



Avaya Solution & Interoperability Test Lab

Application Notes for configuring NICE Engage Platform to interoperate with Avaya Proactive Outreach Manager, Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services using DMCC Multi-Registration to record calls - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the NICE Engage Platform to interoperate with the Avaya solution consisting of an Avaya Proactive Outreach Manager R3.0, an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, an Avaya Aura® Contact Center R7.0 and Avaya Aura® Application Enablement Services R7.0 using Multi-Registration.

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 for the NICE Engage Platform R6.5 to interoperate with the Avaya solution consisting of an Avaya Proactive Outreach Manager R3.0, an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Contact Center R7.0 and Avaya Aura® Application Enablement Services R7.0. NICE Engage Platform uses Communication Manager's Multiple Registration feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Web Services Interface on Avaya Proactive Outreach Manager to capture the audio and call details for outbound calls initiated from outbound campaigns on Avaya Proactive Outreach Manager.

Avaya Proactive Outreach Manager was used to create a preview and progressive outbound campaigns. With a preview campaign the Contact Center agent is popped with the next call and thus the agent is in control of when the call is to be made. This can be ideal for more complex sales where a bit of research is required between calls to increase the chances of success. A progressive campaign removes the option of when the next call is made from the agent. On completing the previous call (or moving from "Wrap-up" to "Go ready") the system automatically dials the next number on the list. This removes the wait time between calls and can improve productivity significantly. This is ideal where the calls are very similar in nature and agents benefit from having the system tee up the next call for them.

DMCC works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with the AES server monitors the digital and VoIP extensions. The application uses the AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device and records the call.

The NICE Engage Platform is fully integrated into a LAN (Local Area Network), and includes easy-to-use Web based applications (i.e. Nice Application) that works with the Microsoft .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. This application registers an extension with Avaya Aura® Communication Manager and waits for that extension to be dialed. The NICE Engage Platform contains tools for audio retrieval, centralized system security authorization, system control, and system status monitoring. Also included is a call parameters database (Nice Application Server) that tightly integrates via CTI link PABXs and ACD's including optional advanced audio archive database management, search tools, a wide variety of Recording-on-Demand capabilities, and comprehensive long-term call database for immediate retrieval.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the NICE Engage Platform to carry out call recording of outbound dialling campaigns initiated by Avaya Proactive Outreach Manager using DMCC Multi-Registration with AES and Communication Manager to record the calls. A preview and a progressive campaign were created on Proactive Outreach Manager and Contact Center agents were given the Proactive Outreach Manager skillset in order to allow the outbound calls be made from the agents desktop using Avaya Aura® Agent Desktop (AAAD). These outbound calls were then recorded and played back in order to verify that NICE Engage Platform could be used to record outbound calls from Proactive Outreach Manager using AAAD.

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 interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Outbound calls in a Preview Campaign** – Test call recording for outbound calls in a preview campaign created on POM made to both QSIG and SIP PSTN endpoints.
- **Hold/Transferred/Conference calls** – Test call recording of outbound calls in a preview campaign on hold, transferred and conferenced.
- **Outbound calls in a Progressive Campaign** - Test call recording for outbound calls in a progressive campaign created on POM made to both QSIG and SIP PSTN endpoints.
- **Hold/Transferred/Conference calls** - Test call recording of outbound calls in a progressive campaign on hold, transferred and conferenced.
- **Serviceability testing** - The behavior of NICE Engage Platform under different simulated failure conditions.

2.2. Test Results

Most functionality and serviceability test cases were completed successfully. The following observation was noted.

1. **Call on Hold.** The Agent can always be heard, there is no hold on the recording from the agent side only from the PSTN side. This is as per NICE design.

2.3. Support

Technical support can be obtained for NICE Engage Platform from the website <http://www.nice.com/engage/services/support>

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Engage Platform with the Avaya solution using DMCC Multi-Registration to record calls. The NICE Application Server is setup for DMCC Multi-Registration mode and connects to the AES. The Avaya solution consists of Contact Center agents making outbound calls from campaigns run from Proactive Outreach Manager.

