Application Notes for configuring Amtelco Intelligent Soft Agent Version 4.0.4647 with Avaya Aura® Application Enablement Services Release 6.2 and Avaya Aura® Communication Manager Release 6.2 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Amtelco Intelligent Soft Agent to successfully interoperate with Avaya Aura® Application Enablement Services Release 6.2 and Avaya Aura® Communication Manager Release 6.2.

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 a solution comprised of Avaya Aura® Application Enablement Services Release 6.2 and Avaya Aura® Communication Manager Release 6.2 and Amtelco Intelligent Soft Agent (hereafter referred to as Soft Agent). The Soft Agent streamlines the activities of healthcare attendant console operators and call center agents by making any information available with a just a few keystrokes. The Soft Agent is an integral component of the Amtelco Intelligent Series suite of applications.

The objective of this compliance test was to validate the Soft Agent successfully interacted with Application Enablement Service (AES) DMCC services to control and monitor activities of the physical agent phone on the Avaya Aura® Communication Manager switch.

2. General Test Approach and Test Results

The general test approach was to verify interoperability feature and serviceability test cases between Amtelco Soft Agent and Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager. All test cases were executed manually.

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 compliance test concentrates on the AES DMCC based integration of the Amtelco Intelligent Soft Agent with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Application Enablement Services. The compliance test verified the ability for an operator to:

- Login, logout, and change agent states (aux, auto in, manual in, after call…).
- Receive ACD calls with identity of the calling party, called party, and forwarded party.
- Answer incoming calls in queue.
- Receive direct agent calls with identity of the calling party.
- Play Amtelco Perfect Answer greetings to connected calls.
- Record connected calls using Amtelco Soft Agent Logger.
- Generate outgoing calls.
- Overdial DTMF on outgoing calls to dial long distance codes and other overdial applications.
- Place calls on hold and reconnect.
- Perform blind transfers of answered calls to any configured station or PSTN number.
- Perform supervised transfers of answered calls to any configured station or PSTN number.
- Perform call conferencing of answered calls to any configured station or PSTN number.

- Ensure that the resources used during the process are released and are available for reuse.
- Serviceability: restart DMCC services.

2.2. Test Results

All test cases were tested and passed.

3. Support

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

- Call the Amtelco technical support at 1 (800) 356-9148 or 1 (800) 553-7679.
- Submit email question to Amtelco Infinity technical email support at info@amtelco.com.

For more information visit http://www.1call.com or http://www.amtelco.com

4. Reference Configuration

Figure 1 below illustrates the test configuration diagram between Avaya Aura® Application Enablement Services, Avaya Aura® Communication Manager and Amtelco Soft Agent. The Compliance test used the Avaya Communication Server 1000 to have SIP Trunk to Communication Manager for test cases external calls via SIP Trunk.

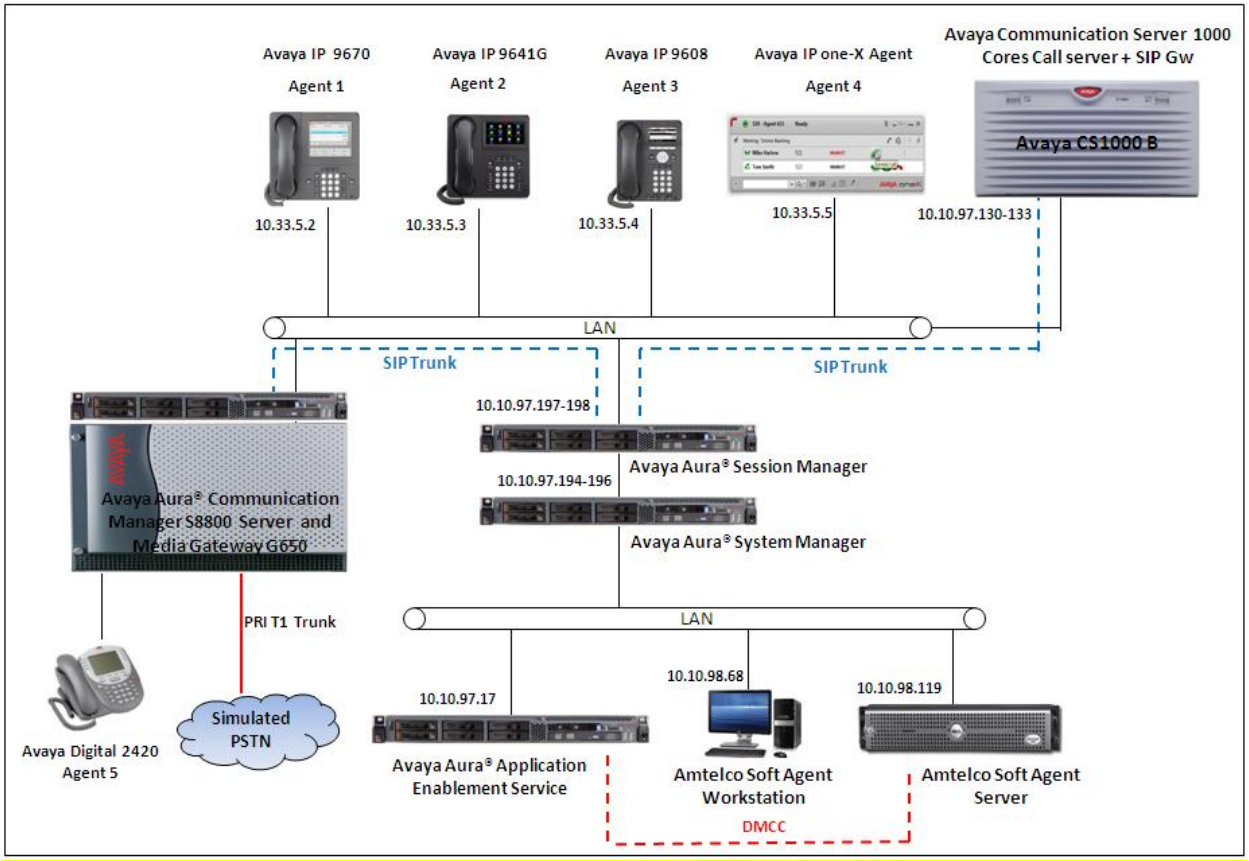


Figure 1: Test Configuration Diagram

5. Equipment and Software Validated

The following equipment and software were used for the compliance test:

Equipment/Software	Release/Version
Avaya S8800 server running Avaya Aura® Session Manager	6.2 (Build No 6.2.3.0.623006)
Avaya S8800 server running Avaya Aura® System Manager Server	6.2 (Build No: 6.2.0 Software Update Revision No: 6.2.12.1.1822)
Avaya S8800 server running Avaya Aura® Application Enablement Services	6.2 SP2
Avaya S8800 server running Avaya Aura® Communication Manager	6.2 SP2
Avaya IP 9670	3.1
Avaya IP 9641G	6.2209
Avaya IP 9608	6.02S
Avaya IP one-X Agent	2.5 SP5
Avaya Digital 2420	-
Amtelco Dell Server	Windows 2008 64-bit R2 Standard SP1
Amtelco Intelligent Soft Agent Server	4.0.4647.
Amtelco Intelligent Soft Agent Client	4.0.4647.22731

6. Configure Avaya Aura® Communication Manager

This section provides the steps required to configure Avaya Aura® Communication Manager to interoperate with AES and Amtelco Soft Agent. These Application Notes assume the Avaya Media Gateway (including circuit packs) has already been administered. Please refer to **Section 11** for additional details.

The commands listed in this section were issued at the System Access Terminal (SAT) screen. For all steps where data are modified, submit the completed administration form for the changes to take effect.

The following summarizes the tasks which need to be done on the Communication Manager System:

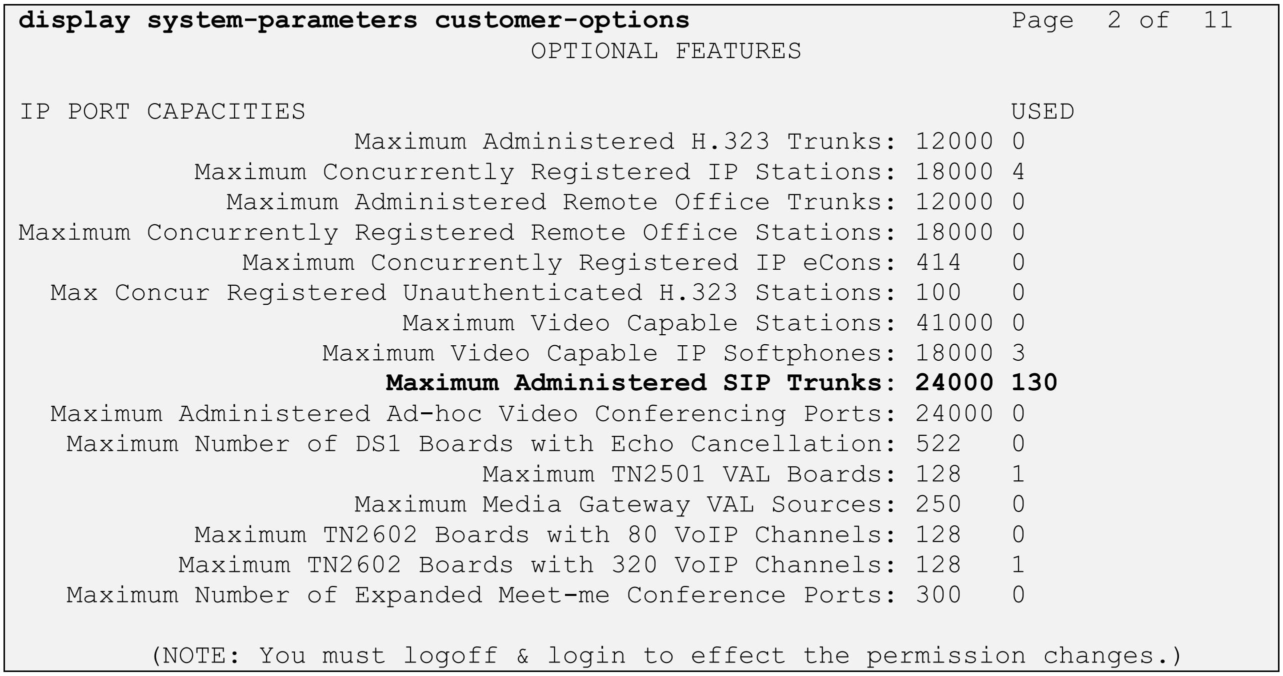
- Verify Avaya Aura® Communication Manager License.
- Administer Expert Agent Selection (EAS) Feature.
- Administer IP Node Name.
- Administer IP Codec.
- Administer IP Network Region.
- Administer IP Service.
- Administer CTI Link.
- Administer Feature Access Codes.
- Administer Hunt Group.

- Administer Vector and VDN number.
- Administer Agent Login ID.
- Administer Agent Station.

6.1. Verify Avaya Communication Manager License

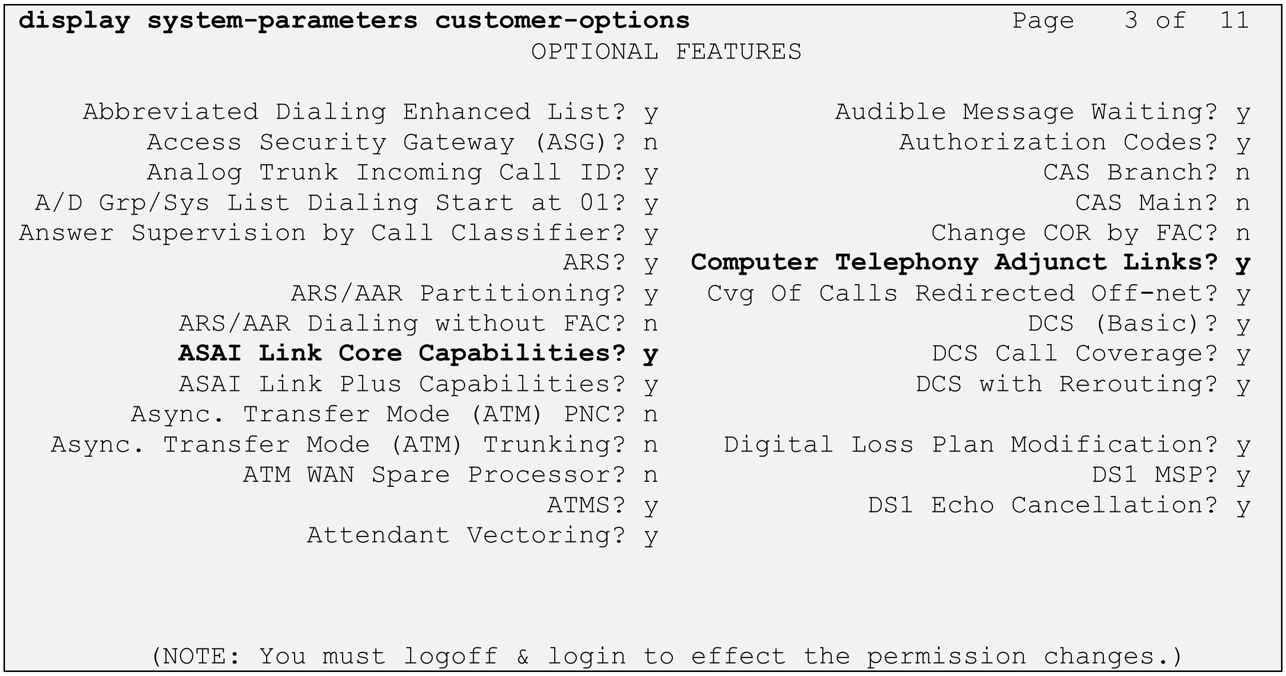
Use the “**display system-parameters customer-options**” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.



