



Avaya Solution & Interoperability Test Lab

Application Notes for Amtelco Intelligent Soft Agent 5.0 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Amtelco Intelligent Soft Agent 5.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0.

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 Communication Manager to provide screen pop, agent state change, and call control capabilities from the agent desktops.

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 Intelligent Soft Agent (Soft Agent) 5.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0.

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 Announcement feature on Soft Agent, a virtual DMCC station is created on Communication Manager for each agent, for play back of pre-recorded announcements 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 announcement. 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 announcement.

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.

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 announcement.
- 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.

- There were several issues encountered with the call recording optional feature. There were some scenarios where call legs were not recorded. Customers intending to use this optional feature should consult with Amtelco to understand its limitations and for required configuration.
- 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 Soft Agent can be obtained through the following:

- **Phone:** (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	60001, 60002
Agent Station	65001, 65002

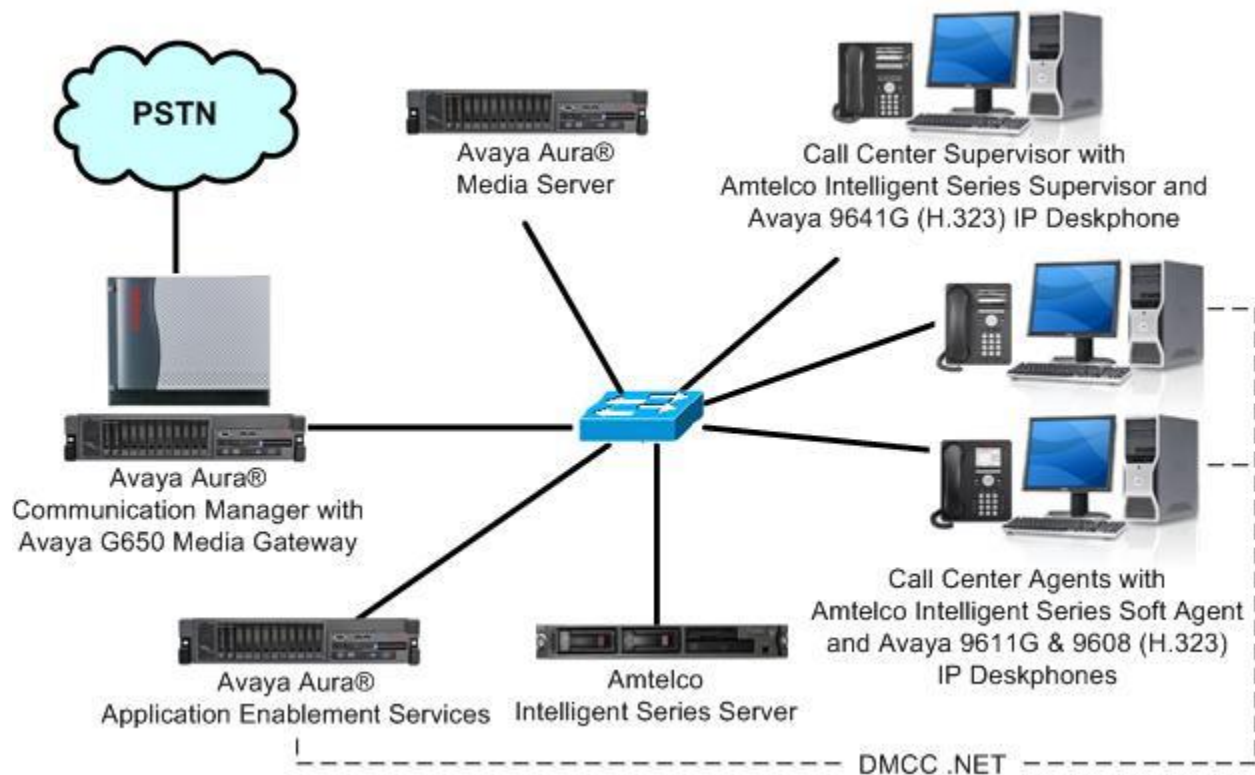


Figure 1: Compliance Testing Configuration

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	7.0.1.1 (7.0.1.1.0.441.23169)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.2.15-0)
Avaya 9608, 9611G, 9641G IP Deskphones (H.323)	6.6302
Amtelco Intelligent Series Server on Microsoft Windows Server 2008 R2 Enterprise <ul style="list-style-type: none">Microsoft SQL Server 2014	5.0.6291.16498 SP1 12.0.2000.8
Amtelco Intelligent Series Supervisor on Microsoft Windows 10 Pro	5.0.6263.7
Amtelco Intelligent Series Soft Agent on Microsoft Windows 10 Pro <ul style="list-style-type: none">Avaya DMCC .NET (ServiceProvider.dll)	5.0.6263.09 6.2.0.29

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 IP codec set
- Administer DMCC stations

5.1. Verify License

Log in to the System Access Terminal 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 to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. 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? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	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	

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: 60111		
Type: ADJ-IP		
COR: 1		
Name: AES CTI Link		

5.3. 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.711 is included, which is the only codec supported by Soft Agent.

For **Media Encryption**, make certain “none” is included, as required for Soft Agent.