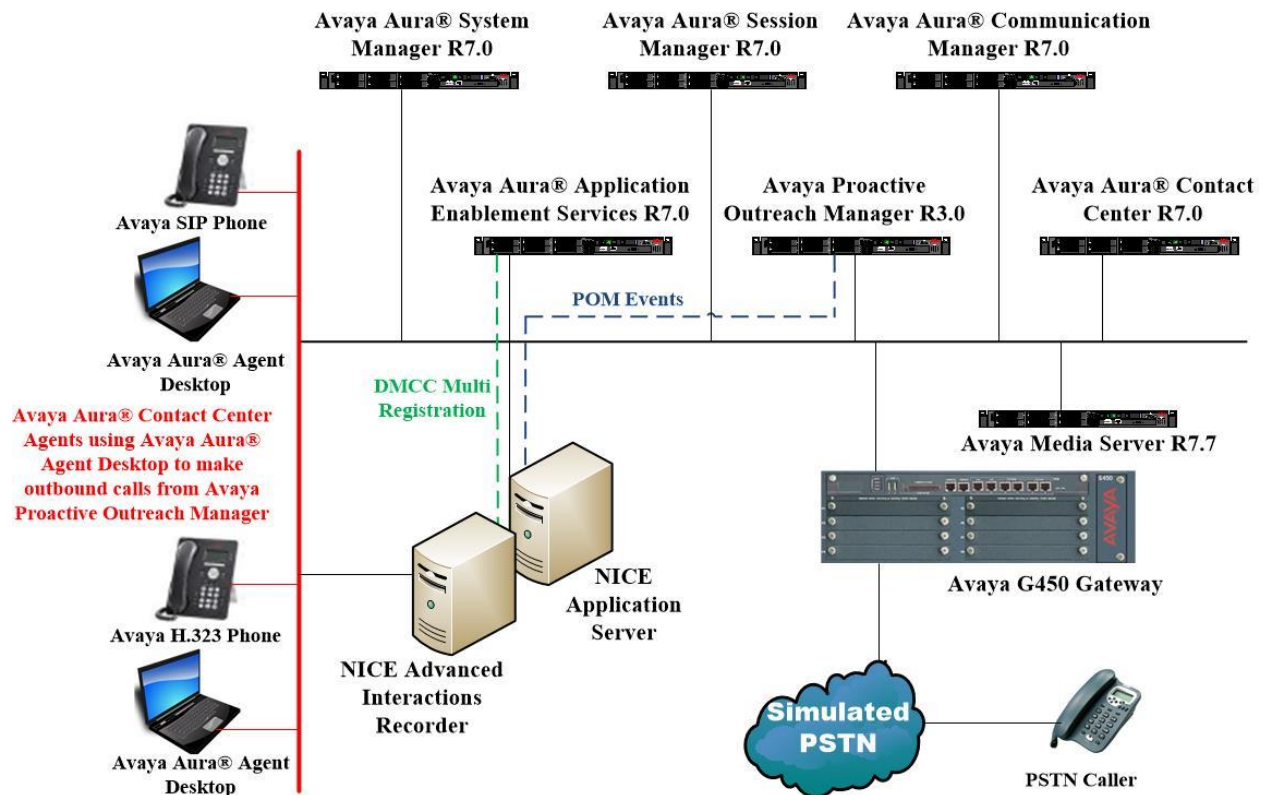


Figure 1: Connection of NICE Engage Platform R6.5 with Avaya Proactive Outreach Manager R3.0, Avaya Aura® Contact Center R7.0, Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager R7.0 and Avaya Aura® Application Enablement Services R7.0

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 7.0.1.1 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.1.065378 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP1 Build No. – 7.0.1.1.701114
Avaya Aura® Communication Manager running on a virtual server	R7.0 R017x.00.0.441.0 00.0.441.0-23169
Avaya Aura® Application Enablement Services running on Virtual Server	R7.0 Build No – 7.0.1.0.3.15-0
Avaya Proactive Outreach Manager	R3.0 POM 03.00.03.03.008
Avaya Aura® Contact Center	R7.0
Avaya Aura® Agent Desktop	R7.0
Avaya G450 Gateway	37.19.0 /1
Avaya Media Server running on a virtual server	Media Server System R7.7.0.8 Media Server R7.7.0.200
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 7.0.0.39
NICE Engage Platform - Application Server - Advanced Interactions Recorder	R6.5

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. Verify System Features

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

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

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

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes70vmpg**).