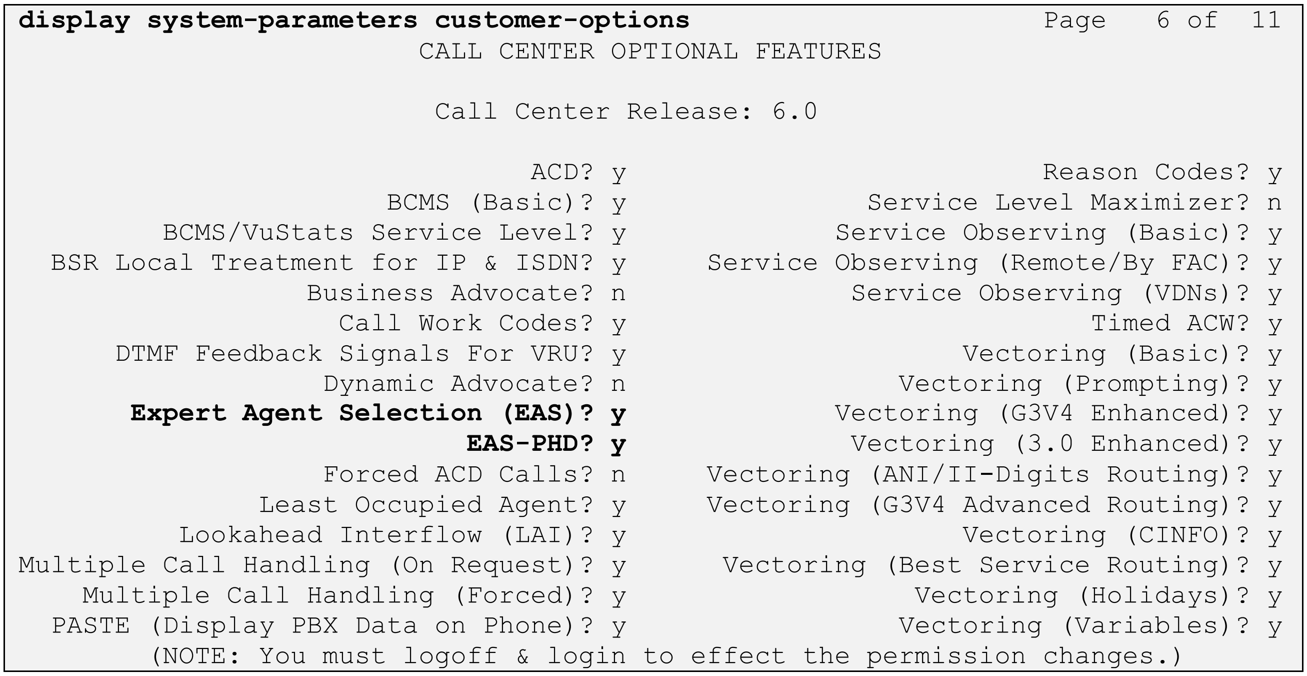
```
display system-parameters customer-options                    Page  2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 3
                       Maximum Administered SIP Trunks: 24000 130
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   1
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

Go to **Page 3** and verify that the **ASAI Link Core Capabilities**, and **Computer Telephony Adjunct Links** are set to “**y**”. If these options are not set to “**y**”, then contact the Avaya sales team or business partner for a proper license file.



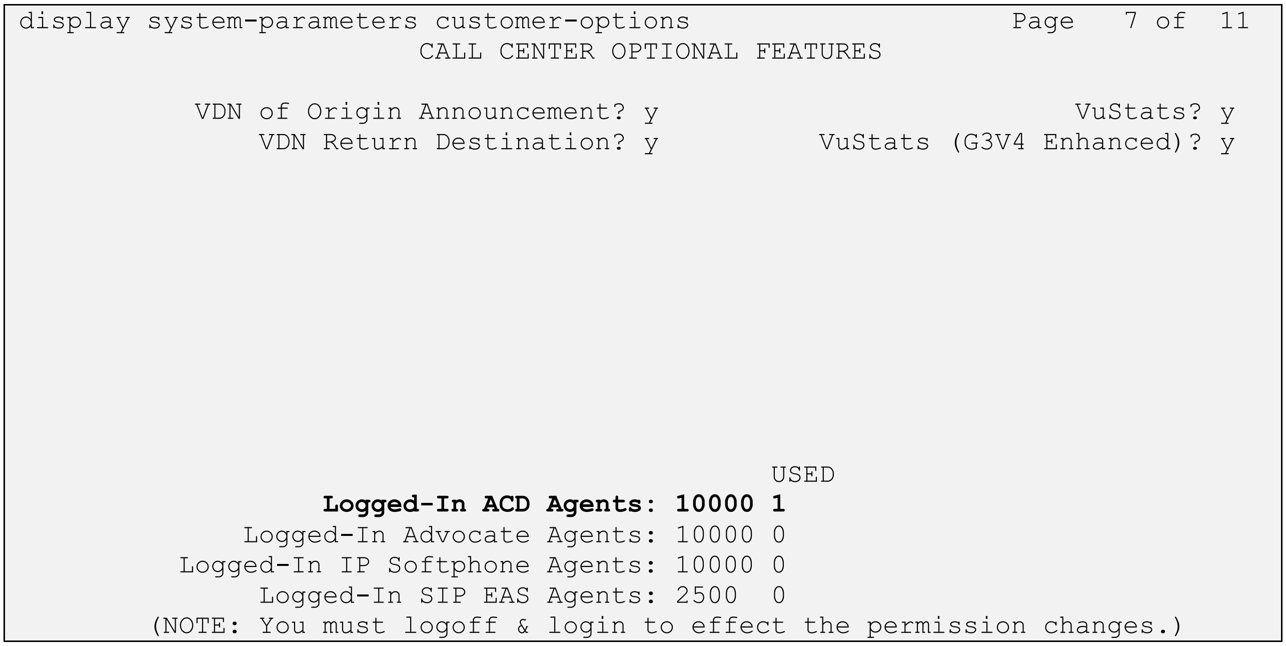
```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

    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.)
```

Go to **Page 6**, and verify that the **Expert Agent Selection (EAS)** and **EAS-PHD** are set to “Y”.



```
display system-parameters customer-options                      Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 6.0

                                ACD? y                           Reason Codes? y
                       BCMS (Basic)? y                Service Level Maximizer? n
         BCMS/VuStats Service Level? y             Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                  Business Advocate? n              Service Observing (VDNs)? y
                    Call Work Codes? y                             Timed ACW? y
      DTMF Feedback Signals For VRU? y                     Vectoring (Basic)? y
                   Dynamic Advocate? n                 Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y             Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? y              Vectoring (3.0 Enhanced)? y
                   Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
         Lookahead Interflow (LAI)? y                      Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
     Multiple Call Handling (Forced)? y                 Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                 Vectoring (Variables)? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

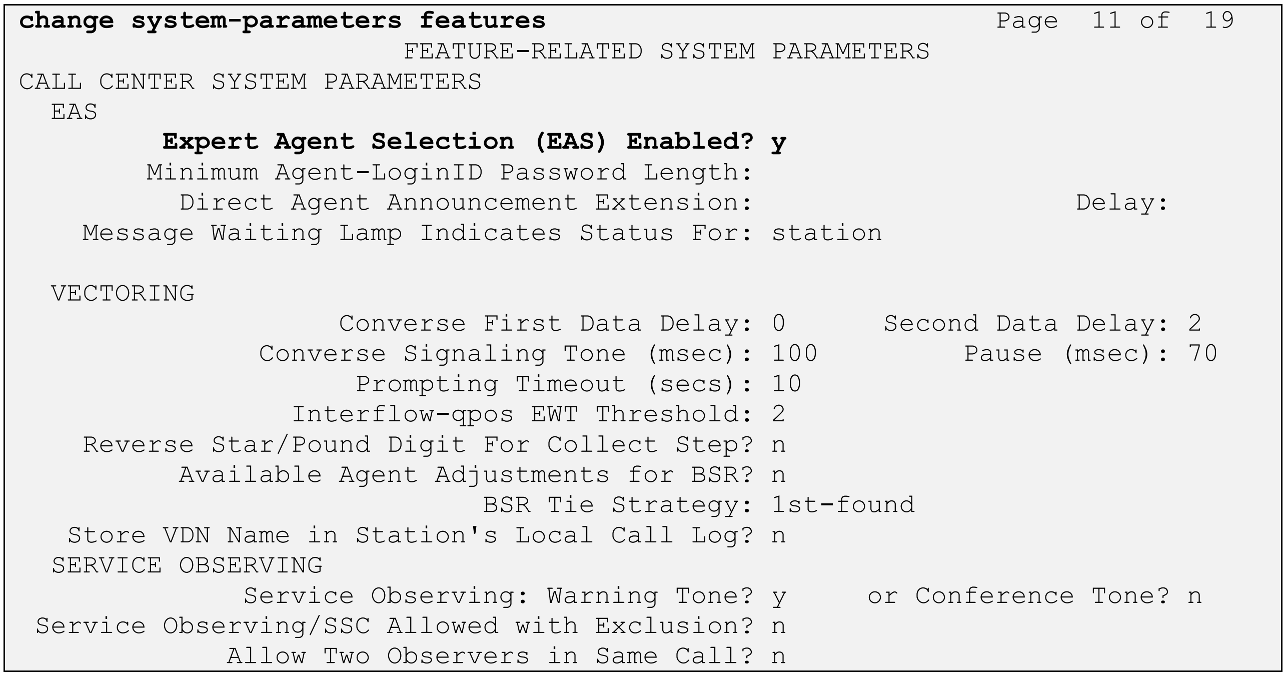
Go to **Page 7**, and verify that there is sufficient remaining capacity for **Logged-In ACD Agents**.



```
display system-parameters customer-options                    Page   7 of  11
                         CALL CENTER OPTIONAL FEATURES

           VDN of Origin Announcement? y                          VuStats? y
               VDN Return Destination? y          VuStats (G3V4 Enhanced)? y











                                               USED
                   Logged-In ACD Agents: 10000 1
              Logged-In Advocate Agents: 10000 0
          Logged-In IP Softphone Agents: 10000 0
               Logged-In SIP EAS Agents: 2500  0
        (NOTE: You must logoff & login to effect the permission changes.)
```

6.2. Administer Expert Agent Selection (EAS) Feature

To enable EAS feature on Communication Manager, use the command "**change system-parameters features**" and set the **Expert Agent Selection (EAS) Enabled** in the **Page 11** to "Y".



```
change system-parameters features                            Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                    Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
               Converse Signaling Tone (msec): 100        Pause (msec): 70
                     Prompting Timeout (secs): 10
                 Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                             BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? y     or Conference Tone? n
 Service Observing/SSC Allowed with Exclusion? n
             Allow Two Observers in Same Call? n
```

Go to **Page 12**, and also set the field **BCMS/VuStats LoginIDs?** to “**Y**”. This will help to monitor agent’s activity by issuing the command “**monitor bcms skill <ID>**”

```
change system-parameters features                            Page  12 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

  AGENT AND CALL SELECTION
                         MIA Across Splits or Skills? n
                          ACW Agents Considered Idle? y
                          Call Selection Measurement: current-wait-time
    Service Level Supervisor Call Selection Override? n
                                 Auto Reserve Agents: none
       Block Hang-up by Logged-in Auto-Answer Agents? n

  CALL MANAGEMENT SYSTEM
     REPORTING ADJUNCT RELEASE (determines protocol used by appl link)
                                      CMS (appl mis):
                                  AAPC/IQ (appl ccr):

                               BCMS/VuStats LoginIDs? y
                   BCMS/VuStats Measurement Interval: hour
           BCMS/VuStats Abandon Call Timer (seconds):
                     Validate BCMS/VuStats Login IDs? n
                            Clear VuStats Shift Data: on-login
                 Remove Inactive BCMS/VuStats Agents? n
```

6.3. Administer IP Node Name

This section describes the steps for configuring IP node names for Session Manager and AES in Communication Manager. Enter the “**change node-names ip”** command, and add a node name for **Session Manager**, **CLAN** card and its IP addresses. Make a note for the Communication Manager “**procr**” IP address.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AES62               10.10.98.17
CLAN1               10.10.97.217
CLAN2               10.10.97.218
GW                  10.10.97.193
SM62                10.10.97.198
default             0.0.0.0
procr               10.10.97.201
procr6              ::
```

6.4. Administer IP Codec

The IP codec set is used in the IP network region for communications between Avaya Communication Manager and Session Manager and between stations. To administer the IP Codec in Communication Manager, enter “**change ip-codec-set <n>**” command, where **n** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 6.5** when configuring an IP network region to specify which audio codecs may be used within and between network regions. In the sample configuration, only one network region is used.

```
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: G.722-64K                   2        20
 4:
 5:
 6:
 7:
```

6.5. Administer IP Network Region

To administer the IP Network Region, enter "**change ip-network-region <n>**" command, where **n** is a number between **1** and **250** inclusive, configure the following and leave other fields at default.

- **Authoritative Domain**: Enter the appropriate value. In the test configuration, sip domain name "**bvwdev.com**" was used.
- **Codec Set**: Enter the IP codec set number as provisioned in **Section 6.4**.

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: bvwdev.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

6.6. Administer IP Service

To administer IP Services for AES Transport Link, use the “**change ip-services**” command and add an entry with the following values for fields on **Page 1**:

- **Service Type:** “**AESVCS**”.
- **Enabled:** set to “**Y**”.
- **Local Node:** “**CLAN2**”.
- **Local Port:** Retain the default value of “**8765**”.