In the 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 Codec Set

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 SRTCP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
5:
```


5.4. 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 “9620”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 5
STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 9620	Security Code: 123456	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Amtelco DMCC 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests: y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 65991	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	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 65991 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65991	S00131	Amtelco DMCC 1				1			
	9620		no			1			
65992	S00140	Amtelco DMCC 2				1			
	9620		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 OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer Amtelco user
- Administer security database
- Administer ports
- Restart services

6.1. Launch OAM Interface

Access the OAM 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" and "Management Console" is displayed. Below this is a red horizontal bar. The main content area contains a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are "Login" and "Reset" buttons. At the bottom of the page, below another red horizontal bar, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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 red navigation bar at the top contains "Home", "Help", and "Logout". On the left, a sidebar menu lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, which explains that the OAM Web provides tools for managing the AE Server and lists administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be served by a single administrator or separate administrators.

Welcome: User
Last login: Tue Mar 21 12:10:24 2017 from 192.168.200.201
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Mar 21 13:19:11 EDT 2017
HA Status: Not Configured

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 Avaya Application Enablement Services Management Console with the "Licensing" section selected in the sidebar. The main content area displays the "Licensing" message, which provides instructions on how to set up and maintain the WebLM, import and set up the license, and administer TSAPI Reserved Licenses or DMCC Reserved Licenses. It lists the following steps: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

