**Avaya Solution & Interoperability Test Lab**

# Application Notes for configuring ContactPro from CCT Deutschland GmbH with Avaya Co-Browsing Snap-In 3.0 and Avaya Engagement Development Platform 3.1 - Issue 1.0

## Abstract


These Application Notes describe the configuration steps required for ContactPro from CCT Deutschland GmbH to interoperate with Avaya Co-Browsing Snap-In and Avaya Engagement Development Platform. ContactPro is an interaction management application that connects to Avaya Aura® Call Center Elite Multichannel using Avaya Aura® Application Enablement Services for call control.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for ContactPro from CCT Deutschland GmbH, to interoperate with Avaya Co-Browsing Snap-In 3.0 and Avaya Engagement Development Platform 3.1.1. The CCT ContactPro solutions offer a variety of integrations into the Avaya call center environment supporting different Avaya platforms, to interact for multimedia agents as well as for voice only agents.

ContactPro offers a connection to Avaya Aura® Call Center Elite multichannel using CCT ContactPro EMC, Avaya Interaction Center using CCT ContactPro AIC and Avaya Application Enablement Server (AES) using ContactPro Elite Voice. The connection to Avaya Engagement Platform CoBrowse Snap-in although is common to all desktops use the same interface to display the CoBrowse features. These Application Notes will go through the setup and configuration for both CCT ContactPro EMC and CCT ContactPro AIC to connect to Avaya Engagement Development Platform EDP Snap-in.

CCT ContactPro EMC offers a lightweight multi-channel agent desktop replacement for the current Avaya EMC solution. All EMC channels (Voice, Chat and Email) are unified into one convenient desktop that reflects the customer being interacted with and the channel being used. Its Multi-Channel capabilities ensure quick, effective and simultaneous management of multiple customers across all EMC channels. For more information on the setup and configuration of ContactPro EMC please refer to the Application Notes titled, *Application Notes for configuring ContactPro EMC from CCT Deutschland GmbH with Avaya Aura® Call Center Elite Multichannel R6.4.1 and Avaya Aura® Application Enablement Services R7.0*.

CCT ContactPro IC is an interaction management application for Avaya Interaction Center. It is used as an alternative to and expands on the features provided by Avaya Agent Rich Client and provides a flexible and modular client solution for a multi-channel contact center. CCT ContactPro can be customized for each customer according to requirements. From more information on the setup and configuration of ContactPro IC please refer to the Application Notes titled, *Application Notes for configuring Avaya Aura® Communication Manager R7.0, Avaya Aura® Application Enablement Services R7.0 and Avaya Interaction Center R7.3 with CCT ContactPro v3*.

# 2. General Test Approach and Test Results

The general test approach was to validate successful creation of Co-Browsing sessions between an agent logged into the ContactPro client and a customer. This was performed by creating a Co-Browsing Session and providing a URL for the customer to join the session. When the Session was established the agent can observe and take control of the customers browser.

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

## 2.1. Interoperability Compliance Testing

The testing focuses on the following areas:

- **Co-Broswing Session Creation** – Create a new Session from ContactPro client.
- **Join Co-Browsing Session** – Join a Session from ContactPro client..
- **Have the customer Browse to the provided URL** – Customer can see the Join Session pop up in the provided URL.
- **Have customer Join Co-Browsing Session** – Customer can join the session with a Session ID provided by the Agent.
- **Observe and Control the Session** – Observe and control a session from ContactPro client.

## 2.2. Test Results

All test cases passed successfully.

## 2.3. Support

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

**WEBSITE**
www.cct-solutions.com

**CONTACT**
Phone: +49 69 7191 4969 0
Email: contact@cct-solutions.com

**SUPPORT**
Hotline: +49 821 455152 455
Email: helpdesk@cct-solutions.com

**CCT Deutschland GmbH**
Street Heinrich-Hertz-Strasse 5
ZIP 60486
Frankfurt am Main
Germany
Phone +49 69 7191 4969 0
Fax +49 69 7191 4969 666

Kohlenstrasse 2
ZIP 04107
Leipzig
Germany
Phone +49 341 5909 1251

Street Am Eser 2
ZIP 86150 Augsburg
Germany
Phone +49 821 455 152 700
Fax +49 821 455 152 777

Street Werner-von-Siemens-Strasse 6
ZIP 86159
Augsburg
Germany

**CCT Europe GmbH**
Street Sumpfstrasse 26
ZIP 6312
Steinhausen
Switzerland
Phone. +41 41 748 42 22
Fax +41 41 748 42 23

**CCT Software LLC**

1735 Market Street STE 3750
19103 Philadelphia, PA
USA
office: +1 267 507 6196

2020 North Bayshore Drv. Appt. 2408
33137 Miami FL
United States of America
Phone. +1 844 720 3897

# 3. Reference Configuration

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

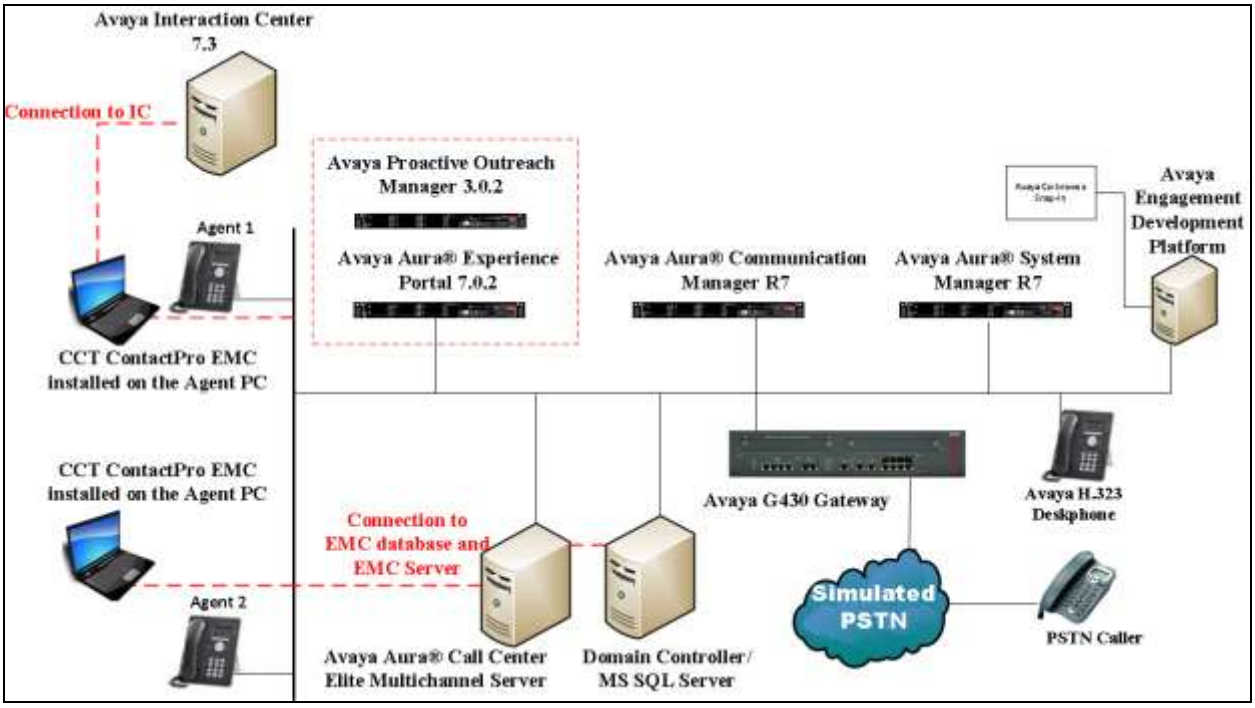



**Figure 1: Connection of CCT Deutschland GmbH ContactPro with Avaya Co-Browsing Snap-In and Avaya Engagement Development Platform.**

# 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 7.0 (SP1)<br>Build No. – 7.0.0.0.16266-7.0.9.7001011<br>Software Update Revision No:<br>7.0.0.1.4212 |
| Avaya Aura® Communication Manager running on a virtual server | R7.0 SP1<br>R017x.00.0.441.0<br>Updates:<br>00.0.441.0-22477<br>PLAT-rhel6.5-0010 |
| Avaya Aura® Session Manager running on a virtual server | Session Manager R7 SP1<br>Build No. – 7.0.0.1.700102 |
| Avaya Aura® Application Enablement Services running on a virtual server | R7.0<br>Build No – 7.0.0.0.0.13-0 |
| Avaya Aura® Call Center Elite Multichannel running on Virtual Server | R6.4.1 |
| Avaya Interaction Center | R7.3.4 |
| Avaya Co-Browsing Snap-In | R3.0.0.0.201 |
| Avaya G430 Gateway | 37.20.0 |
| Avaya 9611G Series Deskphone | 96x1 H323 Release 6.6.028 |
| Avaya 9641G Series Deskphone | 96x1 SIP Release 6.6.028 |
| CCT Deutschland GmbH ContactPro - Client Agent Desktop | V 3.5.2.340 |

# 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 12**.

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

## 5.1. Configure 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 (**aes63vmpg**).

```
display node-names ip                                          Page   1 of   2
                                IP NODE NAMES
    Name                IP Address
SM100               10.10.40.34
AES71678            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:        AES71678          ********          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: AES7 CTI
```

## 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 **CoBrowse** 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: CoBrowse                         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 10                                          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

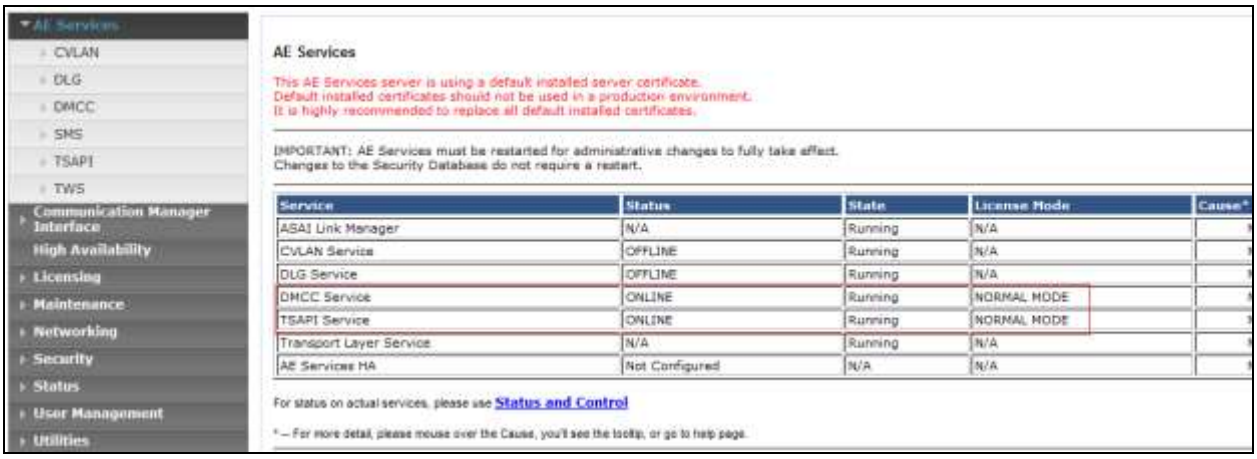
This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI & DMCC Ports
- Create CTI User
- Change Security setting for 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.

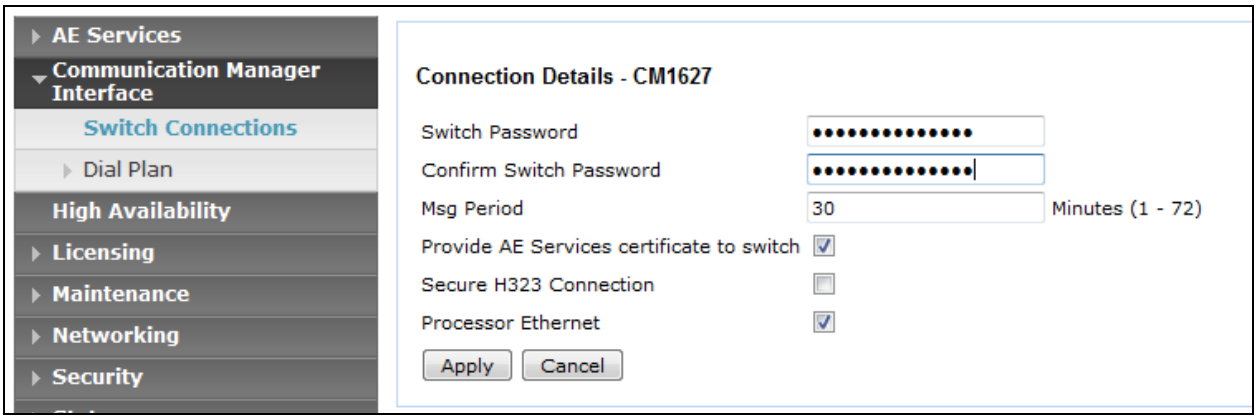
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL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



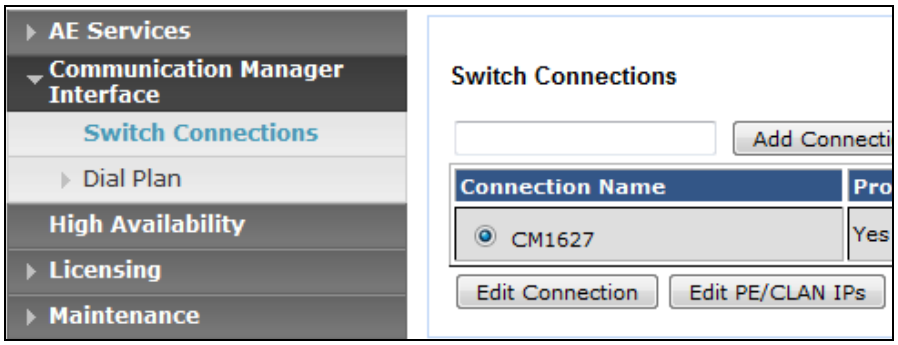

## 6.2. Create Switch Connection

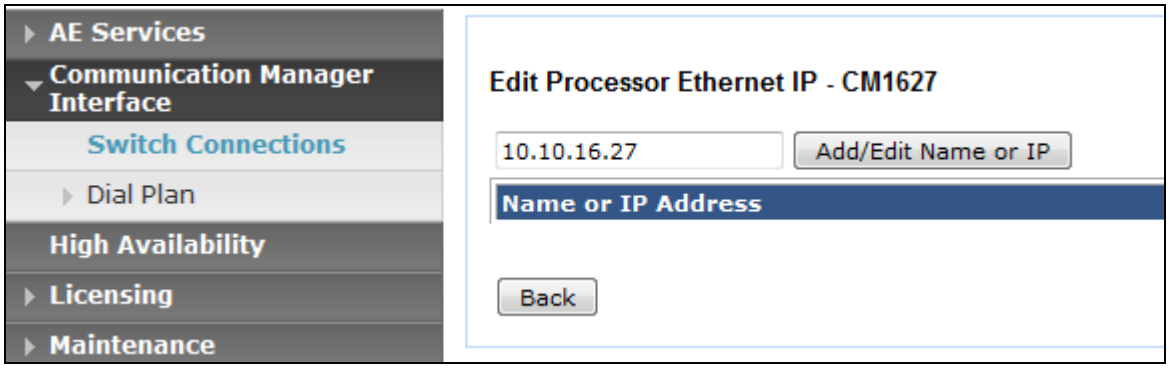
From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

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.



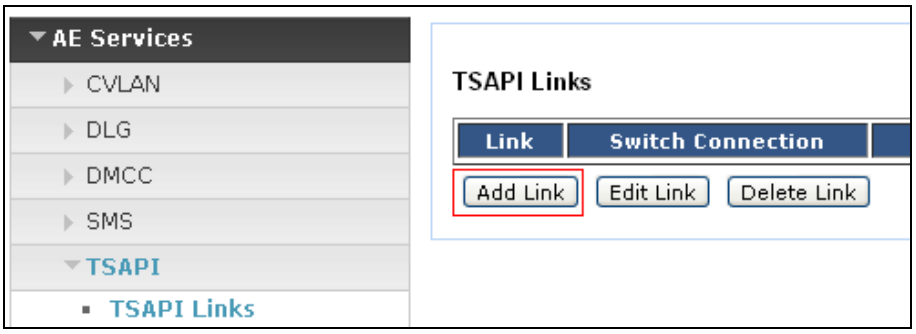

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button. In the resulting screen, enter the IP address of the procr as shown in **Section 5.1.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.



## 6.3. Administer TSAPI link

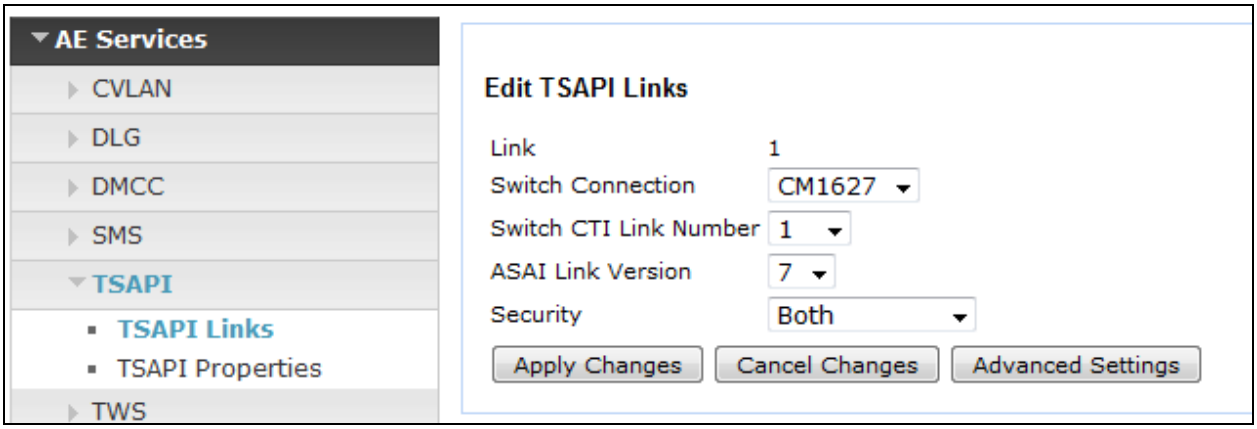
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



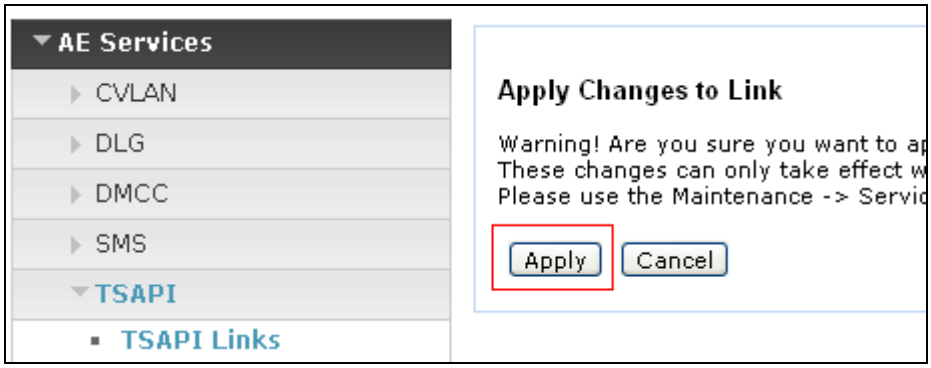

On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **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.

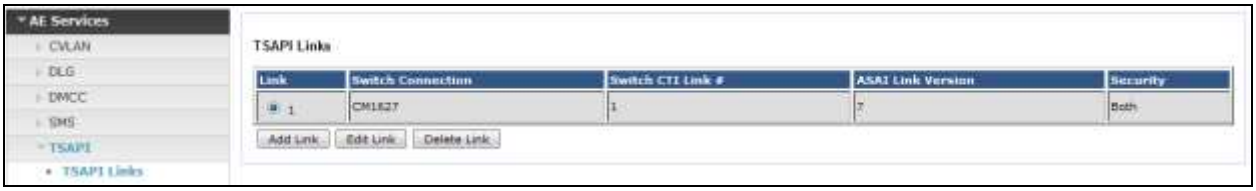
Once completed, select **Apply Changes**.



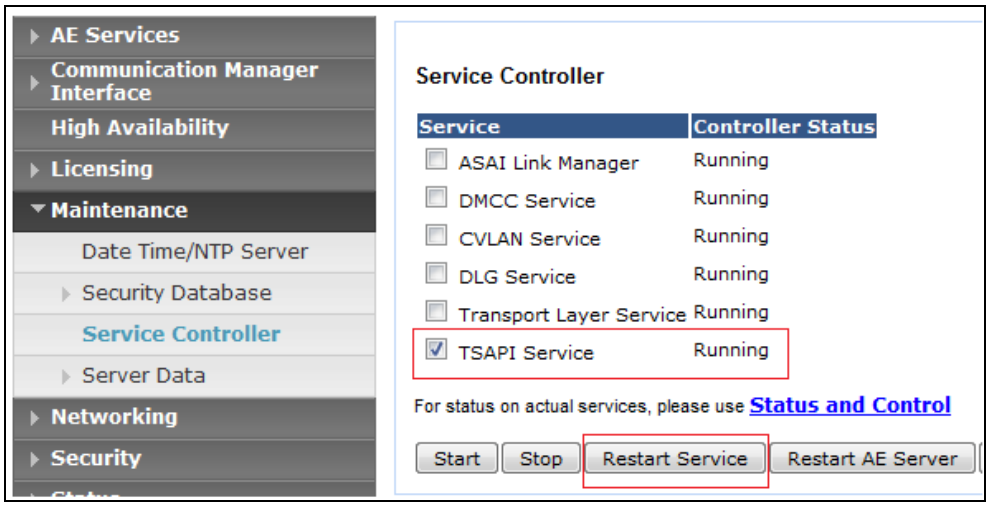
Another screen appears for confirmation of the changes made. Choose **Apply**.




When the TSAPI Link is completed, it resembles the screen below.

