Avaya Solution & Interoperability Test Lab

Application Notes for CCT ContactPro® 5.3 with Avaya Proactive Outreach Manager 3.1.3 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CCT ContactPro® to interoperate with Avaya Proactive Outreach Manager. CCT 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.

1. Introduction

These Application Notes describe the configuration steps required for CCT ContactPro®, 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.

CCT ContactPro® offers a connection to Avaya Application Enablement Server (AES) and Avaya Aura® Call Center Elite. 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 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.

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 Predictive 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 log out.
- **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 successfully.

2.3. Support

Support for CCT 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
Tilsiter Str. 1
60487 Frankfurt am Main
Germany
Phone: +49 69 7191 4969 0
Fax: +49 69 7191 4969 666

Werner-von-Siemens-Str. 6
86159 Augsburg
Germany
Phone: +49 821 455 152 700
Fax: +49 821 455 152 777

CCT Europe GmbH
Sumpfstrasse 26
6312 Steinhausen
Switzerland
Phone: +41 41 748 42 22
Fax: +41 41 748 42 23

CCT Software LLC
1801 N.E. 123rd Street, Suite 314
North Miami, 33138 FL
United States of America
Phone: +1 786 738 5253

3. Reference Configuration

The configuration in **Figure 1** will be used to compliance test ContactPro using a connection to POM.

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

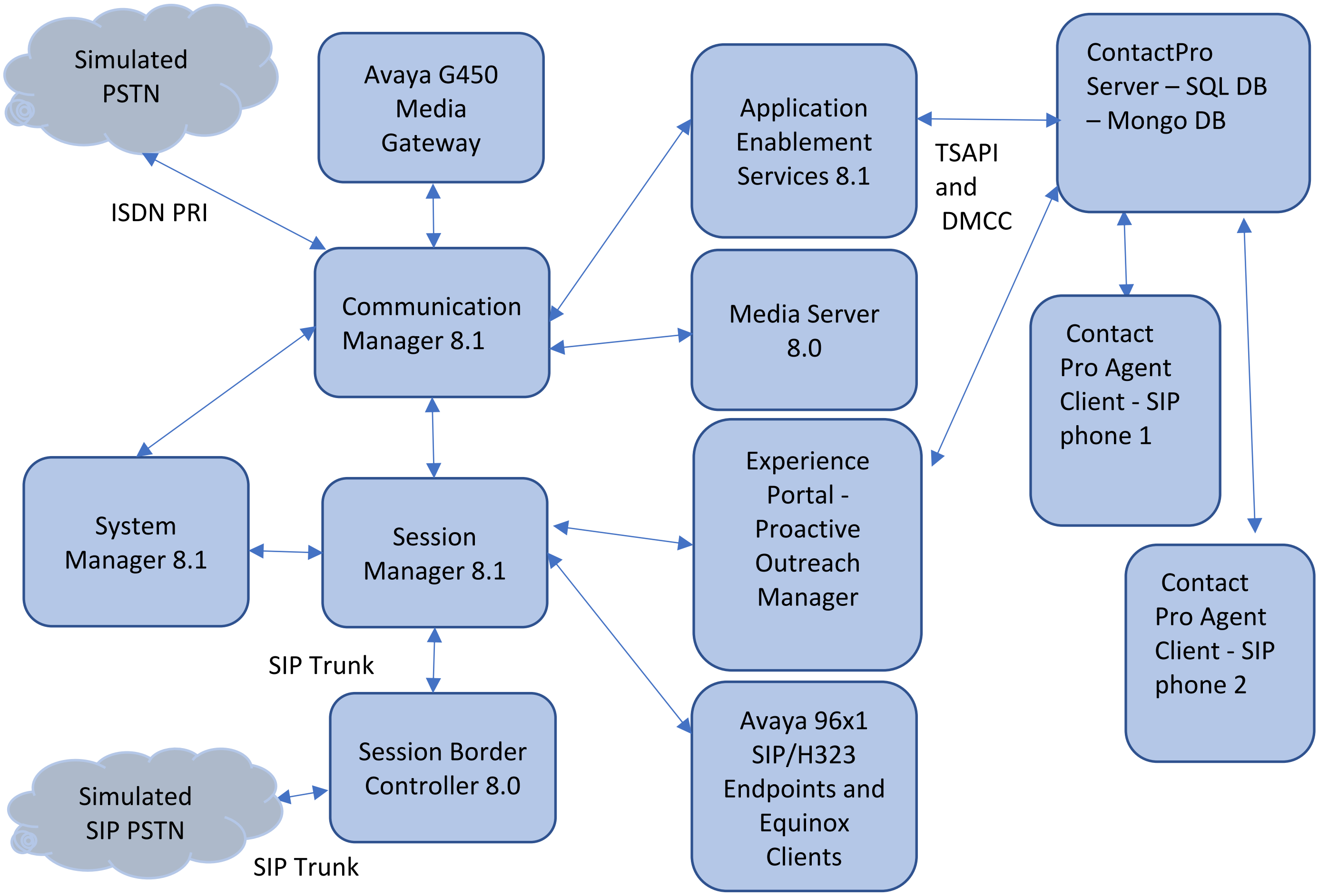

Simulated PSTN
Avaya G450 Media Gateway
Application Enablement Services 8.1
ContactPro Server – SQL DB – Mongo DB
TSAPI and DMCC
ISDN PRI
Communication Manager 8.1
Media Server 8.0
Contact Pro Agent Client - SIP phone 1
Experience Portal - Proactive Outreach Manager
System Manager 8.1
Session Manager 8.1
Contact Pro Agent Client - SIP phone 2
SIP Trunk
Session Border Controller 8.0
Avaya 96x1 SIP/H323 Endpoints and Equinox Clients
Simulated SIP PSTN
SIP Trunk

Figure 1: Compliance Testing Configuration

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 in Virtual Environment	8.1.1
Avaya Aura® Session Manager in Virtual Environment	8.1.1
Avaya Aura® Communication Manager in Virtual Environment	8.1.1
Avaya G450 Media Gateway	41.9.0
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.1
Avaya Aura® Experience Portal	7.2.3
Avaya Proactive Outreach Manager	3.1.3
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya 9641 & 9621 IP Deskphone (SIP)	7.1.6
CCT Deutschland GmbH ContactPro - Client Agent Desktop	5.3.0.310

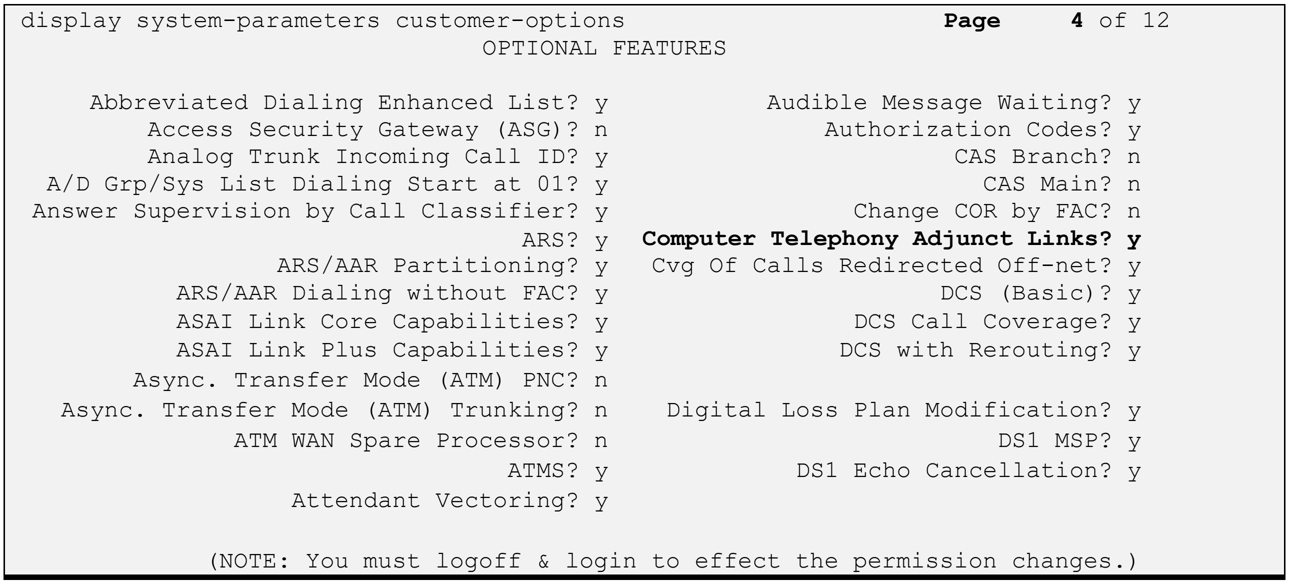
5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer hunt group and agent

5.1. Verify License

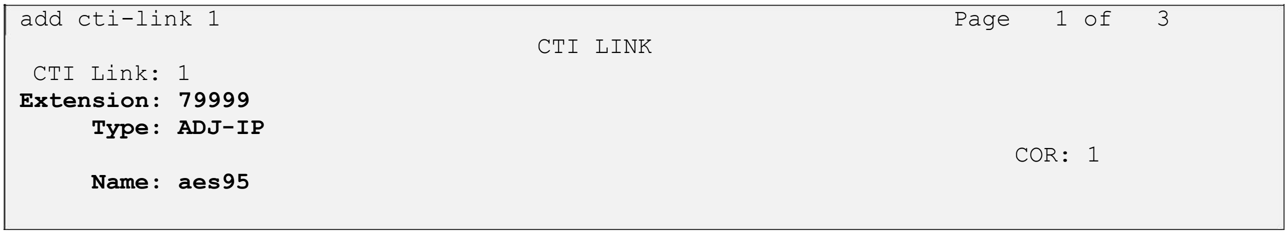
Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.



```
display system-parameters customer-options                        Page     4 of 12
                                OPTIONAL FEATURES

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

              (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer CTI Link

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



```
add cti-link 1                                                    Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 79999
     Type: ADJ-IP
                                                                      COR: 1
     Name: aes95
```

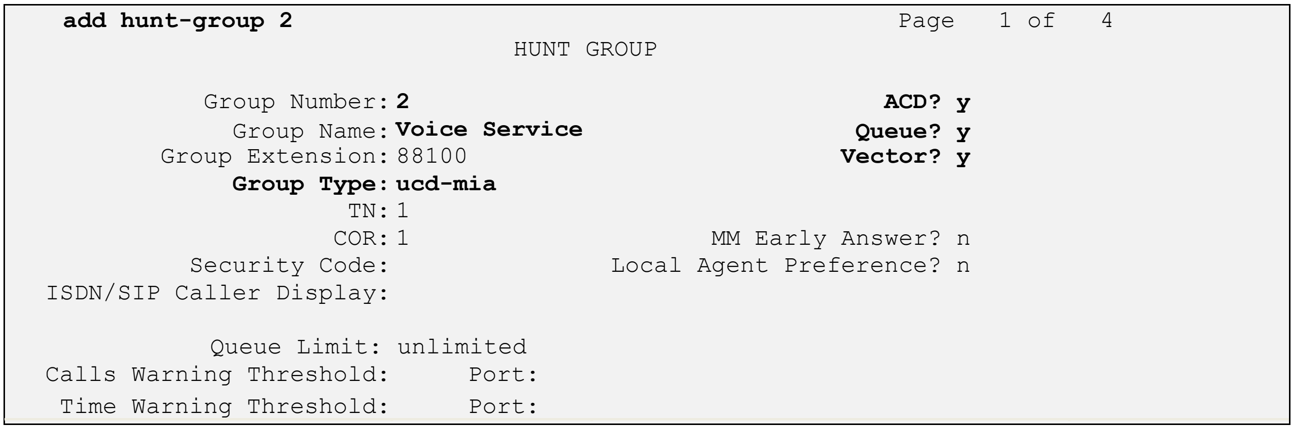
5.3. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Vector Directory Number (VDN), which points to a vector. The vector then points to a hunt group associated with an agent. The following sections give step by step instructions on how to add the following:

- Hunt Group
- Agent

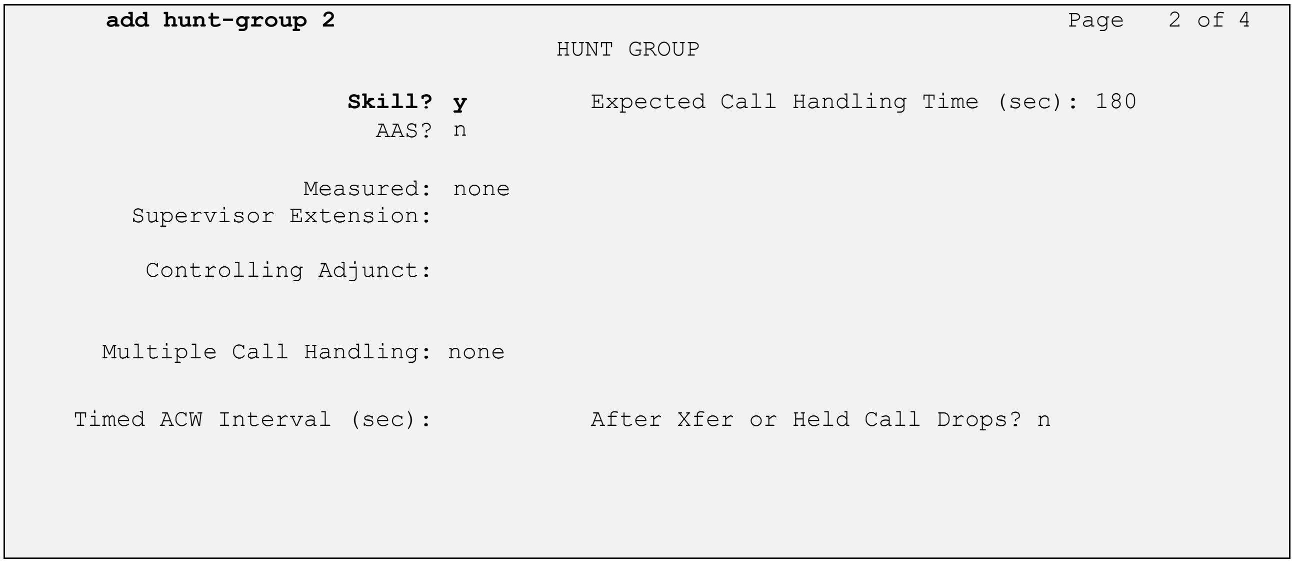
5.3.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x,** where **x** is the new hunt group number. For example, hunt group **2** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.



```
  add hunt-group 2                                           Page   1 of   4
                                   HUNT GROUP

            Group Number: 2                                    ACD? y
              Group Name: Voice Service                      Queue? y
         Group Extension: 88100                             Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                        MM Early Answer? n
           Security Code:                    Local Agent Preference? n
 ISDN/SIP Caller Display:

            Queue Limit: unlimited
 Calls Warning Threshold:     Port:
  Time Warning Threshold:     Port:
```

On **Page 2** ensure that **Skill** is set to **y** as shown below.

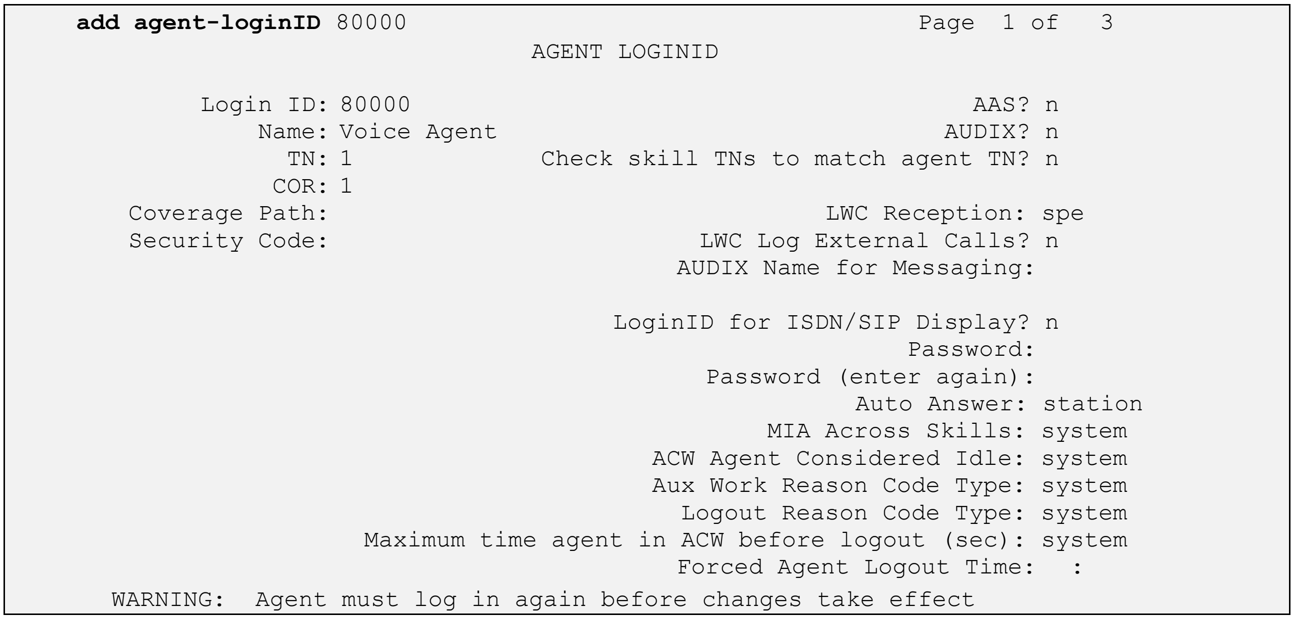


```
     add hunt-group 2                                                Page   2 of 4
                                   HUNT GROUP

                        Skill? y        Expected Call Handling Time (sec): 180
                          AAS? n

                     Measured: none
         Supervisor Extension:

          Controlling Adjunct:


      Multiple Call Handling: none


    Timed ACW Interval (sec):           After Xfer or Held Call Drops? n
```

5.3.2. Add Agent

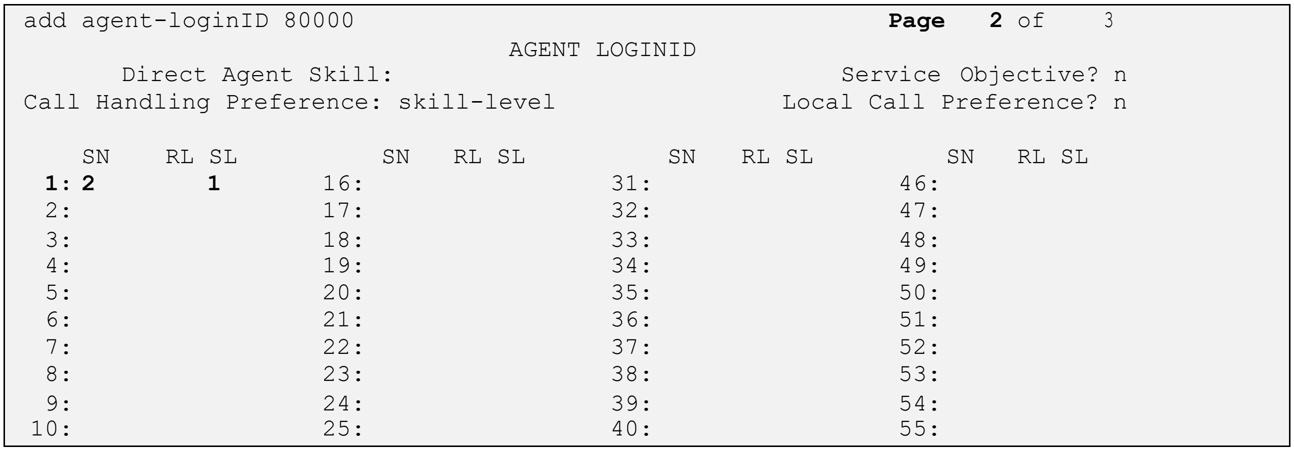
In the compliance testing, the agents 80000 and 80001 were created.

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



```
    add agent-loginID 80000                                     Page  1 of   3
                                     AGENT LOGINID

           Login ID: 80000                                          AAS? n
               Name: Voice Agent                                  AUDIX? n
                 TN: 1            Check skill TNs to match agent TN? n
                COR: 1
      Coverage Path:                                    LWC Reception: spe
      Security Code:                             LWC Log External Calls? n
                                               AUDIX Name for Messaging:

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

On **Page 2,** add the required skills. Note that the skill **2** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly to this agent.



```
add agent-loginID 80000                                        Page   2 of    3
                                    AGENT LOGINID
      Direct Agent Skill:                                   Service Objective? n
Call Handling Preference: skill-level                   Local Call Preference? n

    SN    RL SL          SN   RL SL          SN   RL SL          SN   RL SL
  1: 2        1        16:                 31:                 46:
  2:                   17:                 32:                 47:
  3:                   18:                 33:                 48:
  4:                   19:                 34:                 49:
  5:                   20:                 35:                 50:
  6:                   21:                 36:                 51:
  7:                   22:                 37:                 52:
  8:                   23:                 38:                 53:
  9:                   24:                 39:                 54:
 10:                   25:                 40:                 55:
```

Repeat this section to add another agent 80001.

