



Avaya Solution & Interoperability Test Lab

Application Notes for configuring CCT ContactPro V5 from CCT Deutschland GmbH with Avaya Aura® Application Enablement Services R7.1 and Avaya Aura® Call Center Elite Multichannel R6.5 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CCT ContactPro to interoperate with Avaya Aura® Application Enablement Services and Avaya Aura® Call Center Elite Multichannel. CCT ContactPro is an interaction management application that can connect to both Avaya Aura® Application Enablement Services and Avaya Aura® Call Center Elite Multichannel.

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 CCT ContactPro V5 from CCT Deutschland GmbH, to interoperate with Avaya Aura® Application Enablement Services (AES) R7.1 and Avaya Aura® Call Center Elite Multichannel R6.5. CCT ContactPro solutions offer a variety of integrations into the Avaya call center environment supporting different Avaya platforms, to interact for multimedia agents as well as for voice only agents.

Note: CCT Contact Pro connects to Avaya Aura® Application Enablement Services allowing for basic call control for voice-only calls. For the setup and configuration of this solution, please refer to **Sections 5, 6, and 8**.

Note: CCT Contact Pro offers an add-on module which allows for multimedia calls by connecting to Avaya Aura® Call Center Elite Multichannel. For the setup and configuration of this add-on module please refer to the extra **Sections 7, 8.2.2 and 8.2.3**.

CCT ContactPro is a solution for agent desktops in an Avaya call center environment focused on voice and multimedia, such as email and webchat. CCT ContactPro can be installed with enabled Presence Services and integrated Customer Data and empowers agents to efficiently serve customers by allowing the agents have full call control from the agents screen. CCT 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 desk phones Avaya Aura® Call Center Elite Multichannel agents are logged into.

CCT ContactPro offers a multi-channel agent desktop replacement for the current Avaya Aura® Call Center Elite Multichannel client. All Elite Multichannel channels (Voice, Chat and Email) are unified into one convenient desktop that reflects the customer being interacted with and the channel being used.

CCT ContactPro can also connect to Avaya Proactive Outreach Manager for Outbound campaigns in Preview, Progressive or Predictive modes.

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 and/or outbound from the elite call center using CCT ContactPro to answer calls. Where applicable, agent actions were performed using both the physical phone and CCT ContactPro Agent client in synchronisation.

CCT ContactPro can be used to answer and respond to Voice, Email and Webchat requests from “customers”. Test cases are selected to exercise a sufficiently broad segment of functionality to have a reasonable expectation of interoperability in production configurations.

CCT ContactPro software was installed on each client PC utilised by an agent. A configuration file on this software points to a database that was created on an existing Avaya Aura® Call

Center Elite Multichannel database server, this being a standalone MS SQL server that hosts the Avaya Aura® Call Center Elite Multichannel database.

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.

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

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

For the testing associated with these Application Notes, the interface between Avaya Aura® Call Center Elite Multichannel and CCT ContactPro utilized security features that were available to them by connecting on secure ports to the Avaya Aura® Call Center Elite Multichannel as requested by CCT Deutschland GmbH. All other connections were as default.

2.1. Interoperability Compliance Testing

The testing focuses 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.
- **Multimedia calls** – Email and Webchat.
- **Serviceability Testing** - Verify the ability of CCT ContactPro to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

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

- Upon logging into CCT ContactPro using a valid Communication Manager desk phone, there is no need for any password for the extension even though it asks for one. However, the correct extension password is required when Telecommuter mode is used

during login. **Note:** Telecommuter requires “softphone = y” in the station settings as well as additional licenses, AES DMCC Station License and ACM IP_A Station Licenses.

- Blind Conference is not supported on CCT ContactPro. This is also the standard behaviour of the Avaya EMC Client.
- When an email item is opened from the Agent History the agent goes to active but there is no VDN phantom call present. This is also the standard behaviour of the Avaya EMC Client.

2.3. Support

Support for CCT Deutschland GmbH products can be obtained as follows:

WEBSITE

www.cct-solutions.com

CONTACT

Europe Phone: +49 69 7191 4969 0

U.S. Phone +1 786 738 5253

Email: contact@cct-solutions.com

SUPPORT

Europe Hotline: +49 821 455152 455

U.S. Hotline: +1-305-985-5485

Email: helpdesk@cct-solutions.com

CCT Deutschland GmbH

Voltastrasse 81

60486 Frankfurt am Main

Germany

Phone +49 69 7191 4969 0

Fax +49 69 7191 4969 666

CCT Europe GmbH

Sumpfstrasse 26

6312 Steinhausen

Swiss

Phone. +41 41 748 42 22

Fax +41 41 748 42 23

Street Werner-von-Siemens-Strasse 6

86159 Augsburg

Germany

CCT Software LLC

1735 Market Street **STE** 3750

19103 Philadelphia, PA

USA

Phone: +1 267 507 6196

1801 N.E. 123rd Street, Suite 314

North Miami, 33181 FL

Phone +1 786 738 5253

USA

Office +1 786 738 5253

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test CCT ContactPro with Avaya Elite Multichannel and AES using a CTI connection through AES to gain call control of the Avaya Elite Multichannel agents.

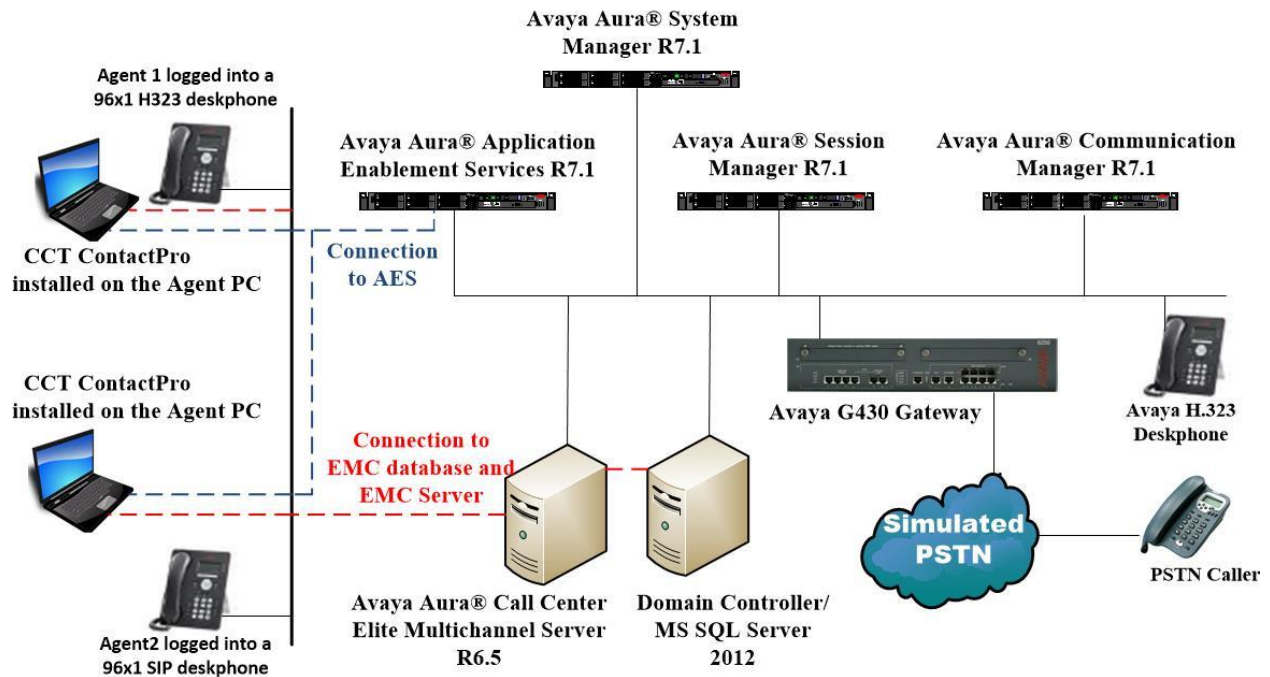


Figure 1: Connection of CCT ContactPro with Avaya Aura® Application Enablement Services R7.1 and Avaya Aura® Call Center Elite Multichannel R6.5

The configuration in **Figure 2** describes a more detailed Voice Only environment for CCT ContactPro.

ContactPro with AES

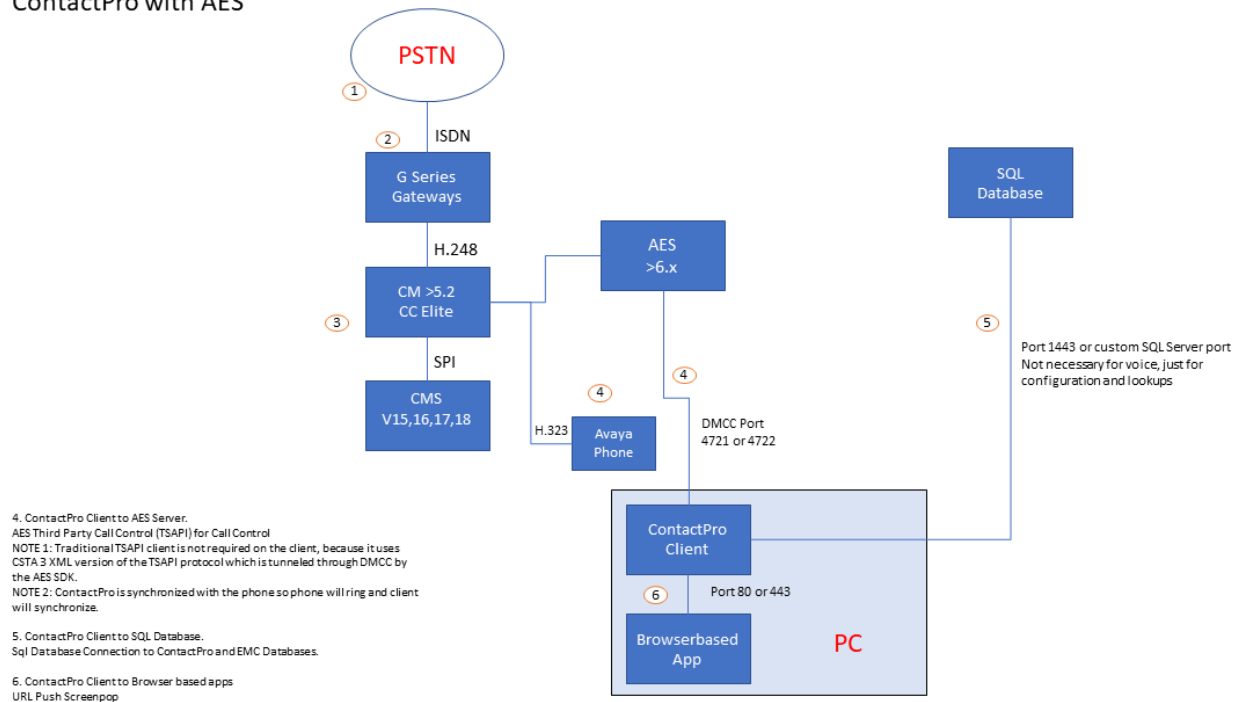


Figure 2: Connection of CCT ContactPro with Other Components in a Voice Only Environment

The configuration in **Figure 3** describes a more detailed EMC Multimedia environment for CCT ContactPro.

