



Avaya Solution & Interoperability Test Lab

Application Notes for CCT ContactPro® 5.2 for Breeze Client SDK 4.1 with Avaya Aura® Session Manager R8, and Avaya Aura® Application Enablement Services R8 - Issue 1.2

Abstract

These Application Notes describe the configuration steps required for CCT ContactPro® to interoperate with Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services.

CCT ContactPro® is an interaction management application that connects to both Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for CCT ContactPro® to interoperate with Avaya Session Manager R8, Avaya Aura® Communication Manager R8 and Aura® Application Enablement Services R8. CCT ContactPro® offers a variety of integrations in an Avaya call center environment supporting different Avaya platforms 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 agents to have full call control from the agent's screen. CCT ContactPro® is an interaction management application which integrated with Breeze Client SDK 4.1 for SIP voice call control and audio to register as SIP endpoints with Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The general test approach was to validate successful handling of inbound skillset/VDN calls using CCT ContactPro®. This was performed by calling inbound to a VDN or outbound from the elite call center using CCT ContactPro®. Where applicable, agent actions were performed using the CCT ContactPro® Agent client.

CCT ContactPro® software is installed on each client PC utilised by an agent. A configuration file on this software points to a database for all further configuration.

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 this Application Note, the interface between Avaya systems and CCT ContactPro® Client used TLS as a security feature.

2.1. Interoperability Compliance Testing

The testing focused on the following areas:

- **Agent state change**– Login, Ready/Not Ready using CCT ContactPro® Agent.
- **Inbound Calls** – Answer calls using CCT ContactPro® Agent.
- **Outbound Calls** – Make calls using CCT ContactPro® Agent.
- **Hold/Transfer/Conference** – Place callers on hold and transfer and conference using CCT ContactPro® Agent.
- **Failover Testing** – Verify the ability of CCT ContactPro® Agent to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

All test cases passed successfully. The following observations were noted.

- Blind Conference is not supported on CCT ContactPro®.
- CCT ContactPro® does not have log out button.

2.3. Support

Support for CCT products can be obtained as follows:

WEBSITE

www.cct-solutions.com

CONTACT

Phone: +49 69 7191 4969 0

Email: contact@cct-solutions.com

SUPPORT

Hotline: +49 821 455152 455

Email: helpdesk@cct-solutions.com

CCT Deutschland GmbH

Street Tilsterstrasse 1

ZIP 60487

Frankfurt am Main

Germany

Phone +49 69 7191 4969 0

Fax +49 69 7191 4969 666

Street Werner-von-Siemens-Strasse 6

ZIP 86159

Augsburg

Germany

Phone +49 821 455 152 700

Fax +49 821 455 152 777

CCT Europe GmbH

Street Sumpfstrasse 26

ZIP 6312

Steinhausen

Switzerland

Phone. +41 41 748 42 22

Fax +41 41 748 42 23

CCT Software LLC

1801 N.E. 123rd Street, Suite 314

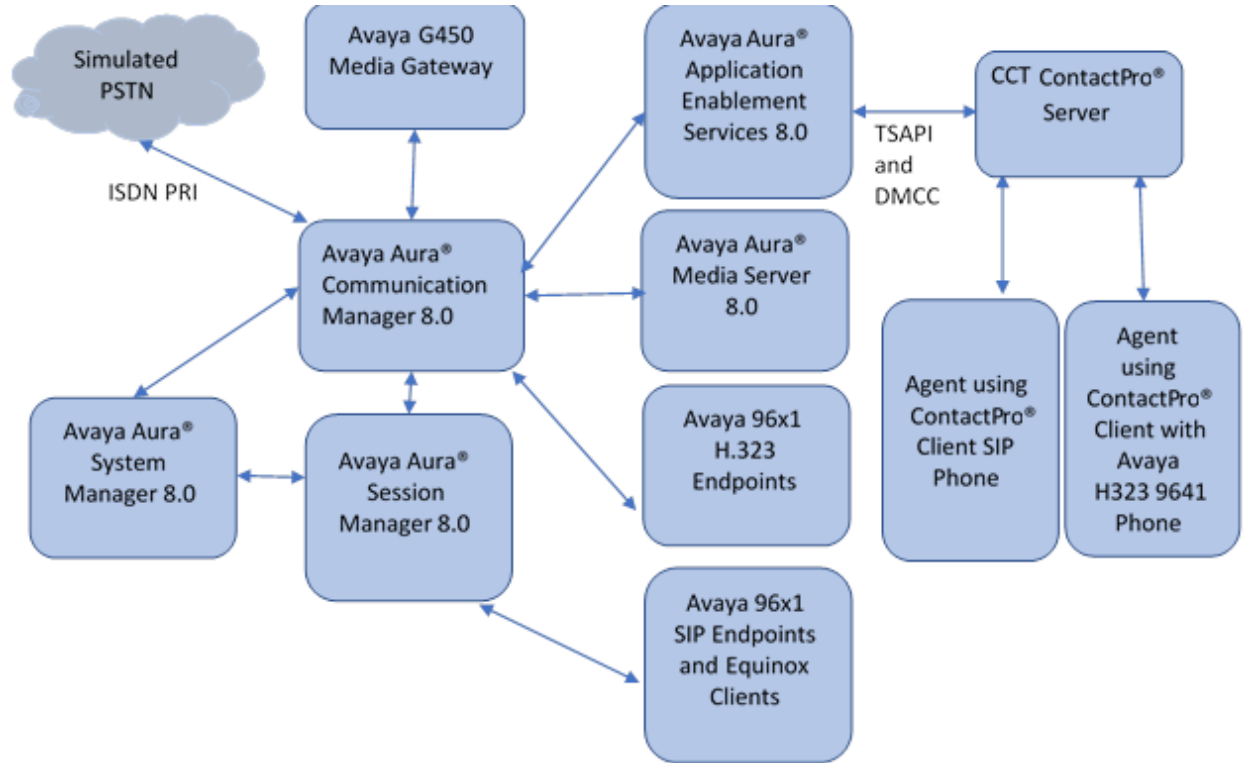
North Miami, 33181 FL

United States of America

Phone. +1 844 720 3897

3. Reference Configuration

The configuration in **Figure 1** will be used to compliance test ContactPro® with Avaya Aura® Session Manager and Avaya Aura® AES and Avaya Aura® Communication Manager.



- ContactPro® Client to AES Server: AES Third Party Call Control (TSAPI) for Call Control
Note 1: Traditional TSPAI Client is not required on the client because it uses CSTA3 XML version of the TSAPI Protocol which is tunneled through DMCC by AES SDK
- ContactPro® Client to ContactPro® Server: SQL Database Connection to ContactPro® Databases

Figure 1: Connection of CCT Deutschland GmbH ContactPro® with Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.0.1.0.0 (8.0 FP1)
Avaya G450 Media Gateway	40.10.1
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.0.1
Avaya Aura® Session Manager	8.0.1
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Breeze Client SDK	4.1
CCT Deutschland GmbH ContactPro®	R5.2.0.681
CCT Deutschland GmbH ContactPro® Client Agent Desktop	R5.2.0.447

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer vectors and VDNs

5.1. 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.)			

Navigate to **Page 7** and verify that the **Vectoring (Basic)** customer option is set to “y”.

display system-parameters customer-options		Page	7 of 12
CALL CENTER OPTIONAL FEATURES			
Call Center Release: 7.0			
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	

5.2. Administer CTI Link

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

add cti-link 1	Page	1 of 3
CTI LINK		
CTI Link: 1		
Extension: 79999		
Type: ADJ-IP		
COR: 1		
Name: aes8		

5.3. Administer Vector and VDN

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

- VDN
- Hunt Group
- Vector
- Agent

5.3.1. Add VDN

To add a VDN type **add vdn x**, where x is a VDN number. Enter a suitable name for example the **VDN 87100** below will be used for the queue.

add vdn 87100	Page 1 of 2
VECTOR DIRECTORY NUMBER	
Extension: 87100	
Name: Voice Service	
Destination: Vector Number	100
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*:	
* Follows VDN Override Rules	

5.3.2. 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 **100** 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 2	Page 1 of 4
HUNT GROUP	
Group Number: 2	ACD? y
Group Name: Voice Service	Queue? y
Group Extension: 88100	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 2	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

5.3.3. Add Vector

To administer the vector used by the VDN in **Section 5.3.1**, type **change vector x** where x is the vector number. The example below shows the call queuing to skill or hunt group 100 (queue-to skill **100**).

```
change vector 100                                     Page 1 of 6
                                     CALL VECTOR
Number:100      Name: Voice Service
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 adjunct      routing link 1
02 wait-time    2      secs hearing silence
03 queue-to     skill 2      pri m
04 wait-time    10     secs hearing ringback
05 queue-to     skill 2      pri m
06 wait-time    10     secs hearing ringback
07 disconnect   after announcement none
08
09
```