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM100	10.10.40.34		
aes70vmpg	10.10.40.26		
default	0.0.0.0		
g450	10.10.40.15		
procr	10.10.40.13		

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

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

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

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

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

- **AE Services Server:** Name obtained from the AES server, in this case **aes70vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

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

change ip-services				Page	4	of	4
AE Services Administration							
Server ID	AE Services Server	Password	Enabled	Status			
1:	aes70vmpg	*****	y	idle			
2:							
3:							

5.4. Configure CTI Link for TSAPI Service

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

add cti-link 1		Page 1 of 3	
CTI LINK			
CTI Link: 1			
Extension: 2002			
Type: ADJ-IP			
COR: 1			
Name: aes70vmpg			

5.5. Configure H323 Stations for Multi-Registration

All endpoints that are to be monitored by NICE will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required in **Section 8.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

change station x	Page 1 of 6	
STATION		
Extension: x	Lock Messages? n	BCC: 0
Type: 9608	Security Code: 1234	TN: 1
Port: S00101	Coverage Path 1:	COR: 1
Name: Extension	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 1591	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

5.6. Configure SIP Stations for Multi-Registration

Any SIP extension that is to be recorded requires some configuration changes to allow call recording using multiple registration. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.

Note: The following shows changes to a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.

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.

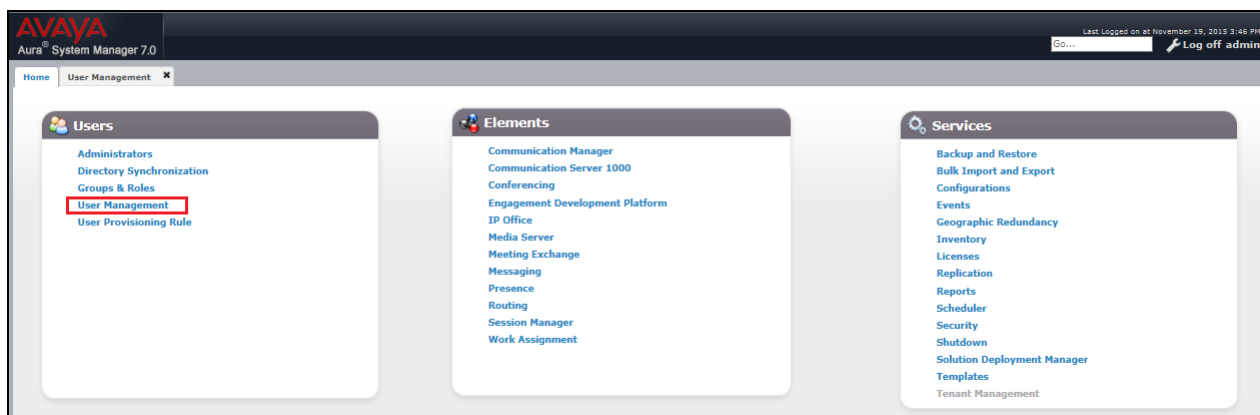
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:
Password:

[Change Password](#)

Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

From the home page click on **User Management** highlighted below.



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.

Avaya Aura System Manager 7.0

Home / Users / User Management / Manage Users

User Management

Users

View Edit New Duplicate Delete More Actions

15 Items Show All

	Last Name	First Name	Display Name	Login Name	SIP Handle
<input checked="" type="checkbox"/>	7100	SIPEXt	7100, SIPEXt	7100@devconnect.local	7100
<input type="checkbox"/>	7101	SIPEXt	7101, SIPEXt	7101@devconnect.local	7101
<input type="checkbox"/>	7200	Ascom i62	7200, Ascom i62	7200@devconnect.local	7200
<input type="checkbox"/>	7201	Ascom i62	7201, Ascom i62	7201@devconnect.local	7201
<input type="checkbox"/>	7202	Ascom i62	7202, Ascom i62	7202@devconnect.local	7202
<input type="checkbox"/>	7203	Ascom i62	7203, Ascom i62	7203@devconnect.local	7203

Click on the **Communication Profile** tab. Ensure that the **Communication Profile Password** is known and if not click on edit to change it.