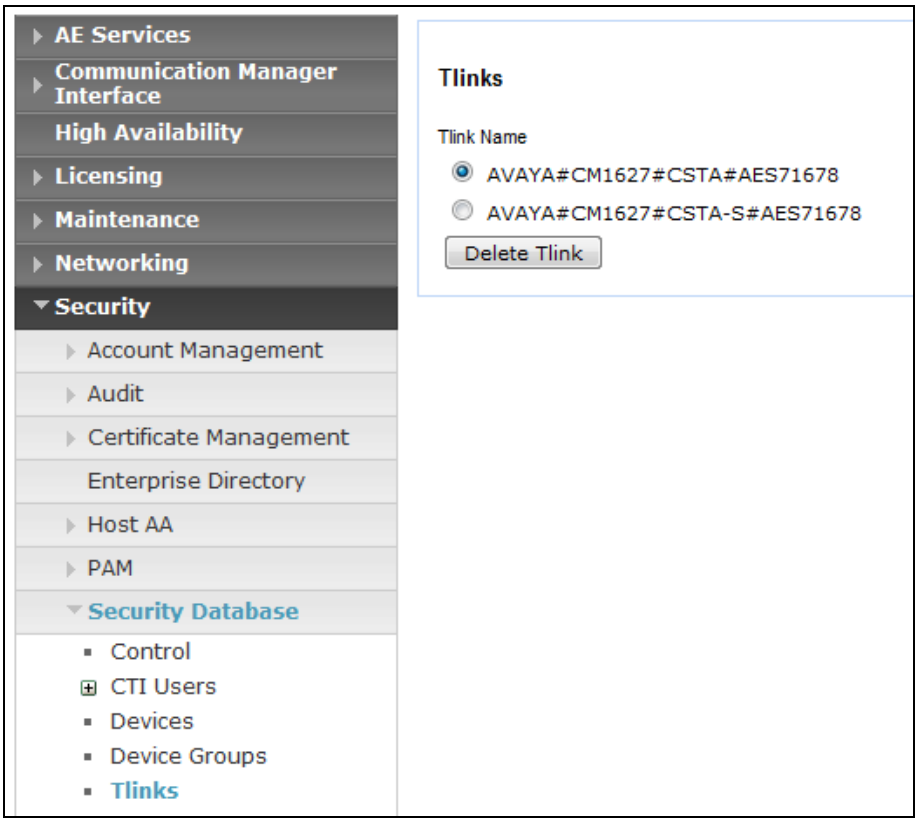



The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



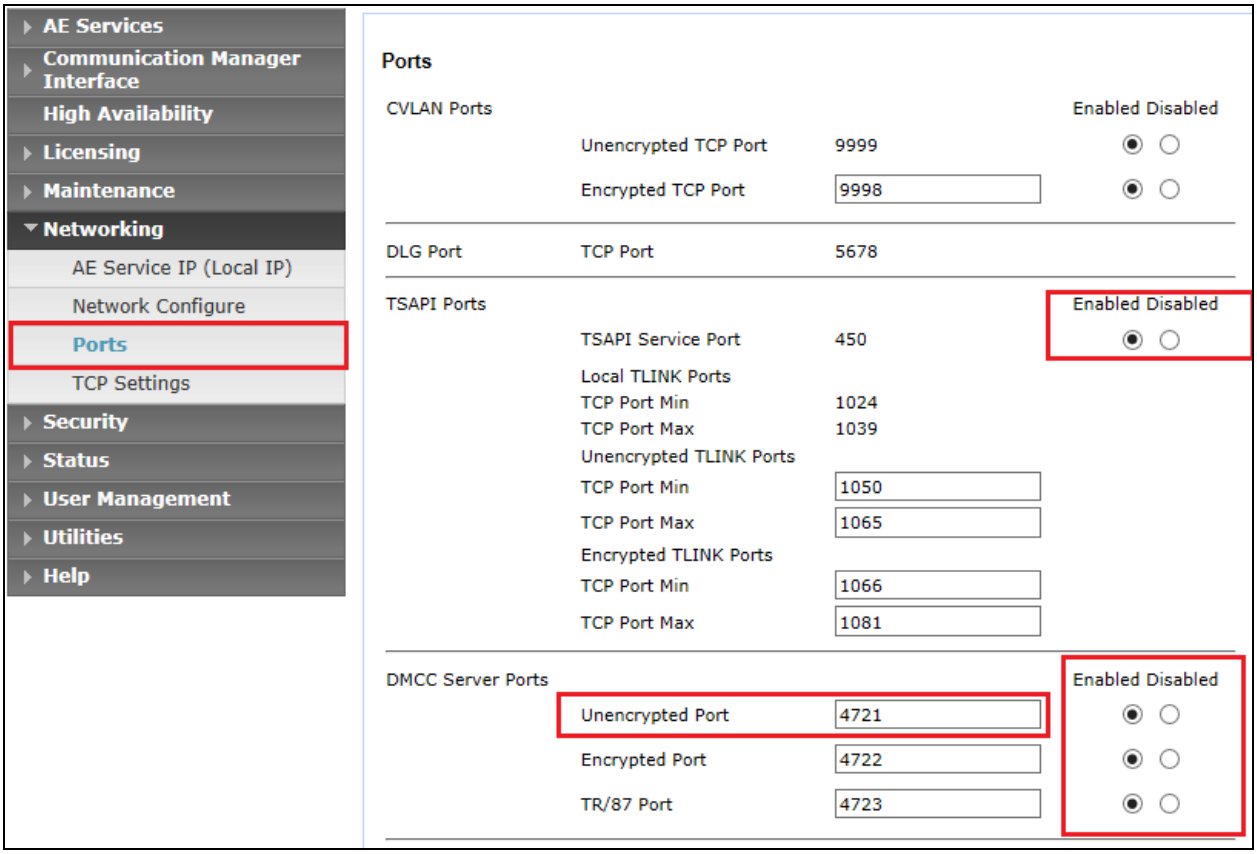
## 6.4. Identify Tlinks

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



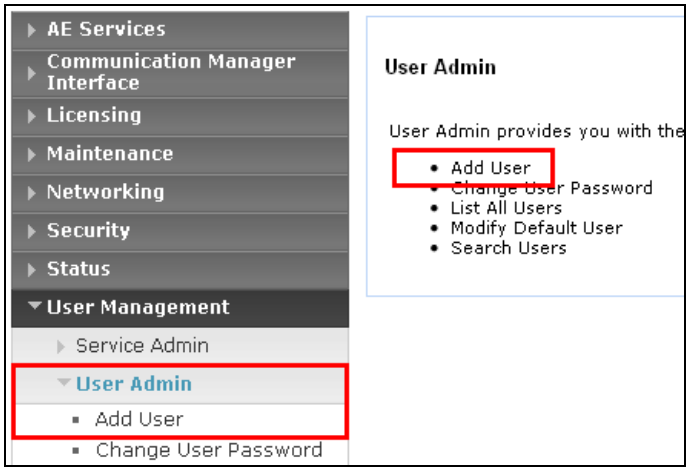
## 6.5. Enable TSAPI and DMCC Ports

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 8.3.1**. 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

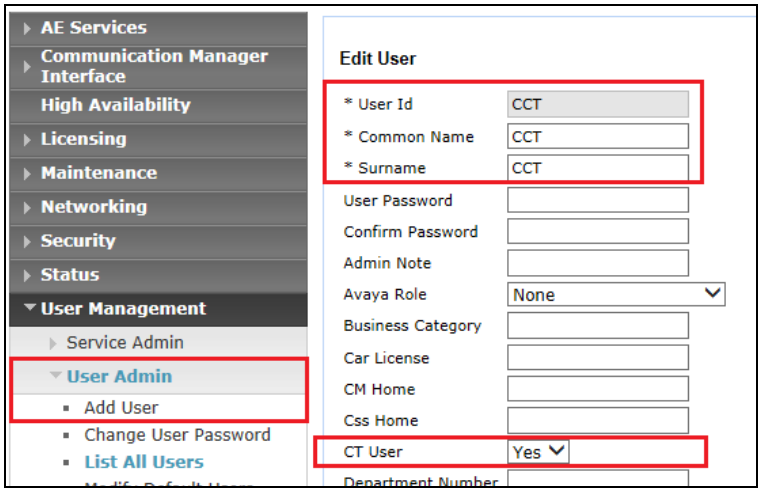
A User ID and password needs to be configured for ContactPro to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.




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 **PrimaryAESLoginUsername & PrimaryAESLoginPassword** in **Section 8.3.1**.
- **CT User** - Select **Yes** from the drop-down menu.

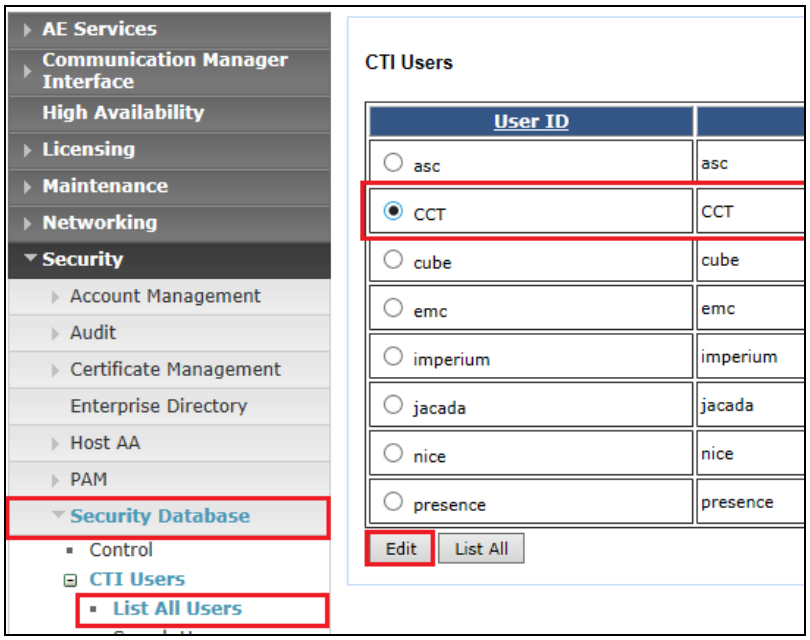
Complete the process by choosing **Apply** at the bottom of the screen (not shown).



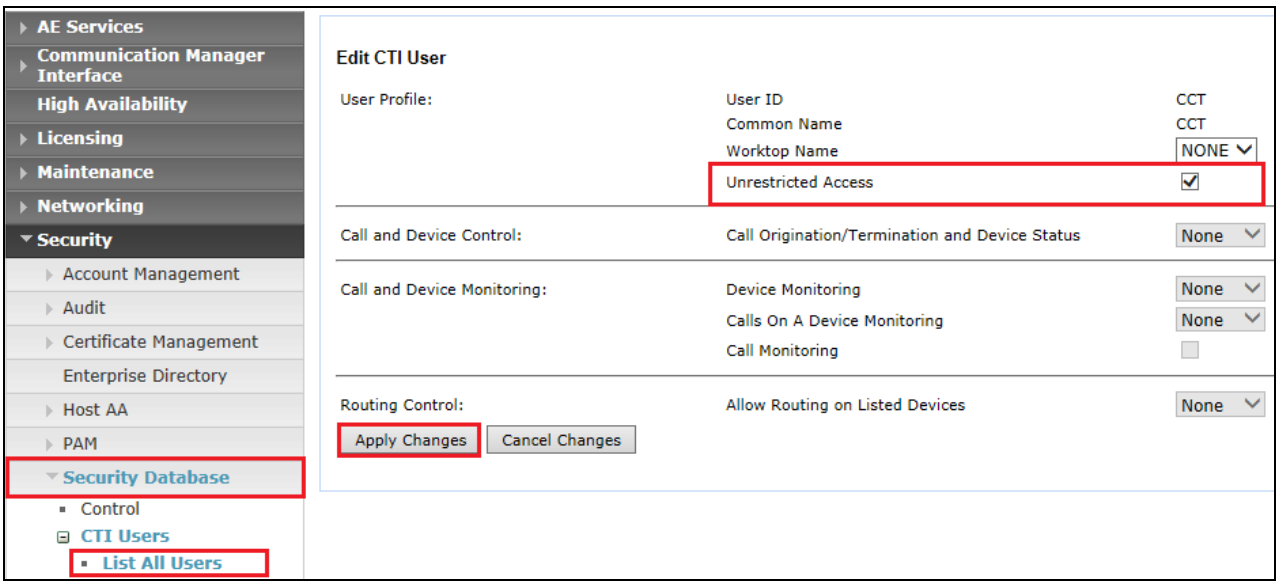

The next screen will show a message indicating that the user was created successfully (not shown).

## 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**.



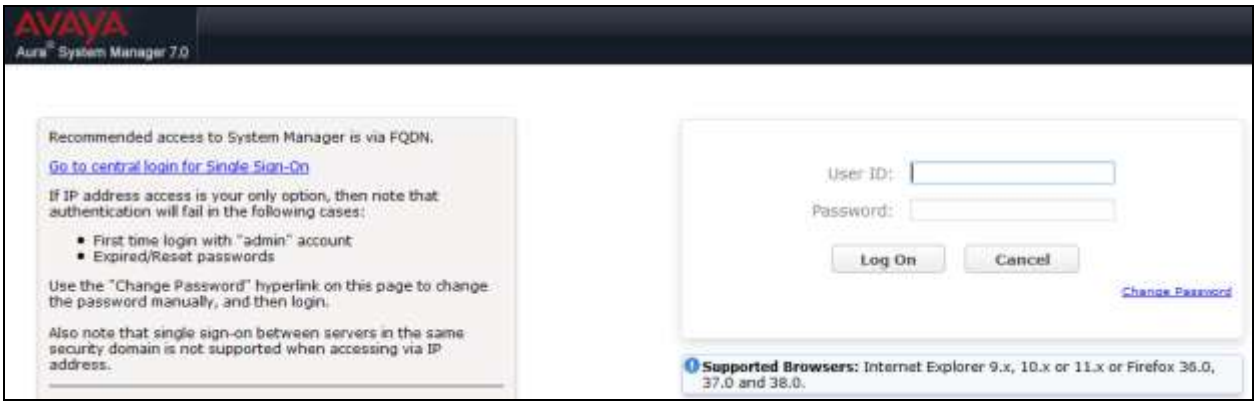

Tick the box **Unrestricted Access** to allow this user access to all devices on Communication Manager. If this is not required then a list of devices to be allocated to this user will need to be setup and the procedure for achieving this can be found in the following document listed in **Section 12** *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*. Click on **Apply Changes** to complete the setup.



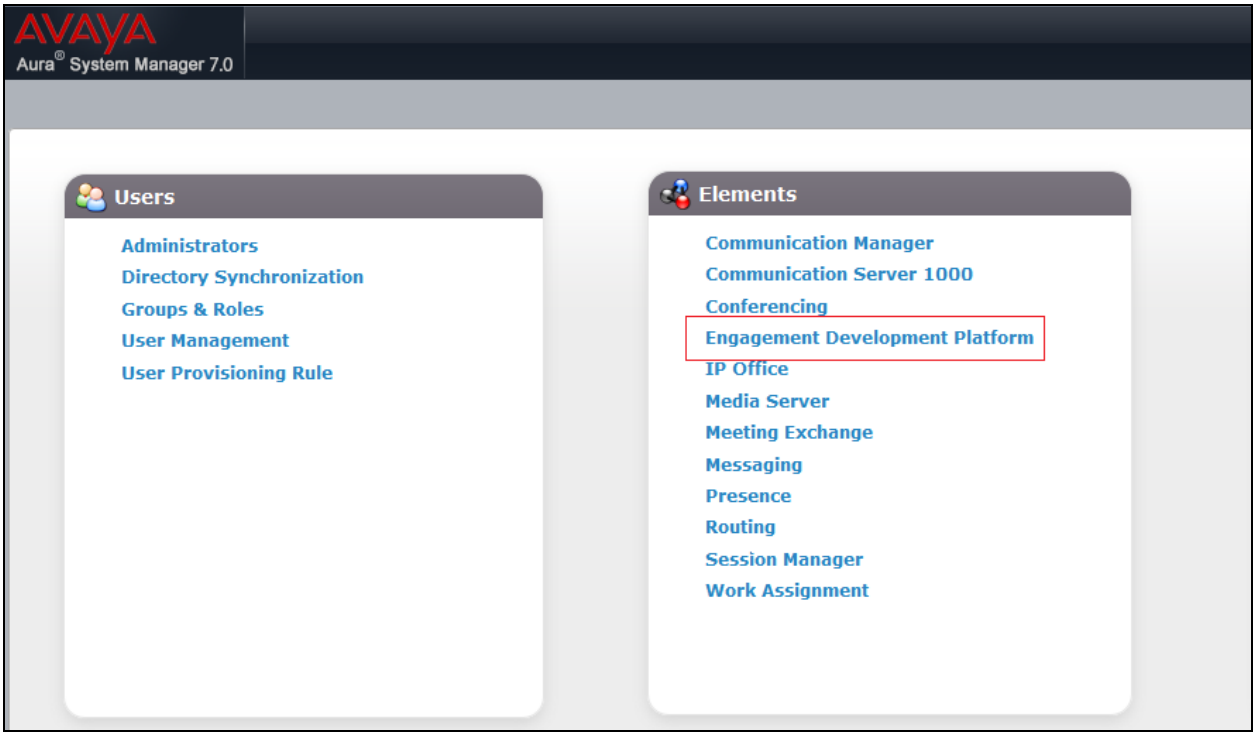
# 7. Check Avaya Co-Browsing Snap-In is installed on the Engagement Development Platform

This section describes the steps required check that the Avaya Co-Browsing Snap-In is installed correctly and is ready for ContactPro. There is no extra configuration required for this Snap-In. The installation and configuration of the Engagement Development Platform and Co-Browsing Snap-In are out with the scope of this document and are assumed to have been competed using the Reference Documentation in **Section 12** using the System Manager Web interface.

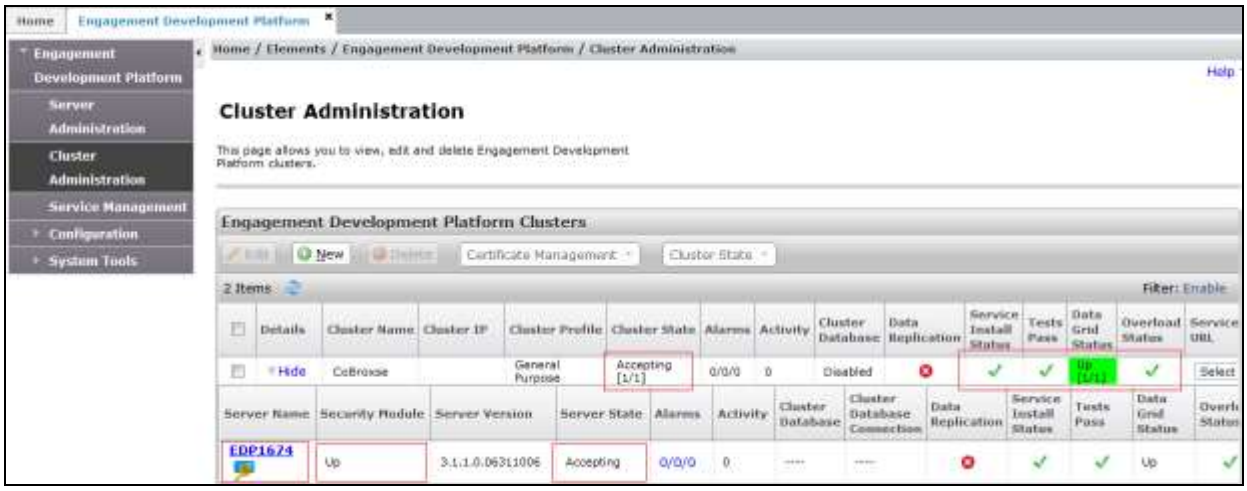
Log in to System Manager using the appropriate credentials.



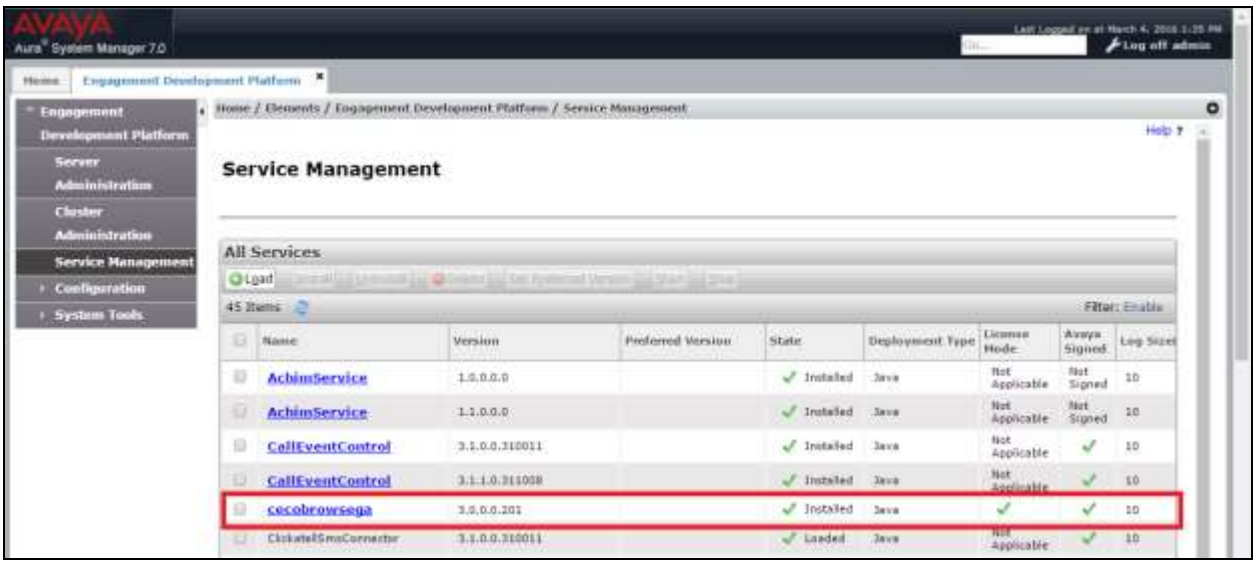

From the home screen select **Elements → Engagement Development Platform**



From the left hand menu Select **Cluster Administration**. Check that the **Cluster State** is **Accepting [1/1]**, **Service Install Status** has a green tick and **Data Grid Status** is **Up[1/1]**. Click on Show under **Details** (not shown) and check that **Security Module** is **Up** and **Server State** is **Accepting**.




Verify that the Avaya CoBrowse Snap-in (**cecobrowsega**) has been installed successfully under **Service Management**.



# 8. Configure CCT ContactPro

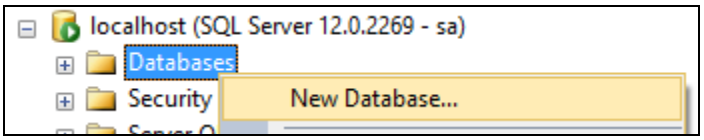
This section outlines the steps required to configure the connections from CCT ContactPro to both the AES and EMC.