5.3.4. Add Agent

To add a new agent type **add agent-loginID x**, where x is the login id for the new agent.

```
add agent-loginID 80000                               Page 1 of 3
                                     AGENT LOGINID
Login ID: 80000      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 **2** 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 80000										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: 2		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:			
11:			26:			41:			56:			
12:			27:			42:			57:			
13:			28:			43:			58:			
14:			29:			44:			59:			
15:			30:			45:			60:			

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer CCT user
- Administer security database
- Administer ports
- Administer TCP settings
- Restart services
- Obtain Tlink name

6.1. Launch OAM Interface

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

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




Application Enablement Services Management Console

A login form with a light gray background. It contains the text "Please login here:" followed by "Username" and a text input field. Below the input field is a button labeled "Continue".

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

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

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Tue Mar 26 15:47:40 ICT 2019
HA Status: Not Configured

Home

Home | Help | Logout

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

Welcome to OAM

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


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

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

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

6.2. Verify License

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

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Tue Mar 26 15:49:11 ICT 2019
HA Status: Not Configured

Licensing

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▼ Licensing
 - WebLM Server Address
 - WebLM Server Access**
 - Reserved Licenses
- ▶ Maintenance

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users and Device Media and Call Control**, as shown below. The TSAPI license is used for device monitoring and the DMCC license is used for the virtual IP softphones. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH**, which is needed for adjunct routing.

AVAYA
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 🔔 ☰ | admin

Home Licenses

Licenses

Licensed products

APPL_ENAB

▼ Application_Enablement

View license capacity

View peak usage

CE

► COLLABORATION_ENVIRONMENT

COLLABORATION_DESIGNER

► Collaboration_Designer

MESSAGING

► Messaging

MSR

► Media_Server

SYSTEM_MANAGER

► System_Manager

SessionManager

► SessionManager

Uninstall license

Server properties

Shortcuts

Help for Licensed products

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

License installed on: December 28, 2018 11:22:53 AM +07:00

License File Host IDs: V0-55-3B-33-B4-26-01

Licensed Features

13 Items Show All ▾

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 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
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	1000

6.3. Administer TSAPI Link

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



Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Mon Mar 25 17:49:07 ICT 2019
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services


- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<div>Add LinkEdit LinkDelete Link</div>				

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 “CM8” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Mon Mar 25 17:58:54 ICT 2019
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
- ▶ TWS

Add TSAPI Links

Link1
Switch ConnectionCM8
Switch CTI Link Number1
ASAI Link Version9
SecurityUnencrypted

Apply ChangesCancel Changes

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
- High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> CM8	Yes	30	1

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
- High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> CM8	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.30.5.93” as shown below. Click **Add Name or IP**.

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
- High Availability
- ▶ Licensing
- ▶ Maintenance

Edit H.323 Gatekeeper - CM8

Name or IP Address

6.5. 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.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Mon Mar 25 18:10:58 ICT 2019
HA Status: Not Configured

User Management | User Admin | Add User


[Home](#) | [Help](#) | [Logout](#)

