



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for CCT Deutschland GmbH ContactPro® 7.0 using Avaya Client SDK and Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Enablement Services 10.1 - Issue 1.0

## Abstract

These Application Notes describe the configuration steps required to integrate CCT ContactPro® Version 7.0 using Avaya Client SDK, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Application Enablement Services 10.1.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1**, as well as 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 CCT ContactPro® 7.0 from CCT Deutschland GmbH, to interoperate with Avaya Client SDK, Avaya Aura® Session Manager 10.1, Avaya Aura® Communication Manager 10.1, and Avaya Aura® Application Enablement Services (AES) 10.1.

The CCT ContactPro® solutions offer a variety of integrations into the Avaya call center environment, supporting different Avaya platforms to interact for multimedia agents as well as for voice only agents. CCT ContactPro® is a solution for agent desktops in an Avaya call center environment focused on voice and multimedia such as email and webchat. CCT ContactPro® can be installed with enabled Presence Services and integrated Customer Data and empowers agents to efficiently serve customers by allowing the agents have full call control from the agent's screen.

CCT ContactPro® 7.0 includes a software application that serves as a softphone running as a rich client. CCT ContactPro® 7.0 solution integrated with Avaya Client SDK to register as SIP endpoint with Avaya Aura® Session Manager.

## 2. General Test Approach and Test Results

Interoperability testing contained functional tests mentioned in **Section 2.1**. All test cases were performed manually. The general test approach was to validate successful handling of inbound skillset/VDN calls using ContactPro Client. This was performed by calling inbound to a VDN and/or outbound from the elite call center using ContactPro to answer calls. Where applicable, agent actions were performed using the ContactPro Agent Client.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the CCT ContactPro® 7.0 solution with DMCC interface between Avaya Aura® AES and the CCT ContactPro® 7.0 solution did not include use of any specific encryption features as requested by CCT.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. Feature testing included the validation of the following:

- **Registration** - Successful registration of CCT ContactPro® 7.0 with Avaya Aura® Session Manager and Avaya Aura® AES.
- **Agent state change**– Login, Ready/Not Ready using ContactPro Agent.
- **Inbound and Outbound Calls** between CCT ContactPro® 7.0 Client and Avaya SIP, H.323, and digital telephones. Calls between Contact Pro Client and PSTN endpoints. Calls with G.711, OPUS codec support and negotiation, with and without media shuffling. Calls with SRTP enabled and disabled. DTMF transmission.
- **Hold/Transfer/Conference** – Place callers on hold and transfer and conference using ContactPro Agent.
- **Serviceability** - The serviceability testing focused on verifying the ability of CCT ContactPro® 7.0 Client to recover from adverse conditions, such as disconnecting/reconnecting the network to ContactPro Server.

## 2.2. Test Results

The testing was successful. All test cases passed.

## 2.3. Support

Support for CCT products can be obtained as follows:

### WEBSITE

[www.cct-solutions.com](http://www.cct-solutions.com)

### CONTACT

Phone: +49 69 7191 4969 0

Email: [contact@cct-solutions.com](mailto:contact@cct-solutions.com)

### SUPPORT

Hotline: +49 821 455152 455

Email: [helpdesk@cct-solutions.com](mailto:helpdesk@cct-solutions.com)

### CCT Solutions

#### Deutschland GmbH

Tilsiter Str. 1

60486, Frankfurt am Main

Germany

Phone +49 69 7191 4969 0

#### CCT Software LLC

1801 N.E. 123rd Street, Suite 314

North Miami, 33181 FL

United States of America

Phone +1 786 738 5253

### 3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya products and the CCT ContactPro® 7.0.

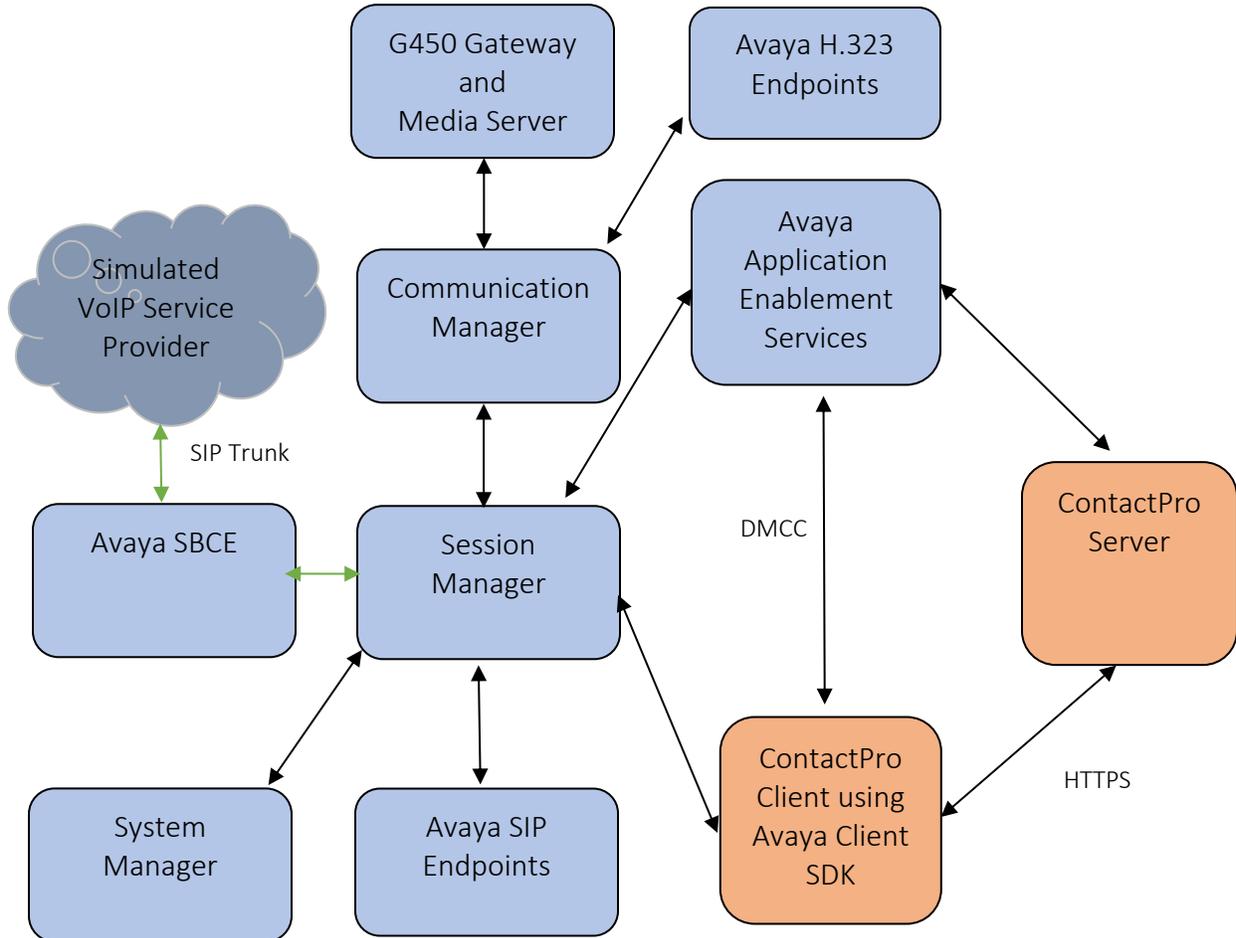


Figure 1: Test Configuration for CCT ContactPro® and the Avaya Platforms.

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

<b>Equipment/Software</b>	<b>Release/Version</b>
Avaya Aura® System Manager in Virtual Environment	10.1.2.
Avaya Aura® Session Manager in Virtual Environment	10.1.2.0.1012016
Avaya Aura® Communication Manager in Virtual Environment	10.1.2 - 01.0.974.0-27783
Avaya G450 Media Gateway	41.16.30
Avaya Aura® Media Server in Virtual Environment	10.1.0.125
Avaya Session Border Controller for Enterprise in Virtual Environment	10.1.0.0-32-21432
Avaya Client SDK	4.25.0
Avaya Workplace Client for Windows	3.29.0.54
Avaya 9641 and J159 (H.323) Deskphone	6.8.5
Avaya J159 and Avaya J179 (SIP) Deskphone	4.0.7
CCT ContactPro® Server	7.0

## 5. Configure Avaya Aura® System Manager

In this section, the configuration steps to create a user on System Manager and Session Manager. It is assumed that an existing Session manager instance has already been installed and configured as this is out of scope of this document. All Configuration steps were carried out using System Manager. Configuration steps will include:

- Launch System Manager
- Add SIP Users

### 5.1. Launch System Manager

Access the System Manager Web interface by using the URL “https://<IP Address>/SMGR” in an internet browser window, where <IP Address> is the IP address of the System Manager server. Log in using the appropriate credentials.

