uptime: 190 days, 20 hours 52 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 474

Number of Existing Devices: 5

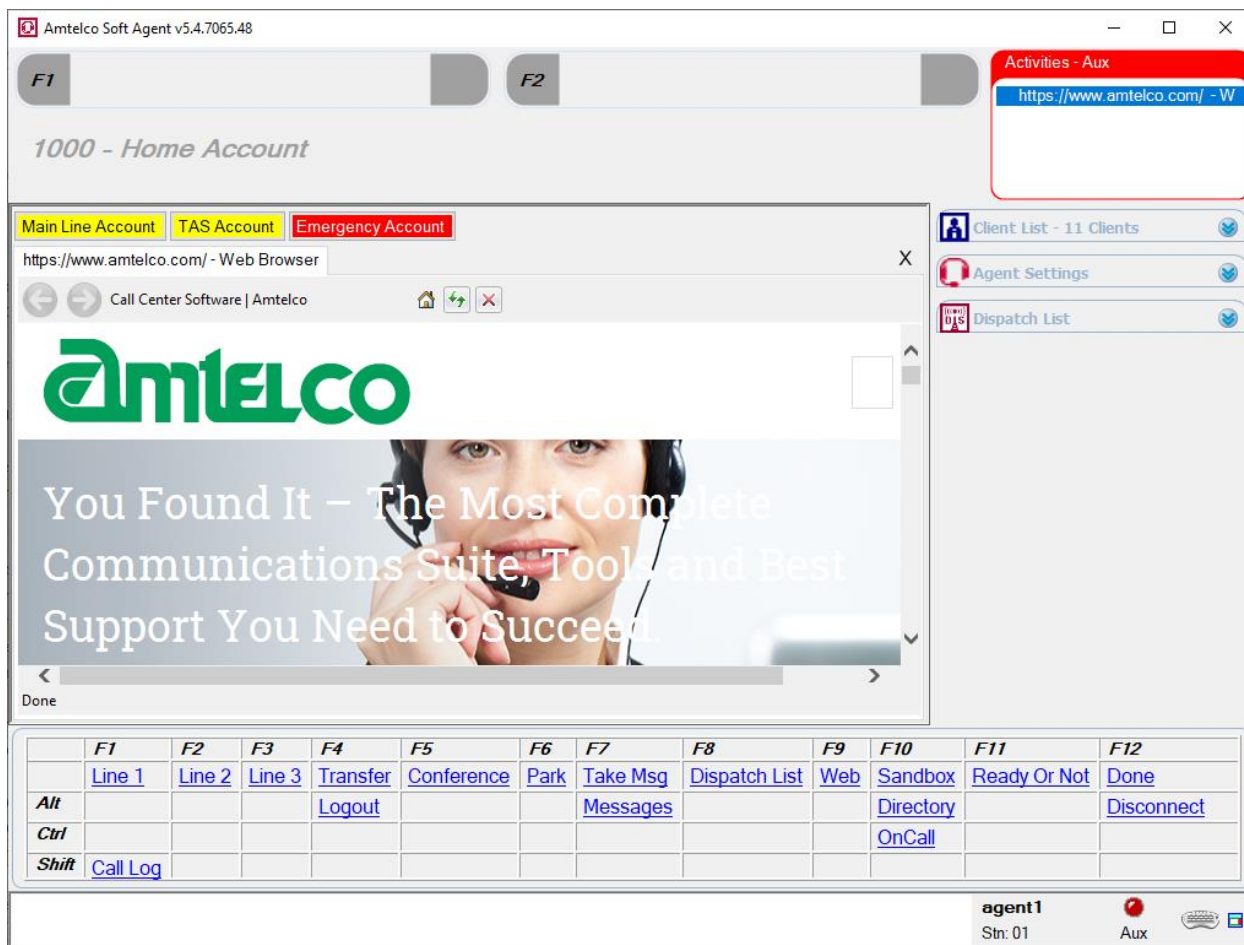
Number of Devices Created Since Service Boot: 272

