



Avaya Solution & Interoperability Test Lab

Application Notes for configuring CCT ContactPro v3 with Avaya Aura® Application Enablement Services R6.3 and Avaya Aura® Communication Manager R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for ContactPro from CCT to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. The CCT ContactPro is an interaction management application that connects to Avaya Aura® Application Enablement Services using TSAPI.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the 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 ContactPro from CCT Software, to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. The CCT ContactPro Solutions offers 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. ContactPro is a solution for agent desktops in an Avaya call center environment focused on voice. ContactPro can be installed with enabled Presence Services and integrated Customer Data. ContactPro empowers agents to efficiently serve customers by allowing the agents have full call control from the agents screen. ContactPro is an interaction management application which utilises the TSAPI connection to gain call control of existing Avaya Aura® Communication Manager endpoints. Typically these endpoints are hardphones that Avaya Aura® Communication Manager elite agents are logged into. So therefore it can be considered as an alternative to, and expands on the features provided by, Avaya one-X® Agent.

2. General Test Approach and Test Results

The general test approach was to validate successful handling of inbound skillset/VDN calls using ContactPro. 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 both the physical phone and ContactPro Agent client in synchronisation.

ContactPro has a Client/Server relationship and ContactPro server was installed on a Windows 2012 Server R2 running an MS SQL 2012 database. Tables are created on this database specifically for ContactPro and contained in these tables is the configuration information required for the connection to AES. The database has also many other tables utilised by ContactPro clients such as contact and customer database information but these are not the focus of these Application Notes. The primary concern is the connection to the AES in order to gain call control of the endpoints on Communication Manager.

ContactPro client software is installed on each client PC utilised by an agent. A configuration file on this software points to the database on the ContactPro server ensuring that each agent PC will get its connection information to AES from a single source i.e., the database on the ContactPro server. When the ContactPro client starts it makes a connection to the database on the ContactPro server and gets the necessary information to connect to AES. Once this information has been received upon start-up, there is no further requirement of the ContactPro server until the client is restarted again. For compliance testing the ContactPro server was not required except for providing the AES information to the ContactPro clients upon start-up. However the Contact Pro server serves a much greater purpose in most production environments.

Avaya SIP endpoints were included in the compliance testing and these endpoints are registered with Session Manager. An assumption is made that Session Manager and System Manager are already installed and basic configuration have been performed.

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

2.1. Interoperability Compliance Testing

The testing focuses on the following areas:

- **Agent state change**– Make agent Ready/Not Ready using ContactPro Agent.
- **Inbound Calls** – Answer calls using ContactPro Agent.
- **Outbound Calls** – Make calls using ContactPro Agent.
- **Call Hold** – Place calls on hold and retrieve calls using ContactPro Agent.
- **Blind Transfer** – Transfer callers using ContactPro Agent.
- **Consultative Transfer** - Transfer callers using ContactPro Agent.
- **Inbound Skillset Calls** – Answer skillset/VDN calls using ContactPro Agent.
- **Failover Testing** - Verify the ability of 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.

- All test cases involving "Transfers" have an issue where the CLID is not being updated on the ContactPro agents screens. Once the calls are transferred, the CLID is updated on the phone set displays, but the CLID shown on the ContactPro screen is that of the original caller and not the transferred number. The fix will be implemented in the next release of ContactPro.
- All test cases involving "Conference" have an issue where the CLID is not being updated on the ContactPro agents screens, when the original caller in the conference hangs up the call. When "Party A" is in conference with Parties B & Contact Pro, then Party A hangs up the call, the ContactPro agents screen displays the CLID of the original caller but the original caller has hung up. This is the same issue reported above. The fix will be implemented in the next release of ContactPro.

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 Heinrich-Hertz-Strasse 5

ZIP 60486

Frankfurt am Main

Germany

Phone +49 69 7191 4969 0

Fax +49 69 7191 4969 666

Kohlenstrasse 2

ZIP 04107

Leipzig

Germany

Phone +49 341 5909 1251

Street Am Eser 2

ZIP 86150 Augsburg

Germany

Phone +49 821 455 152 700

Fax +49 821 455 152 777

Street Werner-von-Siemens-Strasse 6

ZIP 86159

Augsburg

Germany

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

1735 Market Street STE 3750

19103 Philadelphia, PA

USA

office: +1 267 507 6196

2020 North Bayshore Drv. Appt. 2408

33137 Miami FL

United States of America

Phone. +1 844 720 3897

3. Reference Configuration

Below is a diagram of the setup that was used during compliance testing, this setup includes an Avaya Aura® Communication Manager R6.3 and an Avaya G430 Media Gateway. The H323 endpoints are registered to Communication Manager while the SIP endpoints register to Avaya Aura® Session Manager. The CCT ContactPro utilises a TSAPI CTI connection through Avaya Aura® Application Enablement Services to gain call control of existing Avaya SIP and H323 Deskphones.

Note: ContactPro is installed on each client PC that is associated with an Avaya hard phone.

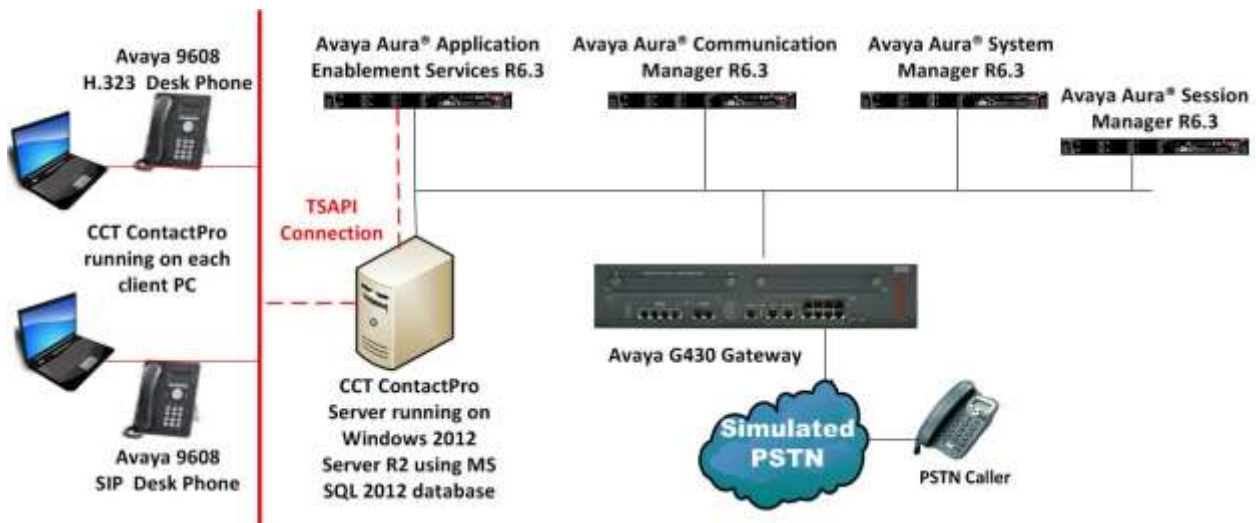


Figure 1: Connection of CCT ContactPro with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 6.3.11 (SP11) Build No. – 6.3.0.8.5682-6.3.8.3204 Software Update Revision No: 6.3.7.7.2275
Avaya Aura® Communication Manager running on a virtual server	R6.3 SP9 R016x.03.0.124.0
Avaya Aura® Application Enablement Services running on a virtual server	R6.3 SP3 Build No – 6.3.3.1.10-0
Avaya Aura® Session Manager running on a virtual server	Session Manager R 6.3 SP11 Build No. – 6.3.11.0.631103
Avaya G430 Gateway	33.12.0 /1
Avaya 9620 Series Deskphone	96xx H.323 Release 3.1 SP2
Avaya 9608 Series Deskphone	96x1 H323 Release 6.4014U
Avaya 9641 Series Deskphone	96x1 SIP Release 6.2.1.26
Avaya 9608 Series Deskphone	96x1 SIP Release 6.4.0.33
CCT ContactPro Server running on a Windows Server using MS SQL 2012	Windows 2012 R2 MS SQL 2012 ContactPro 3.2.12
CCT ContactPro Agent running on Windows 7 Client PC	ContactPro 3.2.12

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	Computer Telephony Adjunct Links?	y
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	y		
Attendant Vectoring?	y		

5.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and note the IP address for the **procr** and **AES (aes63vmpg)**.

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM100	10.10.40.34		
aes63vmpg	10.10.40.30		
default	0.0.0.0		
g430	10.10.40.15		
procr	10.10.40.31		

5.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 5.2**.
- **Local Port:** Retain the default value of **8765**.

