AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for ContactPro from CCT Deutschland GmbH with Avaya Proactive Outreach Manager 3.1.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for ContactPro from CCT Deutschland GmbH to interoperate with Avaya Proactive Outreach Manager. ContactPro is an interaction management application that connects to both Avaya Aura® Call Center Elite Multichannel and Avaya Interaction Center, however the Avaya Proactive Outreach Manager is common for both.

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.

SJW; Reviewed:
SPOC 4/9/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

1 of 50
ConPro_POM31

1. Introduction

These Application Notes describe the configuration steps required for ContactPro from CCT Deutschland GmbH, to interoperate with Avaya Proactive Outreach Manager (POM). 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.

ContactPro offers a connection to Avaya Aura® Application Enablement Server (AES), Avaya Aura® Call Center Elite multichannel and Avaya Interaction Center. The connection to Avaya Proactive Outreach Manager, although is common to all desktops, use the same interface to display the POM outbound features. These Application Notes will go through the setup and configuration for CCT ContactPro to connect to Avaya Proactive Outreach Manager.

2. General Test Approach and Test Results

The general test approach was to validate the ContactPro client's ability to join Proactive Outreach Manager outbound Campaigns. This was performed by creating Preview, Predictive and Progressive campaigns with agent scripts and handled them in the ContactPro client.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and the Contact Pro did not include use of any specific encryption features as requested by CCT Deutschland GmbH.

2.1. Interoperability Compliance Testing

The testing focuses on the following areas:

- **Agent Can Join an outbound Campaign** – log in an Agent to a campaign
- **Agent is presented with calls in Progressive Campaign** – POM Presents agent with calls. Call can be answered, put on hold, Transferred and cleared using ContactPro Client.
- **Agent is presented with calls in Predicitve Campaign** – POM Presents agent with calls. Call can be answered, put on hold, Transferred and cleared using ContactPro Client.
- **Agent can Preview, Cancel or Dial record in a Preview campaign** – Agent operates correctly in a Preview campaign. Call can be answered, put on hold, Transferred and cleared using ContactPro Client.
- **Agent can assign Completion Codes to a call** – Completion codes are correctly recorded at the end of calls
- **Agent can assign a Record to the Do Not Call (DNC) list** – Call is added to DNC list and is not selected to be called in subsequent campaigns.
- **Agent can assign a callback** – Agent assigns callback for a time in the future and record is called at the correct time
- **Agent can leave a POM Campaign** – Agent can leave a Campaign. Agent shows as not ready and is then removed from POM Campaign on logout
- **ContactPro Client recovers in Failure scenarios** – Observe the behaviour of ContactPro and its ability to recover from failure scenarios.

2.2. Test Results

All test cases passed.

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 ContactPro using a connection to POM.
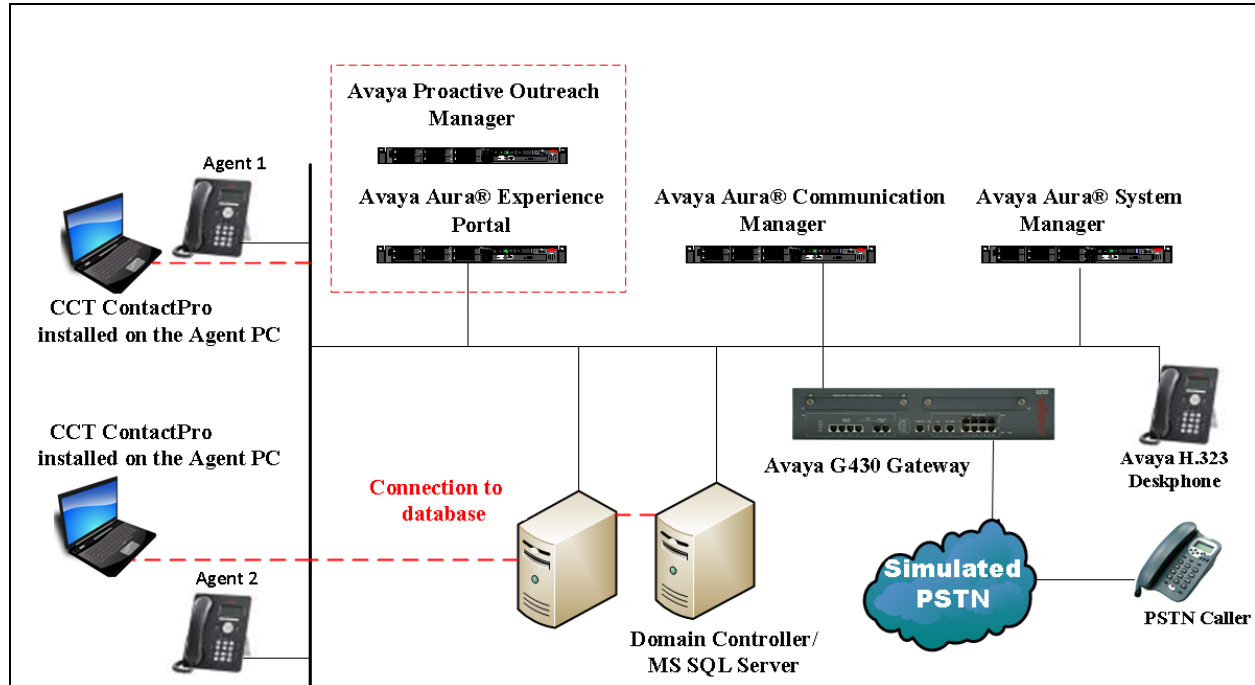
Figure 1: Connection of CCT Deutschland GmbH ContactPro with Avaya Proactive Outreach Manager.

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 Build No. – 7.1.0.0.1125193 Software Update Revision No: 7.1.1.0.46931 Feature Pack 1
Avaya Aura® Communication Manager running on a virtual server	R7.0 SP1 R017x.01.0.532.0 Updates: 01.0.532.0-24184 KERNEL-3.1.0-693.e17.AV1 PLAT-rhel7.2-0010
Avaya Aura® Session Manager running on a virtual server	Session Manager R7 SP1 Build No. – 7.1.1.0.711008
Avaya Aura® Application Enablement Services running on a virtual server	R7.0 SP Build No – 7.1.2.0.0.3-0
Avaya Aura® Experience Portal	7.2.0.0.1204
Avaya Proactive Outreach Manager	POM.03.01.00.00.01.018
Avaya G430 Gateway	38.20.1/1
Avaya 9611G Series Deskphone	96x1 H323 Release 6.6229
Avaya 9641G Series Deskphone	96x1 SIP Release 6.6229
CCT Deutschland GmbH ContactPro - Client Agent Desktop	V5.0.0.900

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
  Async. Transfer Mode (ATM) Trunking? n   Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                            DS1 MSP? y
                                 ATMS? y        DS1 Echo Cancellation? y
                   Attendant Vectoring? y
```

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 (**AES701678**).

```
display node-names ip                                        Page   1 of   2
                            IP NODE NAMES
    Name              IP Address
SM100             10.10.40.34
AES701678         10.10.16.78
default           0.0.0.0
g430              10.10.40.15
procr             10.10.16.27
```

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      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** 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       Password        Enabled   Status
                 Server
     1:          AES701678         ********           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: 8279999
     Type: ADJ-IP
                                                                     COR: 1
     Name: AESlink1
```

5.2. Configure an Agent in Communication Manager

The ContactPro Client requires an agent login on the Communication Manager. In this document it is assumed that an extension capable of allow and agent login has been configured already.

5.2.1. Add Hunt Group

To add a new skillset or hunt group, type **add hunt-group x,** where x is the new hunt group number. For example, the hunt group **10** is added for the **POMSkill** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also that **Group Type** is set to **ucd-mia**.

```
add hunt-group 10                                        Page   1 of   4
                              HUNT GROUP

           Group Number: 10                              ACD? y
             Group Name: POMSkill                       Queue? y
          Group Extension: 8273010                      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
```

5.2.2. 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 8271001                                      Page   1 of   3
                              AGENT LOGINID

                Login ID: 8271001                             AAS? n
                    Name: Agent1                            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 **10** is added to this agent so as when a call for "CoBrowse" is initiated the call is routed correctly to this agent.

```
add agent-loginID 8271001                                    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: 10      1       16:                31:                46:
 2:                 17:                32:                47:
 3:                 18:                33:                48:
 4:                 19:                34:                49:
 5:                 20:                35:                50:
 6:                 21:                36:                51:
 7:                 22:                37:                52:
 8:                 23:                38:                53:
 9:                 24:                39:                54:
10:                 25:                40:                55:
11:                 26:                41:                56:
12:                 27:                42:                57:
13:                 28:                43:                58:
14:                 29:                44:                59:
15:                 30:                45:                60:
```

5.3. 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.
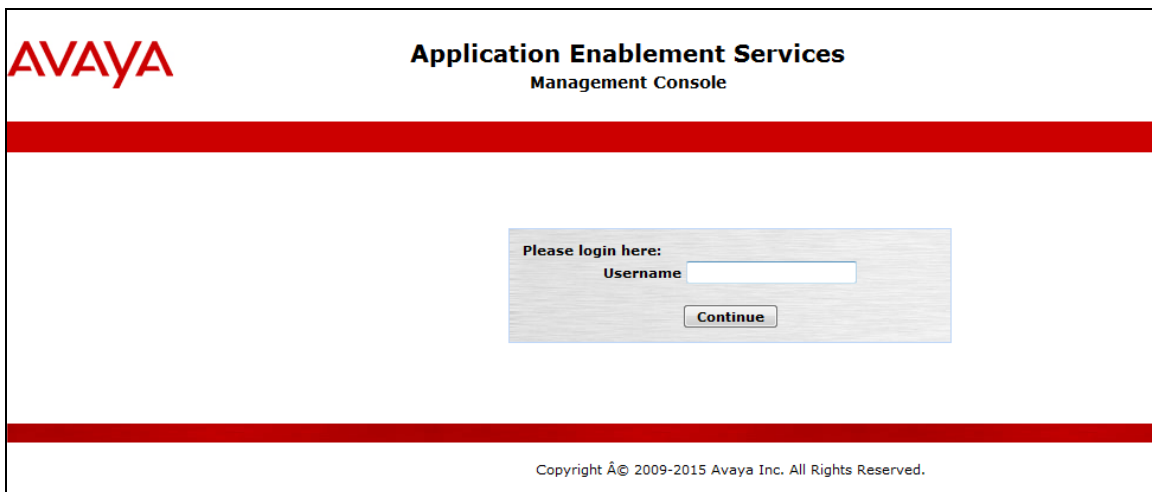
6. Configure Avaya Aura® Application Enablement Services Server

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 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.