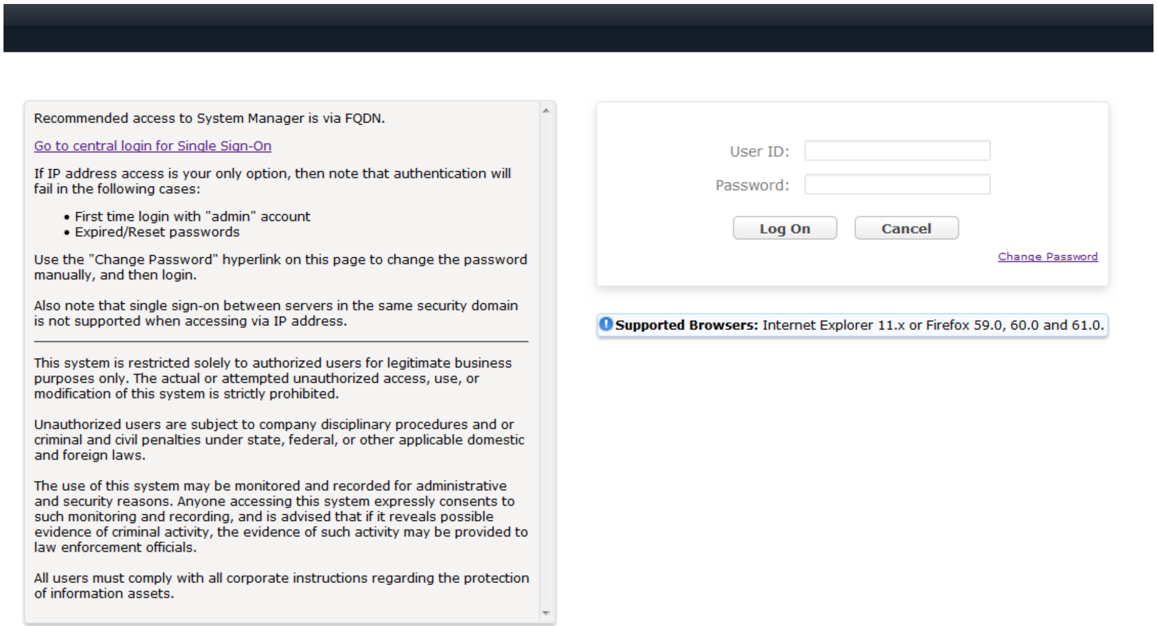
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer Users

6.1. Launch System Manager

Access the System Manager Web interface by using the URL "**https://<IP Address>/SMGR**" in an internet browser window, where <IP Address> is the IP address of the System Manager server. Log in using the appropriate credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

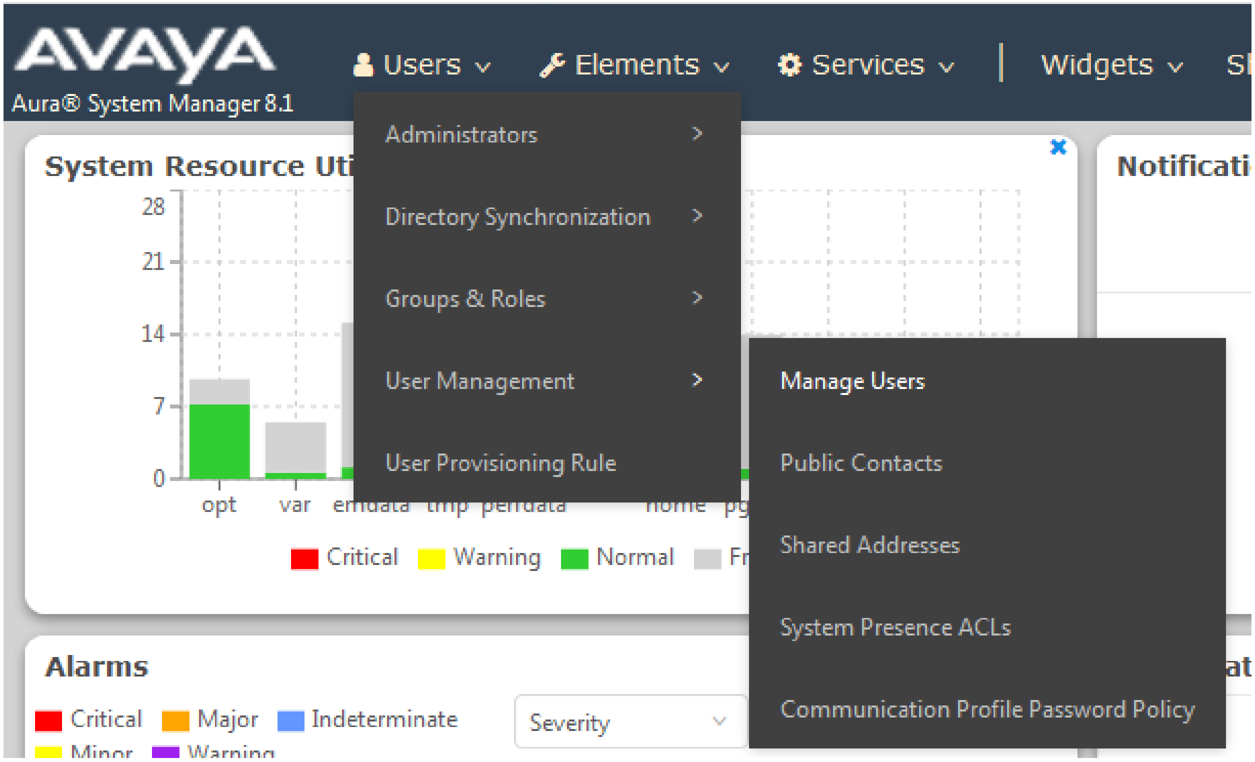
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

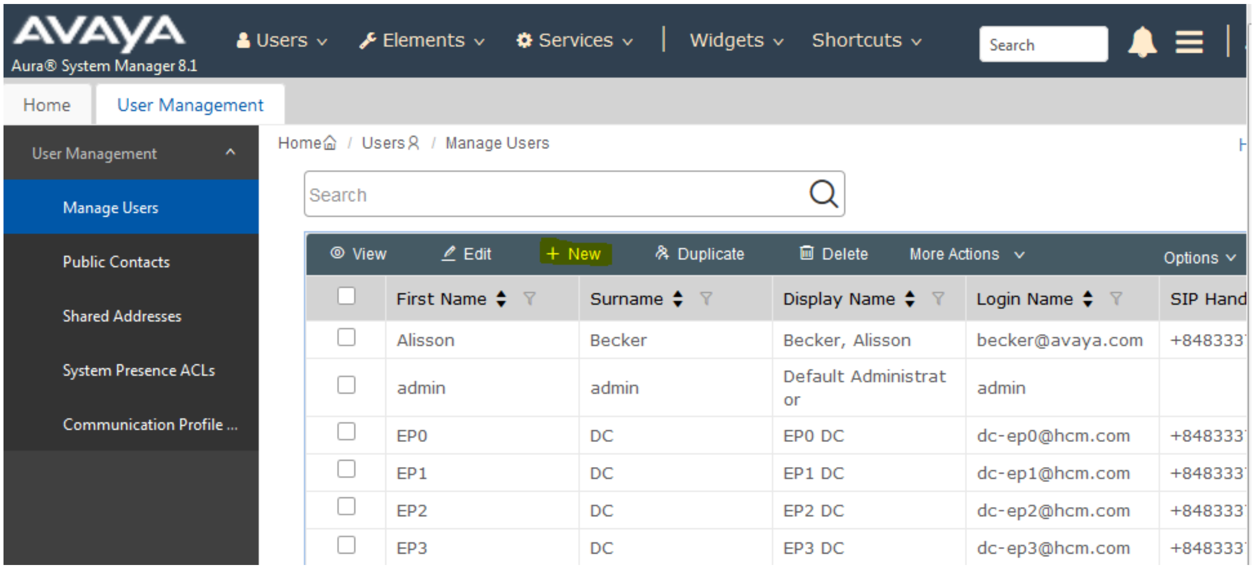
Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

6.2. Administer Users

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

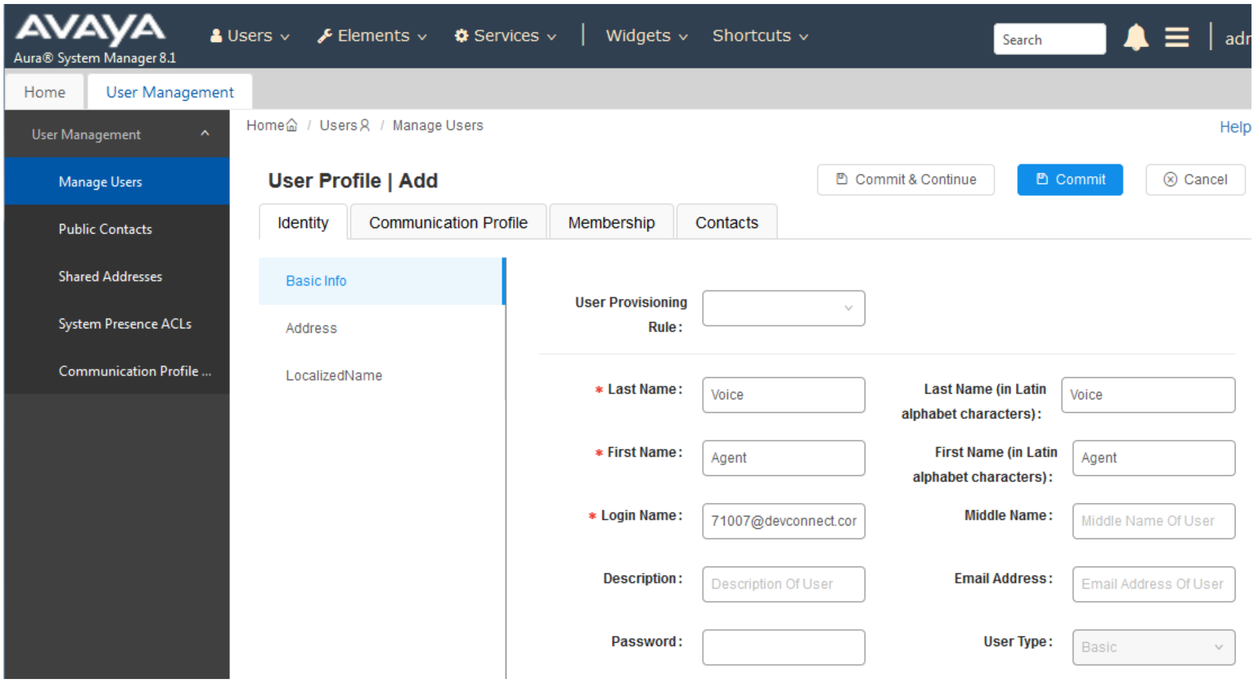


Click **New.**



□	First Name	Surname	Display Name	Login Name	SIP Hand
□	Alisson	Becker	Becker, Alisson	becker@avaya.com	+848333
□	admin	admin	Default Administrator	admin	
□	EP0	DC	EP0 DC	dc-ep0@hcm.com	+848333
□	EP1	DC	EP1 DC	dc-ep1@hcm.com	+848333
□	EP2	DC	EP2 DC	dc-ep2@hcm.com	+848333
□	EP3	DC	EP3 DC	dc-ep3@hcm.com	+848333

On the **Identity** tab enter an identifying **Last Name** and **First Name**, enter an appropriate **Login Name**, set **Authentication Type** to **Basic** and administer a password in the **Password** and **Confirm Password** fields.



User Profile | Add

User Provisioning Rule:

* Last Name: Voice

Last Name (in Latin alphabet characters): Voice

* First Name: Agent

First Name (in Latin alphabet characters): Agent

* Login Name: 71007@devconnect.cor

Middle Name: Middle Name Of User

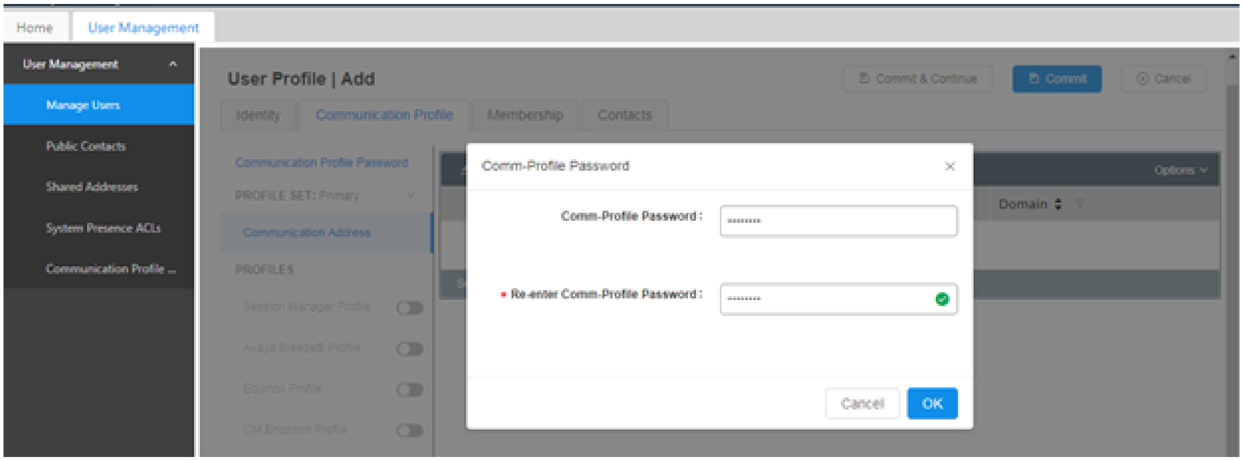
Description: Description Of User

Email Address: Email Address Of User

Password:

User Type: Basic

Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint.



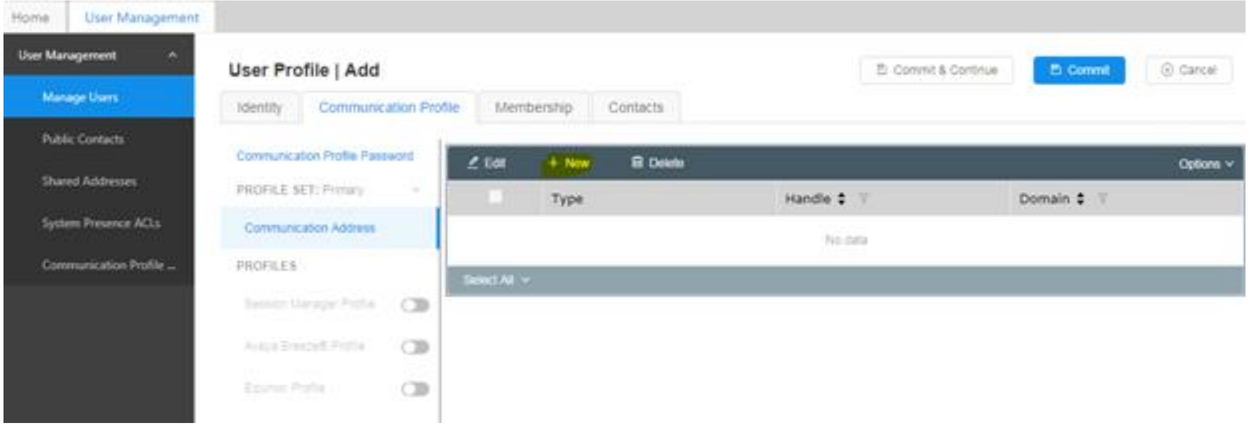
User Profile | Add

Comm-Profile Password

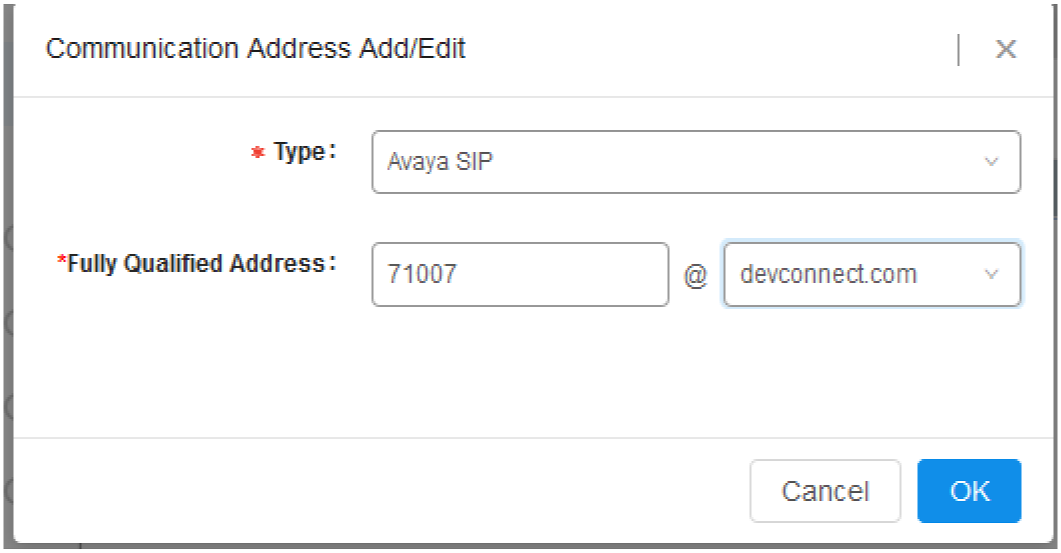
Comm-Profile Password: ••••••••

* Re-enter Comm-Profile Password: ••••••••

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



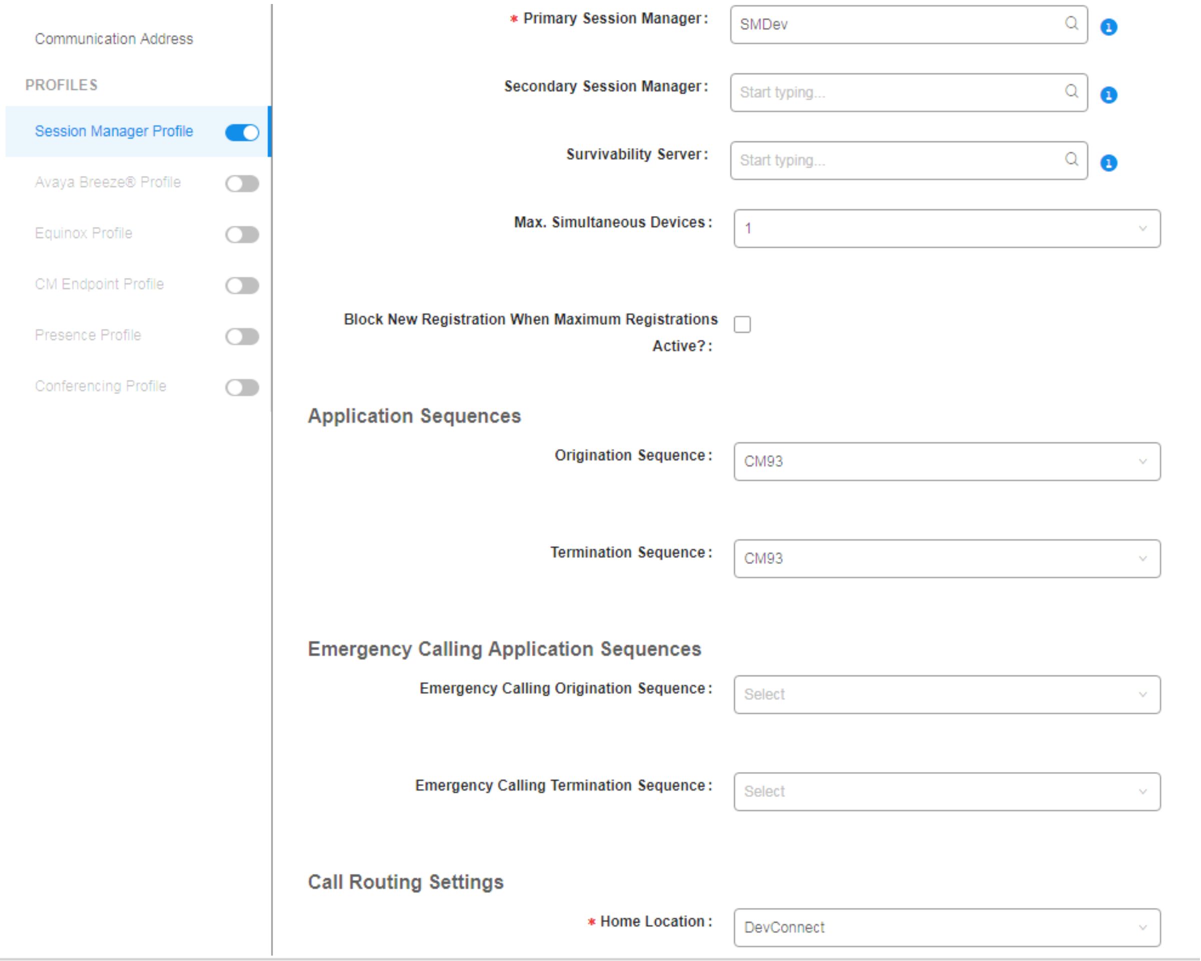
Select **Avaya SIP** from the **Type** drop down box and enter the **Fully Qualified Address** of the new SIP user. Click **Ok** when done.



* Type: Avaya SIP

*Fully Qualified Address: 71007 @ devconnect.com

Scroll down on the same page. Enable **Session Manager Profile** and enter the **Primary Session Manager, Origination Application Sequence, Termination Application Sequence** and **Home Location** relevant to the implementation.



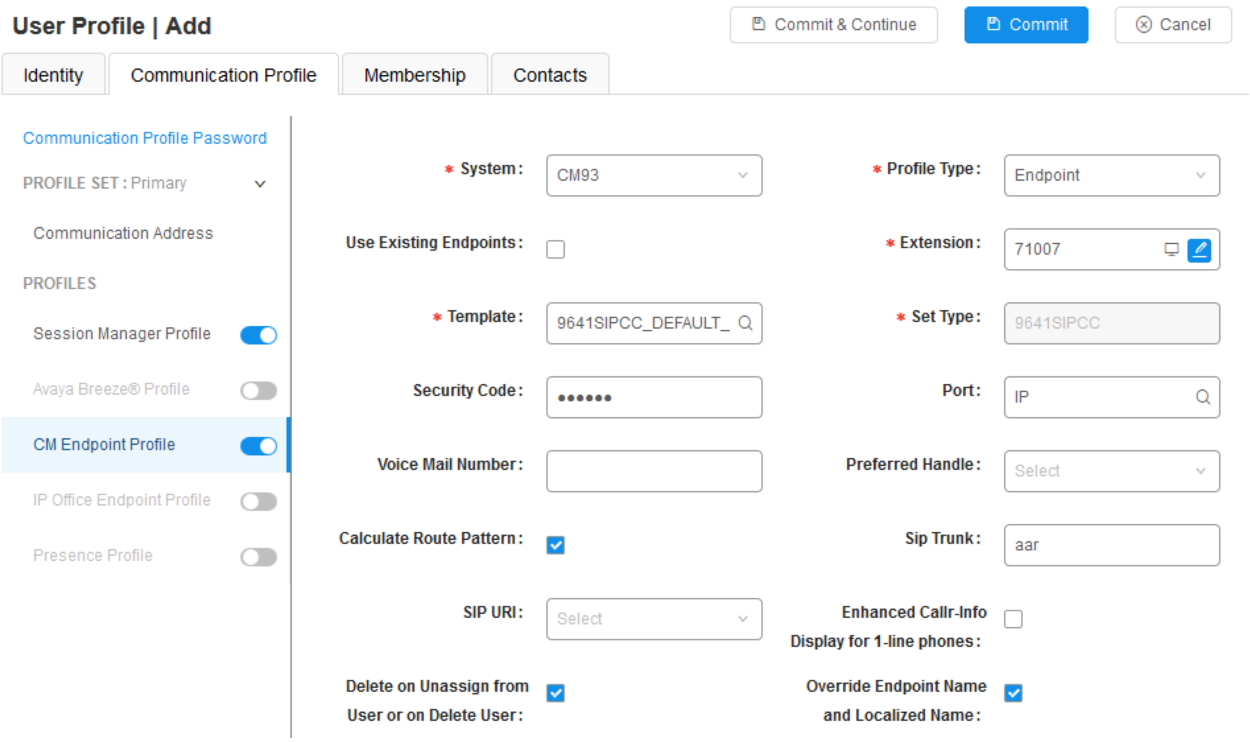
* Primary Session Manager: SMDev
Secondary Session Manager: Start typing...
Survivability Server: Start typing...
Max. Simultaneous Devices: 1
Block New Registration When Maximum Registrations Active?: □

Application Sequences
Origination Sequence: CM93
Termination Sequence: CM93

Emergency Calling Application Sequences
Emergency Calling Origination Sequence: Select
Emergency Calling Termination Sequence: Select

Call Routing Settings
* Home Location: DevConnect

Scroll down the page and enable **CM Endpoint Profile** section. Select the Communication Manager system from the **System** drop down box, select **Endpoint** as the **Profile Type**, enter the **Extension** number you wish to use, select **9641SIPCC_DEFAULT_CM_8_1** as the **Template** and ensure **IP** is configured as the **Port**, click **Commit** & **Continue** (not shown) when finished.