Welcome: User
Last login: Tue Mar 21 12:10:24 2017 from 192.168.200.201
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Mar 21 13:19:11 EDT 2017
HA Status: Not Configured

Licensing | **Home** | **Help** | **Logout**

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

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

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** and **Device Media and Call Control**, as shown below. Note that the TSAPI license was used for agent monitoring and call control via DMCC, and the DMCC license was used for the virtual DMCC stations.

AVAYA

Aura® System Manager 7.0

Last Logged on at March

Home

Licenses

WebLM Home

Install license

Licensed products

APPL_ENAB

Application Enablement

View license capacity

View peak usage

COMMUNICATION_MANAGER

Communication_Manager

Call_Center

Configure Centralized Licensing

MSR

Media_Server

SessionManager

SessionManager

Uninstall license

Server properties

Shortcuts

Help for Installed Product

Application Enablement (CTI) - Release: 7 - SID: 10503000

Stan

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: October 12, 2015 2:21:49 PM -05:00

License File Host IDs: V1-19-37-80-8F-BF

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted; DMCUnrestricted; 1XM_001, BasicUnrestricted; DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES CCE_001, BasicUnrestricted, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnre CSI_T2_001, BasicUnrestricted, AdvancedUnre AVAYAVERINT_001, BasicUnrestricted, Advanc DMCUnrestricted; CCT_ELITE_CALL_CTRL_00; AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000

6.3. 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 Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes 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 next.

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 "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. Each field has a dropdown menu. The "Link" field is set to 1, "Switch Connection" is set to cm7, "Switch CTI Link Number" is set to 1, "ASAI Link Version" is set to 7, and "Security" is set to Unencrypted. Below the fields are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' expanded, with 'Switch Connections' selected. The main area displays the 'Switch Connections' screen. At the top right, a welcome message for 'User' is shown, including login details and system status. Below this, a table lists switch connections. The 'cm7' connection is selected with a radio button. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - cm7' screen. The left navigation pane is the same as the previous screenshot. The main area shows a form with a text input field containing '10.64.101.236' and an 'Add Name or IP' button. Below the input field is a 'Name or IP Address' label and two buttons: 'Delete IP' and 'Back'.

6.5. Administer Amtelco 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Mar 21 12:10:24 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Mar 21 13:19:11 EDT 2017
HA Status: Not Configured

User Management | User Admin | Add UserHome | 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

Add User

Fields marked with * can not be empty.

* User Idamtelco

* Common Nameamtelco

* Surnameamtelco

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.6. Administer 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. Uncheck both fields below.

In the event that the parameters are enabled with security database used by the customer, then follow reference [2] to configure access privileges for the Amtelco user from **Section 6.5**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "Security" expanded, leading to "Security Database" and then "Control". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Mar 21 12:10:24 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Mar 21 13:19:11 EDT 2017
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
▶ High Availability
▶ Licensing
▶ Maintenance
▶ Networking
▼ Security
 ▶ Account Management
 ▶ Audit
 ▶ Certificate Management
 Enterprise Directory
 ▶ Host AA
 ▶ PAM
 ▼ Security Database
 ▪ Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
Apply Changes

6.7. Administer Ports

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 Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Mar 21 12:10:24 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Mar 21 13:19:11 EDT 2017
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port

9999

Enabled Disabled

☒ ☐

Encrypted TCP Port

9998

☒ ☐

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port

450

Enabled Disabled

☒ ☐

Local TLINK Ports

TCP Port Min

1024

TCP Port Max

1039

Unencrypted TLINK Ports

TCP Port Min

1050

TCP Port Max

1065

Encrypted TLINK Ports

TCP Port Min

1066

TCP Port Max

1081