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.

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.

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button. 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/Edit Name or IP** button.

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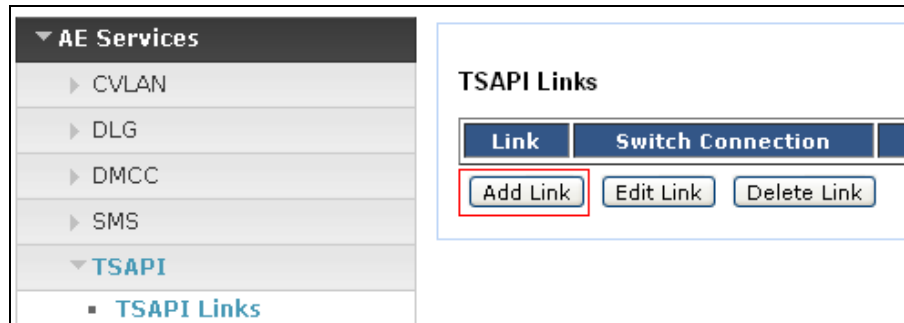
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM1627**, 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 **5**.
- **Security:** This was changed to **both** for compliance testing.

Once completed, select **Apply Changes**.
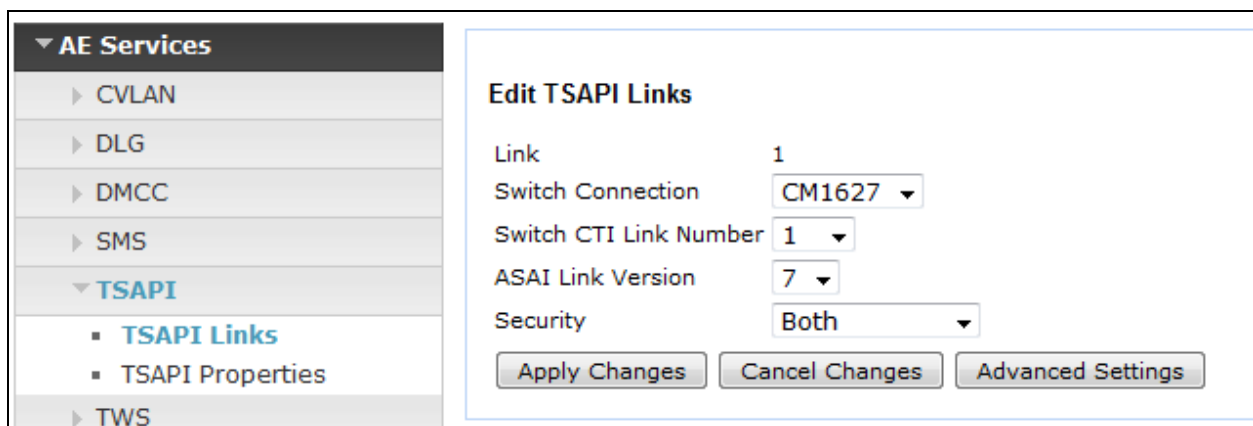
Another screen appears for confirmation of the changes made. Choose **Apply**.
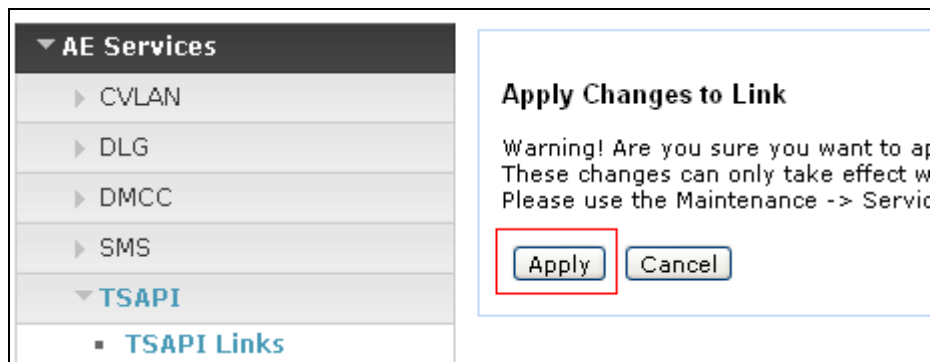
When the TSAPI Link is completed, it resembles the screen below.
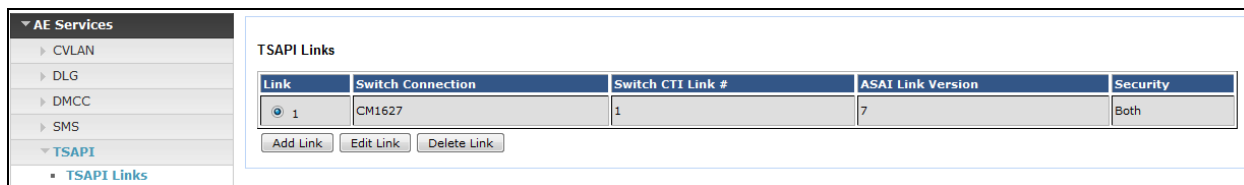
The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.
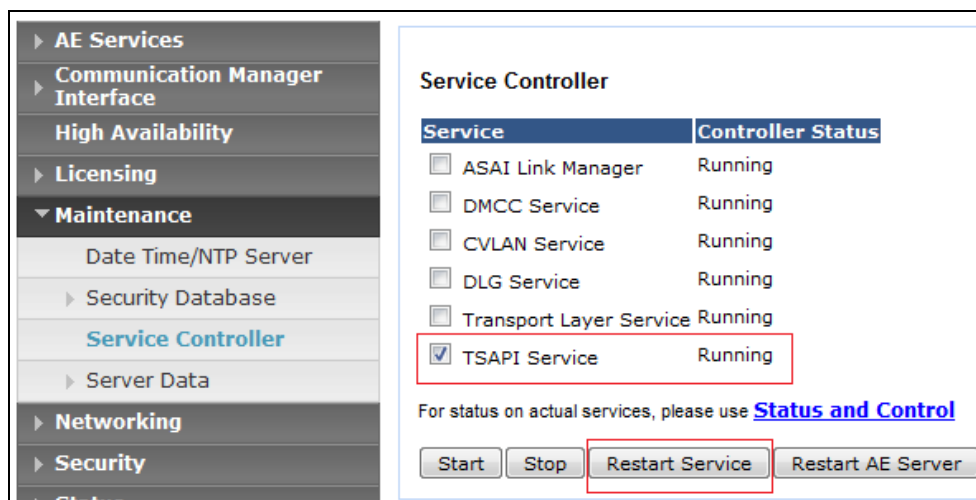
6.4. Identify Tlinks

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

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.

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.
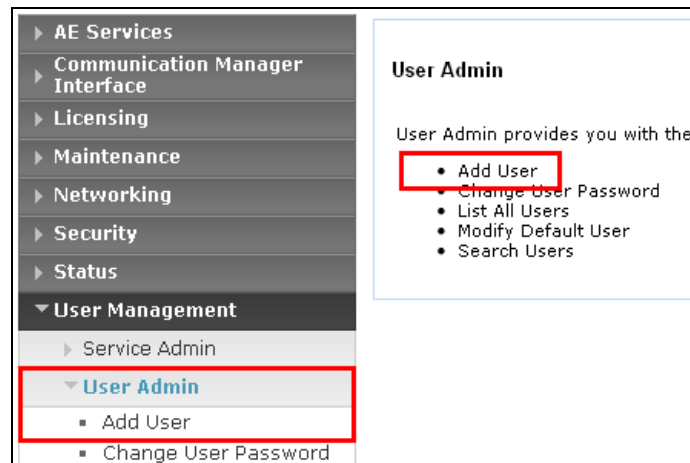
In the **Add User** screen shown below, enter the following values:
- **User Id -** This will be used by the ContactPro setup in **Section 8.1**.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with the **PrimaryAESLogin&Password** 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).

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

SJW; Reviewed:
SPOC 4/9/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
19 of 50
ConPro_POM31

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**.

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 11** *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*. Click on **Apply Changes** to complete the setup.

7. Configure Proactive Outreach Manager campaign

This section will describe the steps required to create a basic outbound campaign in POM.

From the left hand menu, select POM → POM Home. Under **Campaigns,** select **Campaign Manager**.