* System : CM93

* Profile Type : Endpoint

Use Existing Endpoints : □

* Extension : 71007

* Template : 9641SIPCC_DEFAULT_

* Set Type : 9641SIPCC

Security Code : ••••••

Port : IP

Voice Mail Number :

Preferred Handle : Select

Calculate Route Pattern : ☑

Sip Trunk : aar

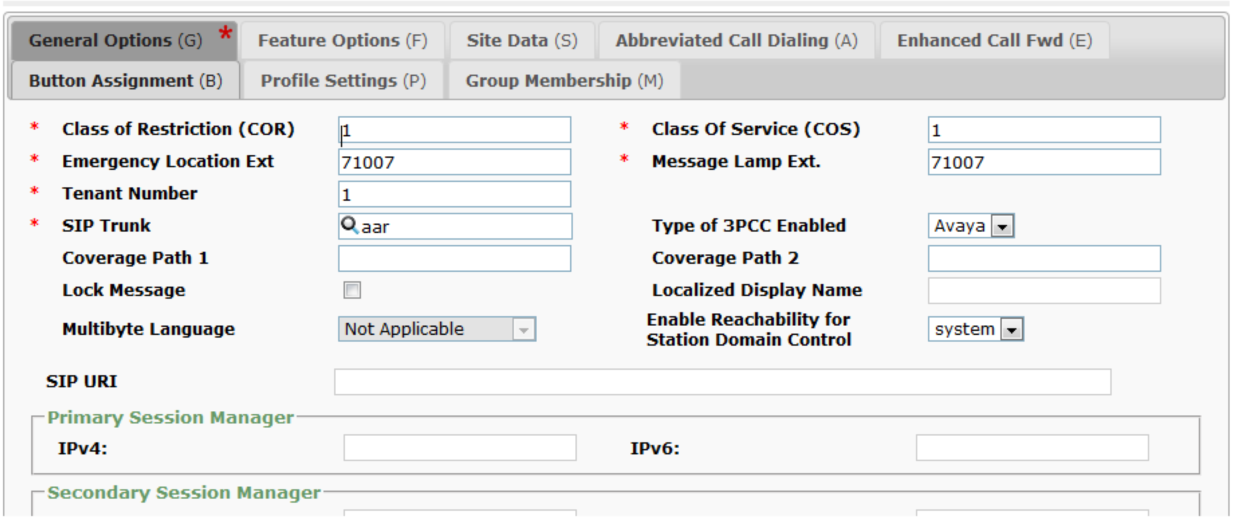
SIP URI : Select

Enhanced Callr-Info Display for 1-line phones : □

Delete on Unassign from User or on Delete User : ☑

Override Endpoint Name and Localized Name : ☑

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



* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	71007	* Message Lamp Ext.	71007
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

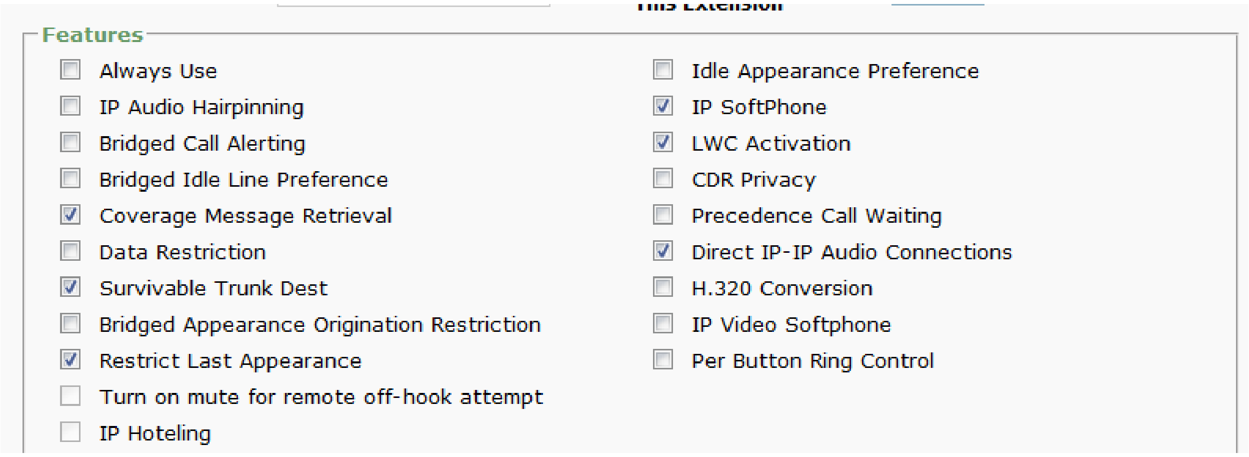
SIP URI

Primary Session Manager

IPv4: IPv6:

Secondary Session Manager

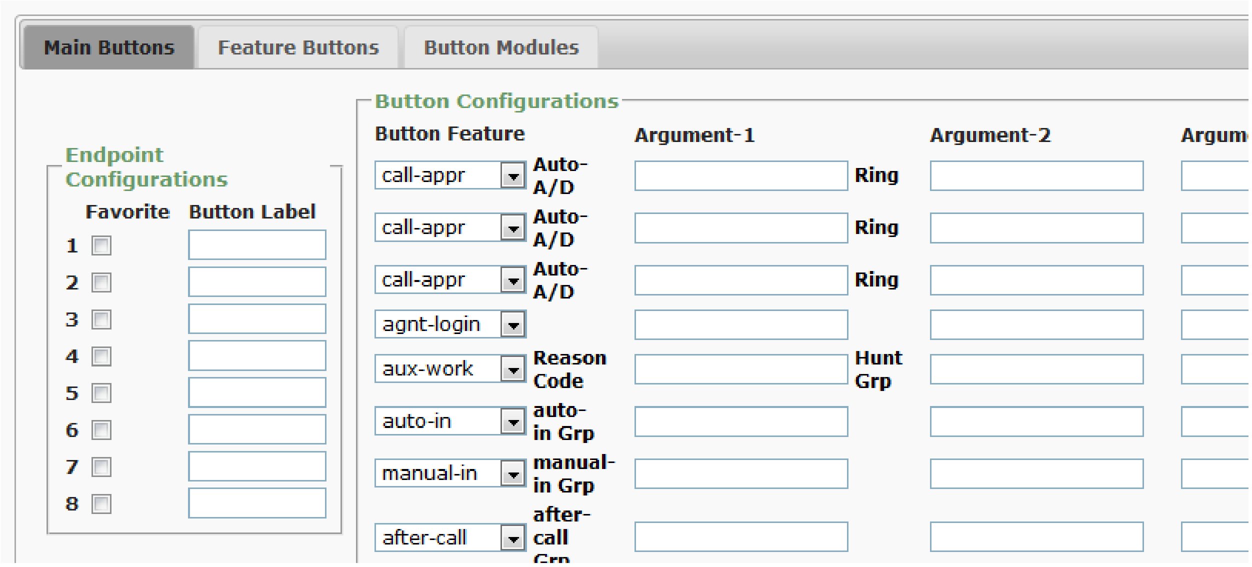
Click on **Feature Options (F)** tab, scroll down and check **IP SoftPhone.** Click on **Done** to save changes and go back to the **User Communication Profile** screen.



Features

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

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



Endpoint Configurations

	Favorite	Button Label
1	☐	
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	
8	☐	

Button Configurations

Button Feature		Argument-1		Argument-2	Argum
call-appr	Auto-A/D		Ring		
call-appr	Auto-A/D		Ring		
call-appr	Auto-A/D		Ring		
agnt-login					
aux-work	Reason Code		Hunt Grp		
auto-in	auto-in Grp				
manual-in	manual-in Grp				
after-call	after-call Grp				

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

7. Configure Avaya Aura® Application Enablement Services

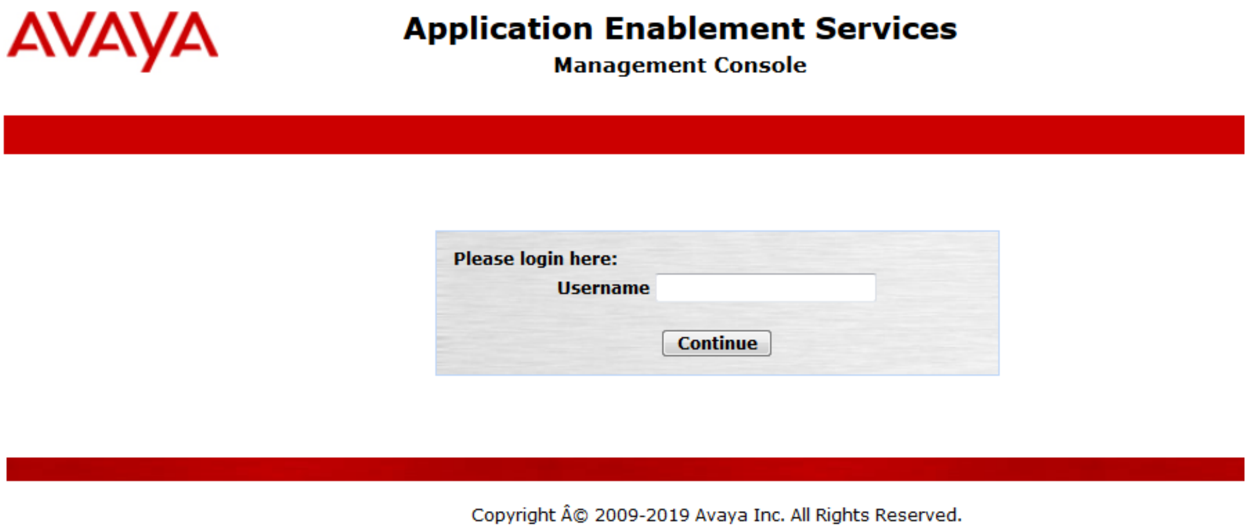
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer avaya user
- Administer security database
- Administer ports
- Restart services
- Obtain Tlink name

7.1. Launch OAM Interface

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

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



Application Enablement Services

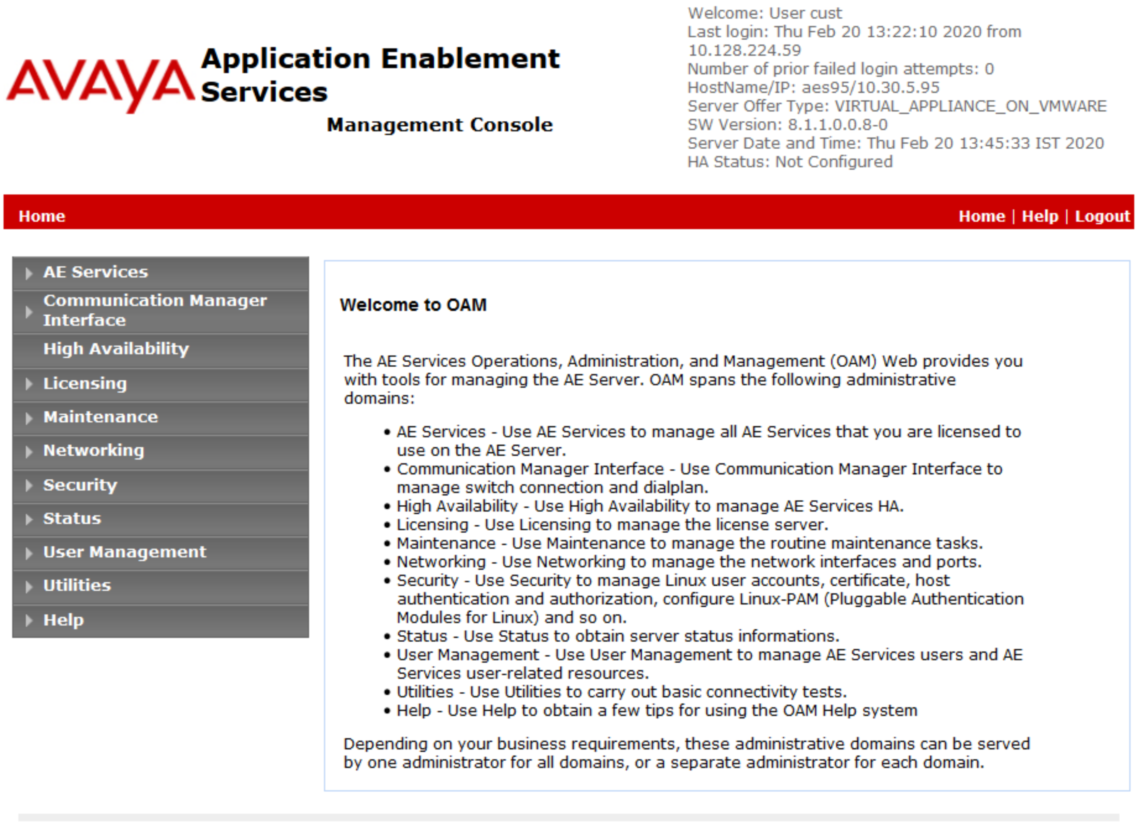
Management Console

Please login here:

Username

Copyright Â© 2009-2019 Avaya Inc. All Rights Reserved.

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



Welcome: User cust
Last login: Thu Feb 20 13:22:10 2020 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.0.8-0
Server Date and Time: Thu Feb 20 13:45:33 IST 2020
HA Status: Not Configured

Welcome to OAM

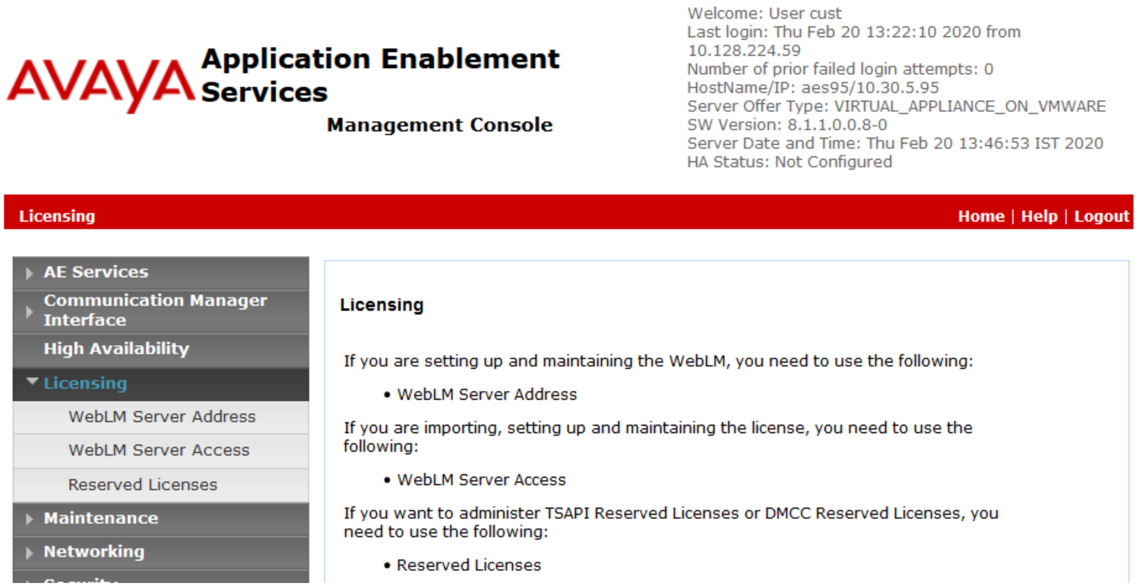
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

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

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

7.2. Verify License

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



Welcome: User cust
Last login: Thu Feb 20 13:22:10 2020 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.0.8-0
Server Date and Time: Thu Feb 20 13:46:53 IST 2020
HA Status: Not Configured

Licensing

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

- WebLM Server Address

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

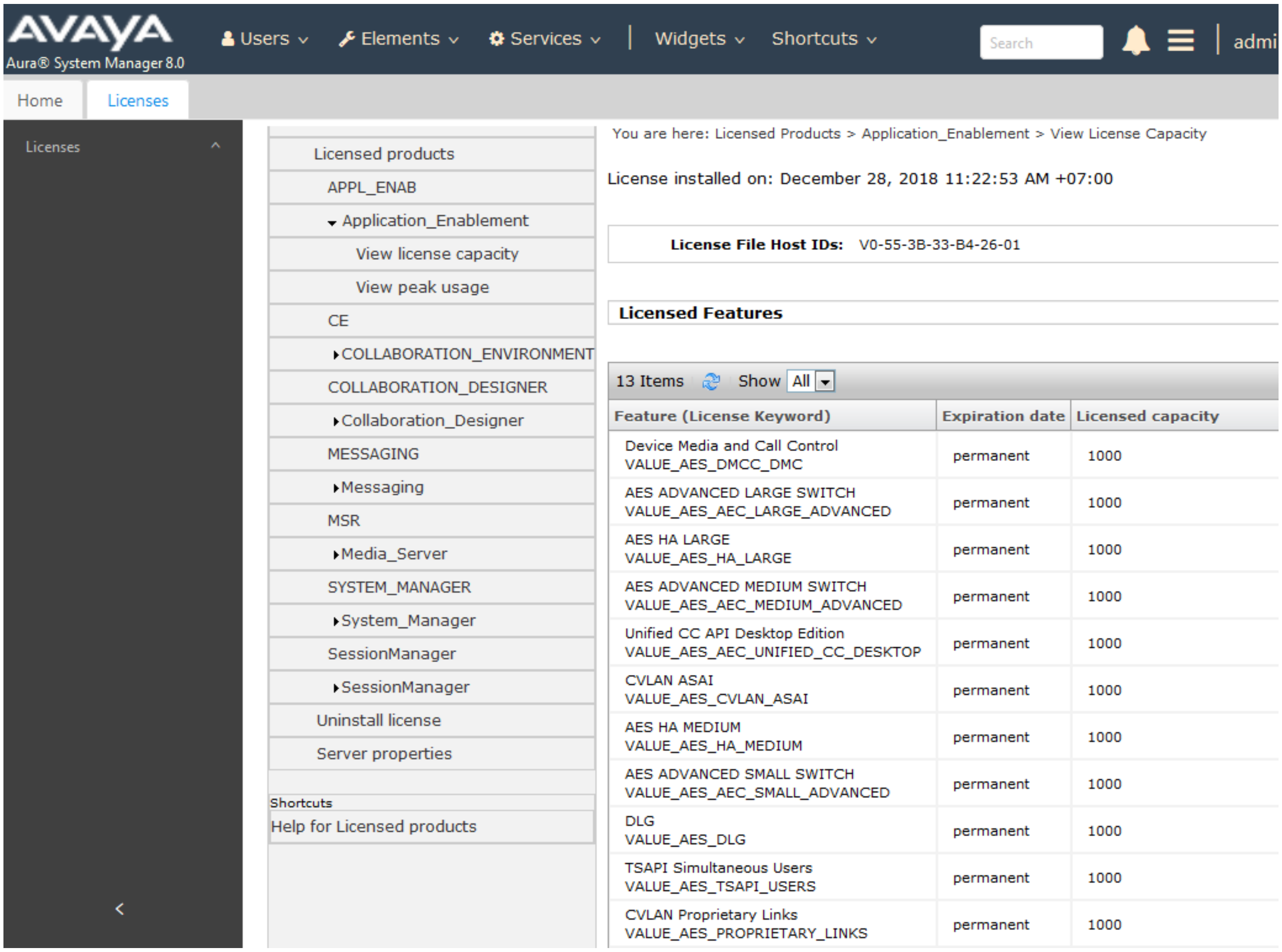
- WebLM Server Access

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

- Reserved Licenses

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

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



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

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

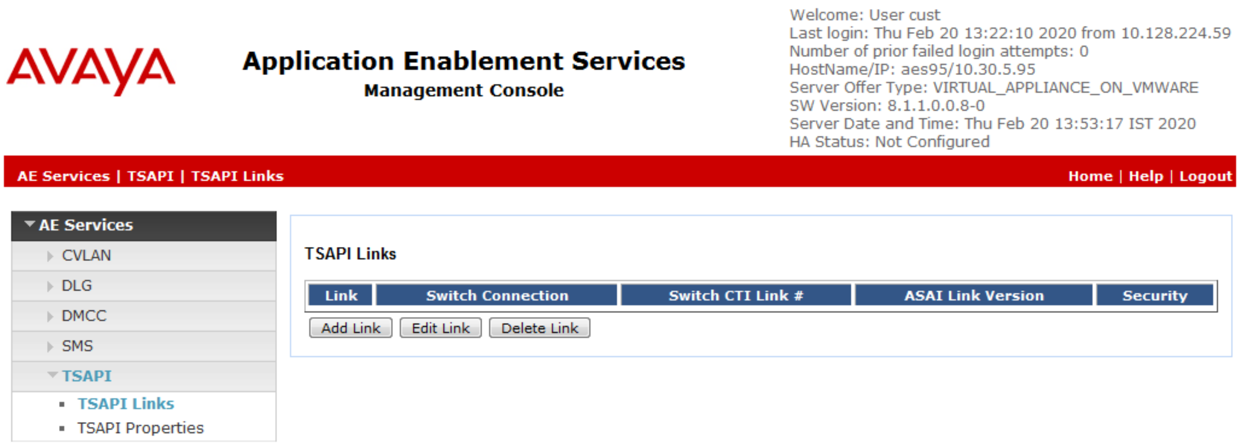
License File Host IDs: V0-55-3B-33-B4-26-01

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	1000
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	1000
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1000
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	1000
DLG VALUE_AES_DLG	permanent	1000
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	1000

7.3. Administer TSAPI Link

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



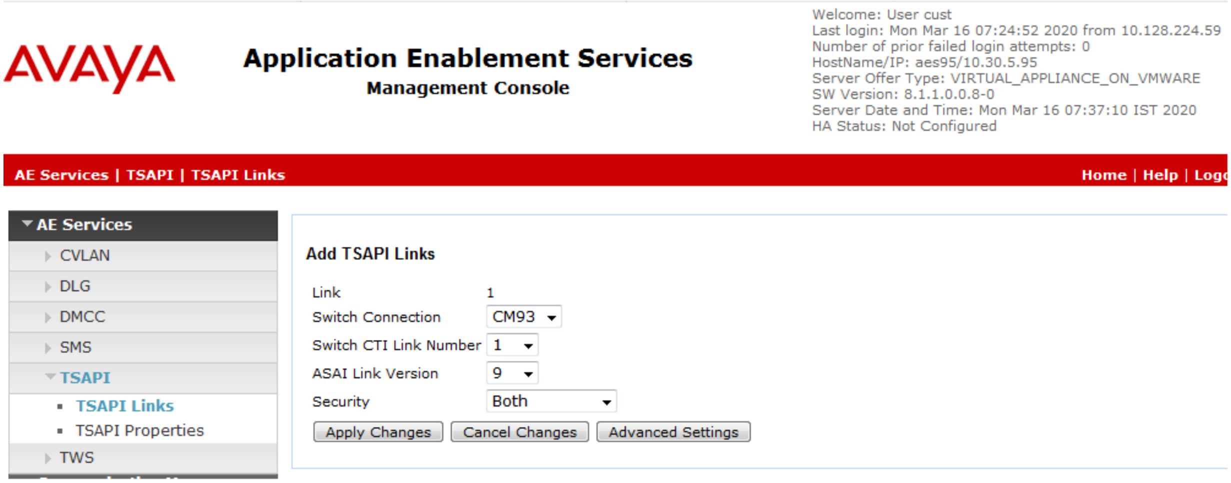
Welcome: User cust
Last login: Thu Feb 20 13:22:10 2020 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.0.8-0
Server Date and Time: Thu Feb 20 13:53:17 IST 2020
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection **CM93** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Welcome: User cust
Last login: Mon Mar 16 07:24:52 2020 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.0.8-0
Server Date and Time: Mon Mar 16 07:37:10 IST 2020
HA Status: Not Configured

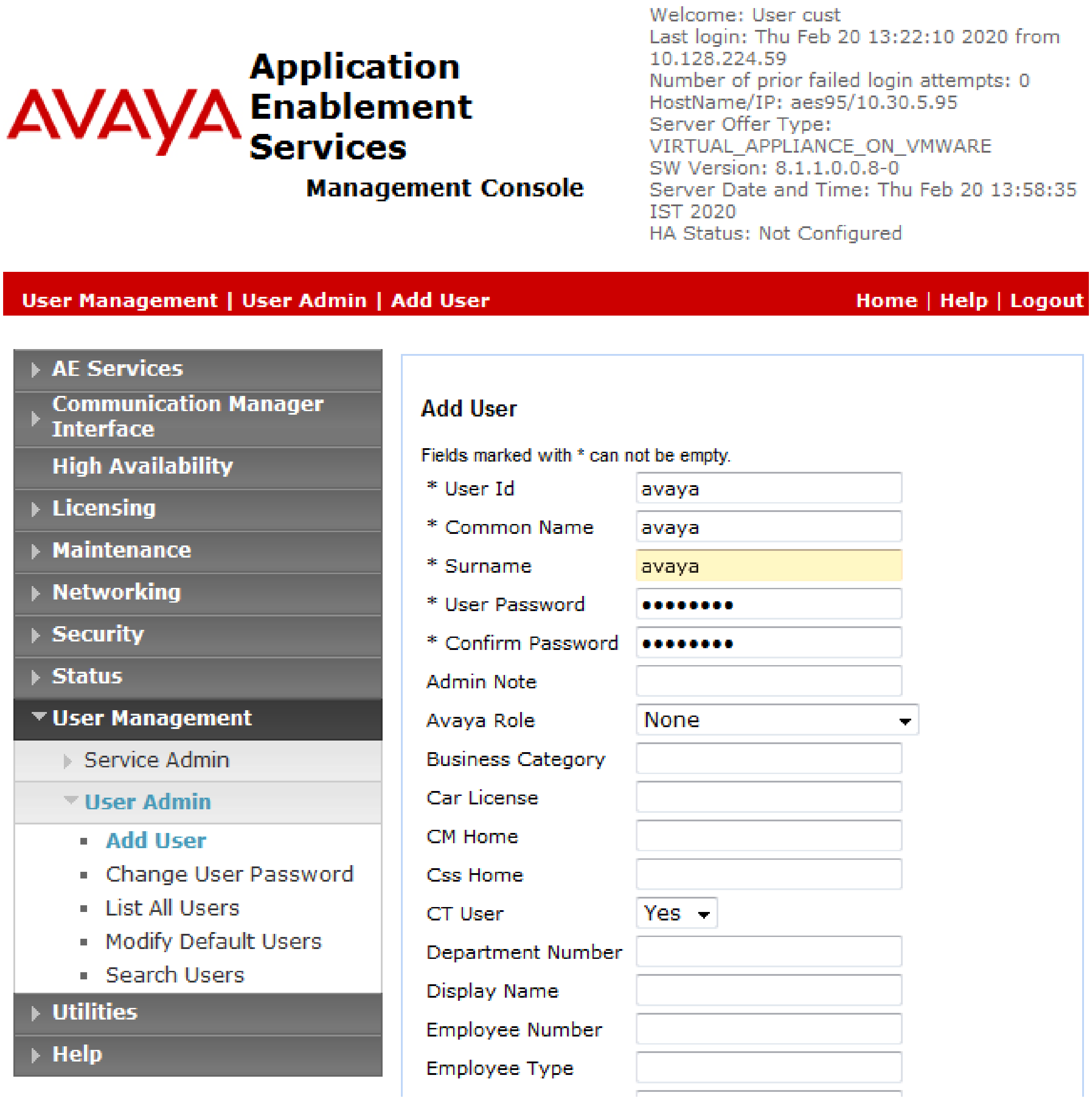
Add TSAPI Links

Link	1
Switch Connection	CM93
Switch CTI Link Number	1
ASAI Link Version	9
Security	Both