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	561E21C04802FBE7A B2A5F39188FA8AE-474	test	Amtelco SoftAgent	192.168.199.200	XML Unencrypted	3
<input type="checkbox"/>	AE145238F5CC5756F 2A2EBCCC16CE4BB-473	test	Amtelco SoftAgent	10.33.100.51	XML Unencrypted	3

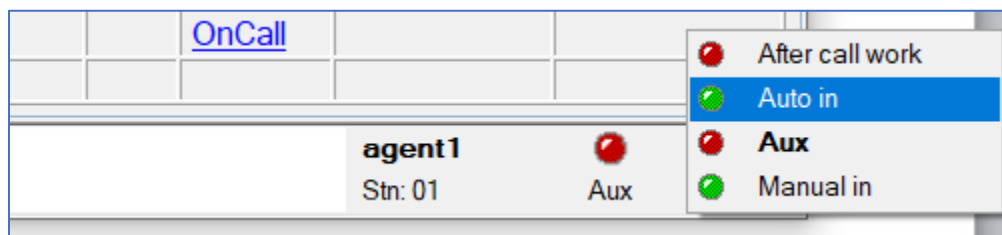
Item 1-2 of 2

8.3. Verify Amtelco Intelligent Soft Agent

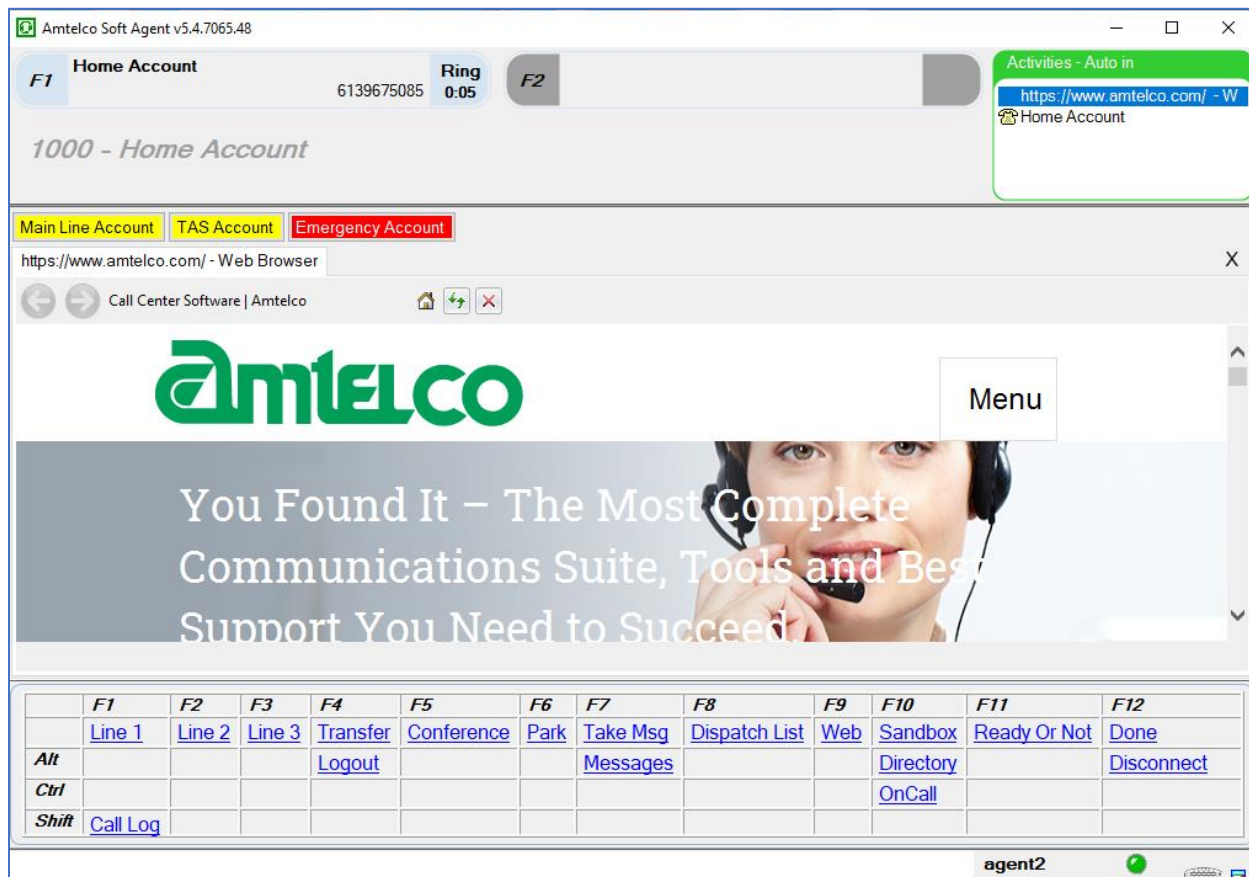
From the agent PC, follow the procedure in **Section 7.5** to launch the Intelligent Series Soft Agent and log in with the appropriate credentials from **Section 7.4**. The **Amtelco Soft Agent** screen below is displayed.