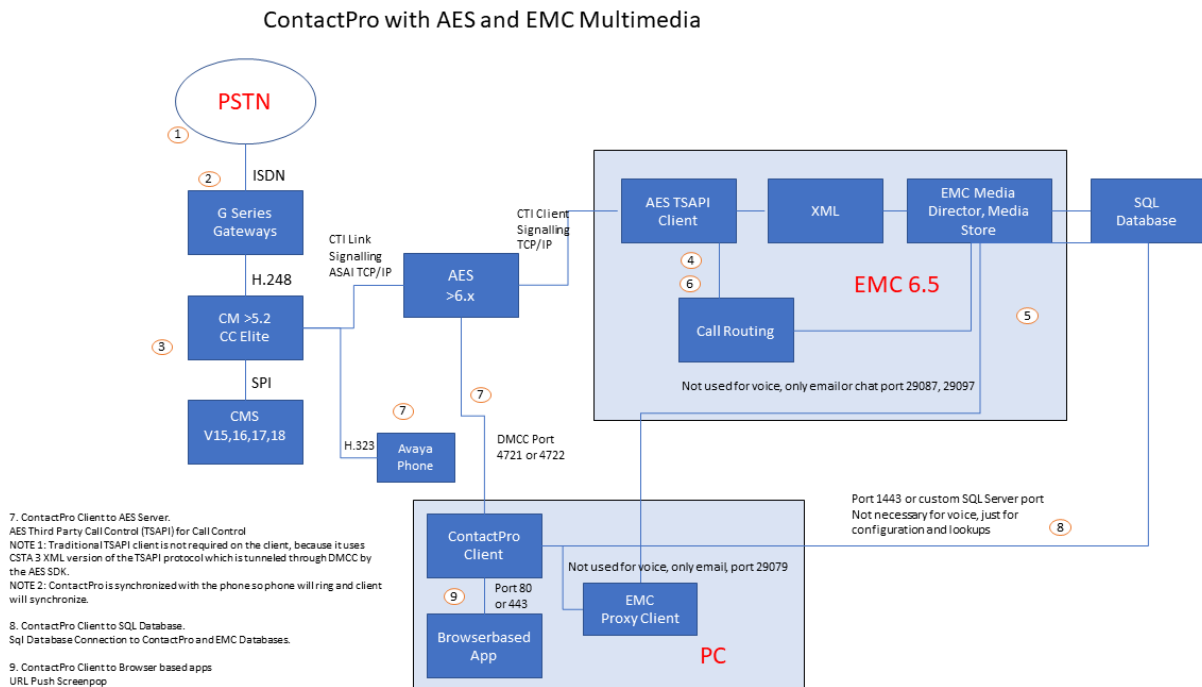


Figure 3: Connection of CCT ContactPro with Other Components in an EMC Multimedia Environment

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 7.1.1.0 Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.1.0.046931 Feature Pack 1 Service Pack 1
Avaya Aura® Session Manager running on a Virtual Server	Session Manager R7.1 SP1 Build No. – 7.1.1.0.711008
Avaya Aura® Communication Manager running on Virtual Server	R017x.01.0.532.0 R7.1.1.0.0 - FP1 Update ID 01.0.532.0-23985
Avaya Aura® Application Enablement Services running on a Virtual Server	R7.1.0.0.0.17-0
Avaya Aura® Call Center Elite Multichannel running on Virtual Server	R6.5.0
Avaya G430 Gateway	37.42.0 /1
Avaya 96x1 H.323 Deskphone	96x1 H.323 Release 6.6401
Avaya 96x1 SIP Deskphone	96x1 SIP Release 7.1.0.1.1
CCT ContactPro - Client Agent Desktop	V5.0.0.790

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 11**.

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

5.1. Configure the Avaya Aura® Communication Manager Connection to Avaya Aura® Application Enablement Services

The connection between Communication Manager and AES is assumed to be already in place; however, the steps required to set this connection are listed in the sections below.

5.1.1. 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		

5.1.2. 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 noting the IP address for the **procr** and AES (**AES71vmpg**).

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM100	10.10.40.52		
AES71vmpg	10.10.40.43		
default	0.0.0.0		
g430	10.10.40.15		
procr	10.10.40.47		

5.1.3. 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 5.1.2**.
- **Local Port:** Retain the default value of **8765**.

change ip-services				Page 1 of 4	
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 **AES71vmpg**.
- **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** must 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:	AES71vmpg	*****	y	idle
2:				
3:				

5.1.4. 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: AES71vmpg			

5.2. Configure Routing on Avaya Aura® Communication Manager

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 hunt group associated with an agent. Queues are created on EMC, for example, “Webchat for Sales” or “Email for Support” and each queue is assigned a VDN on Communication Manager. The following sections give step by step instructions on how to add the following:

- VDN
- Vector
- Hunt Group
- Agent
- Phantom extension

This procedure is required for every queue that is added on EMC both for voice or multimedia, the following sections will show the required steps to add one agent and the necessary routing for a “Webchat” queue on EMC.

5.2.1. Add VDN

To add a VDN type **add vdn x**, where x is a VDN number. Enter a suitable name for example the **VDN 2920** below will be used exclusively for the **Sales Webchat** queue on EMC.

```
add vdn 2920                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER
                                         Extension: 2920
                                         Name*: Sales Webchat
                                         Destination: Vector Number 2920
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
```

5.2.2. Add Vector

To administer the vector used by the VDN in **Section 5.2.1**, type **change vector x** where x is the vector number. The example below shows the call queuing to skill or hunt group 920 (queue-to skill **920**).

change vector 2920		Page 1 of 6	
CALL VECTOR			
Number: 2920		Name: Sales Webchat	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n	Lock? n
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y
Prompting? y	LAI? y	G3V4 Adv Route? y	ASAI Routing? y
Variables? y	3.0 Enhanced? y	CINFO? y	BSR? y
01 adjunct	routing link 1		
02 wait-time	2 secs hearing silence		
03 queue-to	skill 920 pri m		
04 wait-time	10 secs hearing ringback		
05 queue-to	skill 920 pri m		
06 wait-time	10 secs hearing ringback		
07 disconnect	after announcement none		
08			
09			
10			
11			
12			

5.2.3. 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 the hunt group **920** is added for the **Sales_webchat** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also that **Group Type** is set to **ucd-mia**.

add hunt-group 920		Page 1 of 4	
HUNT GROUP			
Group Number: 920		ACD? y	
Group Name: Sales_Webchat		Queue? y	
Group Extension: 1920		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 920		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		
Supervisor Extension:		
Controlling Adjunct: none		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

5.2.4. 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 4405		Page 1 of 3
AGENT LOGINID		
Login ID: 4405	AAS? n	
Name: Paul	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 **920** is added to this agent so when a webchat call for “Sales” is initiated, the call is routed correctly to this agent.

add agent-loginID 4405												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:	900	1	16:			31:			46:					
2:	910	1	17:			32:			47:					
3:	920	1	18:			33:			48:					
4:	930	1	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:					

5.2.5. Add Phantom Extension

A phantom extension must be setup for every multimedia queue that is added on EMC. The phantom station below is setup for the **Webchat Sales** queue on EMC. Type, **add station x** where x is the phantom station number. This is added as type **6408D+**, **Port** is set to **X** and a suitable **Name** is given to the station, all other settings can be left as default.

add station 28901			Page	1 of	5
STATION					
Extension: 28901	Lock Messages? n	BCC: 0			
Type: 6408D+	Security Code:	TN: 1			
Port: X	Coverage Path 1:	COR: 1			
Name: Webchat Sales Phantom	Coverage Path 2:	COS: 1			
	Hunt-to Station:				
STATION OPTIONS					
Loss Group: 2	Time of Day Lock Table:				
Data Module? n	Personalized Ringing Pattern: 1				
Speakerphone: 2-way	Message Lamp Ext: 28901				
Display Language: english	Mute Button Enabled? y				
Survivable COR: internal	Media Complex Ext:				
Survivable Trunk Dest? y	IP SoftPhone? n				
	Remote Office Phone? n				
	IP Video? n				

5.3. Save Avaya Aura® Communication Manager Configuration

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

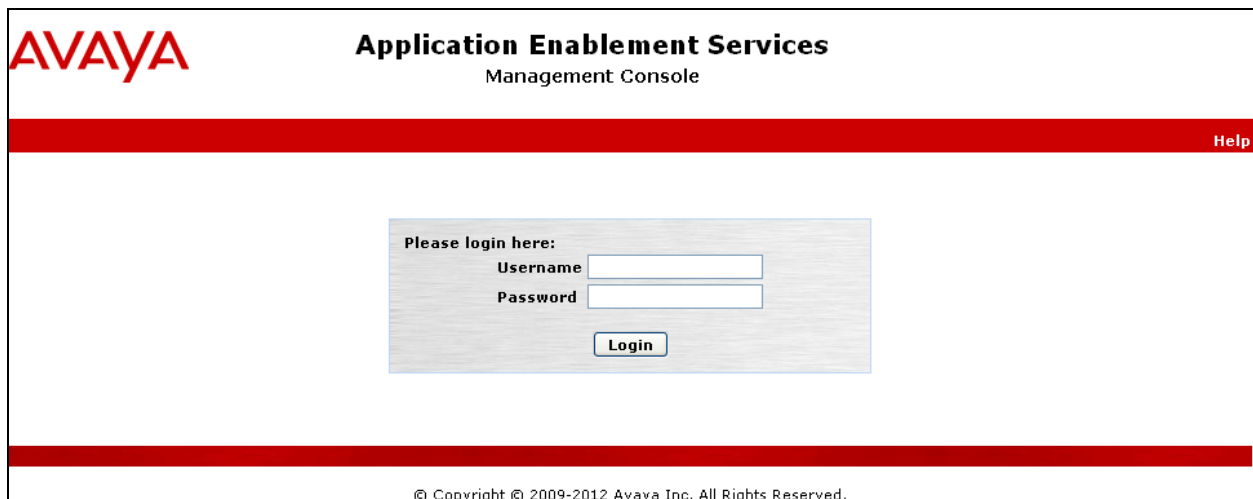
6. Configure Avaya Aura® Application Enablement Services Server

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. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." is displayed.

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 5.1.3**. The remaining fields were left as shown below. Click **Apply** to save changes.

Connection Details - CM71vmpg

Switch Password

.....

Confirm Switch Password

.....

Msg Period

30

Minutes (1 - 72)

Provide AE Services certificate to switch

☐

Secure H323 Connection

☐

Processor Ethernet

☒

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.

Switch Connections

CM71vmpg

Add Connection

Connection Name	Processor Ethernet	Msg Period	
<input checked="" type="radio"/> CM71vmpg	Yes	30	1

Edit Connection

Edit PE/CLAN IPs

Edit H.323 Gatekeeper

Delete Connection

Survivability Hierarchy

In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.1.2** that will be used for the AES connection and select the **Add Name or IP** button.

Edit Processor Ethernet IP - CM71vmpg

10.10.40.47

Add/Edit Name or IP

Name or IP Address
10.10.40.47

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.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar has a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links' (selected), 'TSAPI Properties', and 'TWS'. The main content area is titled 'TSAPI Links' and contains a table with three columns: 'Link', 'Switch Connection', and 'Switch CTI Link #'. Below the table are three buttons: 'Add Link' (highlighted with a red box), 'Edit Link', and 'Delete Link'.

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 **CM71vmpg**, 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 5.1.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **7**.
- **Security:** This was changed to **both** for compliance testing.


Once completed, select **Apply Changes**.

The screenshot shows the 'Edit TSAPI Links' configuration screen. It has five fields with drop-down menus: 'Link' (set to 1), 'Switch Connection' (set to CM71vmpg), 'Switch CTI Link Number' (set to 1), 'ASAI Link Version' (set to 7), and 'Security' (set to Both). At the bottom are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

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

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.

 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

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**.

- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ Maintenance
 - Date Time/NTP Server
 - ▶ Security Database
 - Service Controller**
 - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input 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](#)

6.4. Identify Tlinks

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo on the left and the title "Application Enablement Services Management Console" on the right. Below the header is a red navigation bar with the text "Security | Security Database | Tlinks". On the left side, there is a sidebar menu with various categories: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", and "Security". The "Security" category 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, listing "Control", "CTI Users", "Devices", "Device Groups", "Tlinks" (highlighted in blue), "Tlink Groups", and "Worktops". The main content area on the right is titled "Tlinks" and contains a "Tlink Name" section with two radio button options: "AVAYA#CM71VMPG#CSTA#AES71VMPG" (selected) and "AVAYA#CM71VMPG#CSTA-S#AES71VMPG". Below these options is a "Delete Tlink" button.