7.4. Administer Avaya User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields.



Welcome: User cust
Last login: Thu Feb 20 13:22:10 2020 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.0.8-0
Server Date and Time: Thu Feb 20 13:58:35 IST 2020
HA Status: Not Configured

Add User

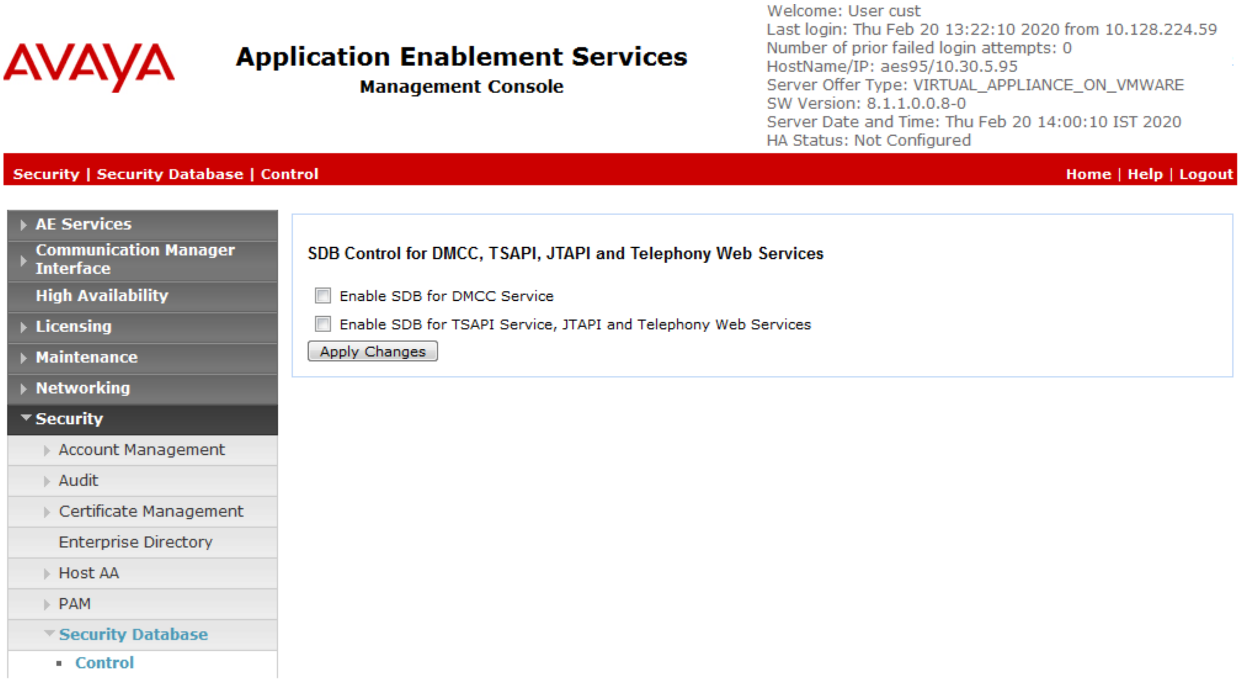
Fields marked with * can not be empty.

* User Id	avaya
* Common Name	avaya
* Surname	avaya
* User Password	••••••••
* Confirm Password	••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	

7.5. Administer Security Database

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

In the event that the security database is used by the customer with parameters already enabled, then follow reference [3] to configure access privileges for the Avaya user from **Section 7.4.**



Welcome: User cust
Last login: Thu Feb 20 13:22:10 2020 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.0.8-0
Server Date and Time: Thu Feb 20 14:00:10 IST 2020
HA Status: Not Configured

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

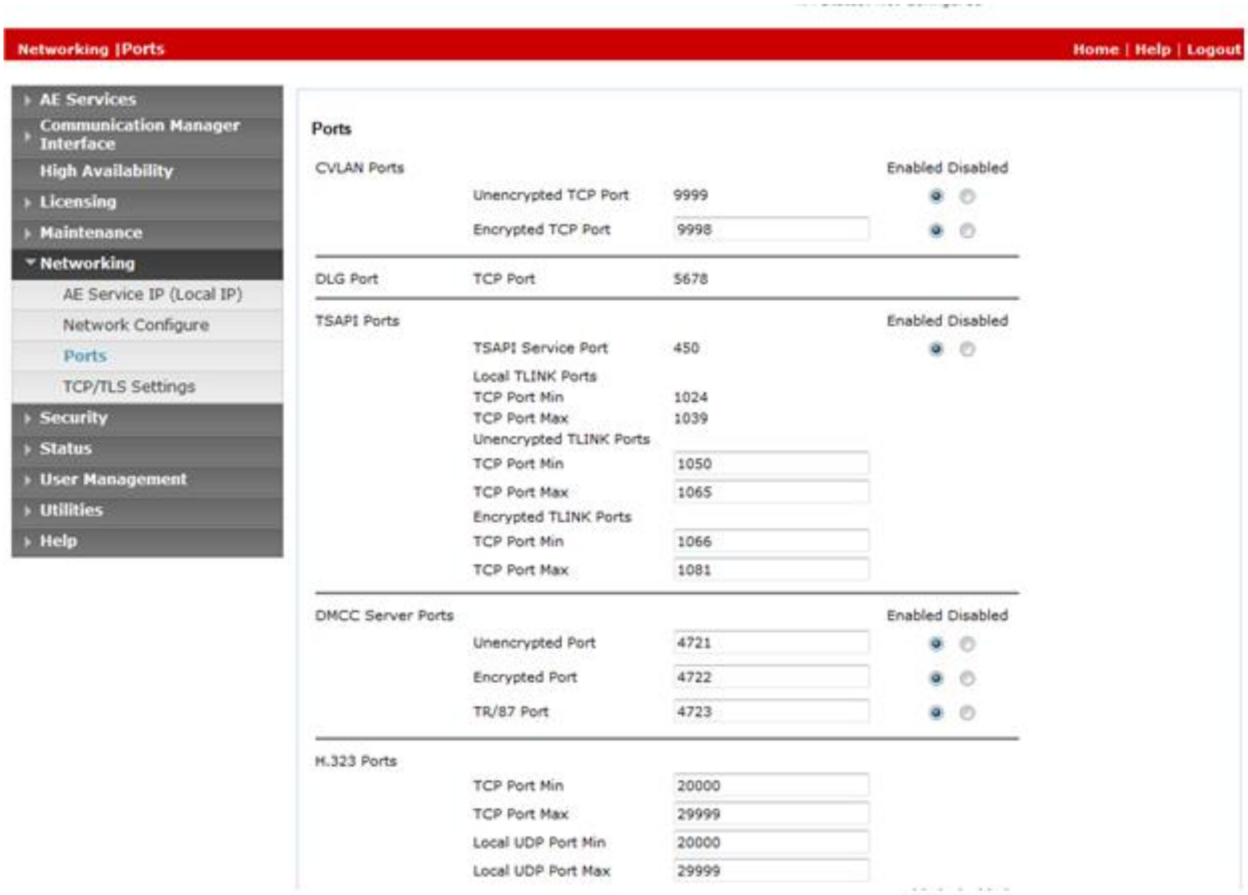
□ Enable SDB for DMCC Service

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

7.6. Administer Ports

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

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

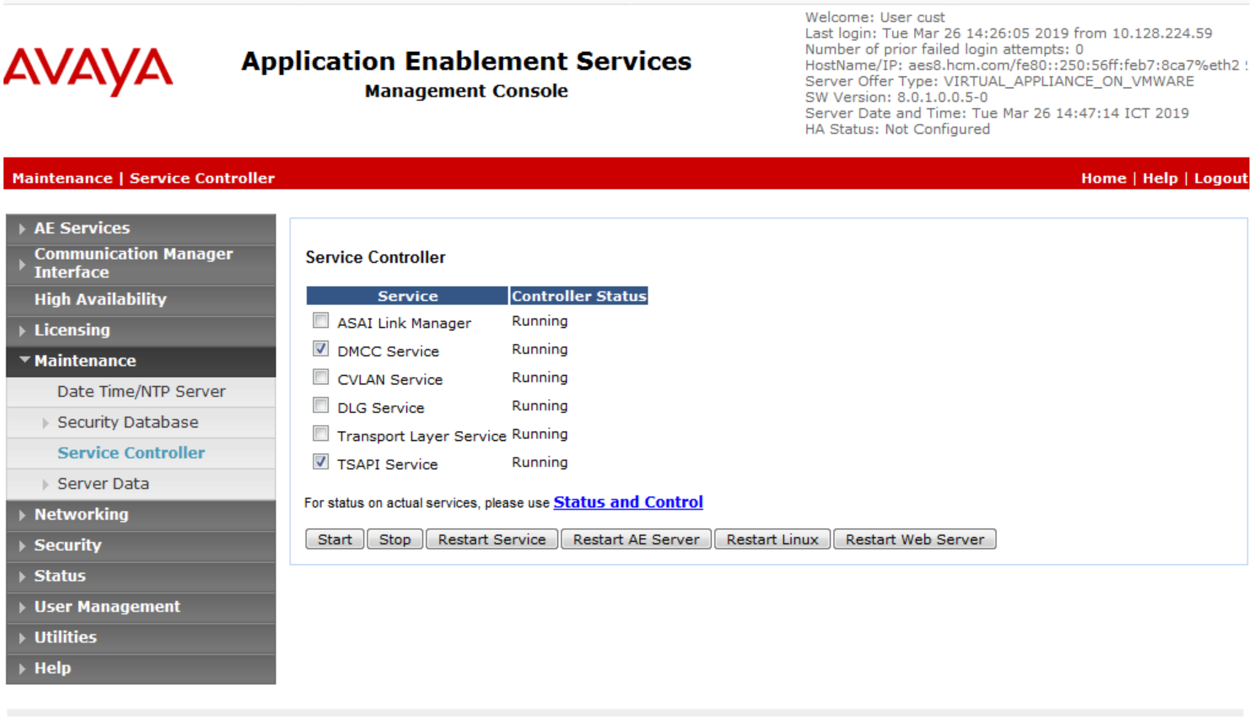


Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○
H.323 Ports				
	TCP Port Min	20000		
	TCP Port Max	29999		
	Local UDP Port Min	20000		
	Local UDP Port Max	29999		

7.7. Restart Services

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



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

Service Controller

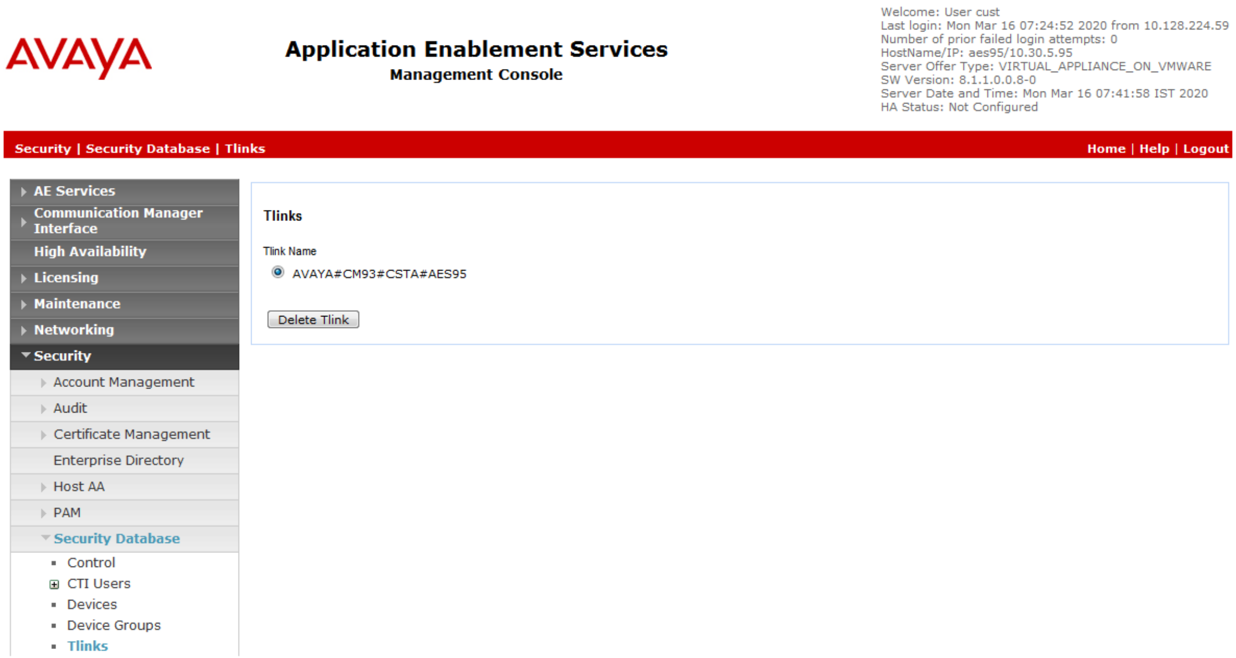
Service	Controller Status
☐ ASAI Link Manager	Running
☑ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

7.8. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Flair Workspace.

In this case, the associated Tlink name is **AVAYA#CM93#CSTA#AES95**. Note the use of the switch connection **CM93** from **Section 7.3** as part of the Tlink name**.**



Welcome: User cust
Last login: Mon Mar 16 07:24:52 2020 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.0.8-0
Server Date and Time: Mon Mar 16 07:41:58 IST 2020
HA Status: Not Configured

Tlinks

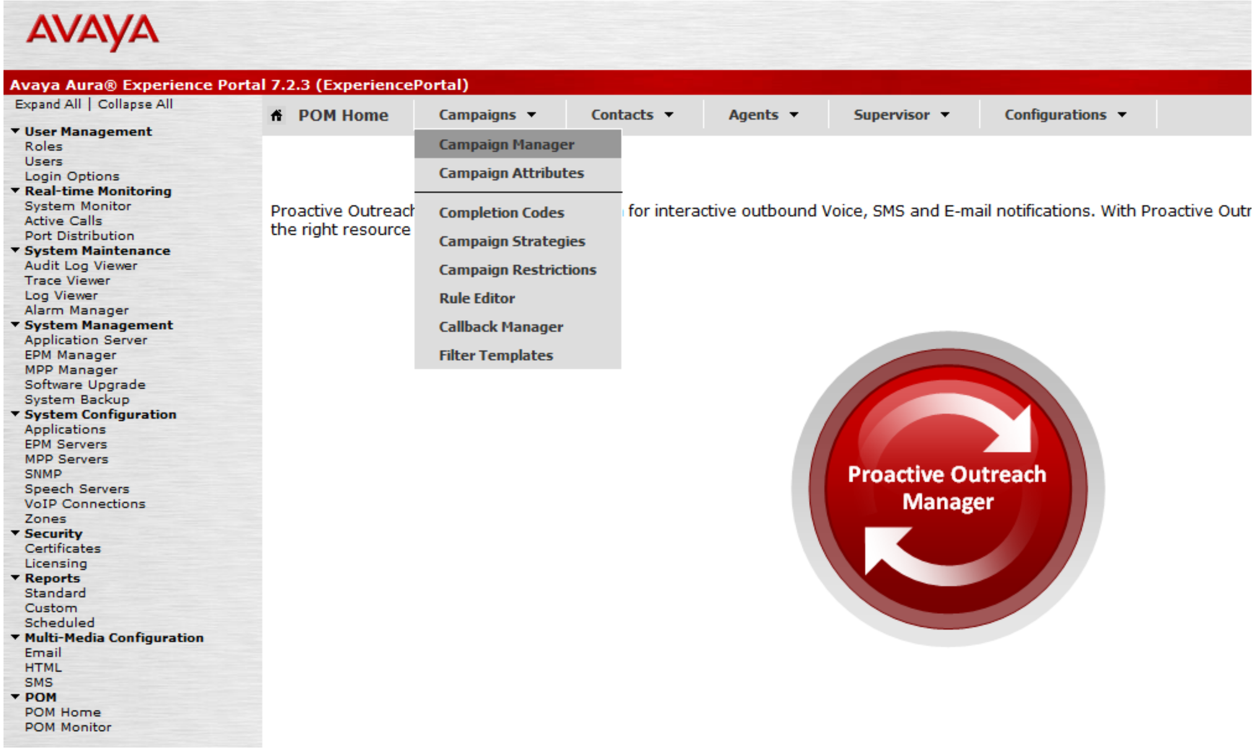
Tlink Name

● AVAYA#CM93#CSTA#AES95

8. Configure Proactive Outreach Manager Campaign

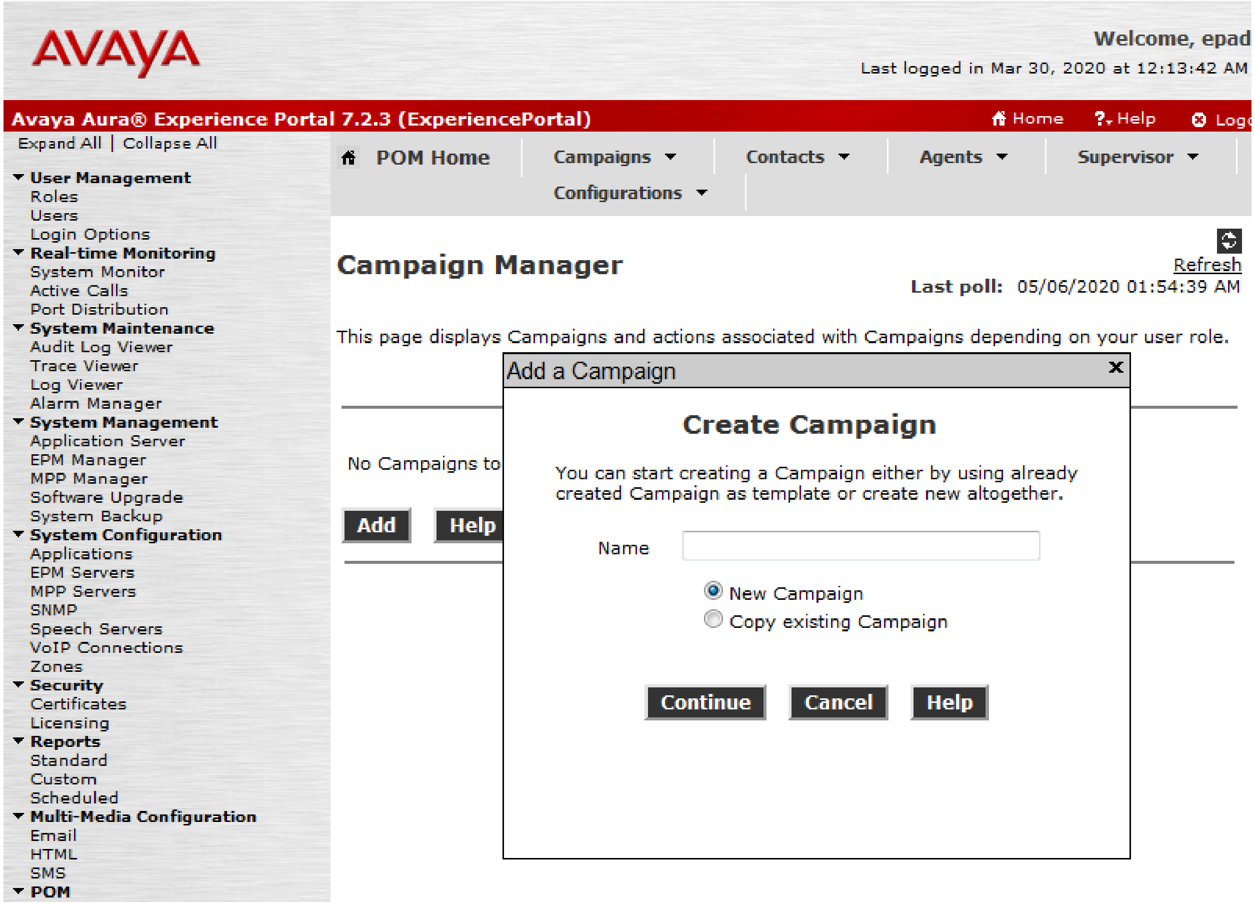
This section will describe the steps required to create a basic outbound campaign in POM.

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



Proactive Outreach ... for interactive outbound Voice, SMS and E-mail notifications. With Proactive Outr
the right resource

In Campaign Manager click on **Add** to create the new campaign. On The **Add a Campaign** screen **Enter** the Name and click on **Continue**.



Campaign Manager

Last poll: 05/06/2020 01:54:39 AM

This page displays Campaigns and actions associated with Campaigns depending on your user role.

No Campaigns to

Add a Campaign

Create Campaign

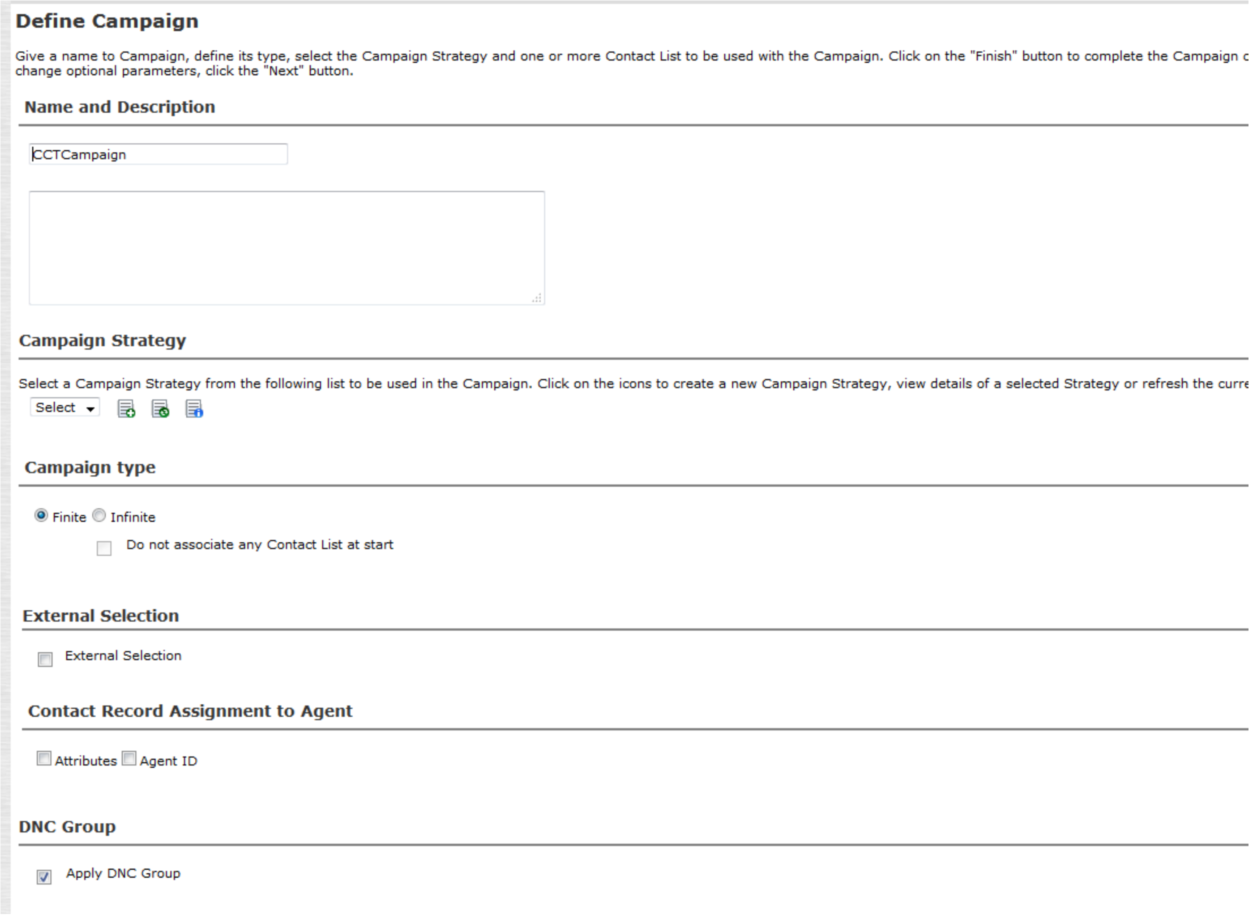
You can start creating a Campaign either by using already created Campaign as template or create new altogether.