Avaya Aura System Manager 7.0

Home / Users / User Management / Manage Users

User Profile Edit: 7100@devconnect.local

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: ***** Edit

New Delete Done Cancel

Name

Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	7100	devconnect.local

Select : All, None

From the same page scroll down to **CM Endpoint Profile** click on **Endpoint Editor** to make further changes.

☒ **CM Endpoint Profile**

* System

cm70vmpg

* Profile Type

Endpoint

Use Existing Endpoints

☐

* Extension

7100

Endpoint Editor

Template

9641SIPCC DEFAULT CM 7 0

Set Type

9641SIPCC

Security Code

Port

S00003

Voice Mail Number

Preferred Handle

(None)

Calculate Route Pattern

☐

Sip Trunk

aar

Enhanced Callr-Info display for 1-line phones

☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User

☒

Override Endpoint Name and Localized Name

☒

Allow H.323 and SIP Endpoint Dual Registration

☐

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

Edit Endpoint

Done Cancel

[Save As Template]

System: cm70vmppg Extension: 7100
 Template: 9641SIPCC_DEFAULT_CM_7_0 Set Type: 9641SIPCC
 Port: 500003 Security Code:
 Name: 7100, SIPExt

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

* **Class of Restriction (COR)**: 1 * **Class Of Service (COS)**: 1
 * **Emergency Location Ext**: 7100 * **Message Lamp Ext.**: 7100
 * **Tenant Number**: 1
 * **SIP Trunk**: aar **Type of 3PCC Enabled**: Avaya
Coverage Path 1:
Lock Message: ☐
Localized Display Name: 7100, SIPExt
Multibyte Language: Not Applicable **Enable Reachability for Station Domain Control**: system

*Required

Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done**, at the bottom of the screen, once this is set.

General Options (G) * **Feature Options (F)** Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

Active Station Ringing: single
MWI Served User Type: sip-adjunct
Per Station CPN - Send Calling Number: None
IP Phone Group ID:
Remote Soft Phone Emergency Calls: as-on-local
LWC Reception: spe
AUDIX Name:
Short/Prefixed Registration Allowed: default
Voice Mail Number:

Auto Answer: none
Coverage After Forwarding: system
Display Language: english
Hunt-to Station:
Loss Group: 19
Survivable COR: internal
Time of Day Lock Table: None
Music Source:

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
- ☐ Idle Appearance Preference
- ☒ **IP SoftPhone**
- ☒ LWC Activation
- ☐ CDR Privacy
- ☒ Direct IP-IP Audio Connections
- ☐ H.320 Conversion
- ☐ IP Video Softphone
- ☐ Per Button Ring Control

*Required

Done Cancel

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

The screenshot shows the Avaya Aura System Manager 7.0 web interface. The top header includes the Avaya logo, 'Aura® System Manager 7.0', and a 'Log off admin' button. The left sidebar contains a 'User Management' menu with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', 'Communication Profile', and 'Password Policy'. The main content area is titled 'User Profile Edit: 7100@devconnect.local' and features a 'Commit' button highlighted with a red box. Below this, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' field and a 'Name' dropdown menu set to 'Primary'. A 'Default' checkbox is checked. At the bottom, there is a 'Communication Address' section.