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

---

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

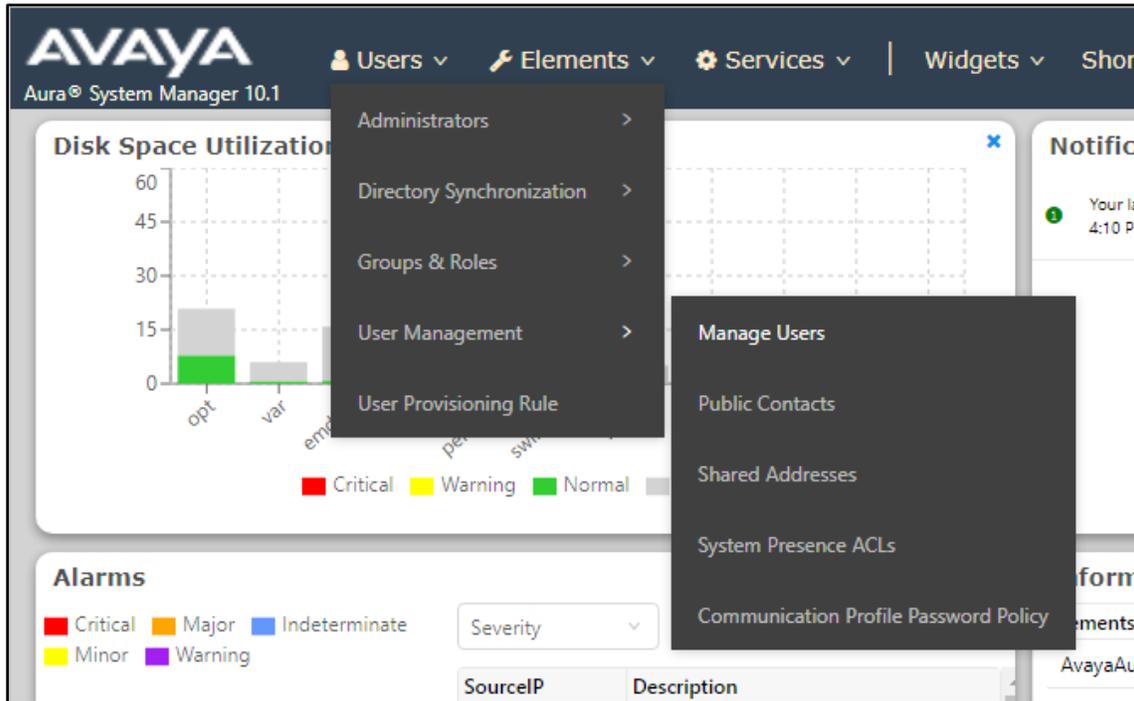
Password:

[Change Password](#)

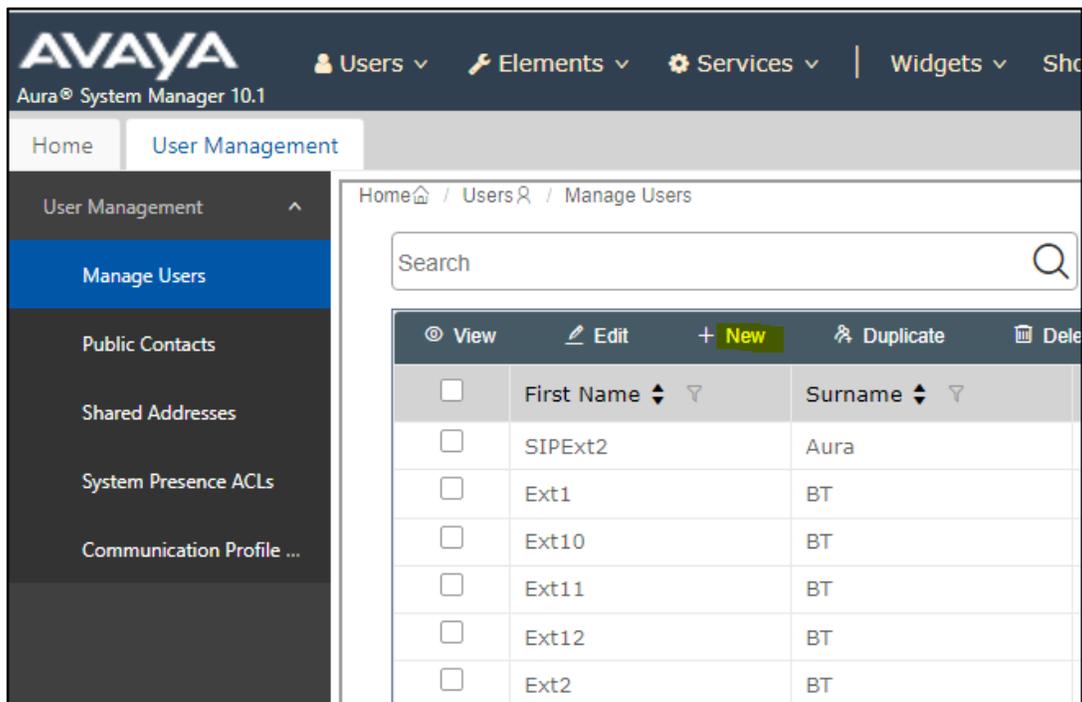
**Supported Browsers:** Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

## 5.2. Add SIP Users

From the Dashboard, select **Users** → **User Management** → **Manage Users**.



Select **New**.



On the Identity tab, enter an identifying **Last Name** and **First Name**, enter an appropriate **Login Name**, set **Authentication Type** to **Basic** and administer a password in the **Password** and **Confirm Password** fields.

The screenshot shows the 'User Profile | Add' form with the 'Identity' tab selected. The 'Basic Info' section is active, showing the following fields:

- User Provisioning Rule:** AuraUPR
- \* Last Name:** ContactPro
- Last Name (in Latin alphabet characters):** ContactPro
- \* First Name:** Ext71018
- First Name (in Latin alphabet characters):** Ext71018
- \* Login Name:** 71018@aura.com
- Middle Name:** Middle Name Of User

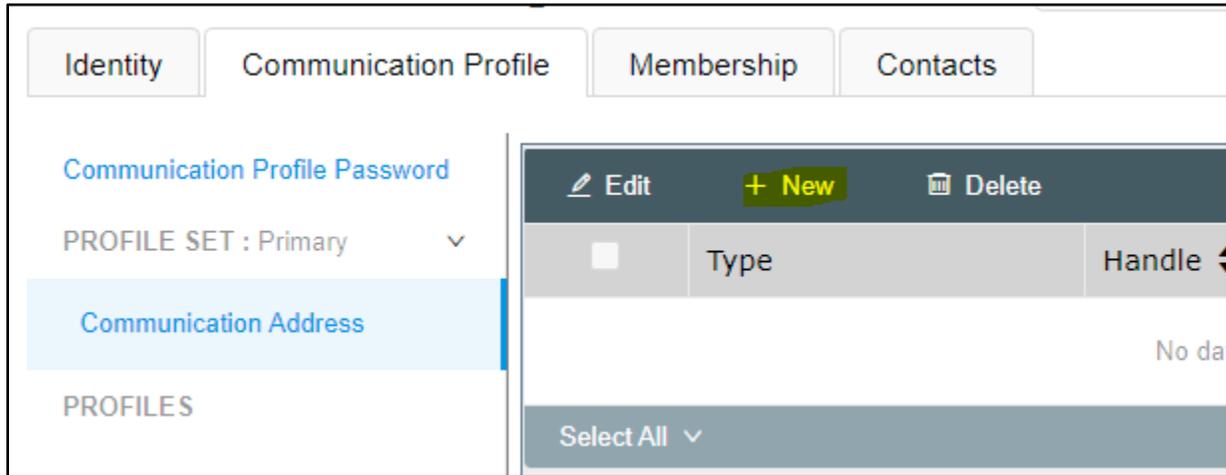
Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint.

The screenshot shows a 'Comm-Profile Password' dialog box with the following fields:

- Comm-Profile Password:** [Masked with dots]
- \* Re-enter Comm-Profile Password:** [Masked with dots and a green checkmark]

Buttons: Cancel, OK, and a link for 'Generate Comm-Profile Password'.

Click on the **Communication Address**, select **New**.



Select **Avaya SIP** from the **Type** drop down box and enter the **Fully Qualified Address** of the new SIP user. Click **Ok** when done.

The dialog box is titled 'Communication Address Add/Edit' and contains the following fields:

- \* Type :** A dropdown menu with 'Avaya SIP' selected.
- \*Fully Qualified Address :** A text input field containing '71018' followed by an '@' symbol and a dropdown menu with 'aura.com' selected.

At the bottom right, there are two buttons: 'Cancel' and 'OK'.