```
change ip-services                                            Page   1 of   3

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      CLAN2            8765
```

Proceed to **Page 3** and enter the following information:

- **AE Services Server:** Name obtained from the AES server.
- **Password:** Same password to be administered on the AES server.
- **Enabled:** “**Y**”.

Note that the name and password entered for the **AE Services Server** and **Password** fields are case sensitive, and must match the name and password on the AES server. The administered name for the AES server is created as part of the AES installation, and can be obtained from the AES server by typing “**uname –n**” at the Linux command prompt. The same password entered in the screen below will need to be set on the AES server, as described in **Section 7.3.**

```
change ip-services                                            Page   3 of   3
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      AES62             *                     y        in use
```

6.7. Administer CTI Link

To add a CTI link, use 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. Submit these changes

```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 50001
     Type: ADJ-IP
                                                                       COR: 1
     Name: AES62
```

6.8. Administer Feature Access Codes

To administer the Feature Access Codes, use the "**change feature-access-codes**" command and go to **Page 5** to enter the access codes for Call Center features such as Login, Logout, etc. like shown below. Note that the access codes also need to be followed by the dial plan table.

```
change feature-access-codes                                  Page   5 of  10
                               FEATURE ACCESS CODE (FAC)

                                 Call Center Features
  AGENT WORK MODES
                    After Call Work Access Code: *36
                             Assist Access Code: *37
                            Auto-In Access Code: *38
                           Aux Work Access Code: *39
                              Login Access Code: *40
                             Logout Access Code: *41
                          Manual-in Access Code: *42
  SERVICE OBSERVING
             Service Observing Listen Only Access Code:
             Service Observing Listen/Talk Access Code:
                 Service Observing No Talk Access Code:
   Service Observing Next Call Listen Only Access Code:
 Service Observing by Location Listen Only Access Code:
 Service Observing by Location Listen/Talk Access Code:
```

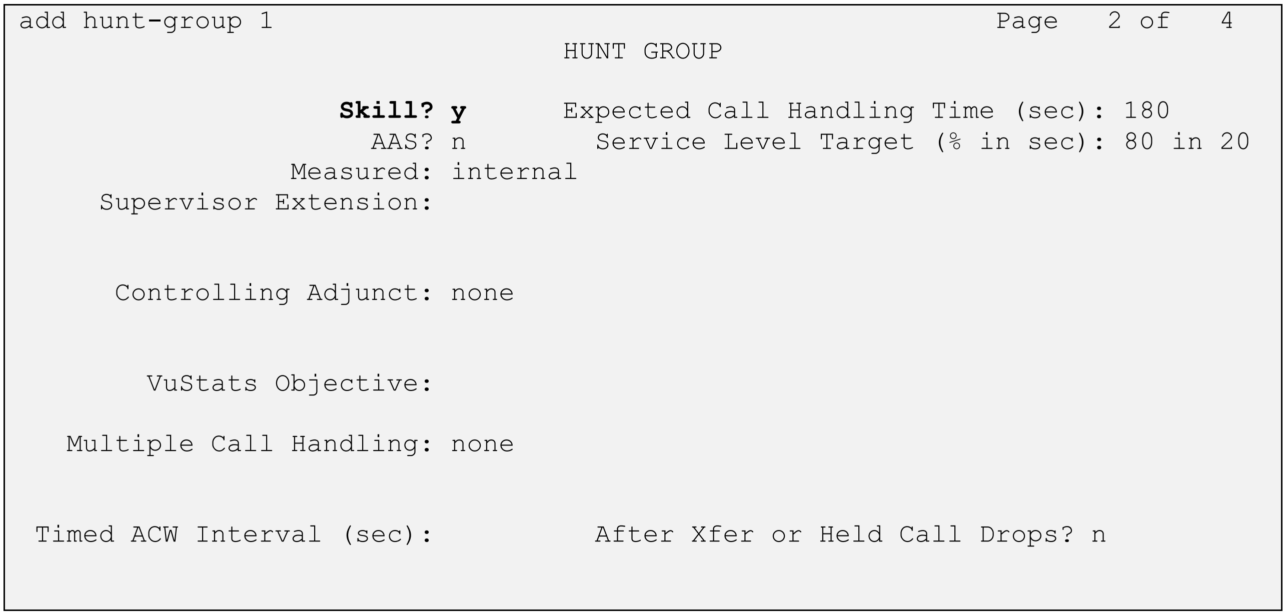
6.9. Administer Hunt Group

To add a hunt group for routing calls to ACD queue, use "**add hunt-group <n>**" command, where <n> is an available hunt group. In **Page 1**, configure following fields and leave others as default.

- **Group Name**: enter a descriptive name e.g. **Hunt1**.
- **Group Extension**: enter an available extension, e.g. "**53016**".
- **Group Type:** enter "**ucd-mia**".
- **ACD?**: set to "Y".
- **Queue?**: set to "Y".
- **Vector?**: set to "Y".

```
add hunt-group 1                                            Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                                     ACD? y
              Group Name: Hunt1                               Queue? y
         Group Extension: 53016                              Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                          MM Early Answer? n
           Security Code:                     Local Agent Preference? n
 ISDN/SIP Caller Display:
```

Go to **Page 2**, set “**Y**” for the **Skill?** field.

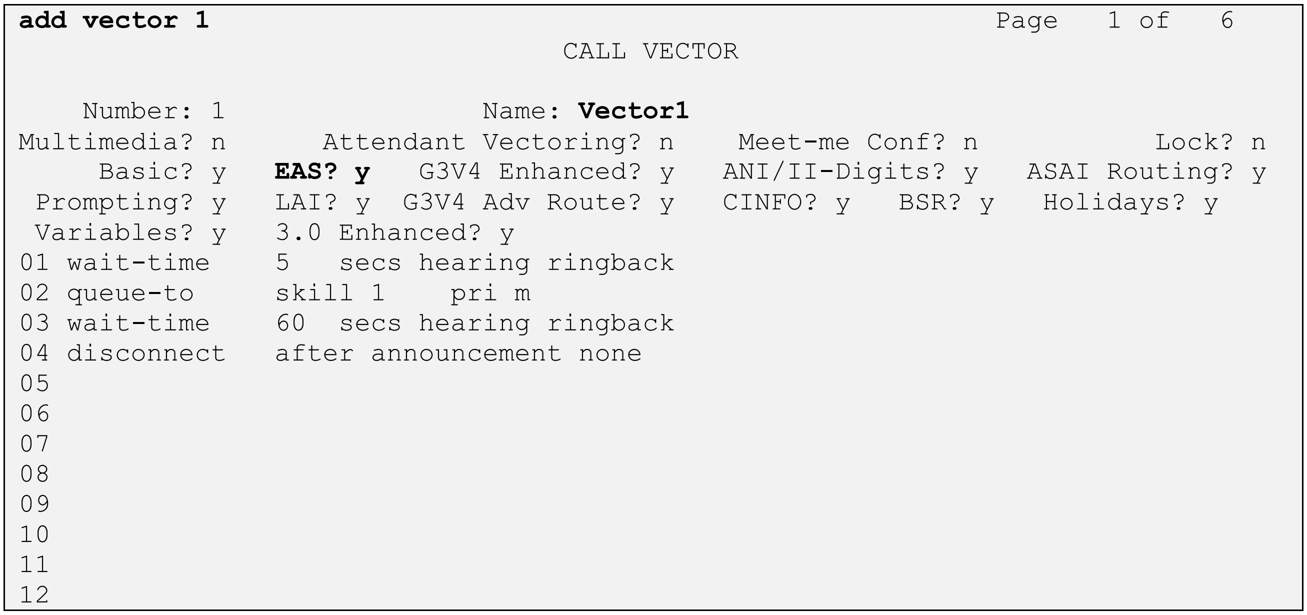


```
add hunt-group 1                                             Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
                 Measured: internal
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:

   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

6.10. Administer Vector and VDN number

To add a vector in Communication Manager, use “**add vector <n>**”, where **<n>** is an available vector number. In **Page 1**, configure following fields and leave other fields at default.

- **Name**: enter a descriptive name e.g. “**Vector1**”.
- **EAS?**: set to “**Y**”.



```
add vector 1                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: Vector1
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    5   secs hearing ringback
02 queue-to     skill 1    pri m
03 wait-time    60  secs hearing ringback
04 disconnect   after announcement none
05
06
07
08
09
10
11
12
```

To add a VDN number in Communication Manager, use "**add vdn <n>**". Where **<n>** is an available extension in the system. In **Page 1**, configure the following fields and leave others at default.

- **Name**: enter a descriptive name e.g. "**Inbound**".
- **Destination**: enter "**Vector Number**" and "**1**" as configured above.

```
add vdn 53050                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 53050
                                 Name*: Inbound
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:

* Follows VDN Override Rules
```

6.11. Administer Agent Login ID

To add agent login ID, use the "**add agent-loginID <extension>**" command, where **<extension>** is an available extension on the switch.

```
add agent-loginID 1000                                       Page   1 of   3
                                 AGENT LOGINID

                Login ID: 1000                                   AAS? n
                    Name: Agent1                               AUDIX? n
                      TN: 1                            LWC Reception: spe
                     COR: 1                   LWC Log External Calls? n
           Coverage Path:                   AUDIX Name for Messaging:
           Security Code:
                                        LoginID for ISDN/SIP Display? n
                                                            Password:
                                              Password (enter again):
                                                         Auto Answer: station
                                                   MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:    :

     WARNING:  Agent must log in again before changes take effect
```

Go to **Page 2**, set **SN** (Skill Number) and **SL** (Skill Level) fields to "**1**".

```
add agent-loginID 1000                                          Page   2 of   3
                                 AGENT LOGINID
      Direct Agent Skill:                                  Service Objective? n
Call Handling Preference: skill-level                  Local Call Preference? n

    SN   RL SL           SN   RL SL           SN   RL SL           SN   RL SL
 1: 1       1        16:                  31:                  46:
 2:                  17:                  32:                  47:
 3:                  18:                  33:                  48:
 4:                  19:                  34:                  49:
 5:                  20:                  35:                  50:
 6:                  21:                  36:                  51:
```

6.12. Administer Agent Station

In the compliance test, there were three H.323 stations, **53010**, **53011**, and **53012,** and one digital station, **53040,** that were configured and used as Contact Center agents.

Issue "**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.

- **Type**: Enter station type, e.g. **4625**.
- **Name**: A descriptive name.
- **Security Code**: Enter a valid code.
- **IP SoftPhone**: "**Y**".

```
add station 53010                                                Page   1 of   5
                                     STATION

Extension: 53010                        Lock Messages? n                BCC: 0
     Type: 4625                         Security Code: *                 TN: 1
     Port: S00004                     Coverage Path 1:                  COR: 1
     Name: H.323,53010                 Coverage Path 2:                  COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                            Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                  Message Lamp Ext: 53010
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                 Expansion Module? n
 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
```

Go to **Page 4**, and assign following buttons for agent station: **Aux-work**, **manual-in**, **after-call**, **auto-in**, and **release**.

```
add station 53010                                                    Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                                  Headset? n
       Jack:                                                  Speaker? n
      Cable:                                                 Mounting: d
      Floor:                                             Cord Length: 0
   Building:                                               Set Color:

ABBREVIATED DIALING
     List1:                   List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                              5: manual-in          Grp:
 2: call-appr                              6: after-call         Grp:
 3: call-appr                              7: auto-in            Grp:
 4: aux-work    RC:    Grp:                8: release
```

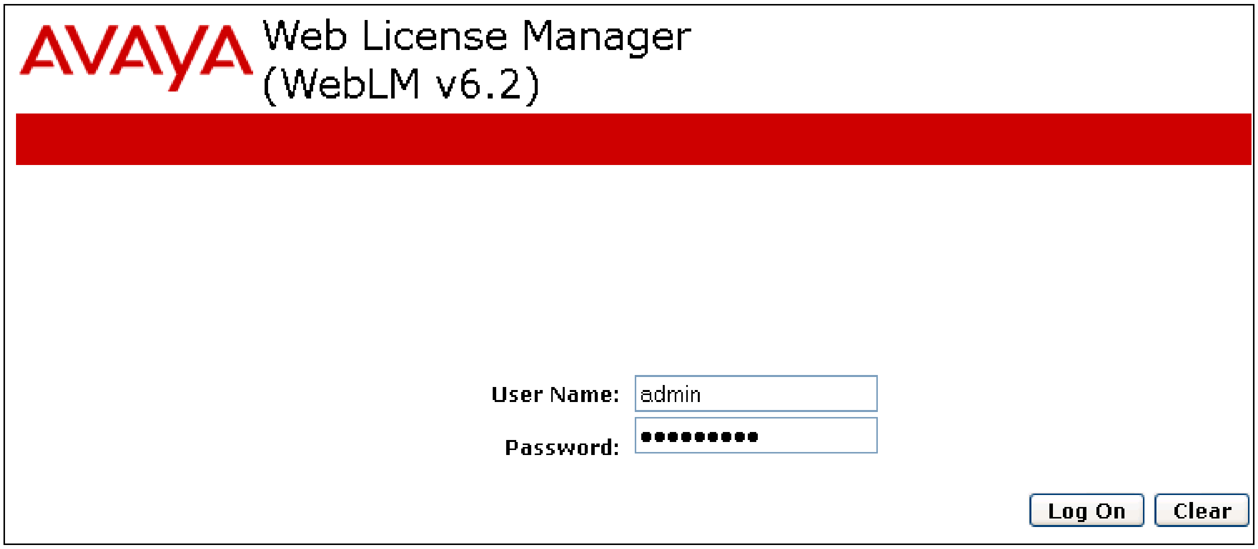
7. Configure Avaya Aura® Application Enablement Services

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

- Verify Application Enablement Services (AES) License.
- Administer Local IP.
- Administer switch connection for Communication Manager.
- Administer TSAPI link.
- Administer DMCC Ports.
- Administer Tlink.
- Administer CTI User.