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**. CCT 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 13:58:43 2014 from 10.10.00.30
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Dec 01 16:06:19 GMT 2014
HA Status: Not Configured

Networking | Ports Home | Help | Logout

Ports

CVLAN Ports

			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	9998		<input checked="" type="radio"/>	<input type="radio"/>

DLG Port

			Enabled	Disabled
TCP Port	5678		<input checked="" type="radio"/>	<input type="radio"/>

TSAPI Ports

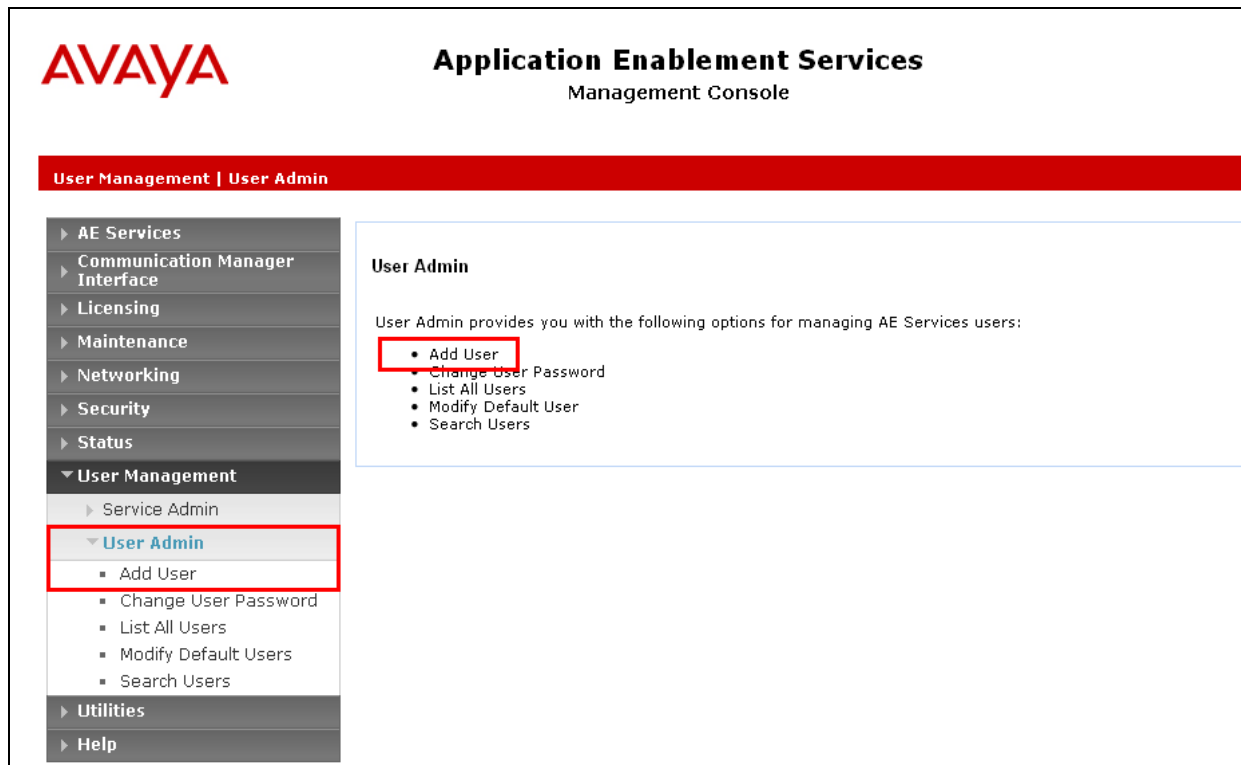
			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	1050			
TCP Port Max	1065			
Encrypted TLINK Ports				
TCP Port Min	1066			
TCP Port Max	1081			

DMCC Server Ports

			Enabled	Disabled
Unencrypted Port	4721		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	4722		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	4723		<input checked="" type="radio"/>	<input type="radio"/>

6.6. Create CTI User

A User ID and password needs to be configured for CCT 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 CCT ContactPro setup in **Section 8.1**.
- **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 8.1**.
- **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 cust
Last login: Tue Jan 13 13:42:04 2015 from 10.10.40.222
Number of prior failed login attempts: 0
HostName/IP: AES63VMPPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Fri Jan 16 14:20:00 GMT 2015
HA Status: Not Configured

User Management | User Admin | List All Users [Home](#) | [Help](#) | [Logout](#)

Edit User

* User Id	CCT
* Common Name	CCT
* Surname	CCT
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Ccs 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' option is selected. 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
<input type="radio"/> asc	asc	NONE	NONE
<input checked="" type="radio"/> CCT	CCT	NONE	NONE
<input type="radio"/> cube	cube	NONE	NONE
<input type="radio"/> emc	emc	NONE	NONE
<input type="radio"/> imperium	imperium	NONE	NONE
<input type="radio"/> jacada	jacada	NONE	NONE
<input type="radio"/> nice	nice	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE

Buttons: Edit, List All

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 set up and the procedure for achieving this can be found in the following document listed in **Section 11 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 visible at the bottom.

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

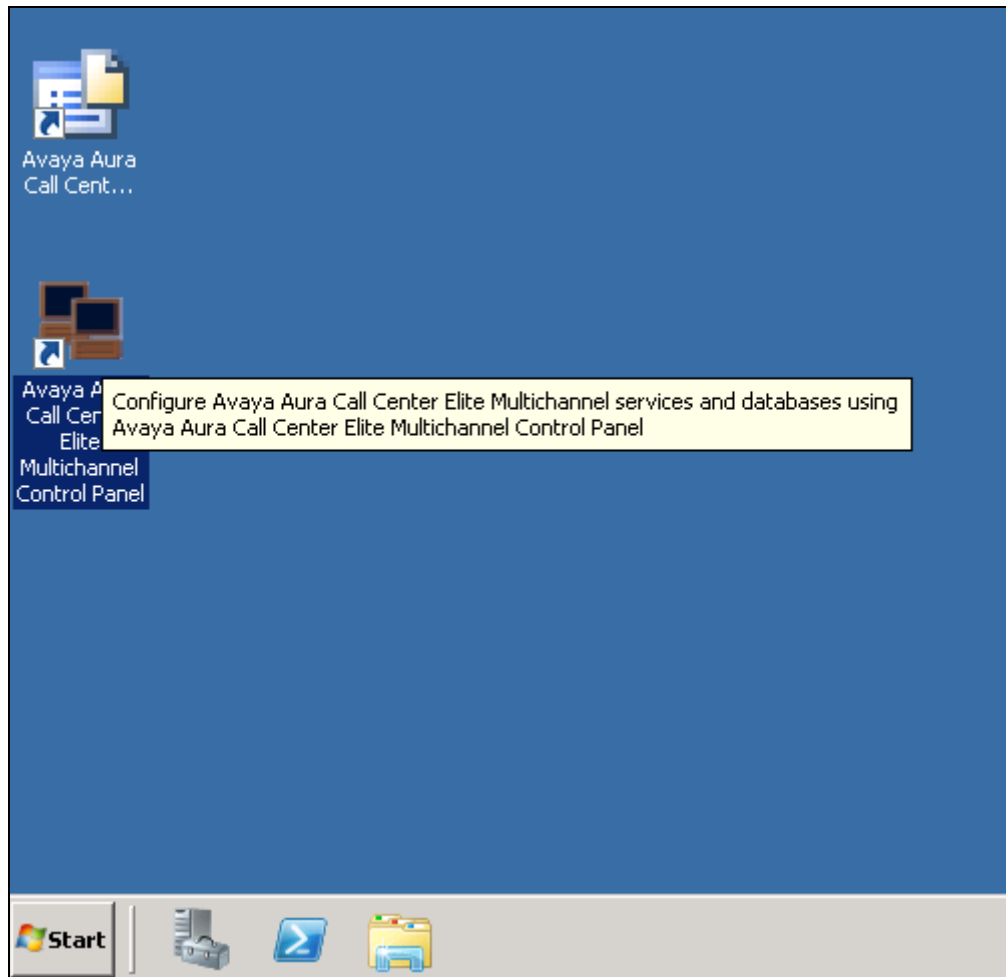
Call and Device Monitoring: Device Monitoring: None, Calls On A Device Monitoring: None, Call Monitoring: ☐

Routing Control: Allow Routing on Listed Devices: None

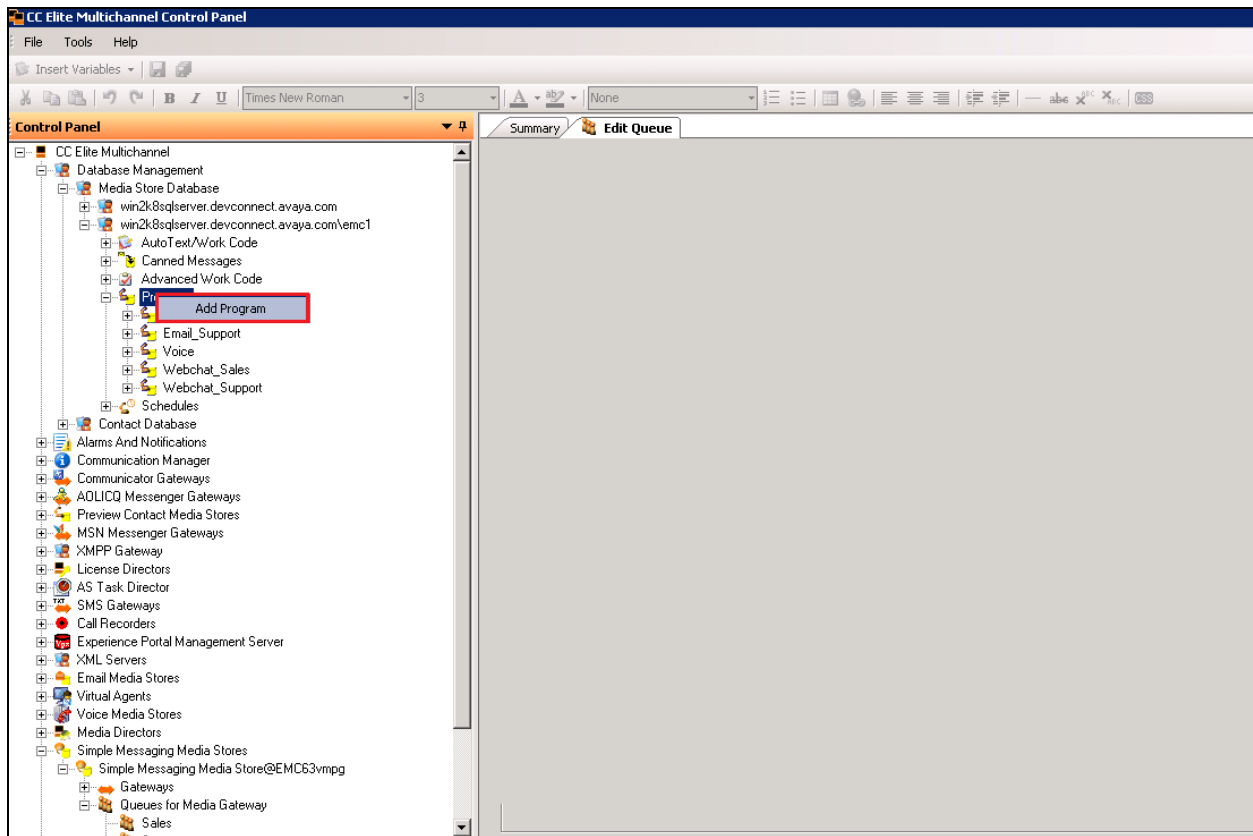
Buttons: Apply Changes, Cancel Changes

7. Configure the Avaya Aura Elite Multichannel Control Panel

Open **Control Panel** to make changes to EMC.



Changes are made to the various components in the left navigation window. Navigate to **Database Management** → **<SQL Server>** → **Programs**. Right-click on **Programs** and select **Add Program**.

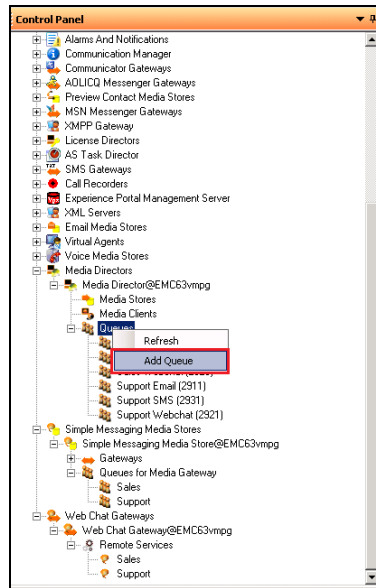


- Enter a suitable **Name**.
- In the Program Configuration panel, select **MyText** from the dropdown as the AutoText List Name.
- Define **Public** as the Program access mode. Select **MyText** as the **Work Code** list name.
- Tick **Automatically Drop Phantom Call**.
- Enter **3** as the Automatic Drop Reason Code.
- Leave the other configuration items with their default values.
- Confirm your selections, and save and close the Program window.