In Campaign Manager, click on **Add** to create the new campaign.
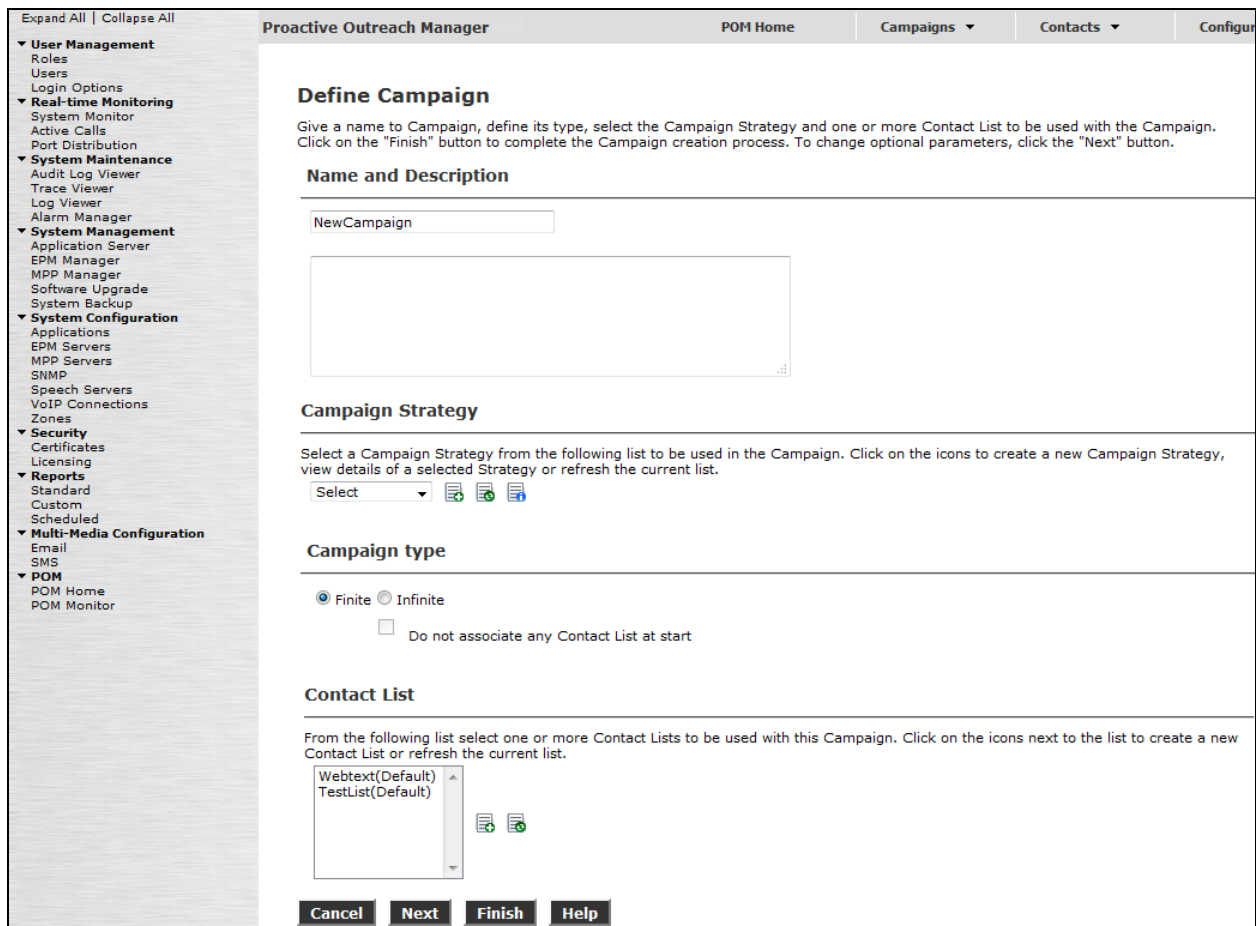
SJW; Reviewed:
SPOC 4/9/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

21 of 50
ConPro_POM31

On the **Add a Campaign** screen, Enter the **Name** and click on **Continue**.

The Campaign must now be defined and a **Campaign Strategy** and **Contact List** must be created.

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

7.1. **Create Campaign Strategy**

First, under Campaign Strategy, click on the add icon to bring up the Campaign Strategy Editor.
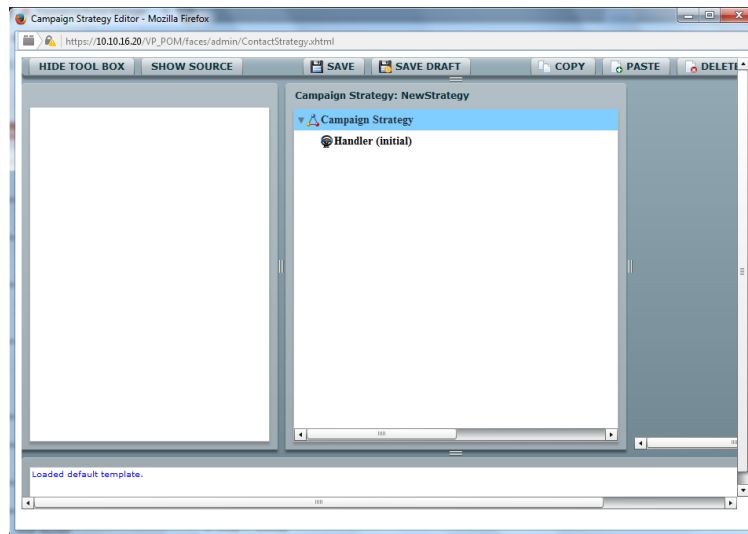
From the **Selected Node: Handler** box while Handler is selected under **Campaign Strategy:** drag and drop the **Call** node into the Campaign Strategy box
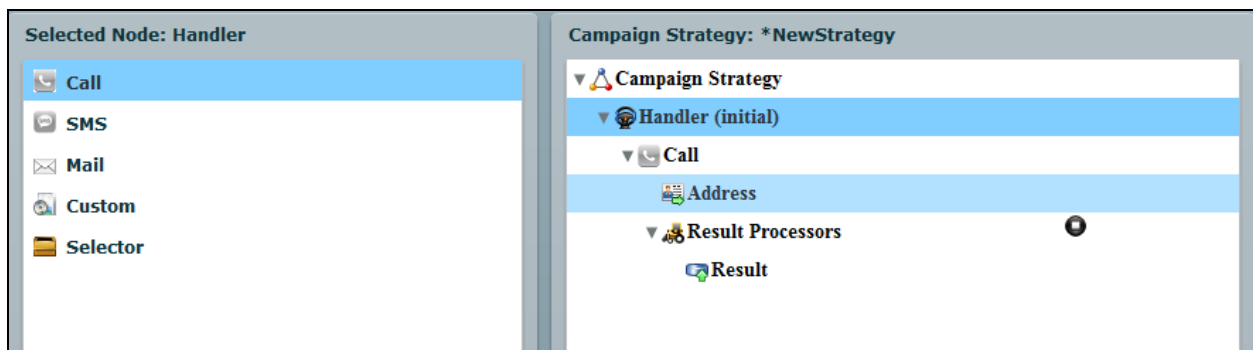
Select the **Call** node in the **Campaign Strategy:** Box and Enter a Name. This will change the Name of the node in the **Campaign Stragtegy:** box. Select the **APPLICATIONS** from the drop down menus and Set the **PACING PARAMETERS** (In this example a Preview Campaign has been selected).

Property	Value
Name	Outbound
Description	Outbound Calling
Sender's Display Name	CCT
Sender's Address	
Timeout (sec)	
Guard Times	Disable
Min Contact Time	
Max Contact Time	
Re-check Interval (min)	
On Media Server Failure	
Enhanced CCA	ON
Priority	5
Allocation Type	Dynamic
APPLICATIONS	
Driver Application	PomDriverApp
Nailer Application	Nailer
Nuisance Call Application	AvayaPOMAnnouncement
On Hold Application	AvayaPOMAnnouncement
PACING PARAMETERS	
Call Pacing Type	Preview
Timed Preview	Yes
Preview Time (Sec)	
Can Cancel Preview	Disable
Min. Agents	1
Max. Agents	10
Agent Outbound Skill	POMOut
ACW Time (Sec)	10
# of ACW extensions	
Default Completion code	NoReply

Campaign Strategy: *NewStrategy

▼ Campaign Strategy
  ▼ Handler (initial)
    ▼ Outbound
      Address
      ▼ Result Processors
        Result

From the **Campaign Strategy:** box select **Result (Call Answered)** and from the Selected Node: box drag the **Agent** node into the Campaign Strategy box.
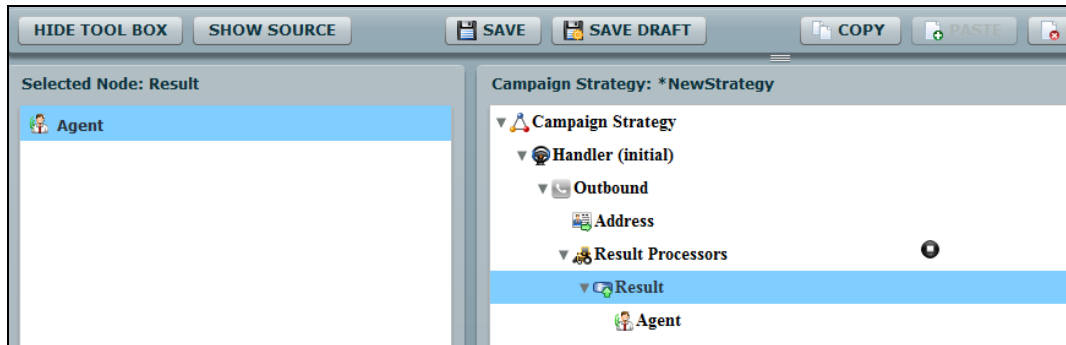
Select the **Agent** node in the **Campaign Strategy** box. Enter a **Name** and select an **Agent Script** from the Drop-down text field.
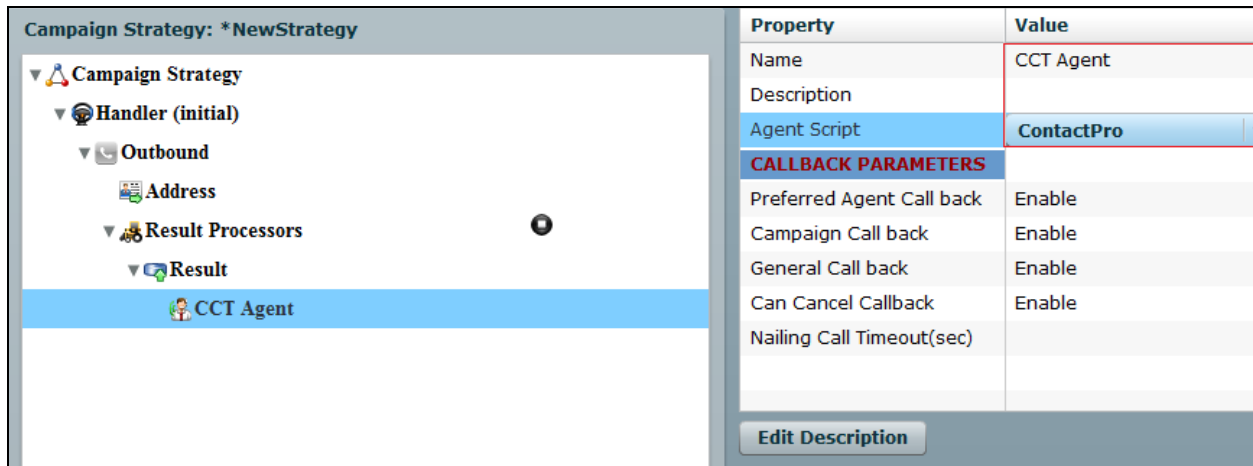
Click on **Save** when complete. A confirmation message will be displayed in the bottom left corner (not shown) and the **Campaign Strategy Editor** window can be closed.
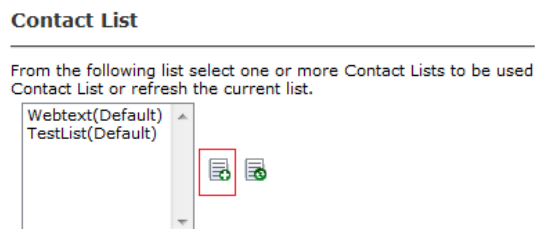