Name

● New Campaign

○ Copy existing Campaign

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



Define Campaign

Give a name to Campaign, define its type, select the Campaign Strategy and one or more Contact List to be used with the Campaign. Click on the "Finish" button to complete the Campaign c change optional parameters, click the "Next" button.

Name and Description

CCTCampaign

Campaign Strategy

Select a Campaign Strategy from the following list to be used in the Campaign. Click on the icons to create a new Campaign Strategy, view details of a selected Strategy or refresh the curre

Select

Campaign type

● Finite ○ Infinite

□ Do not associate any Contact List at start

External Selection

□ External Selection

Contact Record Assignment to Agent

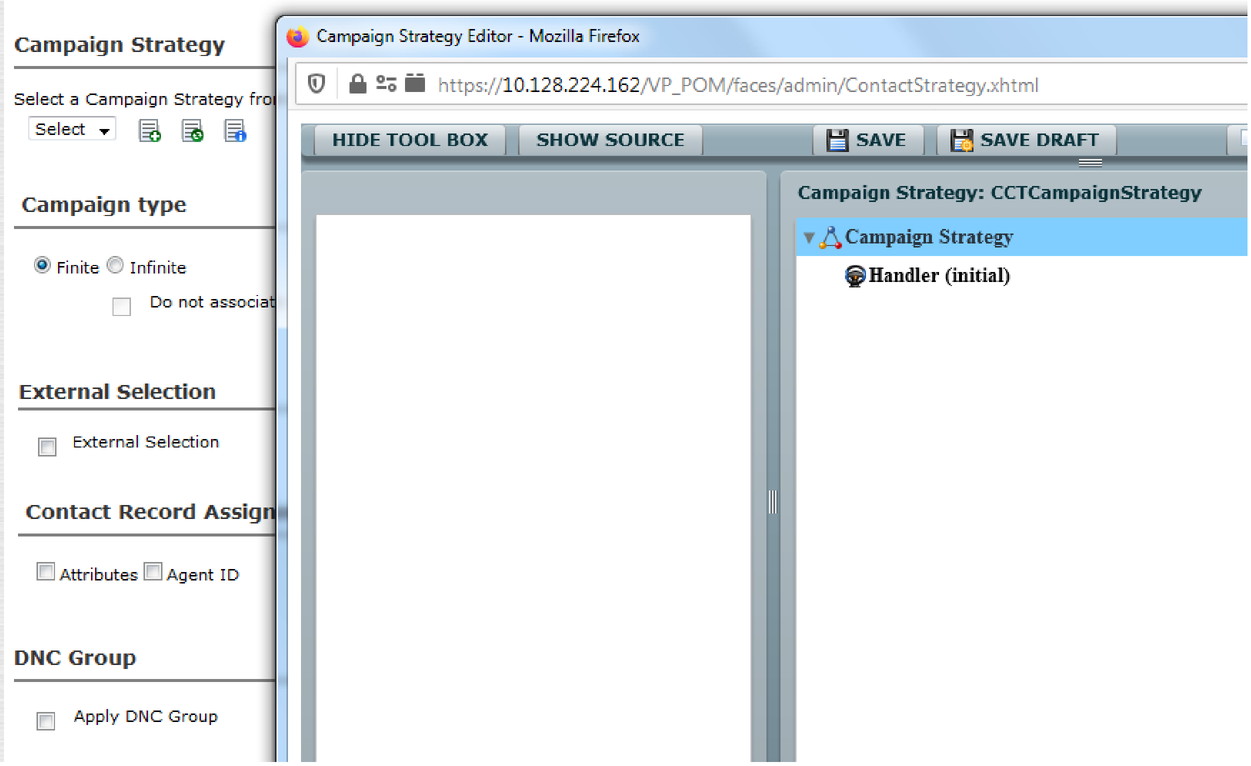
□ Attributes □ Agent ID

DNC Group

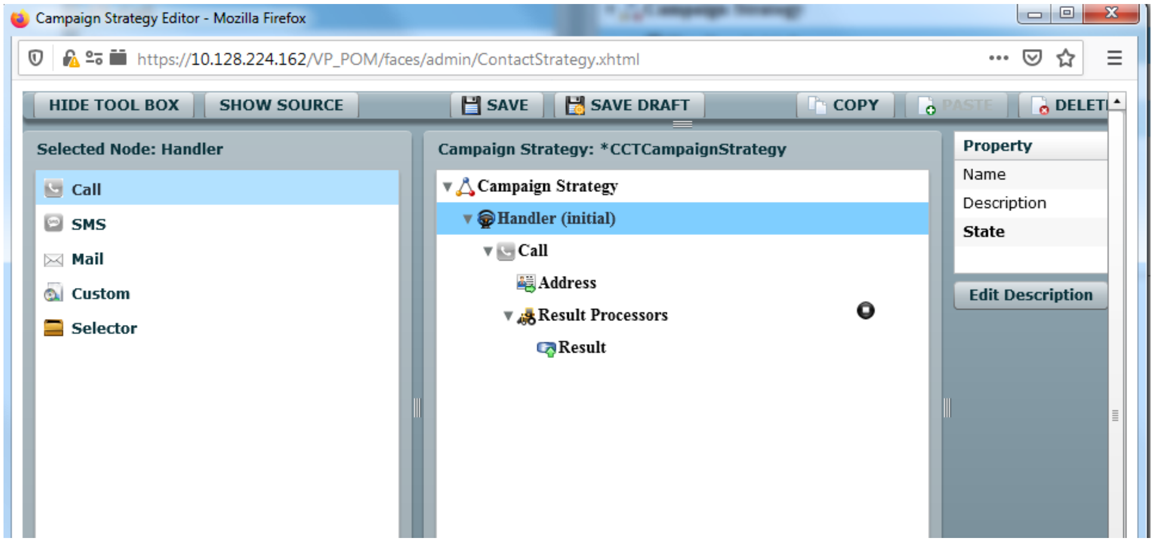
☑ Apply DNC Group

8.1. Create Campaign Strategy

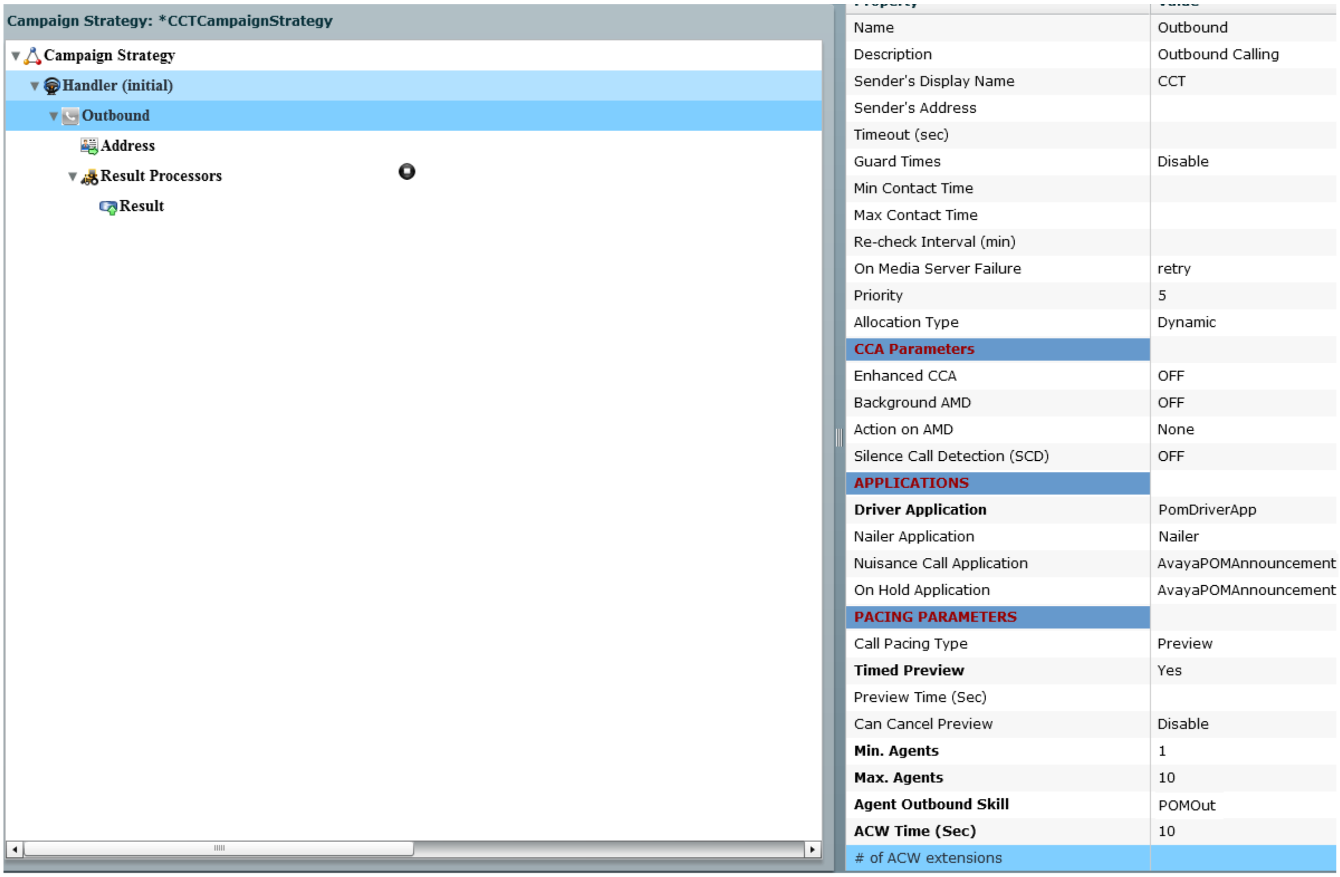
First under Campaign Strategy click on the add icon to bring up the **Campaign Strategy Editor**.



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 Strategy:** box. Select the **APPLICATIONS** from the drop down menus and set the **PACING PARAMETERS** (In this example a Preview Campaign has been selected).

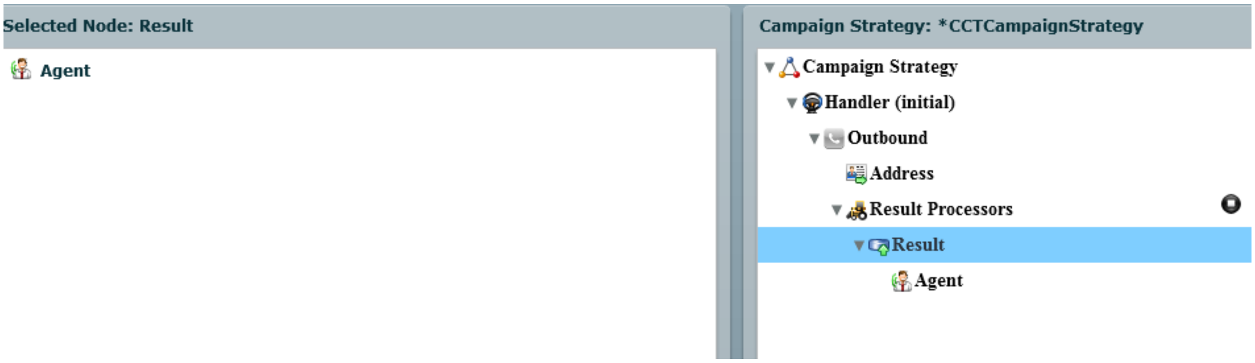


Campaign Strategy: *CCTCampaignStrategy

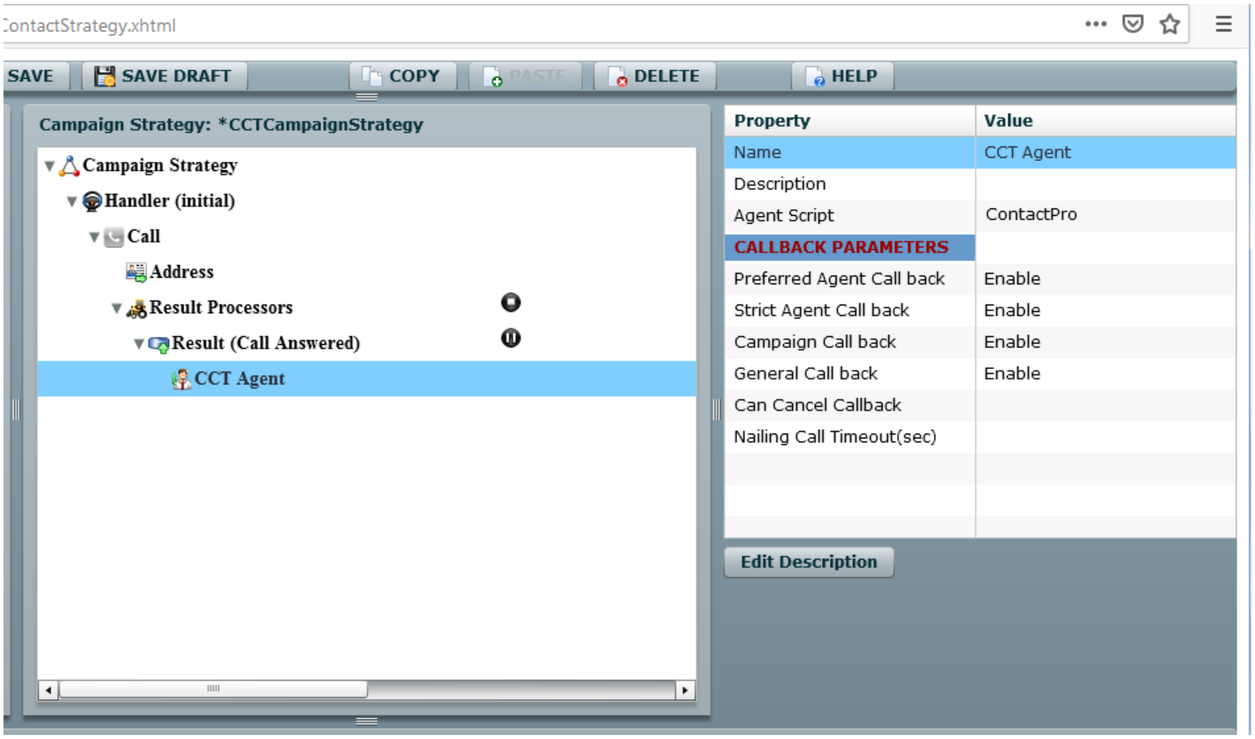
- Campaign Strategy
  - Handler (initial)
    - Outbound
      - Address
      - Result Processors
        - Result

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	retry
Priority	5
Allocation Type	Dynamic
CCA Parameters	
Enhanced CCA	OFF
Background AMD	OFF
Action on AMD	None
Silence Call Detection (SCD)	OFF
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	

From the **Campaign Strategy:** box select **Result (Call Answered)** and from the Selected Node: box drag the **Agent** node into the Campaign Strategy box.

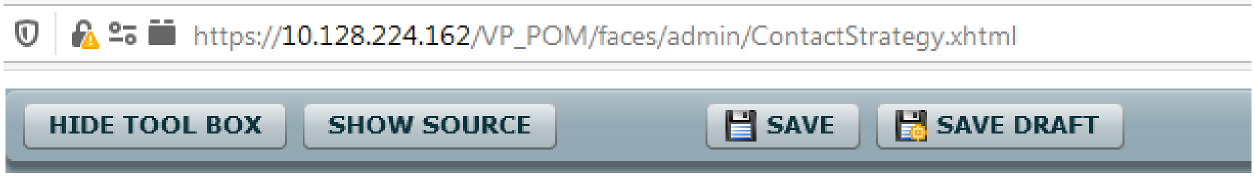


Select the **Agent** node in the **Campaign Strategy** box. Enter a **Name** and select an **Agent Script** from the Drop down.



Property	Value
Name	CCT Agent
Description	
Agent Script	ContactPro
CALLBACK PARAMETERS	
Preferred Agent Call back	Enable
Strict Agent Call back	Enable
Campaign Call back	Enable
General Call back	Enable
Can Cancel Callback	
Nailing Call Timeout(sec)	

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.

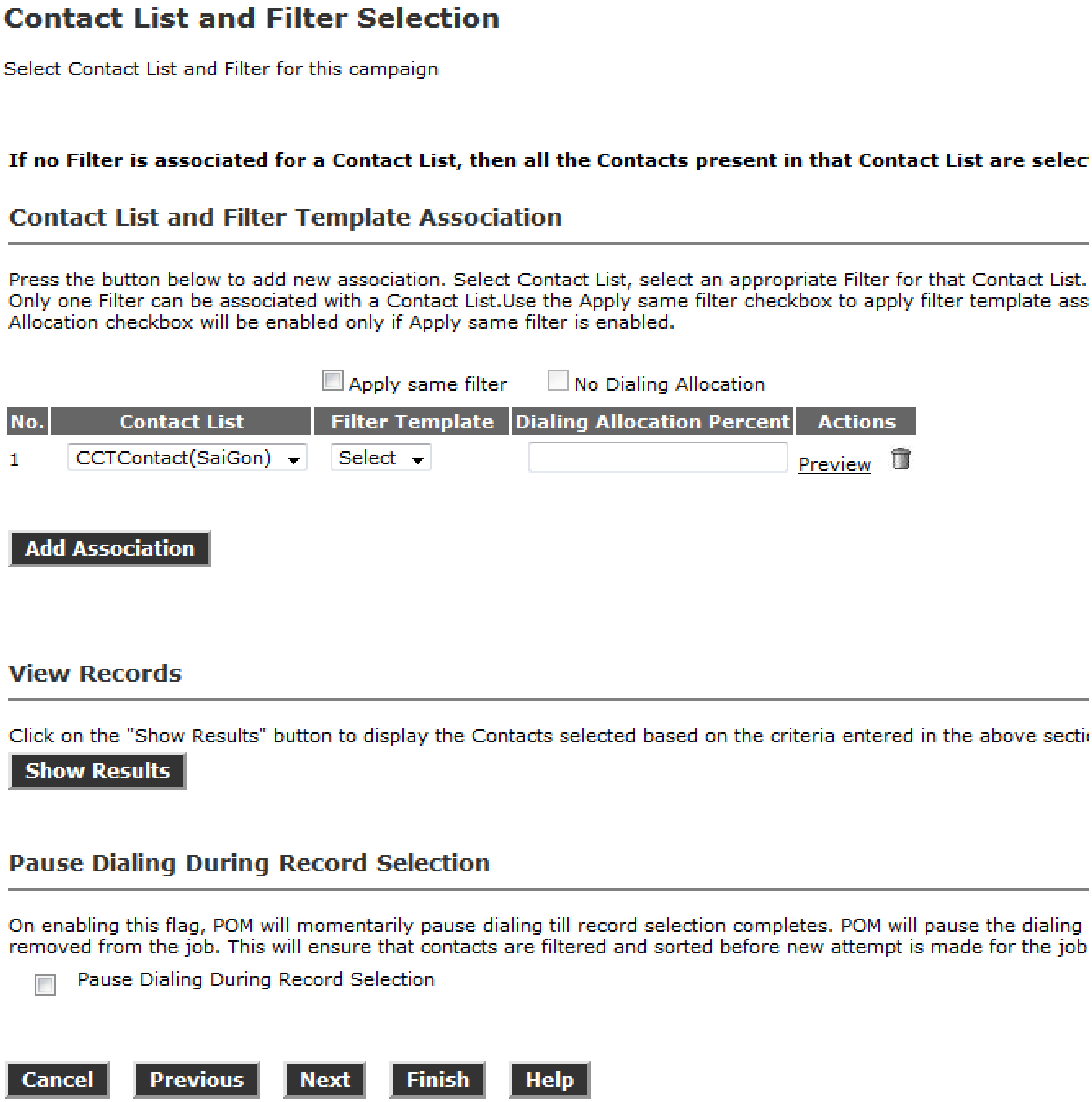

https://10.128.224.162/VP_POM/faces/admin/ContactStrategy.xhtml

Click **Next.**

8.2. Complete the Campaign Creation

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

On the **Contact List and Filter Template Association,** select Contact List (not shown).



Contact List and Filter Selection

Select Contact List and Filter for this campaign

If no Filter is associated for a Contact List, then all the Contacts present in that Contact List are selec

Contact List and Filter Template Association

Press the button below to add new association. Select Contact List, select an appropriate Filter for that Contact List. Only one Filter can be associated with a Contact List.Use the Apply same filter checkbox to apply filter template ass Allocation checkbox will be enabled only if Apply same filter is enabled.