Continue to scroll down on the same page. Enable **Session Manager Profile** and enter the **Primary Session Manager, Origination Application Sequence, Termination Application Sequence** and **Home Location** relevant to the implementation.

Identity	Communication Profile	Membership	Contacts
<b>Communication Profile Password</b>			
PROFILE SET : Primary			
Communication Address			
<b>PROFILES</b>			
Session Manager Profile <input checked="" type="checkbox"/>			
CM Endpoint Profile <input checked="" type="checkbox"/>			
<b>SIP Registration</b>			
* Primary Session Manager : SM126SIP			
Secondary Session Manager : Start typing...			
Survivability Server : Start typing...			
Max. Simultaneous Devices : 3			
Block New Registration When Maximum Registrations Active? : <input type="checkbox"/>			
<b>Application Sequences</b>			
Origination Sequence : CM121			
Termination Sequence : CM121			
<b>Emergency Calling Application Sequences</b>			
Emergency Calling Origination Sequence : Select			
Emergency Calling Termination Sequence : Select			
<b>Call Routing Settings</b>			
* Home Location : HCMC			

Scroll down the page and enable **CM Endpoint Profile** section. Select the Communication Manager system from the **System** drop down box, select **Endpoint** as the **Profile Type**, enter the **Extension** number available, select **J179CC\_DEFAULT\_CM\_10\_1** as the **Template** and ensure **IP** is configured as the **Port**, click **Commit & Continue** (not shown) when finished.

The screenshot shows a configuration form for a CM Endpoint Profile. The fields are as follows:

- \* System:** CMSimplex121
- \* Profile Type:** Endpoint
- Use Existing Endpoints:**
- \* Extension:** 71018
- \* Template:** J179CC\_DEFAULT\_CM
- \* Set Type:** J179CC
- Security Code:** .....
- Port:** IP
- Voice Mail Number:** [Empty]
- Preferred Handle:** Select
- Calculate Route Pattern:**
- Sip Trunk:** [Empty]
- SIP URI:** Select
- Delete on Unassign from User or on Delete User:**
- Override Endpoint Name and Localized Name:**
- Allow H.323 and SIP Endpoint Dual:**

Click on **Endpoint Editor** in the **CM Endpoint Profile** and on the General options tab set **Type** of **3PCC Enabled** as **Avaya**.

The screenshot shows the General Options tab in the Endpoint Editor. The fields are as follows:

- \* Class of Restriction (COR):** 1
- \* Class of Service (COS):** 1
- \* Emergency Location Ext:** 71018
- \* Message Lamp Ext.:** 71018
- \* Tenant Number:** 1
- \* SIP Trunk:** aar
- Type of 3PCC Enabled:** Avaya
- Coverage Path 1:** [Empty]
- Coverage Path 2:** [Empty]
- Localized Display Name:** [Empty]
- Enable Reachability for Station Domain Control:** [Empty]
- SIP URI:** [Empty]
- Primary Session Manager:**
  - IPv4:** [Empty]
  - IPv6:** [Empty]
- Secondary Session Manager:**
  - IPv4:** [Empty]
  - IPv6:** [Empty]

Click on **Feature Options (F)** tab, scroll down and check **IP SoftPhone** and **IP Video Softphone**. Click on **Done** to save changes and go back to the User Communication Profile screen.

**Features**

- Always Use
- IP Audio Hairpinning
- Bridged Call Alerting
- Bridged Idle Line Preference
- Coverage Message Retrieval
- Data Restriction
- Survivable Trunk Dest
- Bridged Appearance Origination Restriction
- Restrict Last Appearance
- Turn on mute for remote off-hook attempt
- IP Hoteling
- Idle Appearance Preference
- IP SoftPhone
- LWC Activation
- CDR Privacy
- Direct IP-IP Audio Connections
- H.320 Conversion
- IP Video Softphone
- Per Button Ring Control

Click on **Button Assignment (B)** tab (not shown), then click on **Button Feature** tab and configure the following:

**Main Buttons** | **Feature Buttons** | **Button Modules**

**Endpoint Configurations**

Favorite	Button Label
<input type="checkbox"/>	

**Button Configurations**

Button Feature	Argument-1	Argument-2	Argument-3
call-appr Auto-A/D	Ring		
call-appr Auto-A/D	Ring		
call-appr Auto-A/D	Ring		
agnt-login			
aux-work Reason Code	Hunt Grp		
auto-in auto-in Grp			
manual-in manual-in Grp			
after-call after-call			

Click on **Commit** to save the user. The user is now listed. In this compliance testing, 4 Users were created.

## 6. 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 hunt group and agent

### 6.1. Verify License

Log into 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? y              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.)
```

### 6.2. 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: 79999
Type: ADJ-IP                                                         COR: 1
Name: aes140
```

### 6.3. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Vector Directory Number (VDN), which points to a vector. The vector then points to a hunt group associated with an agent. Agent can use ContactPro as agent desktops for handling incoming and outgoing calls with WebRTC voice through Avaya Aura® Web Gateway (AAWG).

The following sections give step by step instructions on how to add the following.

- Add Hunt Group
- Add Agent
- Administer Vectors and VDNs

#### 6.3.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x**, where **x** is the new hunt group number. For example, hunt group **1** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.

```
add hunt-group 1                                     Page 1 of 4
                                                    HUNT GROUP
      Group Number: 1                                ACD? y
      Group Name: Voice Service                       Queue? y
      Group Extension: 79010                          Vector? y
      Group Type: ucd-mia
      TN: 1
      COR: 1                                          MM Early Answer? n
      Security Code:                                Local Agent Preference? n
      ISDN/SIP Caller Display:
      Queue Limit: unlimited
      Calls Warning Threshold:      Port:
      Time Warning Threshold:      Port:
```

On **Page 2** ensure that **Skill** is set to **y** as shown below.

```
add hunt-group 1                                     Page 2 of 4
                                                    HUNT GROUP
      Skill? y                                       Expected Call Handling Time (sec): 180
      AAS? n
      Measured: none
      Supervisor Extension:
      Controlling Adjunct:
      Multiple Call Handling: none
      Timed ACW Interval (sec):                    After Xfer or Held Call Drops? n
```

### 6.3.2. Add Agent

In the compliance testing, there are 5 agents are created. To add a new agent, type **add agent-loginID x**, where x is the login id for the new agent. enter an identifying **Name**, set **Password** ad **Password (enter again)**..

```

add agent-loginID 75018                                     Page 1 of 3
                                AGENT LOGINID

Login ID: 75018                                           AAS? n
Name: Voice Agent                                         AUDIX? n
TN: 1                                                     Check skill TNs to match agent TN? n
COR: 1
Coverage Path:                                           LWC Reception: spe
Security Code:                                           LWC Log External Calls? n
                                                AUDIX Name for Messaging:

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
  
```

On **Page 2**, add the required skills. Note that the skill **1** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly to this agent.

```

add agent-loginID 75018                                     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:
7:         22:  37:      52:
8:         23:  38:      53:
9:         24:  39:      54:
10:        25:  40:      55:
  
```

Repeat this section to add other agents.

## 6.4. Administer Vectors and VDNs

Add a vector using the **change vector n** command, where **n** is a vector number. Note that the vector steps may vary, and below is a sample vector used in the compliance testing.

```
change vector 18                                     Page 1 of 6
                                                    CALL VECTOR
Number: 1                                           Name: VoiceService
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      2   secs hearing silence
02 queue-to       skill 1   pri t
03 wait-time      2   secs hearing silence
04 stop
05
06
07
08
09
10
11
12

Press 'Esc f 6' for Vector Editing
```

Add a VDN using the **add vdn n** command, where **n** is an available extension number. Enter a descriptive Name and the vector number from above for **Destination**. Retain the default values for all remaining fields.

```
change vdn 78018                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
Extension: 78018                                     Unicode Name? n
Name*: Voice VDN
Destination: Vector Number      18
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none      Report Adjunct Calls as ACD*? n

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

SIP URI:
* Follows VDN Override Rules
```