7.2. Create Contacts list

Before creating the Contacts list for the campaign a list of contact must be created as a comma delimited .csv file in the following format. For simple SMS messages, no further information is required.

```
id,firstname,lastname,phonenumber2,phonenumber1,email
1,Contact,One, 12125550100, 12125550100,contact1@avaya.com
2,Mobile,One, 12125550101, 12125550101,mobile1@cct.com
3,Bob,Dylan, 12125550102, 12125550102,bobby@hotmail.com
4,SMS,One, 12125550103, 12125550103,SMS@avaya.com
```

From the Define Campaign (not shown) screen under **Contact List,** click on the add icon

Give the Contacts list a **Name** and click on Save.

SJW; Reviewed:
SPOC 4/9/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
26 of 50
ConPro_POM31

Now upload the contacts in the .csv file created. Click on **Upload Contacts now.**
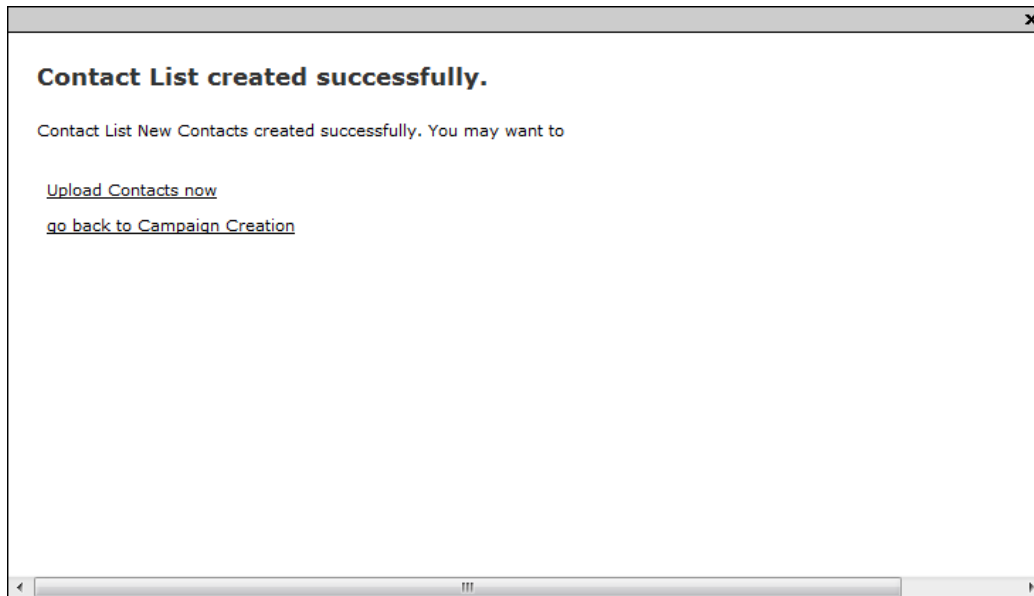
Click on **File to upload** and select the .csv file created. Select **Automatically update time zone for phone numbers**. Click on Continue to upload the contacts and go back to the Define Campaign screen.
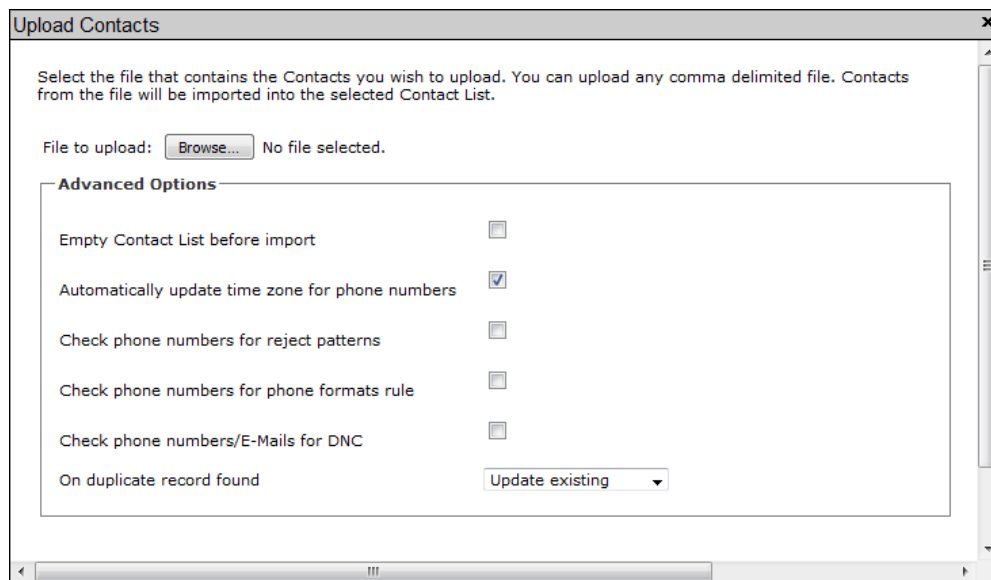
7.3. Complete the Campaign Creation

In this section the campaign creation is completed. Only screens where changes need to be made are mentioned and otherwise just clicking **Next** to move to the next screen is sufficient.

On the **Media Servers and Media Specific Parameters** screen, check that the EPM Zone is selected and then click **Next**.

On **The Completion Code Association** screen, move all **Available** Completion Codes to **Selected**. Click on **Next** to continue.

SJW; Reviewed:
SPOC 4/9/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

28 of 50
ConPro_POM31

Finally, on **Processing Parameters,** click on **Finish** to save the campaign.

Processing Parameters (optional)

Define actions to be taken after a Campaign is finished or stopped and miscellaneous Campaign processing parameters.

Export Data

Export Contacts on completion ☐

Custom Post Processing

Enter the fully resolved class Name (e.g com.avaya.pom.custom.myPostProcessor) implementing the custom post processing interface.

Campaign post processor class

[   ]

Miscellaneous

Batch size decides the number of records that Campaign Manager will fetch from database for processing in a single batch.

Batch size

[600   ]

[Cancel] [Previous] [Finish] [Help]

8. Configure CCT ContactPro

This section outlines the steps required to configure ContactPro.

8.1. Create CCT ContactPro Database and User

A database and database user for CCT ContactPro must be created on an SQL server.

8.1.1. Create Database

To create the CONTACTPRO database, open the provided **CONTACTPRO MsSql Schema.sql** script.
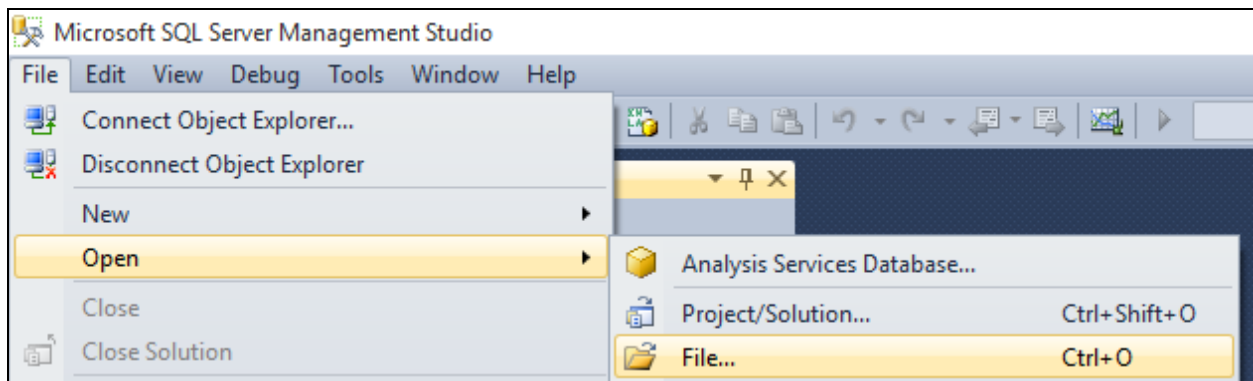
Execute the script by clicking the **Execute** button.