## 8.1. Create ContactPro EMC Database and User

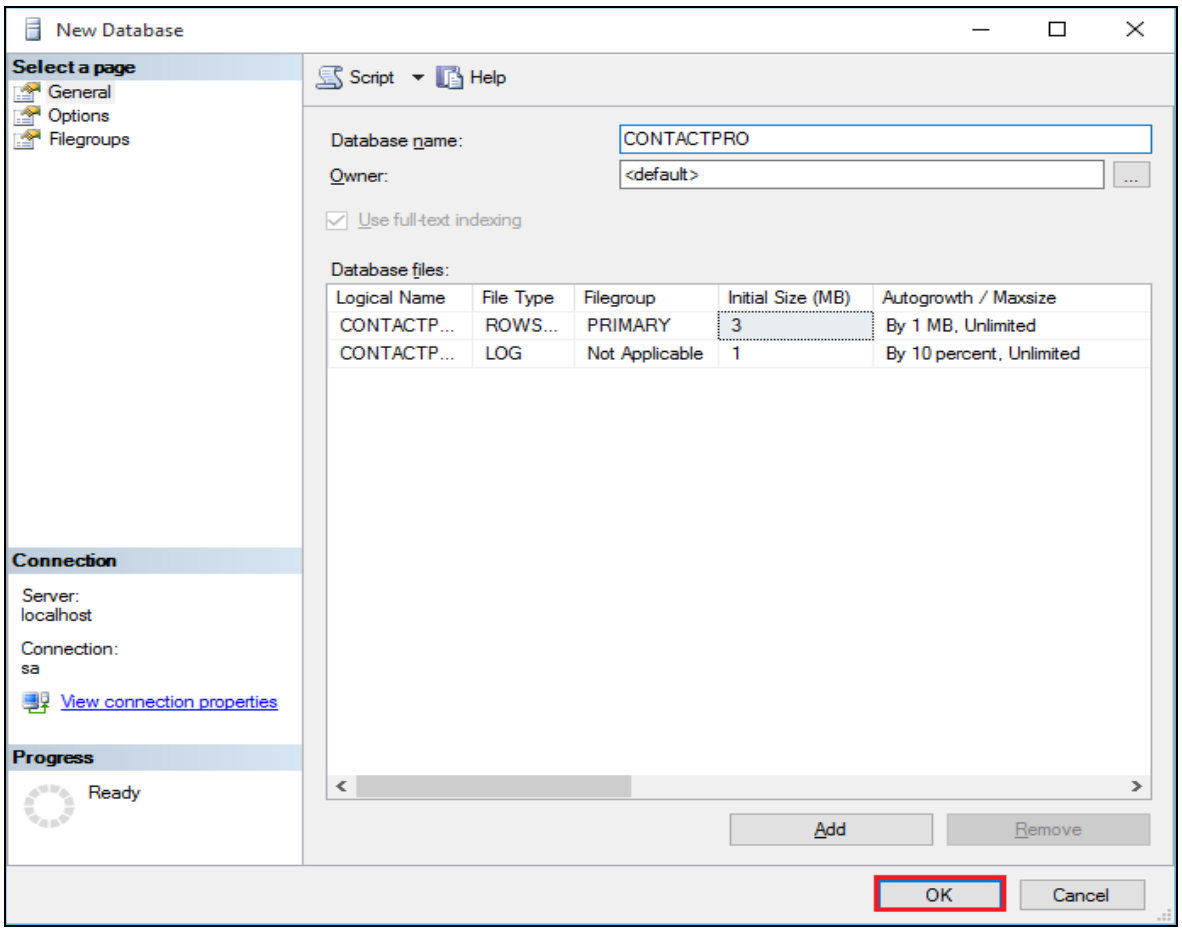
A database and database user for ContactPro EMC must be created on the SQL server that hosts the Avaya EMC database.

### 8.1.1. Create Database

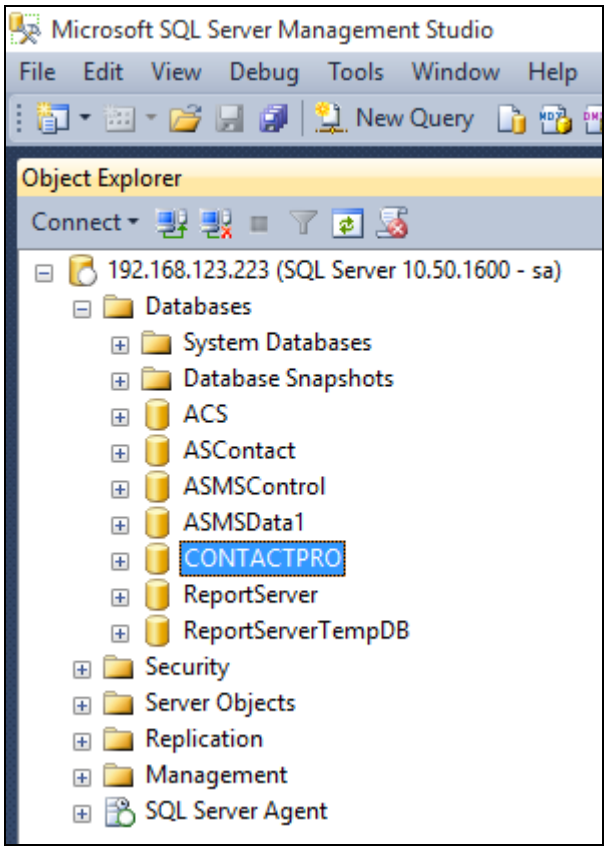
Create a **CONTACTPRO** database on the same Microsoft SQL Server where the Avaya EMC databases are located. Right-click on **Databases** and click on **New Database**.




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

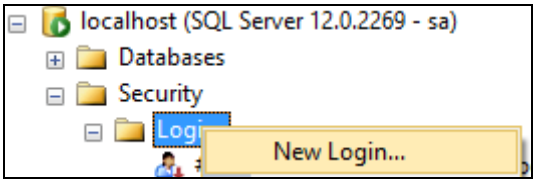


The end result will be as shown in the screenshot below where there are 4 standard Avaya EMC databases (**ACS**, **ASContact**, **ASMSControl**, **ASMSData1**) and the **CONTACTPRO** database which was just created. The default MS SQL **ReportServer** and **ReportServerTempDB** databases may also be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

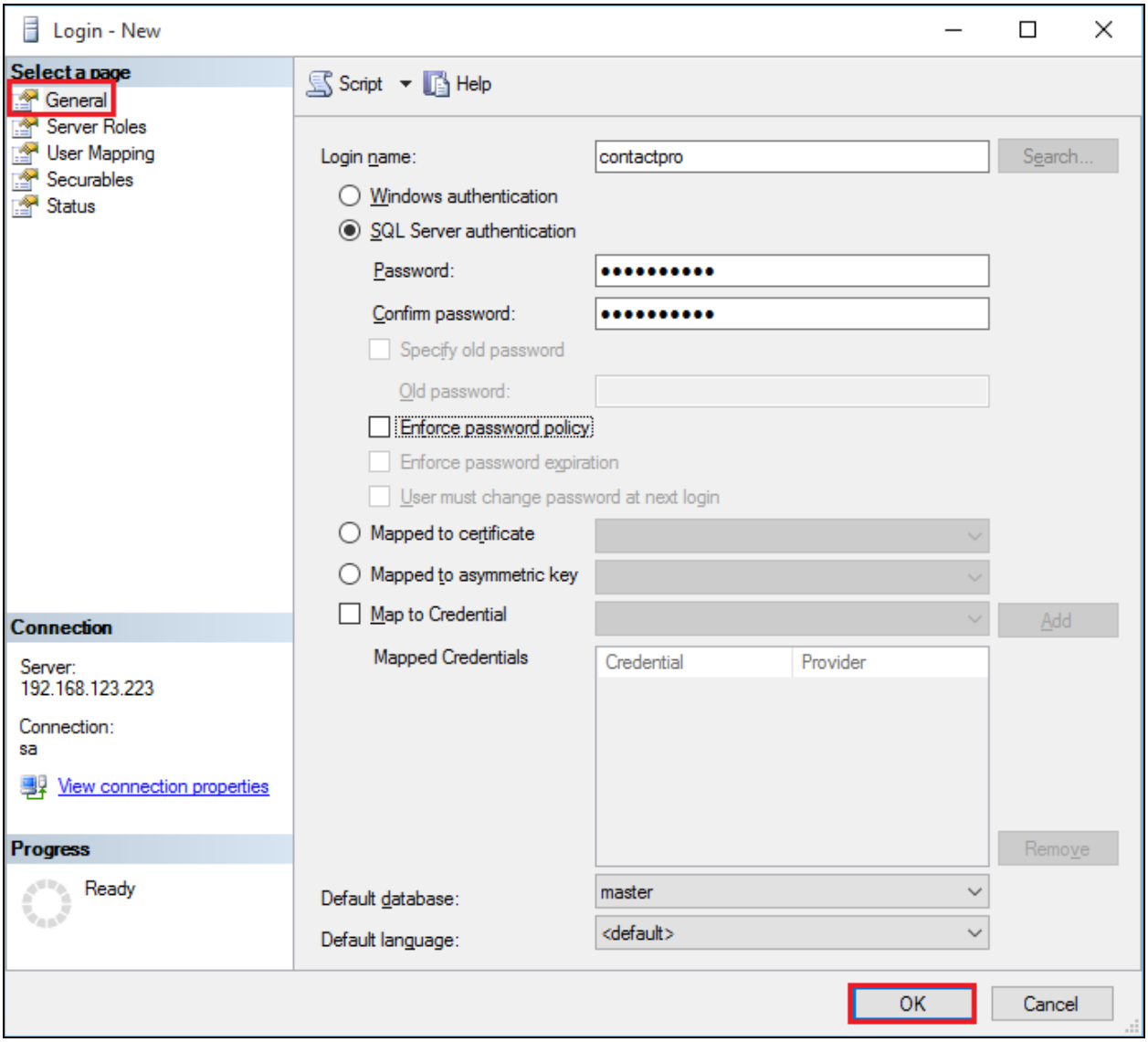


### 8.1.2. Create User

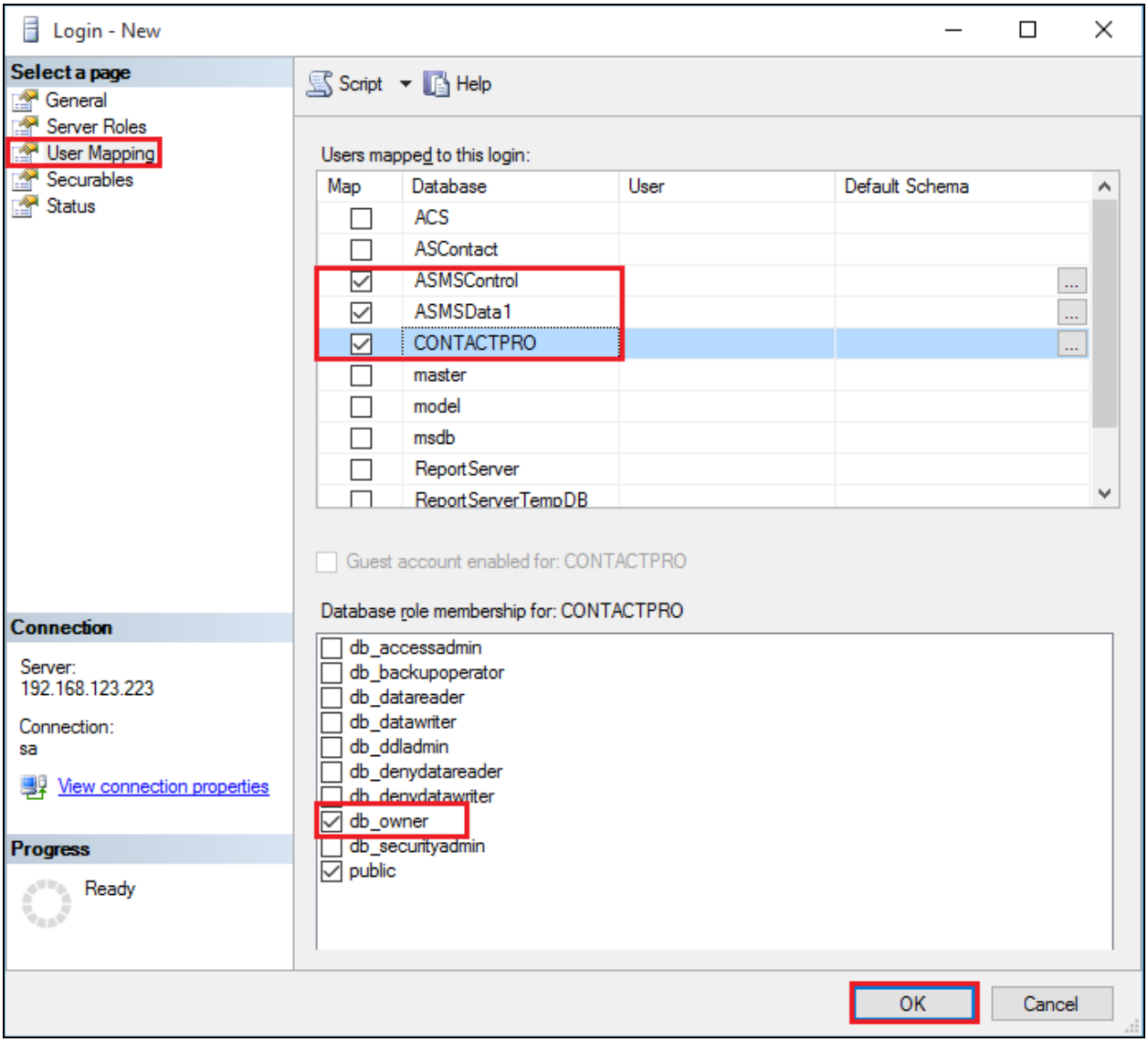
Create a database user named **contactpro**. Right-click on **Login** and click on **New Login**.




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.

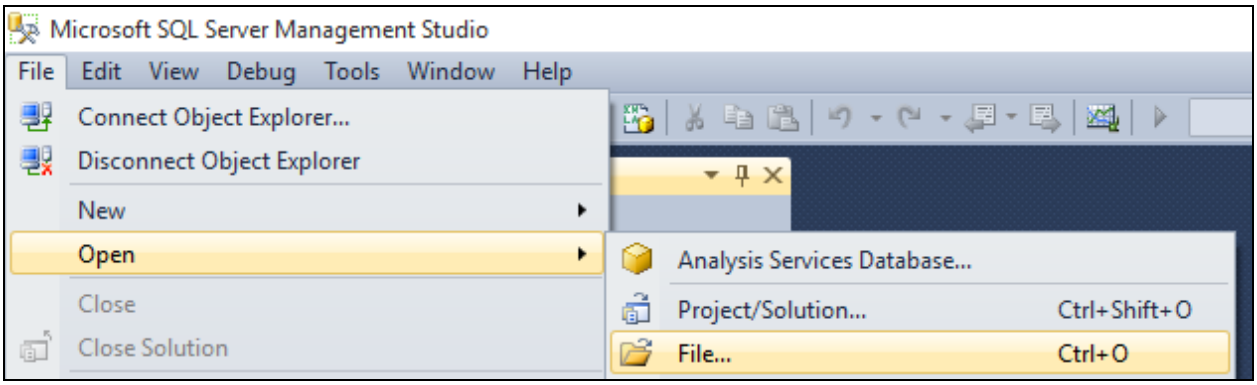


Click on **User Mapping** in the left window. For this user, grant public and **db_owner** access to **ASMSControl**, **ASMSData1** and **CONTACTPRO** databases. Click on **OK** at the bottom of the page once done.

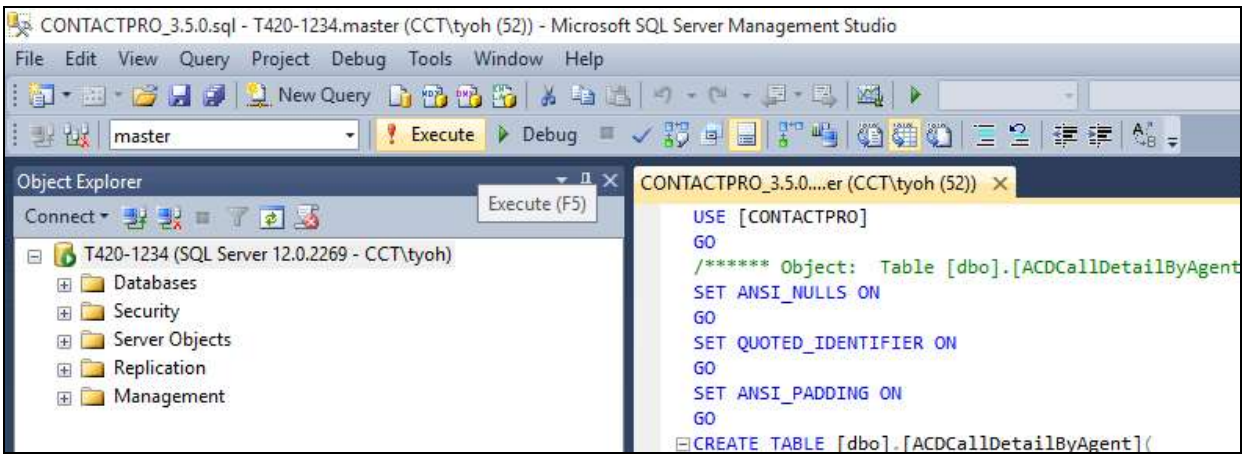


### 8.1.3. Execute CONTACTPRO.sql script

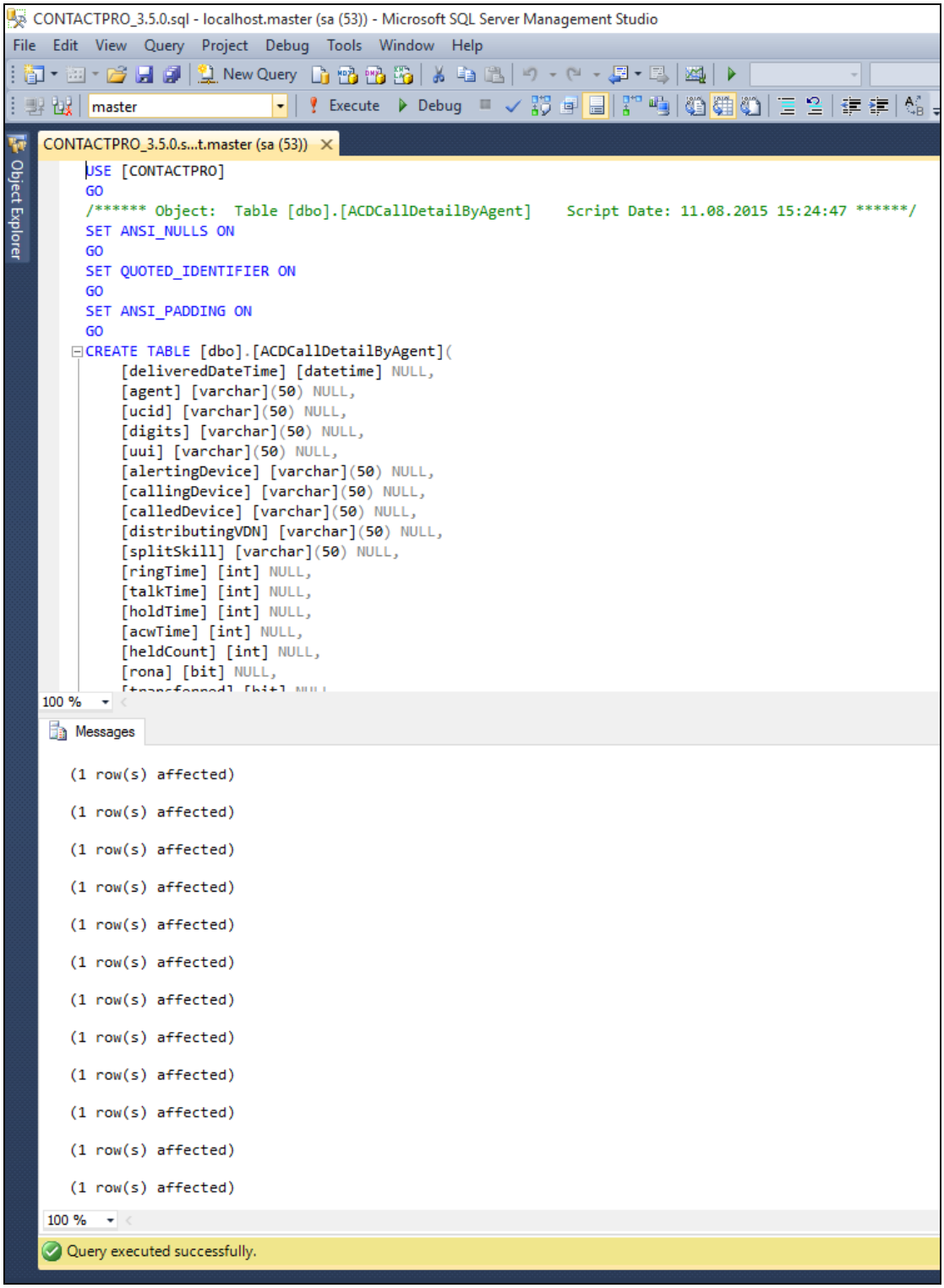
The fill the contents of the **CONTACTPRO** database, open the provided **CONTACTPRO_3.5.sql** script.



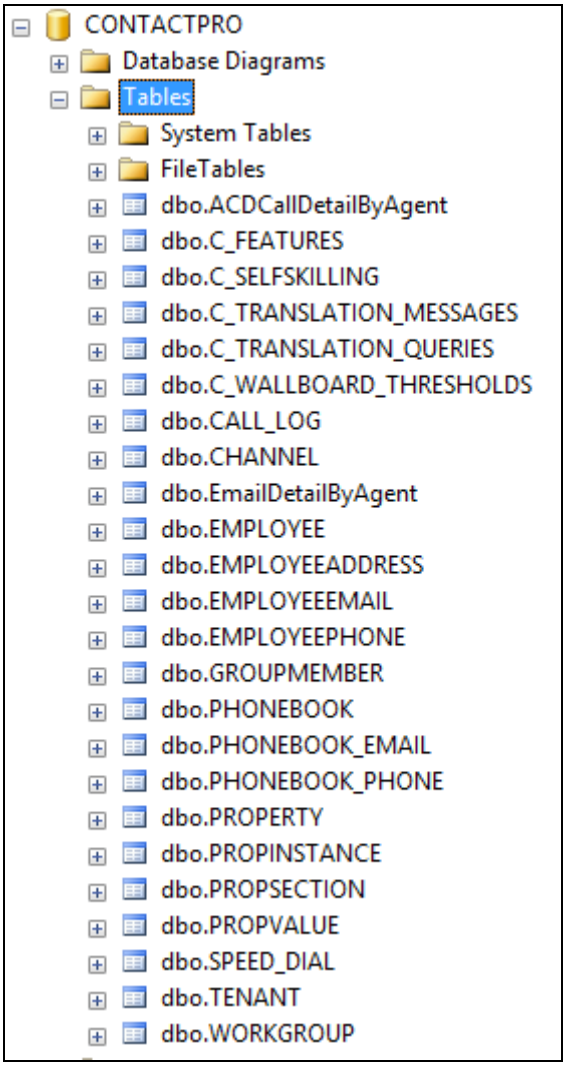

Execute the script by clicking the **Execute** button.



The following shows the script being executed.