DMCC Server Ports

Unencrypted Port

4721

Enabled Disabled

☒ ☐

Encrypted Port

4722

☒ ☐

TR/87 Port

4723

☐ ☒

6.8. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and click **Restart Service**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Mar 21 12:10:24 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Mar 21 13:19:11 EDT 2017
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" 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 checked="" type="checkbox"/> TSAPI Service	Running

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

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

7. Configure Amtelco Intelligent Soft Agent

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

- Launch Intelligent Series Supervisor
- Administer system
- Administer client
- Administer agent
- Launch Intelligent Series Soft Agent
- Administer setup

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

In addition to the shown procedural steps, the application also requires an IS server and a configuration profile to be configured by following reference [3].

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 the Intelligent Series Supervisor installation.

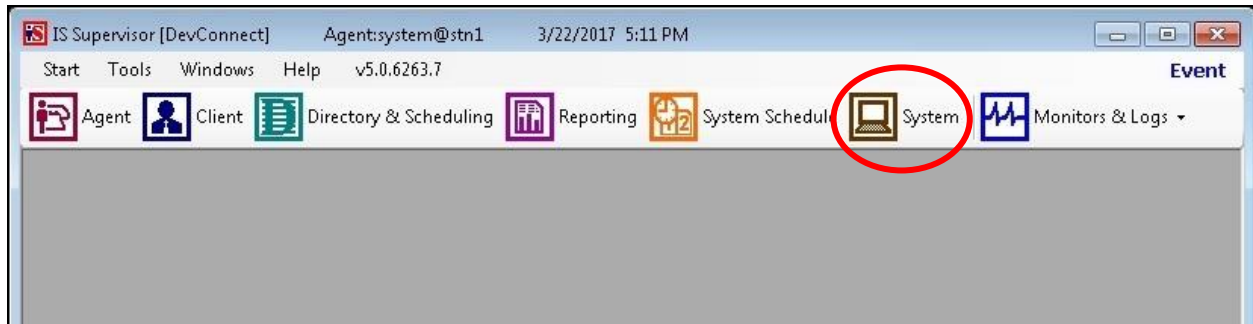


The **Supervisor Login** screen is displayed. Log in using the appropriate credentials.



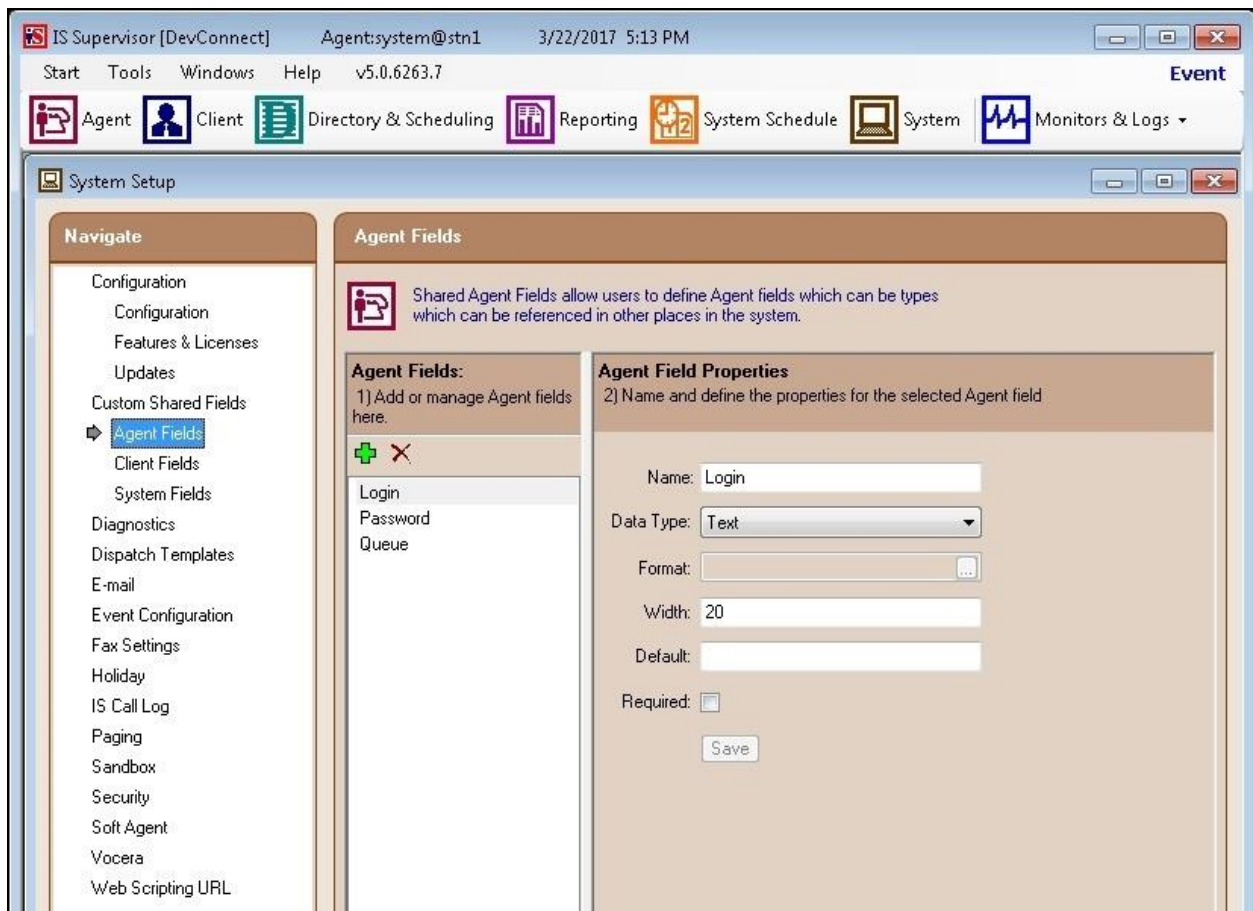
7.2. Administer System

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.

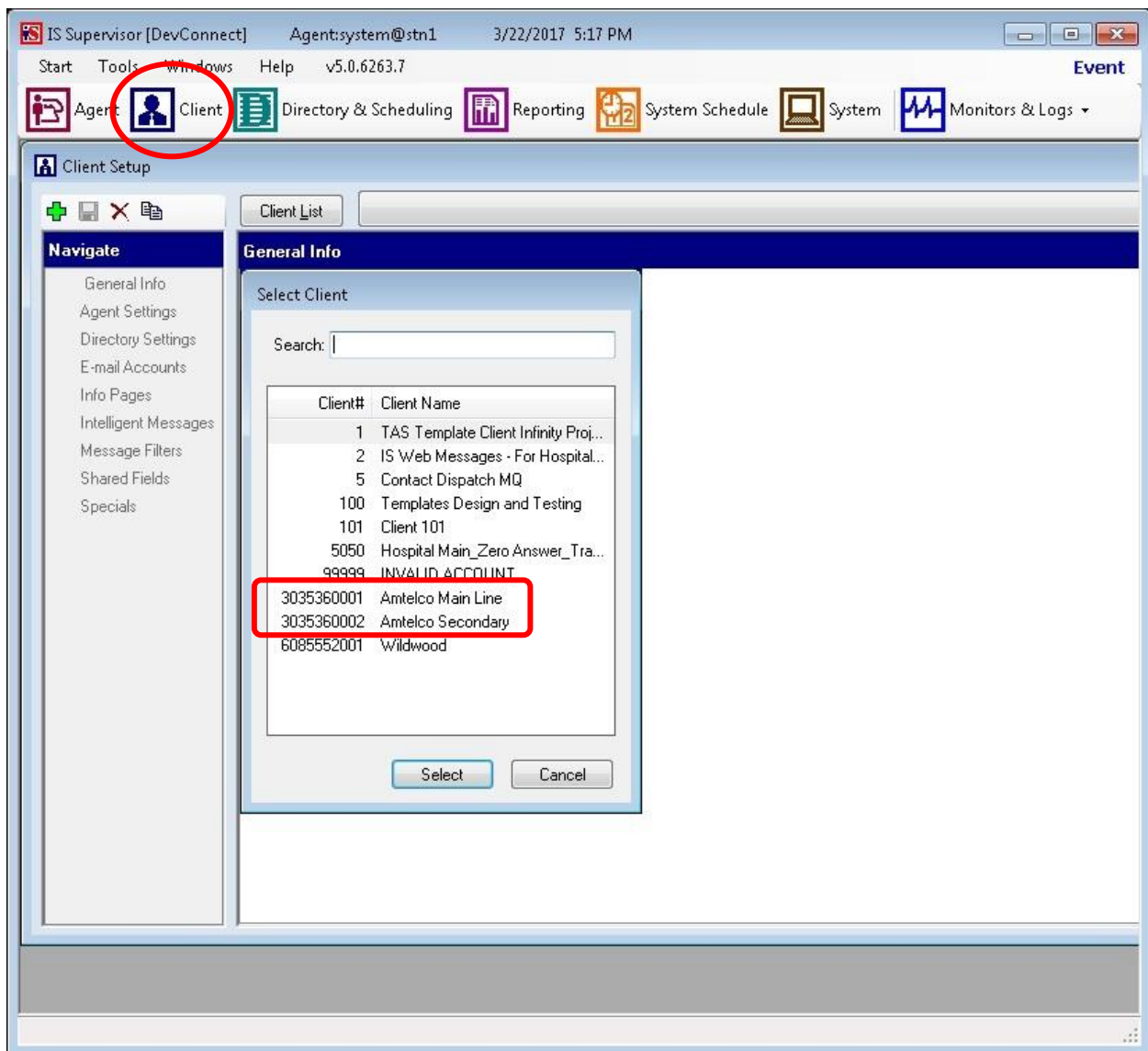
Follow reference [3] to create three agent fields for login, password, and queue, using descriptive values for **Name** and default values for the remaining parameters. In the compliance testing, field names of **Login**, **Password**, and **Queue** were created, as shown below.



7.3. Administer Client

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

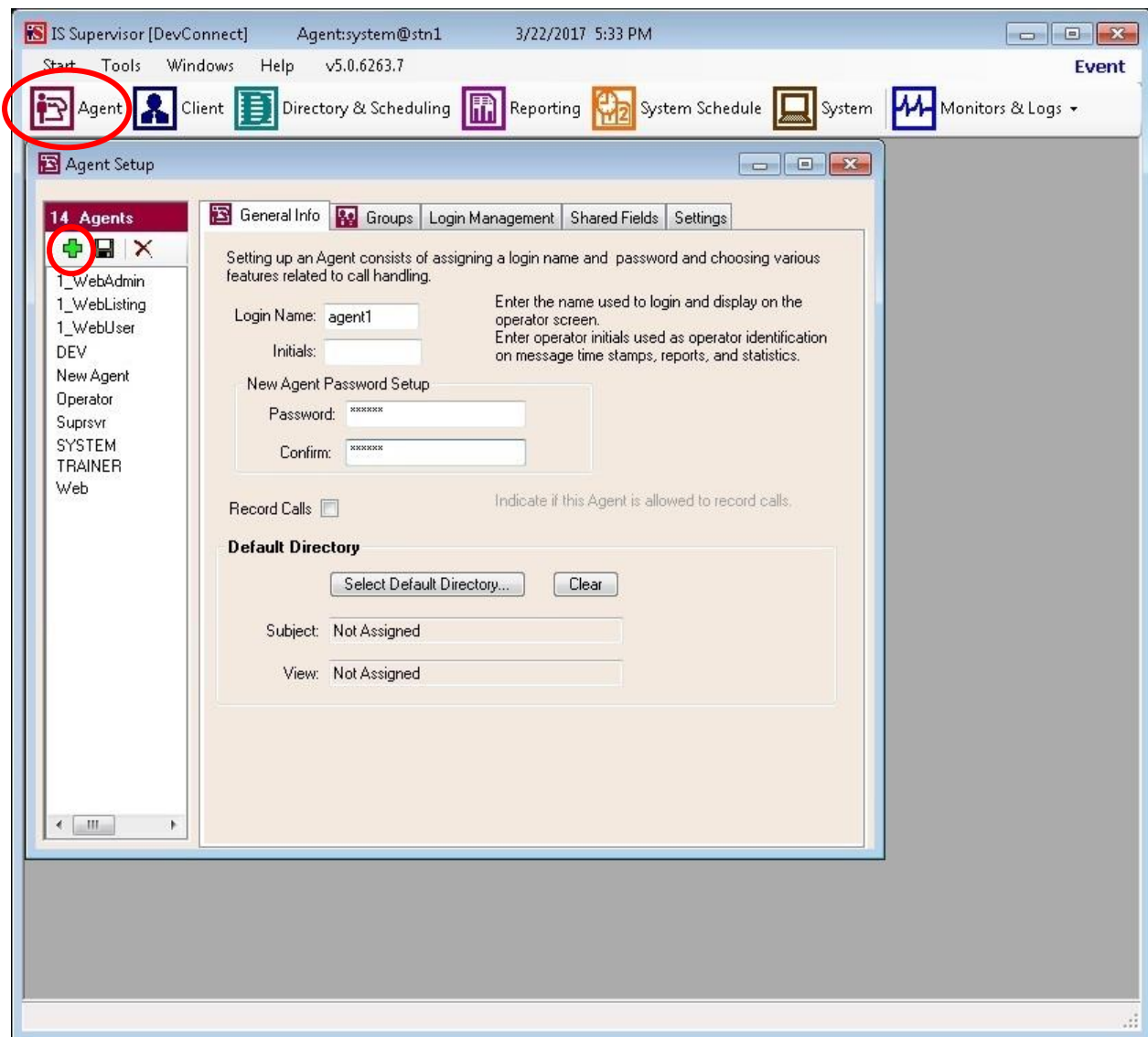
Follow reference [3] to create desired client entries to associate with called numbers for the customer network. In the compliance testing, two client entries were created to correspond to the full PSTN numbers associated with the VDNs in **Section 3**.



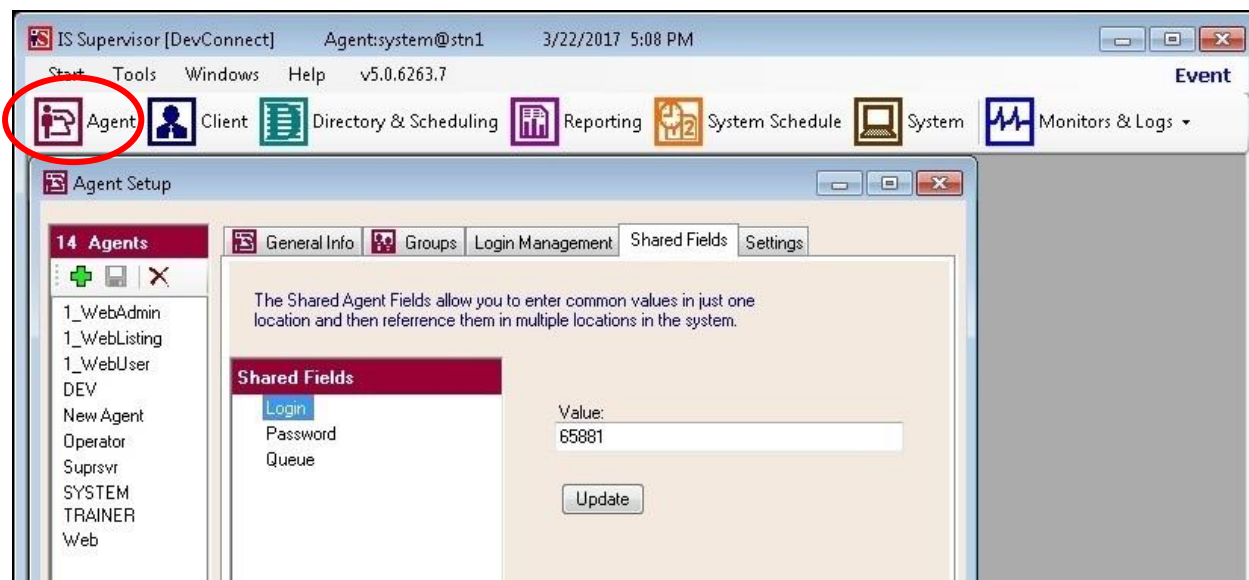
7.4. Administer Agent

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

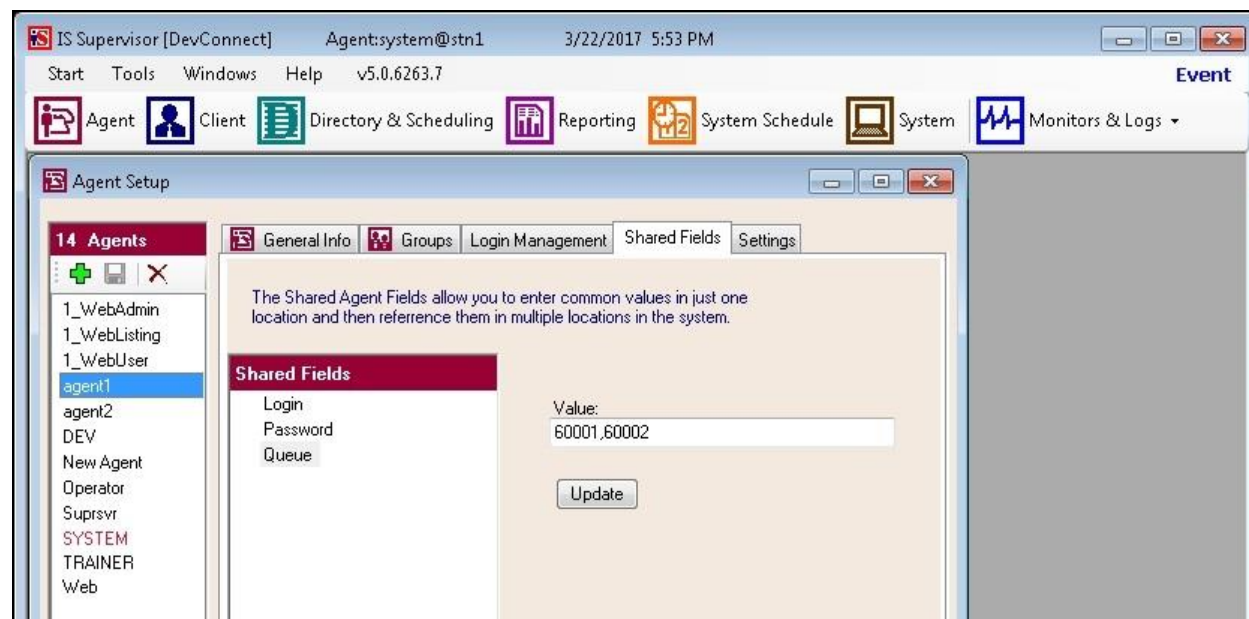


Select the **Shared Fields** tab. For **Login** and **Password**, enter the agent ID and password respectively for the first agent from **Section 3**.