SJW; Reviewed:
SPOC 4/9/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
30 of 50
ConPro_POM31
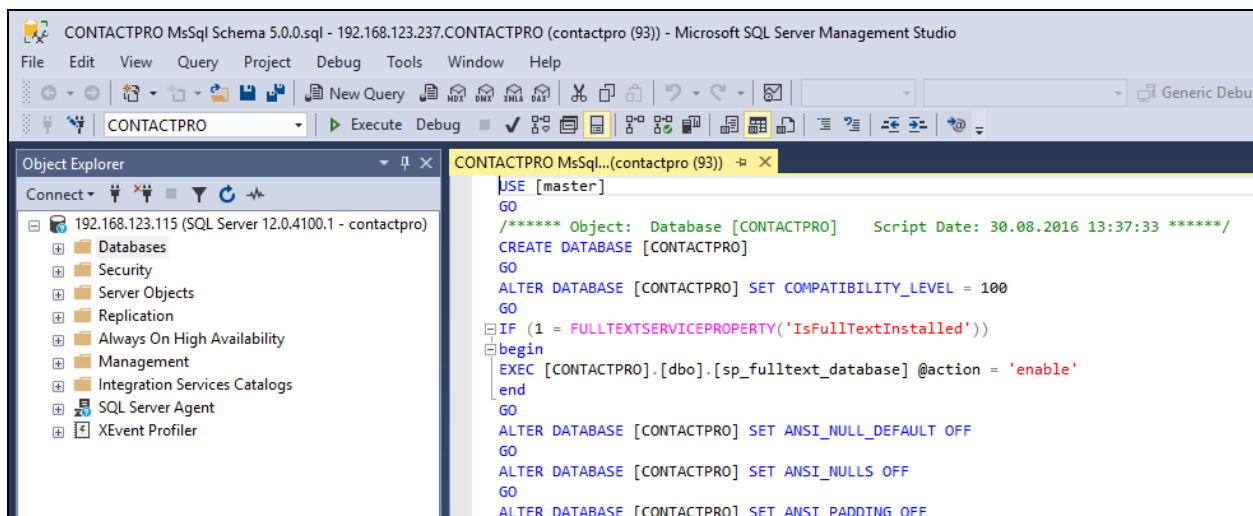
The following shows the script has been successfully executed to create the database.
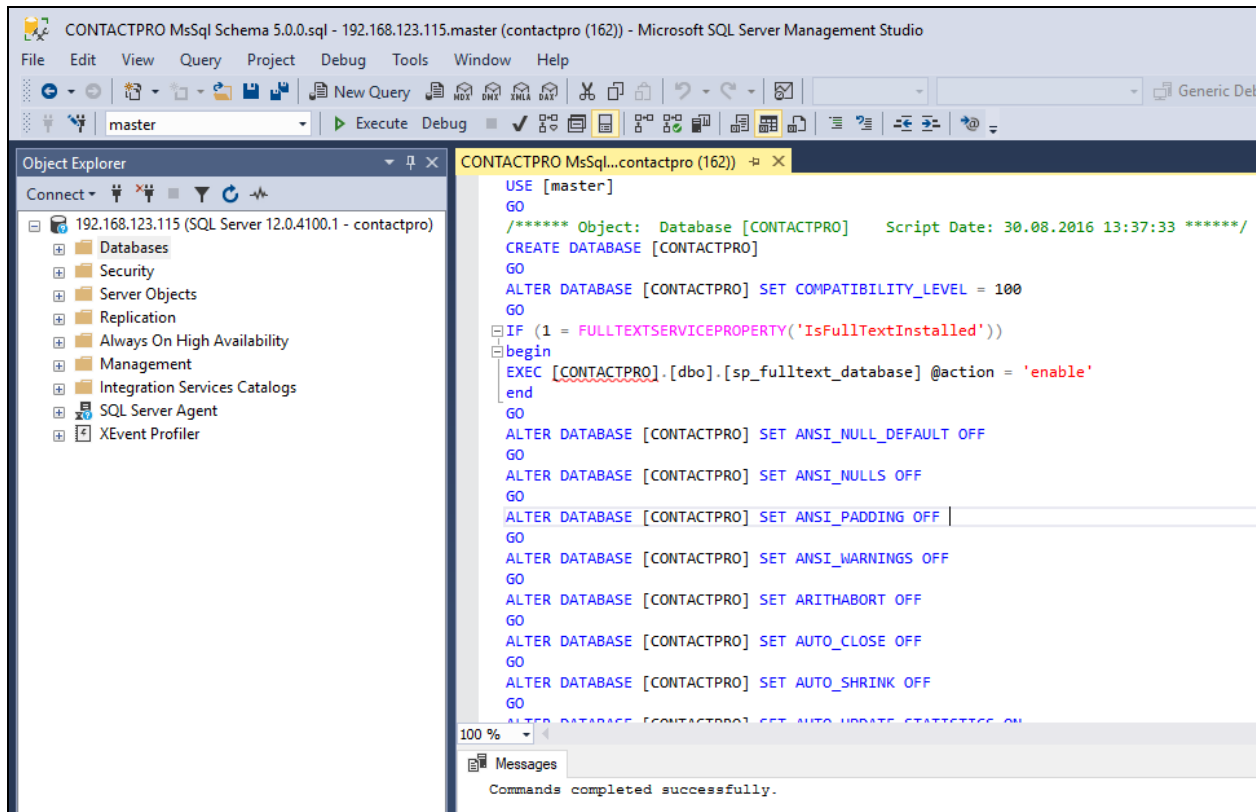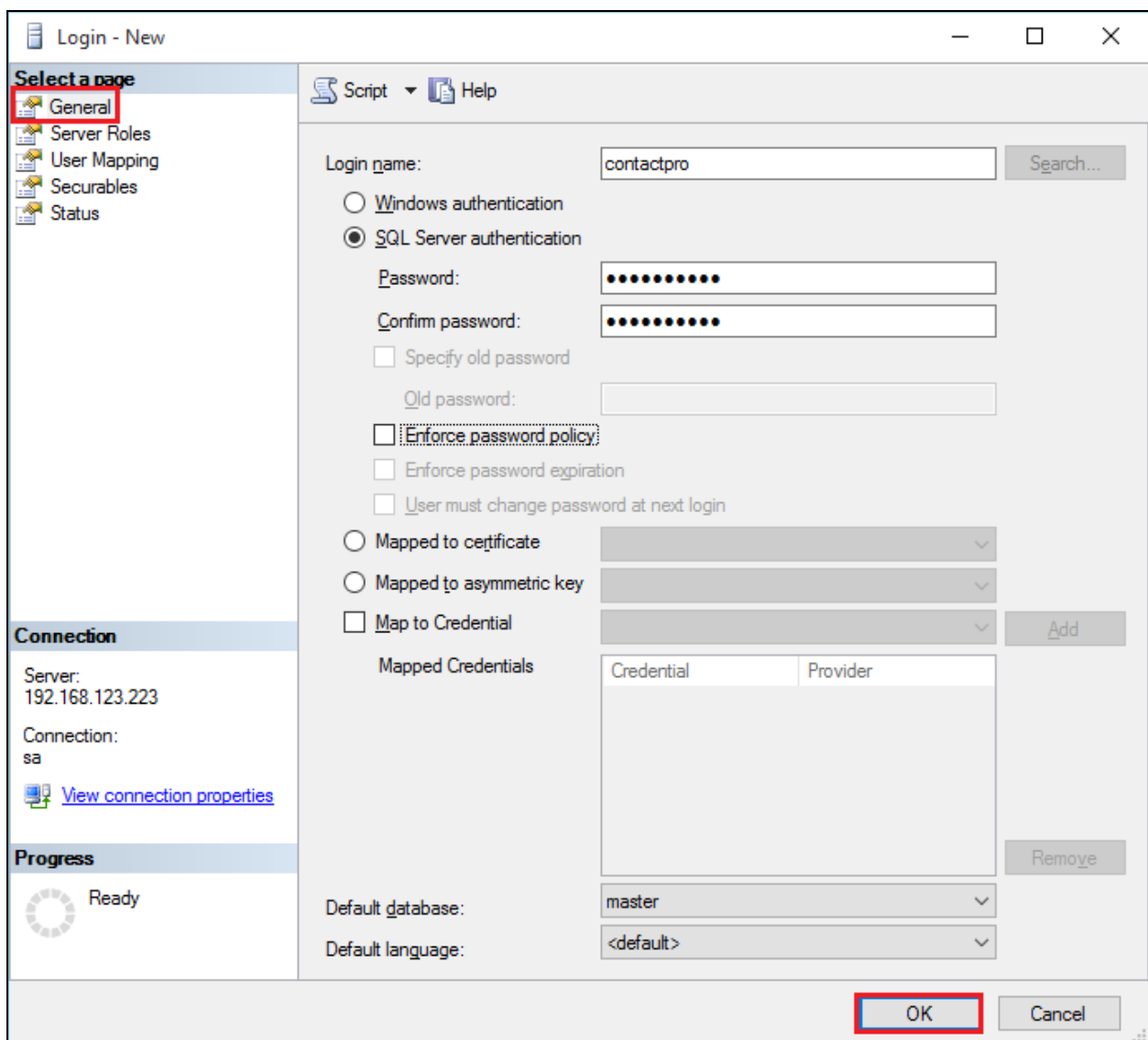
8.1.2. Create User

Create a database user named **contactpro**. Right-click on **Login** and click on **New Login**.
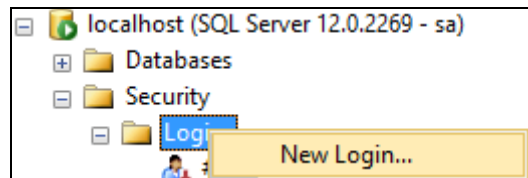
Click on the **General** option in the left pane, enter the **Login name,** click on **SQL Server authentication,** and enter a suitable **Password** for the **contactpro** user. Click on **OK** at the bottom of the screen once done.