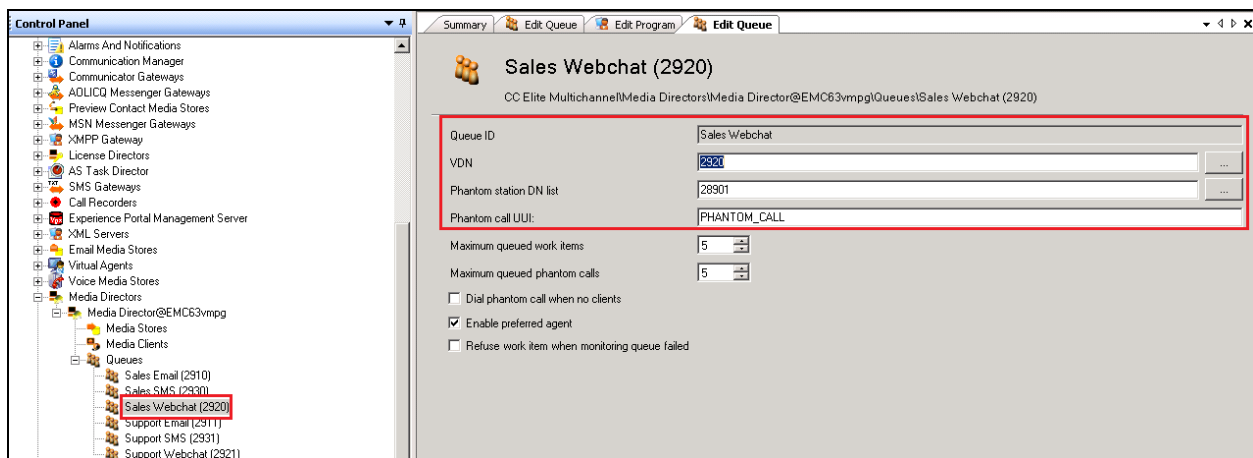
The screenshot displays the 'CC Elite Configuration' window for the 'Webchat_Sales' program. The left sidebar shows a tree view of the system hierarchy, with 'Webchat_Sales' selected under 'Programs'. The main panel is divided into several sections:

- Program Information:**
 - Program ID: 10711327-31da-4fbb-98e1-47354a26d13a
 - Name: Webchat_Sales (highlighted with a red box)
 - Used by: ☐ Preview Contact Media Store, ☐ Auto Contact
 - Description: (empty)
 - Prompt: (empty)
 - Service level seconds: 0
- CC Elite Configuration:**
 - Program Configuration:
 - AutoText list name: MyText (highlighted with a red box)
 - CannedMessage list name: CannedMessageGroup (highlighted with a red box)
 - Program access mode: Public (highlighted with a red box)
 - Work Code:
 - ☐ Use Advanced Work Code style
 - Standard Work Code list name:
 - ☐ AutoText
 - ☒ MyText (highlighted with a red box)
 - ☐ MyCodes
 - Advanced Work Code list name: (empty)
 - Default work code: 0
 - Number of tab pages: 5
 - Minimum required work code(s): 1
- Desktop Utility:**
 - ☒ Automatically drop phantom call
 - Automatic drop reason code: 3
 - Agent available on interaction close: (empty)
 - ☐ Auto accept non-voice interactions
- Preview Contact Client:**
 - Client action: 0 - No Action
 - Auto dial delay (seconds): 20
 - Client window title: Preview Contact

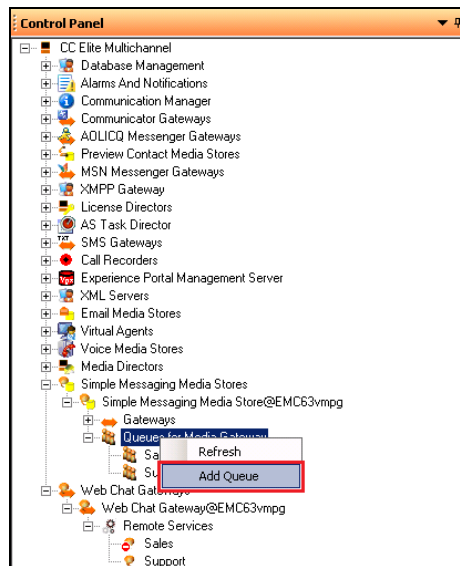
Navigate to **Media Directors** → **MediaDirector@EMC** → **Queues**. Right-click on Queues and select **Add Queue**.



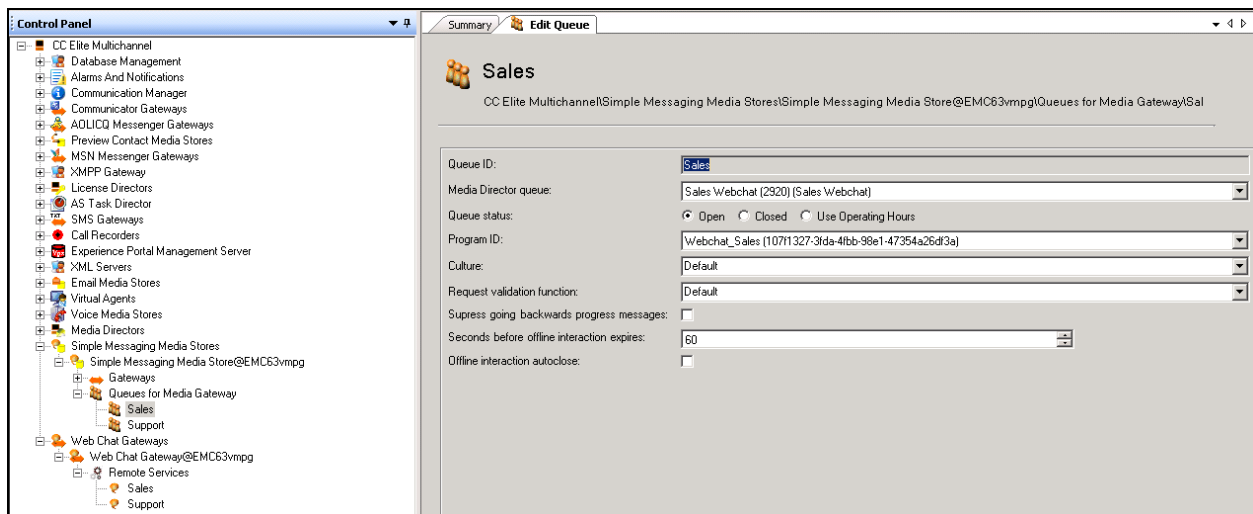
Assign the VDN created in **Section 5.2.1** and the phantom extension created in **Section 5.2.5** to the queue.



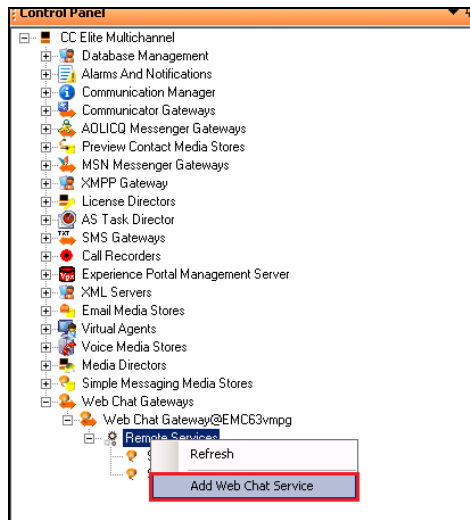
Navigate to **Simple Messaging Media Stores → Simple Messaging Media Stores@<EMCServer> → Queues for Media Gateways**. Right-click on Queues for Media Gateways and select **Add Queue**.



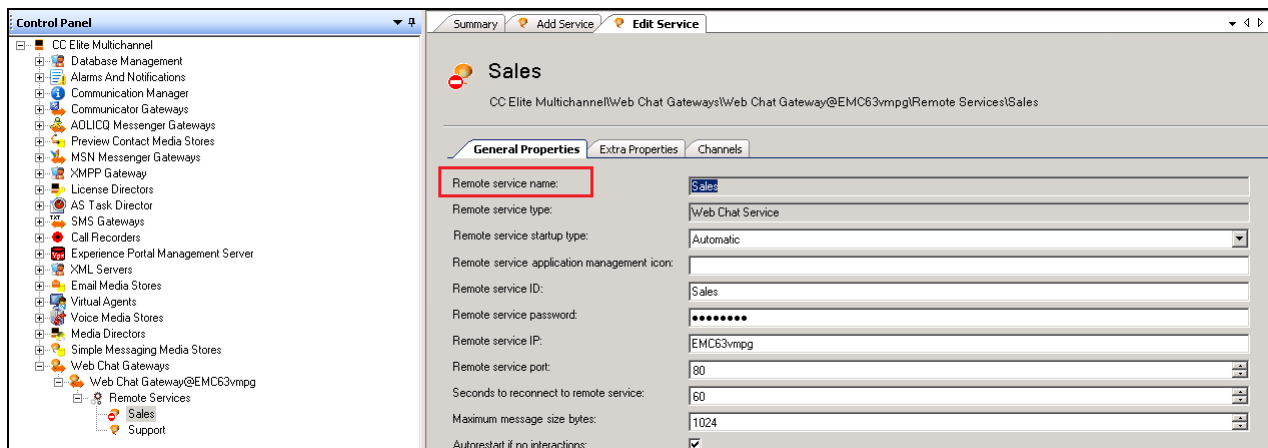
Enter a suitable name and assign the **Media Director queue** and the **Program ID** create above. Everything else can be left as default. Save and close once all is done (not shown).



Navigate to **Web Chat Gateways** → **Web Chat Gateways@ <EMC Server>** → **Remote Services**. Right-click on Remote Services and select **Add Web Chat Service**.



Enter the **Remote service name**.



Leave the fields in the **Extra Properties** tab as default.

The screenshot shows the 'Control Panel' on the left with a tree view containing various system components. The main area displays the 'Sales' service configuration. The 'Extra Properties' tab is active, showing the following fields:

- Remote Service URL: (empty)
- Remote Service URI: /WebChat/WebService/Service.aspx
- Use SSL: ☐
- Seconds to Poll Remote Service: 5
- Address Type: 0

Assign the correct **Simple Messaging Media Store** queue.

The screenshot shows the 'Control Panel' on the left. The main area displays the 'Sales' service configuration. The 'Channels' tab is active, showing a table of channels and an 'Add new channel' section.

Channel ID	Simple Messaging Media Store Queue	Simple Messaging Media Store Queue Priority
Default	Sales	5

Below the table is a 'Delete' button. The 'Add new channel' section contains the following fields:

- Channel ID: Default
- Simple Messaging Media Store queue: Sales (highlighted with a red box)
- Simple Messaging Media Store queue priority: 5
- An 'Add' button.

8. Configure CCT ContactPro

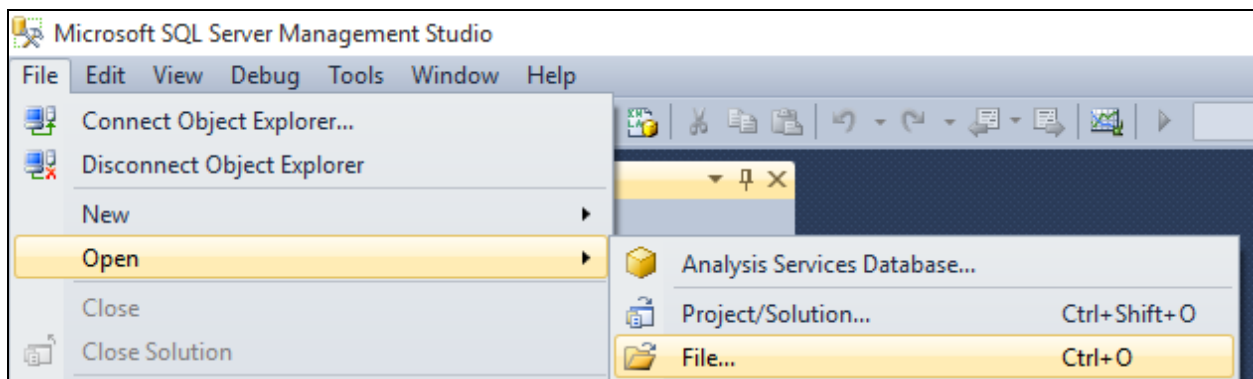
This section outlines the steps required to configure the connections from CCT ContactPro to both the AES and EMC.

8.1. Create CCT ContactPro Database and User

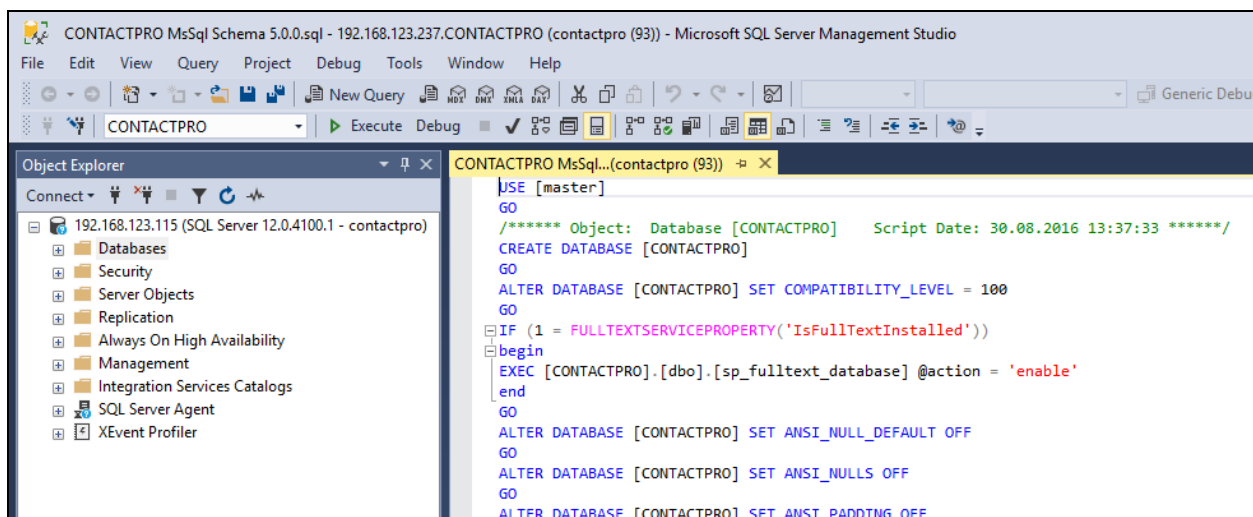
A database and database user for CCT ContactPro must be created on an SQL server. If EMC is being used with the solution the same database that is used by EMC can be used by CCT ContactPro.