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

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes63vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services				Page	4	of	4
AE Services Administration							
Server ID	AE Services Server	Password	Enabled	Status			
1:	aes63vmpg	*****	y	idle			
2:							
3:							

5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. 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: 2002			
Type: ADJ-IP			
COR: 1			
Name: aes63vmpg			

5.5. Add a Hunt Group for a Skill-based Routing

Use the command, **add hunt group x**, where x is the new hunt group to be added. This will add a new hunt group to Communication Manager and this can be utilized as a skill when creating an inbound Vector in **Section 5.6**.

add hunt-group 33		Page 1 of 4
HUNT GROUP		
Group Number: 33	ACD? y	
Group Name: PGPresINBOUND	Queue? y	
Group Extension: 3330	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:	

5.6. Configure Inbound Vector

A vector must be configured; this defines the steps required to route an inbound call to a required destination or hunt group. Enter the command **change vector x** where x is an appropriate vector number and configure as shown below:

- **Name** – assign an identifying name.
- **adjunct routing link 1** – enter the cti-link number created in **Section 5.4**. Adjunct routing is optional. Normally an extra Call Routing Server is required to handle the adjunct link route request and make routing decisions based on a database search etc.

change vector 3		Page 1 of 6
CALL VECTOR		
Number: 3	Name: PresINBOUND	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n
Basic? y	EAS? y	G3V4 Enhanced? y
Prompting? y	LAI? y	G3V4 Adv Route? y
Variables? y	3.0 Enhanced? y	CINFO? y
01 adjunct	routing link 1	BSR? y
02 wait-time	5 secs hearing silence	Holidays? y
03 queue-to	skill 33 pri m	
04 wait-time	10 secs hearing ringback	
05 queue-to	skill 33 pri m	
06 wait-time	10 secs hearing ringback	
07 disconnect	after announcement none	
08		
09		
10		
11		
12		

5.7. Configure Inbound VDN

A VDN must be added; this is the number dialled to reach the vector configured in **Section 5.6**. Enter the command **add VDN x** where **x** is an appropriate extension number and configure an identifying **Name** and the **Destination: Vector Number** configured in **Section 5.6**.

```
add vdn 3300                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 3300
      Name*: PresINBOUND
      Destination: Vector Number              3
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none

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

* Follows VDN Override Rules
```

5.8. Configure Agent ID

To add a new agent use the command, **add agent-loginID x**, where **x** is the Agent ID number. On **Page 1** enter the **Login ID** and a suitable **Name** for the agent. Enter and take note of the **Password** as this will be required again in **Section 8.1**. This is a printout of one of the agents used during compliance testing.

```
add agent-loginID 4401                           Page 1 of 3
                                         AGENT LOGINID

      Login ID: 4401                                AAS? n
      Name: Paul                                    AUDIX? n
      TN: 1                                          LWC Reception: spe
      COR: 1                                         LWC Log External Calls? n
Coverage Path:                                     AUDIX Name for Messaging:
Security Code:

      LoginID for ISDN/SIP Display? n
      Password:
      Password (enter again):
      Auto Answer: station
      MIA Across Skills: system
      ACW Agent Considered Idle: system
      Aux Work Reason Code Type: system
      Logout Reason Code Type: system
      Maximum time agent in ACW before logout (sec): system
      Forced Agent Logout Time: :
```

On **Page 2** associate the skill (**SN**) or hunt group that was created in **Section 5.5** with the agent so that calls routed to that hunt group will be answered by this agent.

add agent-loginID 4401										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: 33		1	16:			31:			46:			
2: 34		1	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:			

5.9. Configure Agent Stations

It is assumed that all agent stations are already properly configured and that all monitored phones are already in place. Please refer to the **Appendix** for a printout of the Avaya 9641 SIP Deskphone that was used during compliance testing.

However the **ACM Station Password** that is required in **Section 8.1**, is the **Security Code** below and if this is not already known type **change station x**, where x is the extension number to be changed. Enter a new **Security Code** and press **F3** to save. This security code will then be used as the **ACM Station Password** in **Section 8.1**.

change station 2015										Page 1 of 5		
STATION												
Extension: 2015				Lock Messages? n				BCC: M				
Type: 9620				Security Code: 1234				TN: 1				
Port: S00099				Coverage Path 1:				COR: 1				
Name: CCT Agent 1				Coverage Path 2:				COS: 1				
				Hunt-to Station:				Tests? y				
STATION OPTIONS												
Location:				Time of Day Lock Table:								
Loss Group: 19				Personalized Ringing Pattern: 1								
				Message Lamp Ext: 2015								
Speakerphone: 2-way				Mute Button Enabled? y								
Display Language: english												
Survivable GK Node Name:				Media Complex Ext:								
Survivable COR: internal				IP SoftPhone? y								
Survivable Trunk Dest? y												
				IP Video Softphone? y								
				Short/Prefixed Registration Allowed: default								

5.10. Save Avaya Aura® Communication Manager Configuration

From the Command Line enter **Save Translation**, in order to commit the changes that have been introduced to memory on Communication Manager.

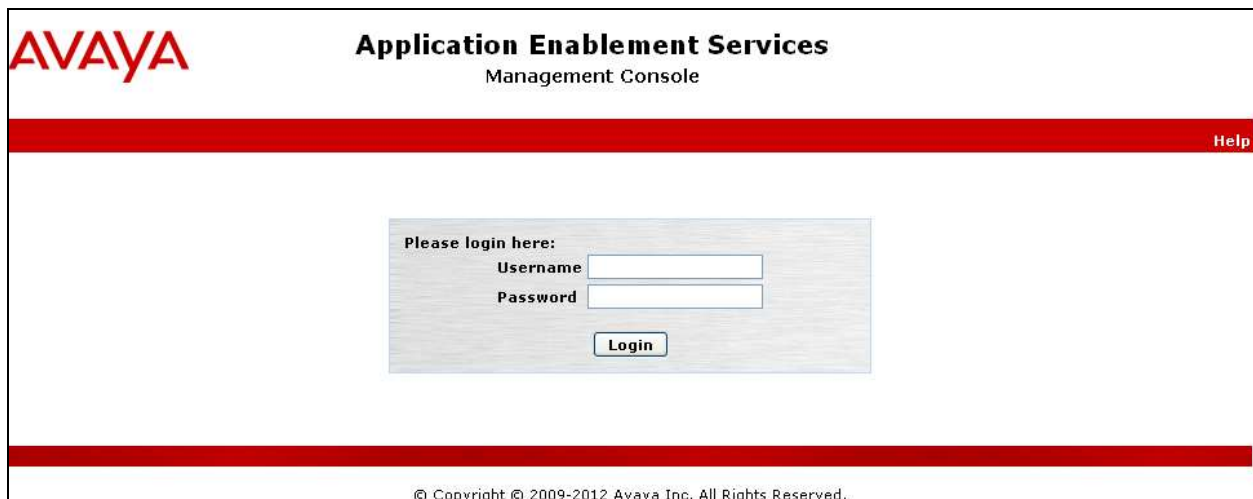
6. Configure Avaya Aura® Application Enablement Services Server

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI & DMCC Ports
- Create CTI User
- Associate Devices with CTI User

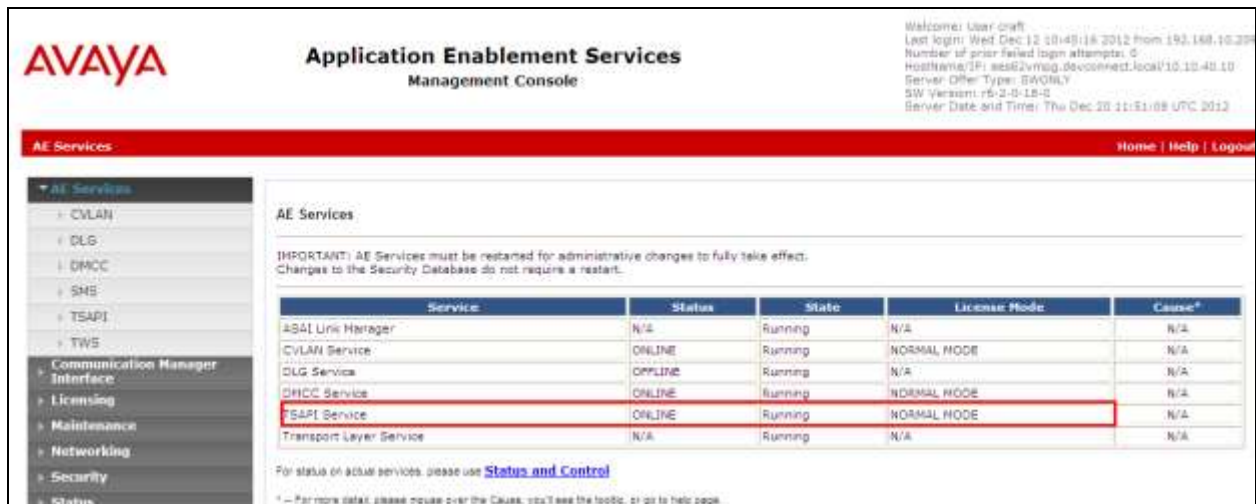
6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login page. The page has a red header bar with the Avaya logo on the left and the text "Application Enablement Services Management Console" in the center. A red bar at the top right contains a "Help" link. The main content area is white and contains a login box with the text "Please login here:". Inside the box, there are two input fields labeled "Username" and "Password", and a "Login" button below them. A red bar at the bottom of the page contains the copyright notice: "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.



AVAYA Application Enablement Services Management Console

Welcome! User: craft
Last login: Wed Dec 12 10:48:16 2012 from 193.168.10.208
Number of prior failed login attempts: 0
HostName/IP: aes62vmag.devconnect.local/10.10.40.10
Server Offer Type: SWONLY
SW Version: r6-2.0-18-0
Server Date and Time: Thu Dec 20 11:51:09 UTC 2012

AE Services Home | Help | Logout

AE Services

IMPORTANT! AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause ¹
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	ONLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

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

¹ - For more detail, please mouse over the Cause; you'll see the tooltip, or go to help page.

6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.