□ Apply same filter □ No Dialing Allocation

No.	Contact List	Filter Template	Dialing Allocation Percent	Actions
1	CCTContact(SaiGon)	Select		Preview 🗑

View Records

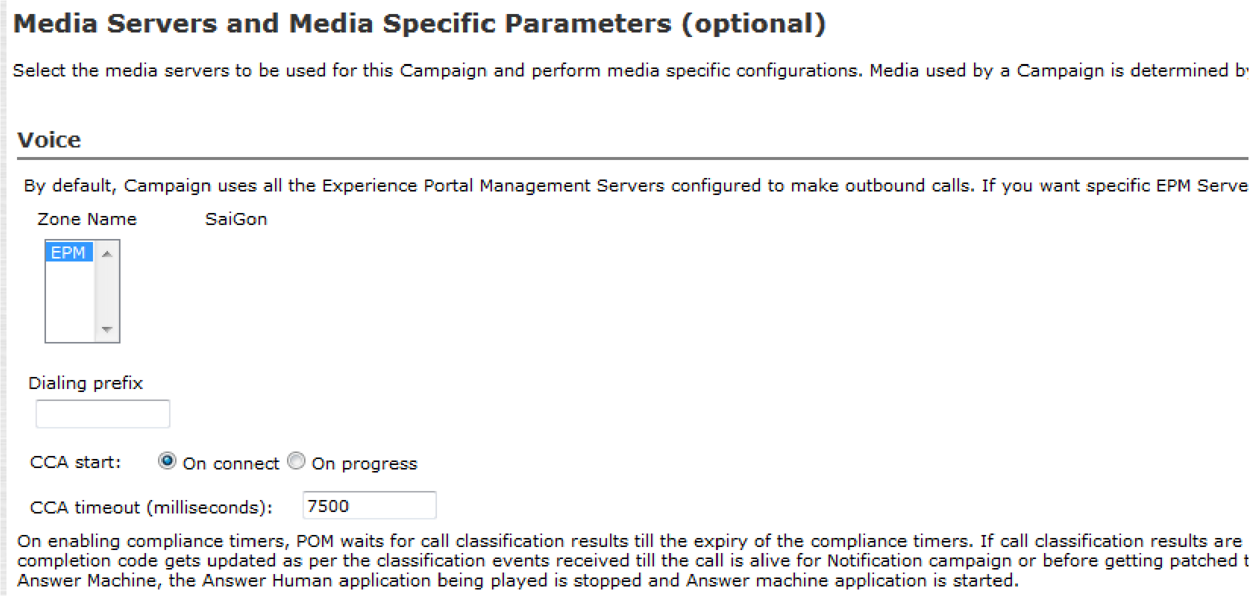
Click on the "Show Results" button to display the Contacts selected based on the criteria entered in the above secti

Pause Dialing During Record Selection

On enabling this flag, POM will momentarily pause dialing till record selection completes. POM will pause the dialing removed from the job. This will ensure that contacts are filtered and sorted before new attempt is made for the job

□ Pause Dialing During Record Selection

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



Media Servers and Media Specific Parameters (optional)

Select the media servers to be used for this Campaign and perform media specific configurations. Media used by a Campaign is determined b

Voice

By default, Campaign uses all the Experience Portal Management Servers configured to make outbound calls. If you want specific EPM Serve

Zone Name SaiGon

EPM

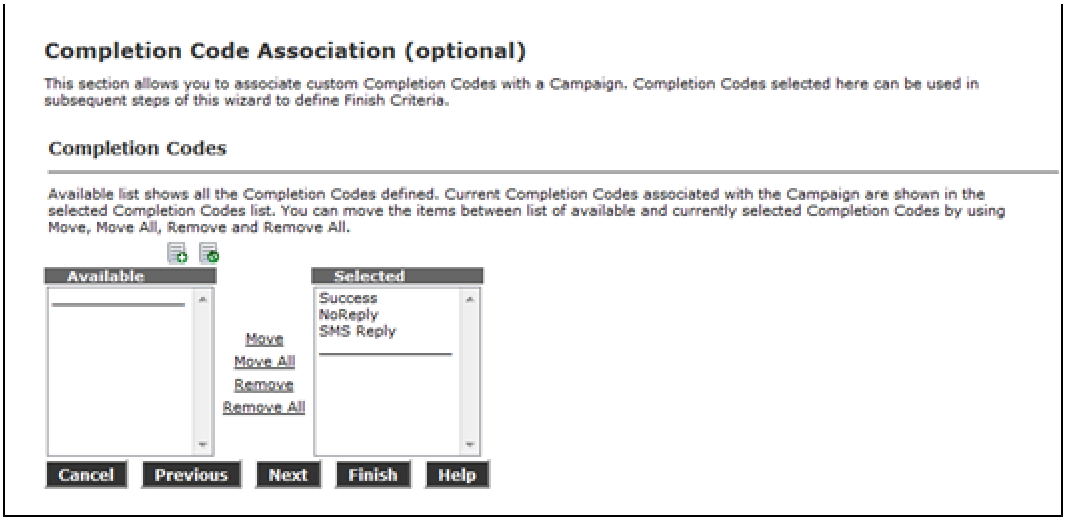
Dialing prefix

CCA start: ● On connect ○ On progress

CCA timeout (milliseconds): 7500

On enabling compliance timers, POM waits for call classification results till the expiry of the compliance timers. If call classification results are completion code gets updated as per the classification events received till the call is alive for Notification campaign or before getting patched t Answer Machine, the Answer Human application being played is stopped and Answer machine application is started.

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



Completion Code Association (optional)

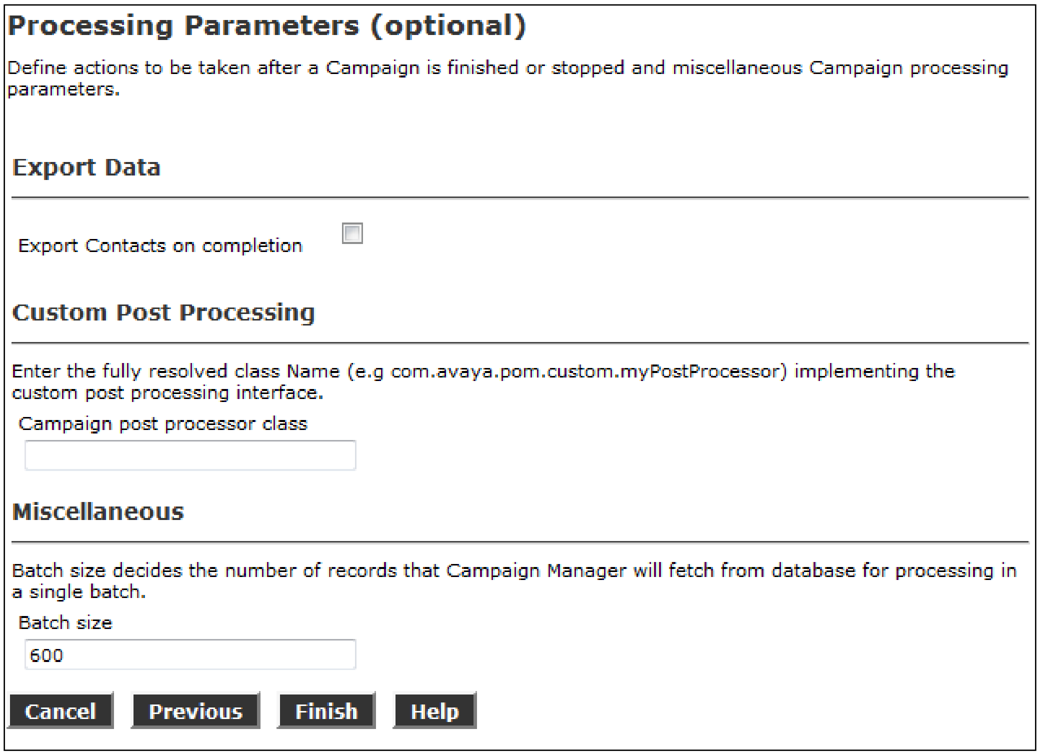
This section allows you to associate custom Completion Codes with a Campaign. Completion Codes selected here can be used in subsequent steps of this wizard to define Finish Criteria.

Completion Codes

Available list shows all the Completion Codes defined. Current Completion Codes associated with the Campaign are shown in the selected Completion Codes list. You can move the items between list of available and currently selected Completion Codes by using Move, Move All, Remove and Remove All.

Selected: Success, NoReply, SMS Reply

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

9. Configure CCT ContactPro

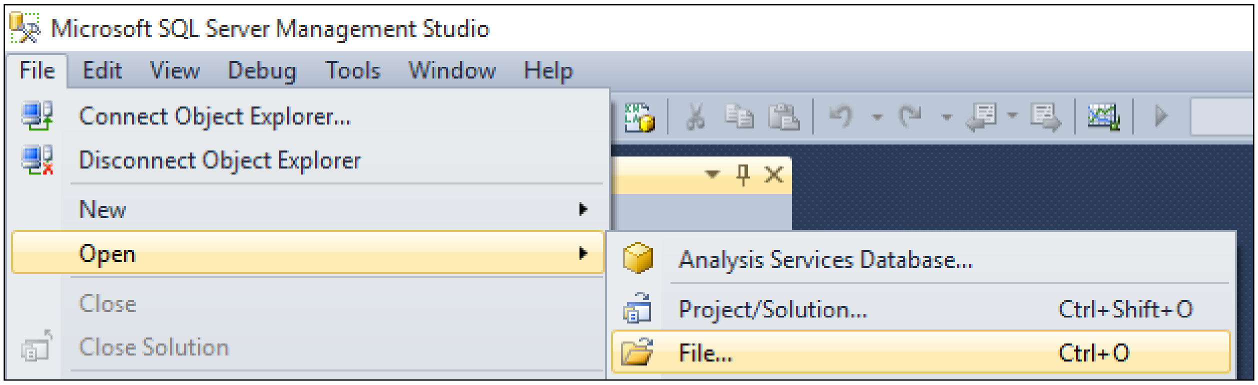
This section outlines the steps required to configure ContactPro.

9.1. Create CCT ContactPro Database and User

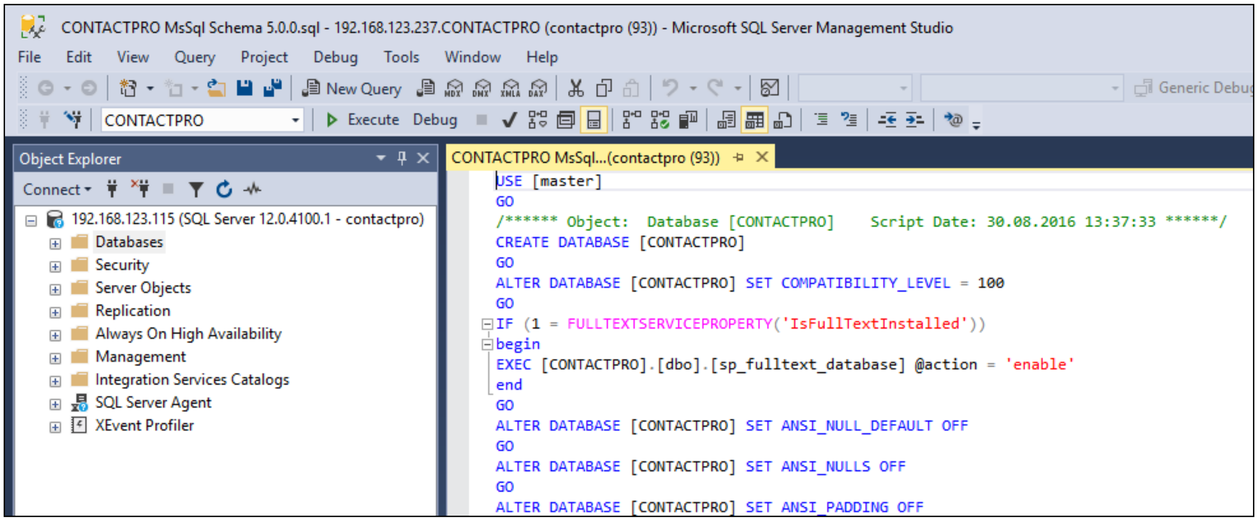
A database and database user for CCT ContactPro must be created on an SQL server.

9.1.1. Create Database

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

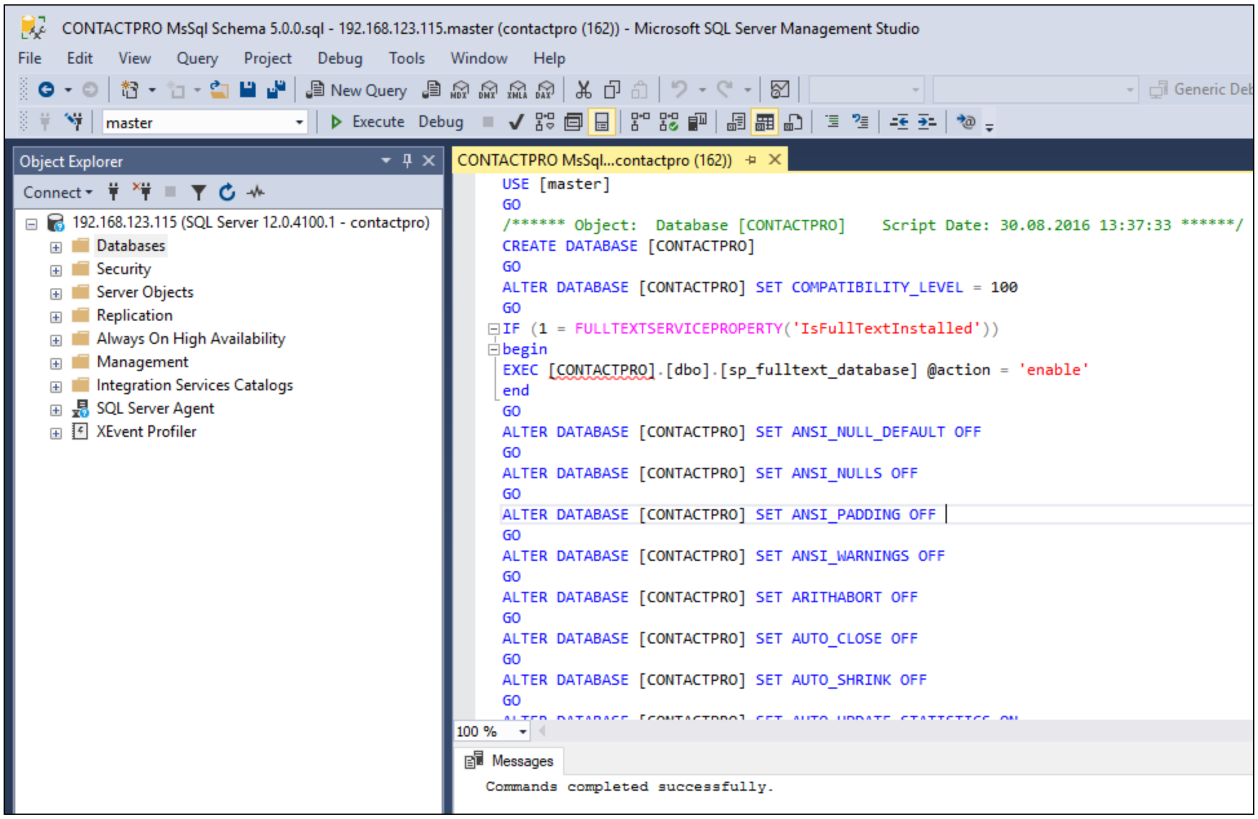

Microsoft SQL Server Management Studio
File
Edit
View
Debug
Tools
Window
Help
Connect Object Explorer...
Disconnect Object Explorer
New
Open
Close
Close Solution
Analysis Services Database...
Project/Solution... Ctrl+Shift+O
File... Ctrl+O

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


CONTACTPRO MsSql Schema 5.0.0.sql - 192.168.123.237.CONTACTPRO (contactpro (93)) - Microsoft SQL Server Management Studio
File
Edit
View
Query
Project
Debug
Tools
Window
Help
New Query
Generic Debug
CONTACTPRO
Execute
Debug
Object Explorer
Connect
192.168.123.115 (SQL Server 12.0.4100.1 - contactpro)
Databases
Security
Server Objects
Replication
Always On High Availability
Management
Integration Services Catalogs
SQL Server Agent
XEvent Profiler
CONTACTPRO MsSql...(contactpro (93))

```
USE [master]
GO
/****** Object:  Database [CONTACTPRO]    Script Date: 30.08.2016 13:37:33 ******/
CREATE DATABASE [CONTACTPRO]
GO
ALTER DATABASE [CONTACTPRO] SET COMPATIBILITY_LEVEL = 100
GO
IF (1 = FULLTEXTSERVICEPROPERTY('IsFullTextInstalled'))
begin
EXEC [CONTACTPRO].[dbo].[sp_fulltext_database] @action = 'enable'
end
GO
ALTER DATABASE [CONTACTPRO] SET ANSI_NULL_DEFAULT OFF
GO
ALTER DATABASE [CONTACTPRO] SET ANSI_NULLS OFF
GO
ALTER DATABASE [CONTACTPRO] SET ANSI_PADDING OFF
```

The following shows the script has been successfully executed to create the database.

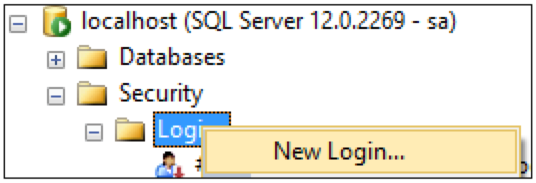

CONTACTPRO MsSql Schema 5.0.0.sql - 192.168.123.115.master (contactpro (162)) - Microsoft SQL Server Management Studio
File
Edit
View
Query
Project
Debug
Tools
Window
Help
New Query
Generic Deb
master
Execute
Debug
Object Explorer
Connect
192.168.123.115 (SQL Server 12.0.4100.1 - contactpro)
Databases
Security
Server Objects
Replication
Always On High Availability
Management
Integration Services Catalogs
SQL Server Agent
XEvent Profiler
CONTACTPRO MsSql...contactpro (162))
100 %
Messages

```
USE [master]
GO
/****** Object:  Database [CONTACTPRO]    Script Date: 30.08.2016 13:37:33 ******/
CREATE DATABASE [CONTACTPRO]
GO
ALTER DATABASE [CONTACTPRO] SET COMPATIBILITY_LEVEL = 100
GO
IF (1 = FULLTEXTSERVICEPROPERTY('IsFullTextInstalled'))
begin
EXEC [CONTACTPRO].[dbo].[sp_fulltext_database] @action = 'enable'
end
GO
ALTER DATABASE [CONTACTPRO] SET ANSI_NULL_DEFAULT OFF
GO
ALTER DATABASE [CONTACTPRO] SET ANSI_NULLS OFF
GO
ALTER DATABASE [CONTACTPRO] SET ANSI_PADDING OFF
GO
ALTER DATABASE [CONTACTPRO] SET ANSI_WARNINGS OFF
GO
ALTER DATABASE [CONTACTPRO] SET ARITHABORT OFF
GO
ALTER DATABASE [CONTACTPRO] SET AUTO_CLOSE OFF
GO
ALTER DATABASE [CONTACTPRO] SET AUTO_SHRINK OFF
GO
ALTER DATABASE [CONTACTPRO] SET AUTO_UPDATE_STATISTICS ON
```

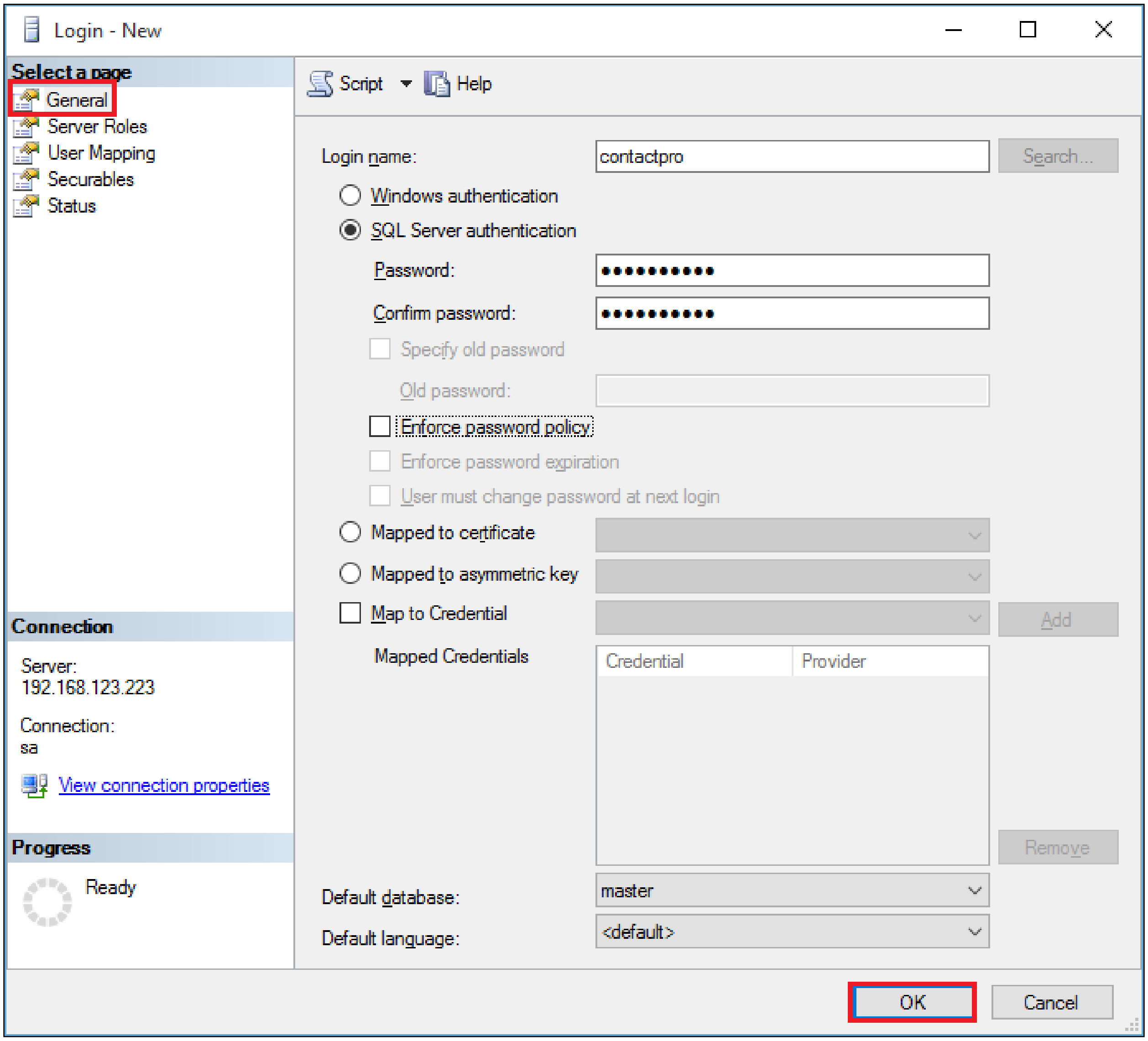
```
Commands completed successfully.
```

9.1.2. 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.** Click on **SQL Server authentication** and enter a suitable **Password** for the **contactpro** user. Click on **OK** at the bottom of the screen once done.



Login - New

Login name: contactpro

○ Windows authentication
● SQL Server authentication

Password: ●●●●●●●●●●●
Confirm password: ●●●●●●●●●●●

□ Specify old password
Old password:
□ Enforce password policy
□ Enforce password expiration
□ User must change password at next login

○ Mapped to certificate
○ Mapped to asymmetric key
□ Map to Credential

Mapped Credentials

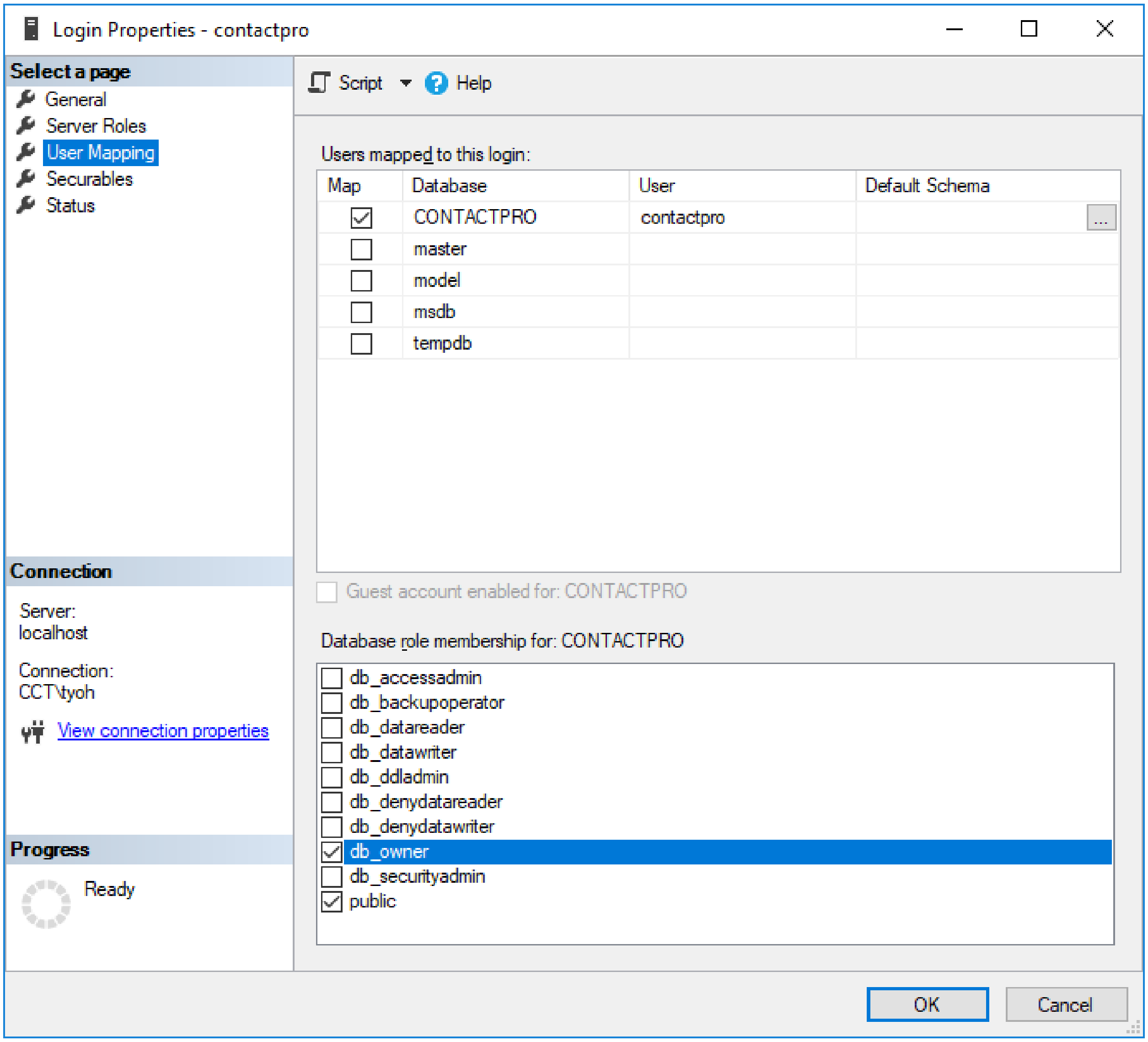
Credential	Provider

Default database: master
Default language: <default>

Server:
192.168.123.223

Connection:
sa

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.