<ul style="list-style-type: none">▶ AE Services▶ Communication Manager Interface▶ High Availability▶ Licensing▶ Maintenance▶ Networking▶ Security▶ Status▼ User Management<ul style="list-style-type: none">▶ Service Admin▼ User Admin<ul style="list-style-type: none">■ Add User■ Change User Password■ List All Users■ Modify Default Users■ Search Users▶ Utilities▶ Help	<h4>Add User</h4> <p>Fields marked with * can not be empty.</p> <table><tr><td>* User Id</td><td><input type="text" value="CCT"/></td></tr><tr><td>* Common Name</td><td><input type="text" value="CCT"/></td></tr><tr><td>* Surname</td><td><input type="text" value="CCT"/></td></tr><tr><td>* User Password</td><td><input type="password" value="....."/></td></tr><tr><td>* Confirm Password</td><td><input type="password" value="....."/></td></tr><tr><td>Admin Note</td><td><input type="text"/></td></tr><tr><td>Avaya Role</td><td><input type="text" value="None"/></td></tr><tr><td>Business Category</td><td><input type="text"/></td></tr><tr><td>Car License</td><td><input type="text"/></td></tr><tr><td>CM Home</td><td><input type="text"/></td></tr><tr><td>Css Home</td><td><input type="text"/></td></tr><tr><td>CT User</td><td><input type="text" value="Yes"/></td></tr><tr><td>Department Number</td><td><input type="text"/></td></tr><tr><td>Display Name</td><td><input type="text"/></td></tr><tr><td>Employee Number</td><td><input type="text"/></td></tr><tr><td>Employee Type</td><td><input type="text"/></td></tr><tr><td>Enterprise Handle</td><td><input type="text"/></td></tr></table>	* User Id	<input type="text" value="CCT"/>	* Common Name	<input type="text" value="CCT"/>	* Surname	<input type="text" value="CCT"/>	* User Password	<input type="password" value="....."/>	* Confirm Password	<input type="password" value="....."/>	Admin Note	<input type="text"/>	Avaya Role	<input type="text" value="None"/>	Business Category	<input type="text"/>	Car License	<input type="text"/>	CM Home	<input type="text"/>	Css Home	<input type="text"/>	CT User	<input type="text" value="Yes"/>	Department Number	<input type="text"/>	Display Name	<input type="text"/>	Employee Number	<input type="text"/>	Employee Type	<input type="text"/>	Enterprise Handle	<input type="text"/>
* User Id	<input type="text" value="CCT"/>																																		
* Common Name	<input type="text" value="CCT"/>																																		
* Surname	<input type="text" value="CCT"/>																																		
* User Password	<input type="password" value="....."/>																																		
* Confirm Password	<input type="password" value="....."/>																																		
Admin Note	<input type="text"/>																																		
Avaya Role	<input type="text" value="None"/>																																		
Business Category	<input type="text"/>																																		
Car License	<input type="text"/>																																		
CM Home	<input type="text"/>																																		
Css Home	<input type="text"/>																																		
CT User	<input type="text" value="Yes"/>																																		
Department Number	<input type="text"/>																																		
Display Name	<input type="text"/>																																		
Employee Number	<input type="text"/>																																		
Employee Type	<input type="text"/>																																		
Enterprise Handle	<input type="text"/>																																		

6.6. Administer Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [4] to configure access privileges for the CCT user from **Section 6.5**.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Mon Mar 25 18:29:44 ICT 2019
HA Status: Not Configured

Security | Security Database | ControlHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

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

☐ Enable SDB for DMCC Service


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

Apply Changes

6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2 :
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Mon Mar 25 18:32:41 ICT 2019
HA Status: Not Configured

Networking | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port

9999

Enabled Disabled

Encrypted TCP Port

9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port

450

Enabled Disabled

Local TLINK Ports

TCP Port Min

1024

TCP Port Max

1039

Unencrypted TLINK Ports

TCP Port Min

1050

TCP Port Max

1065

Encrypted TLINK Ports

TCP Port Min

1066

TCP Port Max

1081

DMCC Server Ports

Unencrypted Port

4721

Enabled Disabled

Encrypted Port

4722

Enabled Disabled

TR/87 Port

4723

Enabled Disabled

H.323 Ports

TCP Port Min

20000

TCP Port Max

29999

Local UDP Port Min


20000

Local UDP Port Max

29999

6.8. Administer TCP Settings

Select **Networking** → **TCP/TLS Settings** from the left pane, to display the **TCP/TLS Settings** screen in the right pane. For **TCP Retransmission Count**, select **TSAPI Routing Application Configuration (6)**, as shown below.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Mon Mar 25 18:34:19 ICT 2019
HA Status: Not Configured

Networking | TCP / TLS SettingsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

TCP / TLS Settings

TLSv1 Protocol Configuration

☐ Support TLSv1.0 Protocol

☐ Support TLSv1.1 Protocol

☒ Support TLSv1.2 Protocol

TCP Retransmission Count

☐ Standard Configuration (15)

☒ TSAPI Routing Application Configuration (6)

Apply Changes

Restore Defaults


Cancel Changes

Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket.
Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.

Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution.

6.9. Restart Services

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



Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Mar 26 14:26:05 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2 :