AVAYA Application Enablement Services Management Console

Welcome! User: craft
Last login: Thu Nov 14 20:22:12 2012 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.8.212-0
Server Date and Time: Tue Dec 3 15:33:26 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

CONJUNG Add Connection

Connection Name	Processor Ethernet	Max Period	Number of Active Connections
Edit Connection Edit PE/CN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy			

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

AVAYA Application Enablement Services Management Console

Welcome: User: cm6j
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63Jmmpg
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.113-0
Server Date and Time: Tue Dec 3 15:35:47 UTC 2013

Communication Manager Interface | Switch Connections

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

Connection Details - CM6Jmmpg

Switch Password: [REDACTED]
Confirm Switch Password: [REDACTED]
Tag Period: 30 Minutes (1 - 72)
SSL: [X]
Processor Ethernet: [X]
[Apply] [Cancel]

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown, see the screen at the bottom of page 14). In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

AVAYA Application Enablement Services Management Console

Welcome: User: cm6j
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63Jmmpg
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.113-0
Server Date and Time: Tue Dec 03 15:36:31 UTC 2013

Communication Manager Interface | Switch Connections

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

Edit Processor Ethernet IP - CM6Jmmpg

10.10.40.31 [Add/Edit Name or IP]

Name or IP Address	Status
10.10.40.31	In Use

[Back]

6.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



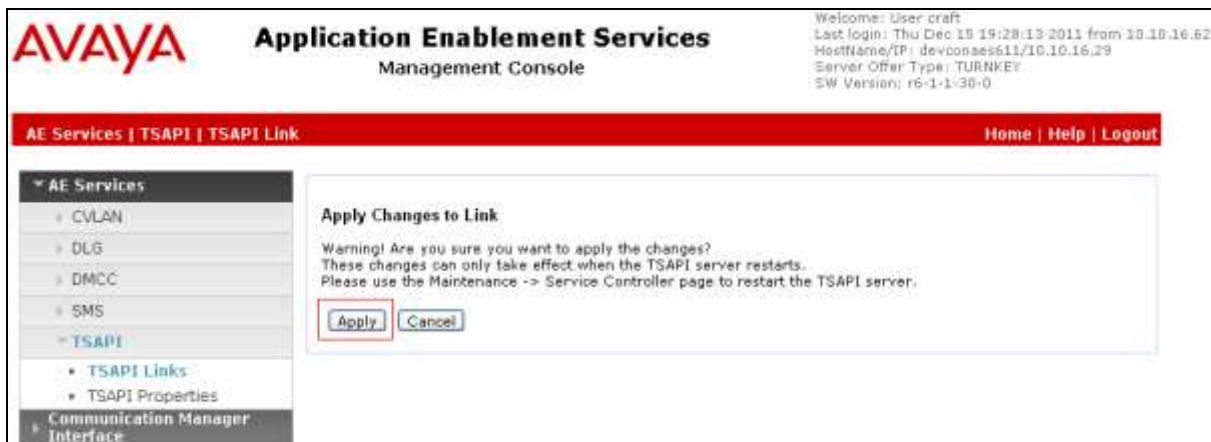
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM63VMPG**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



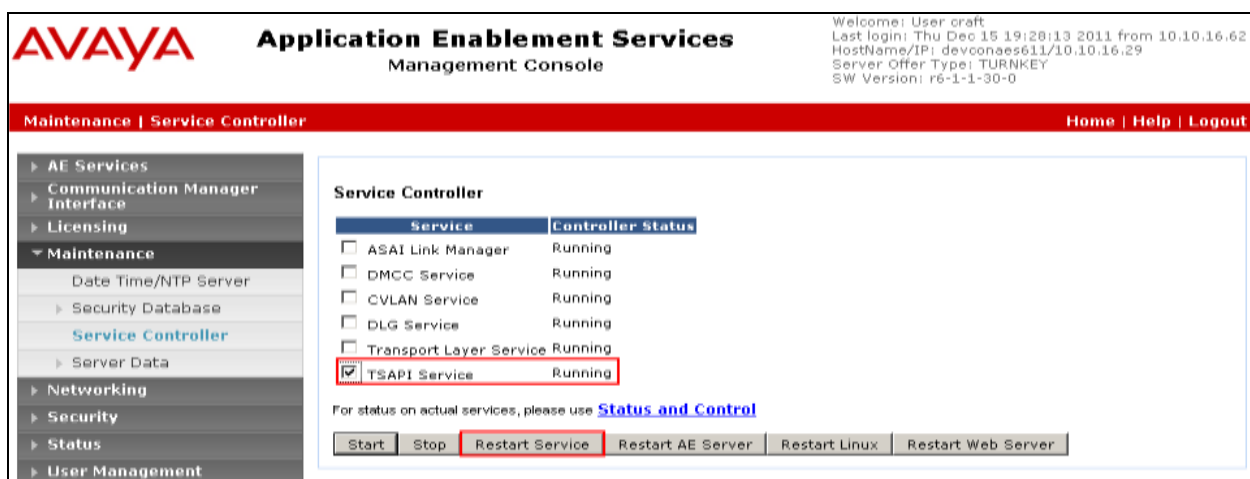
Another screen appears for confirmation of the changes made. Choose **Apply**.



When the TSAPI Link is completed, it should resemble the screen below.



The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance** → **Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". Below this, a red navigation bar contains the text "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. The Security section is expanded, showing sub-items like Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, and Security Database. The Security Database is further expanded, showing Control, CTI Users, Devices, Device Groups, and Tlinks, which is highlighted with a red box. The main content area is titled "Tlinks" and contains a "Tlink Name" field with two radio button options: "AVAYA#CM63VMPG#CSTA#AES63VMPG" (selected) and "AVAYA#CM63VMPG#CSTA-S#AES63VMPG". A "Delete Tlink" button is also present.

6.5. Enable TSAPI and DMCC Ports

To ensure that TSAPI and DMCC ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.1**. ContactPro uses TSAPI functions, but it uses the TSAPI functions via a connection through the DMCC ports. This makes it possible NOT to install the TSAPI Client on the client computer.

AVAYA Application Enablement Services Management Console

Last login: Thu Nov 27 13:26:42 2014 from 10.10.10.10
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.10.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.2.3.1.10-0
Server Date and Time: Mon Dec 01 18:06:19 GMT 2014
HA Status: Not Configured

Networking | Ports Home | Help | Logout

Ports

CVLAN Ports

Unencrypted TCP Port	9999	Enabled Disabled
Encrypted TCP Port	9998	Enabled Disabled

DIG Port

TCP Port	5678
----------	------

TSAPI Ports

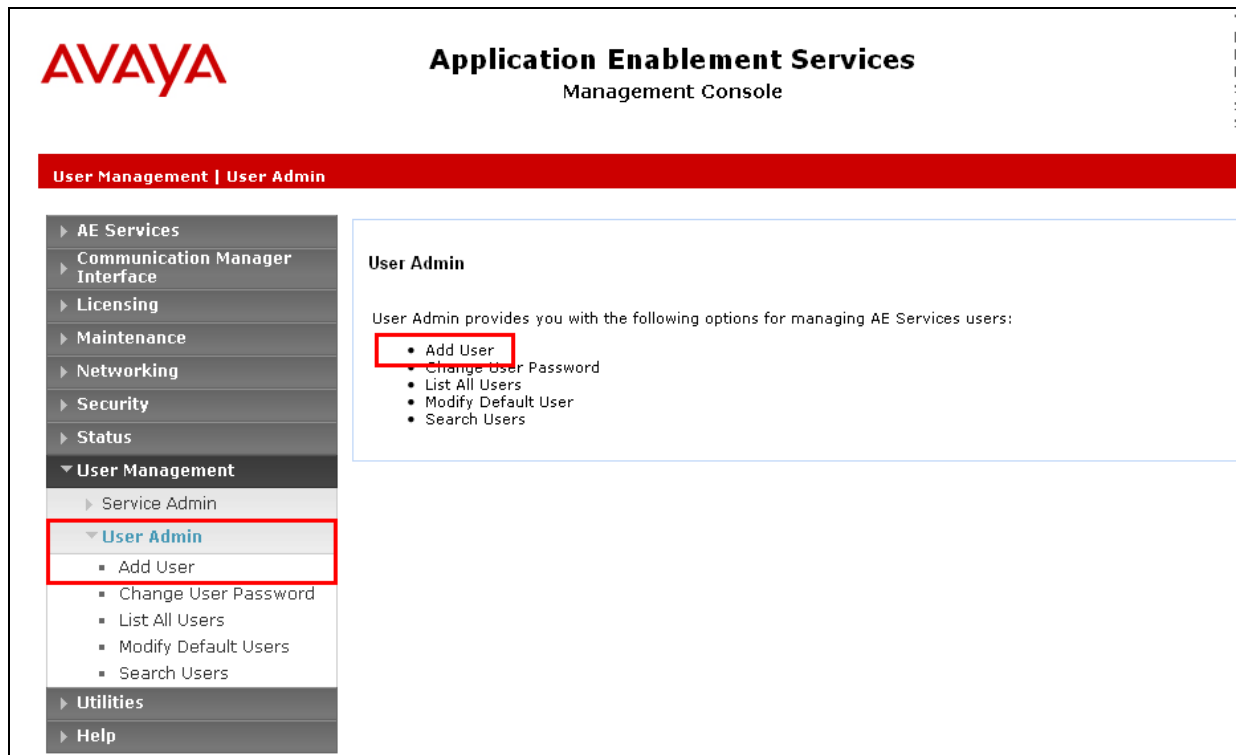
TSAPI Service Port	450	Enabled Disabled
Local TLINK Ports		
TCP Port Min	1024	
TCP Port Max	1039	
Unencrypted TLINK Ports		
TCP Port Min	1050	
TCP Port Max	1065	
Encrypted TLINK Ports		
TCP Port Min	1066	
TCP Port Max	1081	

DMCC Server Ports

Unencrypted Port	4721	Enabled Disabled
Encrypted Port	4722	Enabled Disabled
TIV/87 Port	4723	Enabled Disabled

6.6. Create CTI User

A User ID and password needs to be configured for ContactPro to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the ContactPro setup in **Section 7.1**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **PrimaryAESLogin&Password** in **Section 7.1**.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen (not shown).

AVAYA Application Enablement Services Management Console

Welcome: user call
Last login: Tue Jan 13 13:42:04 2015 from 10.10.40.222
Number of prior failed login attempts: 0
HostName/IP: A6563vMPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1-101-0
Server Date and Time: Fri Jan 16 14:20:00 GMT 2015
RA Status: Not Configured

User Management | User Admin | List All Users

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Service Admin
User Admin
Add User
Change User Password
List All Users
Modify Default Users
Search Users
Utilities
Help

Edit User

* User Id CCT
* Common Name CCT
* Surname CCT

User Password
Confirm Password
Admin Note
Avaya Role None
Business Category
Car License
CH Home
Csa Home
CT User Yes
Department Number
Display Name
Employee Number
Employee Type

The next screen will show a message indicating that the user was created successfully (not shown).