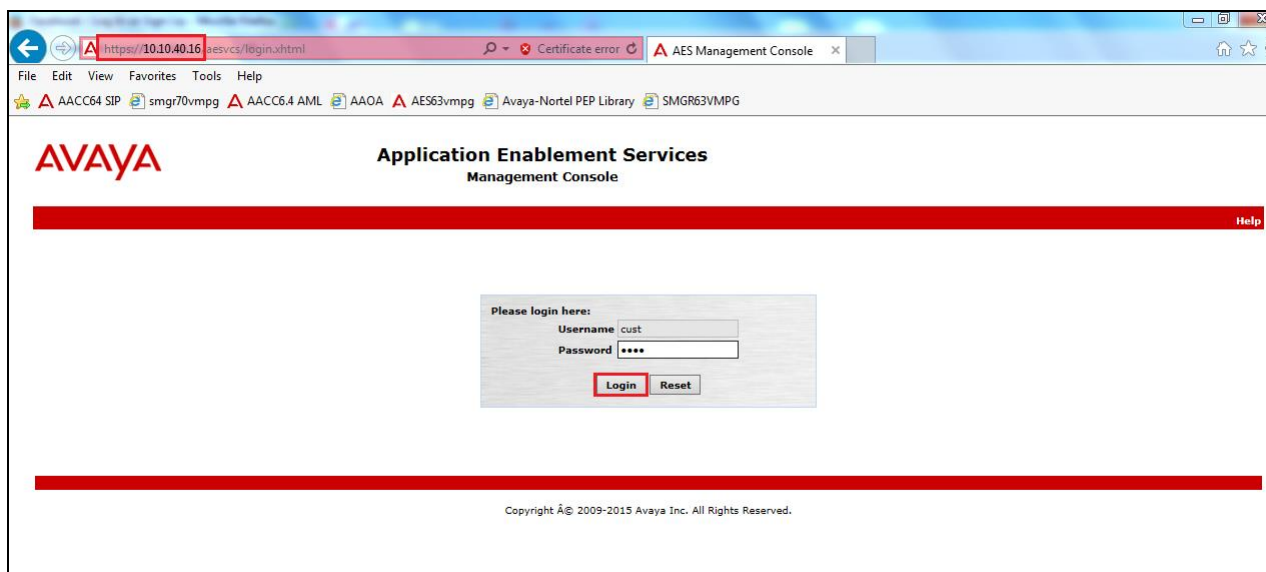
6. Configure Avaya Aura® Application Enablement Services

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 and DMCC Ports
- Create CTI User
- Associate Devices with CTI User

6.1. Verify Licensing

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



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

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222
Number of prior failed login attempts: 1
HostName/IP: aes70vmppg
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-0
Server Date and Time: Tue Nov 24 16:15:51 GMT 2015
HA Status: Not Configured

AE Services Home | Help | Logout

▼ AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI
- TWS
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

AE Services

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

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	N/A	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

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

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

License Information
You are licensed to run Application Enablement (CTI) release 7.x:

6.2. Create Switch Connection

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

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222
Number of prior failed login attempts: 1
HostName/IP: aes70vmppg
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-0
Server Date and Time: Tue Nov 24 16:16:56 GMT 2015
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

▼ AE Services

- Communication Manager Interface
- Switch Connections
- Dial Plan
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

Switch Connections

cm70vmppg x **Add Connection**

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

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

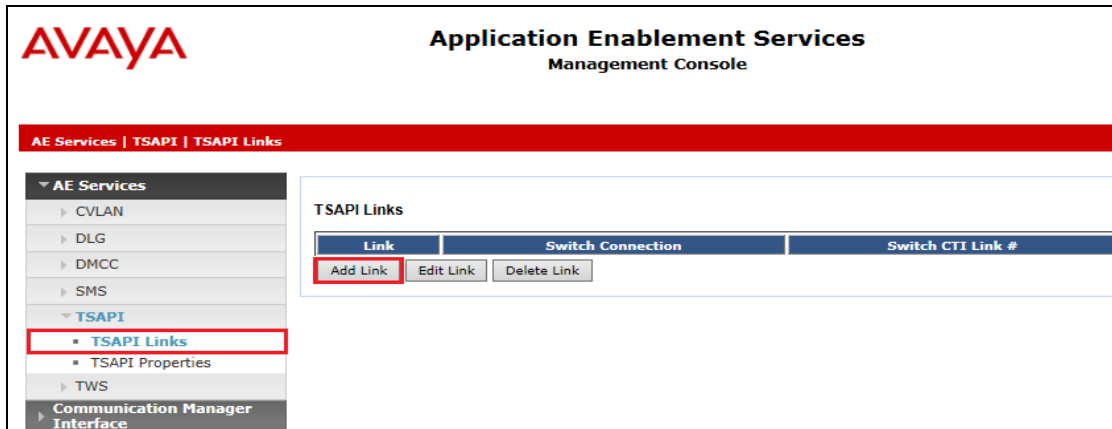
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface (selected), Switch Connections (highlighted with a red box), Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Connection Details - cm70vmppg' and contains the following fields: Switch Password (password field), Confirm Switch Password (password field), Msg Period (30 Minutes (1 - 72)), Provide AE Services certificate to switch (checkbox), Secure H323 Connection (checkbox), and Processor Ethernet (checked checkbox). The 'Apply' button is highlighted with a red box.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar is the same as the previous screenshot. The main content area is titled 'Edit Processor Ethernet IP - cm70vmppg' and contains the following fields: 10.10.40.13 (text field), Add/Edit Name or IP (button, highlighted with a red box), and a table with the following data: 10.10.40.13 (Name or IP Address). The 'Back' button is also visible.