7.1. Verify Application Enablement Services License

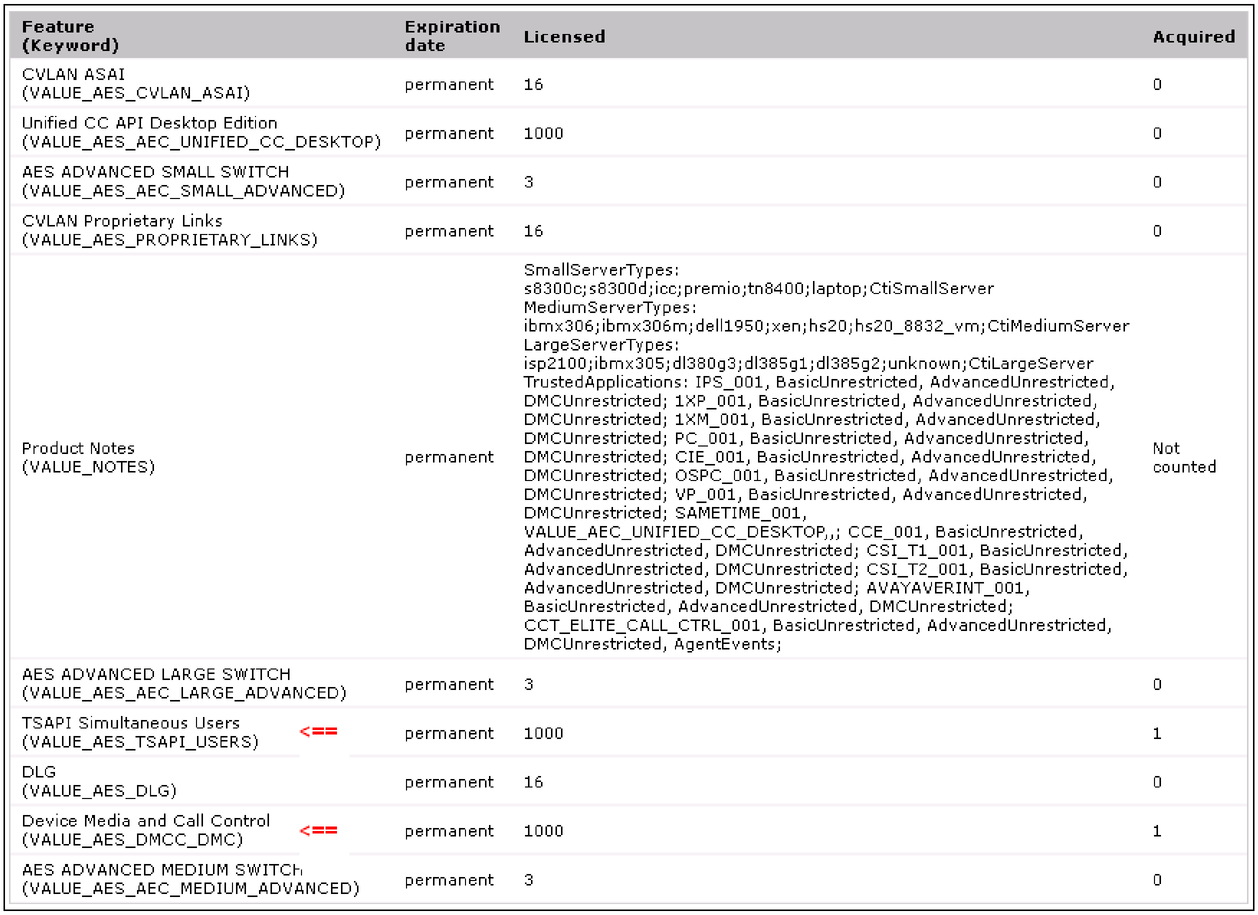
Log in the System Platform in which the AES template installed and navigate to **Server Management → License Management**. The **Server Management** page is displayed in the right, click on **Launch WebLM License Manager**. The Avaya Web License Manager page is displayed. Enter the "**admin**" user in the **User Name** field and its password and click on **Log On** button to log on.



User Name: admin

Password: ●●●●●●●●●●

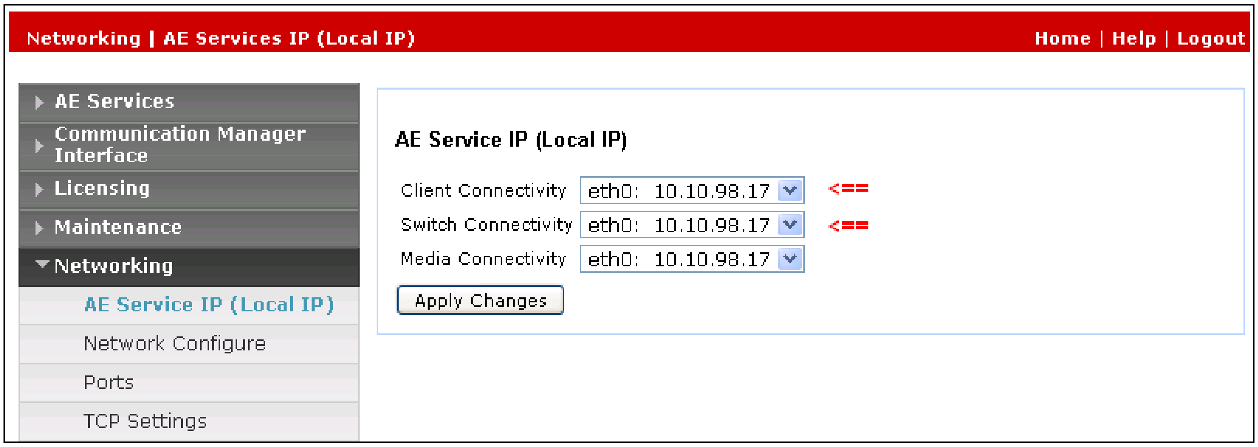
In the left navigation pane, navigate to **Licensed Products → Application_Enablement → View License Capacity**. Verify that AES is licensed for the TSAPI and DMCC services, as shown below. If the TSAPI and DMCC services are not licensed, contact the Avaya sales team or business partner for a proper license file.



Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users <== (VALUE_AES_TSAPI_USERS)	permanent	1000	1
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control <== (VALUE_AES_DMCC_DMC)	permanent	1000	1
AES ADVANCED MEDIUM SWITCh (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3	0

7.2. Administer AE Service Local IP.

Log into AES web management console by using appropriate credentials. From the management console, navigate to **Networking → AE Service IP (Local IP)**. The **AE Service IP (Local IP)** screen is displayed into the right pane, as shown below. In the **Client Connectivity** field, note the AES server IP address that will be used to interface to Amtelco Soft Agent. In the **Switch Connectivity** field, note the AES server IP address that will be used to connect to Avaya Communication Manager. In the sample configuration, the same NIC interface is used for the **Client Connectivity** and **Switch Connectivity**. Note that in some cases, they might be different.

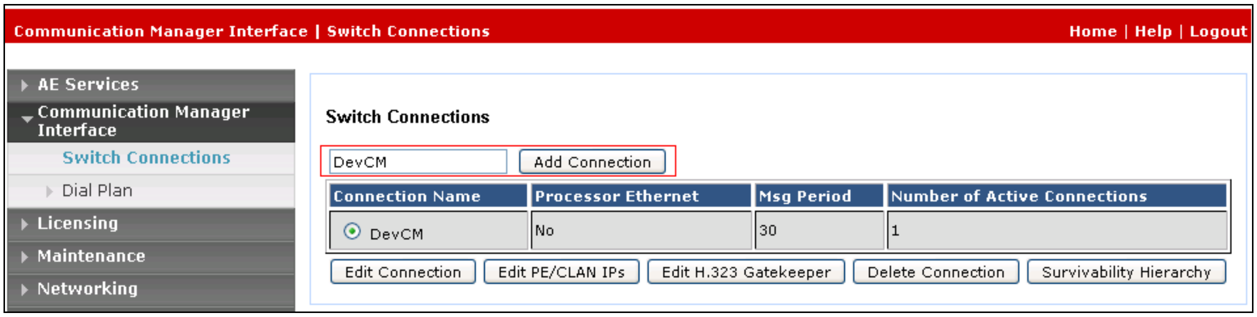


AE Service IP (Local IP)

Client Connectivity	eth0: 10.10.98.17
Switch Connectivity	eth0: 10.10.98.17
Media Connectivity	eth0: 10.10.98.17

7.3. Administer Switch Connection

From the AES Management console, navigate to **Communication Manager Interface → Switch Connections**. Under **Switch Connections** provide the hostname of the Communication Manager and click on **Add Connection**.



Switch Connections

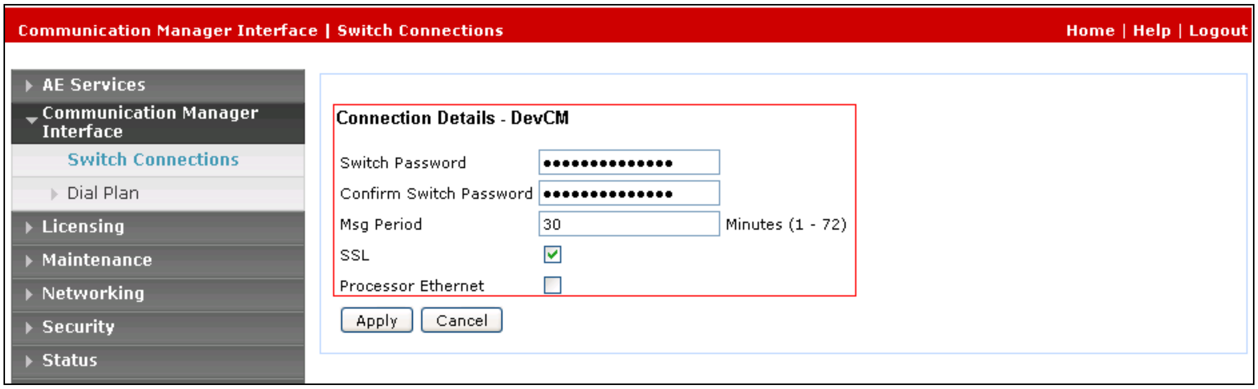
DevCM

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● DevCM	No	30	1

The following highlighted configurations were done to add Communication Manager to the list of switch connections:

- **Switch Password**: Enter the switch password. This password has to be the same as what was entered in **Section 6.6**.
- **Confirm Switch Password**: Re-enter the same password from **Section 6.6**.
- **Msg Period**: Accept the default (30 minutes).
- **SSL**: Check the check box.

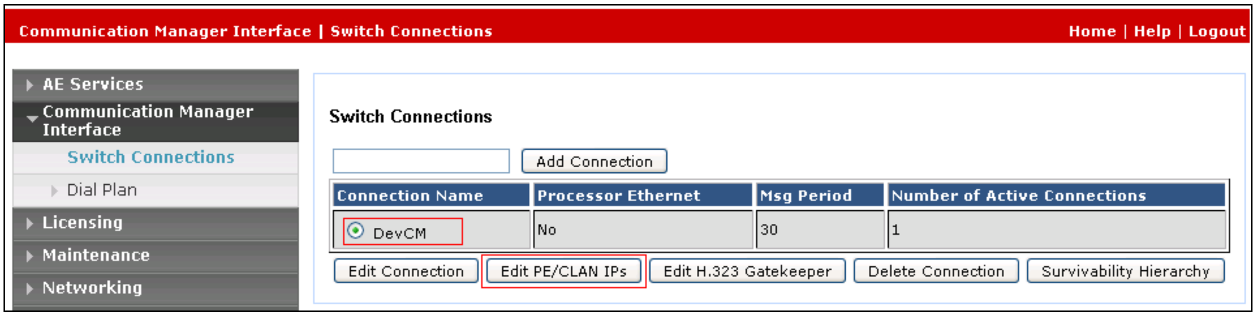
- **Processor Ethernet**: uncheck the check box since the CLAN was used. Note that if the Processor Ethernet is used to connect to AES server, check this check box. In the compliance test, the CLAN was used therefore this check box should be unchecked.



Connection Details - DevCM

Switch Password	••••••••••••••	
Confirm Switch Password	••••••••••••••	
Msg Period	30	Minutes (1 - 72)
SSL	☑	
Processor Ethernet	□	

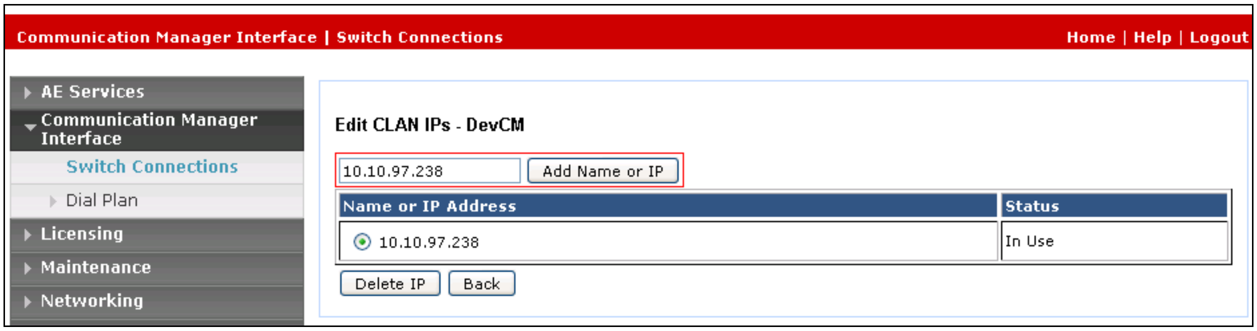
From the **Switch Connections** page, select the newly added **CM** connection and then click on the **Edit PE/CLAN IPs** button as shown below.



Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● DevCM	No	30	1

Enter the IP address **10.10.97.238** as defined as “**CLAN2**” in Communication Manager from **Section 5.3**.



Edit CLAN IPs - DevCM

10.10.97.238

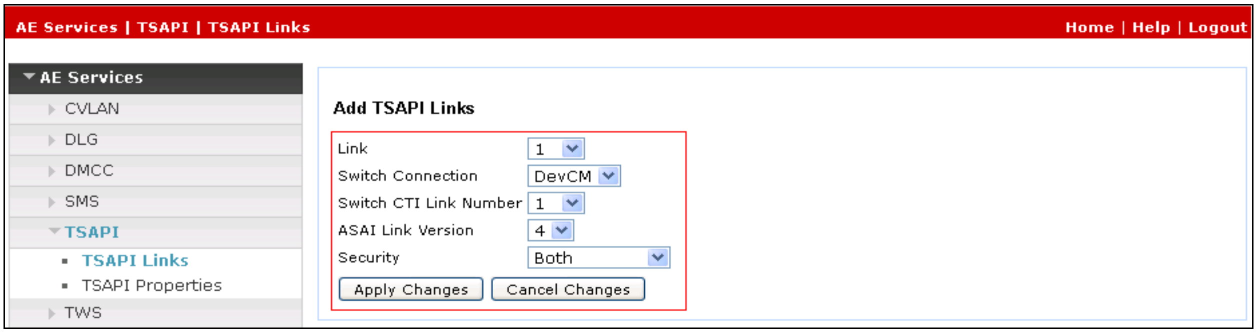
Name or IP Address	Status
● 10.10.97.238	In Use

7.4. Administer TSAPI Link

From the AES Management console, navigate to **AE Services** → **TSAPI** → **TSAPI** Links. The **TSAPI** Links page is displayed in the right (screen not shown), click **Add Link**. Enter the following highlighted values to add the CTI link:

- **Link**: From the drop down menu, select any available link number.
- **Switch Connection**: Select the CM switch connection from **Section 6.3**.
- **Switch CTI Link Number**: Select the CTI link number from **Section 6.7**.
- **ASAI Link Version**: Select **4** from the drop down menu.
- **Security**: Select **both** from drop down menu.

Click on **Apply Changes** when finished.



Add TSAPI Links

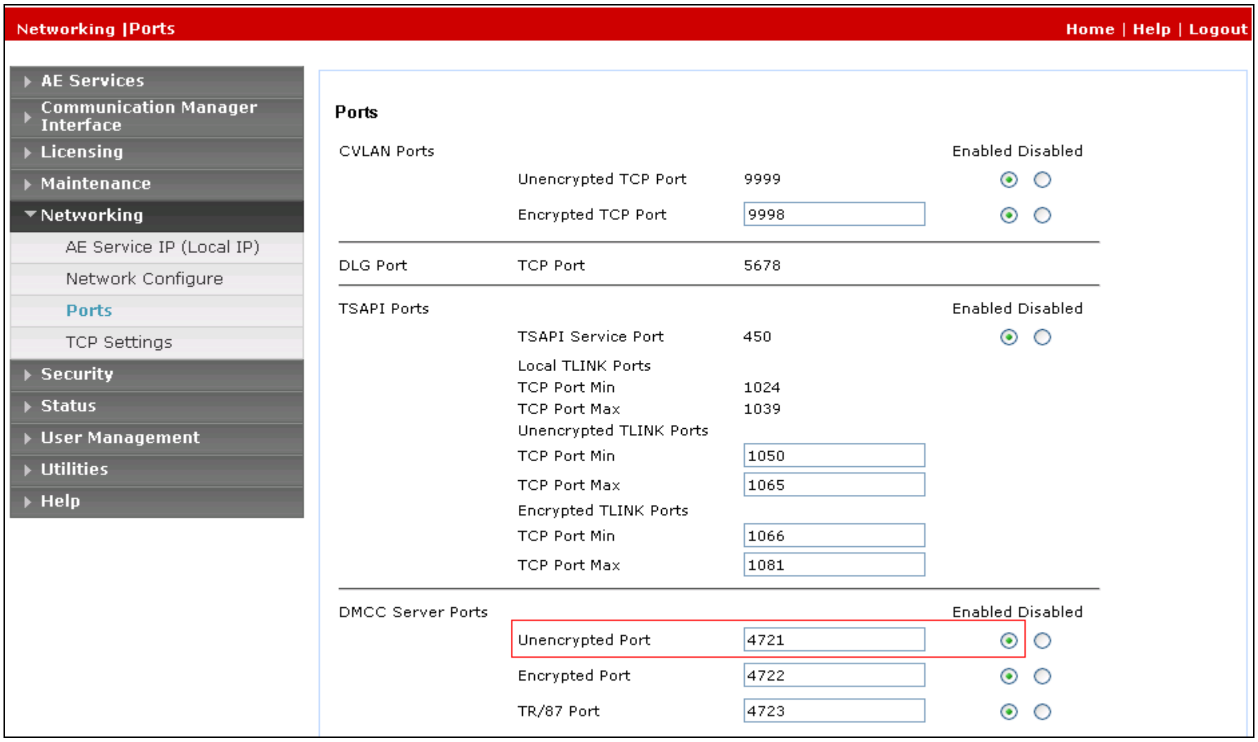
Link	1
Switch Connection	DevCM
Switch CTI Link Number	1
ASAI Link Version	4
Security	Both

7.5. Administer DMCC Ports

From the AES Management console, navigate to **Networking → Ports**. The following highlighted configuration was needed in **DMCC Server Ports** section:

- **Unencrypted Port**: enabled and enter the port **4721**. This port is used for Amtelco Soft Agent to connect to AES server.

Click on **Apply Changes** and Apply when finished.

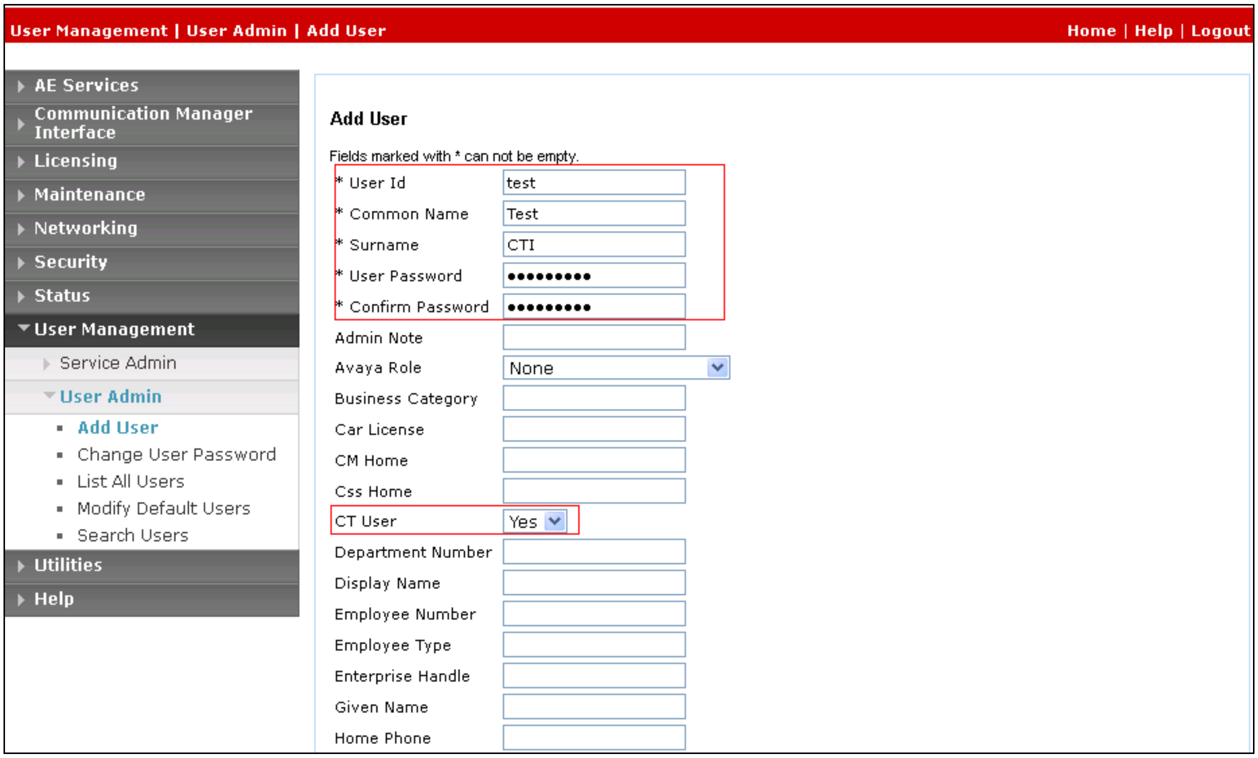


Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	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			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

7.6. Administer CTI User

From the AES Management console, navigate to **User Management** → **User Admin** → **Add User**. The **Add User** page is displayed in the right. Enter desired values for **User Id**, e.g. "**test**", **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. Click **Apply** button at the bottom of the page to complete. This user will be used to configure for the Amtelco Soft Agent application in **Section 7**.



Add User

Fields marked with * can not be empty.

* User Id	test
* Common Name	Test
* Surname	CTI
* 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	

8. Configure Amtelco Intelligent Soft Agent

This document assumes that the Amtelco Soft Agent server and application were properly installed and configured by an Amtelco engineer. This section only provides the steps how to configure the Soft Agent to work with AES and Communication Manager.

8.1. Configure Amtelco Soft Agent Server

The Amtelco Soft Agent Server is installed and configured by an Amtelco Engineer. It uses the Intelligent Series Supervisor application as the administration tool. A number of settings in the system and agent settings need to be configured in the intelligent series supervisor application prior to configuring the soft agent.

8.2. Configure Intelligent Series Supervisor

This section provides the procedures for configuring the Intelligent Series Supervisor application. The procedures include the following areas:

- Launch Intelligent Series Supervisor
- Administer system settings
- Administer agent settings

Note: The following procedures are based on AMTELCO Infinity Intelligent Series software version 5.60.4647.01.

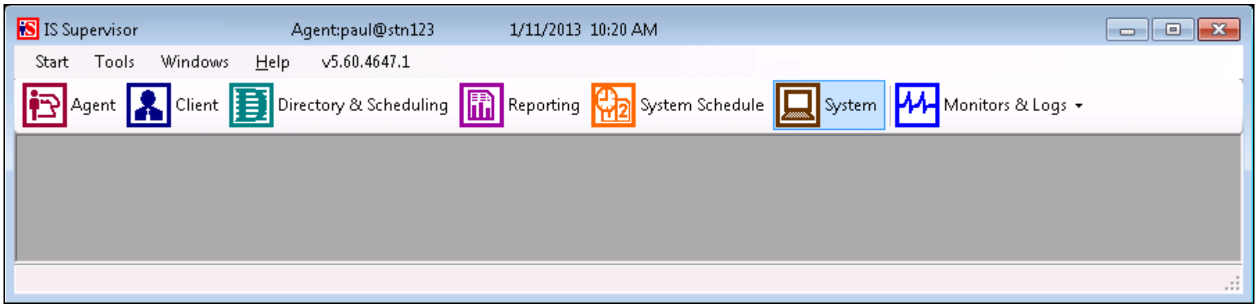
8.3. Launch Intelligent Series Supervisor

At a workstation or server running the Intelligent Series Supervisor, double-click on the **IS Supervisor** icon below, which is created as part of the software installation routine, or select **Start → All Programs → Amtelco → Intelligent Series Supervisor**.

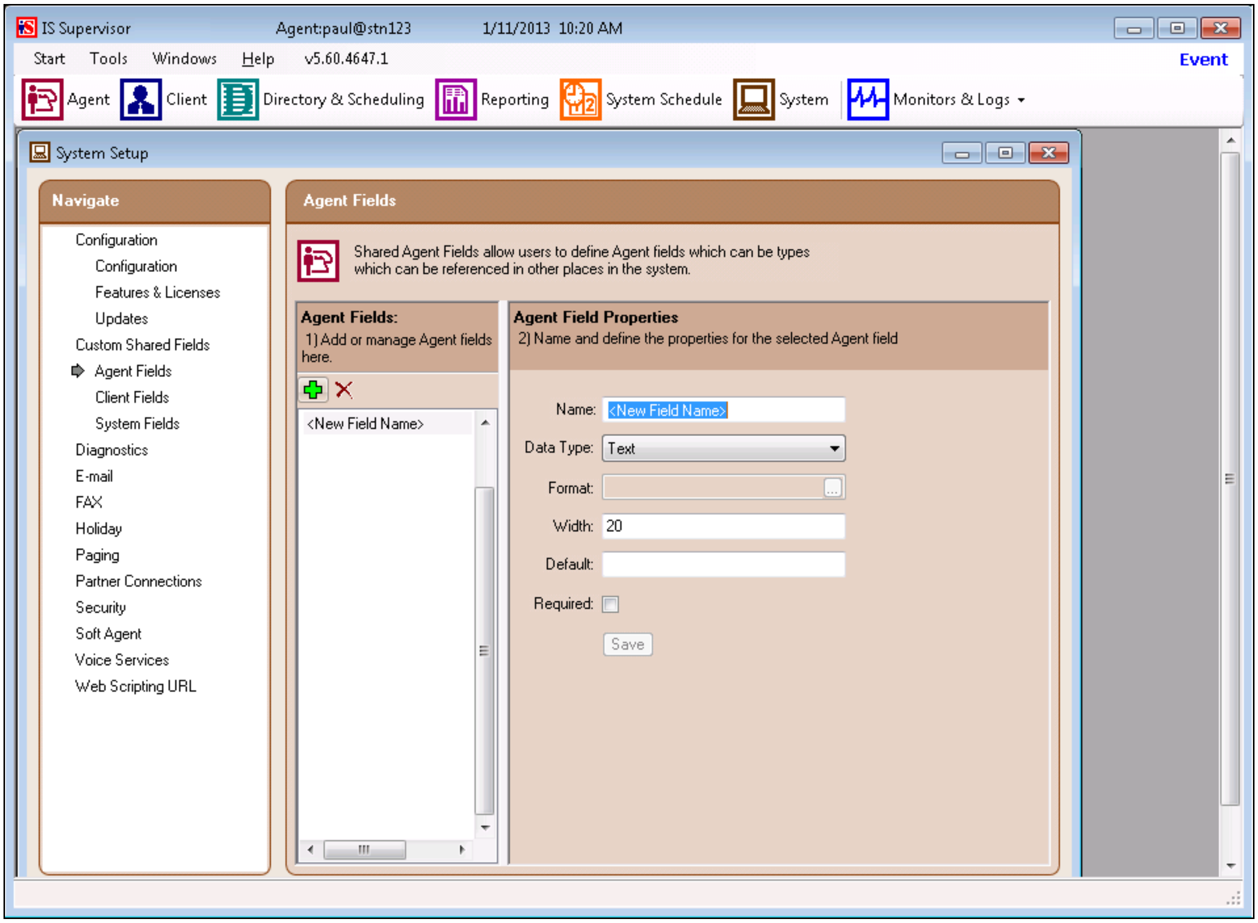
The **IS Supervisor Login** screen is displayed. Log into the Supervisor with the appropriate credentials.