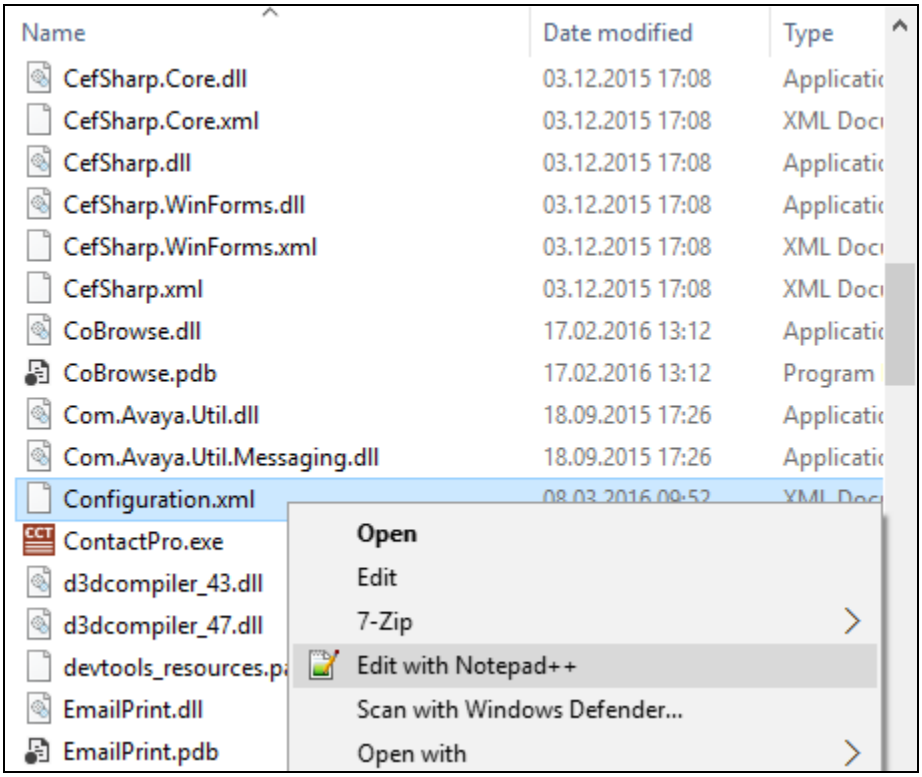
The contents of the **CONTACTPRO** database will now look like this.



## 8.2. Configure ContactPro EMC and ContactPro Manager connections to the database

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

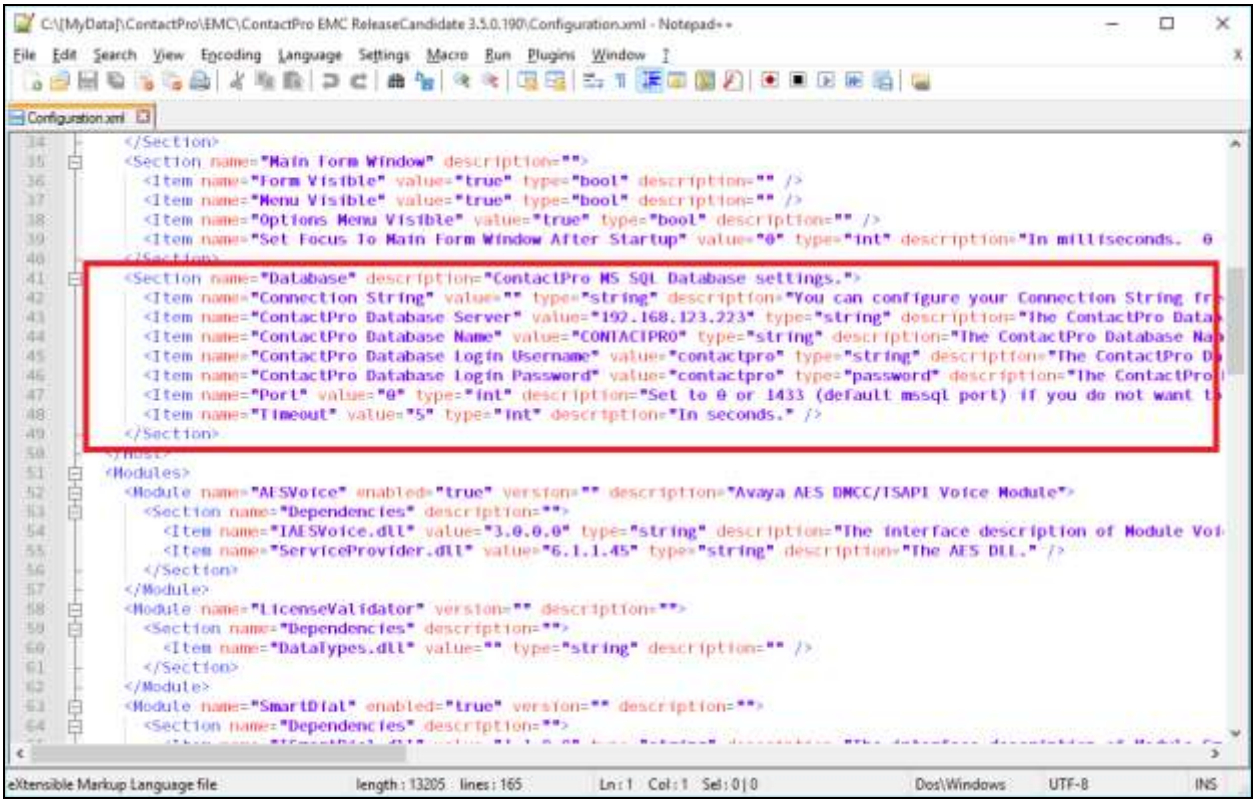
Navigate to the folder where ContactPro EMC and ContactPro Manager have been installed. Right click on the file called **Configuration.xml** and open this with a suitable text editor as is shown below.



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

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

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



## 8.3. Configure Properties with ContactPro Manager

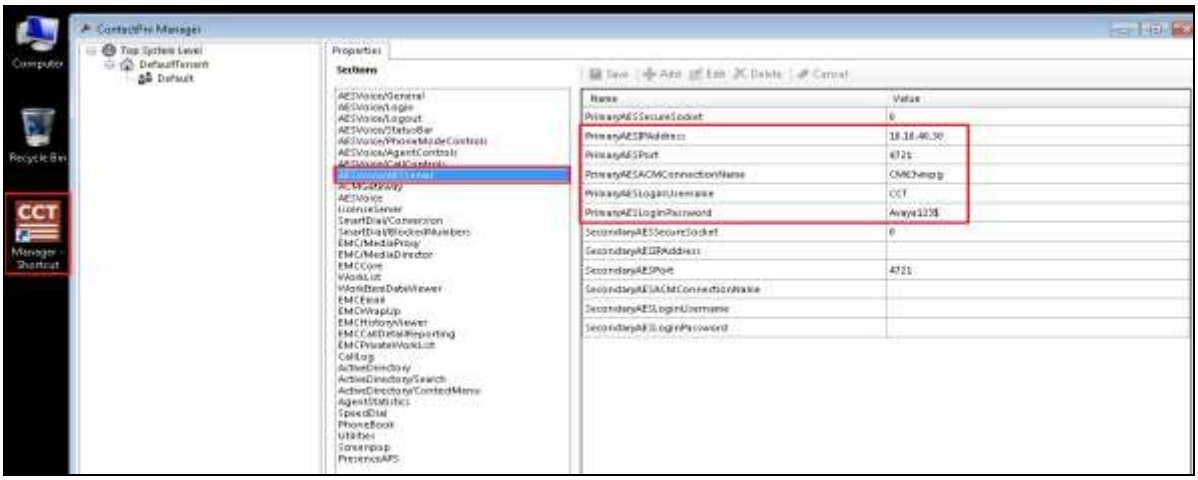
The ContactPro Manager allows the configuration of properties for all ContactPro Clients. Global properties can be set at the **Top System Level** or set different properties at the **Tenant level** or **Workgroup level** or for each **individual Agent**.

Properties only need to be configured in sub levels if different Properties for other Tenants are required. This is well suited for Enterprise deployment and is similar to Avaya Interaction Center IC Manager.

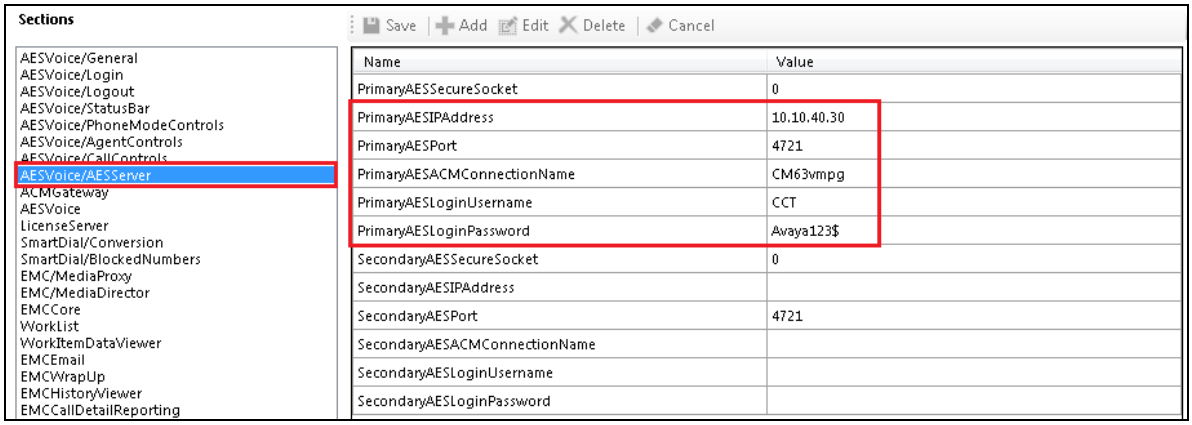
The following sections describe the minimum required properties to configure for ContactPro in order to connect successfully to both the AES and the Avaya EMC Server. All other properties may be left at their default values.

### 8.3.1. Configure the Connection to Avaya Aura® Application Enablement Services

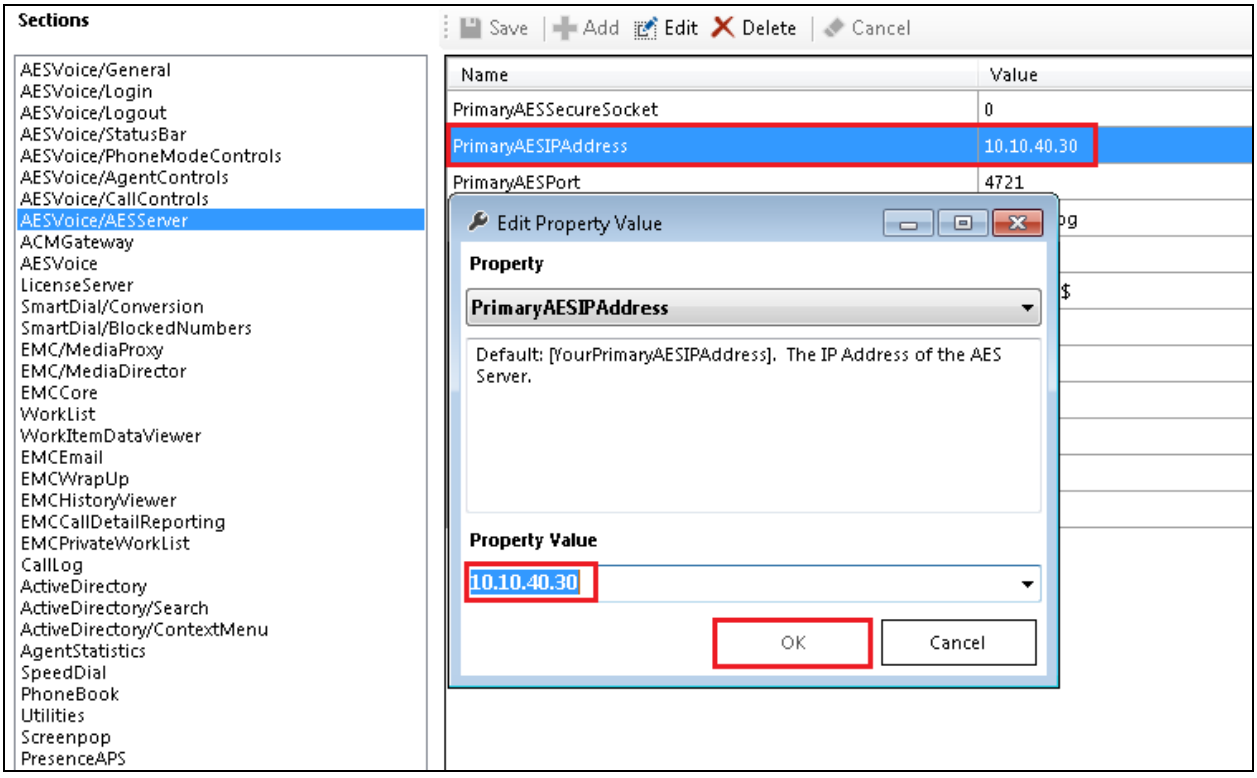
From a Supervisor or Administrator PC where the CCT ContactPro Manager application was installed, double click on the CCT ContactPro Manager shortcut as shown below. The **ContactPro Manager** is opened and select **AESVoice/AESServer** from the **Sections** window.



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




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 **OK** once this is done.

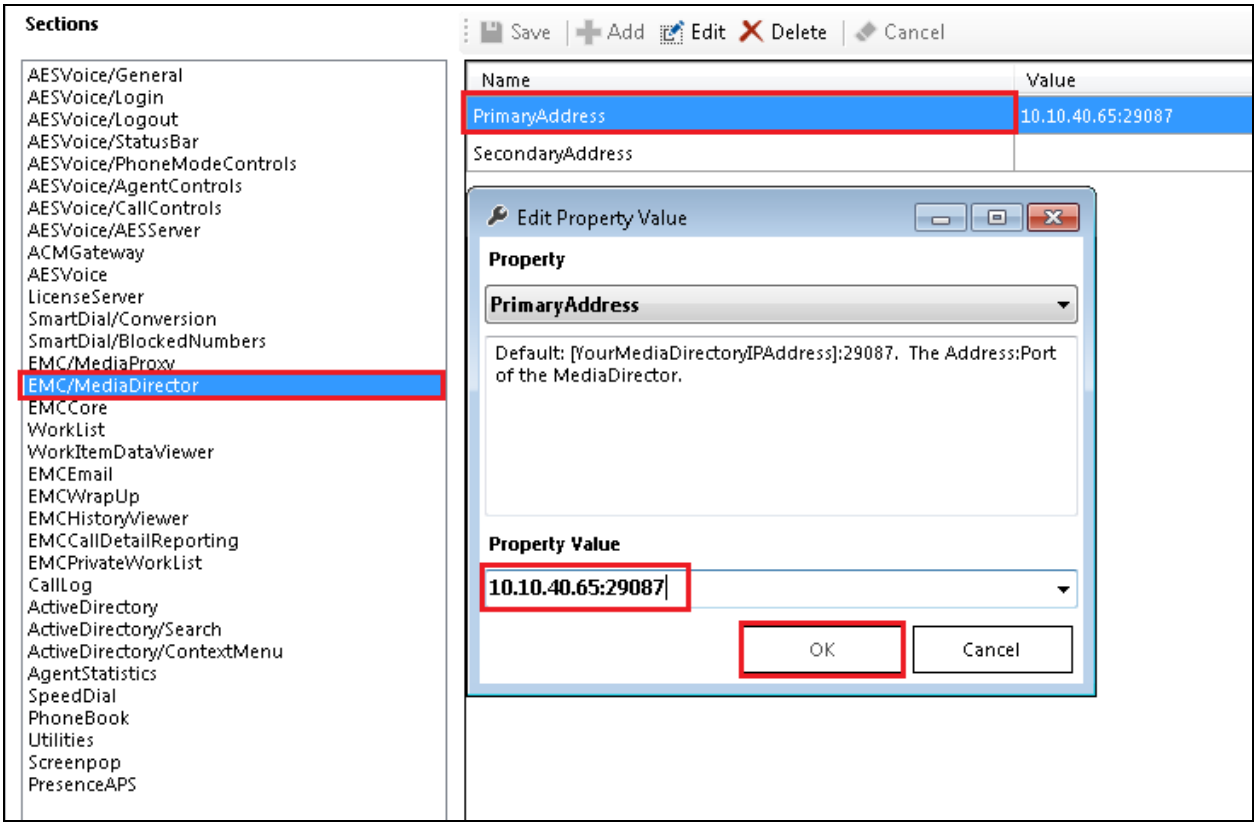


Continue with the other AES information that is highlighted below and this concludes the setup for AES.

| Name | Value |
|---|---|
| PrimaryAESSecureSocket | 0 |
| PrimaryAESIPAddress | 10.10.40.30 |
| PrimaryAESPort | 4721 |
| PrimaryAESACMConnectionName | CM63vmpg |
| PrimaryAESLoginUsername | CCT |
| PrimaryAESLoginPassword | Avaya123$ |
| SecondaryAESSecureSocket | 0 |
| SecondaryAESIPAddress | |
| SecondaryAESPort | 4721 |
| SecondaryAESACMConnectionName | |
| SecondaryAESLoginUsername | |
| SecondaryAESLoginPassword | |

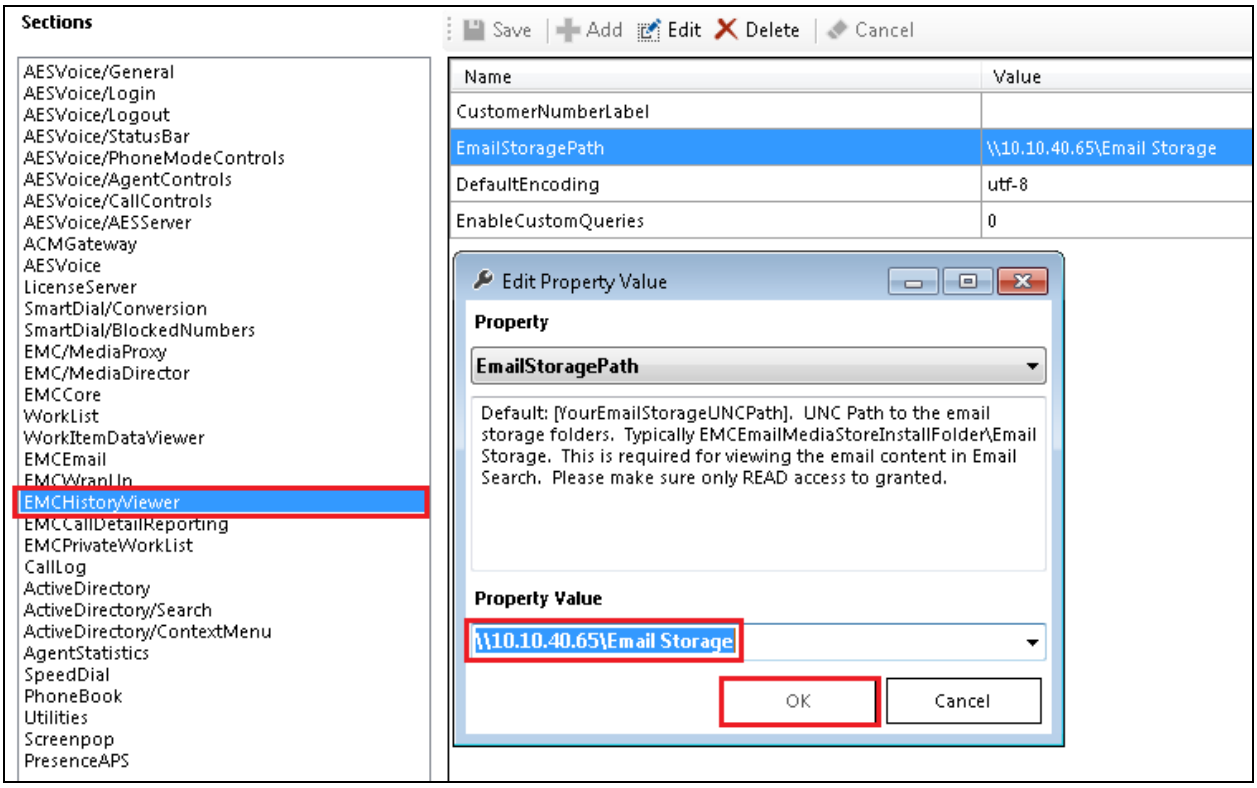
### 8.3.2. Configure the Connection to Avaya Aura® Call Center Elite Multichannel

Select **EMC/MediaDirector** from the **Sections** 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 **29087** is the default port but this information can be obtained from the EMC server. Click on **OK** once this is entered correctly.

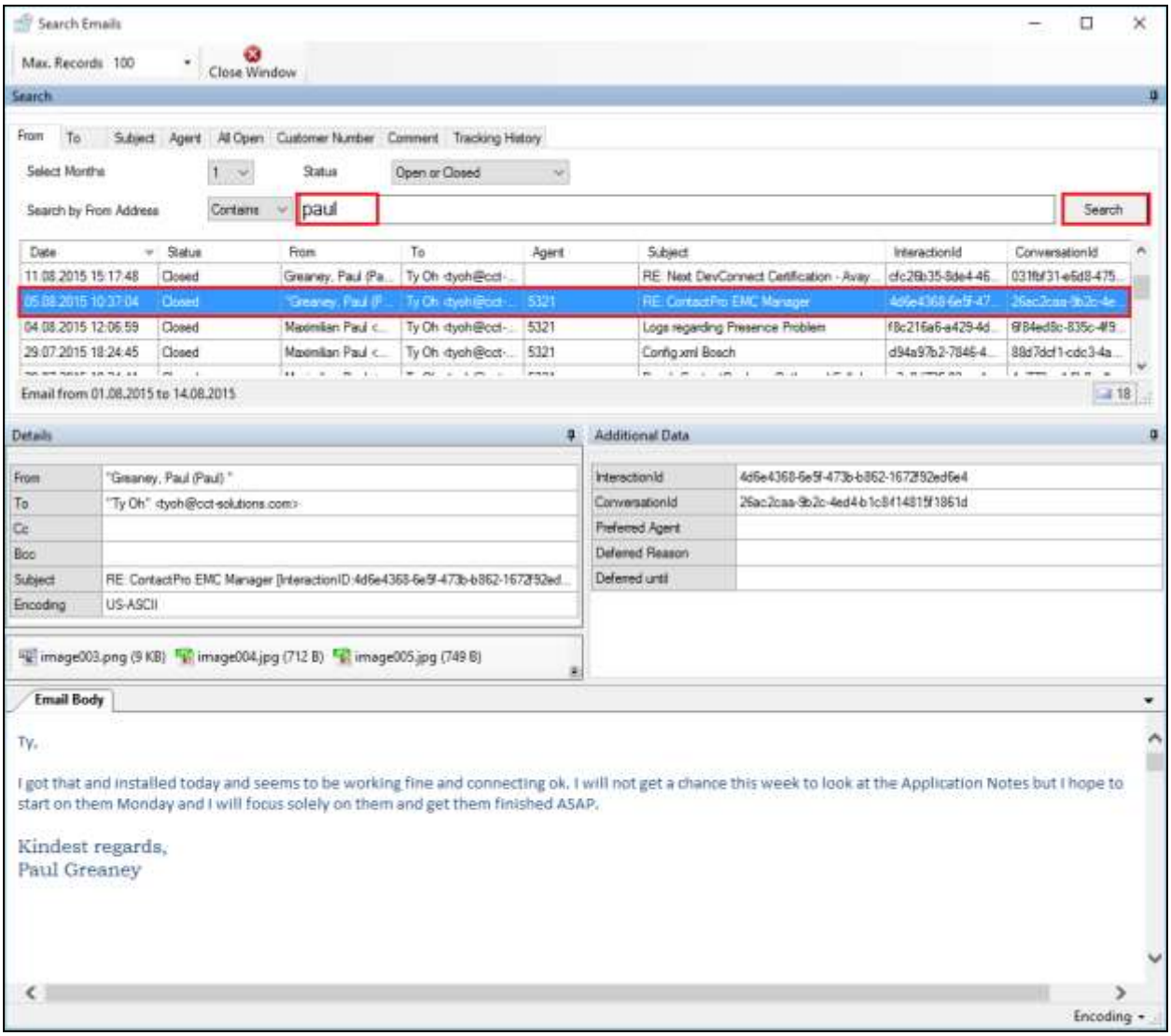


### 8.3.3. Configure the Connection to EMC Email Storage Path

Select **EMCHistoryViewer** from the **Sections** 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.