6.3. Administer TSAPI link

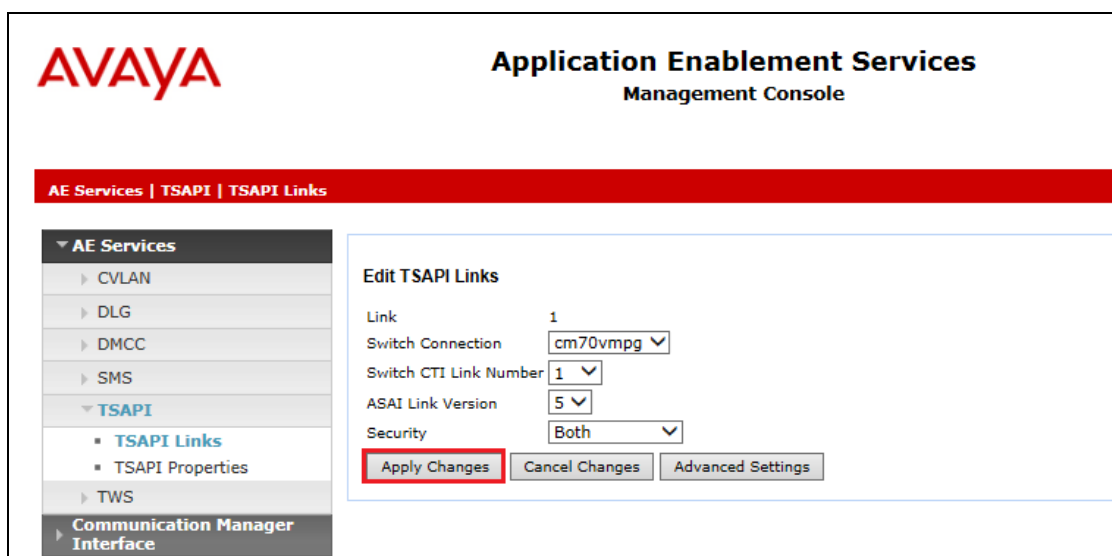
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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 **cm70vmpg**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