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Tue Mar 26 14:47:14 ICT 2019
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

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

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

Start

Stop

Restart Service

Restart AE Server


Restart Linux

Restart Web Server

6.10. 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#CM8#CSTA#AES8”. Note the use of the switch connection “CM8 from **Section 6.3** as part of the Tlink name.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Tue Mar 26 14:26:05 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Tue Mar 26 15:26:16 ICT 2019
HA Status: Not Configured

Security | Security Database | TlinksHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

Tlinks

Tlink Name

☒ AVAYA#CM8#CSTA#AES8

Delete Tlink

7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer Users

7.1. 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.

7.2. Administer Users

From the dashboard, select **Users** → **User Management** → **Manage Users**

System Resource Utilization

Category	Value
opt	7
ver	21
emba	14
emp	7
pend	0

Alarms

Severity: [Dropdown]

SourceIP	Description
No data	

Notifications

No data

Information

Elements	GNRL	Sync	Status
Avaya Aura Device Services	1		Green
Avaya Aura Web Gateway	2		Green
Avaya Breeze	1		Red
AvayaAuraMediaServer	1		Green
CM	2		Green
MMCS	2		Green

Click **New**.

Manage Users

Search: [Input Field]

<input type="checkbox"/>	First Name	Surname	Display Name	Login Name
<input type="checkbox"/>	2010006	TE	2010006 TE	2010006@h
<input type="checkbox"/>	2010007	TE	2010007 TE	2010007@h
<input type="checkbox"/>	2010008 duy	TE duy	2010008 TE duy	2010008@h
<input type="checkbox"/>	2010020	TE	2010020 TE	2010020@h
<input type="checkbox"/>	2012311	TE	2012311 TE	2012311@h
<input type="checkbox"/>	2012312	TE	2012312 TE	2012312@h
<input type="checkbox"/>	2012313	TE	2012313 TE	2012313@h

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 Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and tabs for Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows 'User Management' with 'Manage Users' selected. The main content area is titled 'User Profile | Add' and has tabs for Identity, Communication Profile, Membership, and Contacts. The 'Identity' tab is active, showing fields for 'Basic Info' (User Provisioning Rule, Address, LocalizedName), 'Last Name' (Voice), 'First Name' (Agent), 'Login Name' (70000@devconnect.com), 'Description' (Description Of User), 'Password', 'Last Name (Latin Translation)' (Voice), 'First Name (Latin Translation)' (Agent), 'Middle Name' (Middle Name Of User), 'Email Address' (Email Address Of User), and 'User Type' (Basic).

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 the Avaya Aura System Manager 8.0 interface with the 'Communication Profile' tab selected. The 'Communication Profile Password' section is visible, showing 'PROFILE SET: Primary' and 'Communication Address'. A modal dialog titled 'Comm-Profile Password' is open, prompting for 'Comm-Profile Password' and 'Re-enter Comm-Profile Password'. The 'Re-enter' field has a green checkmark, indicating the passwords match. The background shows the 'Communication Profile' tab with fields for 'Domain' and 'Options'.

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

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows 'User Management' with sub-items like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile ...'. The main content area is titled 'User Profile | Add' and has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section and a 'Communication Address' section. The 'Communication Address' section has a table with columns 'Type', 'Handle', and 'Domain'. The 'New' button is highlighted in the table header. The table shows 'No data'.

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 screenshot shows the 'Communication Address Add/Edit' dialog box. It has a title bar with a close button. The 'Type' dropdown is set to 'Avaya SIP'. The 'Fully Qualified Address' field is split into two parts: a text input containing '70000' and a dropdown menu containing 'devconnect.com'. There are 'Cancel' and 'OK' buttons at the bottom right.

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.

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breeze® Profile ☐

Equinox Profile ☐

CM Endpoint Profile ☐

Presence Profile ☐

Conferencing Profile ☐

* Primary Session Manager : SMDev

Secondary Session Manager : Start typing...

Survivability Server : Start typing...

Max. Simultaneous Devices : 1

Block New Registration When Maximum Registrations Active? : ☐

Application Sequences

Origination Sequence : CM93

Termination Sequence : CM93

Emergency Calling Application Sequences

Emergency Calling Origination Sequence : Select

Emergency Calling Termination Sequence : Select

Call Routing Settings

* Home Location : DevConnect

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 you wish to use, select **9641SIPCC_DEFAULT_CM_8_0** as the **Template** and ensure **IP** is configured as the **Port**, click **Commit & Continue** (not shown) when finished.

* System:	CM93	* Profile Type:	Endpoint
Use Existing Endpoints:	<input type="checkbox"/>	* Extension:	70000