8.1.1. Create Database

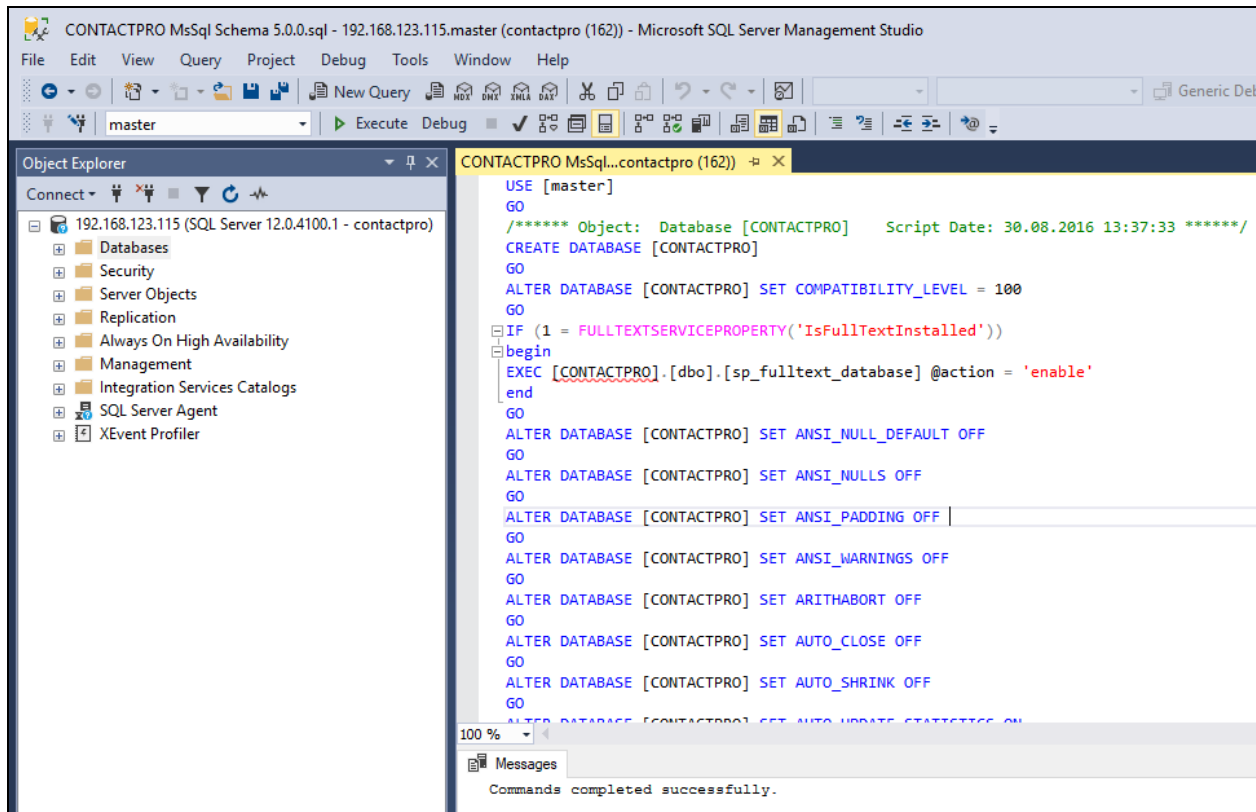
To create the CONTACTPRO database, open the provided **CONTACTPRO MsSql Schema.sql** script.



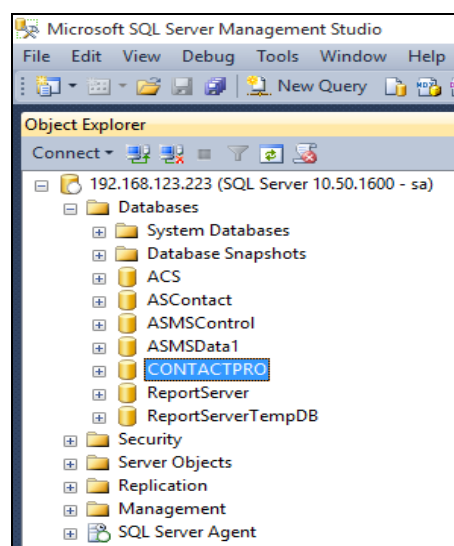
Execute the script by clicking the **Execute** button.



The following shows the script was successfully executed to create the database.

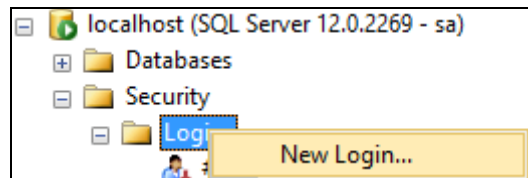


The end result will be as shown in the screenshot below, where there are 4 standard Avaya EMC databases (**ACS**, **ASContact**, **ASMSControl**, **ASMSData1**) and the **CONTACTPRO** database which was just created. The default MS SQL **ReportServer** and **ReportServerTempDB** databases may also be present.

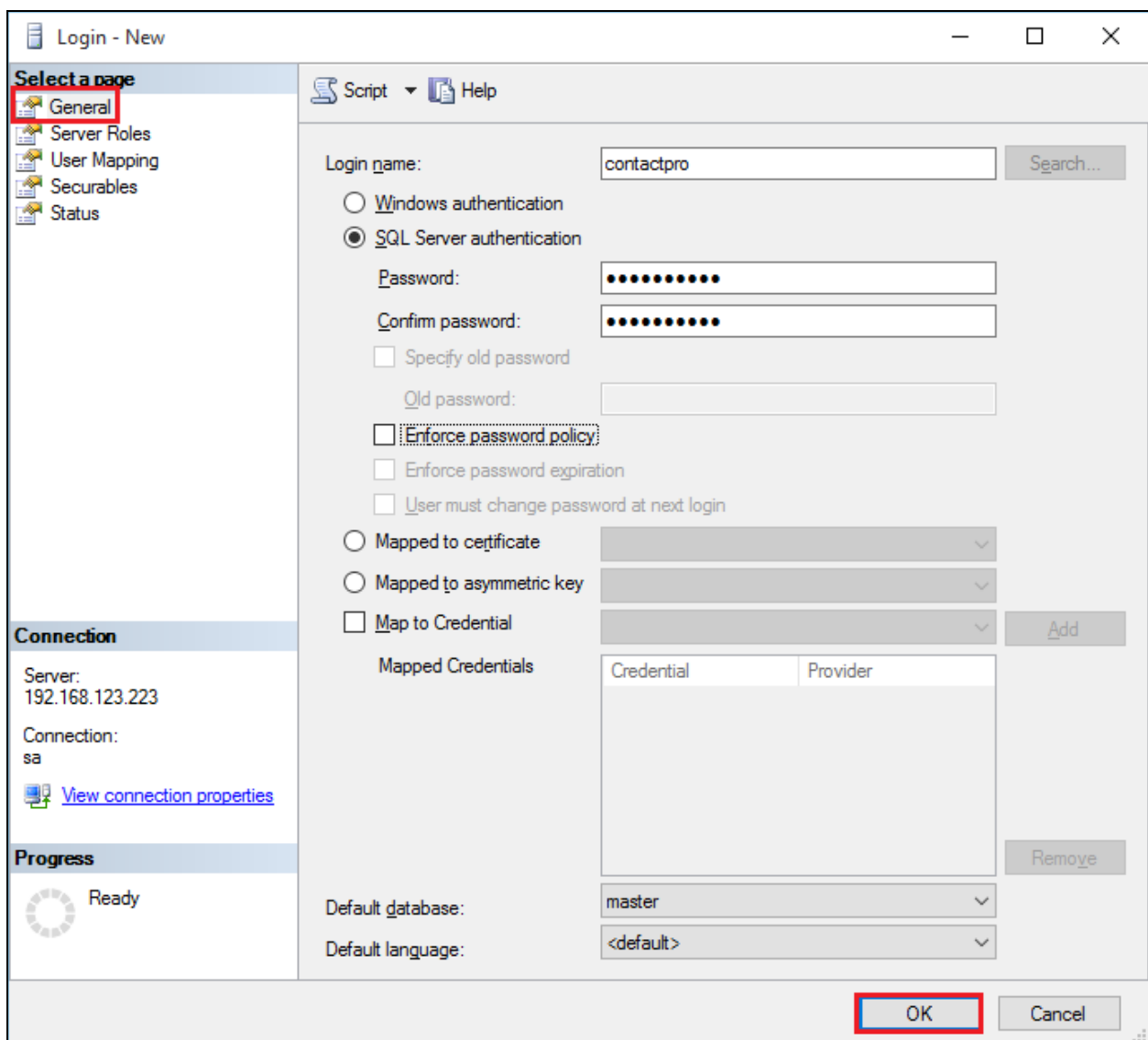


8.1.2. Create User

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.



Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: 192.168.123.223

Connection: sa

[View connection properties](#)

Progress

Ready

Script Help

Login name: contactpro Search...

☐ Windows authentication

☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider
------------	----------

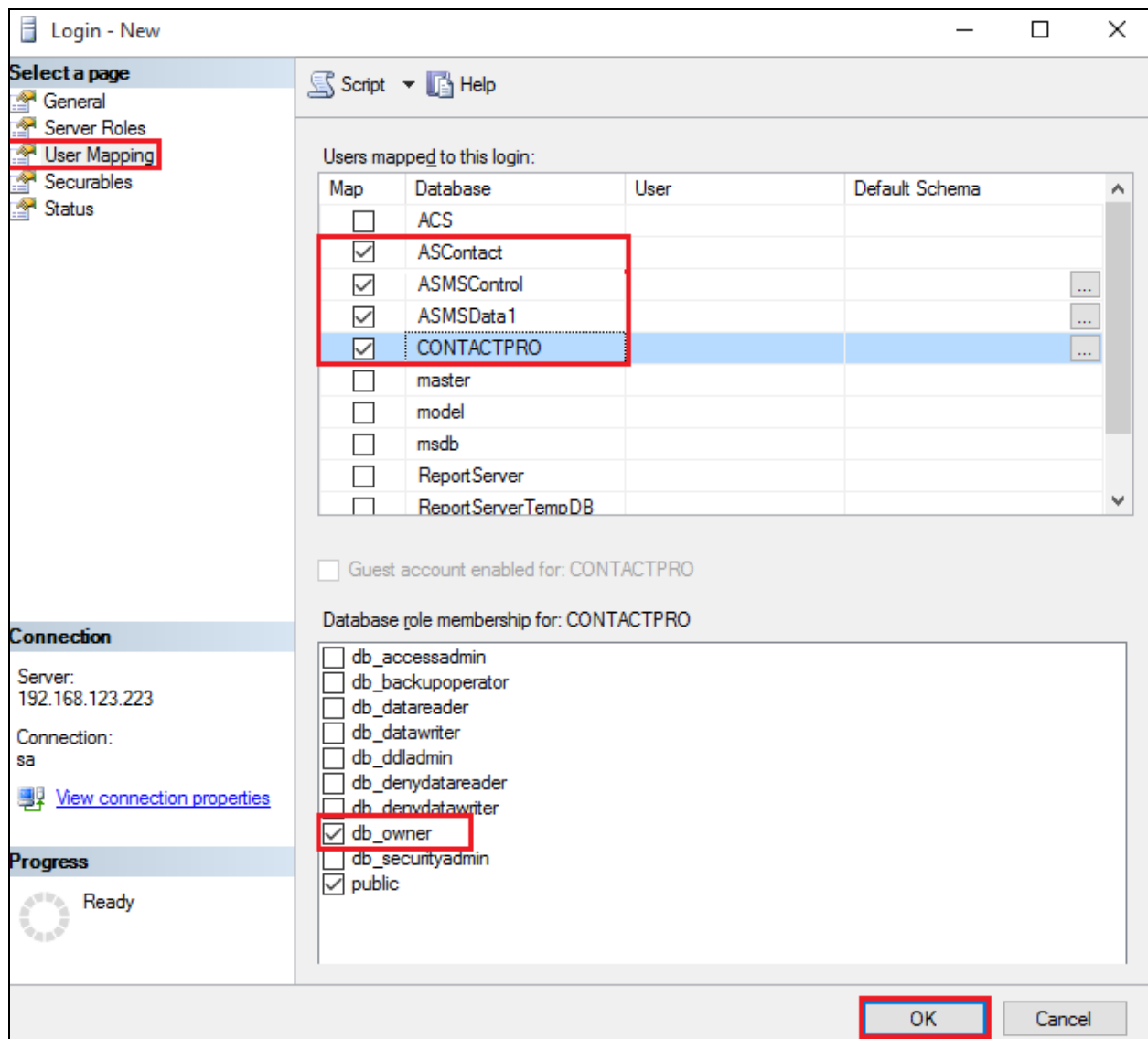
Remove

Default database: master

Default language: <default>

OK Cancel

Click on **User Mapping** in the left window. For this user, grant public and **db_owner** access to **ASContact**, **ASMSControl**, **ASMSData1** and **CONTACTPRO** databases. Click on **OK** at the bottom of the page once done.