6.7. Change Security setting for CTI User

In the left window navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. From the main window select the **CCT** user and click on **Edit**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'Security' expanded, showing 'Security Database' and 'CTI Users'. The 'List All Users' link is highlighted. The main content area displays a table of CTI Users. The 'CCT' user is selected, and the 'Edit' button is visible below the table.

User ID	Common Name	Worktop Name	Device ID
asc	asc	NONE	NONE
CCT	CCT	NONE	NONE
cube	cube	NONE	NONE
emc	emc	NONE	NONE
imperium	imperium	NONE	NONE
jacada	jacada	NONE	NONE
nice	nice	NONE	NONE
presence	presence	NONE	NONE

Tick the box **Unrestricted Access** to allow this user access to all devices on Communication Manager. If this is not required then a list of devices to be allocated to this user will need to be setup and the procedure for achieving this can be found in the following document listed in **Section 10 Avaya Aura® Application Enablement Services Administration and Maintenance Guide**. Click on **Apply Changes** to complete the setup.

The screenshot shows the 'Edit CTI User' page for the 'CCT' user. The 'Unrestricted Access' checkbox is checked. The 'Apply Changes' button is highlighted.

User Profile	User ID	Common Name	Worktop Name	Unrestricted Access
	CCT	CCT	NONE	<input checked="" type="checkbox"/>

Call and Device Control	Call Origination/Termination and Device Status	None
Call and Device Monitoring <td>Device Monitoring</td> <td>None</td>	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	
Routing Control <td>Allow Routing on Listed Devices</td> <td>None</td>	Allow Routing on Listed Devices	None

7. Configure CCT ContactPro Server

Please note that the installation and configuration of CCT ContactPro Server was performed solely by the CCT engineer and is therefore outside the scope of these Application Notes. The installation of Microsoft SQL 2012 was installed as default using the default database. However the installation and the creation of the database specific to ContactPro were achieved by the running of two database scripts provided by CCT.

Once the database scripts are run and the necessary tables are in place, these tables can then be accessed and changed in order to facilitate the connection to the AES. The following section outlines this process showing the tables that need to be accessed in order to input the following information.

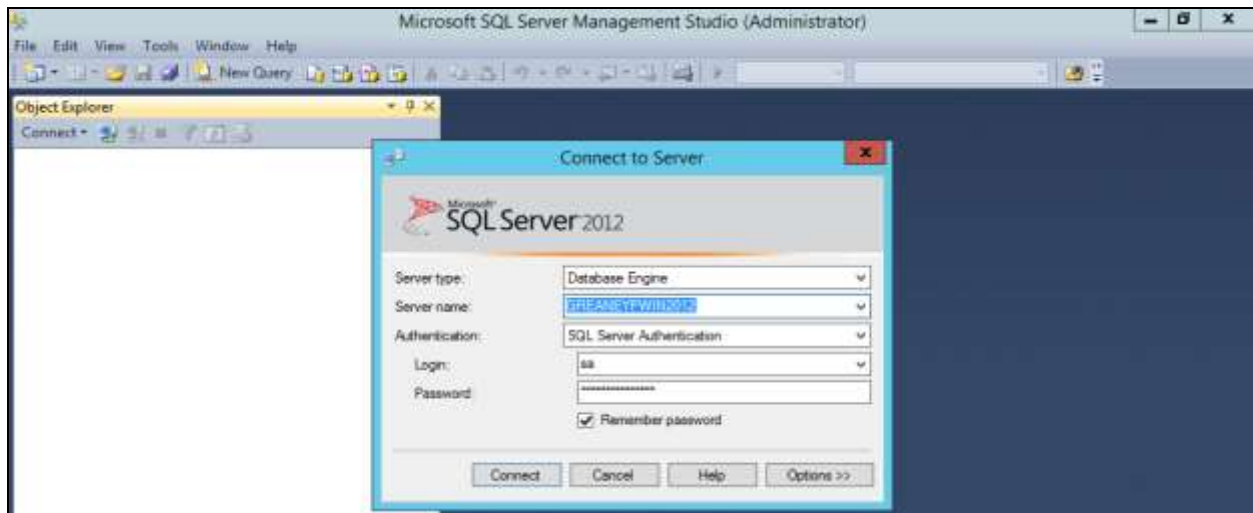
- Primary AES Secure Socket
- Primary AES IP Address
- Primary AES Port
- Primary AES Communication Manager Connection Name
- Primary AES Login Name
- Primary AES Login Password

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

From the Windows 2012 Server running ContactPro open **SQL Server Management Studio**. This will allow access to the database and allow changes to certain tables' specific to the connection to AES.

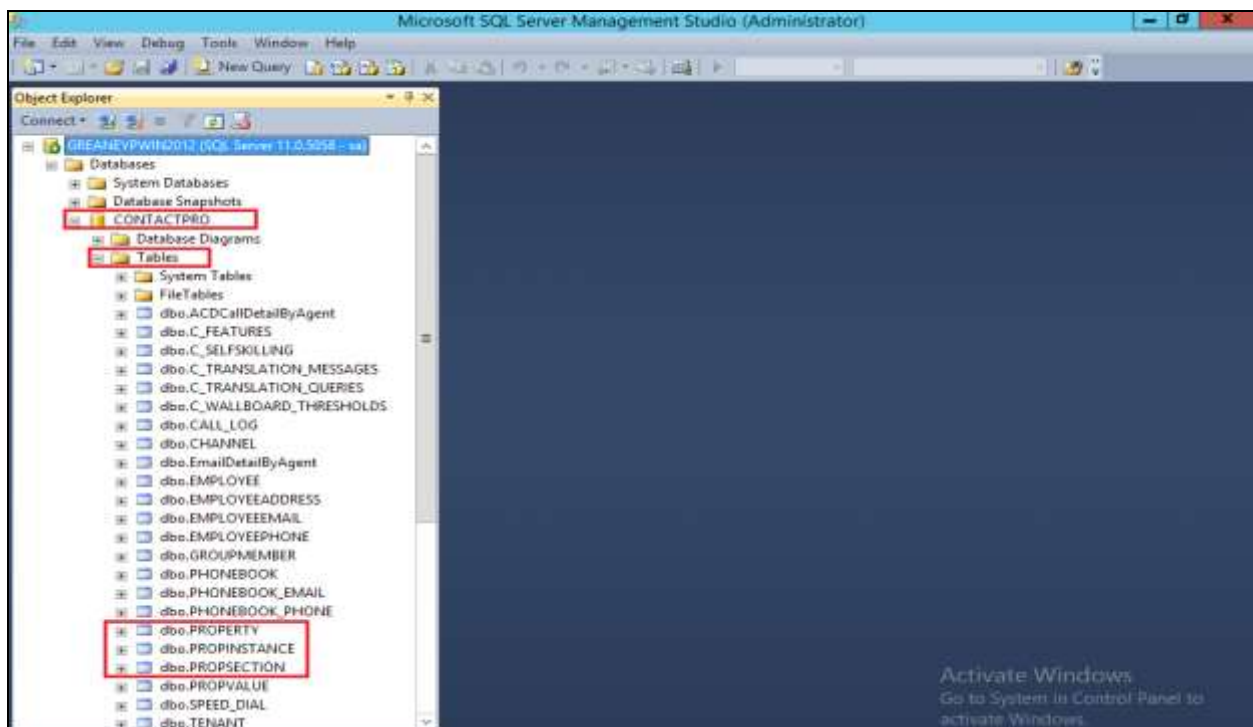


Once the **SQL Server Management Studio** is opened enter the correct credentials (these would be known to the CCT engineer who setup the SQL server) for the **Server type**, **Server Name** and the **Login** details and click on **Connect**.

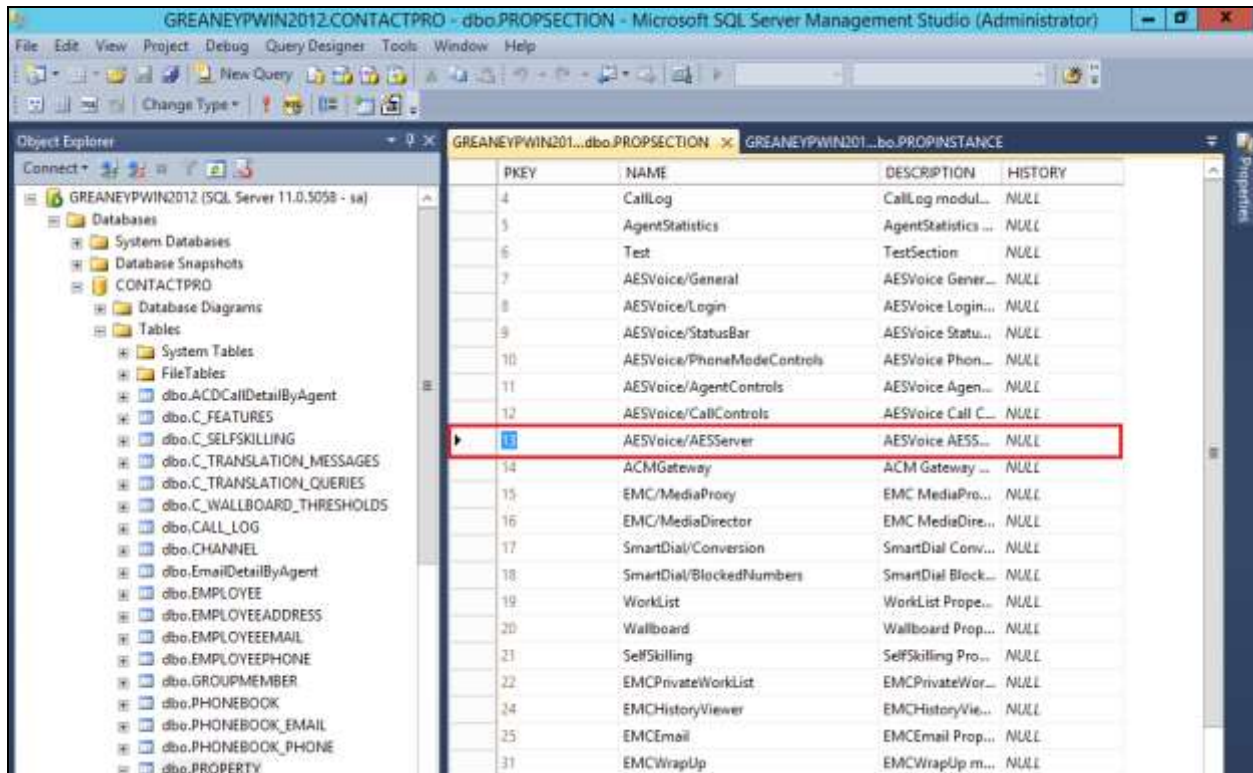


Once logged in correctly, expand the **Database** called **CONTACTPRO** and then open **Tables**. The three tables that need to be opened are.