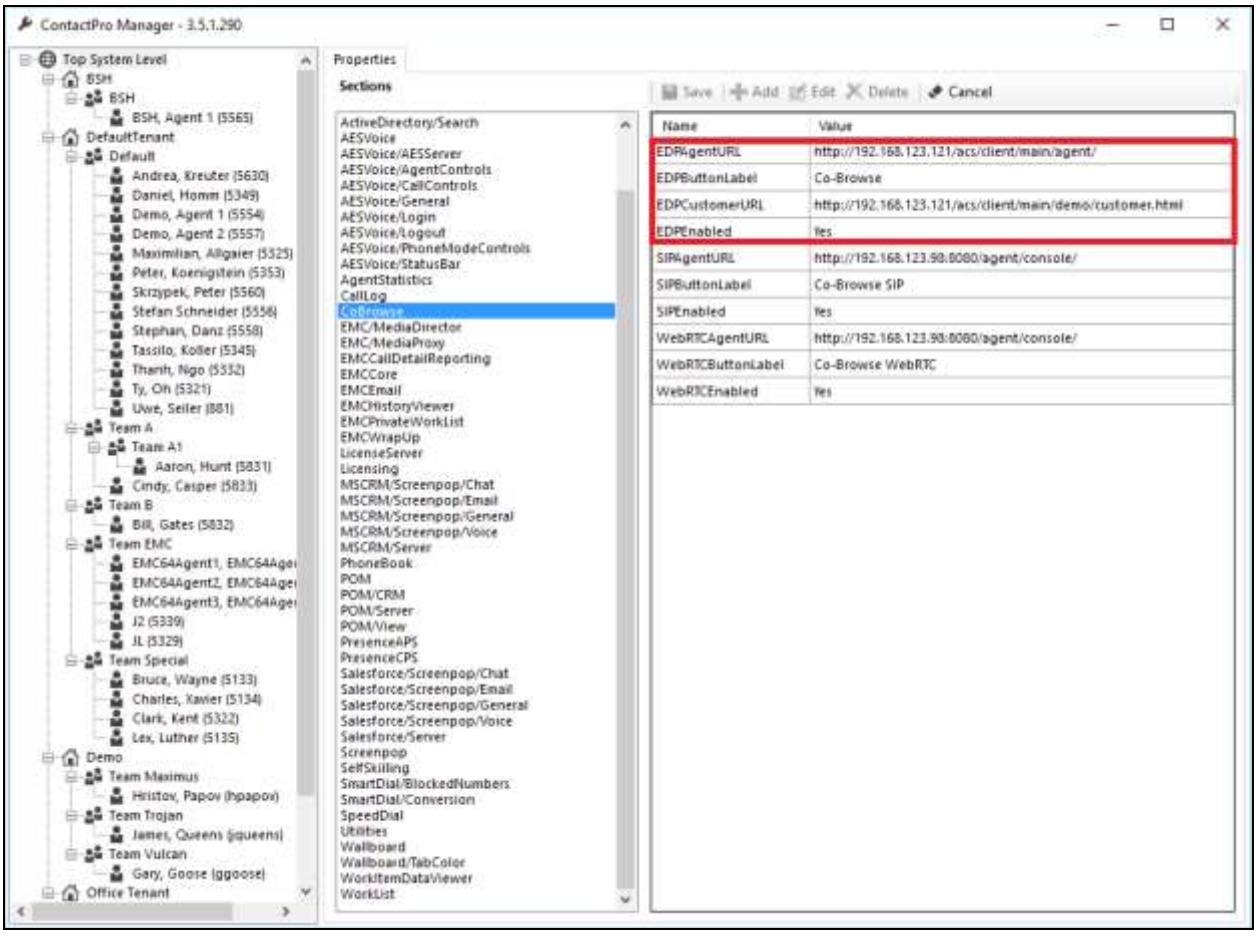
A shared path to the **Email Storage** must be created for clients to access. This is typically in the "C:\Program Files (x86)\Avaya\Avaya Aura CC Elite Multichannel\Server\Media Stores\Email Media Store\Email Storage" of the EMC Server. This is required to provide the feature of viewing the Body of 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 retrievers all the emails associated with the word **paul**. Double-clicking on this item will then open the associated email for viewing.



### 8.3.4. Configure the Connection to EDP CoBrowse

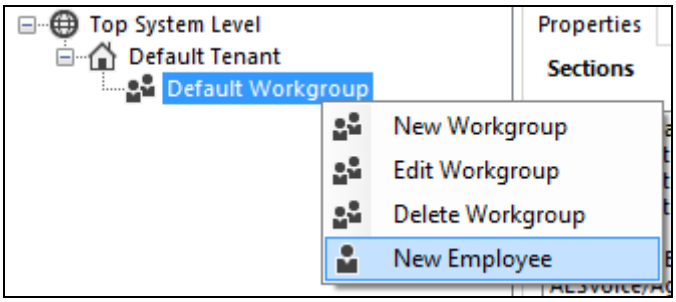
Select **CoBrowse** from the **Sections** window. Configure the following 4 properties.

- EDPEnabled
  - Default:No. Show or Hide the Toolstrip Button.
- EDPButtonLabel
  - Default:Co-Browse. Label text of the button.
- EDPAgentURL
  - Default:http://[YourServer]/acs/client/main/agent/. URL for the Agent.
- EDPCustomerURL
  - Default:http://[YourServer]/acs/client/main/demo/customer.html. URL for the Customer.



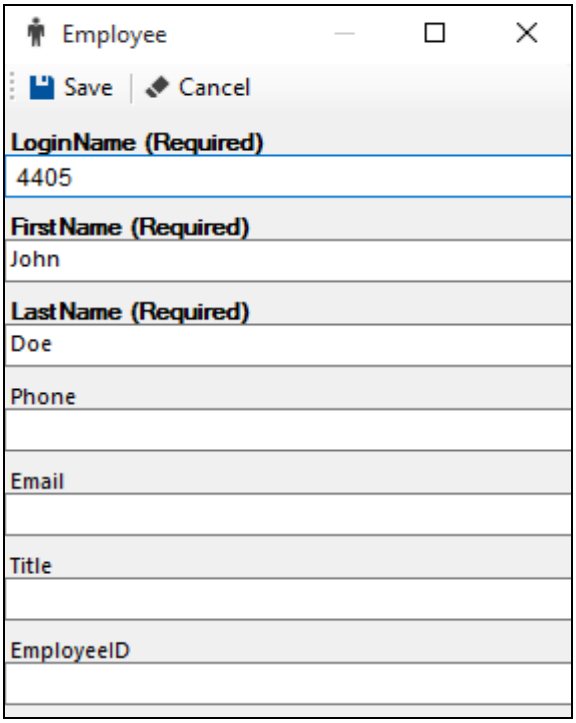
## 8.4. Configure Users with ContactPro Manager

For every ContactPro Client user, a **New Employee** needs to be created. Right Click on a workgroup then click **New Employee**.




The following fields are required.

- **LoginName**
- **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. Configure CCT ContactPro AIC

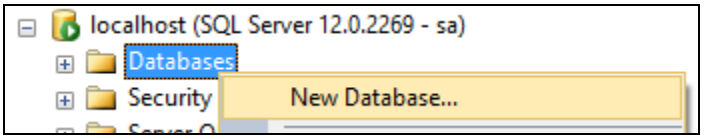
This section outlines the steps required to configure the connections from CCT ContactPro AIC with CoBrowse to the Avaya Interaction Center.

## 9.1. Create ContactPro AIC Database and User for SQL Server

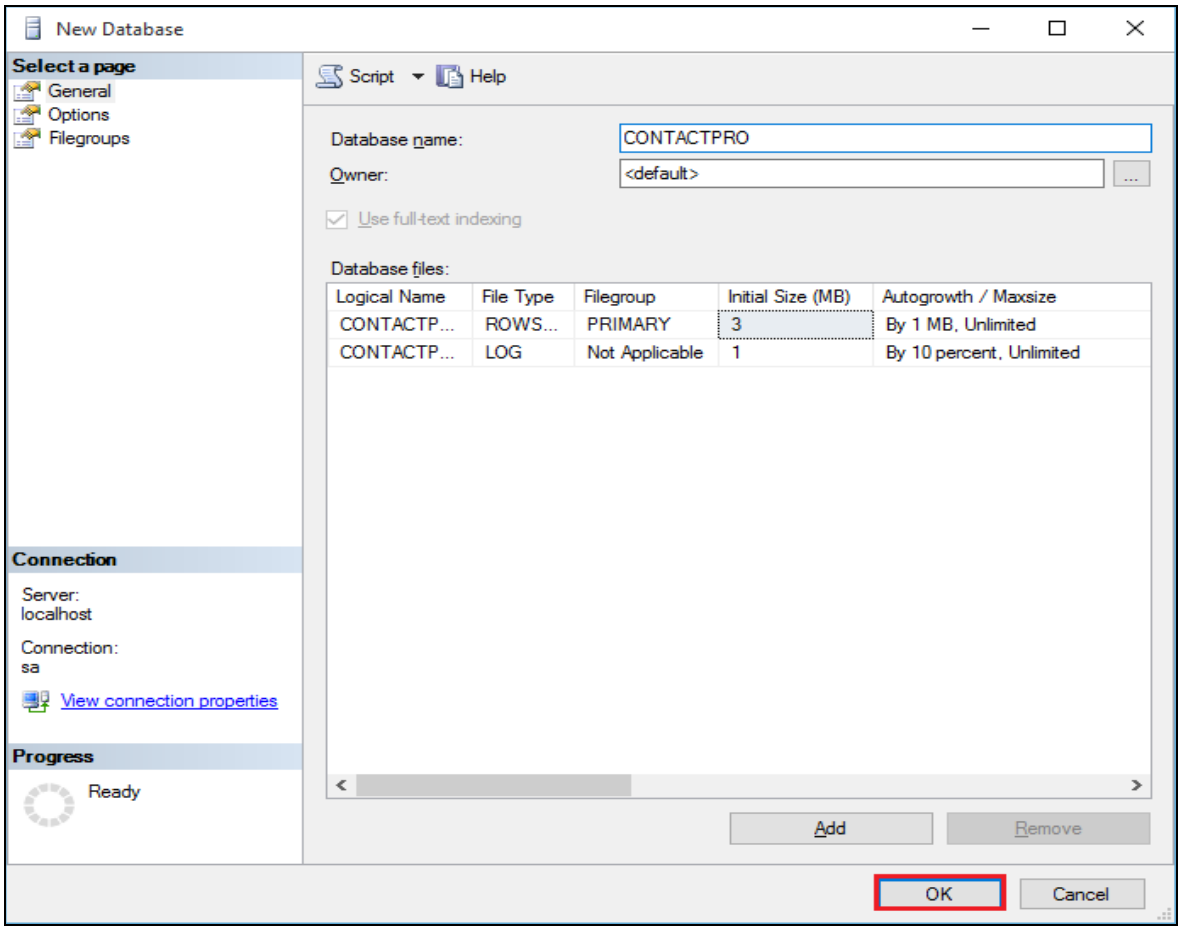
A database and database user for ContactPro AIC must be created on the SQL server database that hosts the Avaya AIC database.

### 9.1.1. Create SQL Server Database

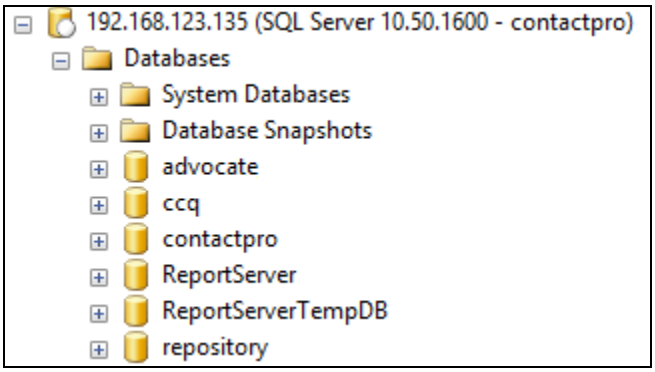
Create a **CONTACTPRO** database on the same Microsoft SQL Server where the Avaya AIC databases are located. Right-click on **Databases** and click on **New Database**.




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

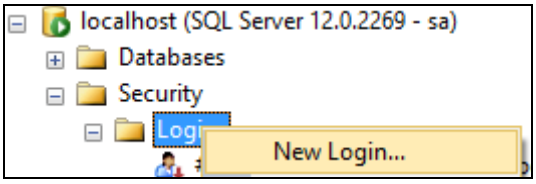


The end result will be as shown in the screenshot below where there are 3 standard Avaya IC databases (**Advocate, CCQ, Repository**) and the **CONTACTPRO** database which was just created. The default MS SQL **ReportServer** and **ReportServerTempDB** databases may also be present.

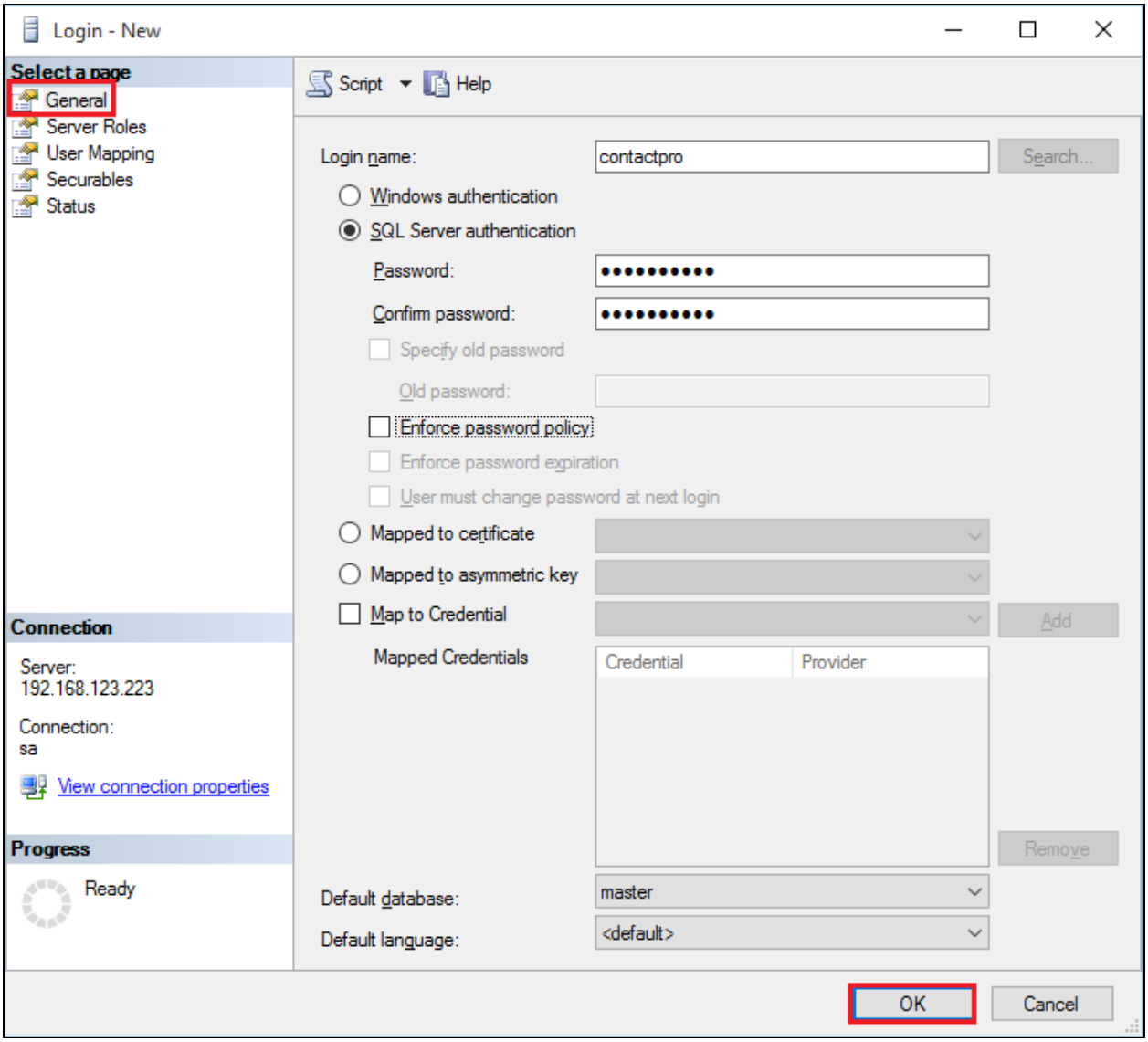


### 9.1.2. Create SQL Server User

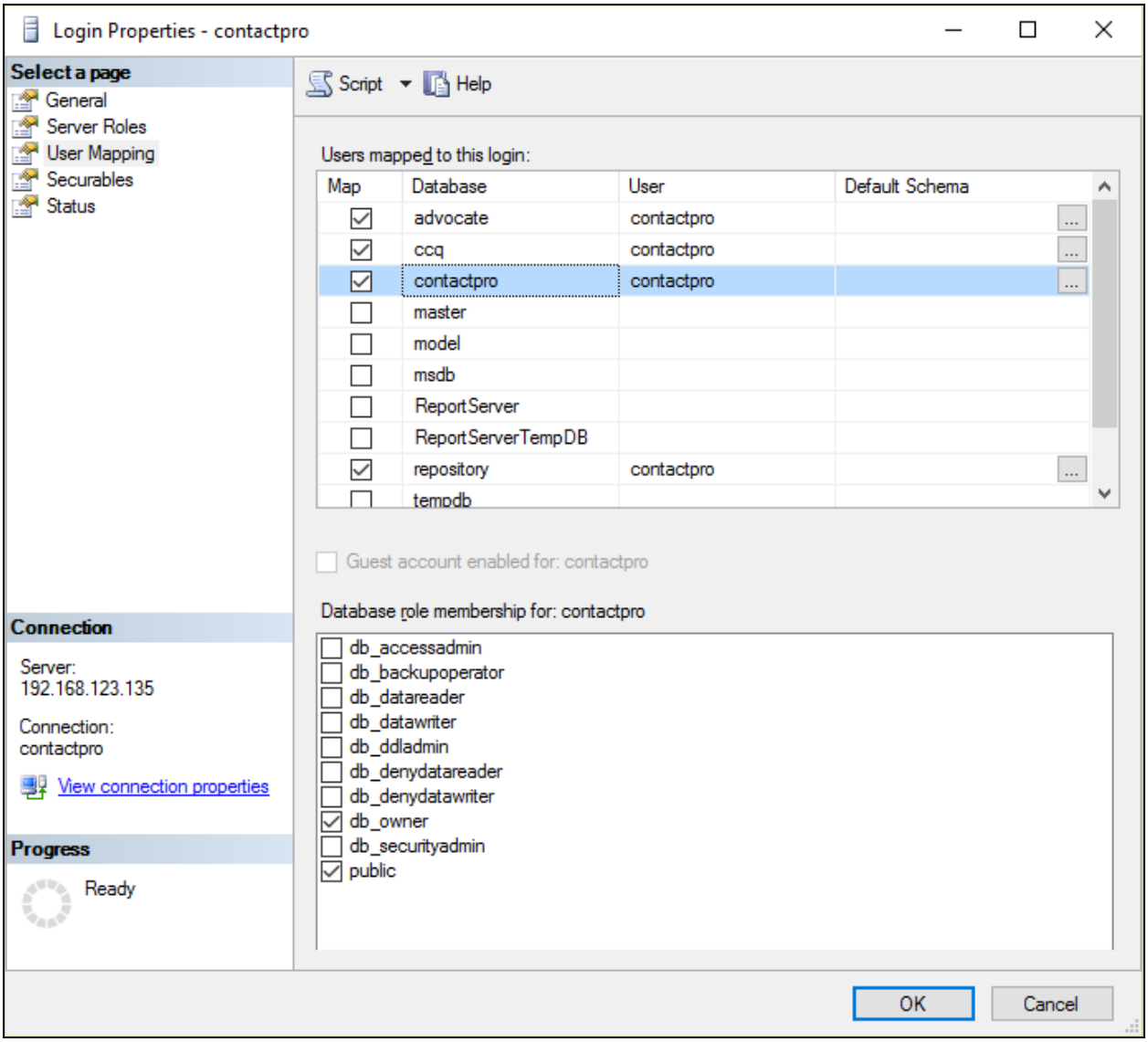
Create a database user named **contactpro**. Right-click on **Login** and click on **New Login**.




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.

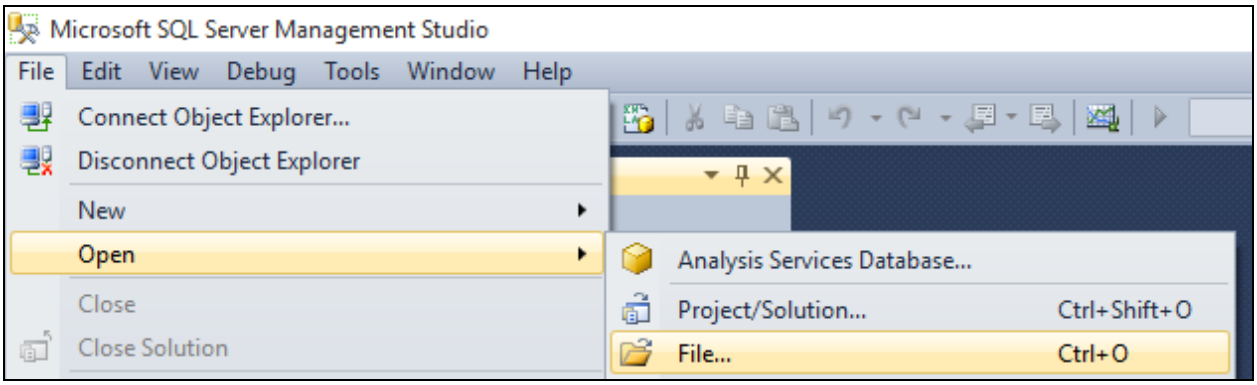


Click on **User Mapping** in the left window. For this user, grant public and **db_owner** access to **Advocate**, **CCQ**, **Repository** and **CONTACTPRO** databases. Click on **OK** at the bottom of the page once done.