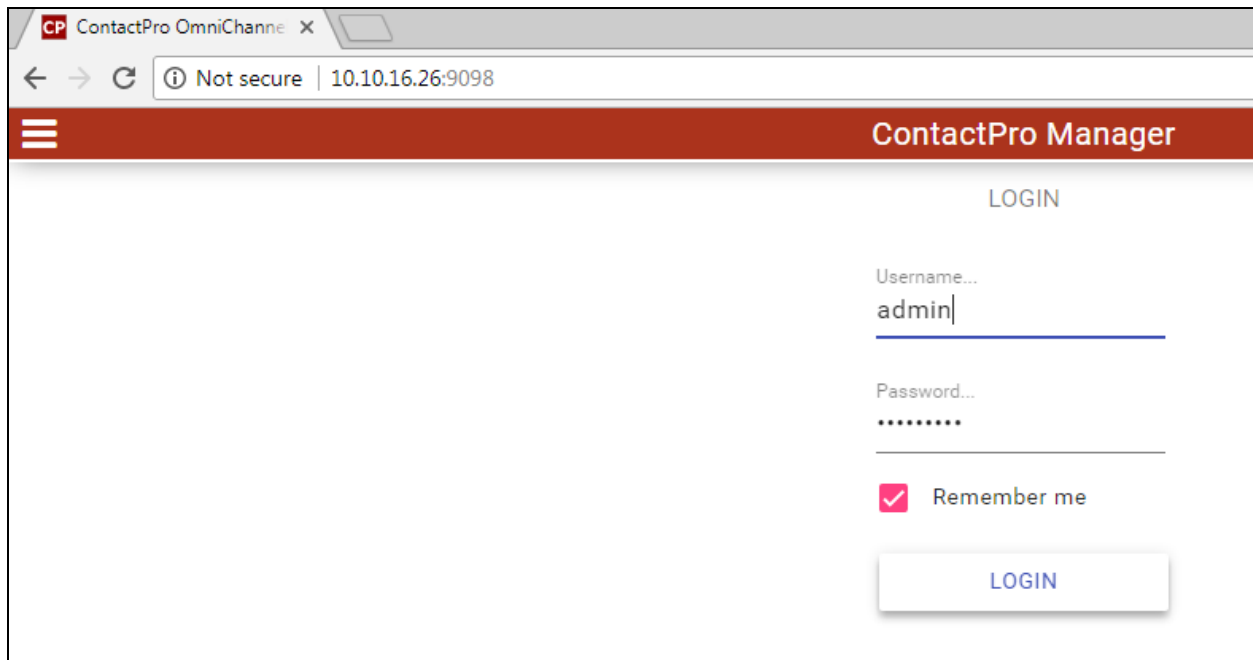
8.2. Configure Properties with ContactPro Manager

The ContactPro Manager allows the configuration of properties for all CCT 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. This is well suited for Enterprise deployment and is similar to Avaya Interaction Center IC Manager.

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

Log in to **ContactPro Manager** via a web session as shown below.



CP ContactPro OmniChannel x

← → ↻ ⓘ Not secure | 10.10.16.26:9098

☰ ContactPro Manager

LOGIN

Username...
admin

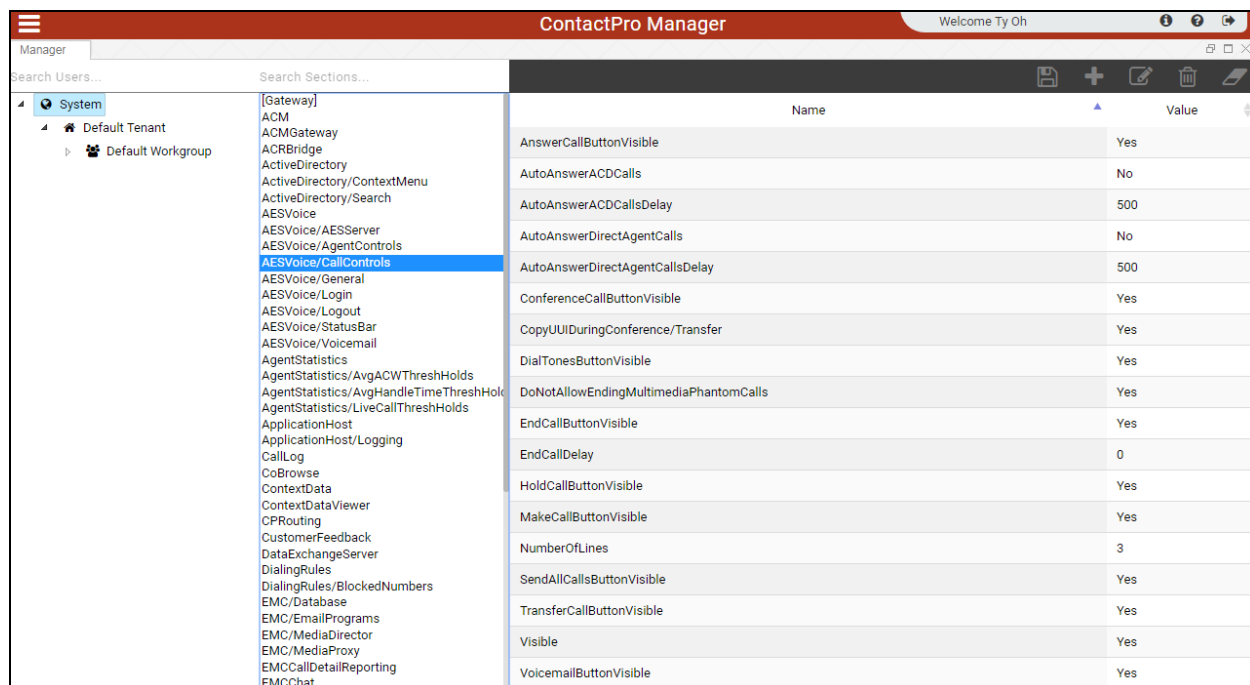
Password...

☒ Remember me

LOGIN

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

Log into **ContactPro Manager** via a web session as shown on the previous page. The **ContactPro Manager** is opened and select **AESVoice/CallControls** from the left window. The main window shows the setup used for compliance testing.



The screenshot shows the ContactPro Manager web interface. The left sidebar contains a tree view with 'System' expanded, showing 'Default Tenant' and 'Default Workgroup'. Under 'Default Workgroup', 'AESVoice/CallControls' is selected. The main area displays a table of configuration settings.

Name	Value
AnswerCallButtonVisible	Yes
AutoAnswerACDCalls	No
AutoAnswerACDCallsDelay	500
AutoAnswerDirectAgentCalls	No
AutoAnswerDirectAgentCallsDelay	500
ConferenceCallButtonVisible	Yes
CopyUIDuringConference/Transfer	Yes
DialTonesButtonVisible	Yes
DoNotAllowEndingMultimediaPhantomCalls	Yes
EndCallButtonVisible	Yes
EndCallDelay	0
HoldCallButtonVisible	Yes
MakeCallButtonVisible	Yes
NumberOfLines	3
SendAllCallsButtonVisible	Yes
TransferCallButtonVisible	Yes
Visible	Yes
VoicemailButtonVisible	Yes

Click on **AESVoice/AESServer** in the left window. Information on the AES server can be filled in the main window; this information is all obtained from **Section 6** and is all required to connect successfully to the AES. Each field can be changed by double-clicking on the field.

[Gateway]	Name	Value
ACM		
ACMGateway		
ACRBridge	AESProtocolVersion	6.3.3
ActiveDirectory		
ActiveDirectory/ContextMenu	PrimaryAESACMConnectionName	CM71vmpg
ActiveDirectory/Search		
AESVoice	PrimaryAESIPAddress	10.10.40.43
AESVoice/AESServer	PrimaryAESLoginPassword	*
AESVoice/AgentControls	PrimaryAESLoginUsername	cct
AESVoice/CallControls		
AESVoice/General	PrimaryAESPort	4721
AESVoice/Login	PrimaryAESSecureSocket	No
AESVoice/Logout		
AESVoice/StatusBar	QuaternaryAESACMConnectionName	
AESVoice/Voicemail	QuaternaryAESIPAddress	
AgentStatistics	QuaternaryAESLoginPassword	*
AgentStatistics/AvgACWThreshHolds	QuaternaryAESLoginUsername	
AgentStatistics/AvgHandleTimeThreshHolds	QuaternaryAESPort	4721
AgentStatistics/LiveCallThreshHolds	QuaternaryAESSecureSocket	No
ApplicationHost	SecondaryAESACMConnectionName	
ApplicationHost/Logging	SecondaryAESIPAddress	
CallLog	SecondaryAESLoginPassword	*
CoBrowse	SecondaryAESLoginUsername	
ContextData	SecondaryAESPort	4721
ContextDataViewer	SecondaryAESSecureSocket	No
CPRouting	TertiaryAESACMConnectionName	
CustomerFeedback	TertiaryAESIPAddress	
DataExchangeServer	TertiaryAESLoginPassword	*
DialingRules	TertiaryAESLoginUsername	
DialingRules/BlockedNumbers	TertiaryAESPort	4721
EMC/Database	TertiaryAESSecureSocket	No
EMC/EmailPrograms		
EMC/MediaDirector		
EMC/MediaProxy		
EMCCallDetailReporting		
EMCChat		
EMCCore		
EMCEmail		
EMCEmailManagement		
EMCHistoryViewer		
EMCPrivateWorkList		
EMCWrapUp		
Help		
LicenseServer		
Login		
Login/Login		
Manager		
MSCRM/Screenpop/Chat		
MSCRM/Screenpop/Email		

To change the Primary AES IP Address, double-click on the **PrimaryAESIPAddress** field highlighted below and this brings up an edit window where a new IP address can be entered and click **UPDATE** once this is done.

Update Property

Name*

PrimaryAESIPAddress

Description

Default: EMPTY. The Server Address of the AES Server.

Property Value

10.10.40.43

UPDATE

CANCEL

8.2.2. Configure the Connection to Avaya Aura® Call Center Elite Multichannel

Select **EMC/MediaDirector** from the left window and double-click on **PrimaryAddress** highlighted below and enter the IP address of the EMC server followed by the port used to connect, note that **39087** is the default secure port but this information can be obtained from the EMC server. Click on **OK** once this is entered correctly.

Note: The default port for the Secure Channel of EMC Media Director is 39087, otherwise it would be 29087. **EMCCore, EnableSecureChannel** property needs to be set to **Yes** (not shown).

[Gateway]	Name	Value
ACM		
ACMGateway		
ACRBridge	PrimaryAddress	10.10.40.82:39087
ActiveDirectory	SecondaryAddress	
ActiveDirectory/ContextMenu		
ActiveDirectory/Search		
AESVoice		
AESVoice/AESServer		
AESVoice/AgentControls		
AESVoice/CallControls		
AESVoice/General		
AESVoice/Login		
AESVoice/Logout		
AESVoice/StatusBar		
AESVoice/Voicemail		
AgentStatistics		
AgentStatistics/AvgACWThreshHolds		
AgentStatistics/AvgHandleTimeThreshHolds		
AgentStatistics/LiveCallThreshHolds		
ApplicationHost		
ApplicationHost/Logging		
CallLog		
CoBrowse		
ContextData		
ContextDataViewer		
CPRouting		
CustomerFeedback		
DataExchangeServer		
DialingRules		
DialingRules/BlockedNumbers		
EMC/Database		
EMC/EmailPrograms		
EMC/MediaDirector		
EMC/MediaProxy		
EMCCallDetailReporting		

Select **EMC/MediaProxy** from the left window and double-click on **PrimaryAddress** highlighted below and enter the IP address of the EMC MediaProxy followed by the port used to connect, note that **39079** is the default secure port but this information can be obtained from the EMC setup. Click on **OK** once this is entered correctly.

Note: A connection can be made to a local EMC MediaProxy Service, or an EMC MediaProxy Service running on the Server. Both options are supported by EMC. The default port for the Secure Channel of EMC Media Proxy is 39079, otherwise it would be 29079. **EMCCore** and **EnableSecureChannel** property also need to be set to **Yes** (not shown).