## 7. Configure Avaya Aura® Application Enablement Services

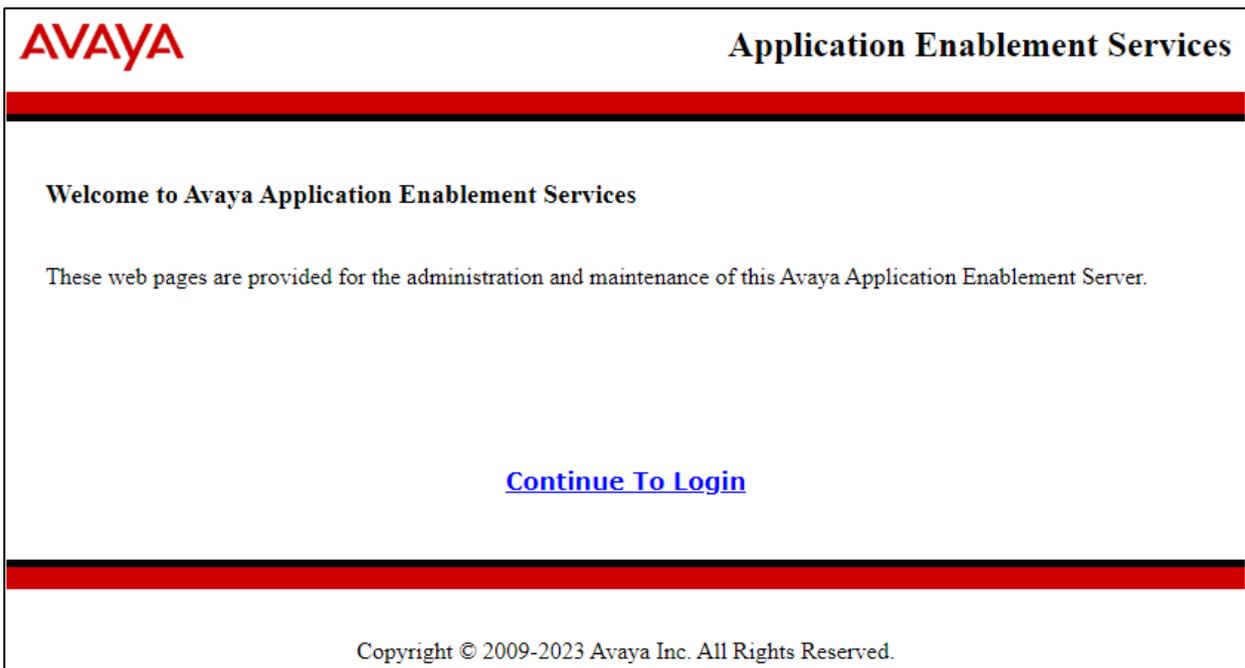
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer CCT user
- Enable CTI User
- Administer security database
- Restart services
- Obtain Tlink name

### 7.1. 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 **Welcome to OAM** screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the text 'Application Enablement Services Management Console'. At the top right, there is a welcome message and system information: 'Welcome: User cust', 'Last login: Fri Mar 17 14:21:10 I.T. 2023 from 172.16.8.85', 'Number of prior failed login attempts: 0', 'HostName/IP: aes140.aura.com/10.30.5.140', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 10.1.2.0.0.12-0', 'Server Date and Time: Wed Mar 29 17:52:27 ICT 2023', and 'HA Status: Not Configured'. Below this is a red navigation bar with 'Home' on the left and 'Home | Help | Logout' on the right. On the left side, there is a vertical menu with the following items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area is titled 'Welcome to OAM' and contains the following text: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. This is followed by a bulleted list of domains and their uses: '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.', and 'Help - Use Help to obtain a few tips for using the OAM Help system'. At the bottom of the main content area, it states: 'Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.'

## 7.2. 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 displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the text "Application Enablement Services Management Console". At the top right, a user status block shows: "Welcome: User cust", "Last login: Fri Mar 17 14:21:10 I.T. 2023 from 172.16.8.85", "Number of prior failed login attempts: 0", "HostName/IP: aes140.aura.com/10.30.5.140", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 10.1.2.0.0.12-0", "Server Date and Time: Wed Mar 29 17:54:11 ICT 2023", and "HA Status: Not Configured". A red navigation bar contains "Licensing | WebLM Server Access" on the left and "Home | Help | Logout" on the right. A left-hand navigation menu lists: "AE Services", "Communication Manager Interface", "High Availability", "Licensing" (expanded), "WebLM Server Address", "WebLM Server Access" (highlighted), "Reserved Licenses", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "WebLM Server Access" and contains the text: "WebLM Server Access helps you to access the WebLM server specified on the WebLM Server Address page." followed by two bullet points: "• If you are using a local Avaya WebLM server, the AE Services management console redirects you to the Web License Manager page for WebLM configuration." and "• If you are using a standalone WebLM server, you must manually log in to the WebLM server for WebLM configuration."

Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

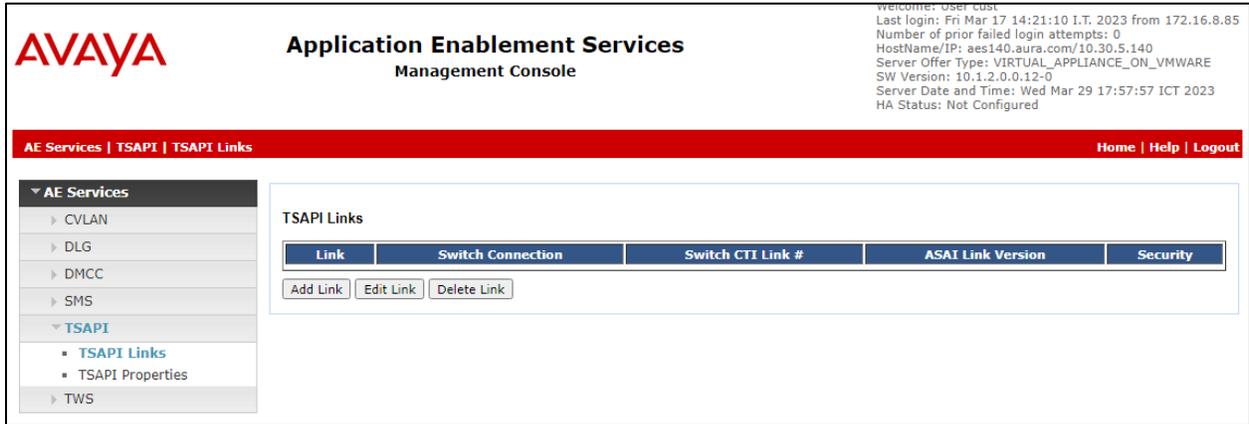
Verify that there are sufficient licenses for **Device Media and Call Control**, as shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left navigation pane is expanded to 'Application\_Enablement'. The main content area displays the 'Application Enablement (CTI) - Release: 10 - SID: 10503000' page. The page includes a breadcrumb trail, the license installation date, and the license file host ID. Below this, there is a 'Licensed Features' section with a table of 14 items.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	1000
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1000
AES ADVANCED AGENT VALUE_AES_ADVANCED_AGENT	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	1000
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1000
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	1000
DLG VALUE_AES_DLG	permanent	1000
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000

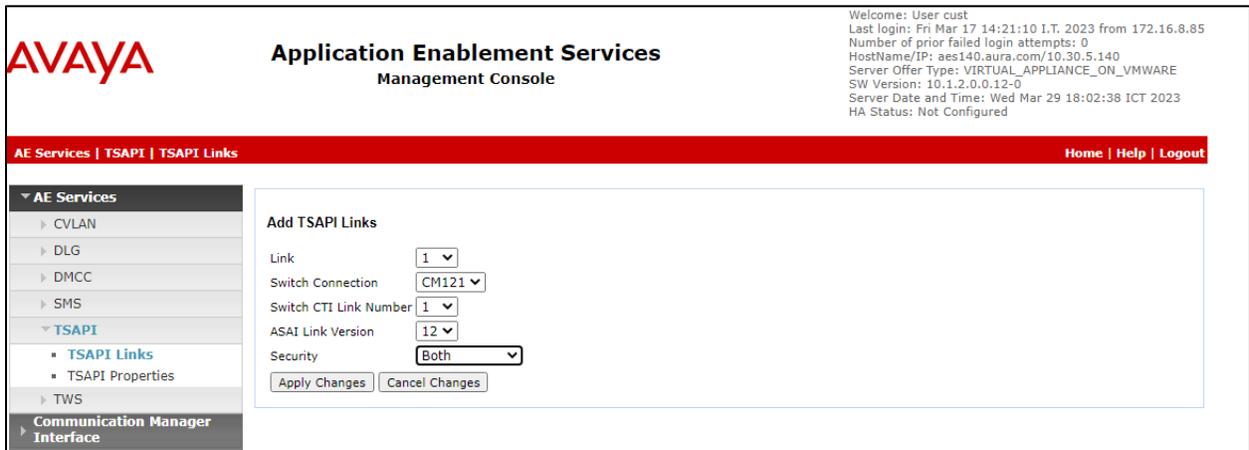
### 7.3. Administer TSAPI Link

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 **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 **CM121** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 7.2**. Retain the default values in the remaining fields.