Click on **User Mapping** in the left window. For this user, grant public and **db_owner** access to the **CONTACTPRO** database. Click on **OK** at the bottom of the page once done.
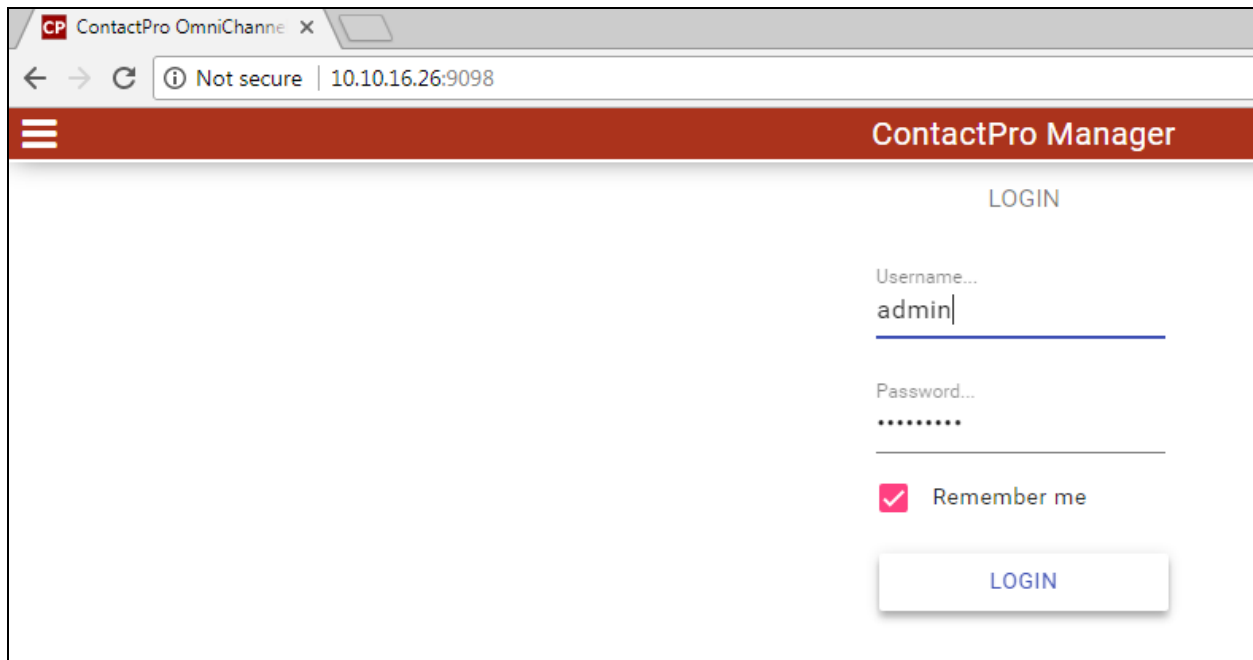
SJW; Reviewed:
SPOC 4/9/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
33 of 50
ConPro_POM31
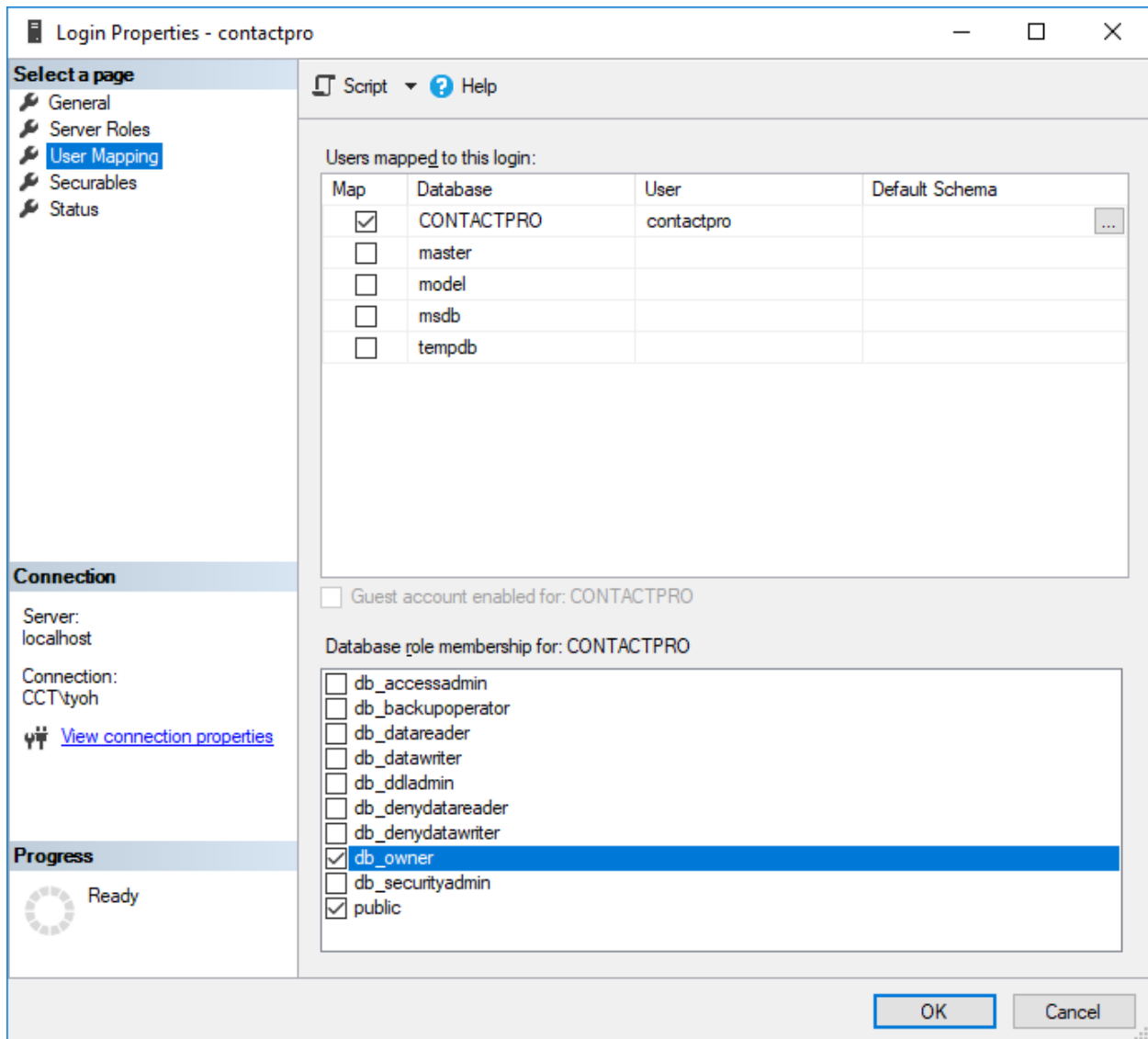
8.2. Configure Properties with ContactPro Manager

The ContactPro Manager allows the configuration of all properties for ContactPro. 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 POM server. All other properties may be left at their default values.

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

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

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.

Name	Value
AESProtocolVersion	6.3.3
PrimaryAESACMConnectionName	CM71vmpg
PrimaryAESIPAddress	10.10.40.43
PrimaryAESLoginPassword	*
PrimaryAESLoginUsername	cct
PrimaryAESPort	4721
PrimaryAESSecureSocket	No
QuaternaryAESACMConnectionName	
QuaternaryAESIPAddress	
QuaternaryAESLoginPassword	*
QuaternaryAESLoginUsername	
QuaternaryAESPort	4721
QuaternaryAESSecureSocket	No
SecondaryAESACMConnectionName	
SecondaryAESIPAddress	
SecondaryAESLoginPassword	*
SecondaryAESLoginUsername	
SecondaryAESPort	4721
SecondaryAESSecureSocket	No
TertiaryAESACMConnectionName	
TertiaryAESIPAddress	
TertiaryAESLoginPassword	*
TertiaryAESLoginUsername	
TertiaryAESPort	4721
TertiaryAESSecureSocket	No