	Name	Value
CustomerFeedback	PrimaryAddress	192.168.123.237:39079
DataExchangeServer	SecondaryAddress	
DialingRules		
DialingRules/BlockedNumbers		
EMC/Database		
EMC/EmailPrograms		
EMC/MediaDirector		
EMC/MediaProxy		
EMCCallDetailReporting		
EMCChat		
EMCCore		
EMCEmail		
EMCEmailManagement		
EMCHistoryViewer		
EMCPrivateWorkList		
EMCWrapUp		
Help		

8.2.3. Configure the Connection to EMC Email Storage Path

Select **EMCHistoryViewer** from the left window and double-click on the **EmailStoragePath** field and enter the path to where the EMC stores the emails. This can be found on the EMC server. Click on **OK** once this is complete.

	Name	Value
ActiveDirectory/Search	ChatSearchFixAgentIDSearch	Yes
AESVoice	ChatSearchMaxRecordsDefault	100
AESVoice/AESServer	CustomerNumberLabel	
AESVoice/AgentControls	DefaultEncoding	utf-8
AESVoice/CallControls	EmailSearchFixAgentIDSearch	Yes
AESVoice/General	EmailSearchMaxRecordsDefault	100
AESVoice/Login	EmailStorageDomain	
AESVoice/Logout	EmailStoragePassword	*
AESVoice/StatusBar	EmailStoragePath	\\EMC2VMFG\Email Storage
AESVoice/Voicemail	EmailStorageUsername	
AgentStatistics	EnableChatSearch	Yes
AgentStatistics/AvgACWThreshHolds	EnableEmailSearch	Yes
AgentStatistics/AvgHandleTimeThreshHolds	EnableTenantBasedSearch	No
AgentStatistics/LiveCallThreshHolds	InformUserAboutIrregularEmails	Yes
ApplicationHost	SearchDateTimeFormat	yyyy-MM-dd
ApplicationHost/Logging	SecondaryEmailStoragePath	
CallLog	UseDatabaseQueries	No
CoBrowse		
ContextData		
ContextDataViewer		
CPRouting		
CustomerFeedback		
DataExchangeServer		
DialingRules		
DialingRules/BlockedNumbers		
EMC/Database		
EMC/EmailPrograms		
EMC/MediaDirector		
EMC/MediaProxy		
EMCCallDetailReporting		
EMCChat		
EMCCore		
EMCEmail		
EMCEmailManagement		
EMCHistoryViewer		
EMCPrivateWorkList		

A shared path to the **Email Storage** must be created for clients to access. This is typically in the “C:\Program Files (x86)\Avaya\Avaya Aura CC Elite Multichannel\Server\Media Stores\Email Media Store\Email Storage” of the EMC Server. This is required to provide the feature of viewing the Body of every email (without having to retrieve it) via the Enhanced History provided by ContactPro. Below is an example of retrieving such an email where the agent does a **Search** for **paul** and retrieves all the emails associated with the word **paul**. Double-clicking on this item will then open the associated email for viewing.

Search Emails

Max. Records 100 Close Window

Search

From To Subject Agent All Open Customer Number Comment Tracking History

Select Months 1 Status Open or Closed

Search by From Address Contains **paul** Search

Date	Status	From	To	Agent	Subject	InteractionId	ConversationId
11.08.2015 15:17:48	Closed	Greaney, Paul (Pa...	Ty Oh <tyoh@cct...		RE: Next DevConnect Certification - Avaya...	cfc26b35-8de4-46...	031fbf31-e6d8-475...
05.08.2015 10:37:04	Closed	"Greaney, Paul (P...	Ty Oh <tyoh@cct...	5321	RE: ContactPro EMC Manager	4d6e4368-6e5f-47...	26ac2caa-9b2c-4e...
04.08.2015 12:06:59	Closed	Maximilian Paul <...	Ty Oh <tyoh@cct...	5321	Logs regarding Presence Problem	f8c216a6-a429-4d...	6f84ed8c-835c-4f9...
29.07.2015 18:24:45	Closed	Maximilian Paul <...	Ty Oh <tyoh@cct...	5321	Config.xml Bosch	d94a97b2-7846-4...	88d7dcf1-cdc3-4a...

Email from 01.08.2015 to 14.08.2015 18

Details

From "Greaney, Paul (Paul) "

To "Ty Oh" <tyoh@cct-solutions.com>

Cc

Bcc

Subject RE: ContactPro EMC Manager [InteractionID:4d6e4368-6e5f-473b-b862-1672f92ed...

Encoding US-ASCII

image003.png (9 KB) image004.jpg (712 B) image005.jpg (749 B)

Additional Data

InteractionId 4d6e4368-6e5f-473b-b862-1672f92ed6e4

ConversationId 26ac2caa-9b2c-4ed4-b1c8f14815f1861d

Preferred Agent

Deferred Reason

Deferred until

Email Body

Ty,

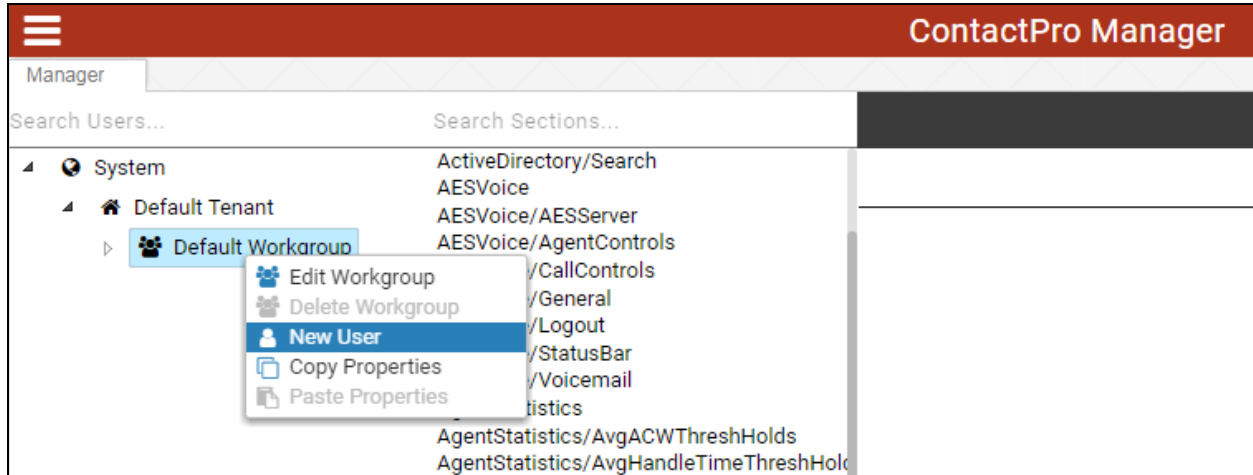
I got that and installed today and seems to be working fine and connecting ok. I will not get a chance this week to look at the Application Notes but I hope to start on them Monday and I will focus solely on them and get them finished ASAP.

Kindest regards,
Paul Greaney

Encoding

8.3. Configure Users with ContactPro Manager

For every ContactPro Client user, a new user needs to be created. Right-click on a workgroup then click **New User**.



The following fields are required.

- **LoginName** (This is the Agent ID such as that created in **Section 5.2.4** for example).
- **First Name**
- **Last Name**

Add User		
Login Name*	Title	
4401		
First Name*	Last Name*	
Paul	Greaney	
Phone	Email	
Active Directory Username	CRM Username	
Agent		
Password		
.....		
<input type="checkbox"/> Change Password On Login		
Agent ID	Agent Password	
Min. password length: 8 Min. number of characters: 1 Min. number of numbers: 1 Min. number of special Characters: 1		
Station	Station Password	
Capacity Email	Capacity WebChat	Capacity Total
1	1	1
<div>ADD CANCEL</div>		

9. Verification Steps

This section provides the verification steps that can be performed to verify proper configurations of both Avaya EMC and AES with CCT ContactPro.

9.1. Verify Status of Communication Manager Agent

Enter the command **list agent-loginID** verify that agent **4405** shown in **Section 5.2.4** is logged-in to extension **4000**.

list agent-loginID									
AGENT LOGINID									
Login ID	Name	Extension		Dir	Agt	AAS/AUD		COR Ag	Pr SO
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
4400	Patrick	unstaffed						1	lvl
	33/01	34/01	/	/	/	/	/	/	/
4401	Agent 1	unstaffed						1	lvl
	33/01	34/01	/	/	/	/	/	/	/
4402	Agent 2	unstaffed						1	lvl
	33/01	34/01	/	/	/	/	/	/	/
4404	Agent 3	unstaffed						1	lvl
	900/01	910/01	920/01	930/01	901/01	911/01	921/01	931/01	
4405	Paul	4000						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 4000** 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 9.5**.

status station 4000							Page 7 of 7
ACD STATUS							
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	
900/AI	/	/	/	/	/	/	
910/AI	/	/	/	/	/	/	
920/AI	/	/	/	/	/	/	
930/AI	/	/	/	/	/	/	
On ACD Call? no							

9.2. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	AES71vmpg	established	18	18

9.3. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

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
1	CM71vmpg	1	Talking	Thu Dec 7 09:12:16 2017	Online	17	4	872	893	30

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

9.4. Verify login of CCT ContactPro

From the Client PC open the application **CCT 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 the **Appendix**.
- **ACM Station Password** This is the password for the station that is to be controlled this is the same password noted in the **Appendix**.
- **ACM Agent ID** This is the Agent ID created or noted in **Section 5.2.4**.
- **ACM Agent Password** This is the password of the agent noted or created in **Section 5.2.4**.

Click on **OK** to log in to **CCT ContactPro**.