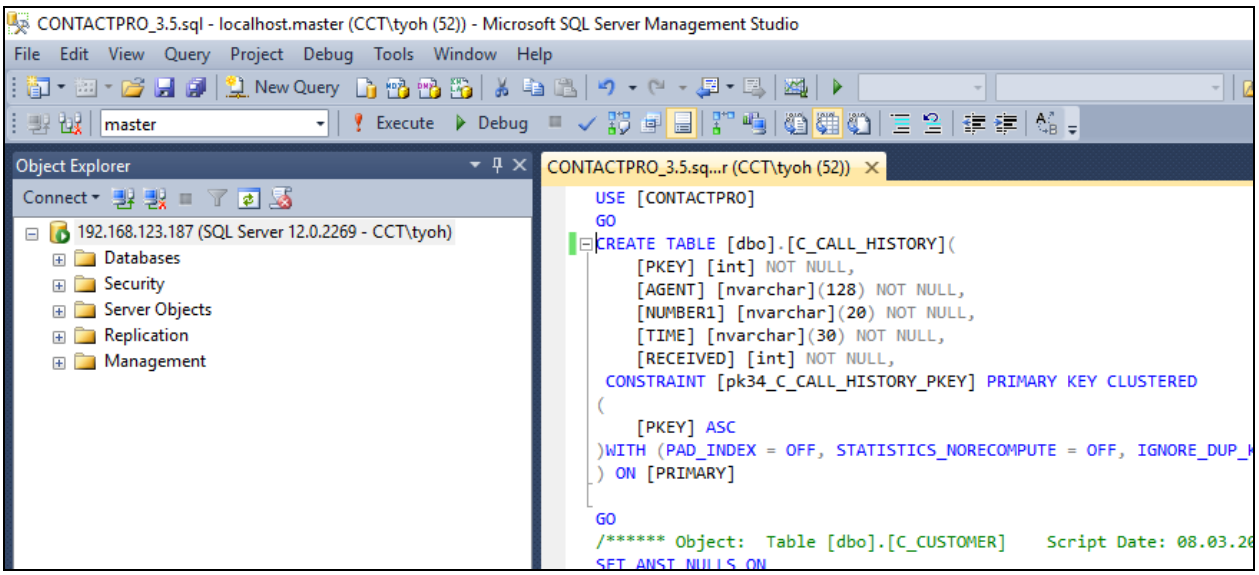


### 9.1.3. Execute CONTACTPRO.sql script for SQL Server

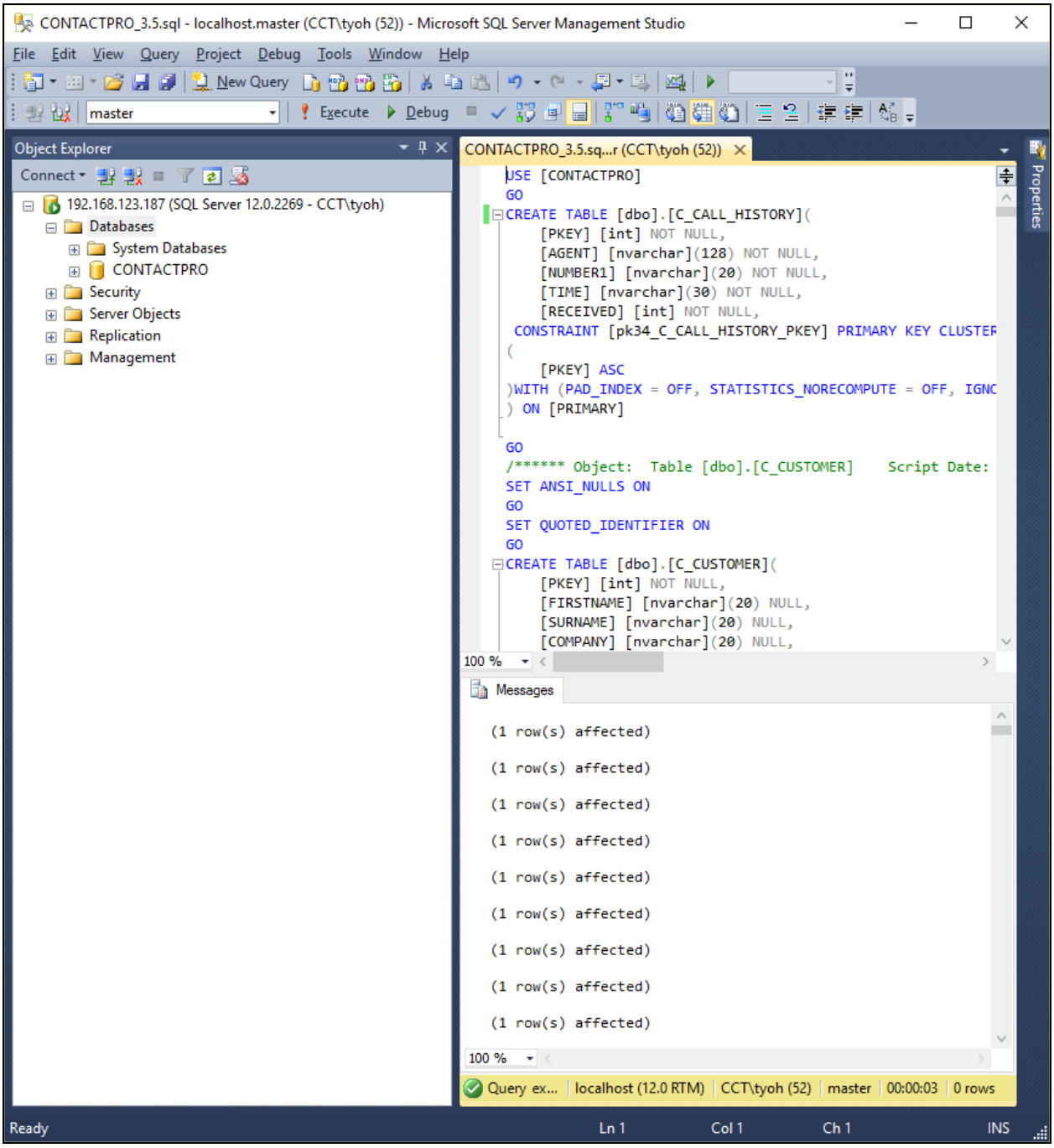
The fill the contents of the **CONTACTPRO** database, open the provided **CONTACTPRO_3.5.sql** script.



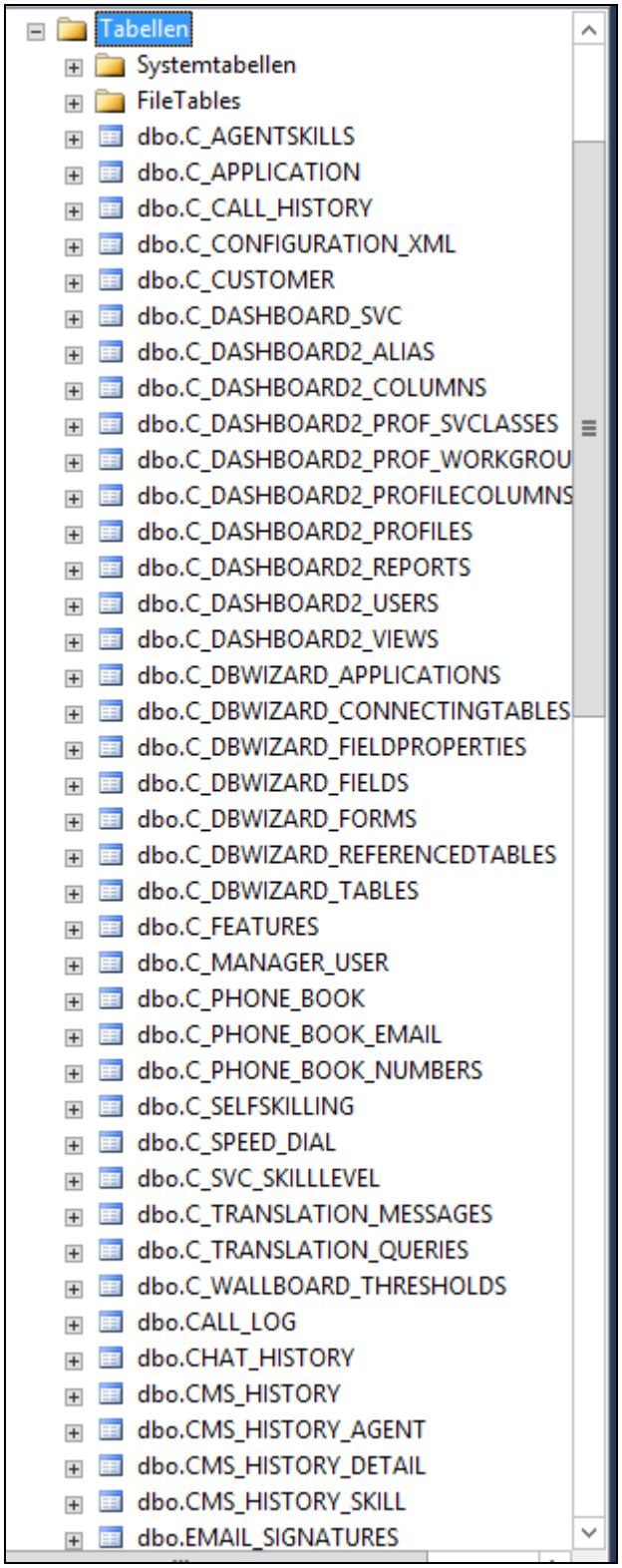

Execute the script by clicking the **Execute** button.



The following shows the script being executed.



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

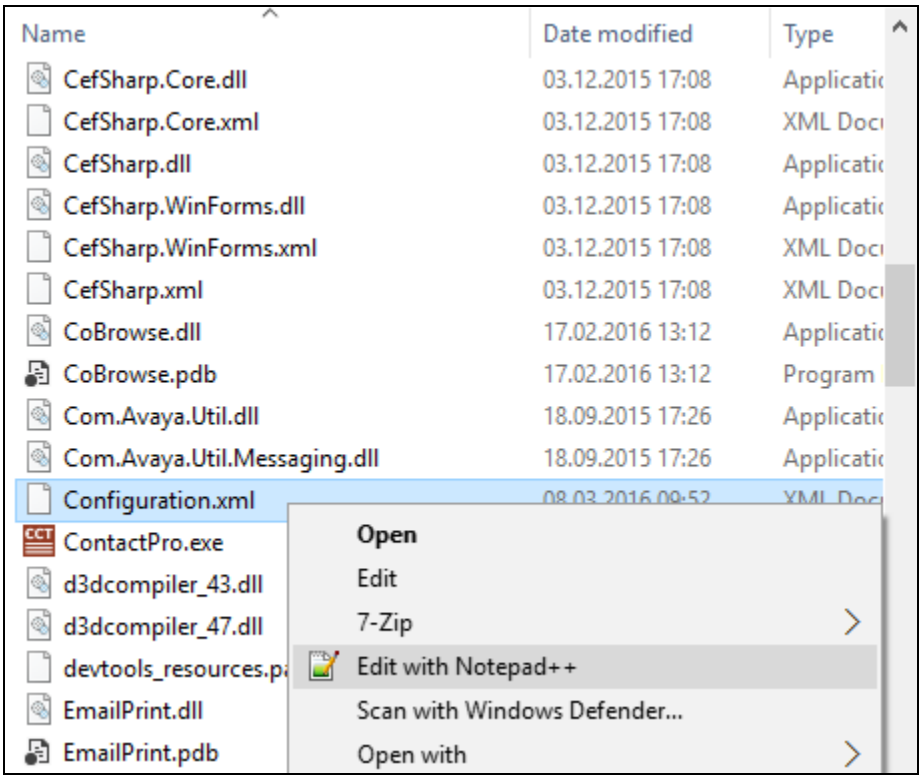


### 9.1.4. Configure ContactPro AIC connection to the database and AIC SDK Server

ContactPro AIC needs the connection settings to the ContactPro Database Connector and the AIC JavaAppBridge (AIC SDK Server). This is the typically the only configuration required before deployment of the software to users.

NOTE: ContactPro AIC utilises a separate ContactPro Database Connector, which is a separate Windows Service providing connection to the database for clients. This service allows security and performance scaling avoiding each client needing to connect directly to the database. There are two versions of the ContactPro Database Connector available. One for MSSQL and one for Oracle.

Navigate to the folder where ContactPro AIC has been installed. Right click on the file called **Configuration.xml** and open this with a suitable text editor as is shown below.

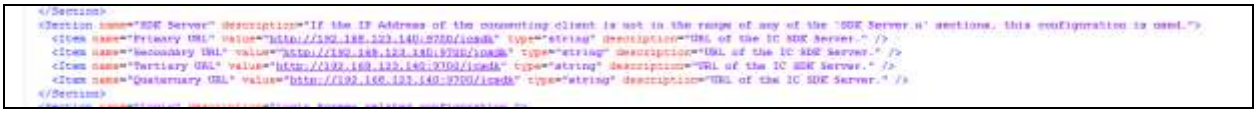


Once this file is opened navigate to the section **Database**. Here the following must be entered correctly.

- **Enabled:** Must be set to true
- **Database Connector:** IP Address and port to the primary CCT database connector
- **Database Connector:** IP Address and port to the secondary CCT database connector


After that, navigate to the section SDK Server. Here the following must be entered correctly.

- **Primary URL:** URL to the primary JavaAppBridge of the AIC system
- **Secondary URL:** URL to the secondary JavaAppBridge of the AIC system
- **Tertiary URL:** URL to the tertiary JavaAppBridge of the AIC system
- **Quaternary URL:** URL to the quaternary JavaAppBridge of the AIC system




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

## 9.2. Create ContactPro AIC Database and User for Oracle database

A database user (and with this the oracle schema) for ContactPro AIC must be created on the Oracle database that hosts the Avaya EMC database.

### 9.2.1. Create Oracle User

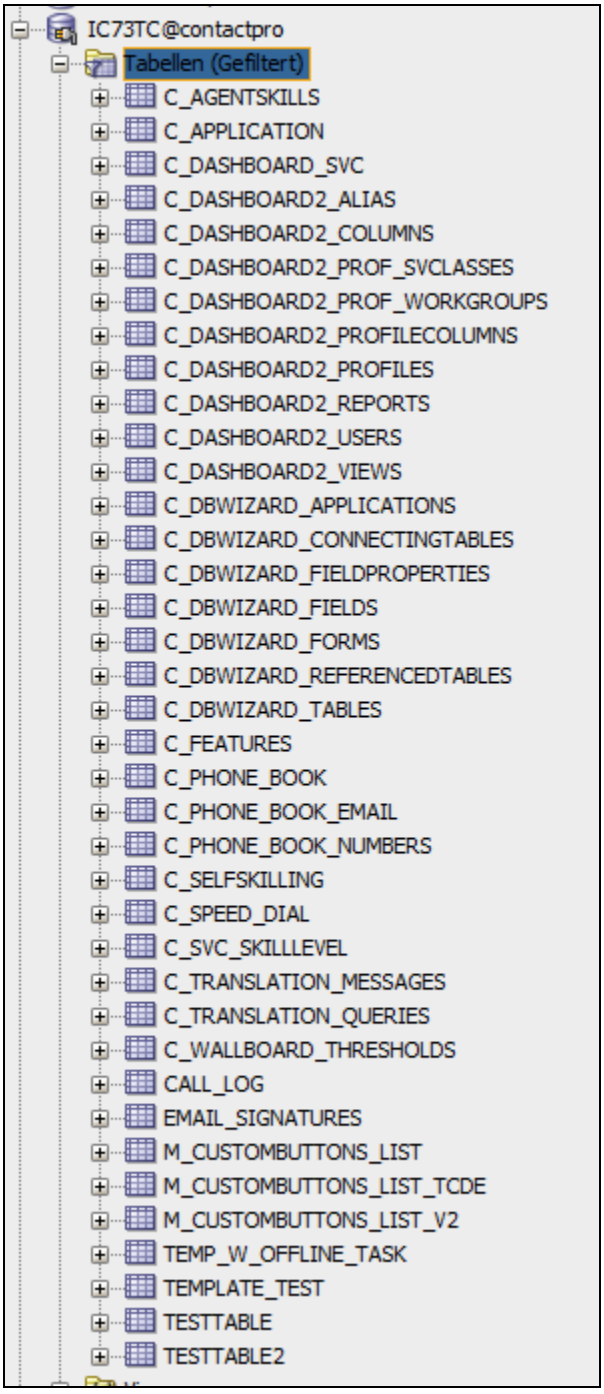
Create a **CONTACTPRO** user on the same Oracle Database where the Avaya AIC databases are located. This can be created by different options (e.g. Oracle EM or SQL Plus). Create the user with the following rights:

- Connect
- Resource
- Unlimited Tablespace
- Select, Insert, Update, Delete, Create, Alter, Drop, Truncate rights to own schema
- Select, Insert, Update and Delete rights to schema ccq and repository
- Select right to schema advocate

### 9.2.2. Execute CONTACTPRO.sql script for Oracle DB

The fill the contents of the **CONTACTPRO** database, open the provided **CONTACTPRO_3.5.sql** script and execute the script.

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

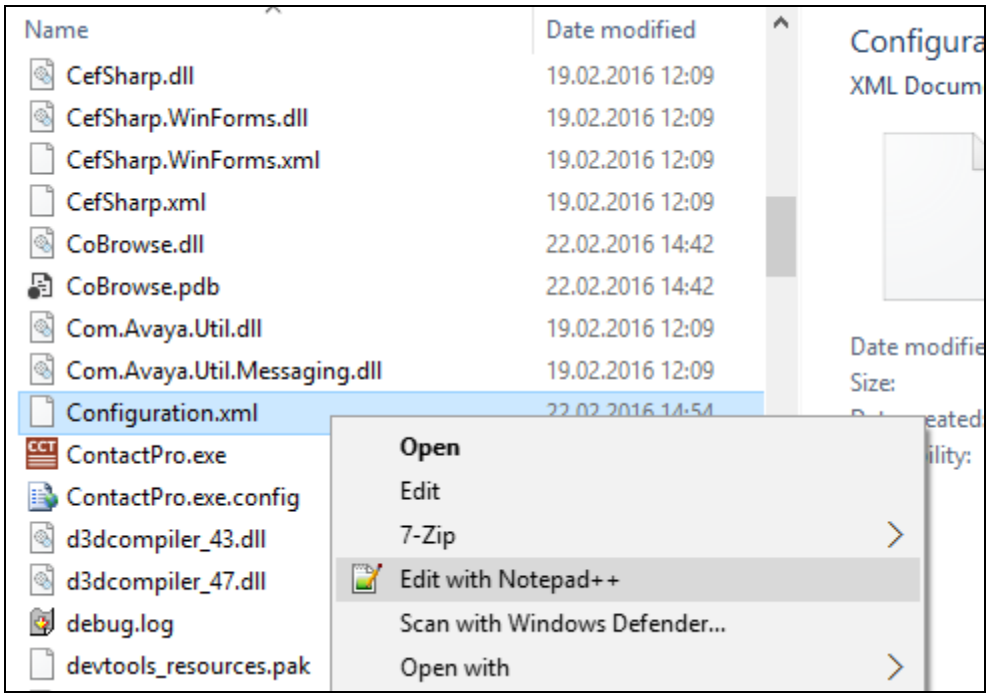


### 9.2.3. Configure ContactPro AIC connection to the database and AIC SDK Server

ContactPro AIC needs the connection settings to the ContactPro Database Connector and the AIC JavaAppBridge (AIC SDK Server). This is the typically the only configuration required before deployment of the software to users.

NOTE: ContactPro AIC utilises a separate ContactPro Database Connector, which is a separate Windows Service providing connection to the database for clients. This service allows security and performance scaling avoiding each client needing to connect directly to the database. There are two versions of the ContactPro Database Connector available. One for MSSQL and one for Oracle.

Navigate to the folder where ContactPro AIC has been installed. Right click on the file called **Configuration.xml** and open this with a suitable text editor as is shown below.

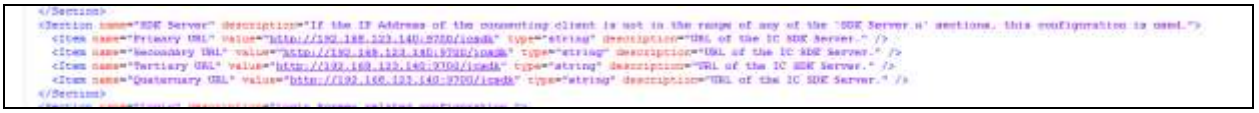


Once this file is opened navigate to the section **Database**. Here the following must be entered correctly.

- **Enabled:** Must be set to true
- **Database Connector:** IP Address and port to the primary CCT database connector
- **Database Connector:** IP Address and port to the secondary CCT database connector


After that, navigate to the section SDK Server. Here the following must be entered correctly.