Left navigation panel:

```
[Gateway]
ACM
ACMGateway
ACRBridge
ActiveDirectory
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/AvgHandleTimeThreshHold
AgentStatistics/LiveCallThreshHolds
ApplicationHost
ApplicationHost/Logging
CallLog
CoBrowse
ContextData
ContextDataViewer
CPRouting
CustomerFeedback
DataExchangeServer
DialingRules
DialingRules/BlockedNumbers
EMC/Database
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.

8.2.2. Configure the Connection to POM

In the **POM** section **,** the information highlighted below must all be filled in where applicable. This information is all required to connect successfully to the POM and each part is changed by double-clicking on the field that needs to be changed.

Name	Value
EnableAddToDNC	Yes
EnableBlending	Yes
EnableConsultDecline	Yes
EnableCountryCode	No
EnableWrapUpDuringCall	No
EnableWrapUpOnTransfer	Yes
FullyLogoutFromPOMWhenPOMButtonIsPressedWhileLoggedIn	Yes
MaxRedialCount	10
NailupCallCLID	96789
OutsideLineNumber	
POMAUXReasonCode	
Servers	192.168.123.210:9970
UseDatabaseQueries	No
Zone	Default

Search Sections...

EMCCallDetailReporting
EMCChat
EMCCore
EMCEmail
EMCEmailManagement
EMCHistoryViewer
EMCPrivateWorkList
EMCWrapUp
Help
IPOCC
IPOCC/KeyboardShortcut
KB
KeyboardShortcuts
KeyboardShortcuts/HotKeys
LicenseServer
Login
Login/Login
Manager
MSCRM/Screenpop/Chat
MSCRM/Screenpop/Email
MSCRM/Screenpop/General
MSCRM/Screenpop/MultipleMatch
MSCRM/Screenpop/Voice
MSCRM/Server
PCICompliance
PhoneBook
POM
POM/Callback
POM/CloseInbound
POM/Database
POM/DeleteFromCallList
POM/WebService/POMAgentAPIService
POM/WrapUp

To change the POM IP address, double-click on the **Connections** field highlighted below to bring up an edit window where a new IP address and port separated by colon can be entered and click **OK** once this is done.

Continue with the other POM information that is highlighted below to conclude the setup for POM.

Name	▲	Value
EnableAddToDNC		Yes
EnableBlending		Yes
EnableConsultDecline		Yes
EnableCountryCode		No
EnableWrapUpDuringCall		No
EnableWrapUpOnTransfer		Yes
FullyLogoutFromPOMWhenPOMButtonIsPressedWhileLoggedIn		Yes
MaxRedialCount		10
NailupCallCLID		96789
OutsideLineNumber		
POMAUXReasonCode		
Servers		192.168.123.210:9970
UseDatabaseQueries		No
Zone		Default

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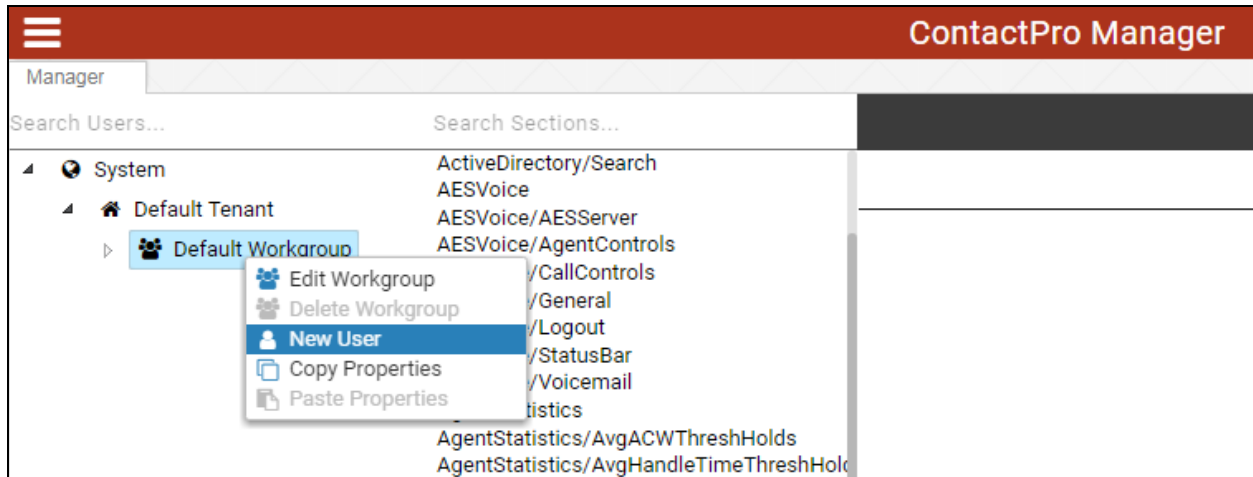
The following fields are required.
- **LoginName** (This is the Agent ID such as that created in **Section 5.2.4** for example).
- **First Name**
- **Last Name**

Employees under different workgroups in different tenants may also be created. This allows easy management of different Properties for different **Tenants** or **Workgroups** or each individual **Employee**.

Note: Properties do not need to be duplicated. The only configuration required is what's different compared to the upper level which could be either the **Top System Level**, **Tenant** or **Workgroup** level.

9. Verification Steps

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

9.1. Verify Status of Communication Manager Agent

Enter the command **list agent-loginID** verify that your agent is logged-in to your extension.