Elite Agent

Station: 4000 Station Password: ****

Agent ID: 4401 Agent Password: ****

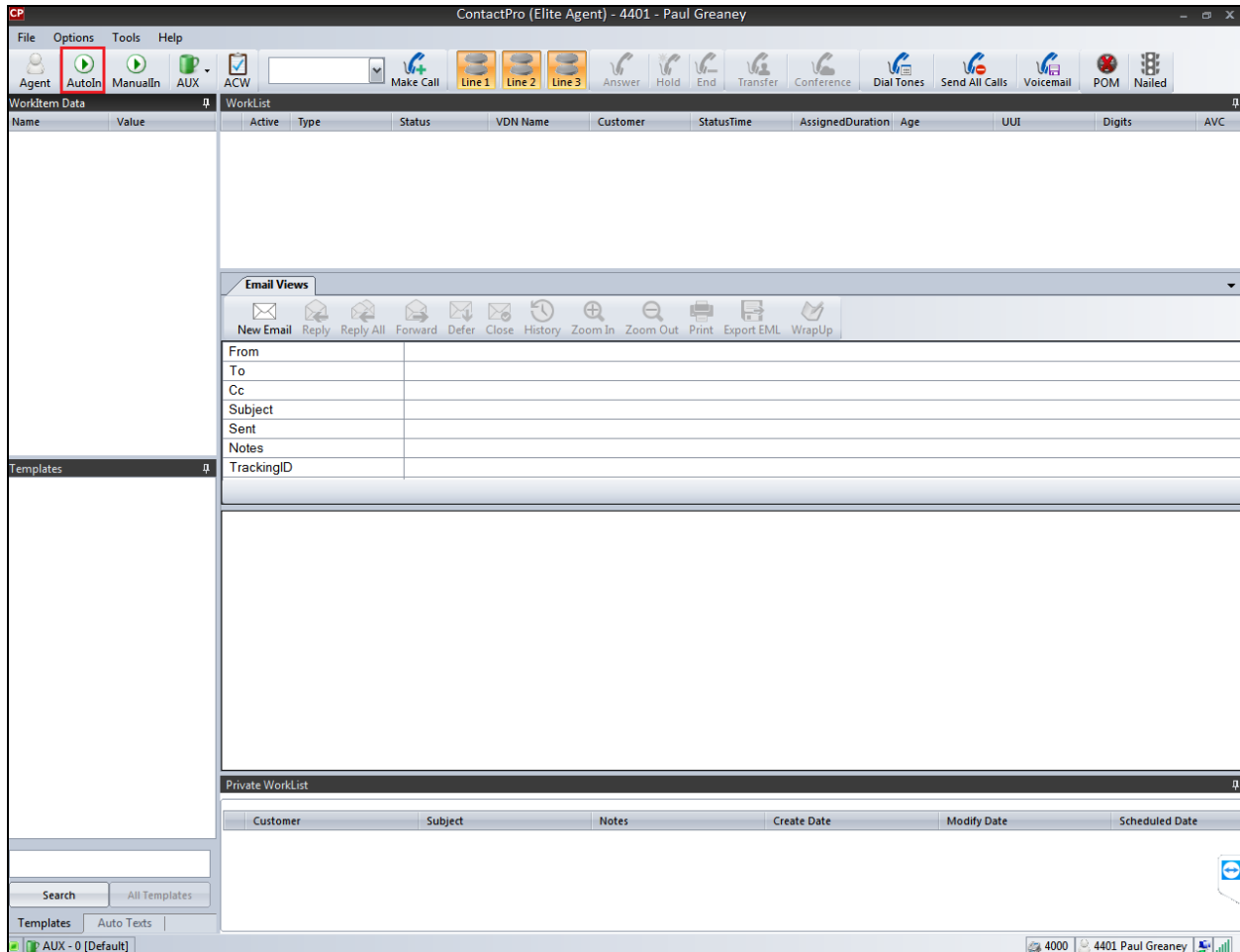
Phone

☒ Desk Phone
☐ This Computer
☐ Other Phone

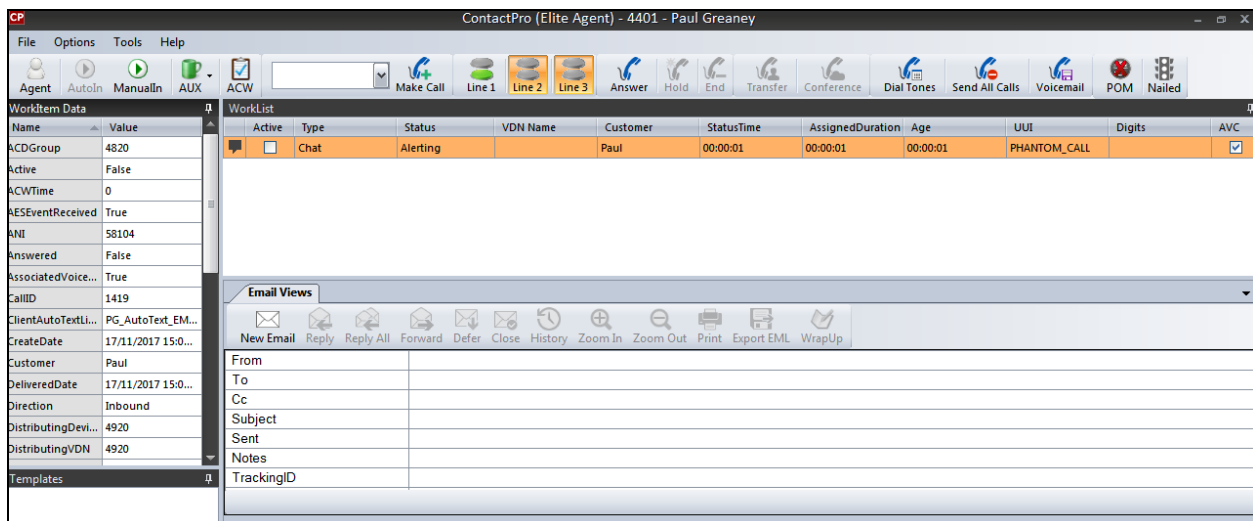
Clear OK Cancel

9.5. Verify Agent Status using CCT ContactPro

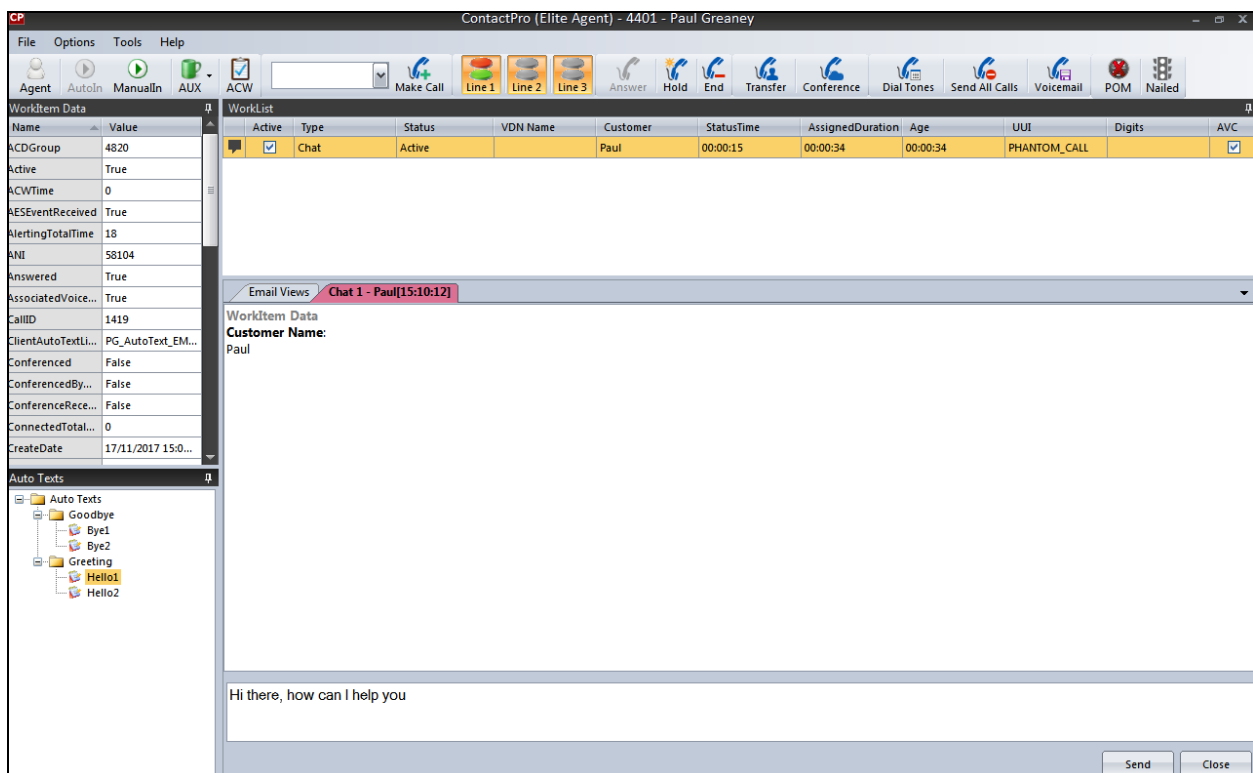
Once logged in the agent state can be changed using the buttons at the top left highlighted below. Note also the station number (**4000**) and Agent ID (**4401**) once logged in. Click on **AutoIn** to make the agent ready.



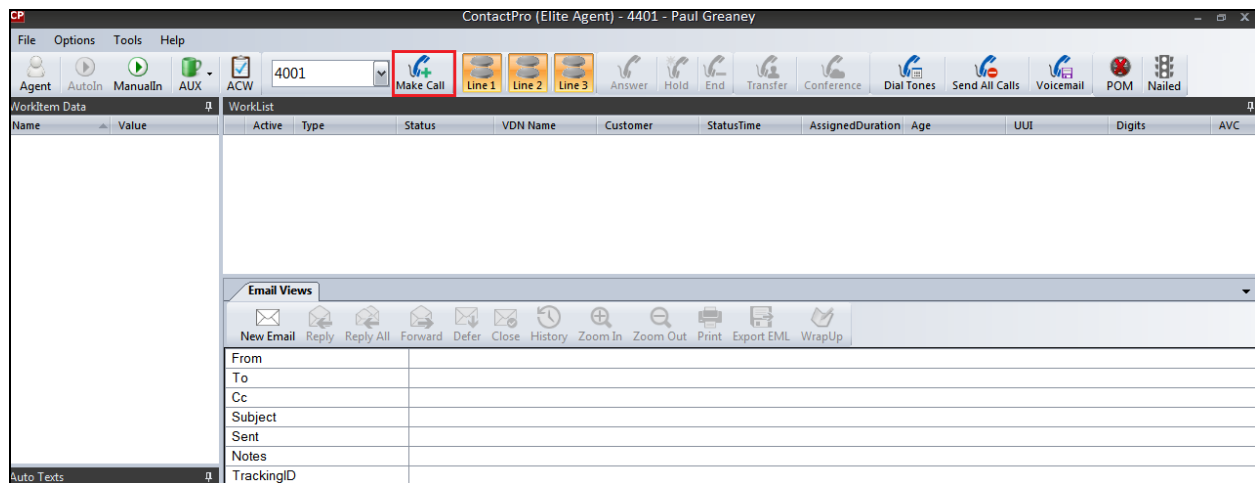
A web request is generated by a customer (not shown) and queued to this agent. Once AutoIn is pressed above the call appears as **Alerting** on the ContactPro desktop. The call can be answered by pressing the **Answer** icon.



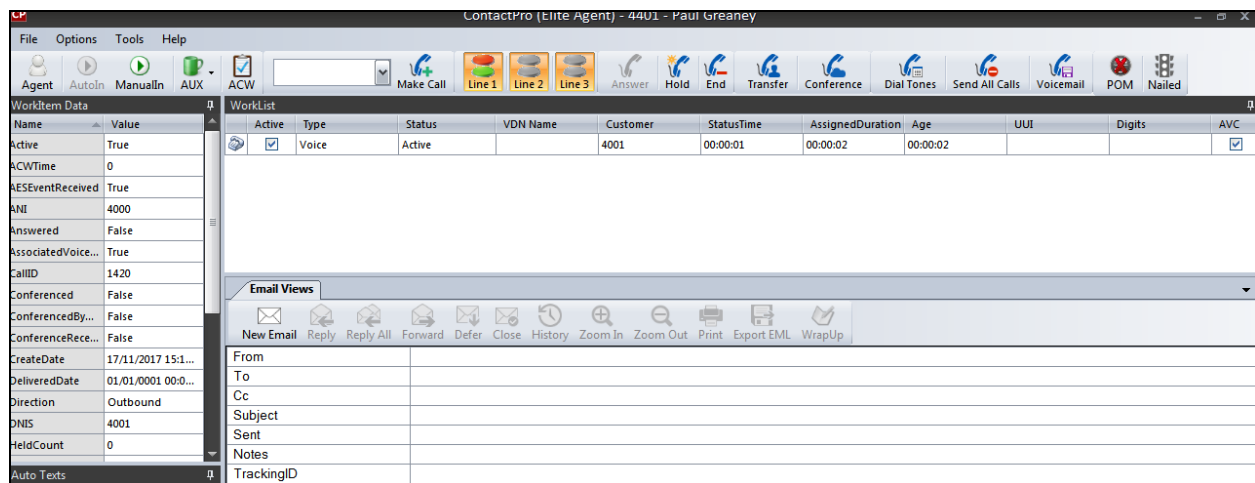
Once the call is answered, a **Multimedia Window** is opened showing the web chat request from the customer and the agent can respond to that request as is shown below, by entering some text and clicking **Send**. Also, we can see that the line is busy and the agent is therefore deemed to be on a call even if this is a multimedia call. The agent can hang up or close the call by clicking on **Close** at the bottom right of the Multimedia Window.



With the multimedia call ended a new call can be made if required again by entering the digits and pressing on **Make Call** as is shown. In this example, the agent is calling the customer at his/her request from the webchat session previous.



The call can then be transferred, conference or put on hold with the buttons displayed along the top of the screen.



10. Conclusion

These Application Notes describe the configuration steps required for CCT ContactPro from CCT Deutschland GmbH to interoperate with Avaya Aura® Application Enablement Services R7.1 and Avaya Aura® Call Center Elite Multichannel R6.5. All feature and serviceability test cases were completed successfully, with any observations noted in **Section 2.2**.

11. Additional References

This section references the Avaya and CCT ContactPro 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] *Deploying Avaya Aura® Call Center Elite Multichannel in an Avaya Customer Experience Virtualized Environment*, Release 6.5.. July 2016.
- [2] *Installing Avaya Aura® Call Center Elite Multichannel*, Release 6.5. July 2016.
- [3] *Administering Avaya Aura® Call Center Elite Multichannel*, Release 6.5. July 2016.
- [4] *Avaya Aura® Call Center Elite Multichannel Release Notes*, Release 6.5. July 2016.
- [5] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509.
- [6] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205.
- [7] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.1.2, December 2017.

The following CCT ContactPro Deutschland GmbH 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 9608 H323 Station 4000

This is a printout of the Avaya 9608 H.323 desk phone used during compliance testing.

Page 1

display station 4000	Page 1 of 6	
STATION		
Extension: 4000	Lock Messages? n	BCC: 0
Type: 9608	Security Code:	TN: 1
Port: S00057	Coverage Path 1:	COR: 1
Name: CCT Agent	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Message Lamp Ext: 4000	
Display Language: english	Button Modules: 0	
Survivable COR: internal	IP SoftPhone? y	
Survivable Trunk Dest? y	IP Video? n	

Page 2

display station 4000	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: 1005	Always Use? n IP Audio Hairpinning? n	

Page 3

display station 4000	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 4000	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	

©2018 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.