- **PROPERTY**
- **PROPINSTANCE**
- **PROPSECTION**



Open the table **PROPSECTION** and note the **PKEY** number for **AESVoice/AESServer**.



The screenshot shows the Microsoft SQL Server Management Studio interface. The Object Explorer on the left displays the database structure for GREANEYPWIN2012 (SQL Server 11.0.5058 - sa). The main window shows the table structure for GREANEYPWIN2012.dbo.PROPSECTION. The table has four columns: PKEY, NAME, DESCRIPTION, and HISTORY. The row for PKEY 13, named 'AESVoice/AESServer', is highlighted with a red box.

PKEY	NAME	DESCRIPTION	HISTORY
4	CallLog	CallLog modul...	NULL
5	AgentStatistics	AgentStatistics ...	NULL
6	Test	TestSection	NULL
7	AESVoice/General	AESVoice Gener...	NULL
8	AESVoice/Login	AESVoice Login...	NULL
9	AESVoice/StatusBar	AESVoice Statu...	NULL
10	AESVoice/PhoneModeControls	AESVoice Phon...	NULL
11	AESVoice/AgentControls	AESVoice Agen...	NULL
12	AESVoice/CallControls	AESVoice Call C...	NULL
13	AESVoice/AESServer	AESVoice AES5...	NULL
14	ACMGateway	ACM Gateway ...	NULL
15	EMC/MediaProxy	EMC MediaPro...	NULL
16	EMC/MediaDirector	EMC MediaDire...	NULL
17	SmartDial/Conversion	SmartDial Conv...	NULL
18	SmartDial/BlockedNumbers	SmartDial Block...	NULL
19	WorkList	WorkList Prop...	NULL
20	Wallboard	Wallboard Prop...	NULL
21	SelfSkilling	SelfSkilling Pro...	NULL
22	EMCPrivateWorkList	EMCPrivateWor...	NULL
24	EMCHistoryViewer	EMCHistoryVie...	NULL
25	EMCEmail	EMCEmail Prop...	NULL
31	EMCWrapUp	EMCWrapUp m...	NULL

Having noted that the PKEY for AESVoice/AESServer is **13** in this example, open the table called **PROPERTY** and look for the corresponding number in the **PROPSECTION** column. Take note of the **PKEYS** for the following.

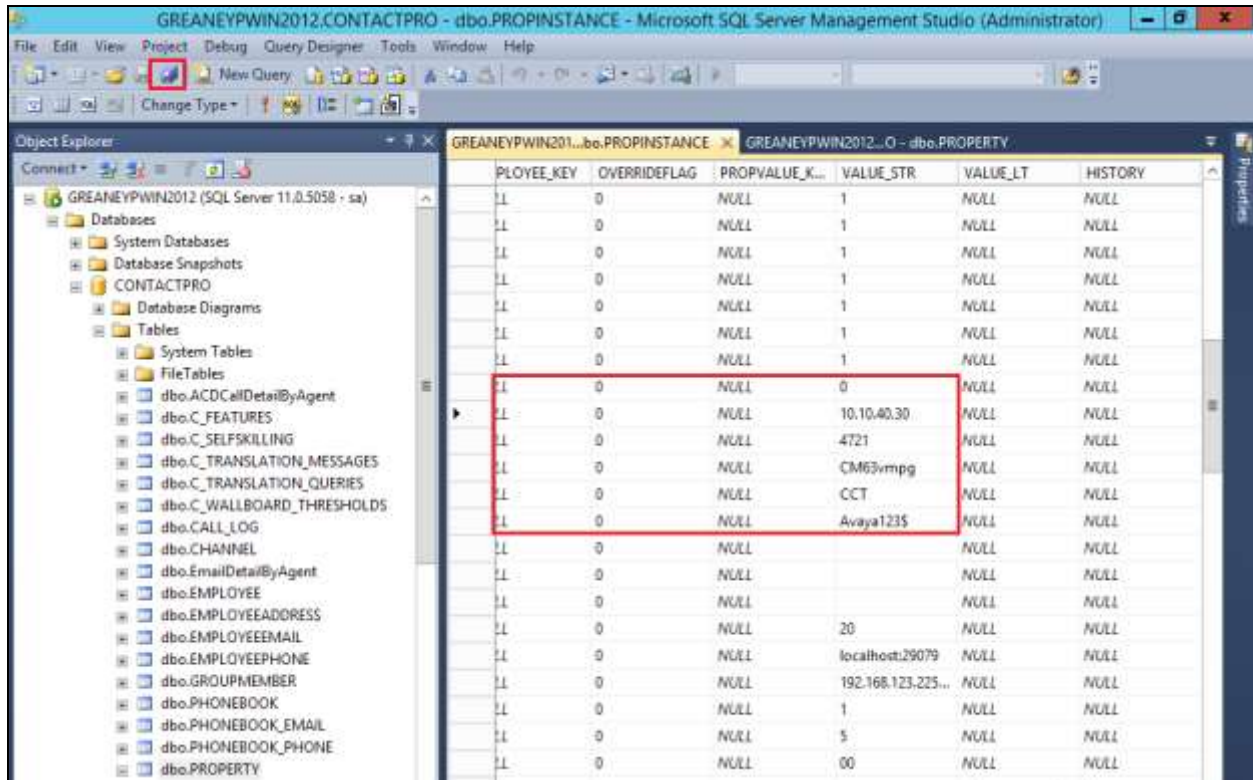
- **PrimaryAESSecureSocket**
- **PrimaryAESIPAddress**
- **PrimaryAESPort**
- **PrimaryAESCMConnectionName**
- **PrimaryAESLoginName**
- **PrimaryAESLoginPassword**

PKEY	PROPSECTION	NAME	DESCRIPTION	REC
40	12	AnswerCallButtonVisible	NULL	0
41	12	MakeCallButtonVisible	NULL	0
42	12	EndCallButtonVisible	NULL	0
43	12	HoldCallButtonVisible	NULL	0
44	12	TransferCallButtonVisible	NULL	0
45	12	ConferenceCallButtonVisible	NULL	0
46	13	PrimaryAESSecureSocket	To use the secu...	0
47	13	PrimaryAESIPAddress	The IP Address ...	0
48	13	PrimaryAESPort	The IP Port of t...	0
49	16	PrimaryAESACMConnectionName	If there is only ...	0
50	13	PrimaryAESLoginUsername	Login name to ...	0
51	13	PrimaryAESLoginPassword	Login password...	0
52	13	SecondaryAESSecureSocket	To use the secu...	0
53	13	SecondaryAESIPAddress	The IP Address ...	0
54	13	SecondaryAESPort	The IP Port of t...	0
55	13	SecondaryAESACMConnectionName	If there is only ...	0
56	13	SecondaryAESLoginUsername	Login name to ...	0
57	13	SecondaryAESLoginPassword	Login password...	0

Open the table called **PROPINSTANCE** and there note the **PKEYS** from above **46 – 51** in the **PROPERTY_KEY** column, then scroll right to see the values.

PKEY	PROPERTY_KEY	INSTANCELEVEL	TENANT_KEY	WORKGROUP	EMPLOYEE_KEY
58	40	0	NULL	NULL	NULL
59	41	0	NULL	NULL	NULL
60	42	0	NULL	NULL	NULL
61	43	0	NULL	NULL	NULL
62	44	0	NULL	NULL	NULL
63	45	0	NULL	NULL	NULL
64	46	0	NULL	NULL	NULL
65	47	0	NULL	NULL	NULL
66	48	0	NULL	NULL	NULL
67	49	0	NULL	NULL	NULL
68	50	0	NULL	NULL	NULL
69	51	0	NULL	NULL	NULL
70	52	0	NULL	NULL	NULL
71	53	0	NULL	NULL	NULL
72	54	0	NULL	NULL	NULL
73	55	0	NULL	NULL	NULL
74	56	0	NULL	NULL	NULL
75	57	0	NULL	NULL	NULL
76	58	0	NULL	NULL	NULL
77	59	0	NULL	NULL	NULL
78	60	0	NULL	NULL	NULL
79	61	0	NULL	NULL	NULL
80	62	0	NULL	NULL	NULL

The property key values must be changed in order to connect to AES. The values for the following are shown in the **VALUE_STR** column and can be changed by simply clicking on the value itself and changing it to suit the setup required. Once the changes below are made click on the **Save All** icon highlighted at the top of the screen or go to **File → Save All** (not shown).