```
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

8271001      Agent 1        8270001                              1   lvl
               10/01            /       /       /       /       /       /
8271002      Agent 2        8270002                              1   lvl
               10/01            /       /       /       /       /       /
```

Enter the command **status station** 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 8270001                                        Page   7 of   7
                             ACD STATUS

 Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod
   10/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     Version     Mnt     AE Services     Service       Msgs     Msgs
Link                Busy    Server          State         Sent     Rcvd

1       4           no      AES701678       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**.

9.4. Verify ContactPro

9.4.1. 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 ContactPro application.
- **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 **ContactPro**.

SJW; Reviewed:
SPOC 4/9/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
43 of 50
ConPro_POM31

9.4.2. 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 (**5009**) and Agent ID (**5321**) once logged in. Log into the desired multimedia channels by clicking any of the **Email**, **WebChat** or **Outbound** buttons on the top left. Click on **Ready** to make the agent ready.

A web request is generated by a customer (not shown) and queued to this agent. Once Ready is pressed above the call appears as **Alerting** on the ContactPro desktop. The call can be answered by pressing the **Answer** icon highlighted below.
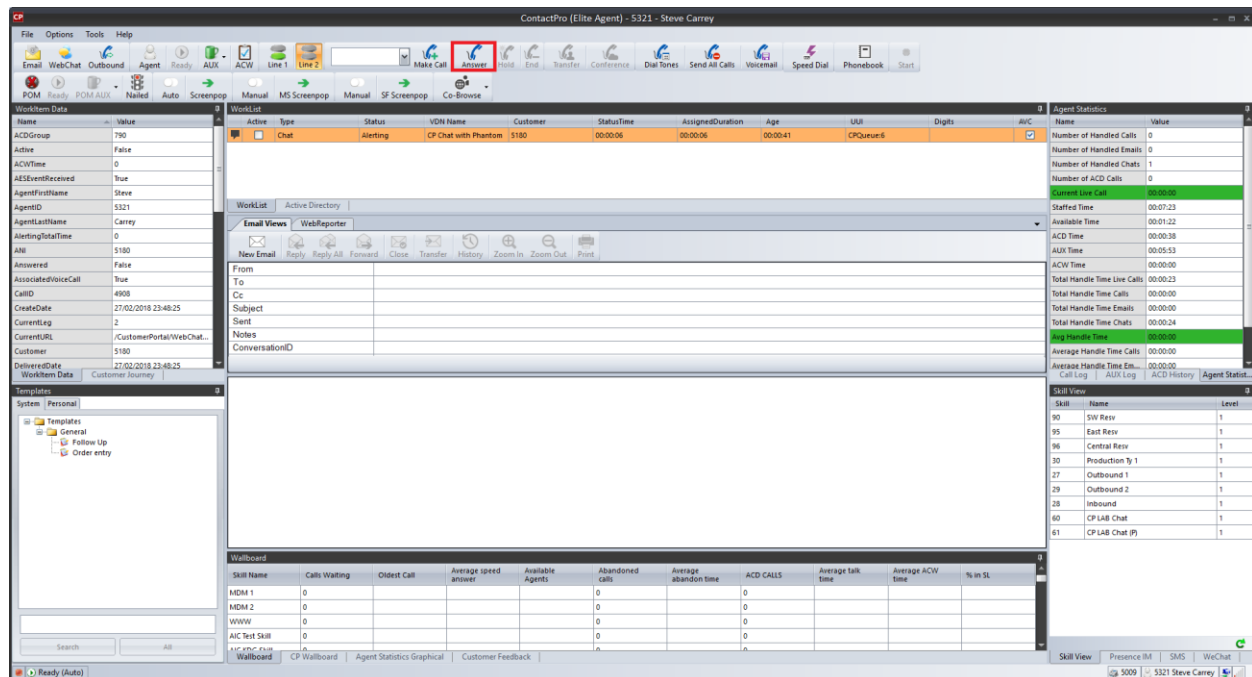
Once the call is answered a tab is opened showing the web chat request from the customer and the agent can respond to that request as is shown below, by entering some text and clicking **Send**. Also, verify that the line is busy indicating the agent is on a call even if this is a multimedia call.
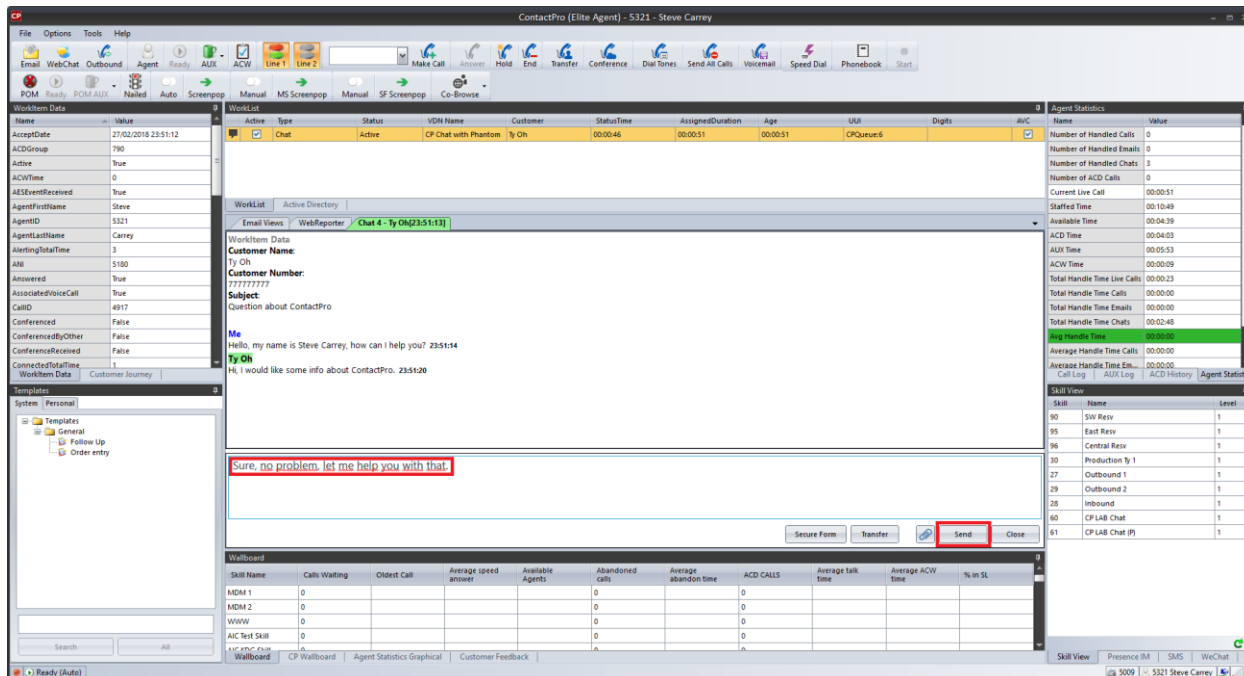
The agent can hang up or close the chat by clicking on **Close** button at the bottom right.
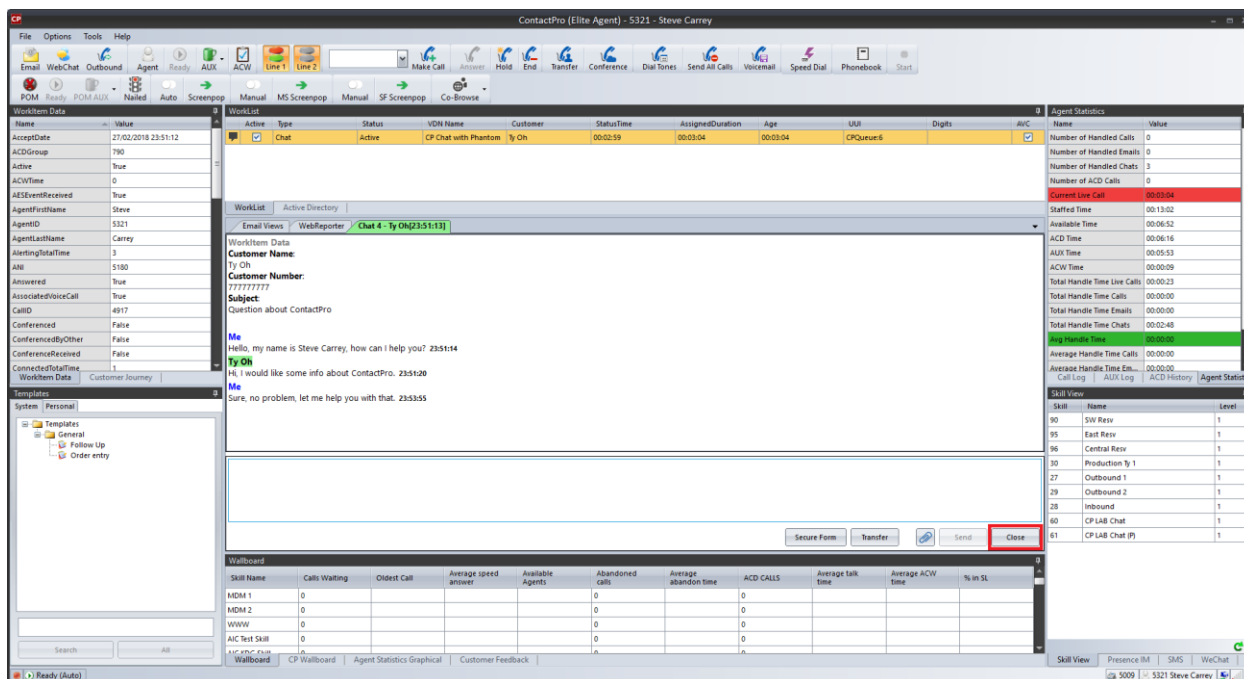
With the chat ended, a new call can be made if required again by entering the digits and pressing on **Make Call** as is shown. In this example, the agent is calling the customer at his/her request from the webchat session previous.
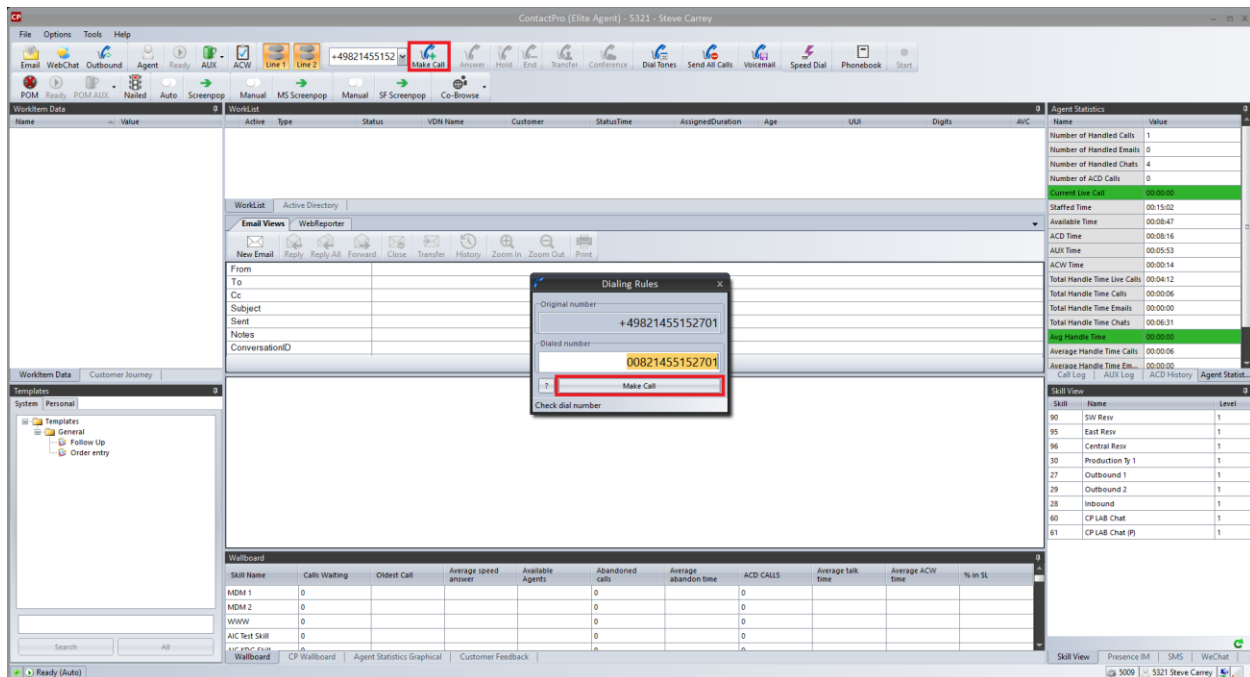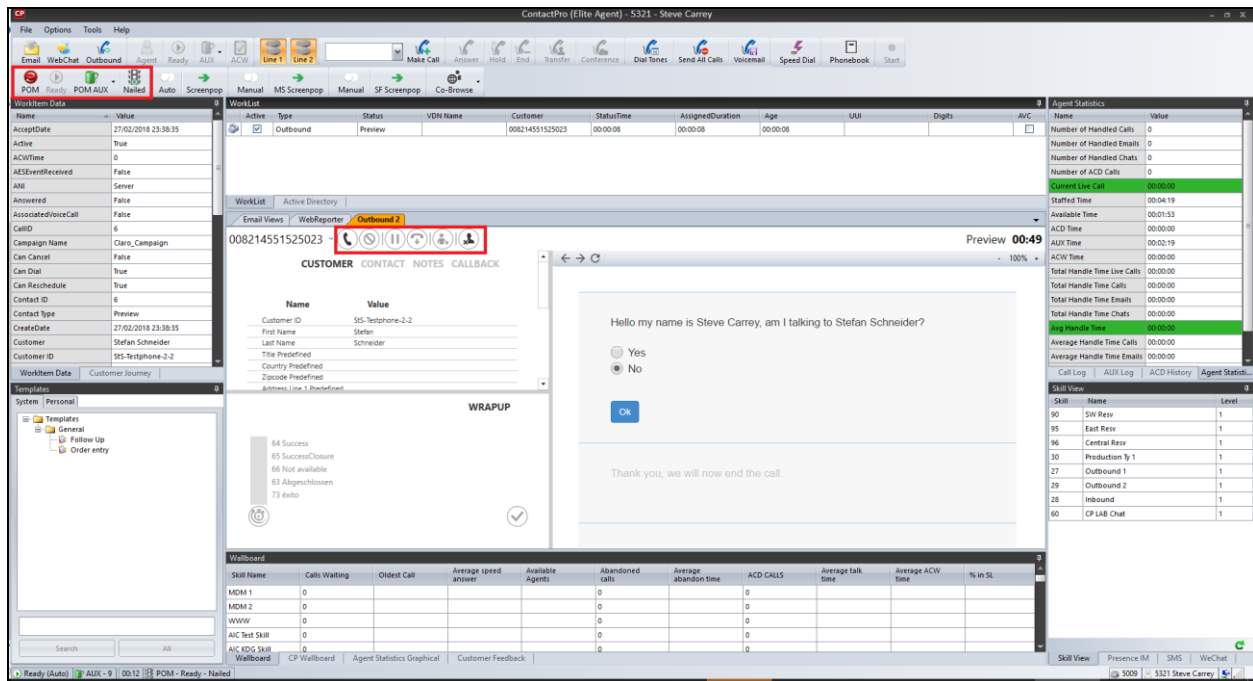

9.4.3. Verify POM status in ContactPro

Click on the **POM** button to login to POM, then click on the **Ready** button. Now check the Nailed status (traffic light icon). The Ready button X should disappear, the Nailed status depends on the POM settings:

- Red: No Outbound skill assigned or no campaign active
- Yellow: Pending, no active campaign
- Green: Nailup Call active and connected to a campaign

The agent will then receive a POM outbound work item. A new outbound tab is created with details of the customer. You can perform POM call actions using the call control buttons inside the tab. You can also follow campaign scripts.

At the end of the call, select a wrap up code.

10. Conclusion

These Application Notes describe the configuration steps required for ContactPro from CCT Deutschland GmbH to interoperate with Avaya Avaya Aura® Application Enablement Services R7.1 and Avaya Proactive Outreach Manager (POM). 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 Deutschland GmbH product documentation that are relevant to these Application Notes.

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

[1] *Administering Avaya Aura® Communication Manager,* Release 7.1.2, Issue 5, February 2018
[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 7.1*
[4] *Avaya Aura® Experience Portal 7.2 Overview and Specification*
[5] *Deploying Avaya Aura® Experience Portal 7.2 in an Avaya Customer Experience Virtualized Environment*
[6] *Proactive Outreach Manager 3.1 Overview and Specification*
[7] *Implementing Proactive Outreach Manager 3.1*
[8] *Application Notes for configuring ContactPro from CCT Deutschland GmbH with Avaya Aura® Application Enablement Services R7.1*
[9] *Application Notes for configuring Avaya Aura® Communication Manager R6.3, Avaya Aura® Application Enablement Services R7.0 and Avaya Interaction Center R7.3 with CCT ContactPro v5*

The following CCT 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.