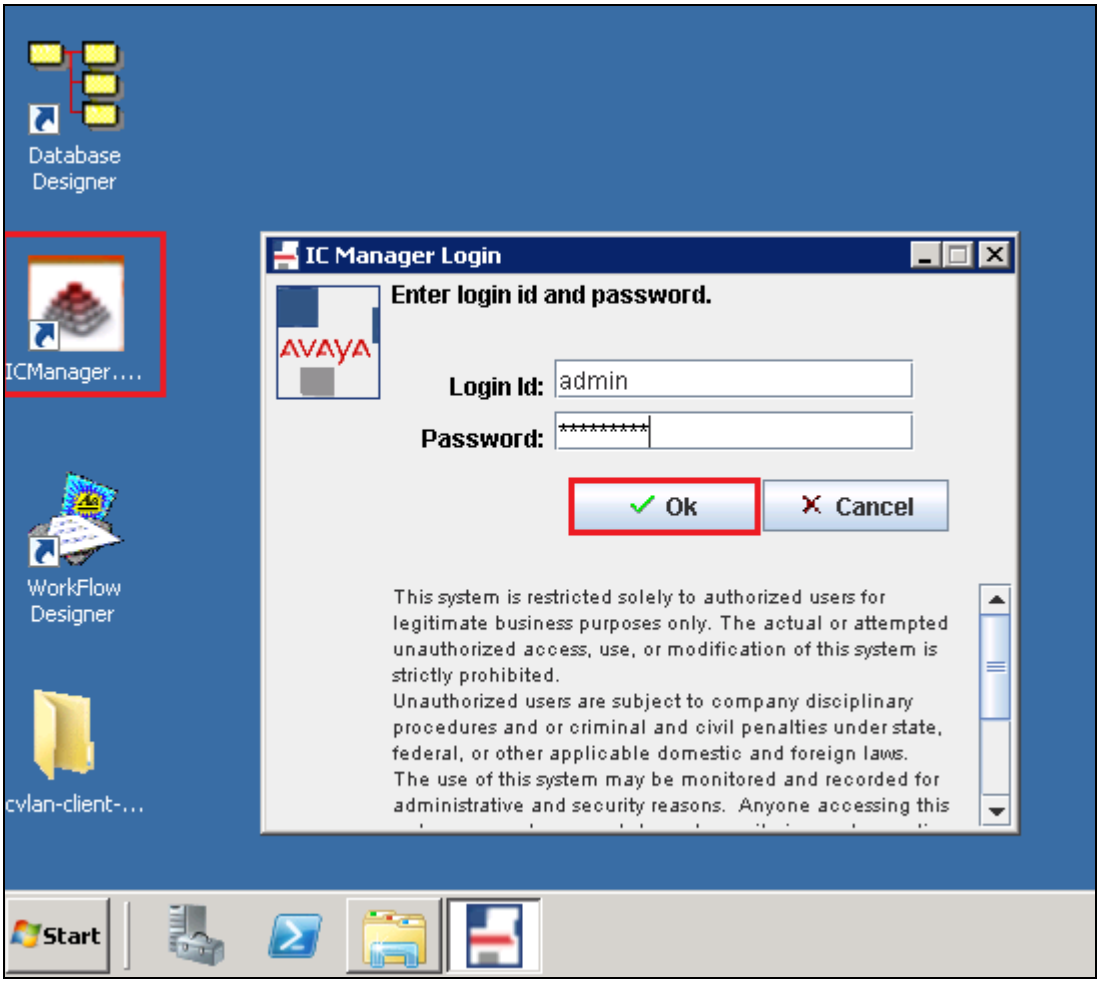
- **Primary URL:** URL to the primary JavaAppBridge of the AIC system
- **Secondary URL:** URL to the secondary JavaAppBridge of the AIC system
- **Tertiary URL:** URL to the tertiary JavaAppBridge of the AIC system
- **Quaternary URL:** URL to the quaternary JavaAppBridge of the AIC system



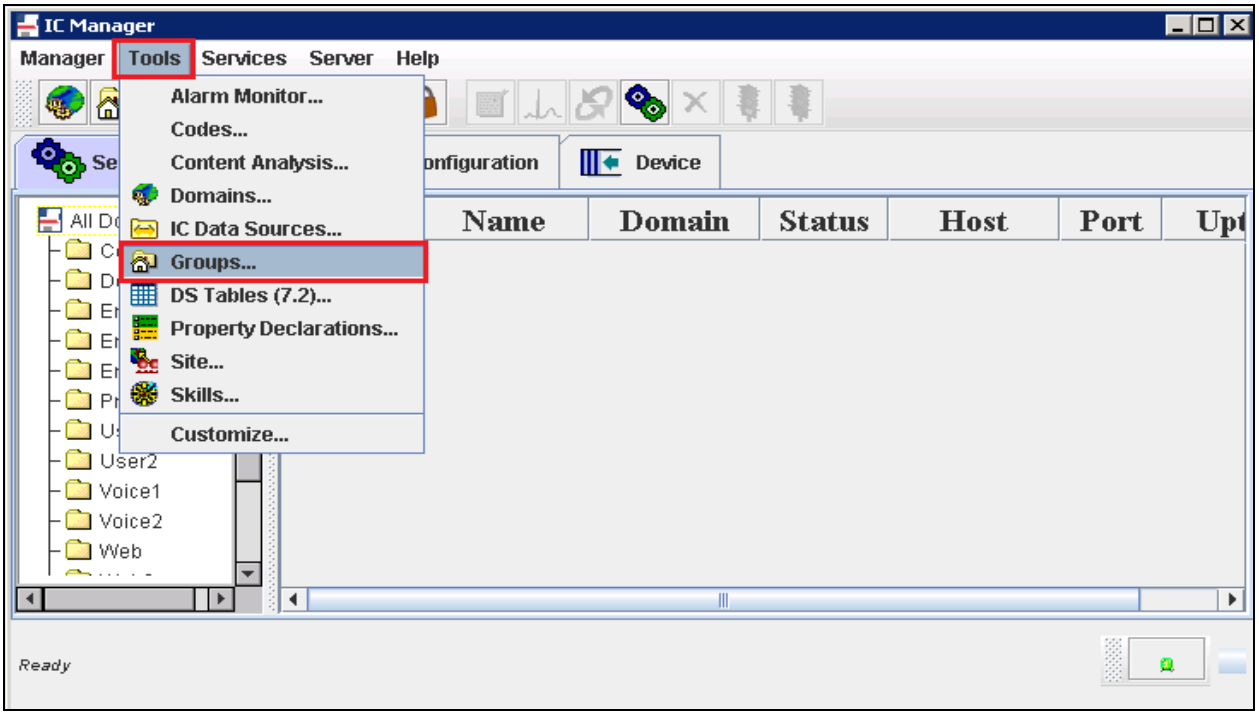

Once this information has been entered correctly sane the file (**File → Save** (not shown)).

## 9.3. Configure the connection to EDP CoBrowse using Avaya Interaction Center Manager

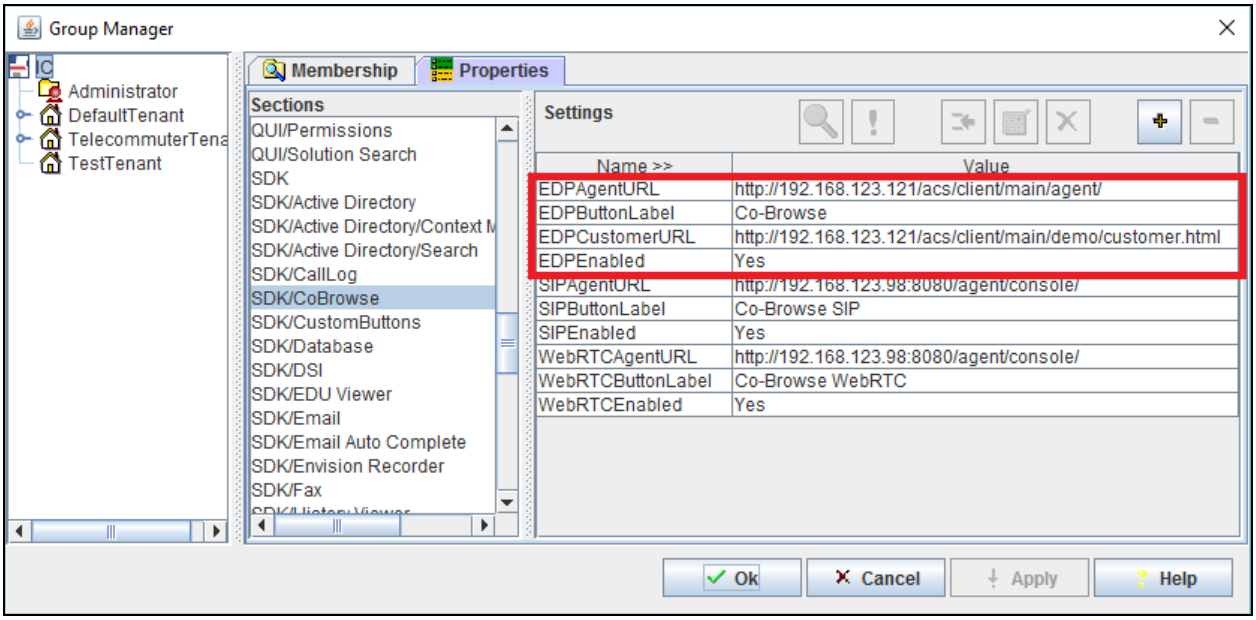
From the Avaya Interaction Center Server open the Interaction Center Manager (**ICManager**). Enter the proper credentials and click on **OK**.



Once logged in, navigate to **Tools → Groups**, as shown below.




Click on the **IC** group in the left window and select the **Properties** tab in the main window. Scroll down to **SDK/CoBrowse** and click on that.




The following properties need to be added or changed:

- EDPEnabled
    - Default:No. Show or Hide the Toolstrip Button.

- EDPButtonLabel
    - Default:Co-Browse.  Label text of the button.
- EDPAgentURL
    - Default:http://[YourServer]/acs/client/main/agent/.  URL for the Agent.
- EDPCustomerURL

Default:http://[YourServer]/acs/client/main/demo/customer.html.  URL for the Customer.

# 10. 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 EMC.

## 10.1. Verify Status of Communication Manager Agent

Enter the command **list agent-loginID** verify that agent **8271001**is logged-in to extension **8270001**.

```
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      Russell         8270001                                  1   lvl
                10/01      /       /       /       /       /       /       /
```

Enter the command **status station 8270001** 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**.**

```
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
     /        /        /        /        /        /        /
     /        /        /        /        /        /        /
     /        /        /        /        /        /        /
```