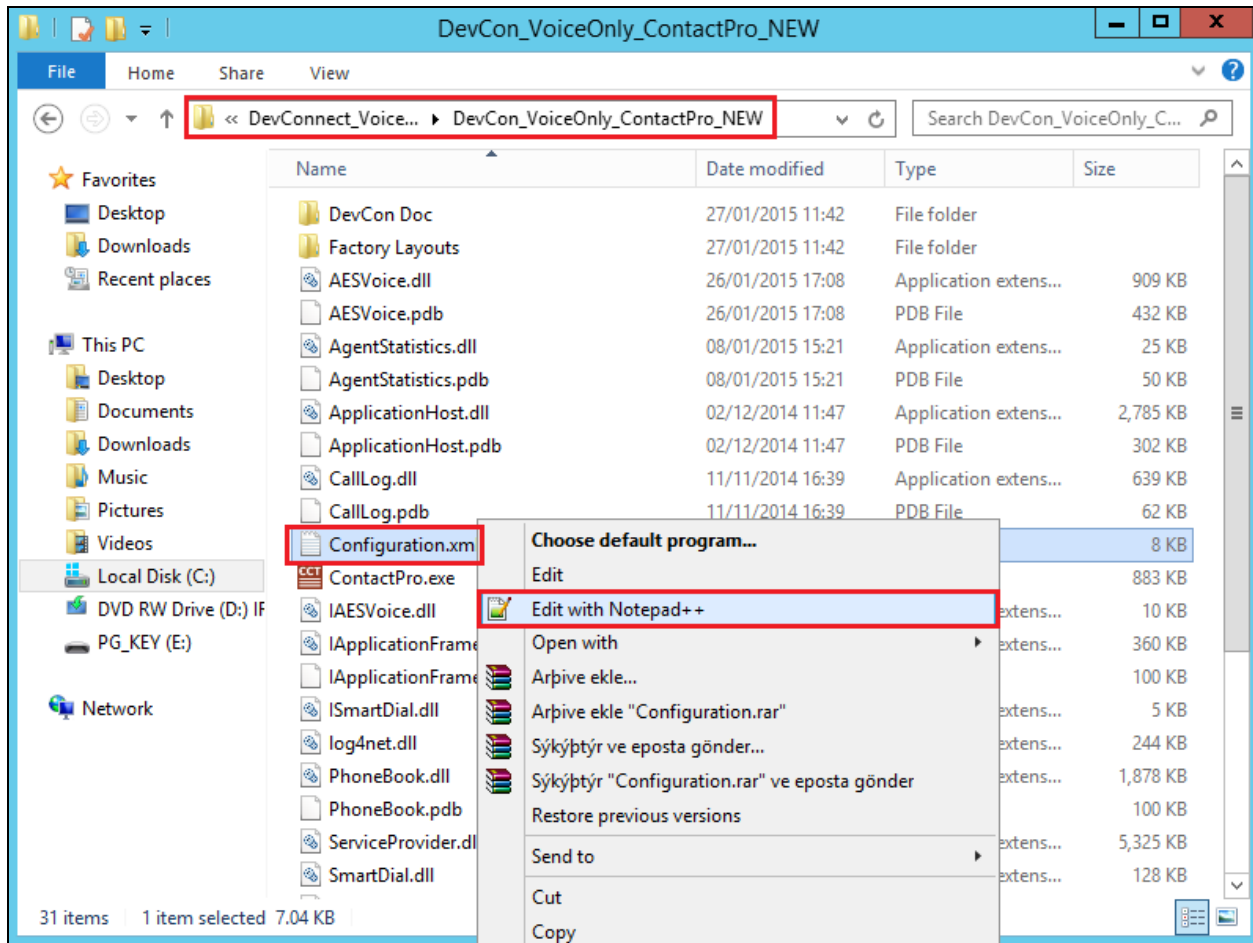


PLOYEE_KEY	OVERRIDEFLAG	PROPVALUE_K...	VALUE_STR	VALUE_LT	HISTORY
11	0	NULL	1	NULL	NULL
11	0	NULL	1	NULL	NULL
11	0	NULL	1	NULL	NULL
11	0	NULL	1	NULL	NULL
11	0	NULL	1	NULL	NULL
11	0	NULL	1	NULL	NULL
11	0	NULL	0	NULL	NULL
11	0	NULL	10.10.40.30	NULL	NULL
11	0	NULL	4721	NULL	NULL
11	0	NULL	CM63vmpg	NULL	NULL
11	0	NULL	CCT	NULL	NULL
11	0	NULL	Avaya123\$	NULL	NULL
11	0	NULL		NULL	NULL
11	0	NULL		NULL	NULL
11	0	NULL		NULL	NULL
11	0	NULL	20	NULL	NULL
11	0	NULL	localhost:29079	NULL	NULL
11	0	NULL	192.168.123.225...	NULL	NULL
11	0	NULL	1	NULL	NULL
11	0	NULL	5	NULL	NULL
11	0	NULL	00	NULL	NULL

7.2. CCT ContactPro Client connection to the database

Each client installation of ContactPro will need to be configured in order to connect to the database on the ContactPro Server. This will allow each client access to information regarding the AES connection and other services provided by ContactPro such as contacts information.

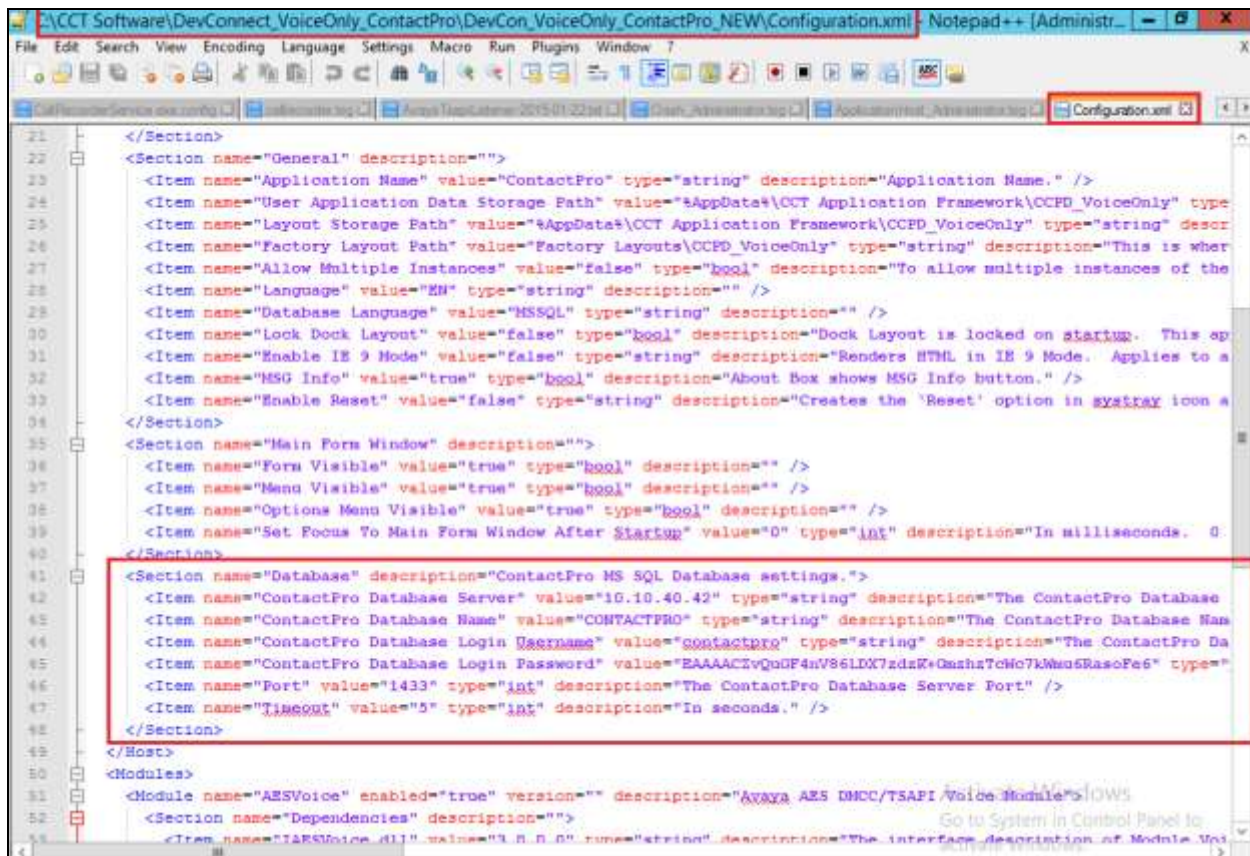
Navigate to the folder where the ContactPro has been installed. Right click on the file called **Configuration.xml** and open this with a program such as Notepad or **Notepad ++** as is shown below.



Once this file is opened navigate to the section regarding the **ContactPro MS SQL Database settings**. Here the following must be entered correctly. This information is known to the CCT engineer.

- **ContactPro Database Servers IP Address**
- **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)).



```
<?xml version="1.0" encoding="utf-8" ?>
<Section name="General" description="">
  <Item name="Application Name" value="ContactPro" type="string" description="Application Name." />
  <Item name="User Application Data Storage Path" value="%AppData%\CCT Application Framework\CCPD_VoiceOnly" type="string" description="User Application Data Storage Path." />
  <Item name="Layout Storage Path" value="%AppData%\CCT Application Framework\CCPD_VoiceOnly" type="string" description="Layout Storage Path." />
  <Item name="Factory Layout Path" value="Factory Layouts\CCPD_VoiceOnly" type="string" description="This is where the factory layout files are stored." />
  <Item name="Allow Multiple Instances" value="false" type="bool" description="To allow multiple instances of the application." />
  <Item name="Language" value="EN" type="string" description="" />
  <Item name="Database Language" value="MSSQL" type="string" description="" />
  <Item name="Lock Dock Layout" value="false" type="bool" description="Dock Layout is locked on startup. This option applies to the dock layout." />
  <Item name="Enable IE 9 Mode" value="false" type="string" description="Renders HTML in IE 9 Mode. Applies to a web browser." />
  <Item name="MSG Info" value="true" type="bool" description="About Box shows MSG Info button." />
  <Item name="Enable Reset" value="false" type="string" description="Creates the 'Reset' option in system tray icon." />
</Section>
<Section name="Main Form Window" description="">
  <Item name="Form Visible" value="true" type="bool" description="" />
  <Item name="Menu Visible" value="true" type="bool" description="" />
  <Item name="Options Menu Visible" value="true" type="bool" description="" />
  <Item name="Set Focus To Main Form Window After Startup" value="0" type="int" description="In milliseconds. 0 means no delay." />
</Section>
<Section name="Database" description="ContactPro MS SQL Database settings.">
  <Item name="ContactPro Database Server" value="10.10.40.42" type="string" description="The ContactPro Database Server IP Address." />
  <Item name="ContactPro Database Name" value="CONTACTPRO" type="string" description="The ContactPro Database Name." />
  <Item name="ContactPro Database Login Username" value="contactpro" type="string" description="The ContactPro Database Login Username." />
  <Item name="ContactPro Database Login Password" value="EAAAACivQoGF4nV86LDX7zdzK+Qasha7cWo7kWuo6RasoFe6" type="string" description="The ContactPro Database Login Password." />
  <Item name="Port" value="1433" type="int" description="The ContactPro Database Server Port." />
  <Item name="Timeout" value="5" type="int" description="In seconds." />
</Section>
</Host>
<Modules>
  <Module name="AESVoice" enabled="true" version="" description="Avaya AES DMCC/TSAPI Voice Module">
    <Section name="Dependencies" description="">
      <Item name="TARSVoice.dll" value="3.0.0.0" type="string" description="The interface description of Module Voice." />
    </Section>
  </Module>
</Modules>
```