* Template:	9641SIPCC_DEFAULT_CM_8_0	* Set Type:	9641SIPCC
* Sub Type:	Select	* Terminal Number:	
System ID:	Enter System Id	Security Code:	*****
Port:	IP	Voice Mail Number:	
Preferred Handle:	Select	Calculate Route Pattern:	<input type="checkbox"/>
Sip Trunk:	aar	SIP URI:	Select
Enhanced Callr-Info display for 1-line phones:	<input type="checkbox"/>	Delete on Unassign from User or on Delete User:	<input checked="" type="checkbox"/>

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

Enhanced Call Fwd (E)	Button Assignment (B)	Profile Settings (P)	Group Membership (M)
* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	70000	* Message Lamp Ext.	70000
* Tenant Number	1		
* SIP Trunk	Qaar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	<input type="checkbox"/>	Localized Display Name	
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			
Primary Session Manager			
IPv4:		IPv6:	
Secondary Session Manager			
IPv4:		IPv6:	

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

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

Click on **Button Assignment (B)** tab, configure **Button Feature** as following:

Endpoint Configurations		Button Configurations			
Favorite	Button Label	Button Feature	Argument-1	Argument-2	Argum
1 <input type="checkbox"/>		call-appr Auto-A/D		Ring	
2 <input type="checkbox"/>		call-appr Auto-A/D		Ring	
3 <input type="checkbox"/>		call-appr Auto-A/D		Ring	
4 <input type="checkbox"/>		agnt-login			
5 <input type="checkbox"/>		aux-work Reason Code		Hunt Grp	
6 <input type="checkbox"/>		auto-in auto-in Grp			
7 <input type="checkbox"/>		manual-in manual-in Grp			
8 <input type="checkbox"/>		after-call after-call Grp			

Click on **Commit** to save the user.

8. Configure CCT Deutschland GmbH ContactPro®

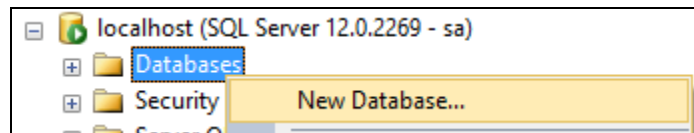
This section outlines the steps required to configure the connections from CCT ContactPro® to the AES.

8.1. Create CONTACTPRO® Database and User

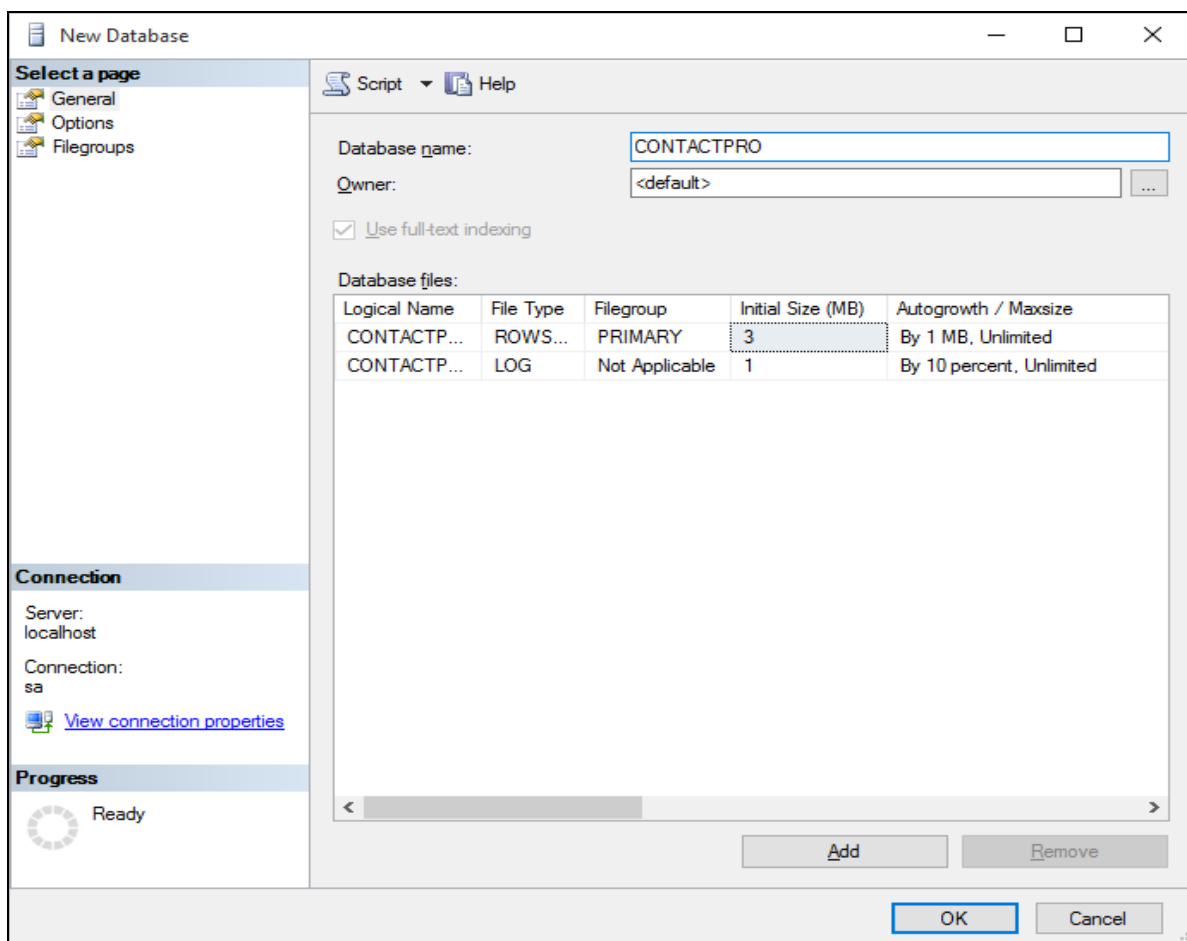
A database and database user for ContactPro® must be created on the SQL server.

8.1.1. Create Database

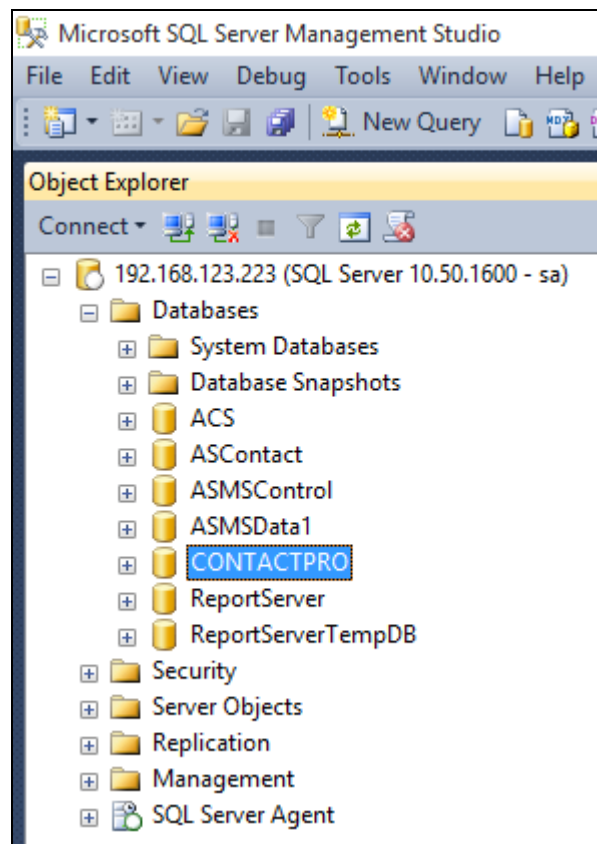
Create a **CONTACTPRO®** database on the same Microsoft SQL Server. Right-click on **Databases** and click on **New Database**.



Give it a suitable **Database name** and click on **OK** at the bottom of the screen.

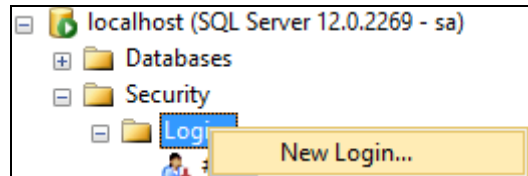


The end result will be as shown in the screenshot below where **CONTACTPRO®** database which was just created. The default MS SQL **ReportServer** and **ReportServerTempDB** databases may also be present.



8.1.2. Create User

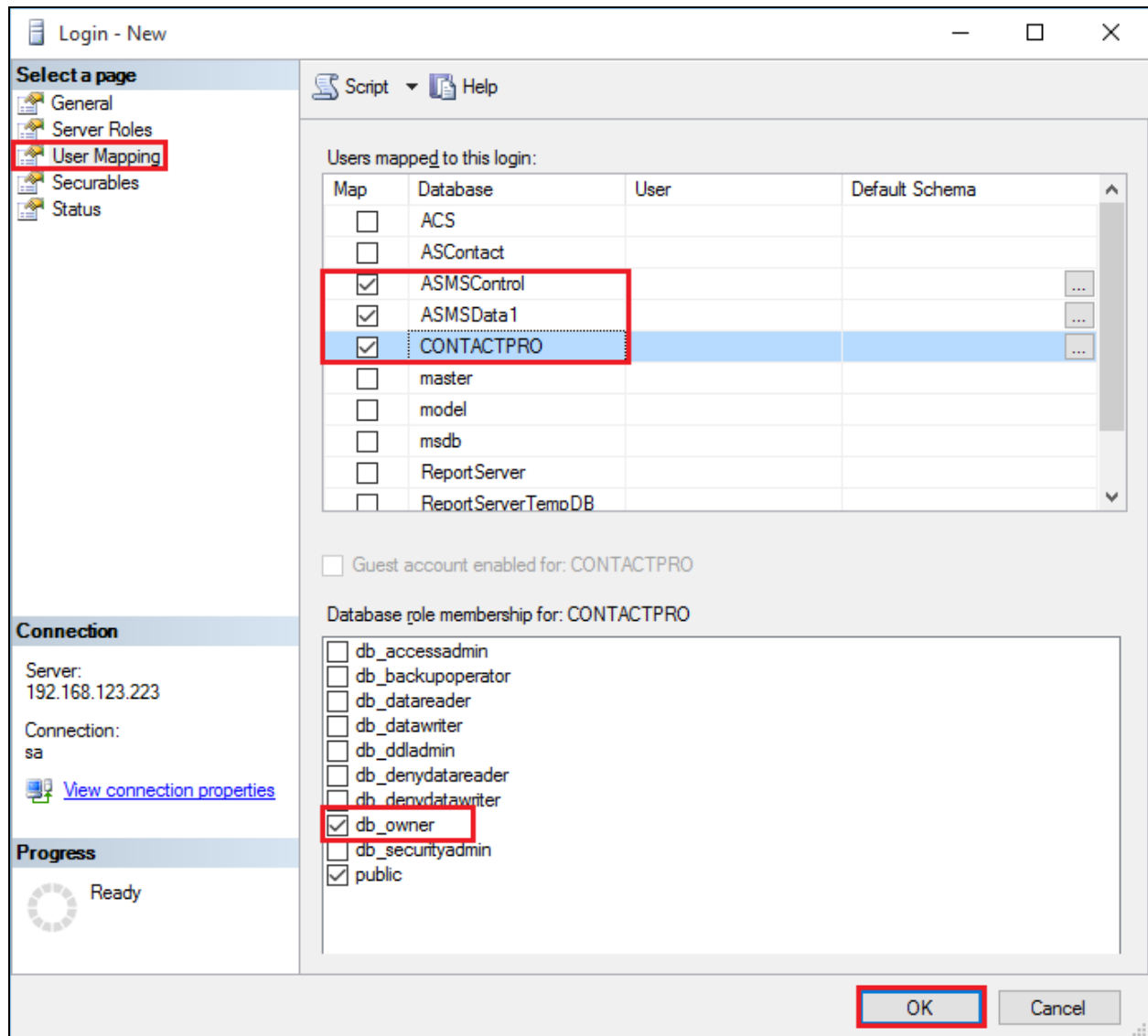
Create a database user named **ContactPro®**. Right-click on **Login** and click on **New Login**.



Click on the **General** tab in the left window and enter the **Login name** and click on **SQL Server authentication** and enter a suitable **Password** for the **ContactPro®** user. Click on **OK** at the bottom of the screen once done.

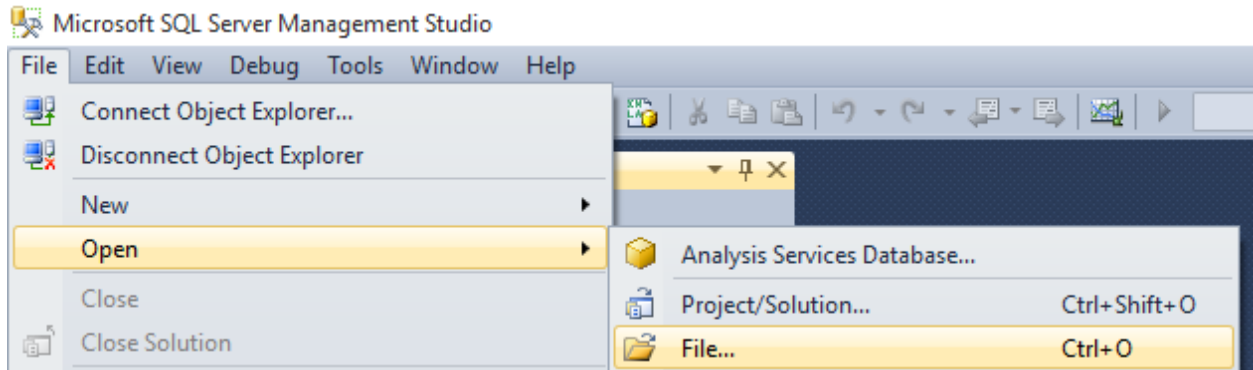
A screenshot of the 'Login - New' dialog box. The 'General' tab is selected and highlighted with a red box. The 'Login name' field contains 'contactpro'. The 'SQL Server authentication' radio button is selected. The 'Password' and 'Confirm password' fields are filled with dots. The 'Enforce password policy' checkbox is checked and highlighted with a red box. The 'Default database' is set to 'master' and the 'Default language' is set to '<default>'. The 'OK' button at the bottom right is highlighted with a red box. The left pane shows the 'Connection' section with 'Server: 192.168.123.223' and 'Connection: sa'. The 'Progress' section shows a 'Ready' status.

Click on **User Mapping** in the left window. For this user, grant public and **db_owner** access to **CONTACTPRO®** databases. Click on **OK** at the bottom of the page once done.

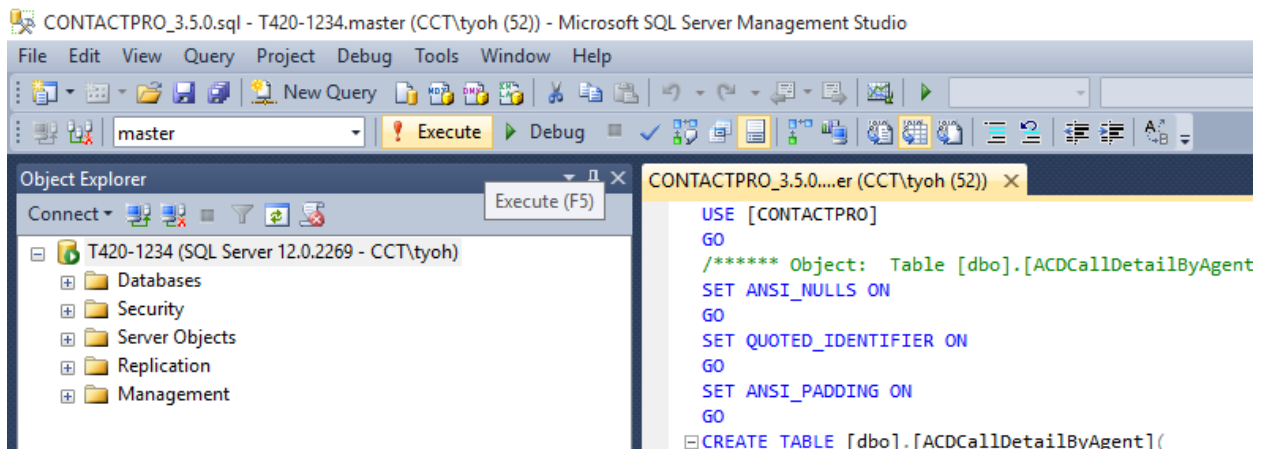


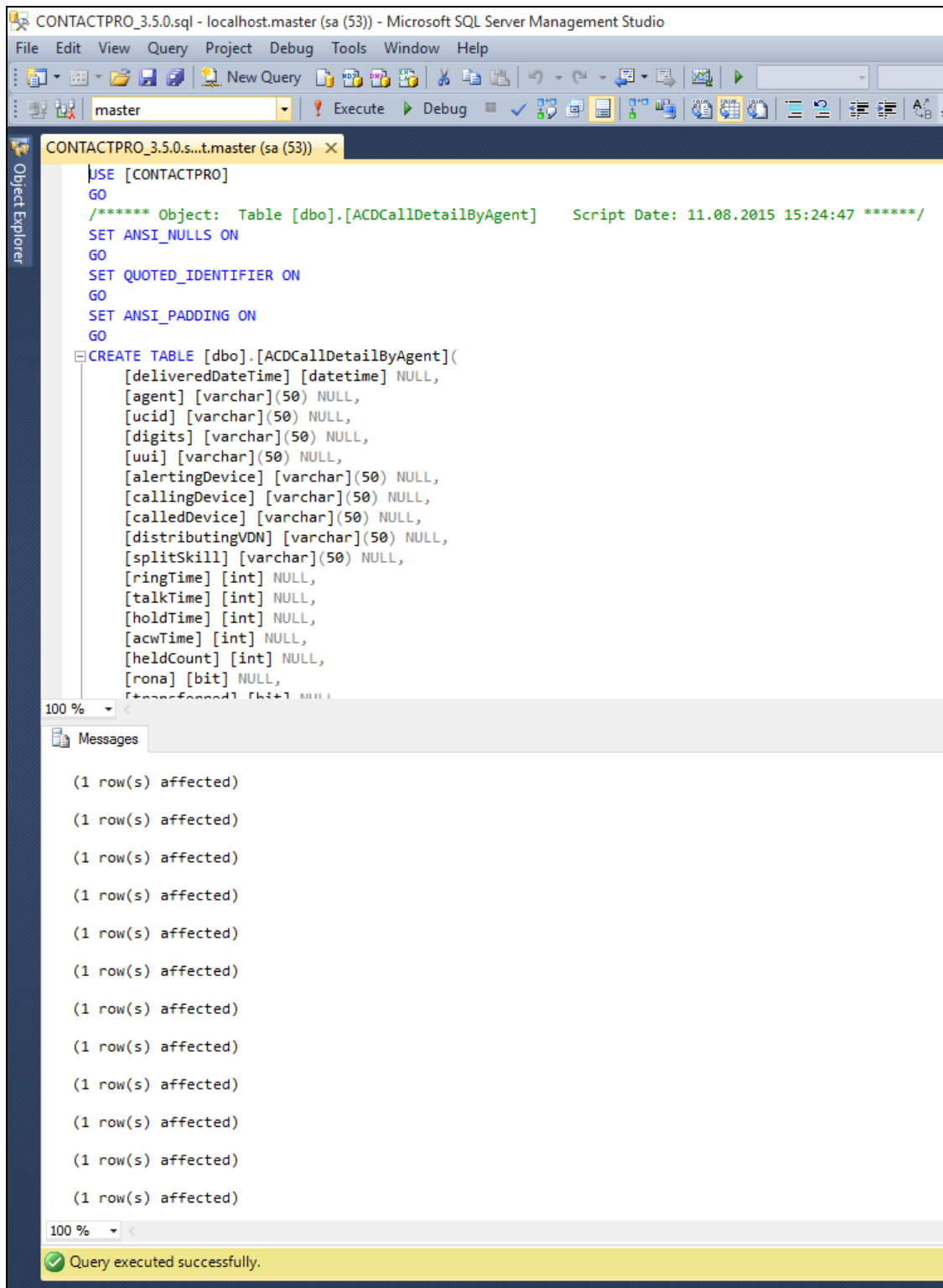
8.1.3. Execute CONTACTPRO®.sql script

Fill the contents of the **CONTACTPRO®** database, open the provided **CONTACTPRO®_3.5.sql** script.

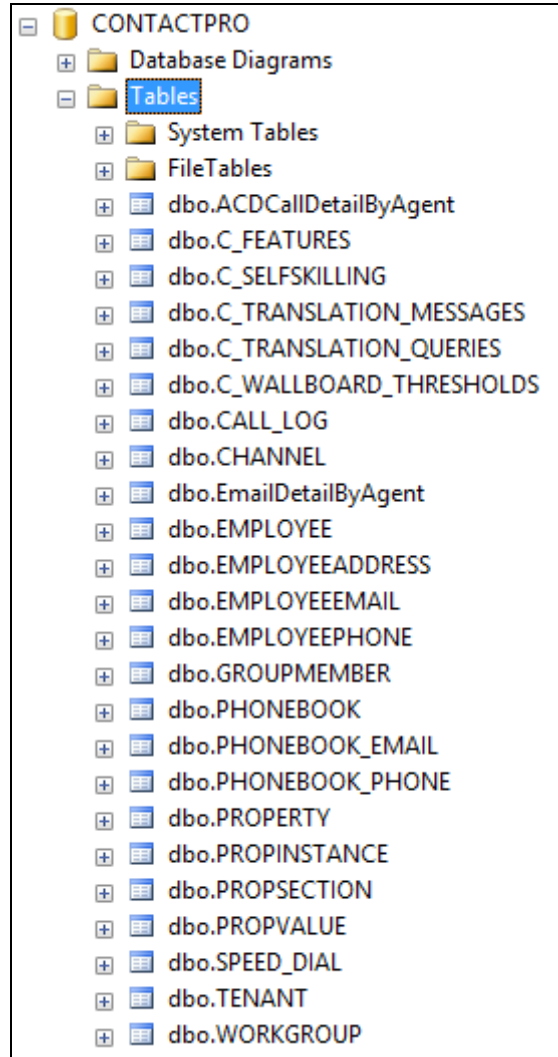


Execute the script by clicking the Execute button.





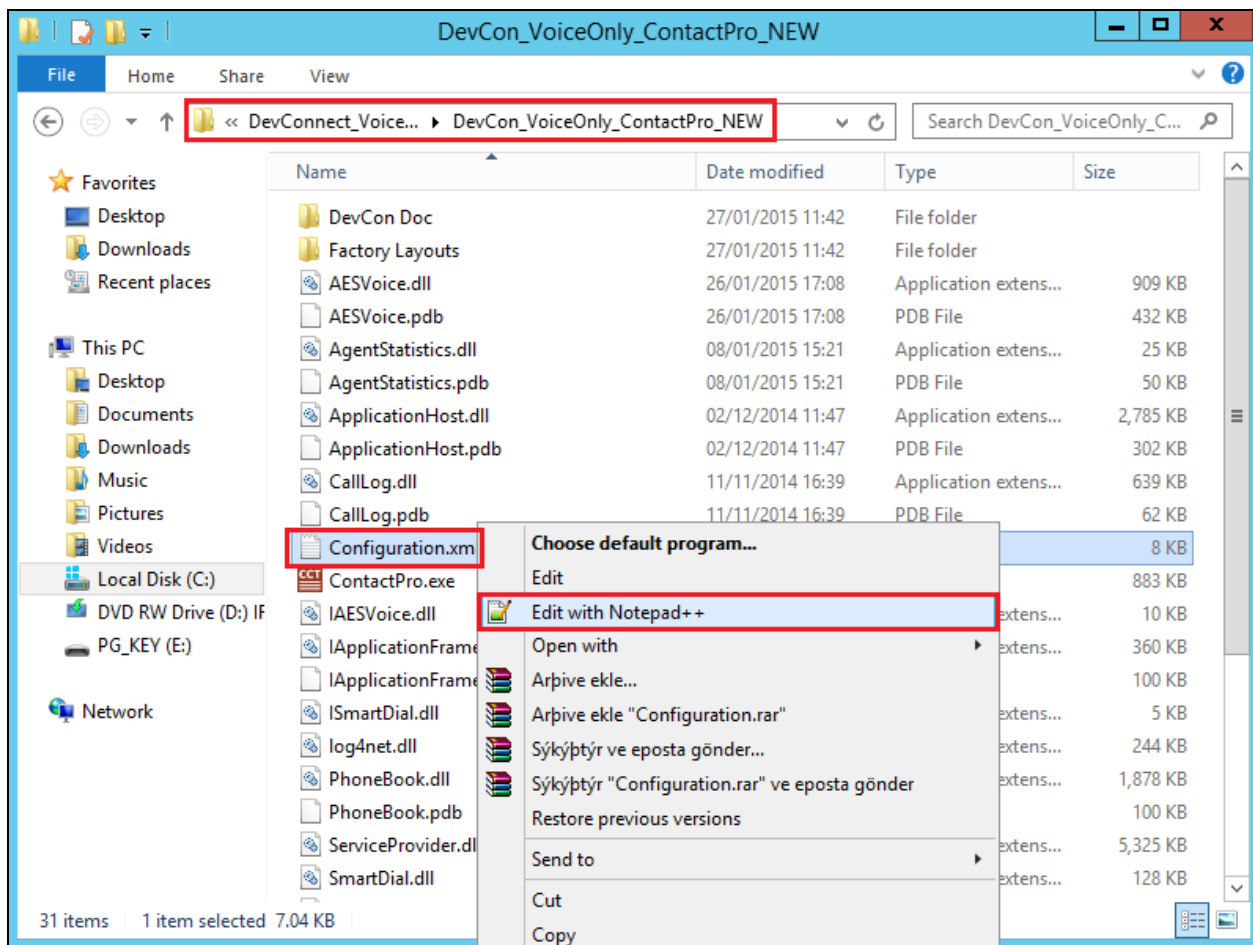
The contents of the **CONTACTPRO®** database will now look like this.



8.2. Configure ContactPro® and ContactPro® Manager Connection to the Database

ContactPro® and ContactPro® Manager need the connection settings to the ContactPro® database. This is typically the only configuration required before deployment of the software to users.

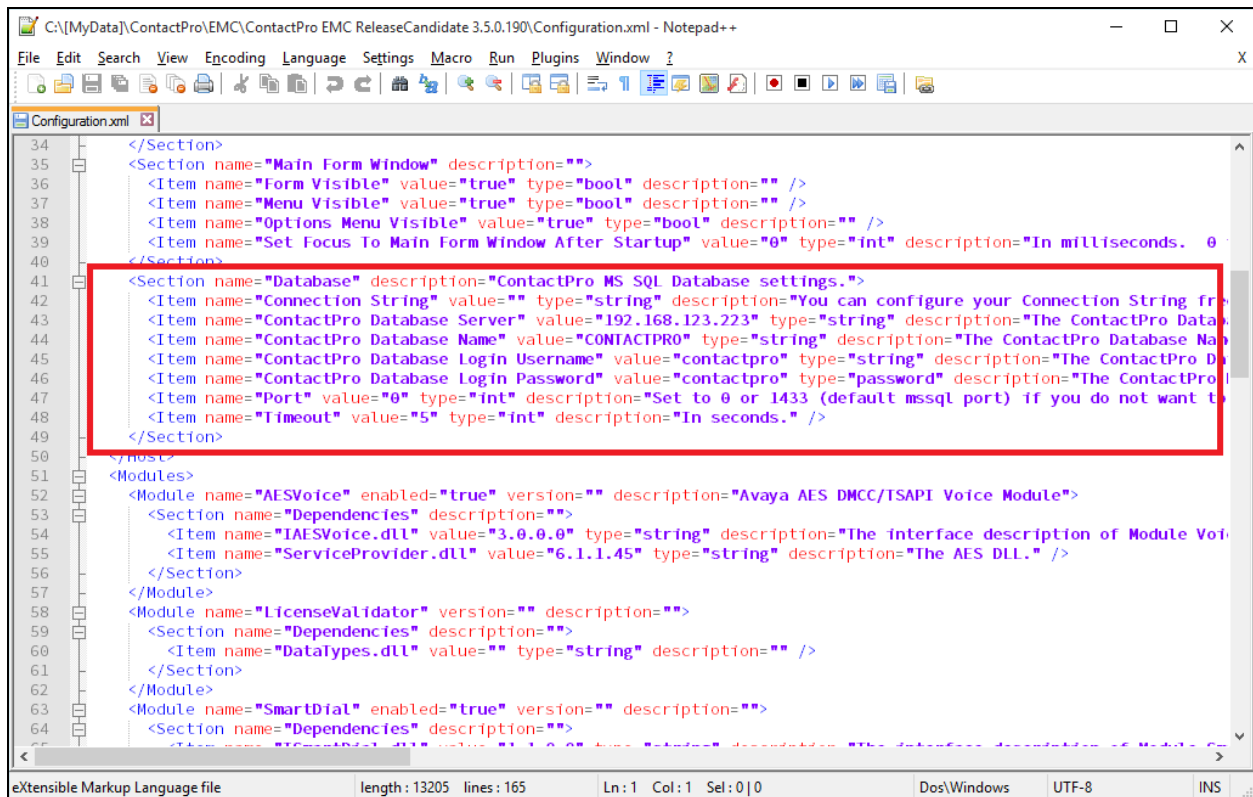
Navigate to the folder where ContactPro® and ContactPro® Manager have been installed. Right click on the file called **Configuration.xml** and open this with a program such as Notepad or **Notepad ++** as is shown below.



Once this file is opened navigate to the section regarding the **ContactPro® MS SQL Database settings**. Here the following must be entered correctly.

- **ContactPro® Database Server**
- **ContactPro® Database Name**
- **ContactPro® Database Login Username**
- **ContactPro® Database Login Password**
- **Database Port**
- **Timeout**

Once this information has been entered correctly save the file (**File → Save** (not shown)).