## 7.4. Administer CCT 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo, and the top right shows the title 'Application Enablement Services Management Console'. A red navigation bar contains the breadcrumb 'User Management | User Admin | Add User'. On the left is a sidebar menu with categories like 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Service Admin', 'User Admin', 'Utilities', and 'Help'. The 'User Admin' section is expanded, showing 'Add User' as the selected option. The main content area is titled 'Add User' and includes a note: 'Fields marked with \* can not be empty.' The form contains the following fields: '\* User Id' (text input with 'cct'), '\* Common Name' (text input with 'cct'), '\* Surname' (text input with 'cct'), '\* User Password' (password input with 8 dots), '\* Confirm Password' (password input with 8 dots), 'Admin Note' (text input), 'Avaya Role' (dropdown menu with 'None' selected), 'Business Category' (text input), 'Car License' (text input), 'CM Home' (text input), 'Css Home' (text input), 'CT User' (dropdown menu with 'Yes' selected), 'Department Number' (text input), 'Display Name' (text input), 'Employee Number' (text input), and 'Employee Type' (text input).

## 7.5. Enable CTI User

Navigate to the CTI Users screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. In the CTI Users window, select the user that was set up in **Section Error!** Reference source not found. and select the **Edit** option.

Security | Security Database | CTI Users | List All Users Home | Help | Logout

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> cct	cct	NONE	NONE
<input type="radio"/> globitel	globitel	NONE	NONE
<input type="radio"/> uniphore	uniphore	NONE	NONE

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

Security | Security Database | CTI Users | List All Users Home | Help | Logout

Edit CTI User

User Profile: User ID: cct  
Common Name: cct  
Worktop Name: NONE  
Unrestricted Access:

---

Call and Device Control: Call Origination/Termination and Device Status: None

---

Call and Device Monitoring: Device Monitoring: None  
Calls On A Device Monitoring: None  
Call Monitoring:

---

Routing Control: Allow Routing on Listed Devices: None

## 7.6. 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 security database is used by the customer with parameters already enabled, then follow reference [4] in **Section 11** to configure access privileges for the CCT user from **Section 7.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". On the right, a welcome message for user "User cust" is shown, including login details and system status. A red navigation bar contains "Security | Security Database | Control" and "Home | Help | Logout". The left sidebar lists various service categories, with "Security" expanded to show "Control" selected. The main content area is titled "SDB Control for DMCC, WTI, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC and WTI Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

## 7.7. Restart Services

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Last login: Fri Mar 31 15:18:01 I.T. 2023 from 172.16.8.167, Number of prior failed login attempts: 0, HostName/IP: aes140.aura.com/10.30.5.140, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 10.1.2.0.0.12-0, Server Date and Time: Fri Mar 31 20:14:42 ICT 2023, HA Status: Not Configured.

The navigation bar shows "Maintenance | Service Controller" and "Home | Help | Logout". The left sidebar menu includes: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, Status, User Management, Utilities, and Help.

The main content area is titled "Service Controller" and contains a table with the following data:

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
<input type="checkbox"/> WTI Service	Running

Below the table, a note states: "Note: DMCC Service must be restarted for WTI service changes to take effect. For status on actual services, please use [Status and Control](#)".

At the bottom of the main content area, there are several buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

## 7.8. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring ContactPro.

In this case, the associated Tlink name is **AVAYA#CM121#CSTA#AES140**. Note the use of the switch connection **CM121** from **Section 7.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". On the right, system information is provided: "Welcome: User cust", "Last login: Fri Mar 17 14:21:10 I.T. 2023 from 172.16.8.85", "Number of prior failed login attempts: 0", "HostName/IP: aes140.aura.com/10.30.5.140", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 10.1.2.0.0.12-0", "Server Date and Time: Wed Mar 29 18:08:48 ICT 2023", and "HA Status: Not Configured".

A red navigation bar contains "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar lists various services, with "Security Database" expanded to show "Tlinks" selected. The main content area, titled "Tlinks", shows a "Tlink Name" section with two radio button options: "AVAYA#CM121#CSTA#AES140" (selected) and "AVAYA#CM121#CSTA-S#AES140". A "Delete Tlink" button is also present.

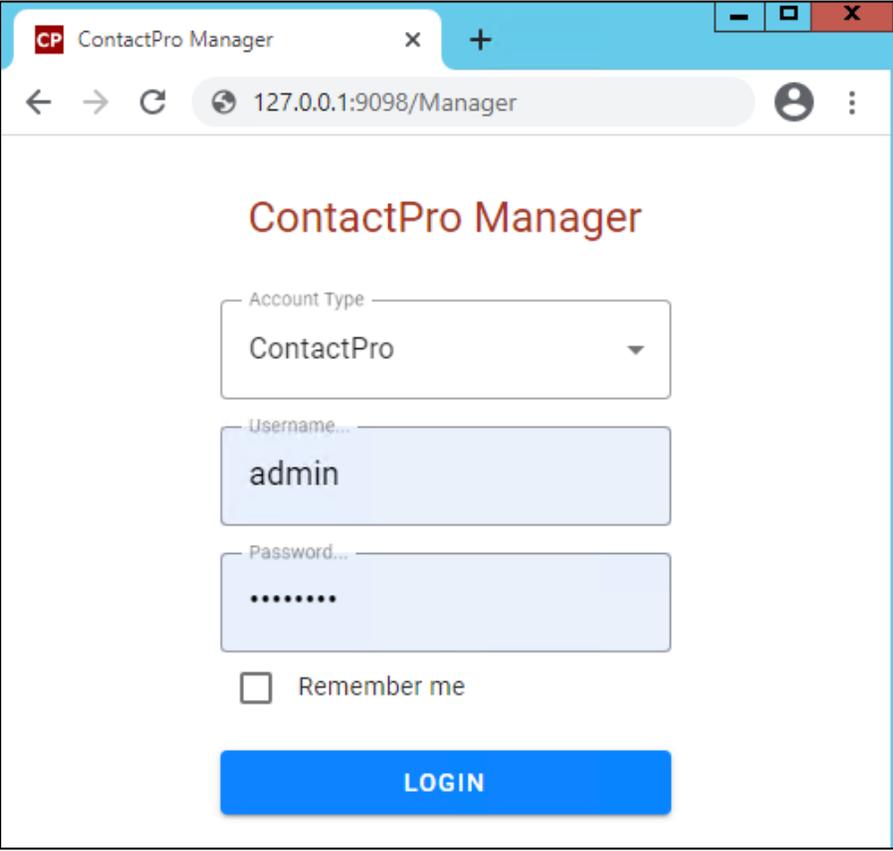
## 8. Configure CCT ContactPro® Server

It is implied a working CCT ContactPro® Server is already in place and connect to AES successfully with the necessary licensing.

### 8.1. Configure Users with CCT ContactPro® Manager

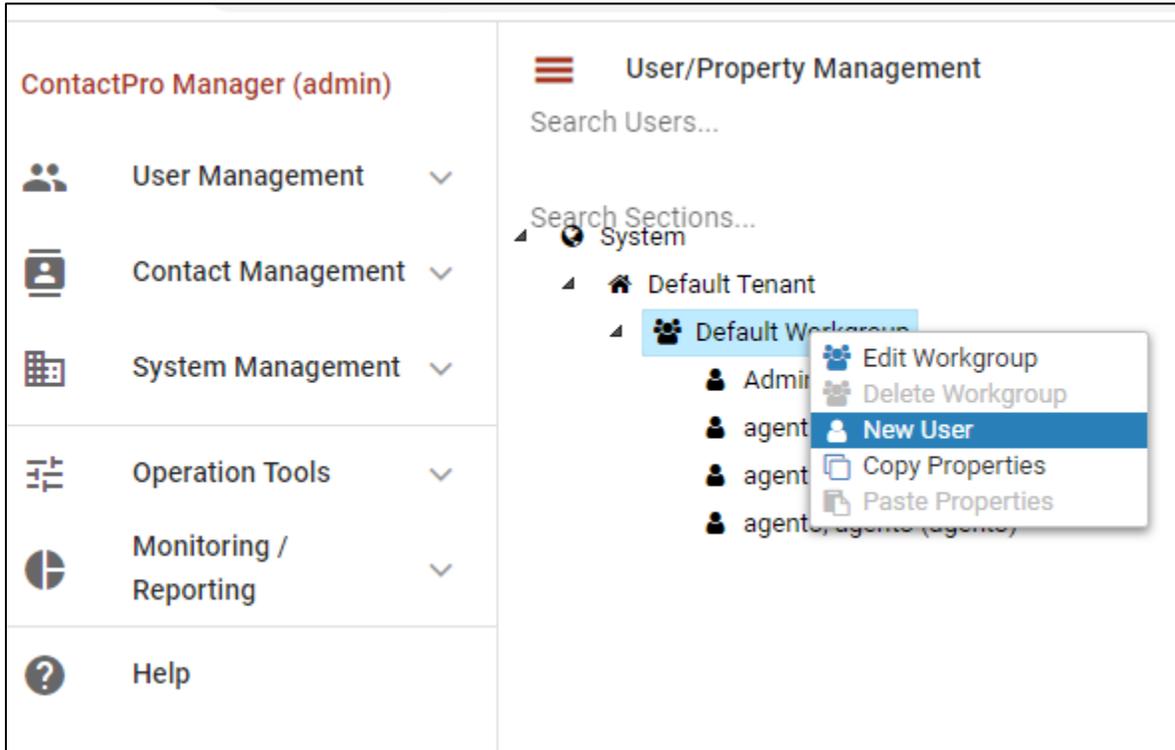
Access the CCT ContactPro® Manager web-based interface by using the URL `https://fqdn:39098` or `http://ip-address_or_fqdn:9098` in an Internet browser window, where **fqdn** is the dns name of the ContactPro server or **ip-address** is the IP address of the ContactPro server.