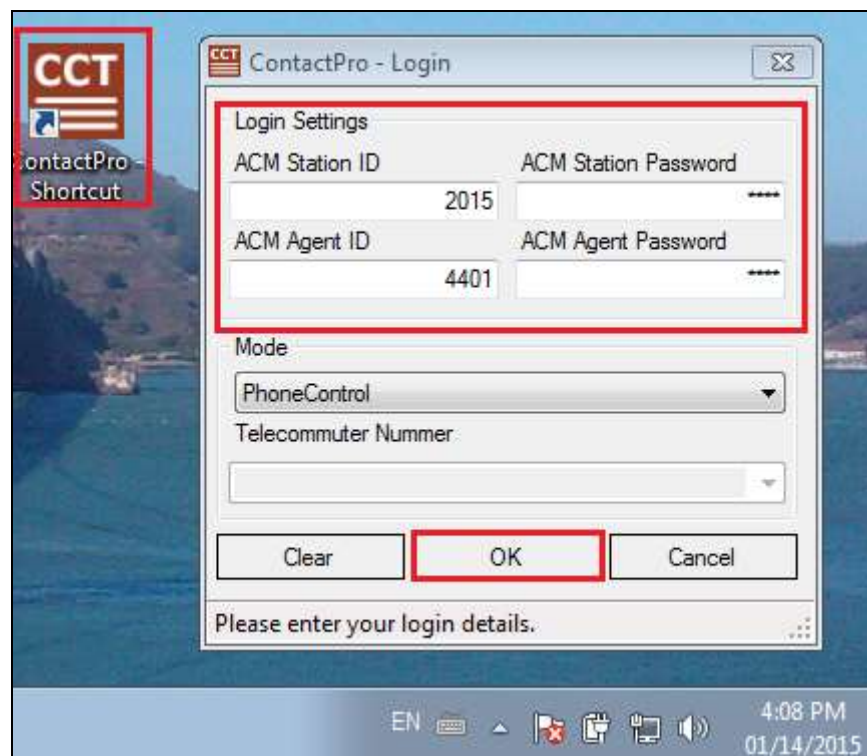
8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of AES and CCT ContactPro.

8.1. Verify login of ContactPro

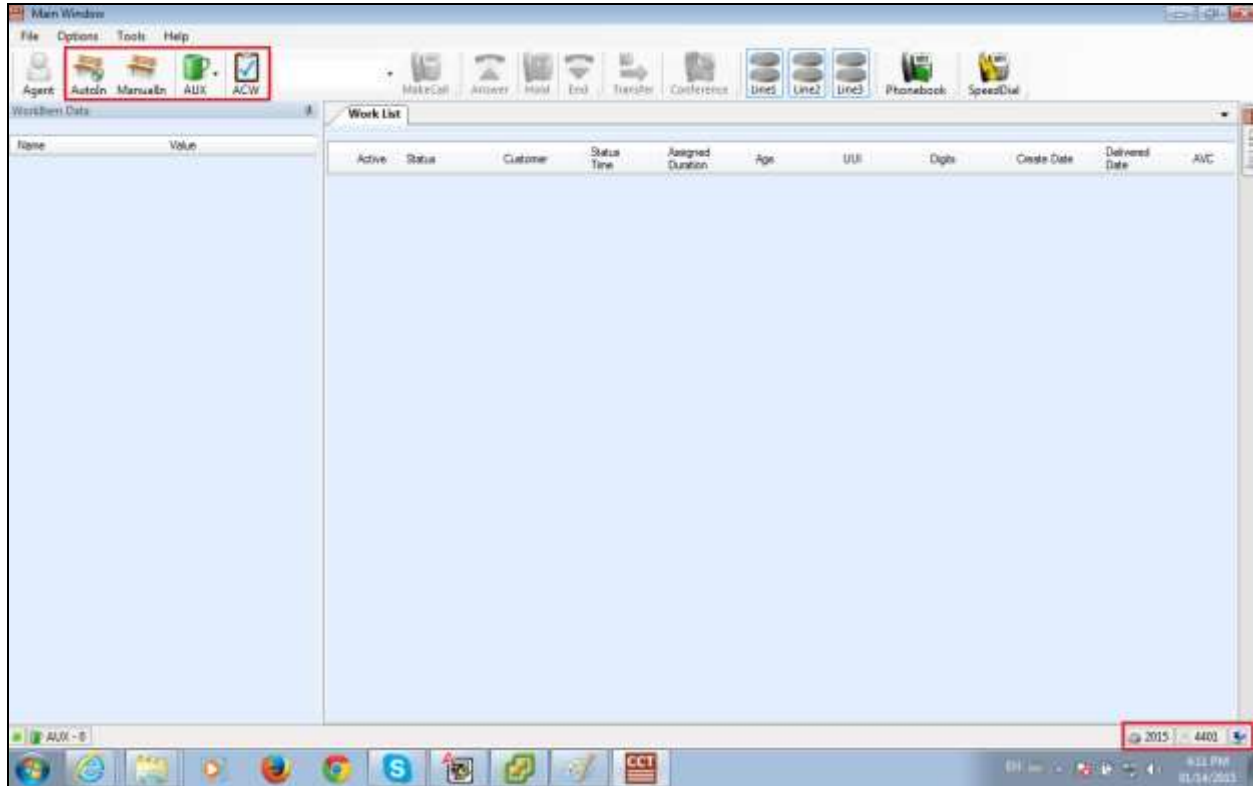
From the Client PC open the application **ContactPro** (shortcut is shown below). Once this is opened fill in the following details:

- **ACM Station ID** This is the station number that is to be controlled by this Contact Pro application. This station number is noted in **Section 5.9**.
- **ACM Station Password** This is the password for the station that is to be controlled this is the same password noted in **Section 5.9**.
- **ACM Agent ID** This is the Agent ID created or noted in **Section 5.8**.
- **ACM Agent Password** This is the password of the agent noted or created in **Section 5.8**.



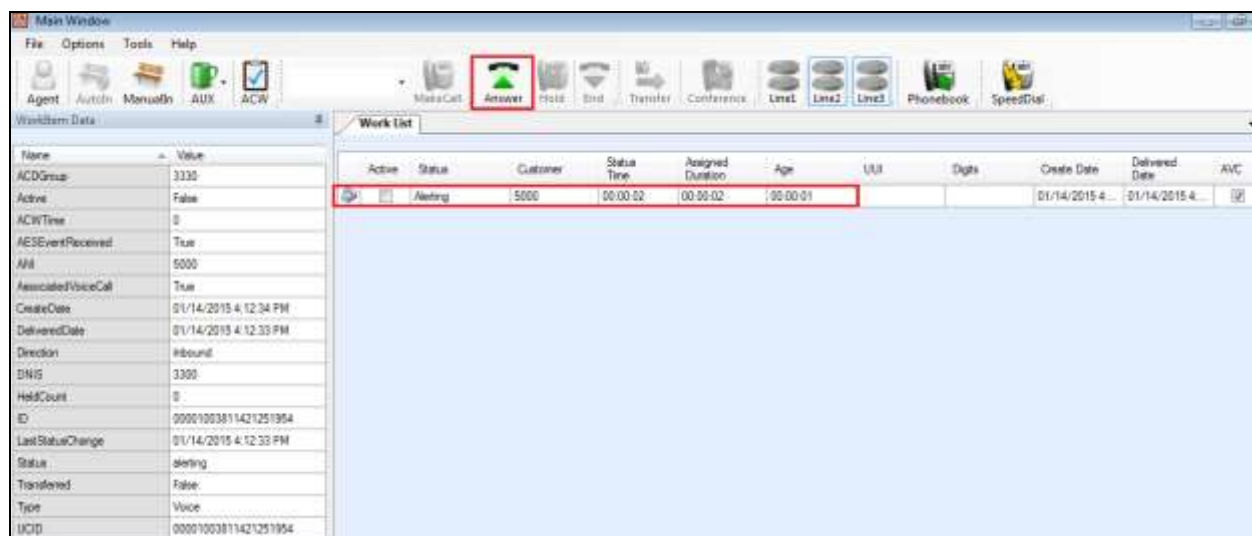
8.2. Verify Agent Status using ContactPro

Once logged in the agent state can be changed using the buttons at the top left highlighted below. Note also the station number (**2015**) and Agent ID (**4401**) once logged in.