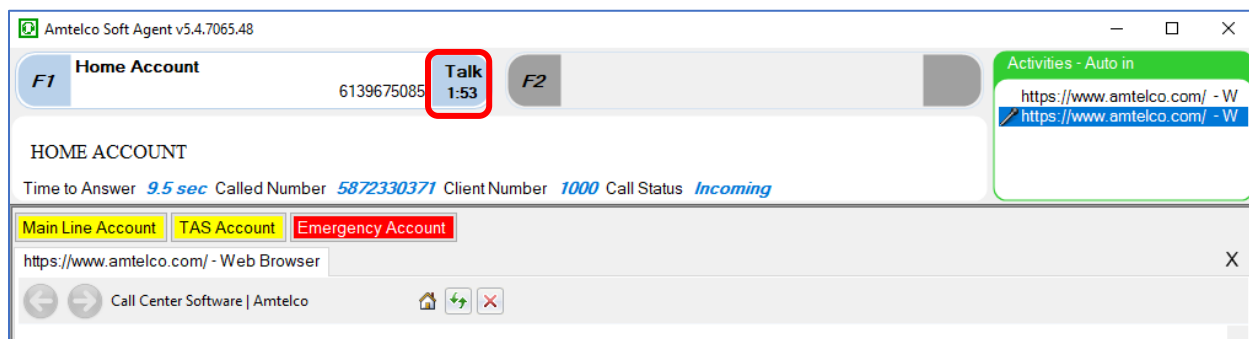
In the lower right portion of the screen, right click on **Aux** and select a desired available state, such as **Auto in**.



Make an incoming call from PSTN to a monitored VDN. Verify that the call is ringing at the available agent station, and that the agent screen is updated to reflect a ringing call along with the calling party number and the called client name, as shown below. In this case, the calling party number is **9089532103**, and the called client name is **Amtelco Main Line**. Press the **F1** key or click in the applicable call line area highlighted below to answer the call.



Verify that the agent telephone is connected to the PSTN with two-way talk paths, and that the applicable perfect answer greeting is played back. Also verify that the agent screen is updated to reflect the **Talk** state, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Amtelco Intelligent Soft Agent 5.4 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. All feature and serviceability test cases were completed with observations noted in Section 2.2.

10. Additional References

This section is optional. Other Application Notes or product documentation may be listed here with Avaya documents listed first followed by other vendor's documents.

- [1] Administering Avaya Aura® Application Enablement Services, Document 03-300509, Issue 10, Release 8.1, August 2019
- [2] Administering Avaya Aura® System Manager, Issue 9.0, Release 8.1, August 2019
- [3] Administering Avaya Aura® Communication Manager, Document 03-300509, Issue 10, Release 8.1, August 2019
- [4] Avaya Aura® Communication Manager Feature Description and Implementation, Document 555-245-205, Issue 9.0, Release 8.1, August 2019
- [5] Soft Agent User Reference Guide, May 2016, available at <https://service.amtelco.com/doclib/library.htm>.

©2020 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.