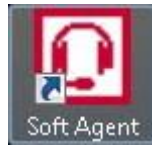
For **Queue**, enter the VDN extensions from **Section 3**, separated by commas, in this case “60001,60002”.

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

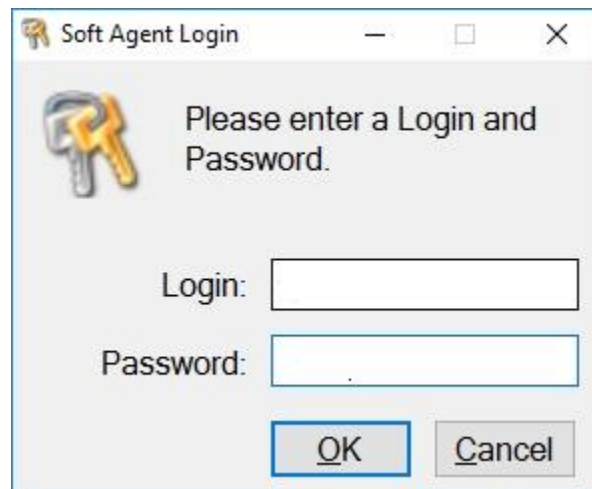


7.5. Launch Intelligent Series Soft Agent

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



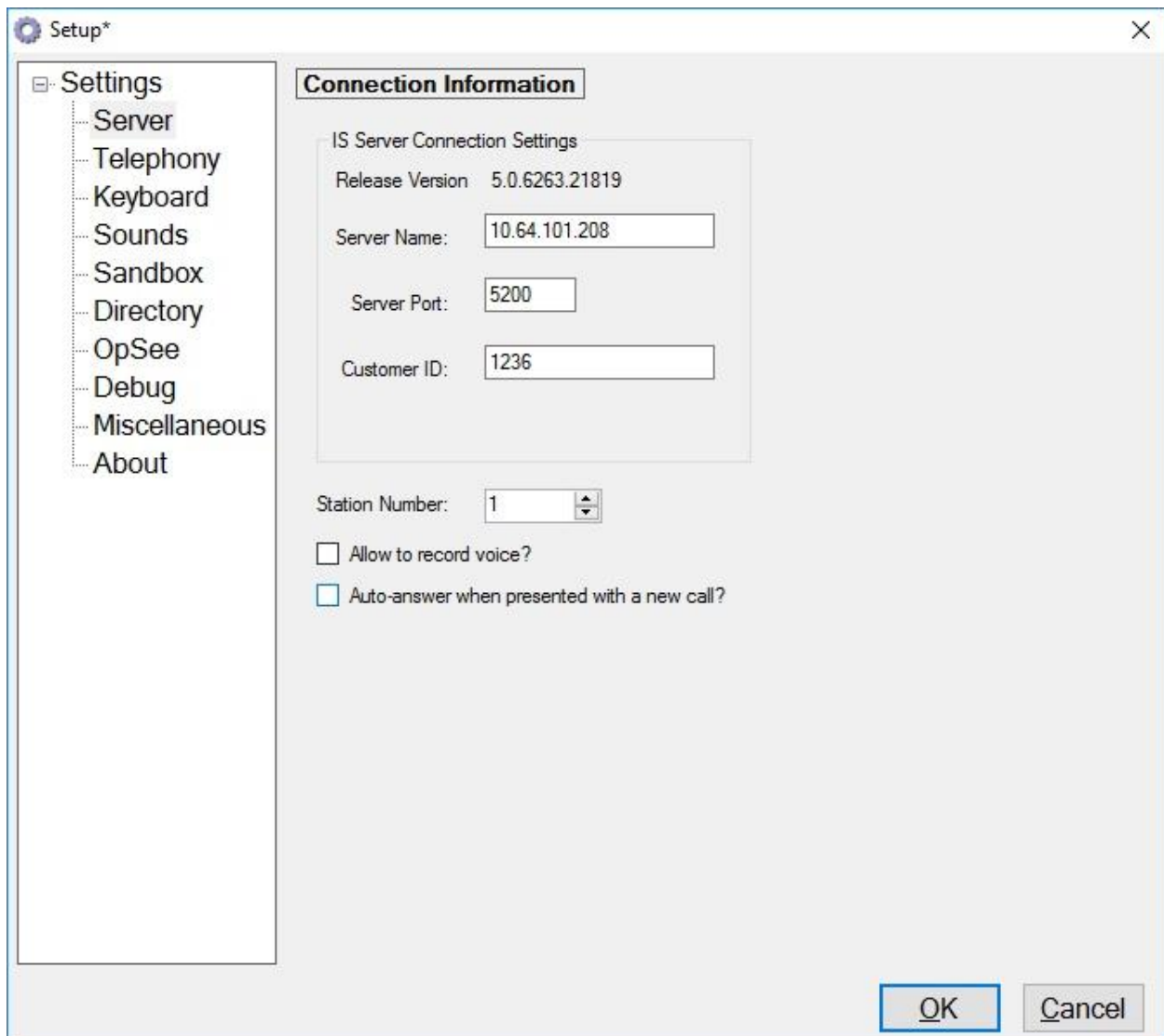
The **Soft Agent Login** screen is displayed. Press the **Ctrl** and **F12** keys together to enter setup.



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 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 “1”.



The screenshot shows a Windows-style dialog box titled "Setup*". On the left is a tree view with the following items: Settings (expanded), Server, Telephony, Keyboard, Sounds, Sandbox, Directory, OpSee, Debug, Miscellaneous, and About. The "Server" item is selected. The main area of the dialog is titled "Connection Information". Inside this area, there is a sub-section titled "IS Server Connection Settings" which contains the following fields: "Release Version" (5.0.6263.21819), "Server Name" (10.64.101.208), "Server Port" (5200), and "Customer ID" (1236). Below this sub-section, there is a "Station Number" field with a spinner box set to "1". At the bottom of the "Connection Information" section, there are two checkboxes: "Allow to record voice?" (unchecked) and "Auto-answer when presented with a new call?" (unchecked). 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 “3”.
- **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 6.4**.
- **User Name:** The Amtelco user credentials from **Section 6.5**.
- **Password:** The Amtelco user credentials from **Section 6.5**.
- **Extension:** The applicable agent station extension from **Section 3**.
- **Agent Login Fields:** The corresponding agent field names from **Section 7.2**.

Setup*

Settings

- Server
- Telephony**
- Keyboard
- Sounds
- Sandbox
- Directory
- OpSee
- Debug
- Miscellaneous
- About

Setup options for telephone interface

Switch Type: Avaya DMCC - Phone

☒ Use the first available appearance for dialouts?
☐ Notify agent when not available for 15 seconds?

AE Server | Media

Number of appearances: 3

AES Address: 10.64.101.239

AES Port: 4721

☐ Use SSL

Switch Name: cm7

Switch Address: 10.64.101.236

User Name: amtelco

Password: Amtelco123;

Local Certificate:

Extension: 65001