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



The screenshot shows a web browser window titled "ContactPro Manager" with the address bar displaying "127.0.0.1:9098/Manager". The login page features the "ContactPro Manager" title in red. Below the title are three input fields: "Account Type" with a dropdown menu set to "ContactPro", "Username..." with the text "admin", and "Password..." with masked characters ".....". There is an unchecked checkbox labeled "Remember me" and a prominent blue "LOGIN" button at the bottom.

Right click on a **Workgroup** then click **New User** to create new employee for every ContactPro Client user.



The following fields are required.

- Username (This is the **Agent ID** such as that created in **Section 6.3.2** for example)
- First Name
- Last Name
- Password

### Add User

Username* voiceagent01	Title
First Name* Voice01	Last Name* Agent
Phone	Email
Active Directory Username	CRM Username

Role  
Agent

Agent Profile

Overwrite Current Skills With Agent Profile

Password  
.....

Min. password length: 8  
Min. number of characters: 1  
Min. number of numbers: 1  
Min. number of special Characters: 1

Change Password On Login

Agent ID 75018	Agent Password .....
Station 71018	Station Password .....

Capacity Email	Capacity WebChat	Capacity Outbound	Capacity SMS	Capacity Task	Capacity Total
1	1	1	1	1	1

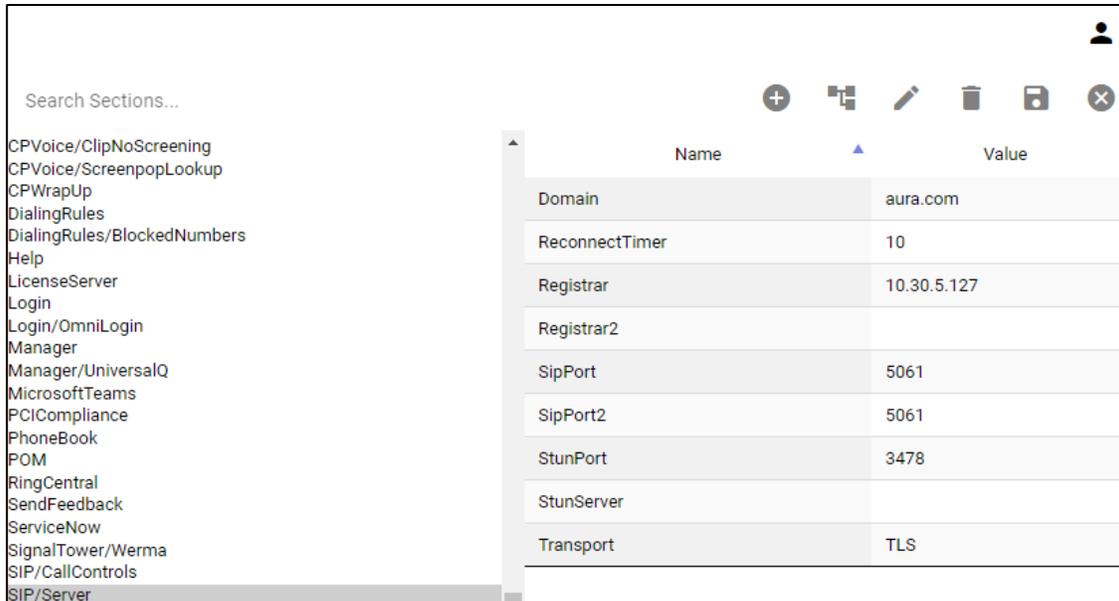
**ADD** **CANCEL**

Create employees under different workgroups in different tenants. This allows management of different Properties easily for different **Tenants** or **Workgroups** or each individual **Employee**.

NOTE: Do not need to duplicate properties. Configure what's different compared to the upper level which could be either the **Top System Level**, **Tenant** or **Workgroup** level.

## 8.2. Configure Avaya Aura® Session Manager

Select **SIP/Server** from the Sections window. This information below is all required to configure Session Manager on CCT ContactPro® Manager.

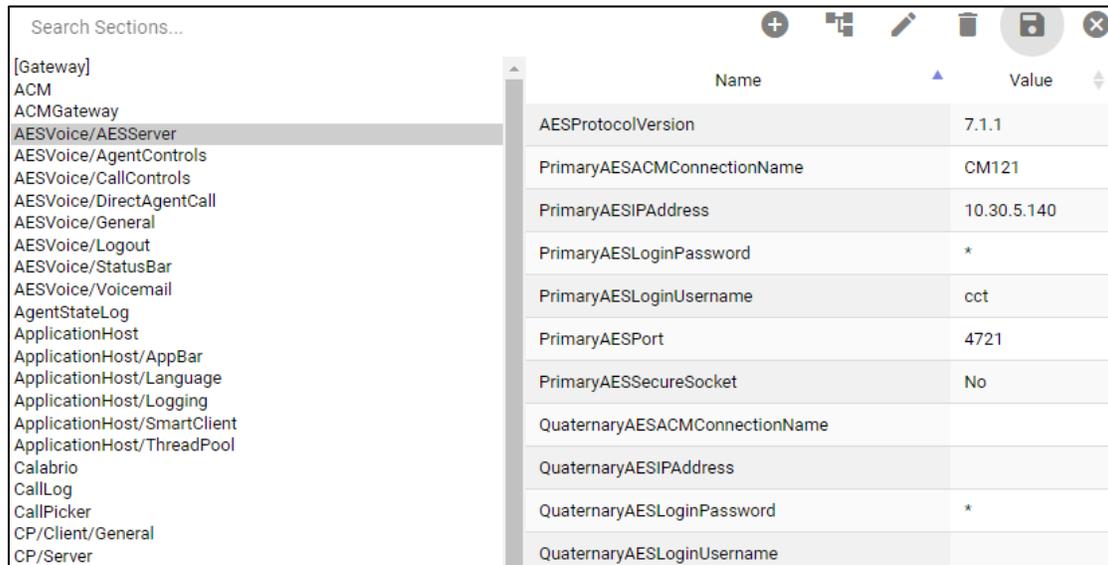


The screenshot shows the configuration interface for the SIP/Server section. The left pane lists various sections, with 'SIP/Server' selected. The right pane displays a table of configuration parameters.

Name	Value
Domain	aura.com
ReconnectTimer	10
Registrar	10.30.5.127
Registrar2	
SipPort	5061
SipPort2	5061
StunPort	3478
StunServer	
Transport	TLS

## 8.3. Configure Avaya Aura® Application Enablement.

Click on **AESVoice/AESServer** in the left window. Information on the AES server can be filled in the main window; this information can all be obtained from **Section 7** and all are required to connect successfully to the AES.



The screenshot shows the configuration interface for the AESVoice/AESServer section. The left pane lists various sections, with 'AESVoice/AESServer' selected. The right pane displays a table of configuration parameters.