Administer System Settings

At the **IS Supervisor** toolbar screen, click the **System** icon at the top of the screen.



The **System Setup** screen is displayed in the lower pane.
Select **Custom Shared Fields → Agent Fields** from the left pane, and then click the **Add Field** icon at the top of the middle pane.



Shared Agent Fields allow users to define Agent fields which can be types which can be referenced in other places in the system.

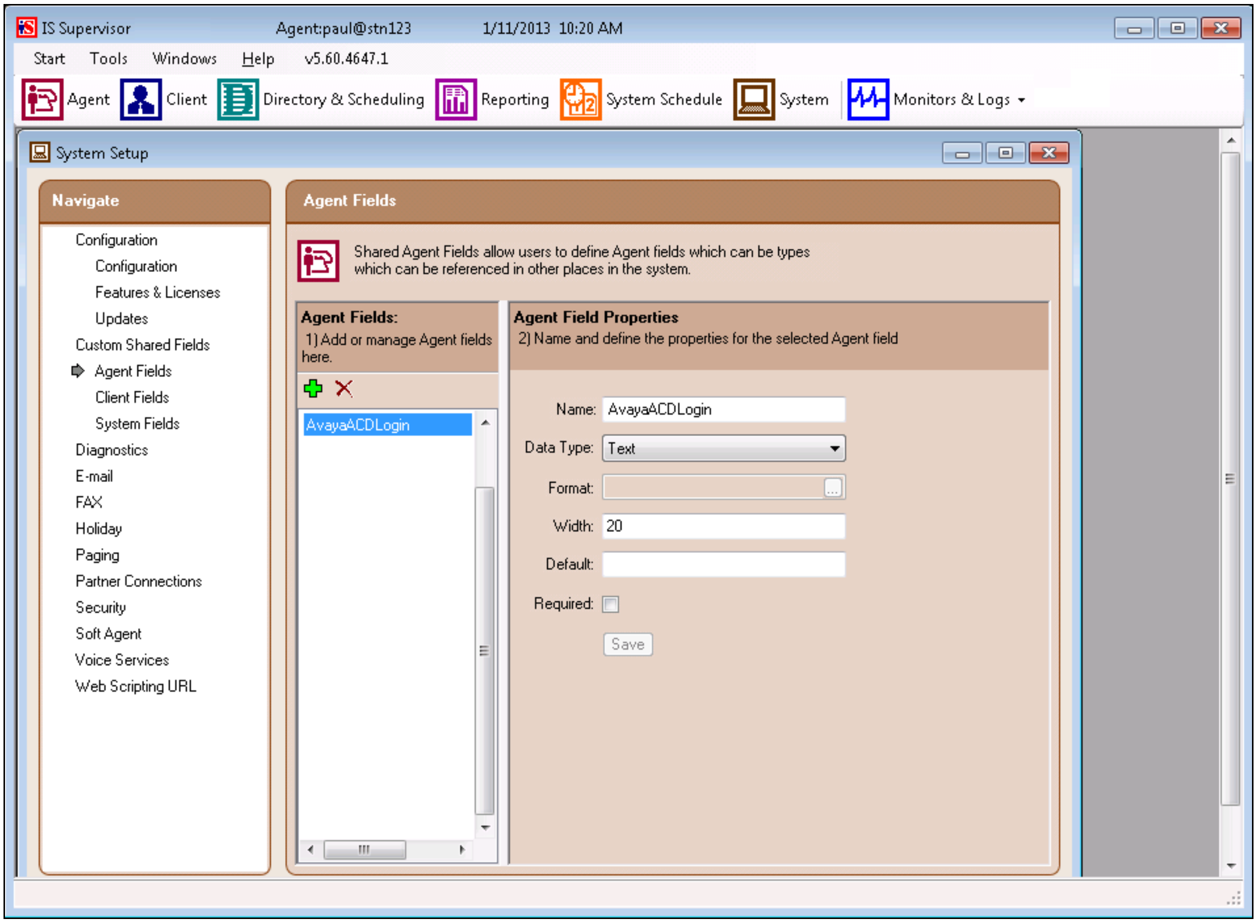
Agent Fields: 1) Add or manage Agent fields here.

Agent Field Properties 2) Name and define the properties for the selected Agent field

Name: <New Field Name>
Data Type: Text
Format:
Width: 20
Default:
Required: □

In the **Agent Field Properties** screen in the right pane, enter the name of the new Shared Agent Field that corresponds to the **Login ID** field previously established in the Avaya Communication Manager software using the "add-agent-loginID *n*" procedure. In this example, the new shared agent field is **AvayaACDLogin**.

Retain the default values for the remaining fields. Click the **Save** button to write your entries to the Intelligent Series database.



Shared Agent Fields allow users to define Agent fields which can be types which can be referenced in other places in the system.

Agent Fields:
1) Add or manage Agent fields here.

AvayaACDLogin

Agent Field Properties
2) Name and define the properties for the selected Agent field

Name: AvayaACDLogin

Data Type: Text

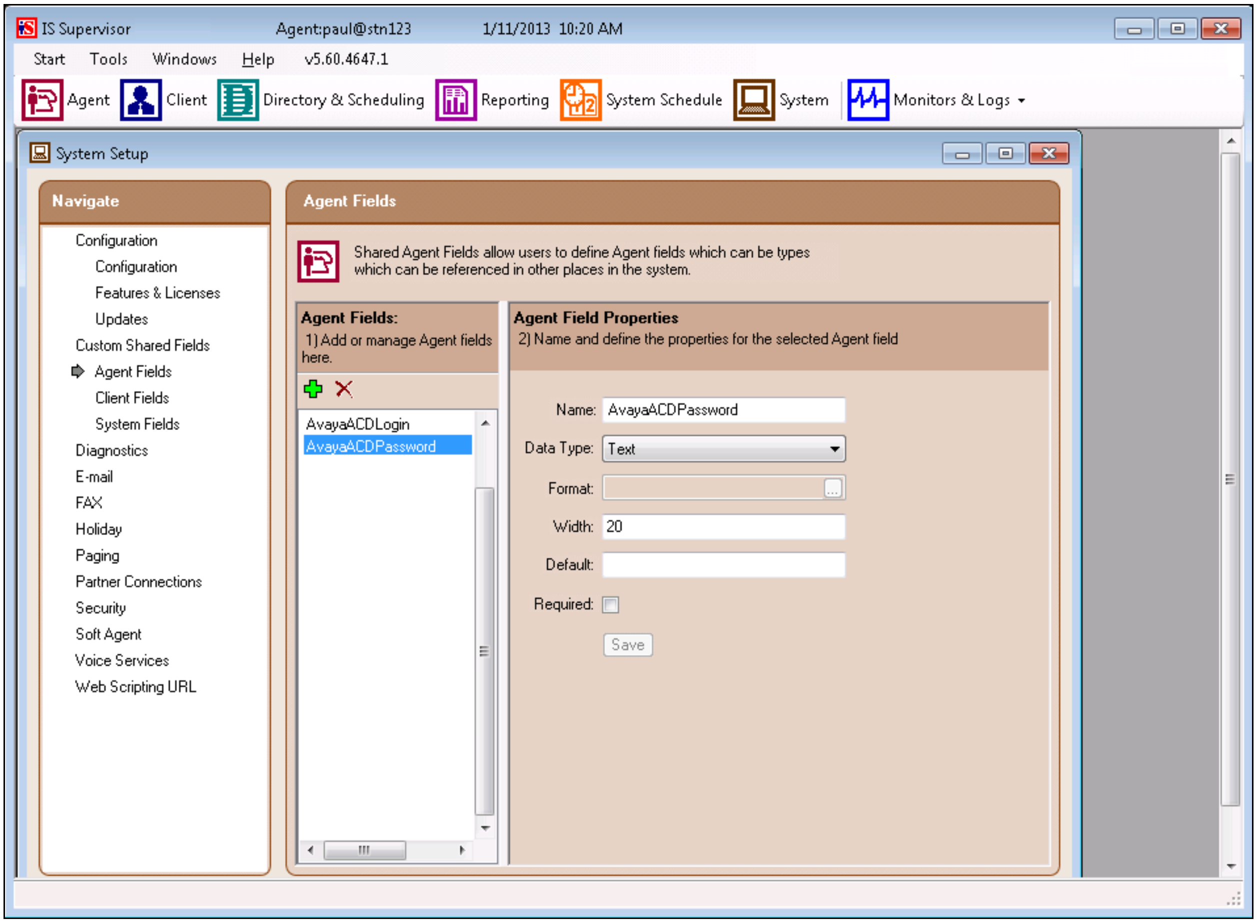
Format:

Width: 20

Default:

Required: □

Repeat this step to create a new shared agent field that corresponds to the **Password** field previously established in the Communication Manager software using the “add-agent-loginID *n*” procedure. In this example, the new shared agent field is **AvayaACDPassword**.
Retain the default values for the remaining fields. Click the **Save** button to write your entries to the Intelligent Series database.



Shared Agent Fields allow users to define Agent fields which can be types which can be referenced in other places in the system.

Agent Fields:
1) Add or manage Agent fields here.

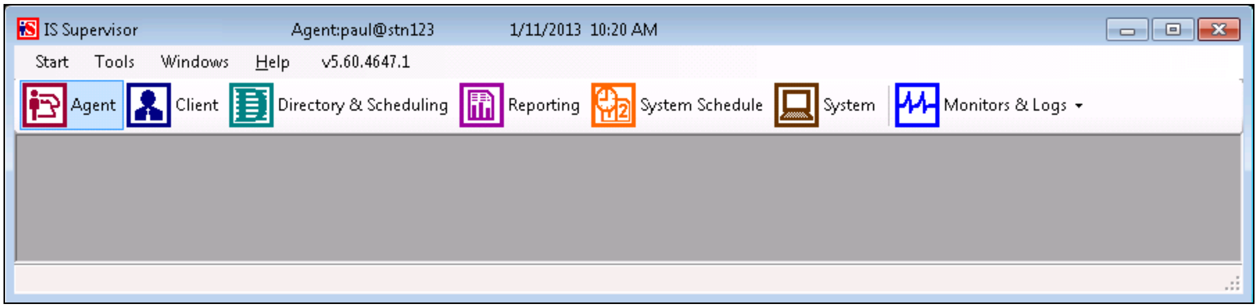
AvayaACDLogin
AvayaACDPassword

Agent Field Properties
2) Name and define the properties for the selected Agent field