```
34 </Section>
35 <Section name="Main Form Window" description="">
36 <Item name="Form Visible" value="true" type="bool" description="" />
37 <Item name="Menu Visible" value="true" type="bool" description="" />
38 <Item name="Options Menu Visible" value="true" type="bool" description="" />
39 <Item name="Set Focus To Main Form Window After Startup" value="0" type="int" description="In milliseconds. 0" />
40 </Section>
41 <Section name="Database" description="ContactPro MS SQL Database settings.">
42 <Item name="Connection String" value="" type="string" description="You can configure your Connection String from here." />
43 <Item name="ContactPro Database Server" value="192.168.123.223" type="string" description="The ContactPro Database Server." />
44 <Item name="ContactPro Database Name" value="CONTACTPRO" type="string" description="The ContactPro Database Name." />
45 <Item name="ContactPro Database Login Username" value="contactpro" type="string" description="The ContactPro Database Login Username." />
46 <Item name="ContactPro Database Login Password" value="contactpro" type="password" description="The ContactPro Database Login Password." />
47 <Item name="Port" value="0" type="int" description="Set to 0 or 1433 (default mssql port) if you do not want to use a port." />
48 <Item name="Timeout" value="5" type="int" description="In seconds." />
49 </Section>
50 </root>
51 <Modules>
52 <Module name="AESVoice" enabled="true" version="" description="Avaya AES DMCC/TSAPI Voice Module">
53 <Section name="Dependencies" description="">
54 <Item name="IAESVoice.dll" value="3.0.0.0" type="string" description="The interface description of Module Voice." />
55 <Item name="ServiceProvider.dll" value="6.1.1.45" type="string" description="The AES DLL." />
56 </Section>
57 </Module>
58 <Module name="LicenseValidator" version="" description="">
59 <Section name="Dependencies" description="">
60 <Item name="DataTypes.dll" value="" type="string" description="" />
61 </Section>
62 </Module>
63 <Module name="SmartDial" enabled="true" version="" description="">
64 <Section name="Dependencies" description="">
65 <Item name="SmartDial.dll" value="1.0.0.0" type="string" description="The SmartDial DLL." />
66 </Section>
67 </Module>
68 </Modules>
```


8.3. Configure Properties with ContactPro® Manager

The ContactPro® Manager allows the configuration of properties for all ContactPro® Clients. Global properties can be set at the **Top System Level** or set different properties at the **Tenant level** or **Workgroup level** or for each **individual Agent**.

Properties only need to be configured in sub levels if different Properties for other Tenants are required.

The following sections describe the minimum required properties to configure for ContactPro® in order to connect successfully to both the Session Manager and AES Server. All other properties may be left at their default values.

8.3.1. Configure the Connection to Avaya Aura® Session Manager

From a Supervisor or Administrator PC where the CCT ContactPro® Manager application was installed double click on the CCT ContactPro® Manager shortcut as shown below. The **ContactPro® Manager** is opened and select **SIP/Server** from the **Sections** window.

The information highlighted below must all be filled in; this information is all obtained from **Section x**. This information is all required to connect successfully to Session Manager.

ContactPro Manager

Search Sections...

POM/WrapUp

POMCloseInbound

PresenceCPS

QuickMenu

Remedy

Remedy/Screenpop/Knowledge

Remedy/Screenpop/Ticket

Salesforce/Screenpop/Chat

Salesforce/Screenpop/Email

Salesforce/Screenpop/General

Salesforce/Screenpop/POM

Salesforce/Screenpop/Voice

Salesforce/Server

SAP

SAP/Screenpop/General

SAP/Screenpop/Voice

SAP/StartupTab

Screenpop

Screenpop/Chat

Screenpop/Custom

Screenpop/Email

Screenpop/General

Screenpop/POM

Screenpop/Voice

SelfSkilling

SendFeedback

SIP/CallControls

SIP/Server

SpeedDial

Properties

Name

Domain

Registrar

SipPort

StunPort

StunServer

Transport

devconnect.com

10.30.5.92

5061

3478

TLS

8.3.2. Configure the Connection to Avaya Aura® Application Enablement Services

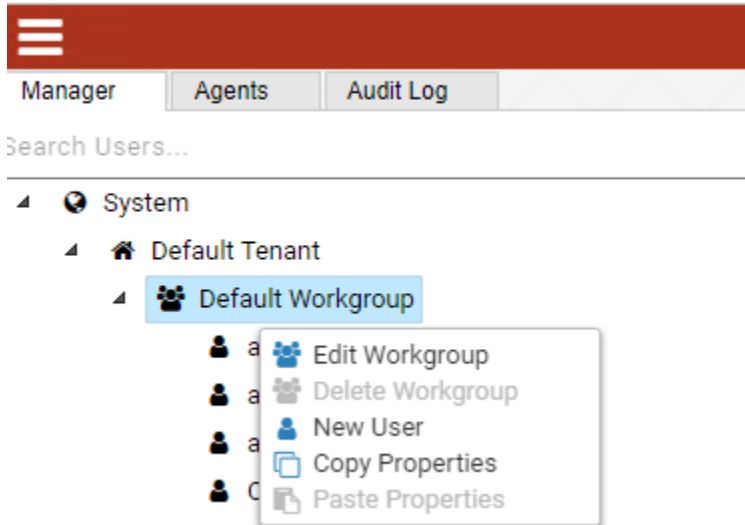
From a Supervisor or Administrator PC where the CCT ContactPro® Manager application was installed double click on the CCT ContactPro® Manager shortcut as shown below. The **ContactPro® Manager** is opened and select **AESVoice/AESServer** from the **Sections** window.

The information highlighted below must all be filled in; this information is all obtained from **Section 6**. This information is all required to connect successfully to the AES and each part is changed by double-clicking on the field that needs to be changed.

ContactPro Manager		
Search Sections...	Properties	
[Gateway]	Name	Value
ACM	AESProtocolVersion	7.1.1
ACMGateway	PrimaryAESACMConnectionName	CM93
ACR	PrimaryAESIPAddress	10.30.5.95
ACR/AutoTag	PrimaryAESLoginPassword	*
ACR/Record	PrimaryAESLoginUsername	cct
ActiveDirectory	PrimaryAESPort	4721
ActiveDirectory/ContextMenu	PrimaryAESSecureSocket	No
ActiveDirectory/Search	QuaternaryAESACMConnectionName	
AESVoice	QuaternaryAESIPAddress	
AESVoice/AESServer	QuaternaryAESLoginPassword	*
AESVoice/AgentControls	QuaternaryAESLoginUsername	
AESVoice/CallControls	QuaternaryAESPort	4721
AESVoice/General	QuaternaryAESSecureSocket	No
AESVoice/Logout	SecondaryAESACMConnectionName	
AESVoice/StatusBar	SecondaryAESIPAddress	
AESVoice/VoiceMail	SecondaryAESLoginPassword	*
AgentStateLog	SecondaryAESLoginUsername	
AgentStatistics	SecondaryAESPort	4721
AgentStatistics/AvgACWThreshHolds	SecondaryAESSecureSocket	No
AgentStatistics/AvgHandleTimeThreshHolds		
AgentStatistics/LiveCallThreshHolds		
ApplicationHost		
ApplicationHost/Language		
ApplicationHost/Logging		
ApplicationHost/SmartClient		
AUXLog		
CallLog		
CoBrowse		
ContextData		
CP/Server		
CPCallDetailReporting		
CPChannels		
CPChat		
CPChat/AutoTranslation		
CPChat/SecureForm		
CpCore		
CpCore/AgentControls		
CpCore/ChannelControls		

8.4. Configure Users with ContactPro® Manager

For every ContactPro® Client user, you need to create a New Employee. Right-click on a workgroup then click “New User”.



The following fields are required.

- Username (This is the **Agent ID** such as that created in **Section 5.4** for example).
- First Name
- Last Name
- Password

Username* 80000	Title
First Name* Agent	Last Name* Voice
Phone 70000	Email
CRM Username	
Active Directory Username	
Agent ▼	
▼	
Password *****	
<input type="checkbox"/> Change Password On Login <input type="checkbox"/> IsQMAgent	
Agent ID	Agent Password

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

Create employees under different workgroups in different tenants. This allows you to easily manage different Properties for different **Tenants** or **Workgroups** or each individual **Employee**. NOTE: You do not need to duplicate properties. You only need to configure what's different compared to the upper level which could be either the **Top System Level, Tenant** or **Workgroup** level.

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 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 5.2. 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	9	no	aes8	established	14	14

Enter the command **list agent-loginID** verify that agent **80000** shown in **Section 5.4** is logged-in to extension **70000**