## 10.2. 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       aes63vmpg      established    18        18
```

## 10.3. 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**.


## 10.4. Verify ContactPro for EMC and AES

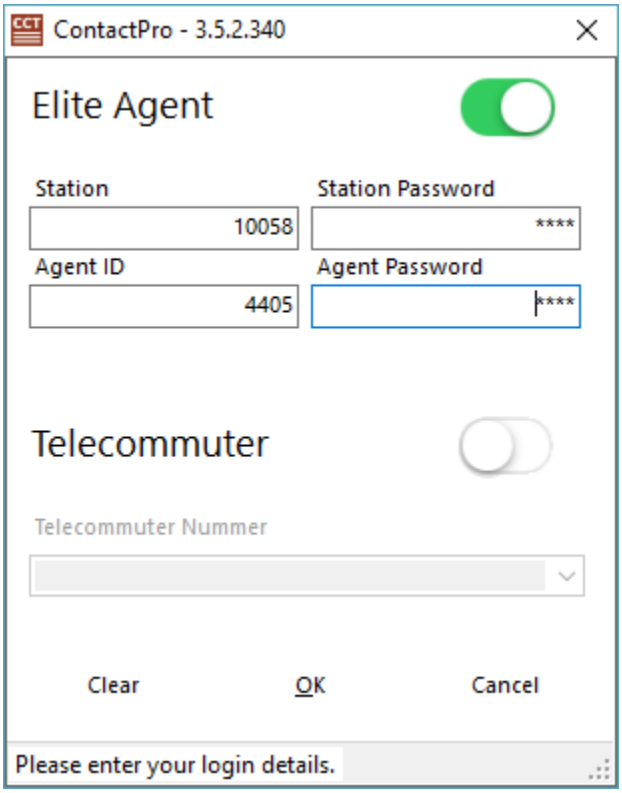
### 10.4.1. Verify login of ContactPro and AES

From the Client PC open the application **ContactPro** or AES (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.

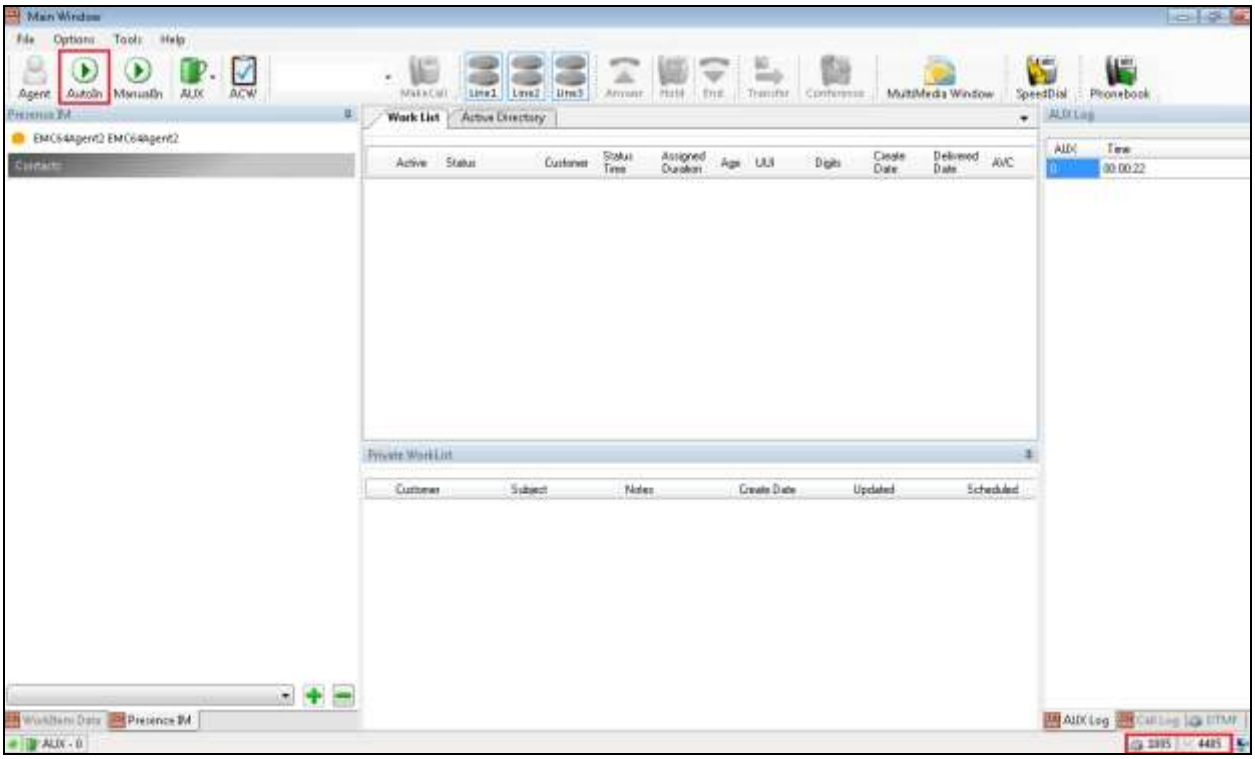
- **ACM Station Password** This is the password for the station that is to be controlled.
- **ACM Agent ID** This is the Agent ID created.
- **ACM Agent Password** This is the password of the agent noted or created.

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



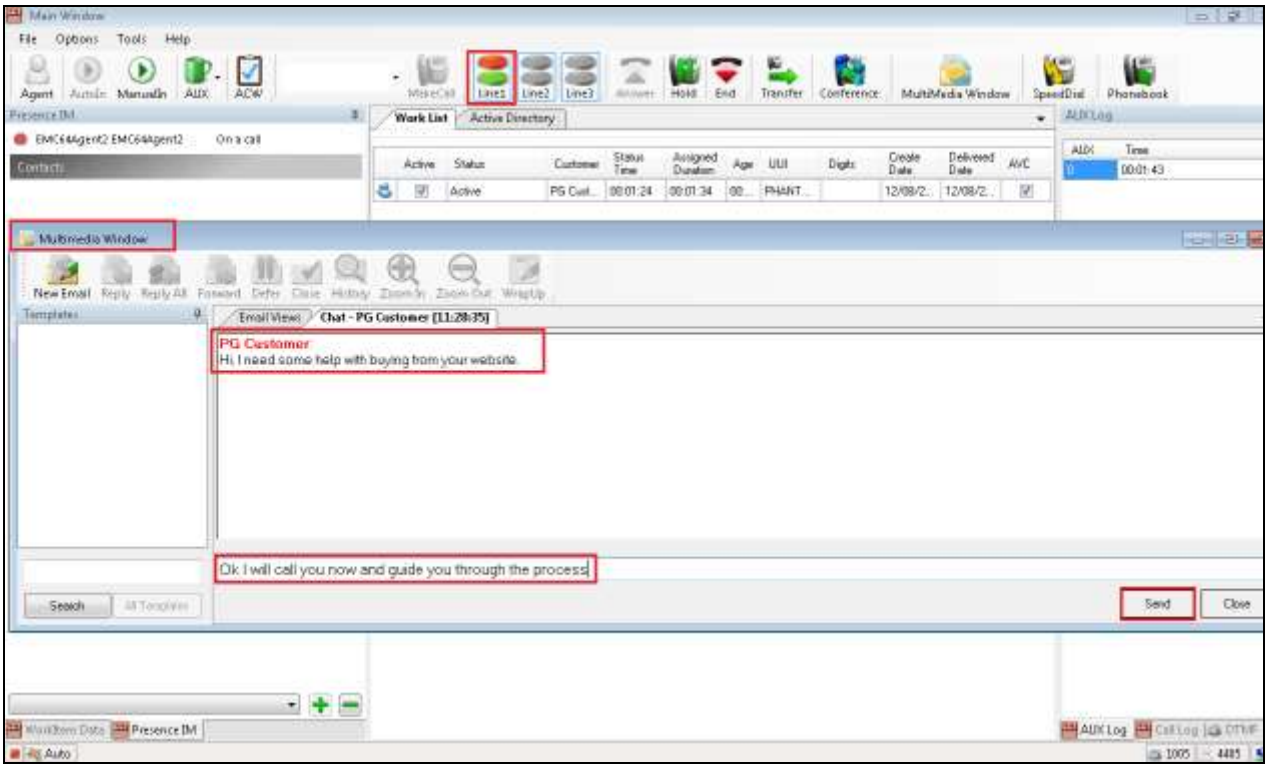
### 10.4.2. Verify Agent Status using ContactPro EMC and AES

Once logged in the agent state can be changed using the buttons at the top left highlighted below. Note also the station number (**1005**) and Agent ID (**4405**) once logged in. Click on **AutoIn** to make the agent ready.

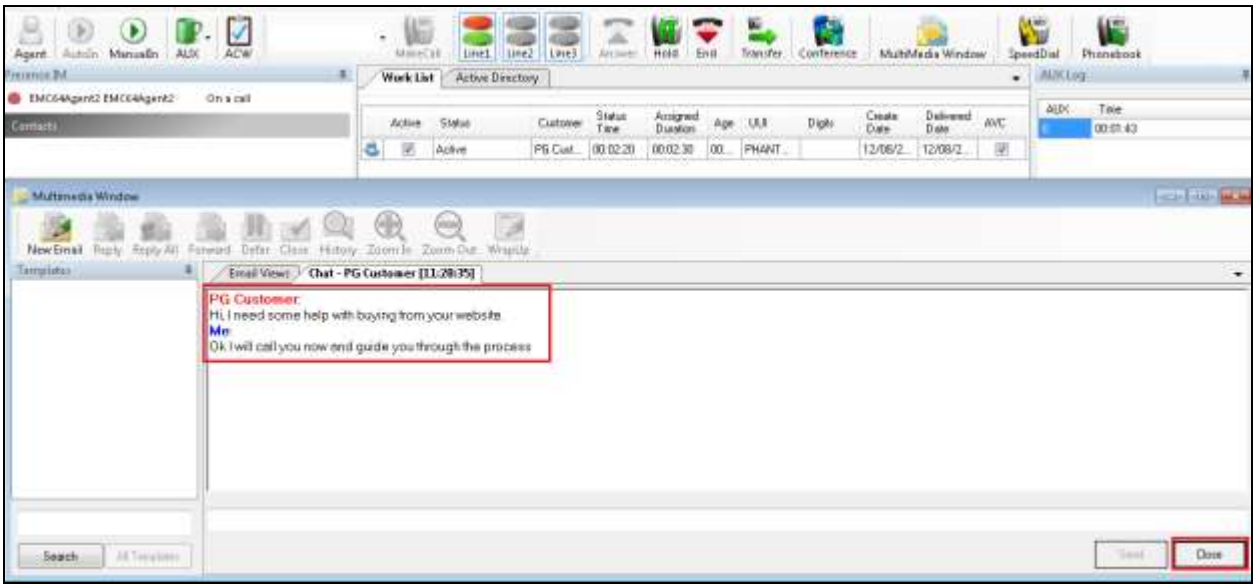


A web request is generated by a customer (not shown) and queued to this agent. Once AutoIn is pressed above the call appears as **Alerting** on the ContactPro desktop. The call can be answered by pressing the **Answer** icon highlighted below.

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.



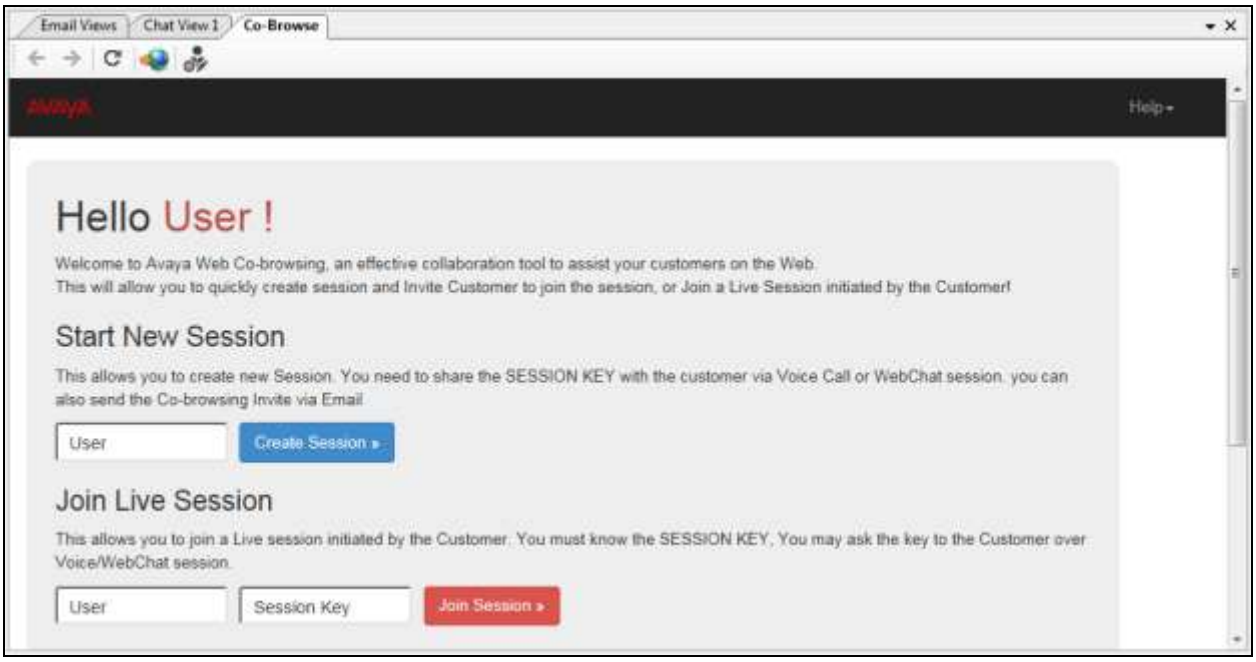
With the multimedia call ended a new call can be made if required again by entering the digits and pressing on **Make Call** as is shown. In this example, the agent is calling the customer at his/her request from the webchat session previous.


## 10.4.3. Verify CoBrowse status in ContactPro EMC and AES

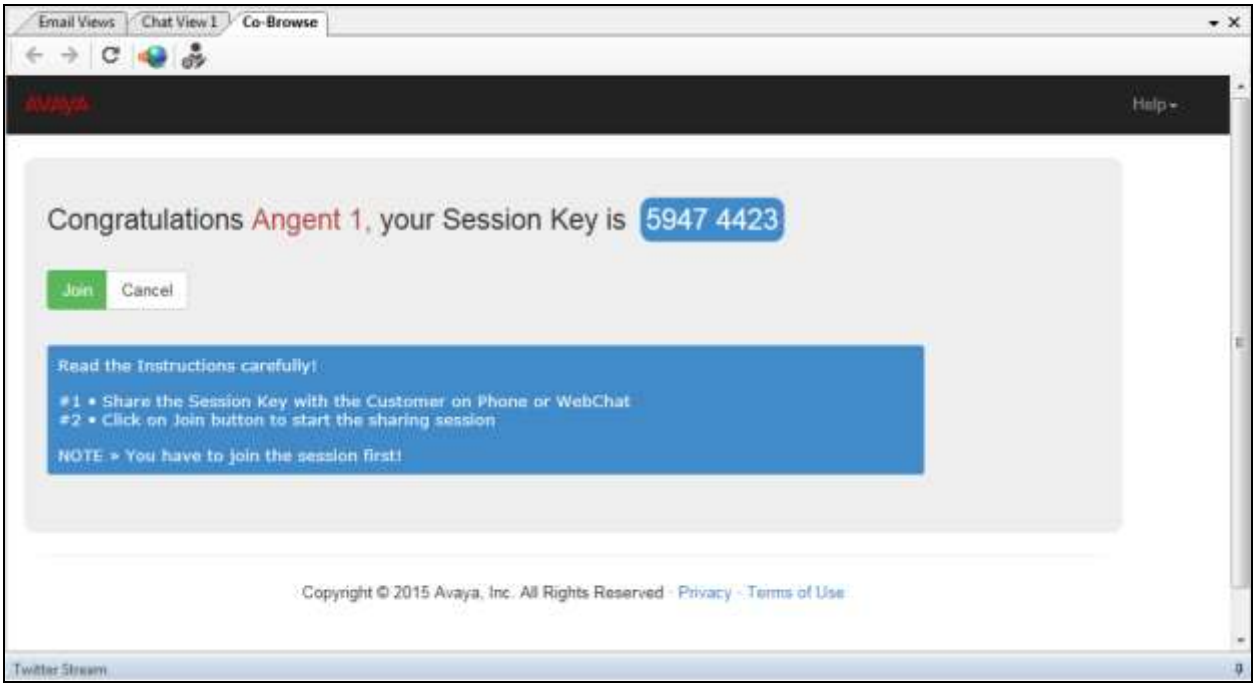
### 10.4.3.1 Initiate Co-Browsing

The EDP Co-Browse snap-in can be started with clicking on the Co-Browse button.


A new Tab view is to be seen:




Enter a **user** name and click on "Create Session". The system shows the **Session Key**.




Click on "Join" to continue.

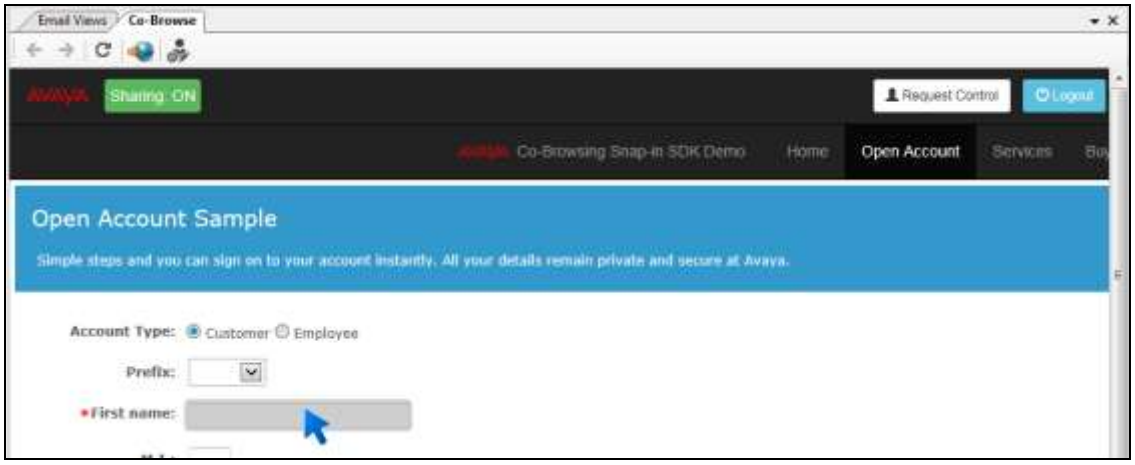
Copy the Customer URL by clicking button  . Paste the URL into customer chat.

As soon as the customer joins the Session, see the screen of the customer and Session control buttons above it:

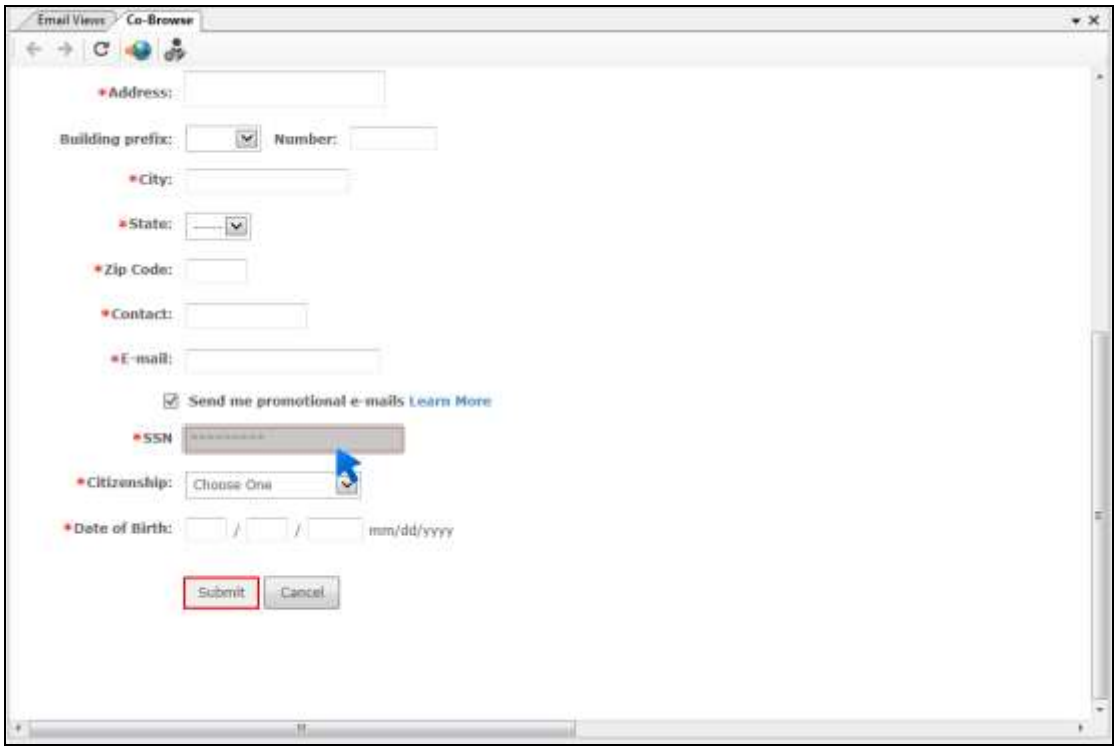

To open the Site in an external browser windows, just click on  .

### 10.4.3.2 Monitor customers Activities

Customer's activities can be viewed. Mouse movements are indicated by an Arrow.



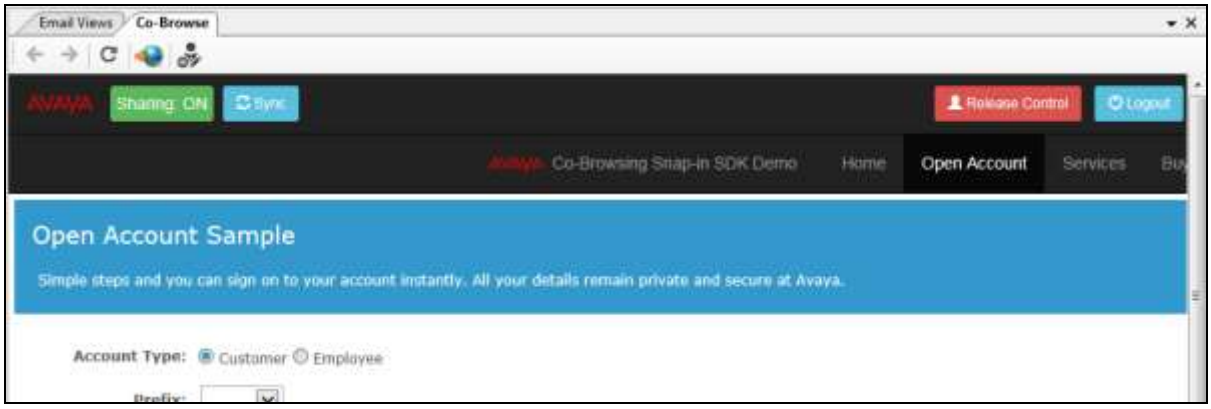

Sensitive data the customer enters into forms are hidden for the agent. The inputs would be represented by stars:



### 10.4.3.3 Control Customer Screen

Click on “Request Control” to be able to control the desktop of customer.

As soon the customer allow the control,  agents are able to navigate through customers screen and insert data to fields.




Press “Release Control” to give control back to customer.

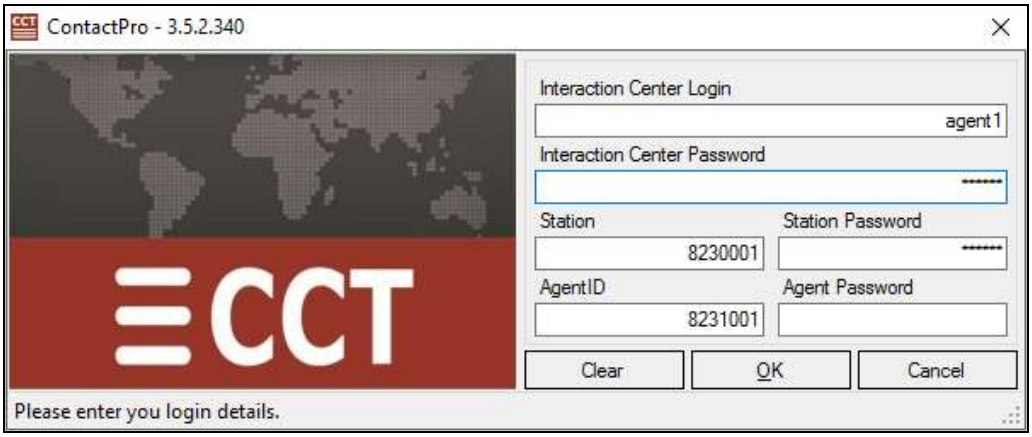
### 10.4.3.4 End Session

To end the Session click on “Logout”. The Tab in the client can be closed by clicking the x.

## 10.5. Verify ContactPro for AIC

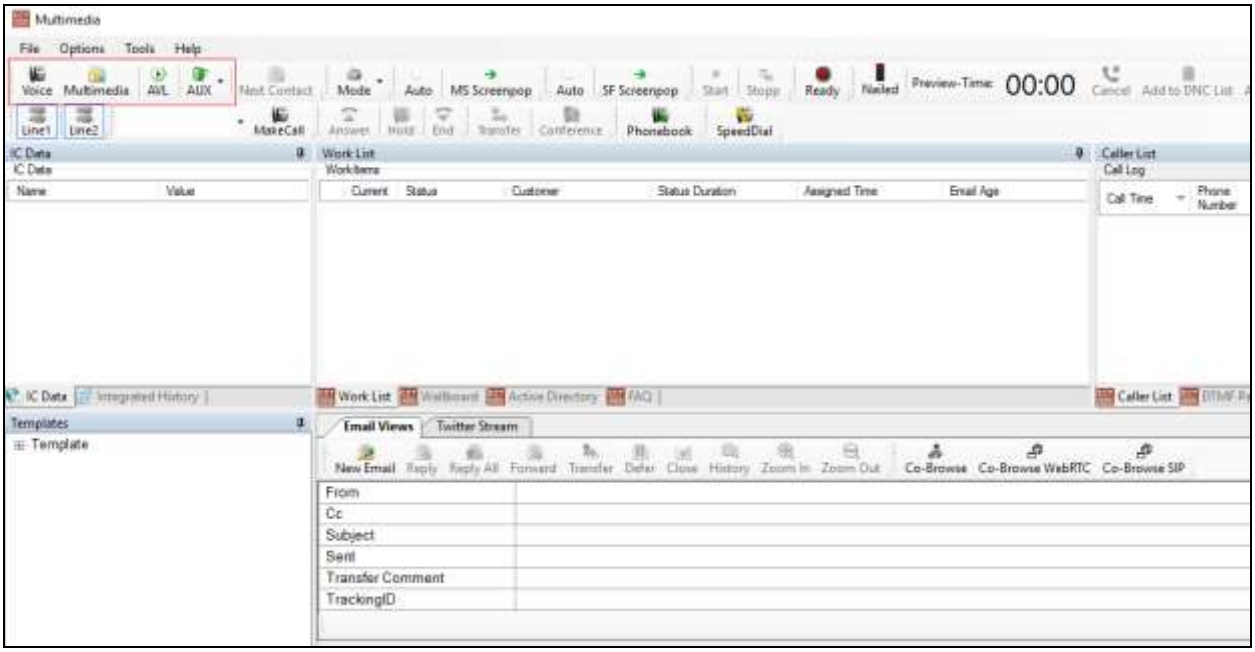
### 10.5.1. Verify CCT ContactPro AIC Login

Open the **ContactPro** AIC desktop, in the example below this was from a shortcut on the agents desktop. Enter the proper credentials and click on **OK**.

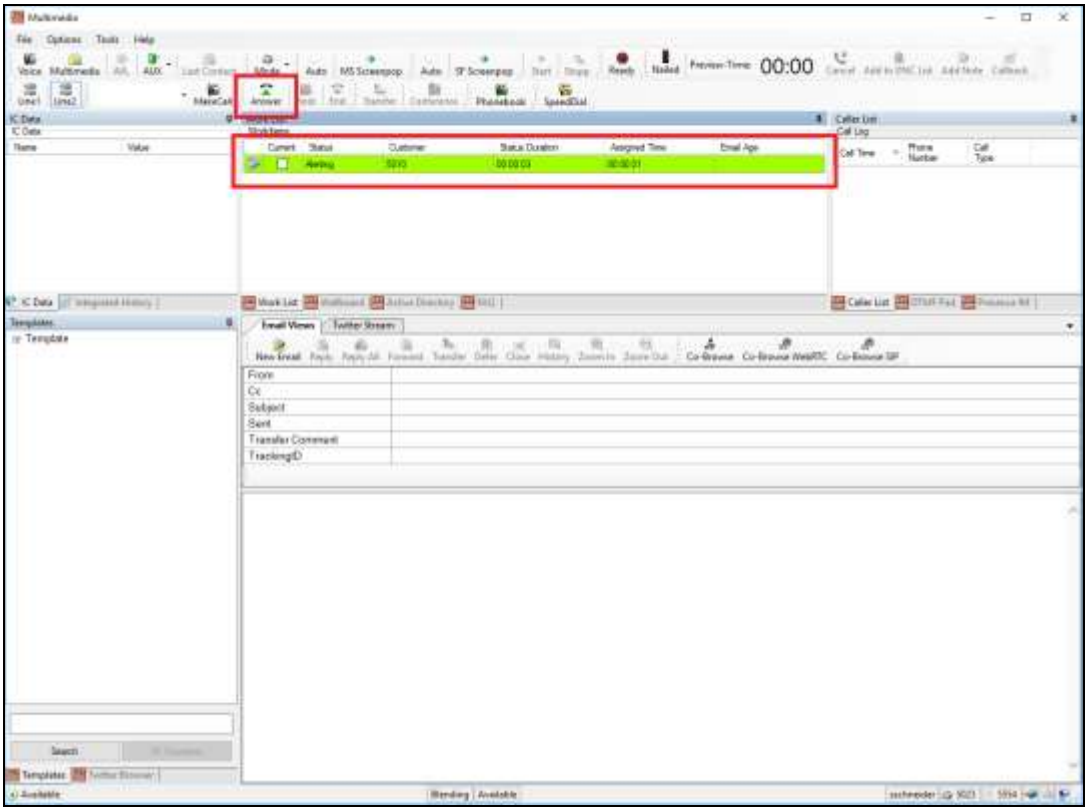



### 10.5.2. Verify Agent Status using ContactPro AIC

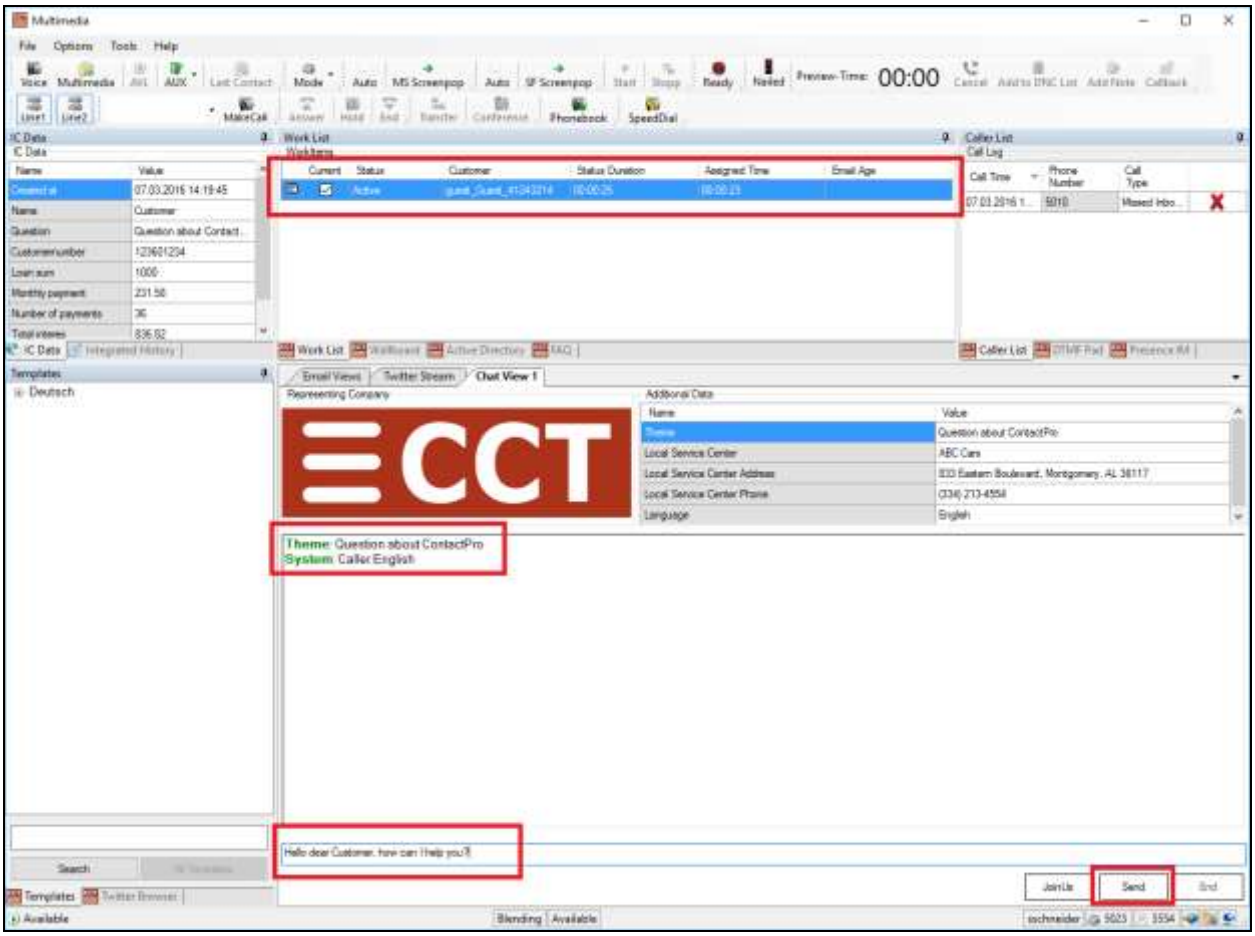
Once logged in the agent state can be changed using the buttons at the top left highlighted below. Note also the station number (**1005**) and Agent ID (**4405**) once logged in. Click on **AVL** to make the agent ready.



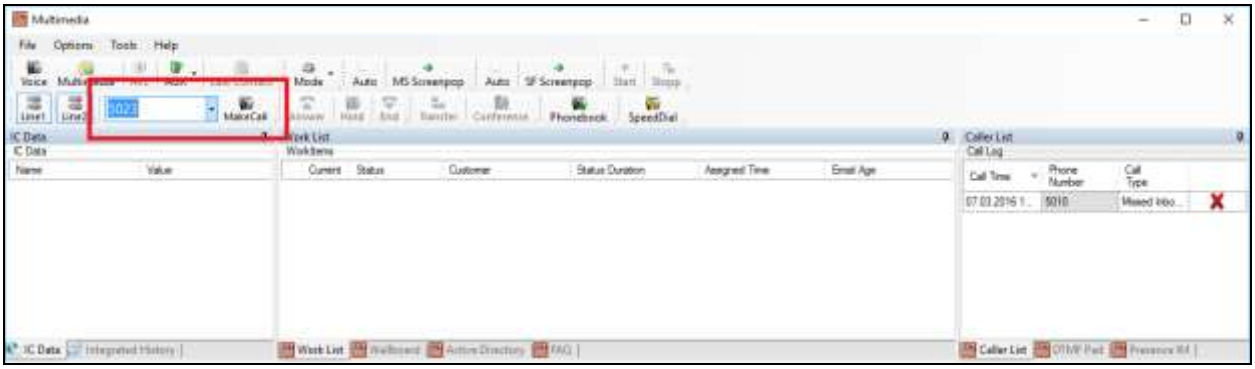
A web request is generated by a customer (not shown) and queued to this agent. Once AVL is pressed above the call appears as **Alerting** on the ContactPro desktop. The call can be answered by pressing the **Answer** icon highlighted below.



Once a chat is answered the web chat is opened in a new tab and the the agent can respond to that request as is shown below, by entering some text and clicking **Send**.




A new call can be made if required by entering the digits and pressing on **Make Call** as is shown. In this example the agent is calling another agent extension.



### 10.5.3. Verify CoBrowse status in ContactPro AIC

This steps to verify CoBrowse status in ContactPro AIC is identical with ContactPro EMC.

Refer to **Section 10.4.3** Verfy CoBrowse status in ContactPro EMC and AES.

# 11. Conclusion

These Application Notes describe the configuration steps required for ContactPro EMC, AES and AIC from CCT Deutschland GmbH to interoperate with Avaya Aura® Call Center Elite Multichannel R6.4.1, Avaya Interaction Center, Avaya Aura® Application Enablement Services R6.3 and Avaya Engagement Development Platform CoBrowse Snap-in. All feature and serviceability test cases were completed successfully.

# 12. 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] *Deploying Avaya Aura® Call Center Elite Multichannel in an Avaya Customer Experience Virtualized Environment* Release 6.4

[2] *Avaya Aura® Call Center Elite Multichannel Installation Guide* Release 6.4

[3] *Administering Avaya Aura® Call Center Elite Multichannel* Release 6.4.x

[4] *Avaya Aura® Call Center Elite Multichannel Release* Notes Release 6.3.1

[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] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 7.0*

[12] *Application Notes for configuring ContactPro EMC from CCT Deutschland GmbH with Avaya Aura® Call Center Elite Multichannel R6.4.1 and Avaya Aura® Application Enablement Services R6.3*

[13] *Application Notes for configuring Avaya Aura® Communication Manager R6.3, Avaya Aura® Application Enablement Services R6.3 and Avaya Interaction Center R7.3 with CCT ContactPro v3*


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

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

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.