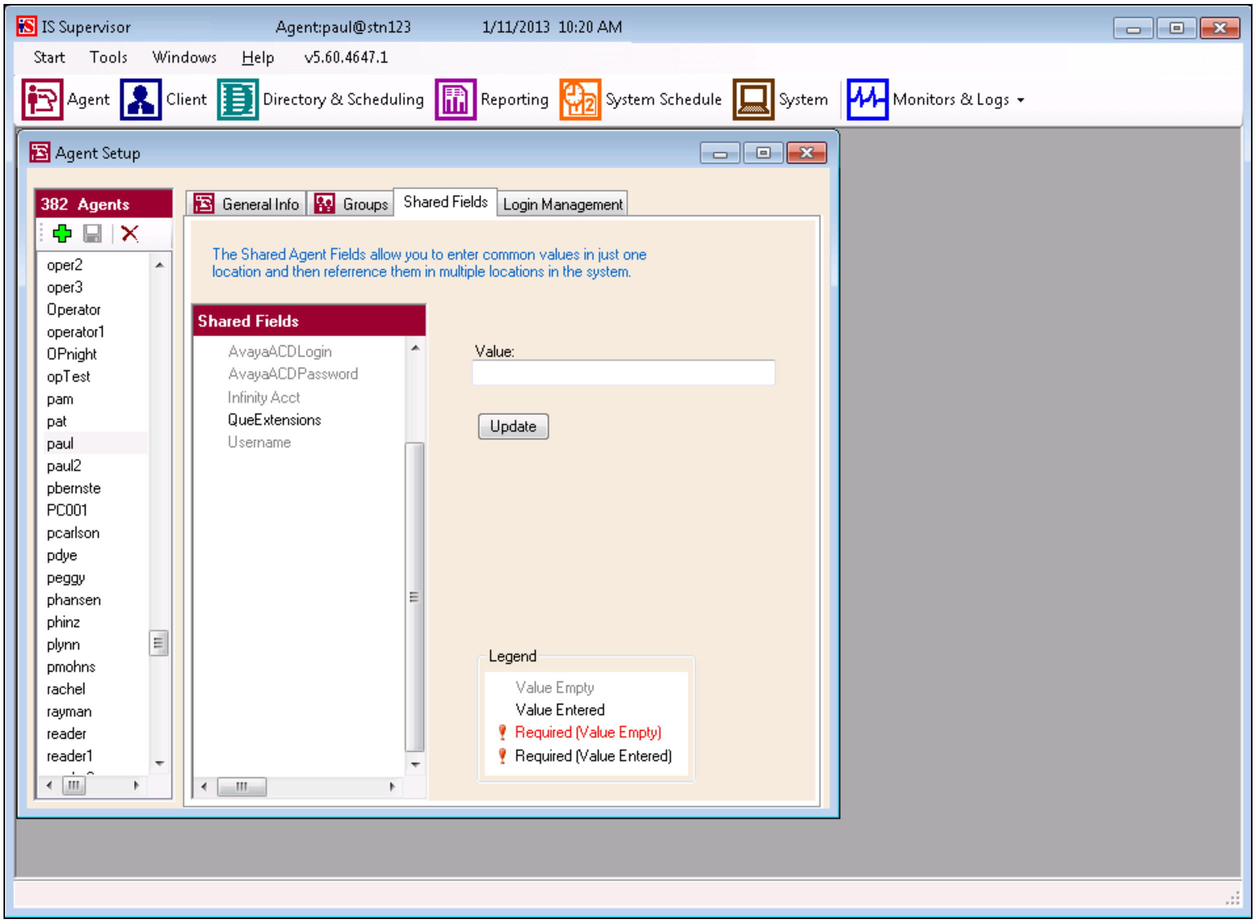
Name: AvayaACDPassword
Data Type: Text
Format:
Width: 20
Default:
Required: □

8.4. Administer Agent Settings

At the **IS Supervisor** toolbar screen, click the **Agent** icon at the top of the screen.



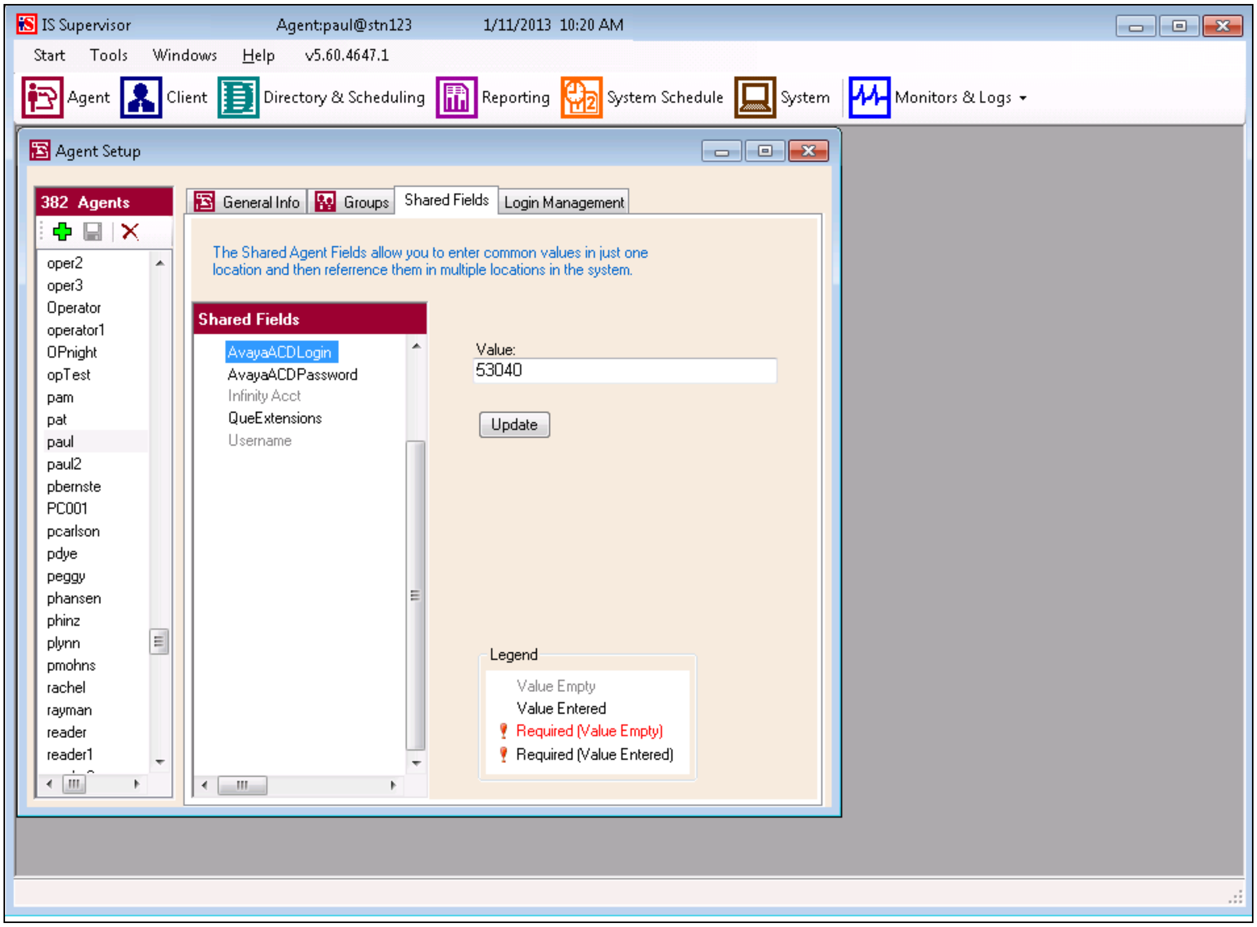
The **Agent Setup** screen is displayed in the lower pane.
Select an **Agent** name from the left pane, then turn to the **Shared Fields** tab at the top of the right pane.



The Shared Agent Fields allow you to enter common values in just one location and then refeerence them in multiple locations in the system.

In the **Shared Fields** list in the right pane, click on the first of the new shared fields just created on the System Setup screen, in this example the field is **AvayaACDLogin**. In the **Value** field list in the right pane, enter the value the new Shared Agent Field that reflects the value of the **Login ID** field previously established in the Communication Manager software using the “add-agent-loginID *n*” procedure. In this example, the value of the shared field is **53040** which is an ex extension on the Communication Manager.

Retain the default values for the remaining fields. Click the **Update** button to write your entry to the Intelligent Series database.


IS Supervisor Agent:paul@stn123 1/11/2013 10:20 AM

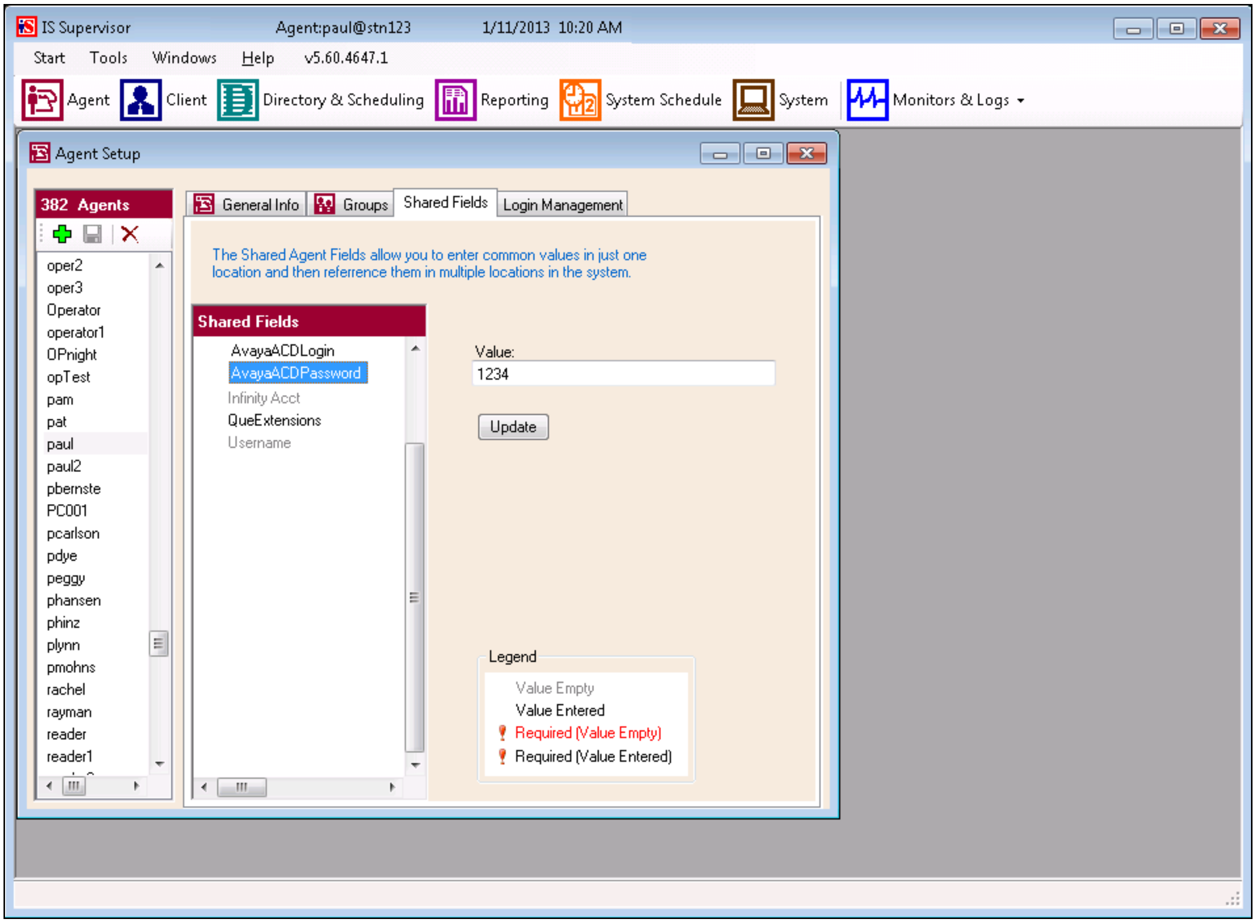
v5.60.4647.1

The Shared Agent Fields allow you to enter common values in just one location and then referrence them in multiple locations in the system.

Shared Fields: AvayaACDLogin

Value: 53040

In the **Shared Fields** list in the right pane, click on the second of the new shared fields just created on the System Setup screen, in this example the field is **AvayaACDPassword**.
In the **Value** field list in the right pane, enter the value the new Shared Agent Field that reflects the value of the **Password** field previously established in the Avaya Communication Manager software using the "add-agent-loginID *n*" procedure. In this example, the value of the shared field is **1234**.
Retain the default values for the remaining fields. Click the **Update** button to write your entry to the Intelligent Series database.



The Shared Agent Fields allow you to enter common values in just one location and then referrence them in multiple locations in the system.

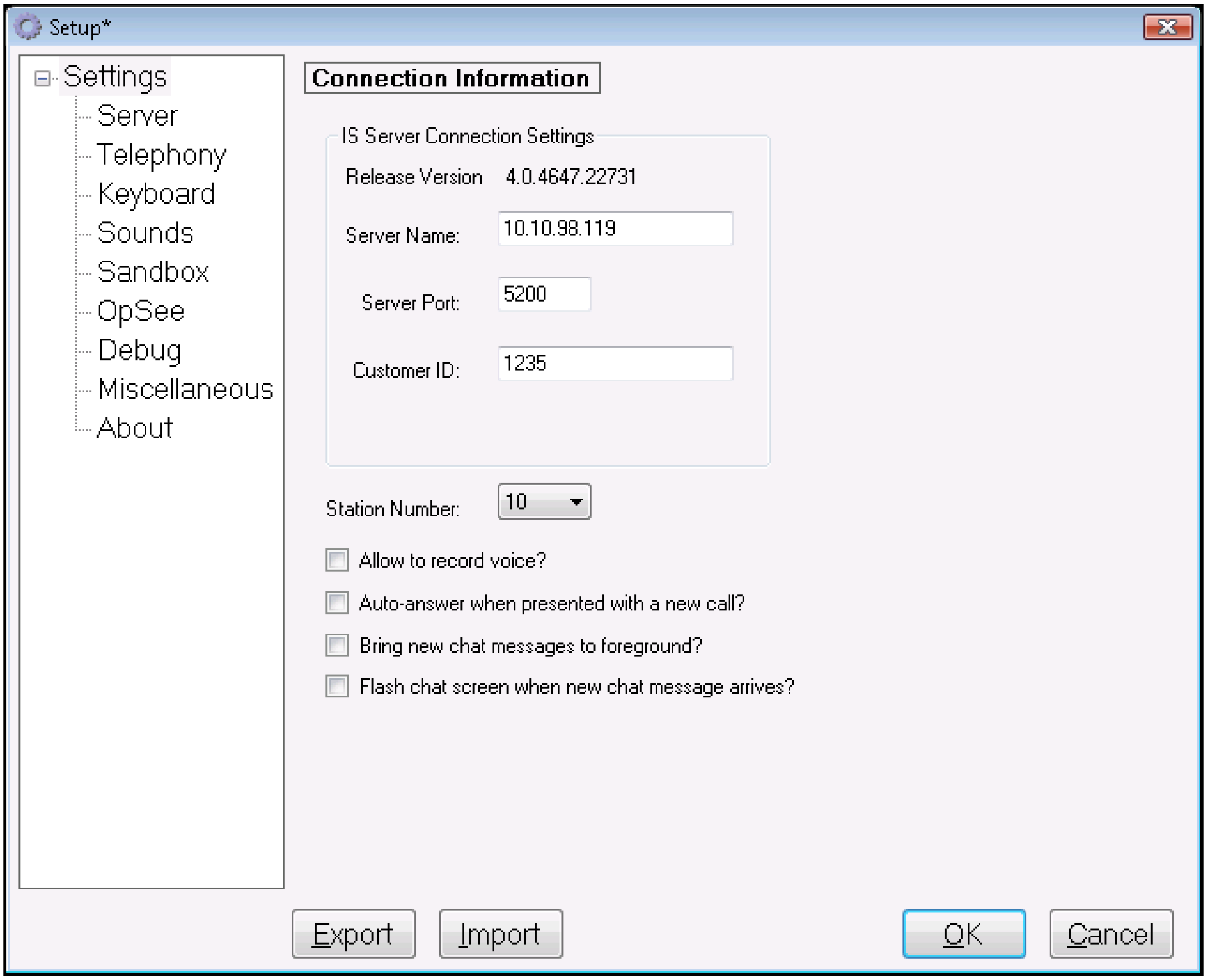
Value: 1234

Note: This completes the necessary steps for configuring the Intelligent Series Supervisor application.