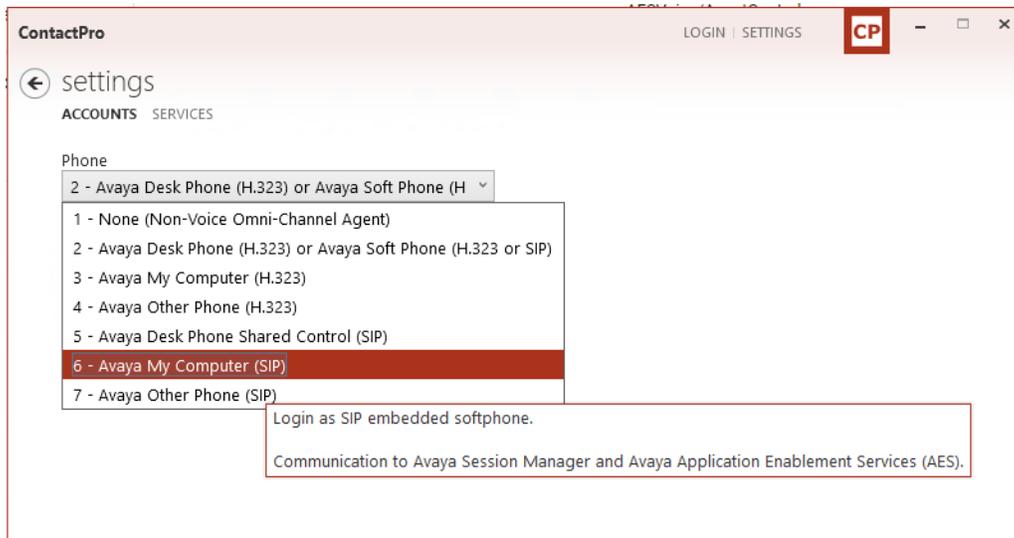
Name	Value
AESProtocolVersion	7.1.1
PrimaryAESACMConnectionName	CM121
PrimaryAESIPAddress	10.30.5.140
PrimaryAESLoginPassword	*
PrimaryAESLoginUsername	cct
PrimaryAESPort	4721
PrimaryAESSecureSocket	No
QuaternaryAESACMConnectionName	
QuaternaryAESIPAddress	
QuaternaryAESLoginPassword	*
QuaternaryAESLoginUsername	

## 9. Verification Steps

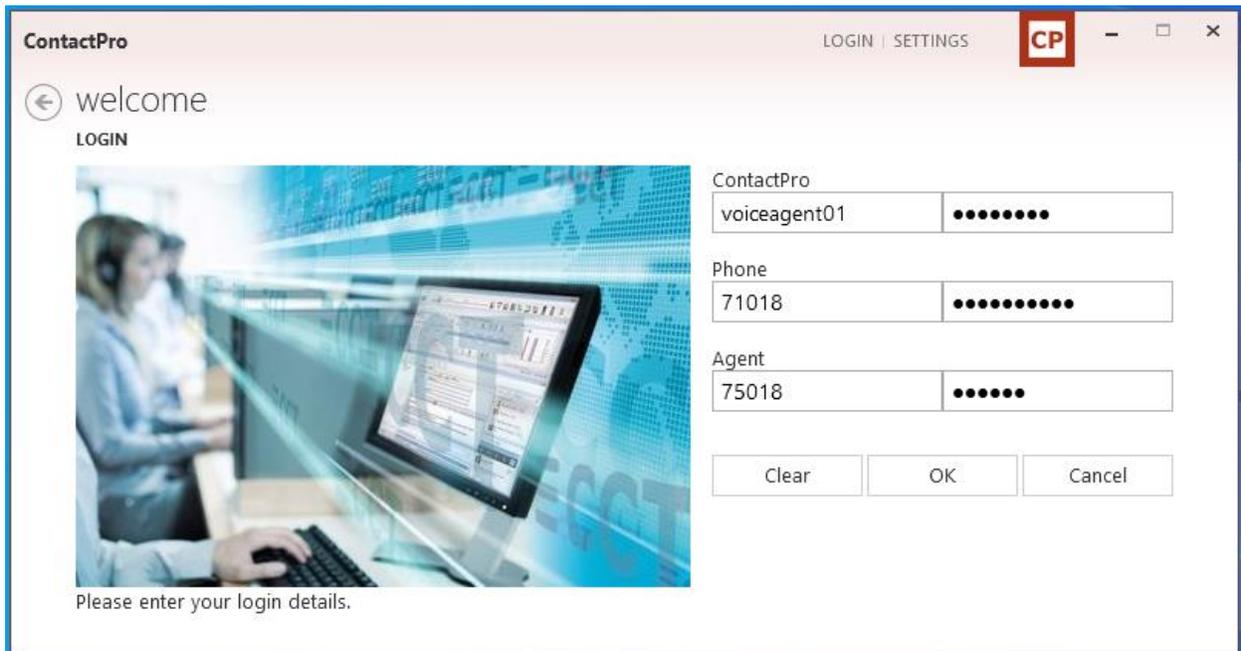
This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services and ContactPro Client.

### 9.1. Verify login of ContactPro Client

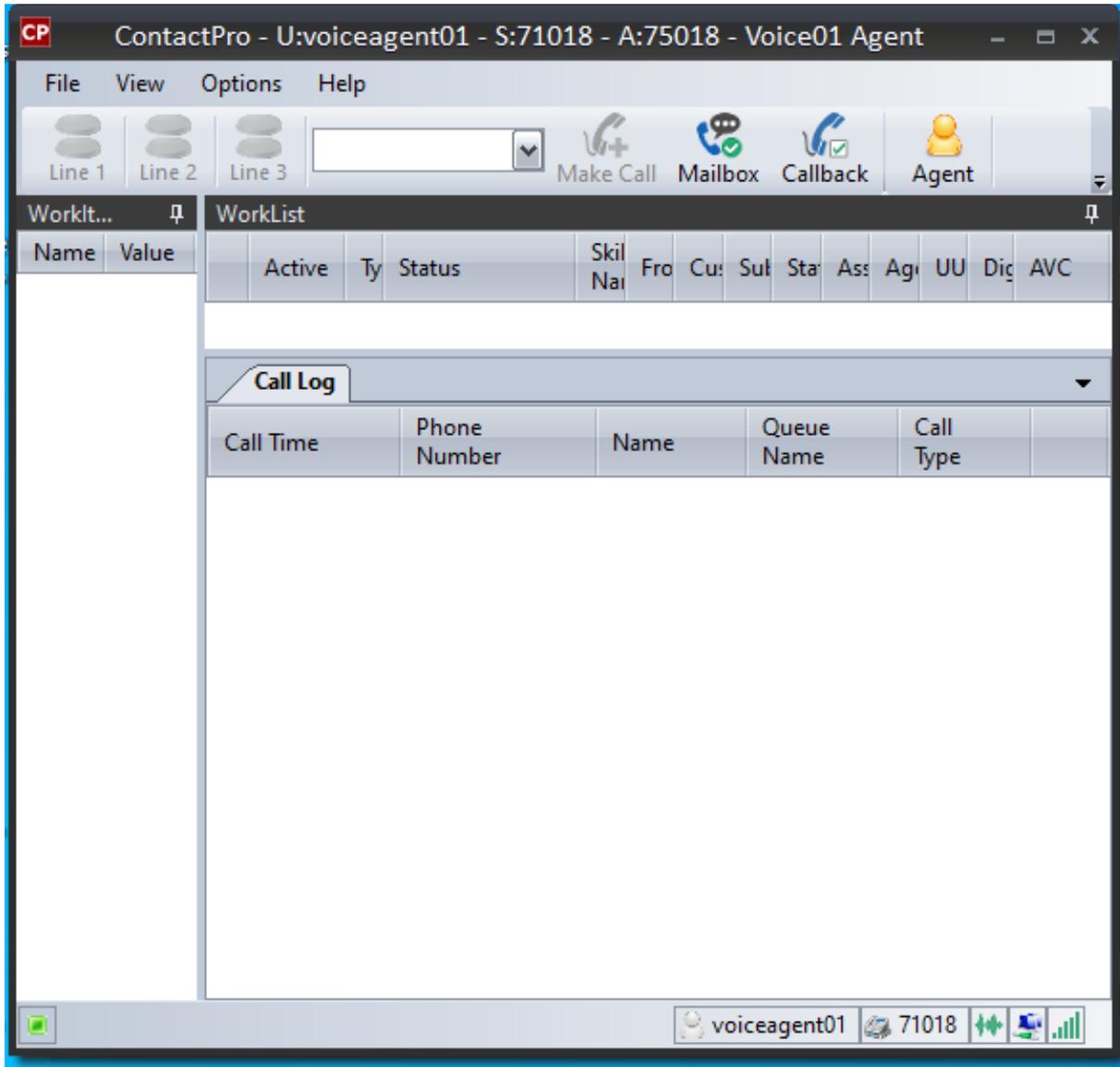
From the Agent Client PC, open the application ContactPro. Once this is opened, select **SETTINGS**, and choose Phone as **6 – Avaya My Computer (SIP)**