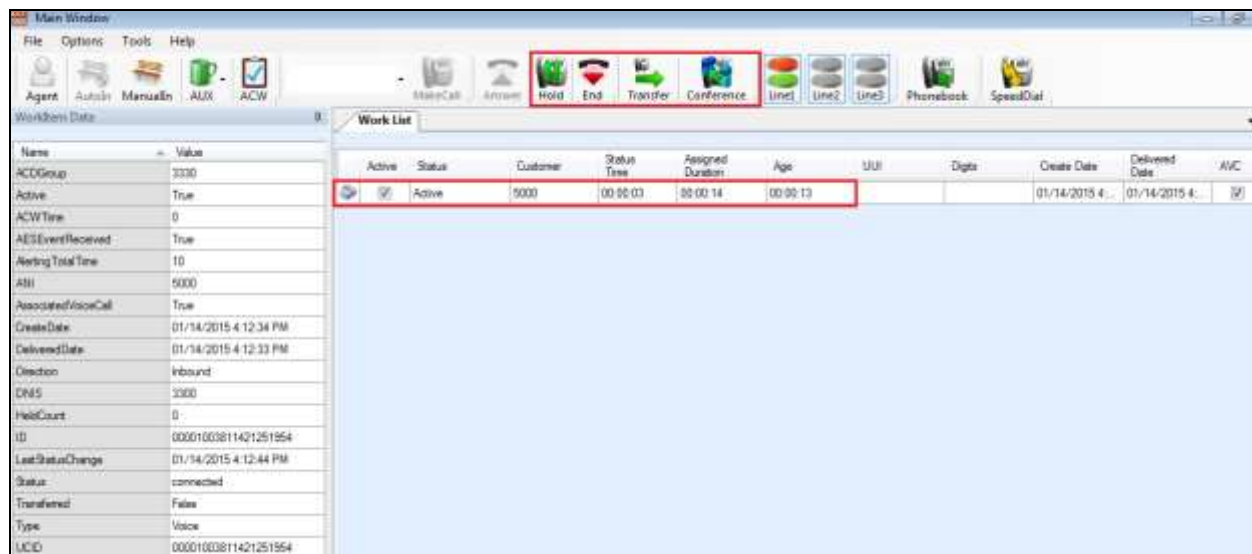


8.3. Verify Successful Operation of CCT ContactPro Agent to answer VDN calls

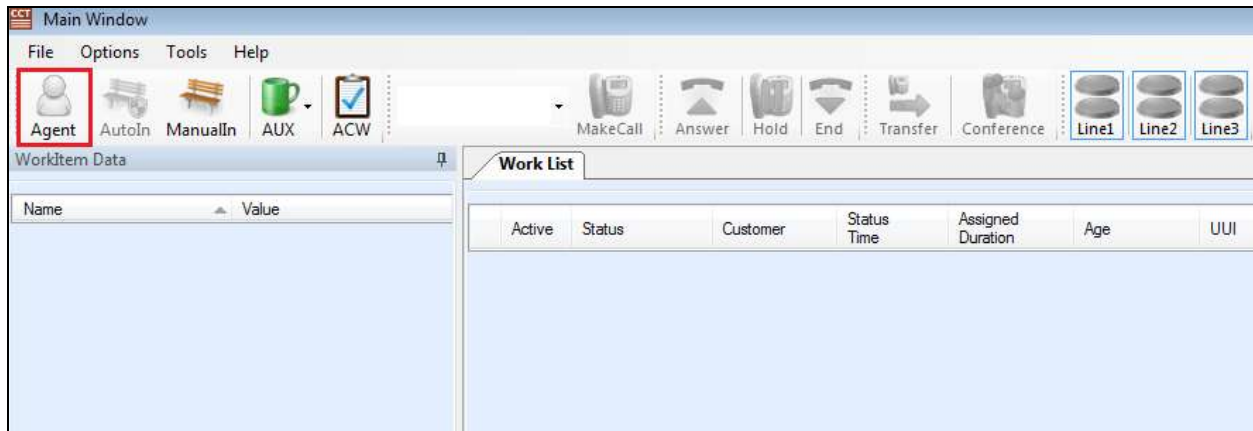
A call is made into a VDN from PSTN number **5000**. The screen should show a **Status** of **Alerting**. The call can be answered by pressing the **Answer** icon, highlighted below.



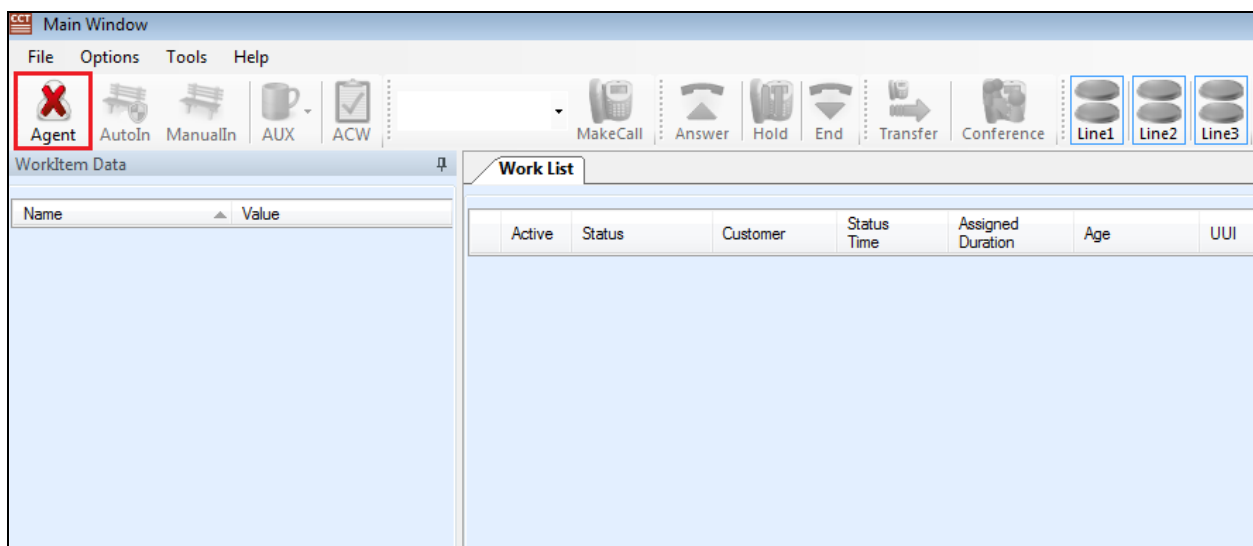
Once the call is answered, the **Status** will show as **Active** and the icons highlighted below become active for such operations as **Hold**, **Transfer** and **Conference**.



To log out the agent click on the **Agent** icon, highlighted.



Once logged out the **Agent** icon will show up as the following highlighted below and to log back in again once again click on the **Agent** icon highlighted.



8.4. Verify Status of Communication Manager Agent

Enter the command **list agent-loginID** verify that agent **4401** shown in **Section 5.8** is logged-in to extension **1004**.

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
4400	Patrick	unstaffed						1	lvl
	33/01	34/01	/	/	/	/	/	/	/
4401	Agent 1	1004						1	lvl
	33/01	34/01	/	/	/	/	/	/	/
4402	Agent 2	unstaffed						1	lvl
	33/01	34/01	/	/	/	/	/	/	/
4404	Paul	unstaffed						1	lvl
	900/01	910/01	920/01	930/01	901/01	911/01	921/01	931/01	
4405	Russell	unstaffed						1	lvl
	900/01	910/01	920/01	930/01	/	/	/	/	/
4406	Dave	unstaffed						1	lvl
	901/01	911/01	921/01	931/01	/	/	/	/	/

Enter the command **status station 1004** and on **Page 7** verify that the agent is logged-in to the appropriate skills and in the **AI** mode, which represents the Auto In button being pressed, highlighted in **Section 8.2**.

status station 1004							Page 7 of 7
ACD STATUS							
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	
33/AI	/	/	/	/	/	/	On ACD Call? no
34/AI	/	/	/	/	/	/	
/	/	/	/	/	/	/	Occupancy: 73.3
/	/	/	/	/	/	/	

9. Conclusion

These Application Notes describe the configuration steps required for ContactPro from CCT Software to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed successfully, with any observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and CCT 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*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 6.3*

The following CCT documentation can be obtained using the contact information detailed in **Section 2.3**.

- CCT ContactPro Implementation Guide.
- CCT ContactPro Installation Guide.
- CCT ContactPro User Guide.
- CCT ContactPro Technical Specification.
- CCT ContactPro Test Specification.
- CCT ContactPro Port Ranges.

Appendix

Avaya 9641 SIP Deskphone

This is a printout of the Avaya 9641 SIP deskphone used during compliance testing.

Page 1

display station 1004	Page 1 of 6	
STATION		
Extension: 1004	Lock Messages? n	BCC: 0
Type: 9641SIPCC	Security Code:	TN: 1
Port: S00057	Coverage Path 1:	COR: 1
Name: EliteCC, Agent4	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Message Lamp Ext: 1004	
Display Language: english	Button Modules: 0	
Survivable COR: internal	IP SoftPhone? n	
Survivable Trunk Dest? y	IP Video? n	

Page 2

display station 1004	Page 2 of 6	
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Coverage Msg Retrieval? y	
LWC Activation? y	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Per Button Ring Control? n	Idle Appearance Preference? n	
Bridged Call Alerting? n	Bridged Idle Line Preference? n	
Active Station Ringing: single	Restrict Last Appearance? y	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
MWI Served User Type:	Coverage After Forwarding? s	
AUDIX Name:	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 1004	Always Use? n IP Audio Hairpinning? n	

Page 3

display station 1004	STATION	Page 3 of 6
Bridged Appearance Origination Restriction? n		
IP Phone Group ID:		
ENHANCED CALL FORWARDING		
	Forwarded Destination	Active
Unconditional For Internal Calls To:		n
External Calls To:		n
Busy For Internal Calls To:		n
External Calls To:		n
No Reply For Internal Calls To:		n
External Calls To:		n

Page 4

display station 1004	STATION	Page 4 of 6
SITE DATA		
Room:	Headset?	n
Jack:	Speaker?	n
Cable:	Mounting:	d
Floor:	Cord Length:	0
Building:	Set Color:	
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5: aux-work	RC: Grp:
2: call-appr	6: auto-in	Grp:
3: call-appr	7: manual-in	Grp:
4: agnt-login	8: work-code	

©2015 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.