Extension Password:

Agent Login Fields

Login: Login

Password: Password

Queue Extensions: Queue

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 “192.168.200.20”.
- **RTP Port:** “4000”
- **Extension:** An available DMCC station extension from **Section 5.4**.
- **Password:** The available DMCC station security code from **Section 5.4**.

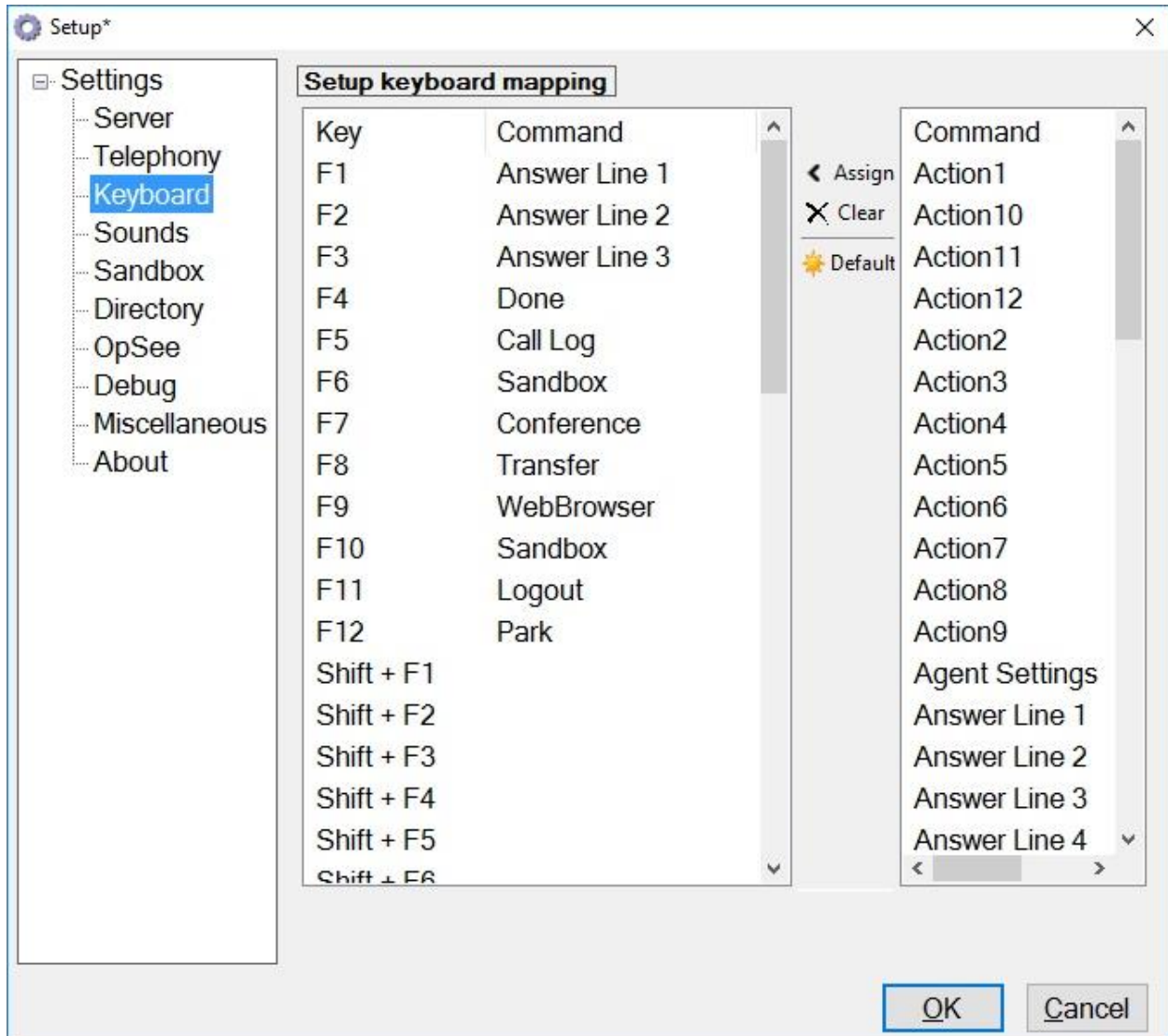
The screenshot shows a 'Setup' window with a sidebar on the left containing a tree view of settings categories: Settings, Server, Telephony, Keyboard, Sounds, Sandbox, Directory, OpSee, Debug, Miscellaneous, and About. The 'Telephony' category is expanded, and the 'Media' tab is selected. The main area is titled 'Setup options for telephone interface'. It contains a 'Switch Type' dropdown menu set to 'Avaya DMCC - Phone'. Below this are two checkboxes: 'Use the first available appearance for dialouts?' (checked) and 'Notify agent when not available for' (unchecked) with a value of '15' seconds. The 'Media' tab is active, showing fields for 'RTP IP Address' (192.168.200.20), 'RTP Port' (4000), 'Perfect Answer Extension' (65991), and 'Password' (123456). At the bottom, there are 'Speaker device' and 'Microphone device' dropdown menus, both set to 'Default'. 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Switch Type	Avaya DMCC - Phone
Use the first available appearance for dialouts?	Checked
Notify agent when not available for	15 seconds
RTP IP Address	192.168.200.20
RTP Port	4000
Perfect Answer Extension	65991
Password	123456
Speaker device	Default
Microphone device	Default

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.

In addition, follow reference [3] to record the agent's perfect answer greeting for each applicable client number.

Repeat **Section 7.5** and **Section 7.6** for each agent in **Section 3**. 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	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Skt Gatekeeper IP Address		
65000	9641	IP_Phone	tls	192.168.200.186	
	1	6.6302		10.64.101.236	
65001	9611	IP_Phone	tls	192.168.200.137	
	1	6.6302		10.64.101.236	
65002	9608	IP_Phone	tls	192.168.200.104	
	1	6.6302		10.64.101.236	
65991	9620	IP_API_A	tcp	10.64.101.239	
	1	3.2040		10.64.101.236	
65992	9620	IP_API_A	tcp	10.64.101.239	
	1	3.2040		10.64.101.236	