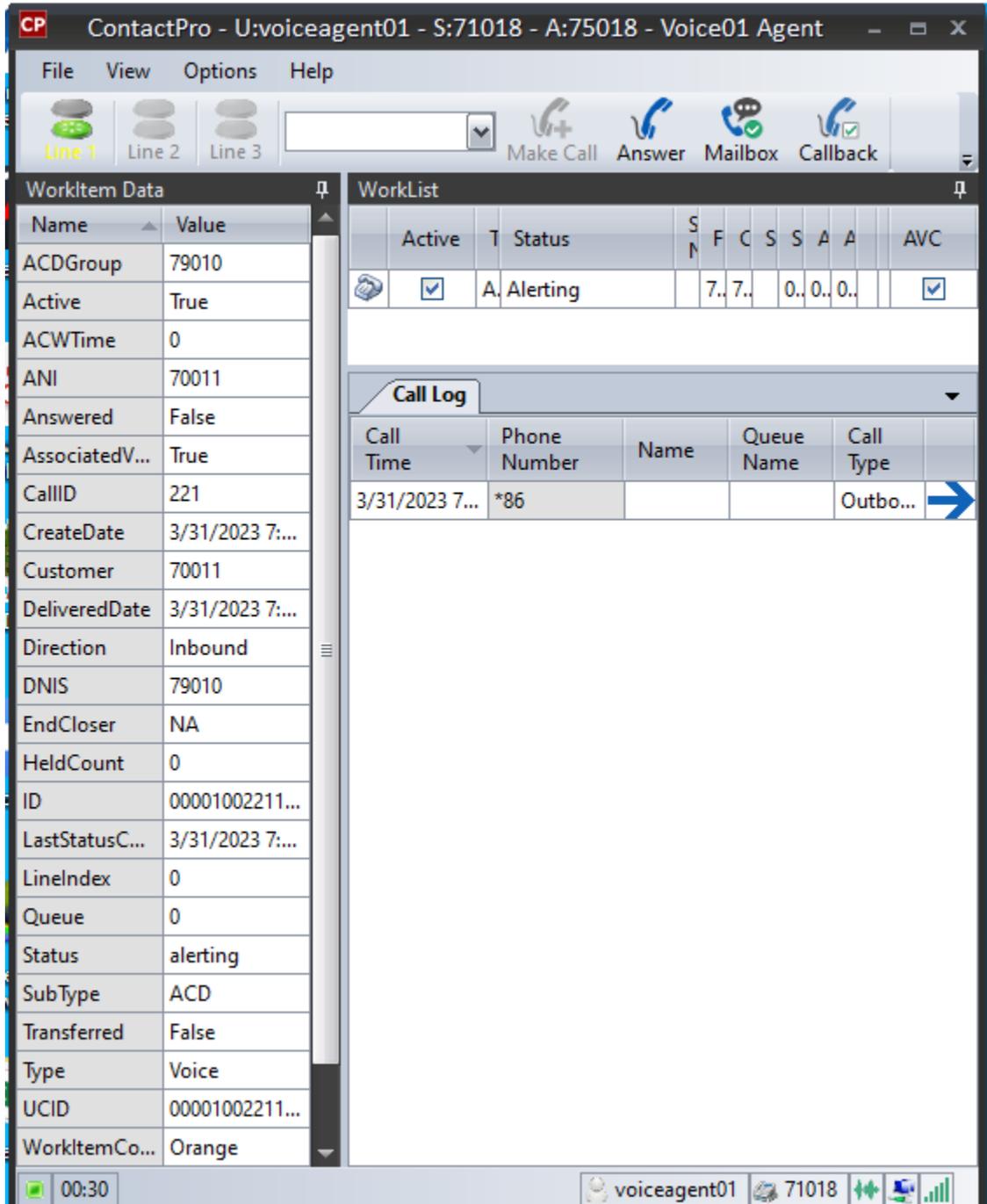
Click on OK to fill following details:



Enter user credentials already created in **Section 5** and **Section 7** and press **Login** with **Agent** enabled. After logging in successfully, ContactPro is shown below:



Place a call to VDN/Hunt Group. Verify that ContactPro Client can receive incoming call:



Answer the call by pressing the **Answer** incoming call name panel.

## 9.2. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is **established** for the CTI link number administered in **Section 7.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aes140	established	952	945

Enter the command **list agent-loginID** verify that agent **75018** shown in **Section 5.2.4** is logged-in to extension **75018**.

```
list agent-loginID
```

AGENT LOGINID									
Login ID	Name	Extension	Dir	Agt	AAS/AUD	COR	Ag	Pr	SO
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
75018	Voice Agent	71018					1	lvl	
	1/01	/	/	/	/	/	/	/	

Enter the command **status station 71018** and on **Page 7** verify that the agent is logged-in to the appropriate skill.

```
status station 71018
```

ACD STATUS							Page	7	of	7
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	On ACD Call? no			
1/AI	/	/	/	/	/	/				

## 9.4. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 9.3**.

### TSAPI Link Details

Enable page refresh every  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	CM121	1	Talking	Mon Mar 20 17:35:10 2023	Online	20	13	895	1014	30

---

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

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

Verify the **User** column shows action sessions with the CCT username from **Section 7.4**.

## Application Enablement Services

### Management Console

Welcome: User cust  
 Last login: Fri Mar 31 15:18:01 I.T. 2023 from 172.16.8.167  
 Number of prior failed login attempts: 0  
 HostName/IP: aes140.aura.com/10.30.5.140  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 10.1.2.0.0.12-0  
 Server Date and Time: Fri Mar 31 20:00:48 ICT 2023  
 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
- ▶ Logs
- ▶ Log Manager
- ▼ Status and Control
- CVLAN Service Summary
- DLG Services Summary
- DMCC Service Summary
- Switch Conn Summary
- TSAPI Service Summary

### DMCC Service Summary - Session Summary

Please do not use back button

Enable page refresh every  seconds

Session Summary [Device Summary](#)  
 Generated on Fri Mar 31 20:00:33 ICT 2023

Service Uptime: 31 days, 2 hours 58 minutes  
 Number of Active Sessions: 2  
 Number of Sessions Created Since Service Boot: 28  
 Number of Existing Devices: 2  
 Number of Devices Created Since Service Boot: 24

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	278A7C6ECE6920EEB CDFA1C4F6A58847-33	cct	AESVoice	172.16.8.167	XML Unencrypted	0
<input type="checkbox"/>	0E89705F0D7496549 BD11555514E0D0A-22	globitel	cmapiApplication	10.103.3.50	XML Unencrypted	2

Item 1-2 of 2

## 9.6. Verify User Registrations on SMGR

From the SMGR Dashboard, go to **Elements** → **Session Manager** → **System Status**.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A dropdown menu is open under 'Elements', listing various system components. The 'Session Manager' option is highlighted, and its sub-menu is visible, showing 'System Status' as the selected option. The background shows a 'System Resource Utilization' bar chart and an 'Alarms' pie chart.

**System Resource Utilization**

Category	Value
opt	7
var	2
emdata	14

**Alarms**

Severity	Count
Critical	0
Major	0
Indeterminate	16
Minor	7
Warning	68

**Elements Menu**

- Avaya Breeze®
- Communication Manager
- Communication Server 1000
- Conferencing
- Device Adapter
- Device Services
- IP Office
- Media Server
- Meeting Exchange
- Messaging
- Presence
- Routing
- Session Manager
- Web Gateway

**Session Manager Sub-menu**

- Dashboard
- Session Manager Administration
- Global Settings
- Communication Profile Editor
- Network Configuration
- Device and Location Configuration
- Application Configuration
- System Status

Select **User Registrations** in left pannel, and verify the user is logged in using the Agent Client IP Address.

**AVAYA** Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home Session Manager User Management

**User Registrations**

Select rows to send notifications to devices. Click on Details column for complete registration status.

View ▾ Default Export Force Unregister **AST Device Notifications:** Reboot

24 Items Show 15 ▾

<input type="checkbox"/>	Details	Address ▾	First Name	Last Name	Actual Location	IP Address
<input type="checkbox"/>	▶ Show	71018@aura.com	Ext71018	ContactPro	---	172.16.8.167
<input type="checkbox"/>	▶ Show	71003@aura.com	Ext3	BT	---	172.27.130.3
<input type="checkbox"/>	▶ Show	71002@aura.com	Ext2	BT	---	172.27.130.3
<input type="checkbox"/>	▶ Show	71001@aura.com	Ext1	BT	---	172.27.130.3
<input type="checkbox"/>	▶ Show	---	Ext17	Recording	---	---
<input type="checkbox"/>	▶ Show	---	Ext6	BT	---	---
<input type="checkbox"/>	▶ Show	---	Ext7	BT	---	---

## 10. Conclusion

CCT Deutschland GmbH ContactPro 7.0 solution was able to successfully interoperate with Avaya Client SDK, Avaya Aura® Session Manager 10.1, Avaya Aura® Communication Manager 10.1, and Avaya Aura® Application Enablement Service 10.1. as listed in **Section 4**. All test cases passed successfully.

## 11. Additional References

Documentation related to Avaya can be obtained from <https://support.avaya.com>.

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 5, Mar 2023

[2] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 5, Feb 2023

[3] *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 5, Feb 2023

[4] *Administering Avaya Aura® System Manager*, Release 10.1, Issue 8, Feb 2023

Documentation related to CCT Deutschland GmbH ContactPro can be obtained from <https://www.cct-solutions.com>.

---

**©2023 Avaya Inc. All Rights Reserved.**

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

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