```
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
80000	Voice Agent	70000						1	lvl
	2/01	/	/	/	/	/	/	/	

Enter the command **status station 70000** and on **Page 7** verify that the agent is logged-in to the appropriate skill.


```
status station 1005
```

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

9.2. 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 6.3**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.0.5-0
Server Date and Time: Tue Mar 26 15:49:11 ICT 2019
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

▶ Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▶ CVLAN Service Summary

▶ DLG Services Summary

▶ DMCC Service Summary

▶ Switch Conn Summary

▶ TSAPI Service Summary

▶ User Management

▶ Utilities

▶ Help

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	CM8	1	Talking	Tue Mar 26 18:48:36 2019	Online	18	0	8	8	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 user name from **Section 6.5**.

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
User Management
Utilities
Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

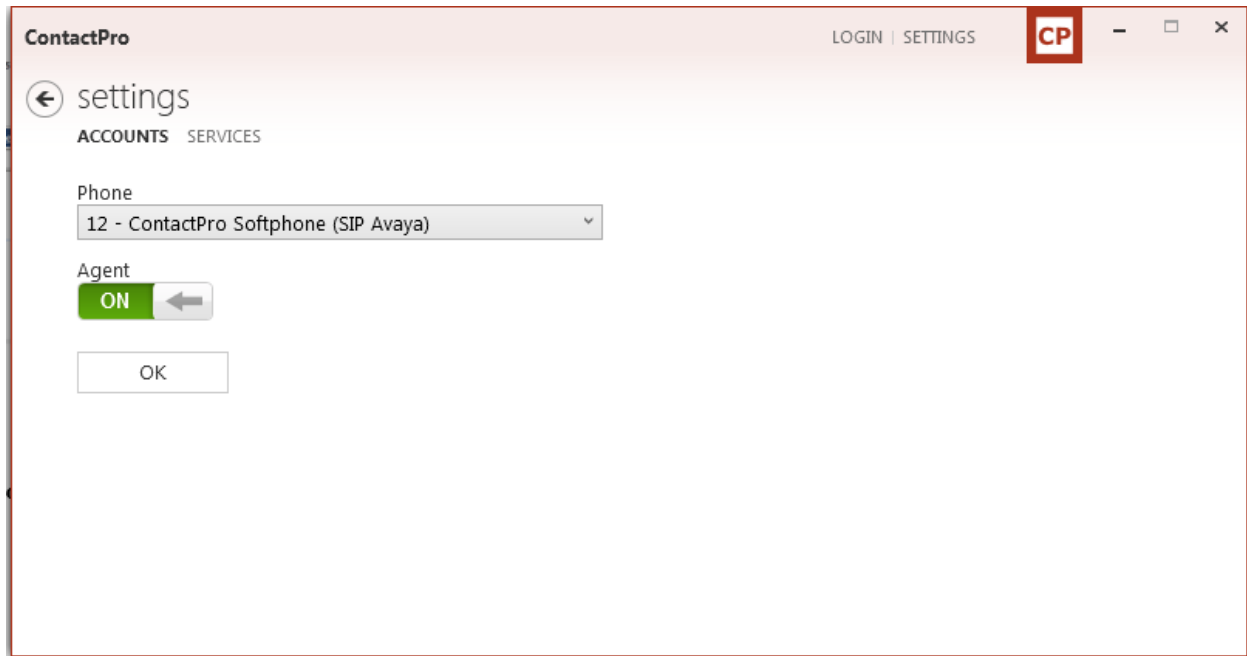
Session Summary [Device Summary](#)
Generated on Mon Apr 08 10:04:44 ICT 2019
Service Uptime: 11 days, 16 hours 57 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 1861
Number of Existing Devices: 0
Number of Devices Created Since Service Boot: 1701

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	82ED47D965F1BFBC5 B296764A7EC224C-1860	cct	AESVoice	10.128.224.59	XML Unencrypted	0

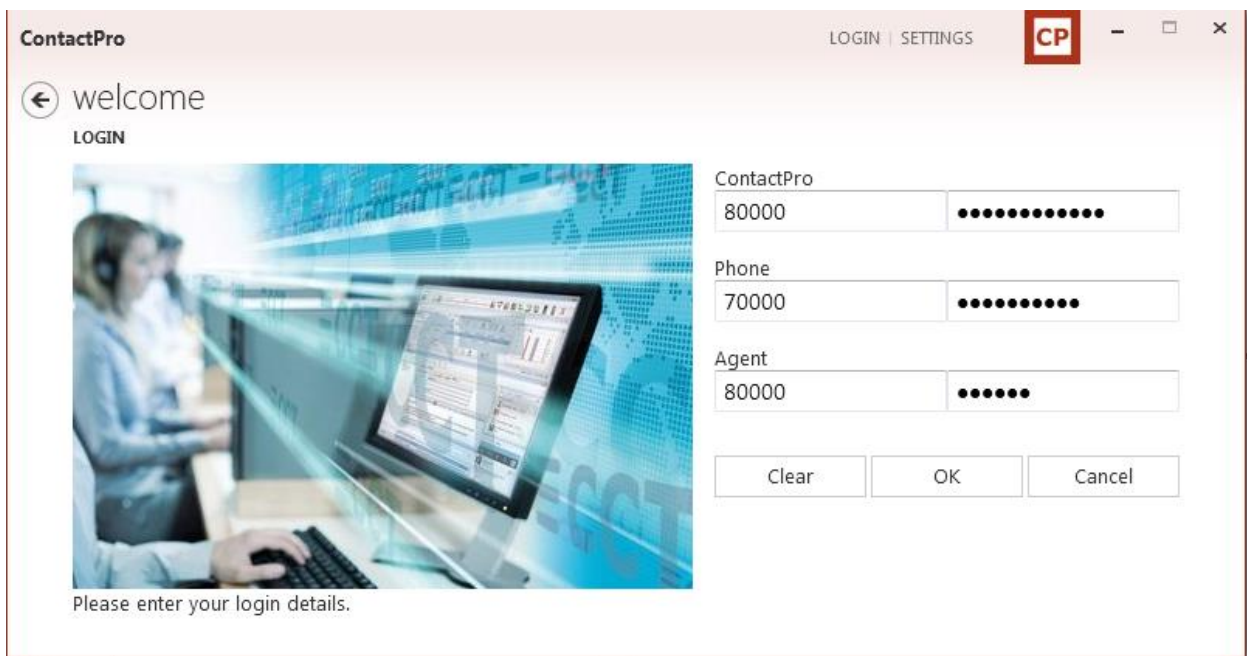
Item 1-1 of 1
1 Go

9.3. Verify Login of ContactPro® Client

From the Client PC open the application **ContactPro®**. Once this is opened, select **SETTINGS** and choose **Phone** as **12 – ContactPro® Softphone (SIP Avaya)**