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 6.3**, and that the **Associations** column reflects the total number of monitored VDNs and agent stations from **Section 3**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Mon Apr 24 10:15:37 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Mon Apr 24 10:37:31 EDT 2017
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ 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	cm7	1	Talking	Tue Apr 4 13:35:52 2017	Online	17	4	62	81	30

OnlineOffline

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

TSAPI Service StatusTLINK StatusUser 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 7.6**.

Application Enablement Services
 Management Console

Welcome: User
 Last login: Mon Apr 24 10:15:37 2017 from 192.168.200.20
 Number of prior failed login attempts: 0
 HostName/IP: aes7/10.64.101.239
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.1.0.2.15-0
 Server Date and Time: Mon Apr 24 10:52:39 EDT 2017
 HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ **DMCC Service Summary**

■ Switch Conn Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

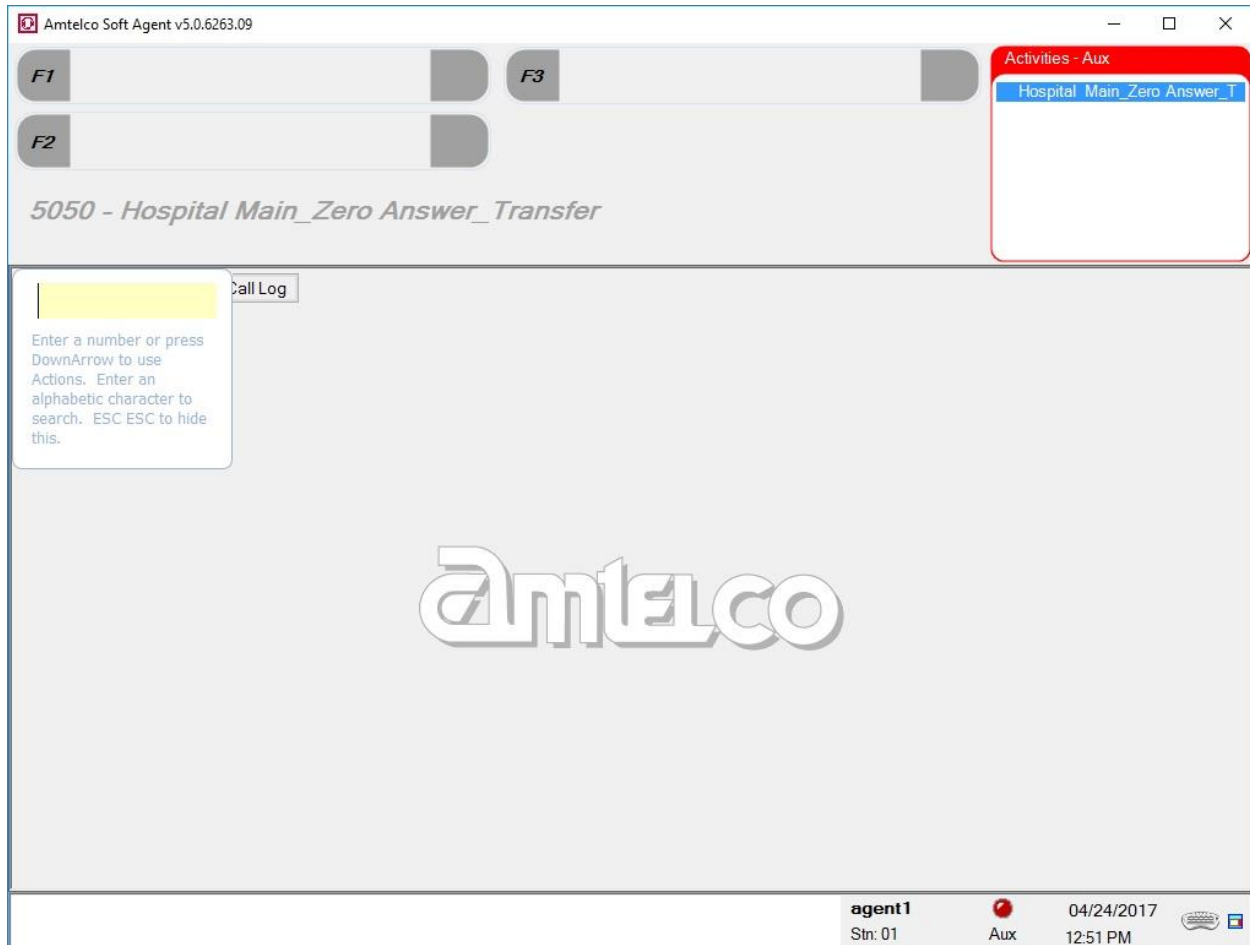
Session Summary [Device Summary](#)
 Generated on Mon Apr 24 10:38:59 EDT 2017
 Service Uptime: 26 days, 23 hours 57 minutes
 Number of Active Sessions: 2
 Number of Sessions Created Since Service Boot: 89
 Number of Existing Devices: 6
 Number of Devices Created Since Service Boot: 176

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	234EC4A44FD0C7E52 C9962EB11B167B9-87	amtelco	Amtelco SoftAgent	192.168.200.20	XML Unencrypted	4
<input type="checkbox"/>	F89B83F7A17A6E125 1A1DF447C8816DD-88	amtelco	Amtelco SoftAgent	10.64.101.200	XML Unencrypted	4

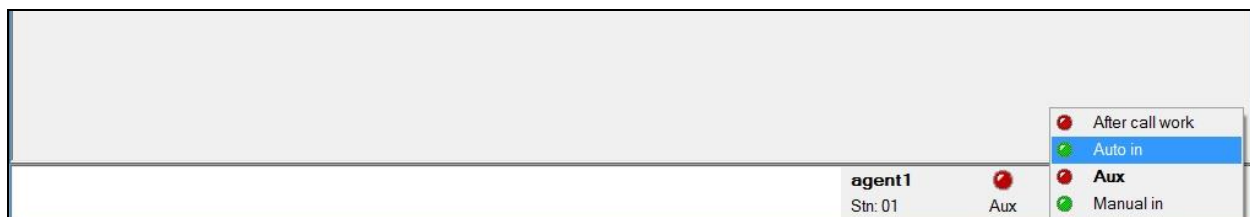
Terminate Sessions
Show Terminated Sessions

8.3. Verify Amtelco Intelligent Soft Agent

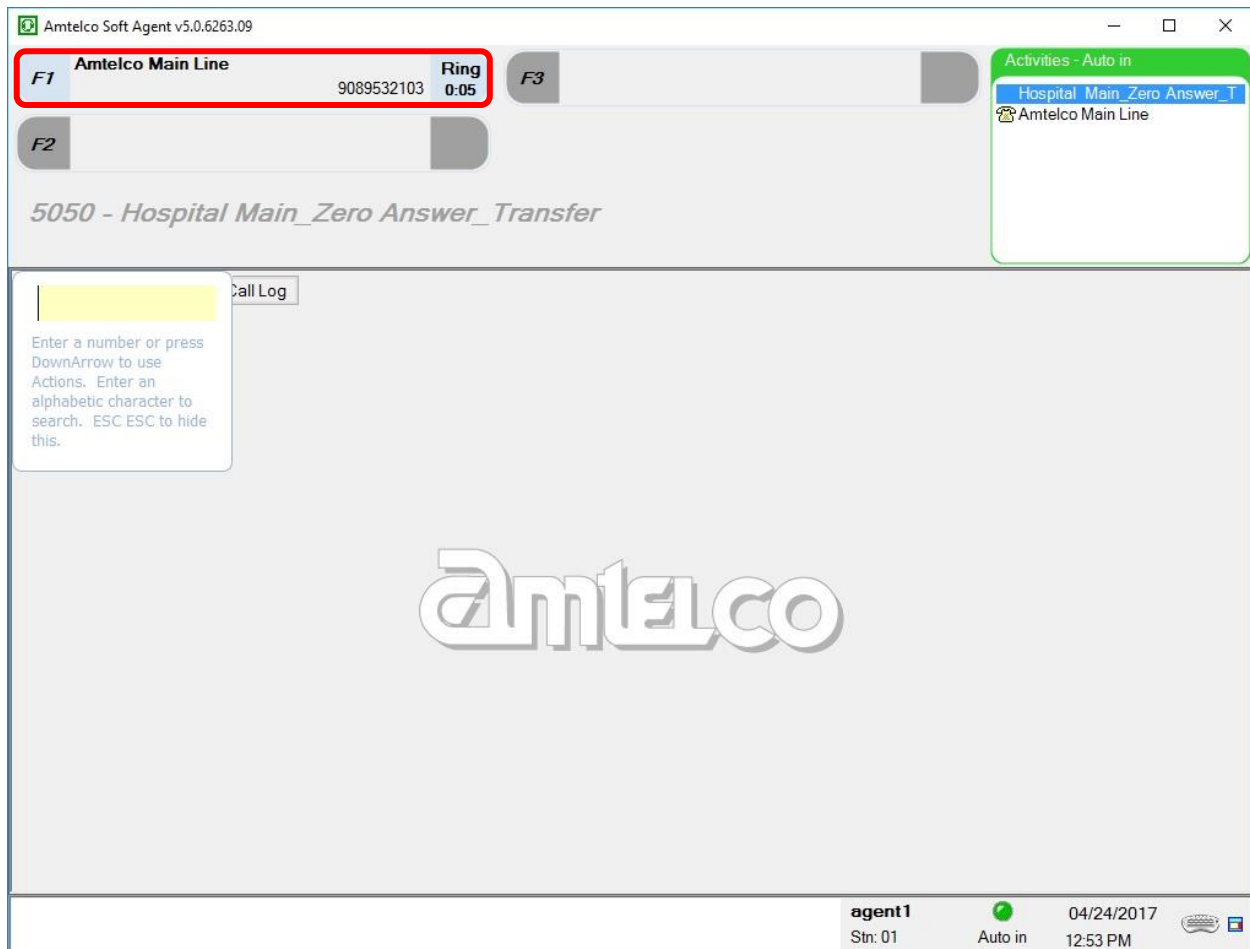
From the agent PC, follow the procedure in **Section 7.5** to launch the Intelligent Series Soft Agent and log in with the appropriate credentials from **Section 7.4**. The **Amtelco Soft Agent** screen below is displayed.



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 5.0 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at <http://support.avaya.com>.
3. *System Setup Supervisor Reference Guide*, March 2017, available at <https://service.amtelco.com/doclib/library.htm>.
4. *Soft Agent User Reference Guide*, May 2016, available at <https://service.amtelco.com/doclib/library.htm>.

©2017 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.