Users mapped to this login:

Map	Database	User	Default Schema
☑	CONTACTPRO	contactpro	...
□	master		
□	model		
□	msdb		
□	tempdb		

□ Guest account enabled for: CONTACTPRO

Database role membership for: CONTACTPRO

- □ db_accessadmin
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- ☑ db_owner
- □ db_securityadmin
- ☑ public

Server:
localhost

Connection:
CCT\tyoh

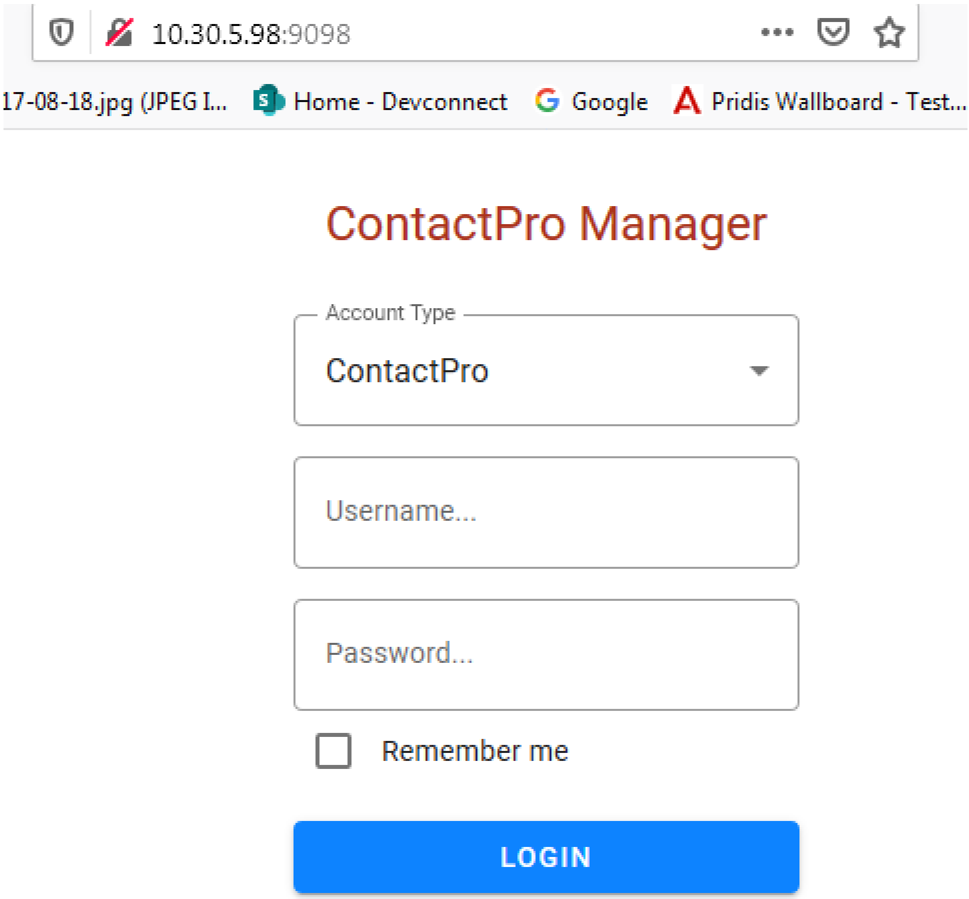
9.2. Configure Properties with ContactPro Manager

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.

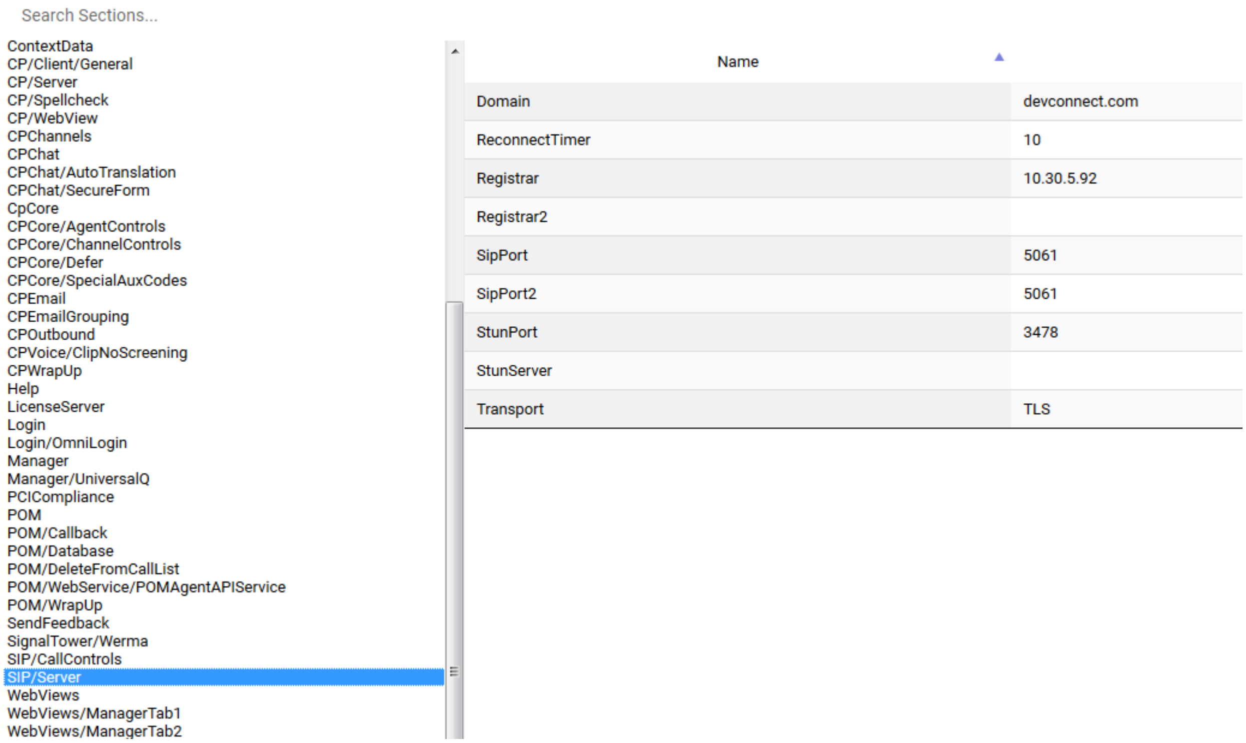
Log in to **ContactPro Manager** via a web session as shown below.



9.2.1. Configure the Connection to Avaya Aura® Session Manager

From a Supervisor or Administrator PC where the CCT ContactPro Manager application was installed, double click on the CCT ContactPro Manager shortcut (not shown). The **ContactPro Manager** is opened and select **SIP/Server** from the **Sections** window.

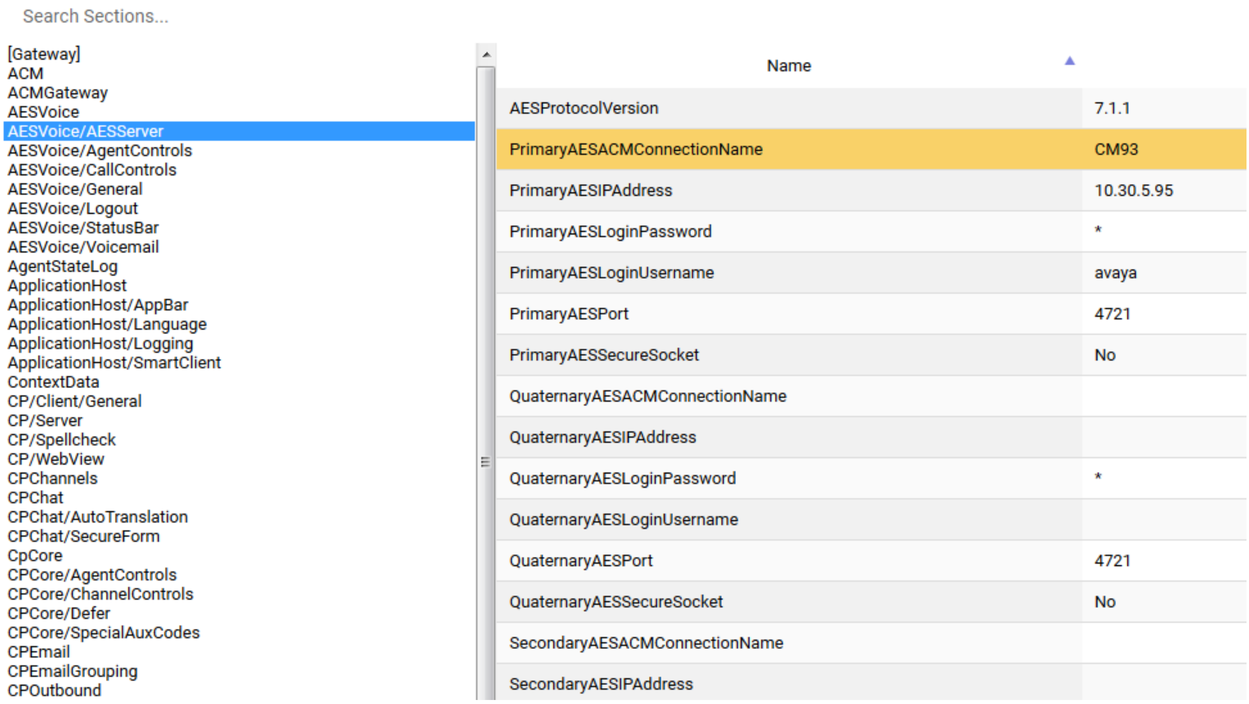
This information below is all required to connect successfully to Session Manager.



Name	
Domain	devconnect.com
ReconnectTimer	10
Registrar	10.30.5.92
Registrar2	
SipPort	5061
SipPort2	5061
StunPort	3478
StunServer	
Transport	TLS

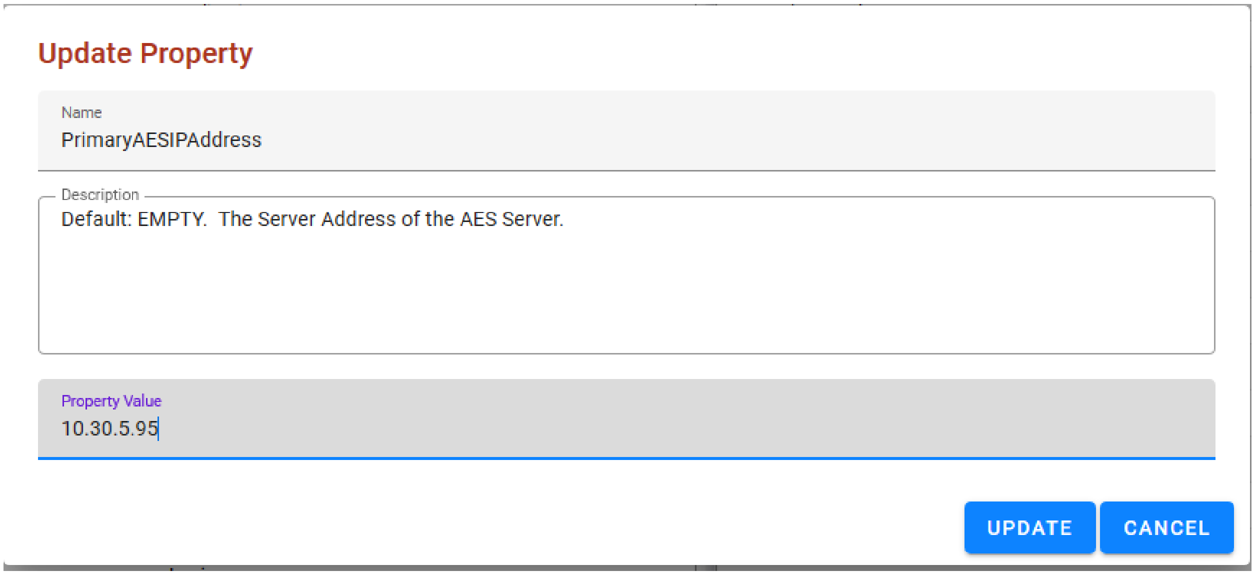
9.2.2. Configure the Connection to Avaya Aura® Application Enablement Services

Click on **AESVoice/AESServer** in the left window. Information on the AES server can be filled in the main window; this information can all be obtained from **Section 7** and all are required to connect successfully to the AES. Each field can be changed by double-clicking on the field.



Name	
AESProtocolVersion	7.1.1
PrimaryAESACMConnectionName	CM93
PrimaryAESIPAddress	10.30.5.95
PrimaryAESLoginPassword	*
PrimaryAESLoginUsername	avaya
PrimaryAESPort	4721
PrimaryAESSecureSocket	No
QuaternaryAESACMConnectionName	
QuaternaryAESIPAddress	
QuaternaryAESLoginPassword	*
QuaternaryAESLoginUsername	
QuaternaryAESPort	4721
QuaternaryAESSecureSocket	No
SecondaryAESACMConnectionName	
SecondaryAESIPAddress	

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



Update Property

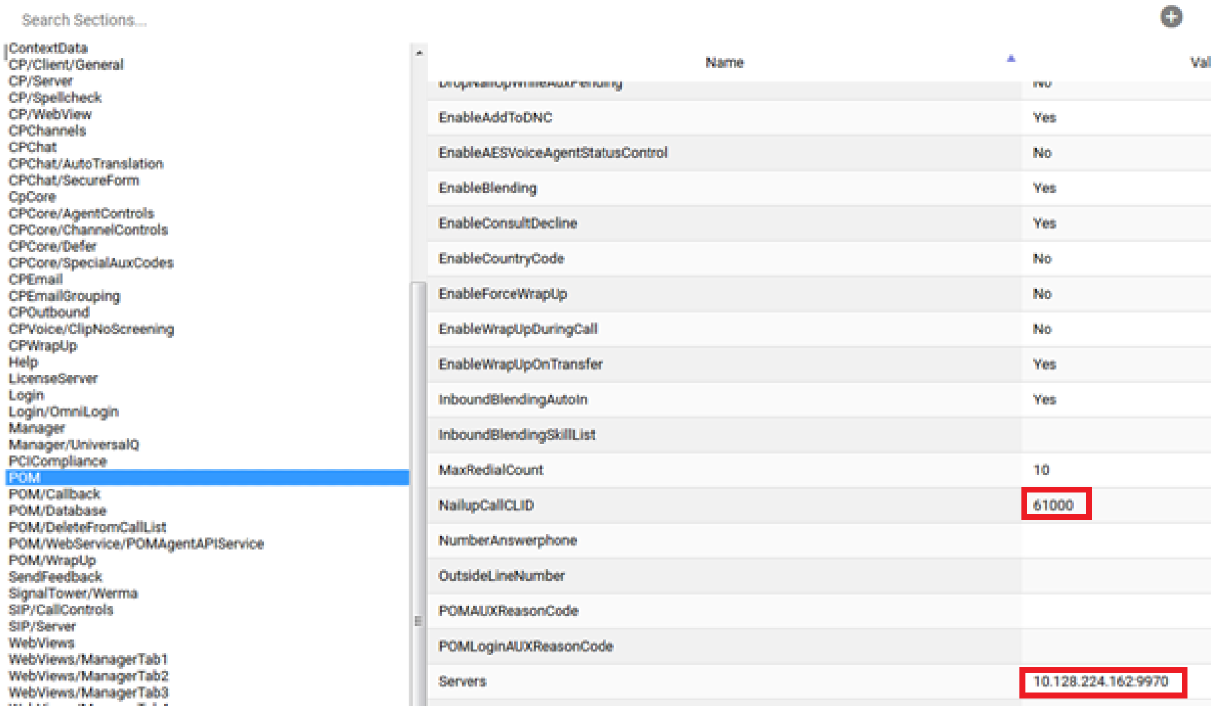
Name: PrimaryAESIPAddress

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

Property Value: 10.30.5.95

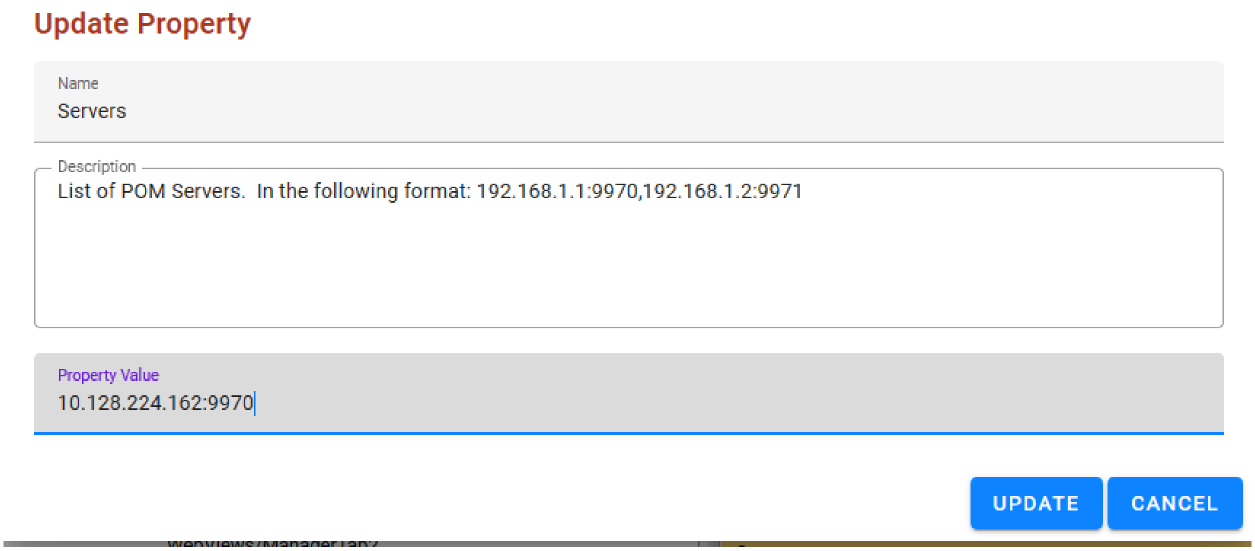
9.2.3. Configure the Connection to POM

In the section **POM,** 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	Val
DropNailUpWhileAuxPending	No
EnableAddToDNC	Yes
EnableAESVoiceAgentStatusControl	No
EnableBlending	Yes
EnableConsultDecline	Yes
EnableCountryCode	No
EnableForceWrapUp	No
EnableWrapUpDuringCall	No
EnableWrapUpOnTransfer	Yes
InboundBlendingAutoIn	Yes
InboundBlendingSkillList	
MaxRedialCount	10
NailupCallCLID	61000
NumberAnswerphone	
OutsideLineNumber	
POMAUXReasonCode	
POMLoginAUXReasonCode	
Servers	10.128.224.162:9970

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



Update Property

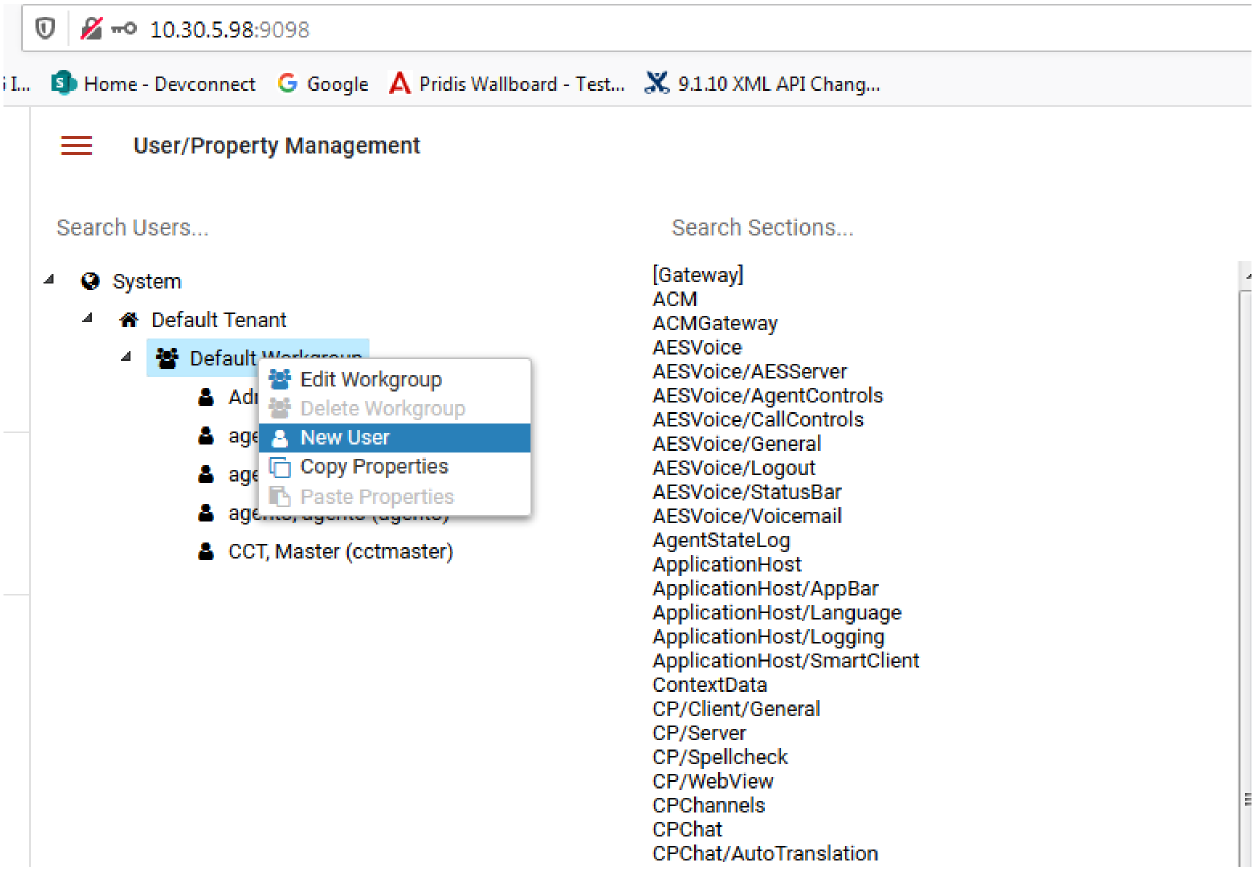
Name
Servers

Description
List of POM Servers. In the following format: 192.168.1.1:9970,192.168.1.2:9971