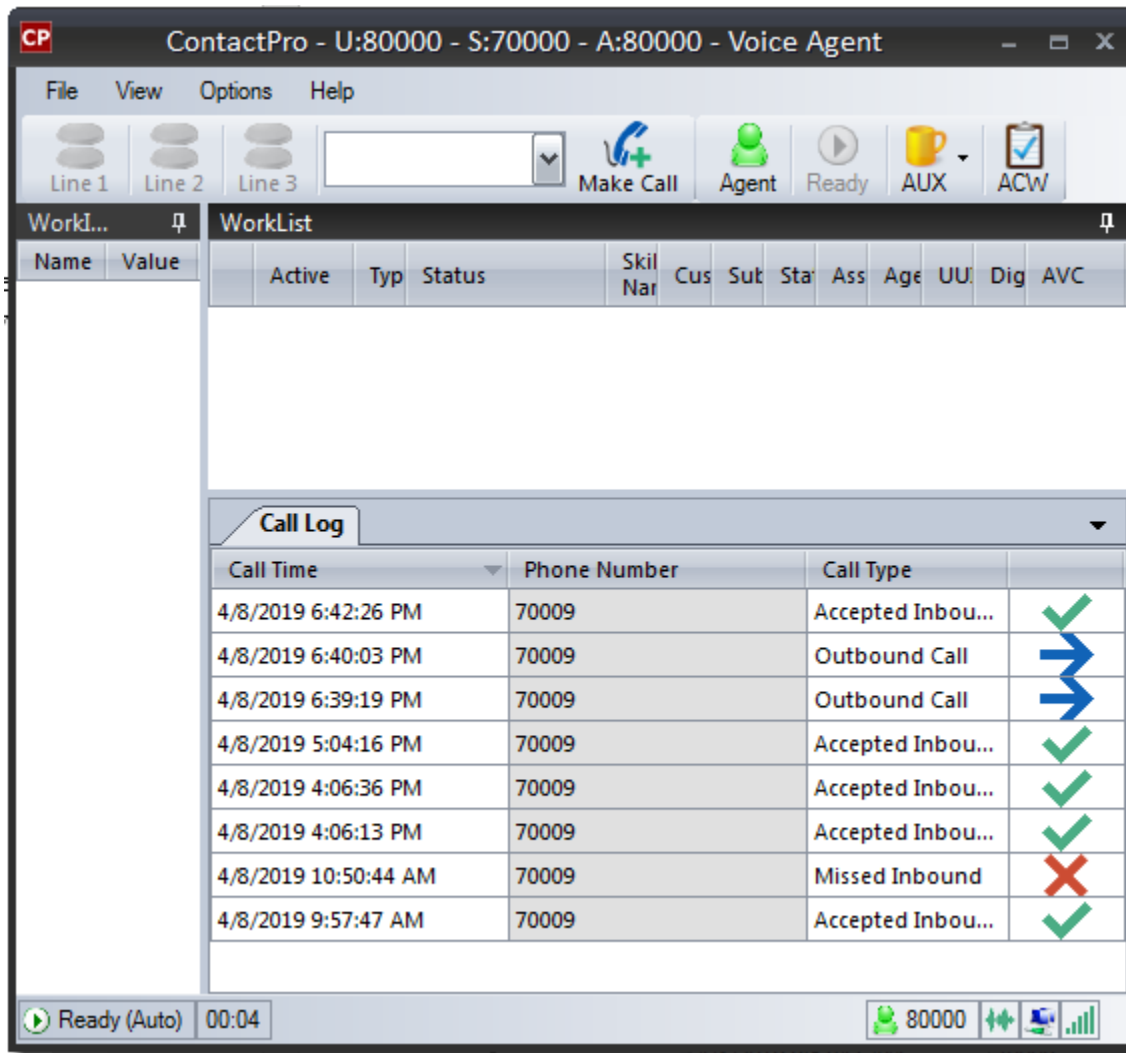
Click on **OK** to fill following details:



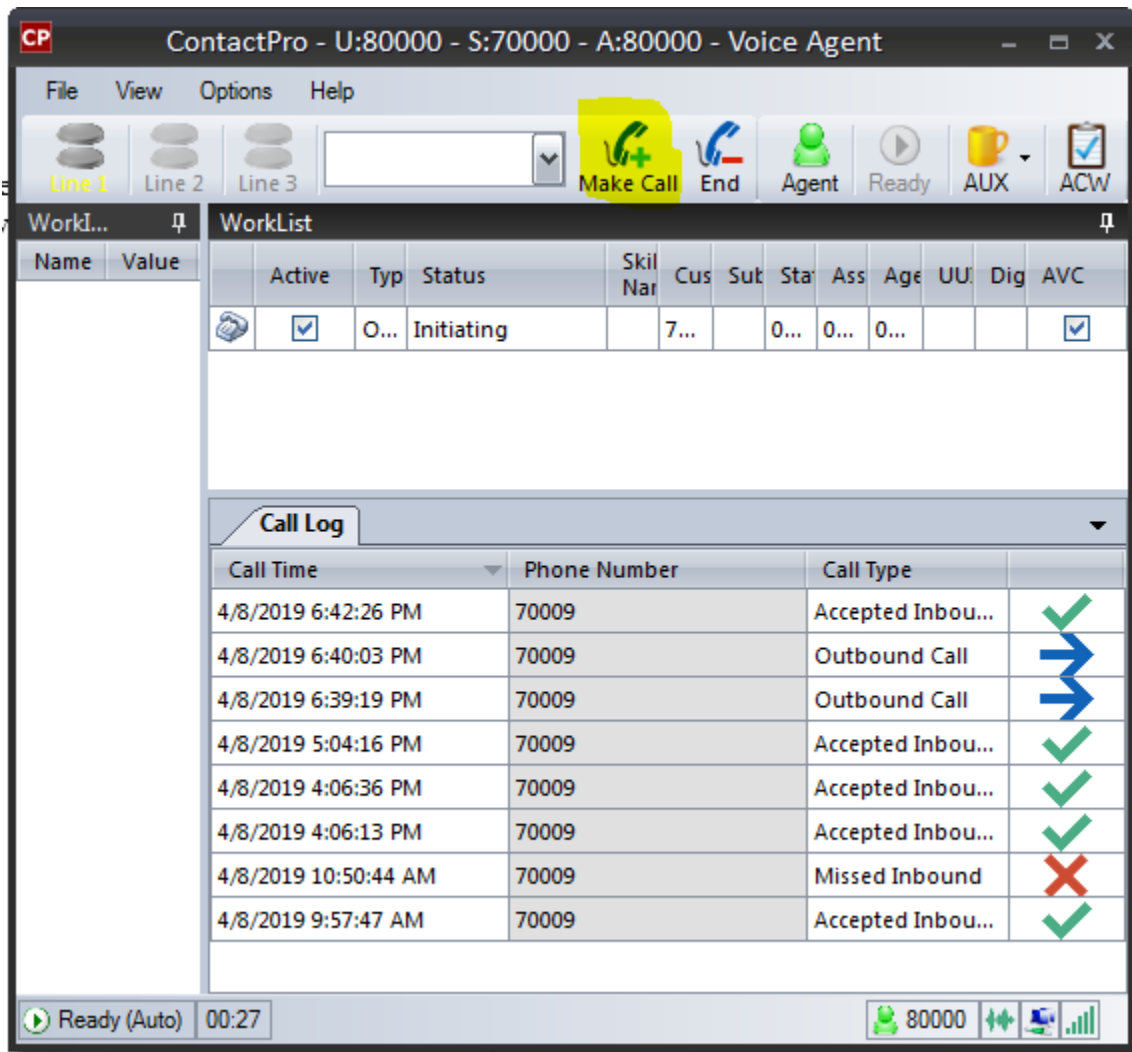
Click on **OK** to log in to **ContactPro®**

9.4. Verify Agent Status using ContactPro®

Once logged in, the agent state can be changed using the buttons at the top left highlighted below. Note also the station number (**70000**) and Agent ID (**80000**) once logged in. Click on **Ready** to make the agent ready.



Make a call with the **MakeCall** button.



Make an incoming call from PSTN to a general routing VDN in **Section 5.1**. Verify that the CCT ContactPro® Client can receive incoming call. Answer incoming calls with the **Answer** button.

ContactPro - U:80000 - S:70000 - A:80000 - Voice Agent

File View Options Help

Line 1 Line 2 Line 3 [Dropdown] Make Call **Answer** Agent Ready AUX

Work... WorkList

Name	Value	Active	Typ	Status	Skill Nar	Cus	Sub	Sta	Ass	Age	UU	Dig	AVC
		<input checked="" type="checkbox"/>	A...	Alerting		7...		0...	0...	0...			<input checked="" type="checkbox"/>

Call Log

Call Time	Phone Number	Call Type	
4/8/2019 6:53:08 PM	70009	Outbound Call	➔
4/8/2019 6:42:26 PM	70009	Accepted Inbound...	✓
4/8/2019 6:40:03 PM	70009	Outbound Call	➔
4/8/2019 6:39:19 PM	70009	Outbound Call	➔
4/8/2019 5:04:16 PM	70009	Accepted Inbound...	✓
4/8/2019 4:06:36 PM	70009	Accepted Inbound...	✓
4/8/2019 4:06:13 PM	70009	Accepted Inbound...	✓
4/8/2019 10:50:44 AM	70009	Missed Inbound	✗
4/8/2019 9:57:47 AM	70009	Accepted Inbound...	✓

Ready (Auto) 01:25 80000 [Icons]

10. Conclusion

These Application Notes describe the configuration steps required for Deutschland GmbH ContactPro® 5.2 from CCT for Breeze Client SDK to successfully interoperate with Avaya Aura® Session Manager R8, and Avaya Aura® Application Enablement Services R8. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the Avaya and CCT Deutschland GmbH product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Administering Avaya Aura® Communication Manager, Release 8, Issue 2.0, Nov 2018*
2. *Administering Avaya Aura® Session Manager, Release 8, Issue 2, August 2018*
3. *Administering Avaya Aura® System Manager, Release 8, Issue 4, September 2018*
4. *Administering Avaya Aura® Application Enablement Services, Release 8.0.1, Issue 2, December 2018*

Product documentation for CCT Deutschland GmbH may be found at <http://cct-solutions.com>

©2019 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.