8.5. Configure Amtelco Soft Agent Client

From workstation in which Amtelco Soft Agent application installed, navigate to menu **Start → All Programs → Amtelco → Soft Agent**. The Soft Agent application window is displayed.

Press combination key **Ctrl + F12** to open the **Setup** window. The **Setup** window is displayed. In the left navigation pane, select the **Server** tab. The **Connection Information** window is displayed in the right. In the **IS Server Connection Settings** section, enter IP address of Amtelco server **10.10.98.119** in the **Server Name** field, port **5200** in the **Server Port**, and a customer number **1235** in **Customer ID** field.



Release Version 4.0.4647.22731

Server Name: 10.10.98.119

Server Port: 5200

Customer ID: 1235

Station Number: 10

□ Allow to record voice?

□ Auto-answer when presented with a new call?

□ Bring new chat messages to foreground?

□ Flash chat screen when new chat message arrives?

Click on the **Telephony** tab, the "**Setup option for telephone interface**" window is displayed in the right. Select **Avaya DMCC-Phone** in the **Switch Type** dropdown menu, the **AE Server and Media** tabs are displayed below. In the **AE Sever** tab, configure following fields:

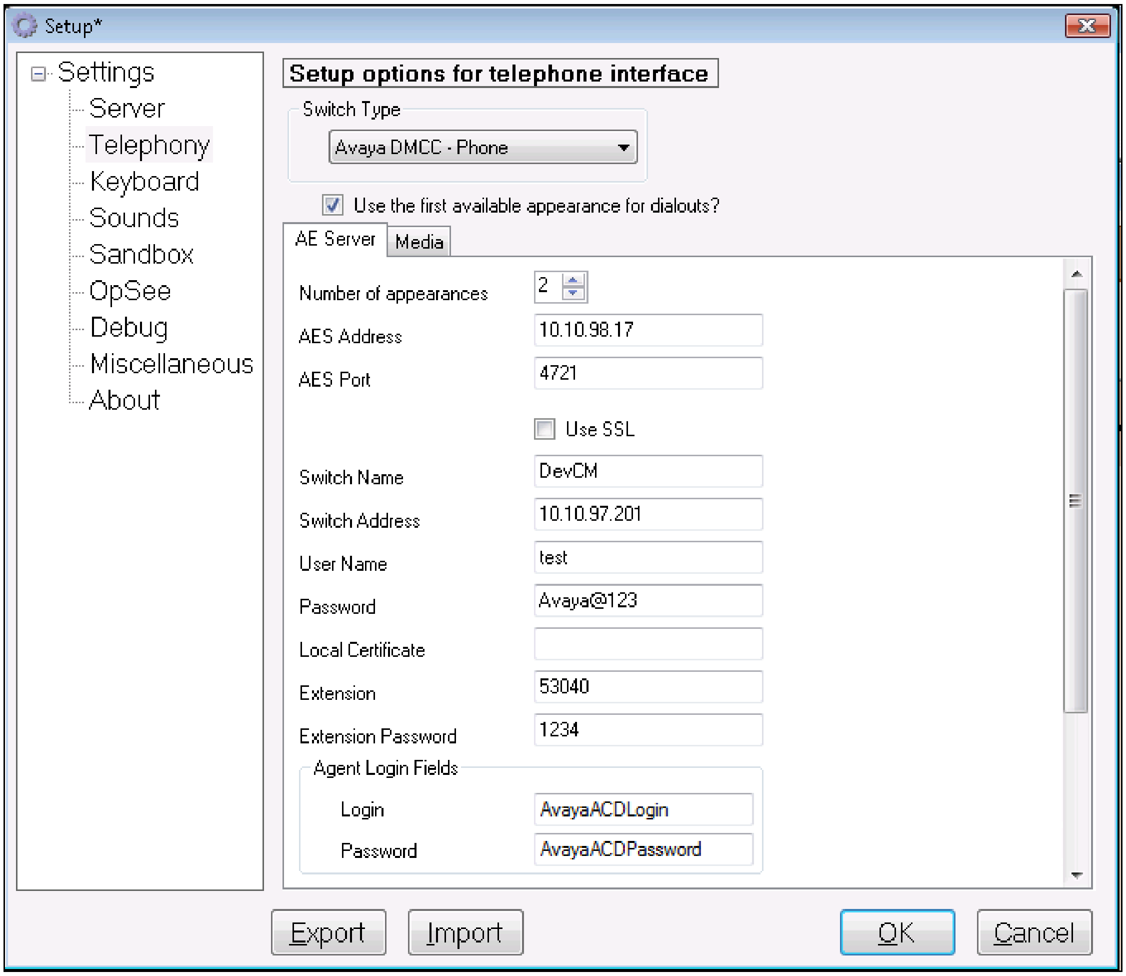
- **AES Address**: enter the IP address of AES client **10.10.98.17** as administered in **Section 7.2**

- **Port**: enter port **4721** as administered in **Section 7.5**.
- **Switch Name**: enter host name of Avaya Communication Manager Switch e.g. "**DevCM**".
- **Switch Address**: enter IP address of Avaya Communication Manager e.g. "**10.10.97.201**".
- **Username**: enter "**test**" CT user as administered in **Section 7.6**.
- **Password**: enter the password for the user "**test**" above.
- **Extension**: enter one of extensions as configured in **Section 6.12**.
- **Extension Password**: enter the security password of the extension above.

Agent Login Fields

- **Login**: enter an Agent Shard field that contains the EAS agent login. Suggested agent shared field name would be "AvayaACDLogin"
- **Password**: enter an Agent Shard field that contains the EAS agent login Suggested agent shared field name would be "AvayaACDPassword"

Press **OK** button to save changes.



Setup options for telephone interface

Switch Type: Avaya DMCC - Phone

☑ Use the first available appearance for dialouts?

Number of appearances	2
AES Address	10.10.98.17
AES Port	4721
	☐ Use SSL
Switch Name	DevCM
Switch Address	10.10.97.201
User Name	test
Password	Avaya@123
Local Certificate	
Extension	53040
Extension Password	1234

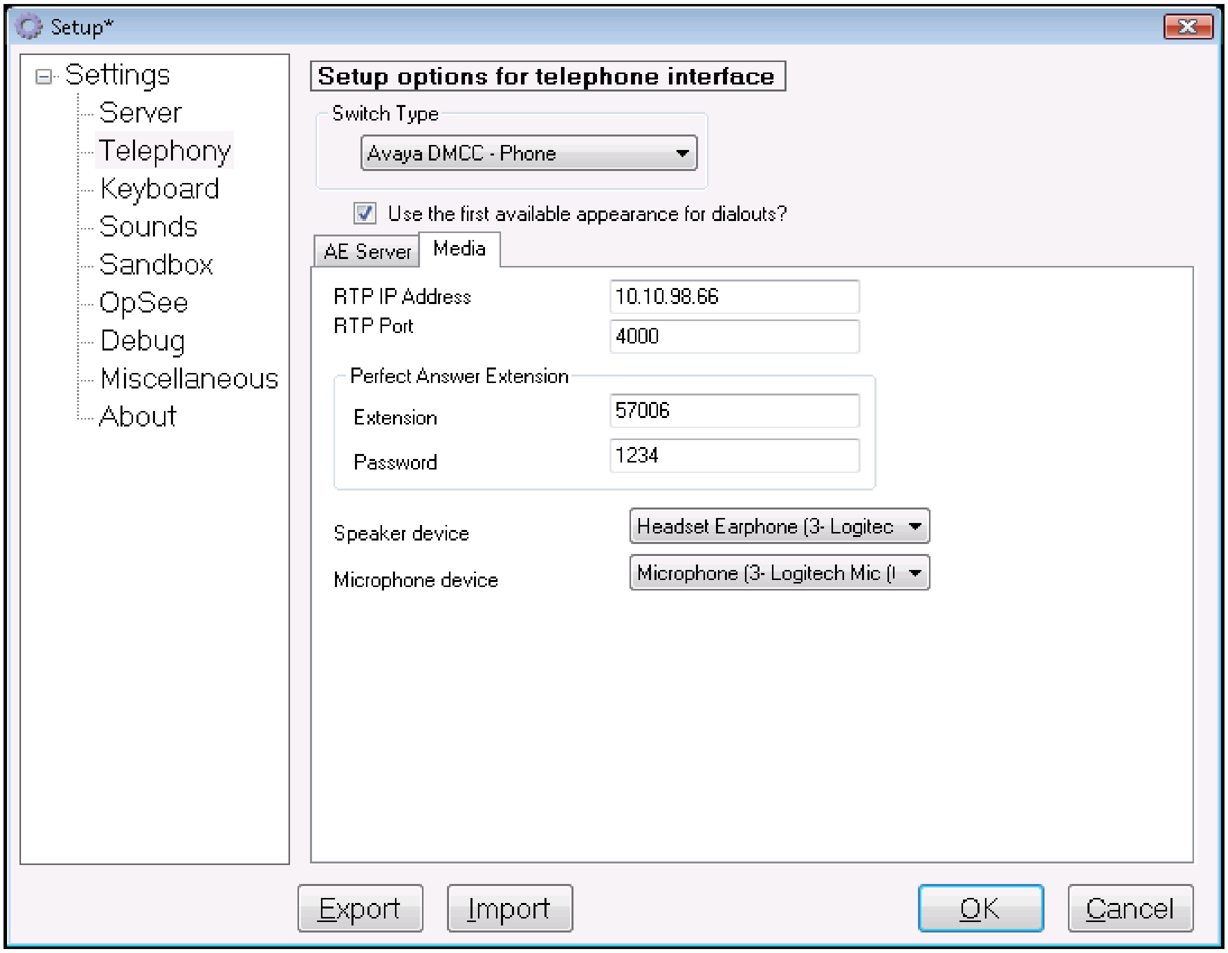
Agent Login Fields

Login	AvayaACDLogin
Password	AvayaACDPassword

Click on the **Media** tab, configure following fields:

- **RTP IP Address**: enter IP address of the workstation PC which the Soft Agent application installed e.g. "**10.10.98.66**".
- **RTP Port**: enter port "**4200**".
- **Perfect Answer Extension**:
- **Extension**: enter an available extension in the Communication Manager switch that is not used by any physical station e.g. "**57006**".
- **Password**: enter the security password of the extension above.
- **Speaker Device**: select an available speaker device in the workstation PC.
- **Microphone Device**: select an available microphone device in the workstation PC.

Click **OK** button to save changes and close the **Setup** window.



Switch Type: Avaya DMCC - Phone

☑ Use the first available appearance for dialouts?

RTP IP Address: 10.10.98.66

RTP Port: 4000

Perfect Answer Extension

Extension: 57006

Password: 1234

Speaker device: Headset Earphone (3- Logitec

Microphone device: Microphone (3- Logitech Mic (l

9. Verification Steps

The following are typical steps used to verify that Amtelco Soft Agent works with Application Enablement Services and Communication Manager.

1. Use the Amtelco Soft Agent to log physical agent phone in and change the status from Auxiliary to Auto-in.
2. Use the command "monitor bcms skill 1" to show the status of the agent that has been logged in by Soft Agent

```
monitor bcms skill 1                                        Page   1 of   1
                           BCMS SKILL (AGENT) STATUS

        Skill: 1                              Date:   0:39 FRI DEC 28 2012
   Skill Name: Hunt1
Calls Waiting:    0                         Acceptable Service Level: 20
  Oldest Call:   0:00                         % Within Service Level:

Staffed: 1   Avail: 1   ACD: 0   ACW: 0   AUX: 0   Extn Calls: 0   Other: 0

                                                              ACD   EXT IN  EXT OUT
AGENT NAME       LOGIN ID      EXT           STATE   TIME   CALLS   CALLS   CALLS

Agent2           1001          53010         Avail   16:51    0       0       0
```

3. Place a call to hunt group. The call is queued to the skill1 and come to available agent phone.
4. Answer the call on the physical agent phone by using the Amtelco Soft Agent.
5. Hang up the call by using the Amtelco Soft Agent.
6. Exit the Amtelco Soft Agent, the physical agent phone is logged out.

10. Conclusion

All test cases in the test plan were executed and passed. The **Amtelco Soft Agent** application Version 4.0.4647 is considered to successfully integrate with Avaya Aura® Application Enablement Services Release 6.2 and Avaya Aura® Communication Manager Release 6.2.

11. Additional References

The following Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Release 6.2, June 2012, Issue 6.0, Document Number 03-300509.

[2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.2, July 2012, Issue 1.

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.