Property Value
10.128.224.162:9970

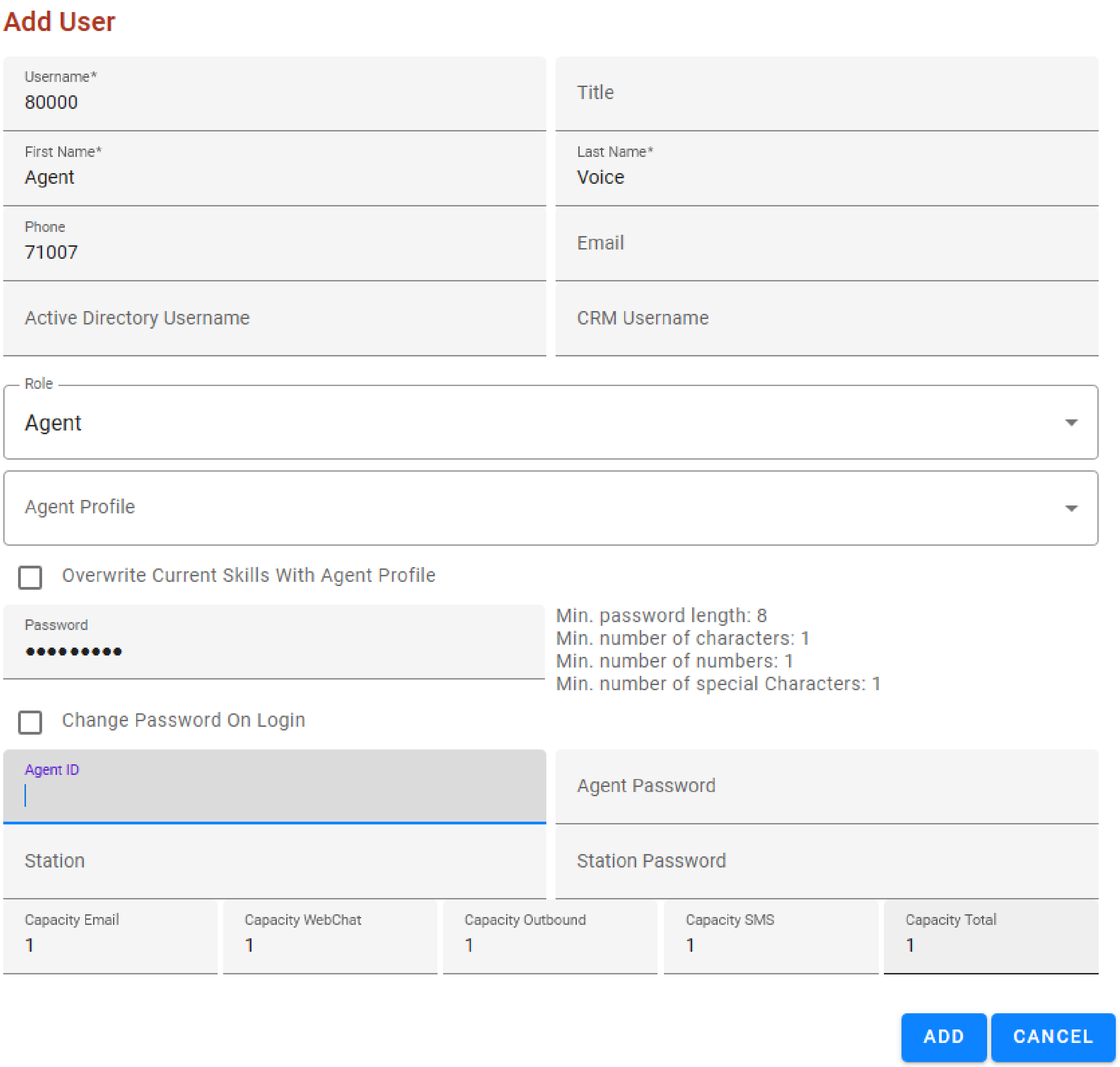
9.3. Configure Users with ContactPro Manager

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 5.3.2** for example).
- **First Name**
- **Last Name**



Add User

Username* 80000	Title
First Name* Agent	Last Name* Voice
Phone 71007	Email
Active Directory Username	CRM Username

Role: Agent

Agent Profile

□ Overwrite Current Skills With Agent Profile

Password: •••••••••

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

□ Change Password On Login

Agent ID	Agent Password
Station	Station Password

Capacity Email	Capacity WebChat	Capacity Outbound	Capacity SMS	Capacity Total
1	1	1	1	1

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.

10. Verification Steps

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

10.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the "status aesvcs cti-link" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**. as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     9        no    aes8             established   14       14
```

Enter the command **list agent-loginID** verify that agent **80000** shown in **Section 5.3.2** is logged-in to extension **71007.**

```
list agent-loginID
                               AGENT LOGINID
Login ID     Name           Extension     Dir Agt  AAS/AUD        COR Ag Pr SO
               Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

80000         Voice Agent    71007                                 1   lvl
                2/01     /       /       /       /       /       /
```

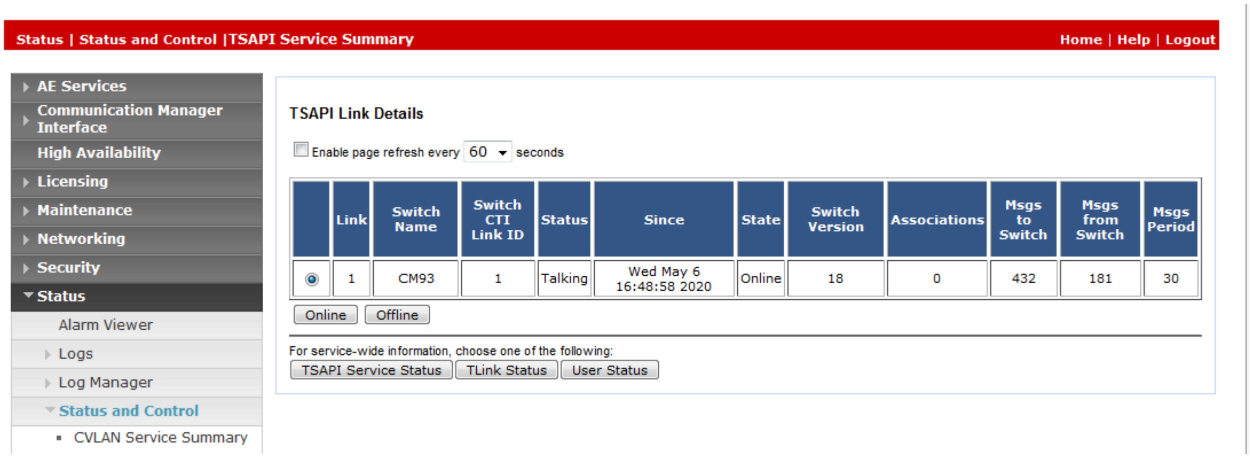
Enter the command **status station 71007** and on **Page 7** verify that the agent is logged-in to the appropriate skill.

```
status station 71007                                           Page   7 of   7
                                   ACD STATUS

 Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod
  2/AI      /        /        /        /        /        /    On ACD Call? no
```

10.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is "Talking" for the TSAPI link administered in **Section 7.3.**



TSAPI Link Details

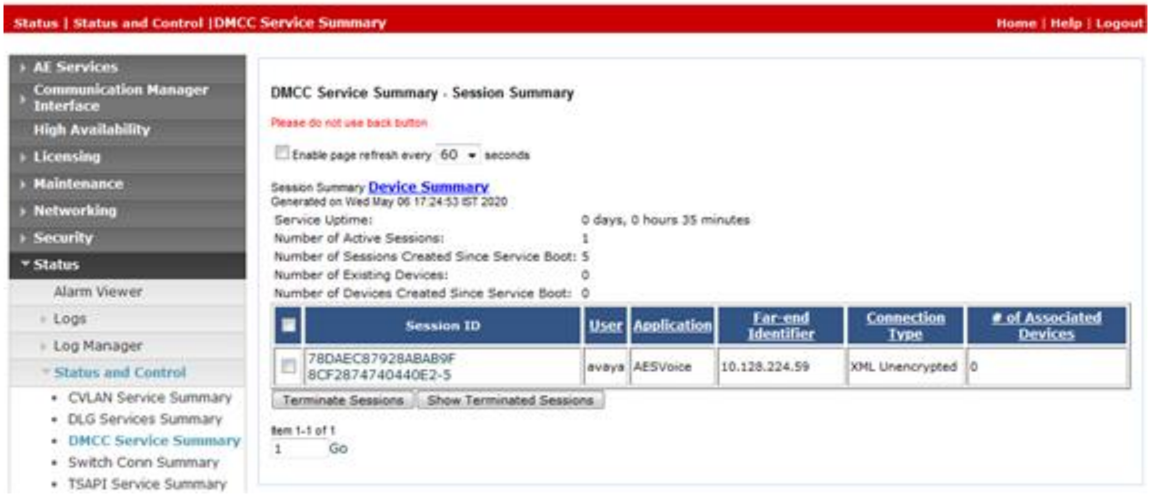
□ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	CM93	1	Talking	Wed May 6 16:48:58 2020	Online	18	0	432	181	30

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

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows action sessions with the CCT user name from **Section 7.5.**



DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Wed May 06 17:24:53 IST 2020

Service Uptime:	0 days, 0 hours 35 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	5
Number of Existing Devices:	0
Number of Devices Created Since Service Boot:	0

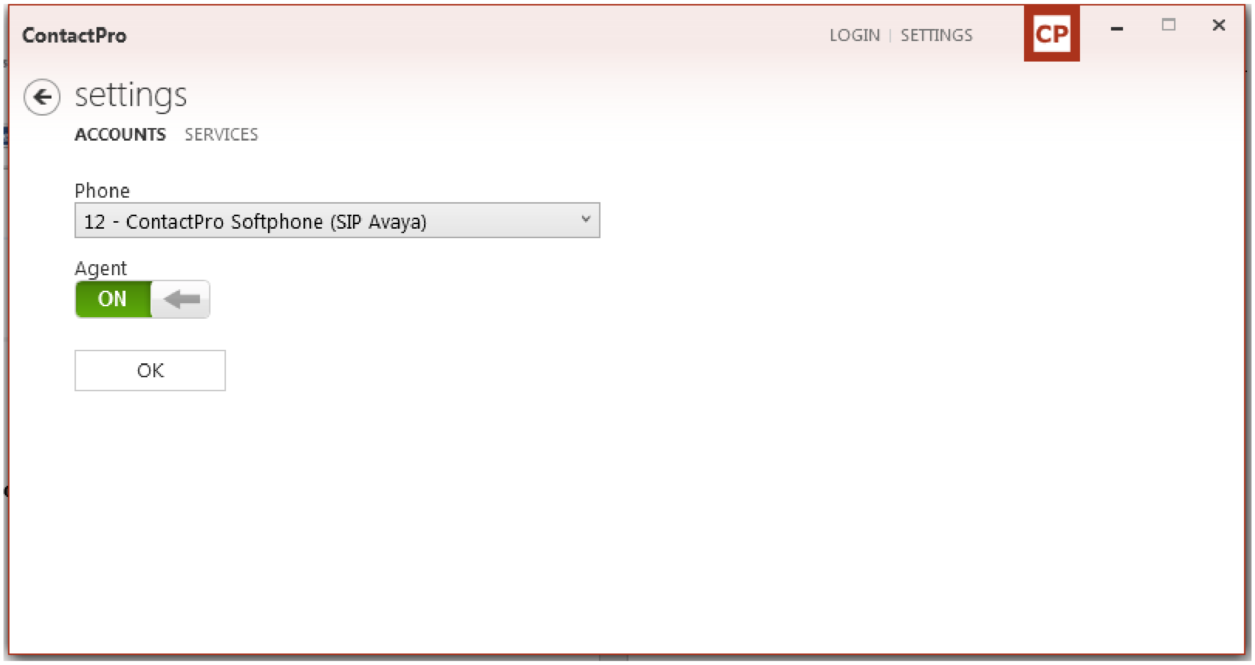
□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	78DAEC87928ABAB9F 8CF2874740440E2-5	avaya	AESVoice	10.128.224.59	XML Unencrypted	0

Item 1-1 of 1

1

10.3. Verify Login of ContactPro Client

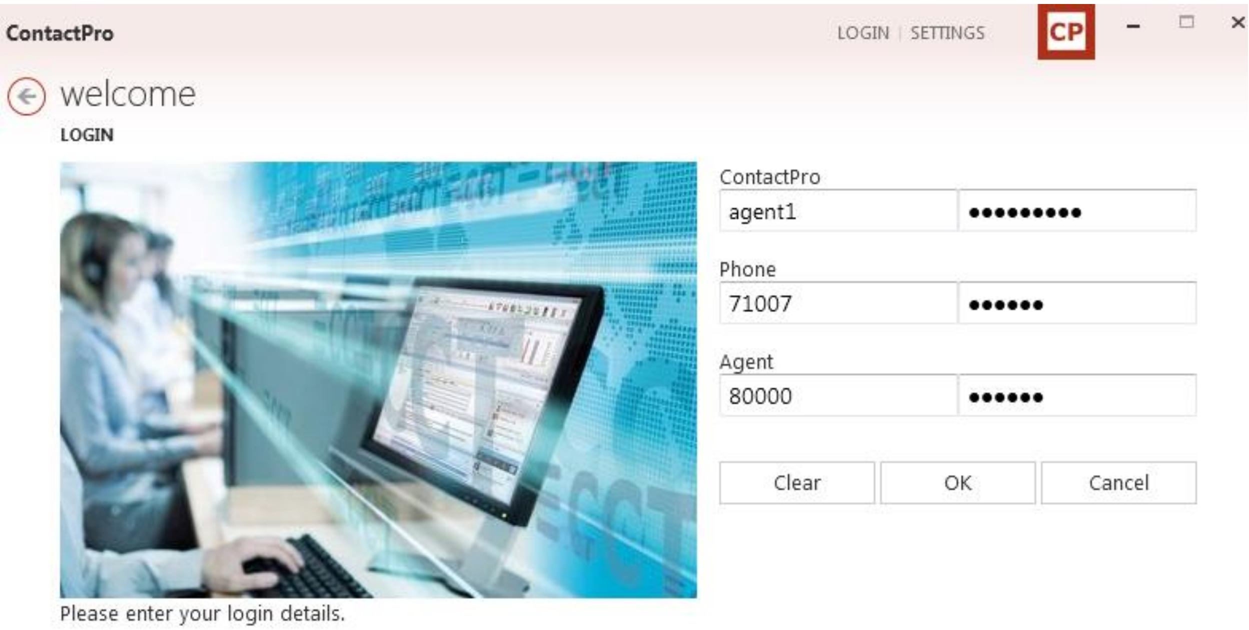
From the Client PC, open the application **ContactPro**. Once this is opened, select **SETTINGS** and choose **Phone** as **12 – ContactPro Softphone (SIP Avaya)**



Phone: 12 - ContactPro Softphone (SIP Avaya)

Agent: ON

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



ContactPro: agent1 ••••••••••

Phone: 71007 ••••••

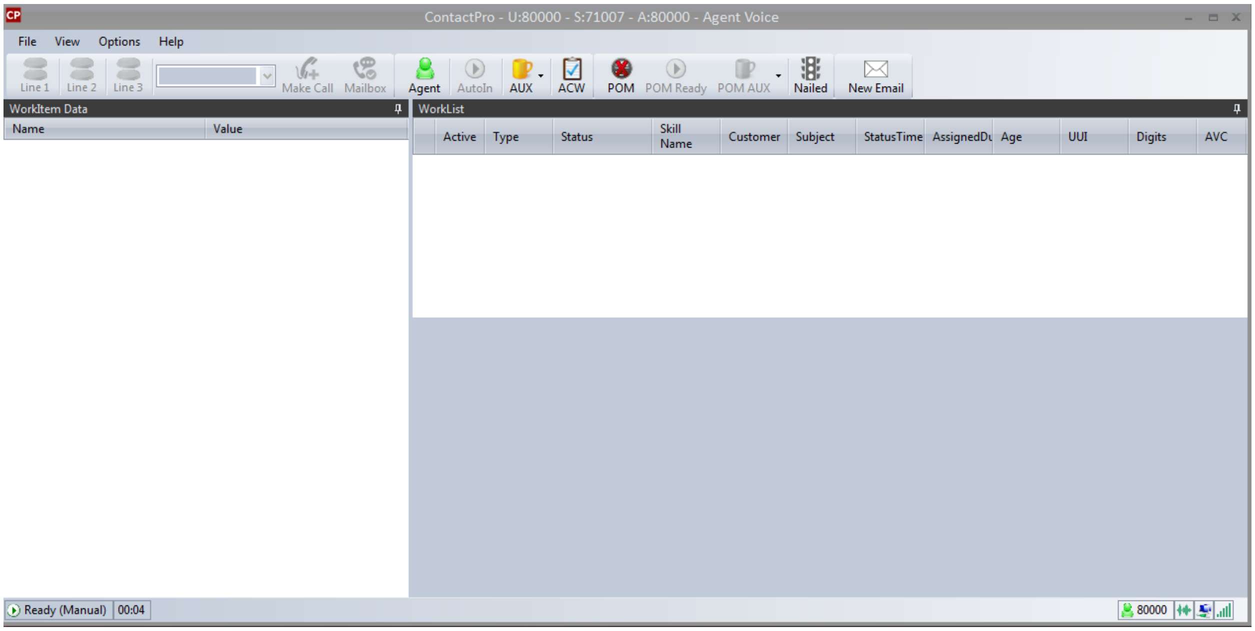
Agent: 80000 ••••••

Please enter your login details.

Click on **OK** to log into **ContactPro.**

10.3.1. 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 (**71007**) and Agent ID (**80000**) once logged in.



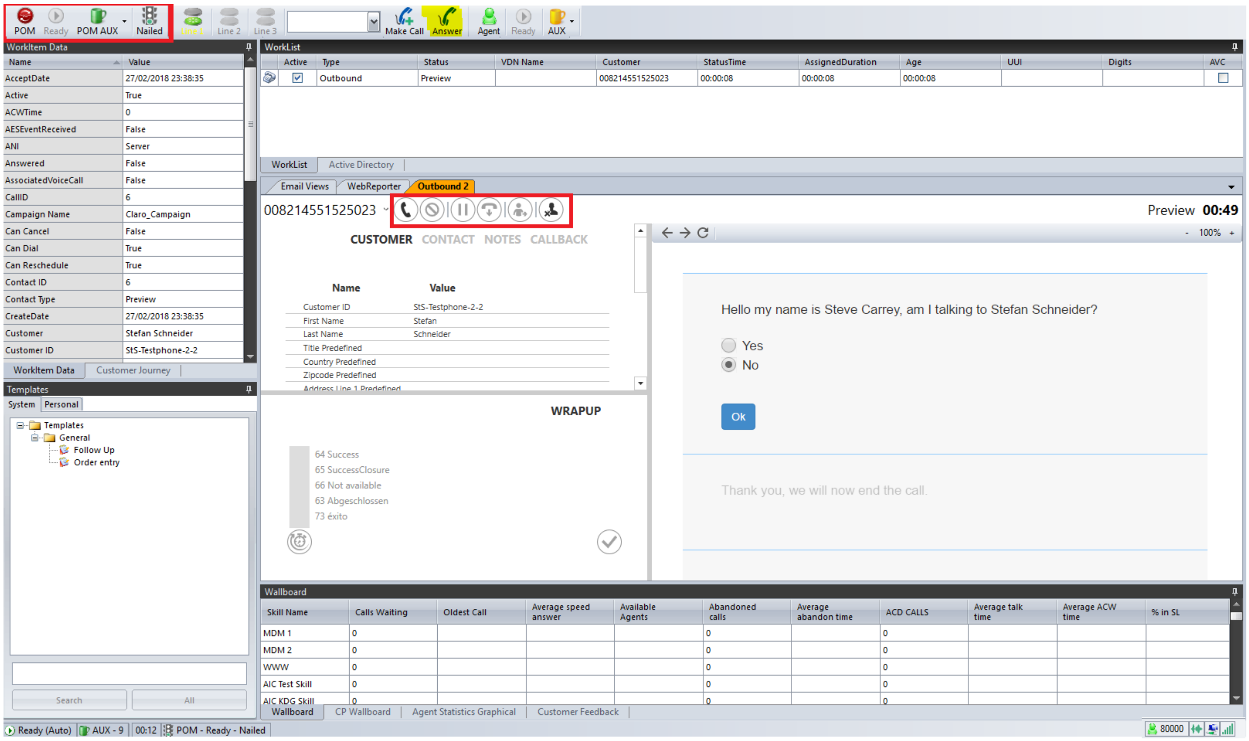
Make an incoming call from PSTN to a general routing Hunt Group in **Section 5.3.1.** Verify that the CCT ContactPro Client can receive incoming call. Answer incoming calls with the **Answer** button (not shown).

10.3.2. 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

A new outbound tab is created with details of the customer. POM call actions can be performed using the call control buttons inside the tab or follow the campaign scripts.



WorkItem Data

Name	Value
AcceptDate	27/02/2018 23:38:35
Active	True
ACWTime	0
AESEventReceived	False
ANI	Server
Answered	False
AssociatedVoiceCall	False
CallID	6
Campaign Name	Claro_Campaign
Can Cancel	False
Can Dial	True
Can Reschedule	True
Contact ID	6
Contact Type	Preview
CreateDate	27/02/2018 23:38:35
Customer	Stefan Schneider
Customer ID	StS-Testphone-2-2

WorkList

	Active	Type	Status	VDN Name	Customer	StatusTime	AssignedDuration	Age	UUI	Digits	AVC
	☑	Outbound	Preview		008214551525023	00:00:08	00:00:08	00:00:08			□

008214551525023

Name	Value
Customer ID	StS-Testphone-2-2
First Name	Stefan
Last Name	Schneider
Title Predefined	
Country Predefined	
Zipcode Predefined	
Address Line 1 Predefined	

WRAPUP

64 Success
65 SuccessClosure
66 Not available
63 Abgeschlossen
73 éxito

Preview 00:49

100%

Hello my name is Steve Carrey, am I talking to Stefan Schneider?

○ Yes
● No

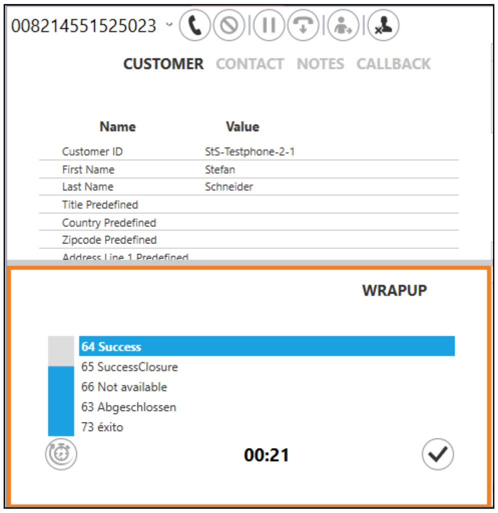
Ok

Thank you, we will now end the call.

Wallboard

Skill Name	Calls Waiting	Oldest Call	Average speed answer	Available Agents	Abandoned calls	Average abandon time	ACD CALLS	Average talk time	Average ACW time	% in SL
MDM 1	0				0		0			
MDM 2	0				0		0			
WWW	0				0		0			
AIC Test Skill	0				0		0			
AIC KDG Skill	0				0		0			

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


008214551525023

Name	Value
Customer ID	StS-Testphone-2-1
First Name	Stefan
Last Name	Schneider
Title Predefined	
Country Predefined	
Zipcode Predefined	
Address Line 1 Predefined	

WRAPUP

64 Success
65 SuccessClosure
66 Not available
63 Abgeschlossen
73 éxito

00:21

11. Conclusion

These Application Notes describe the configuration steps required for ContactPro 5.3 from CCT Deutschland GmbH to interoperate with Avaya Avaya Aura® Application Enablement Services R8.1.1 and Avaya Proactive Outreach Manager (POM) 3.1.3. 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. *Administering Avaya Aura® Communication Manager,* Release 8.0.x, Issue 7, Nov 2019
2. *Administering Avaya Aura® Session Manager,* Release 8.0.x, Issue 5, May 2020
3. *Administering Avaya Aura® Application Enablement Services,* Release 8.1.x, Issue 6, June 2020
4. *Proactive Outreach Manager 3.1 Overview and Specification*
5. *Implementing Proactive Outreach Manager 3.1,* Issue 1.3, June 2020

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.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.