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

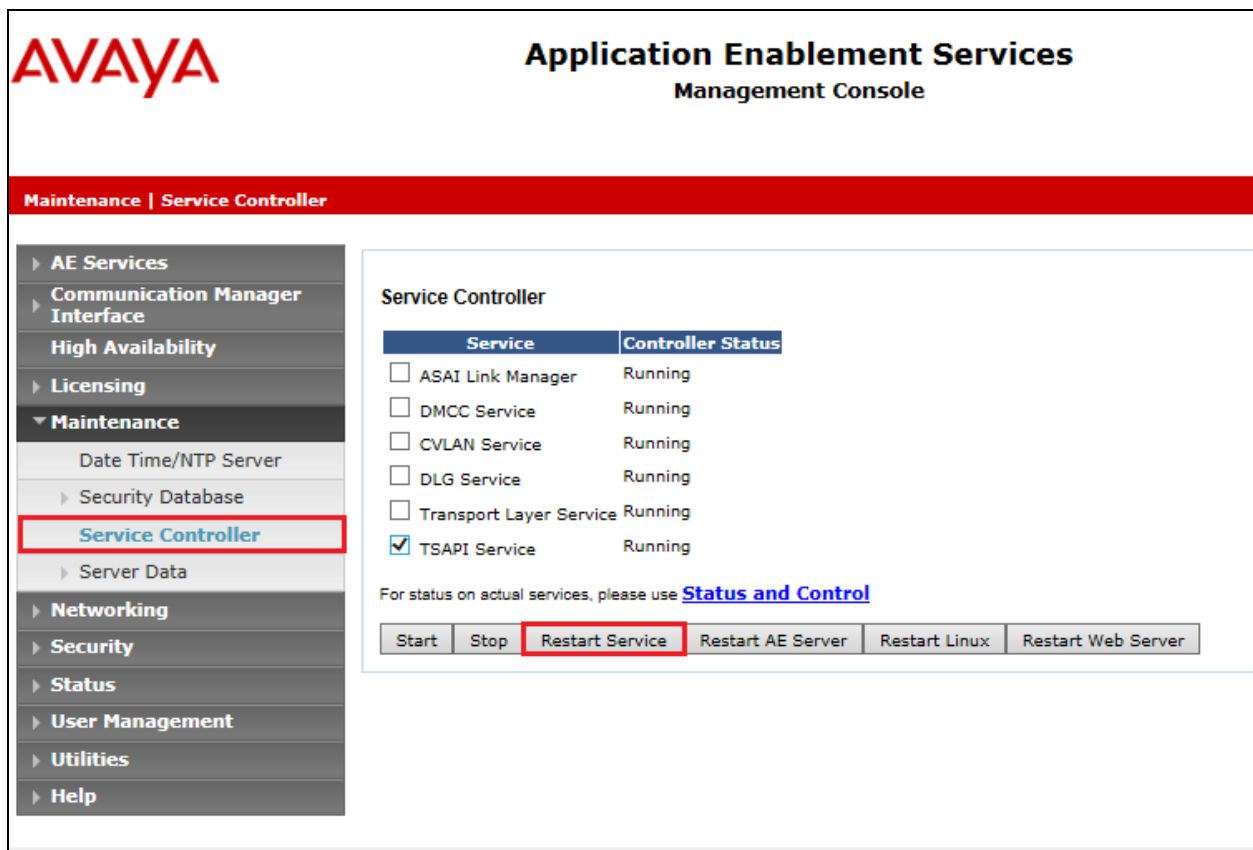
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), 'TSAPI Links', 'TSAPI Properties', 'TWS', and 'Communication Manager Interface'. The main content area displays a confirmation dialog titled 'Apply Changes to Link'. The dialog text reads: 'Warning! Are you sure you want to apply the changes? These changes can only take effect when the TSAPI server restarts. Please use the Maintenance -> Service Controller page to restart the TSAPI server.' There are 'Apply' and 'Cancel' buttons at the bottom of the dialog.

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

The screenshot shows the Avaya Application Enablement Services Management Console after the TSAPI link is completed. The left sidebar is the same as the previous screenshot, but 'TSAPI Links' is now selected. The main content area displays a table titled 'TSAPI Links'. The table has five columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. There is one row with the following data: Link 1, Switch Connection cm70vmpg, Switch CTI Link # 1, ASAI Link Version 5, and Security Both. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'. In the top right corner, there is a welcome message and system information: 'Welcome! User: cust', 'Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222', 'Number of prior failed login attempts: 1', 'HostName/IP: aes70vmpg', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.0.0.0.13-0', 'Server Date and Time: Tue Nov 24 16:26:08 GMT 2015', and 'HA Status: Not Configured'. The bottom right corner has links for 'Home', 'Help', and 'Logout'.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm70vmpg	1	5	Both

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**.



AVAYA Application Enablement Services Management Console

Maintenance | Service Controller

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

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

Start Stop **Restart Service** Restart AE Server Restart Linux Restart Web Server

6.4. Enable TSAPI and DMCC Ports

To ensure that TSAPI 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 9.1**.

AVAYA Application Enablement Services Management Console

Networking | Ports

Ports

CVLAN Ports

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

DLG Port

TCP Port	
5678	

TSAPI Ports

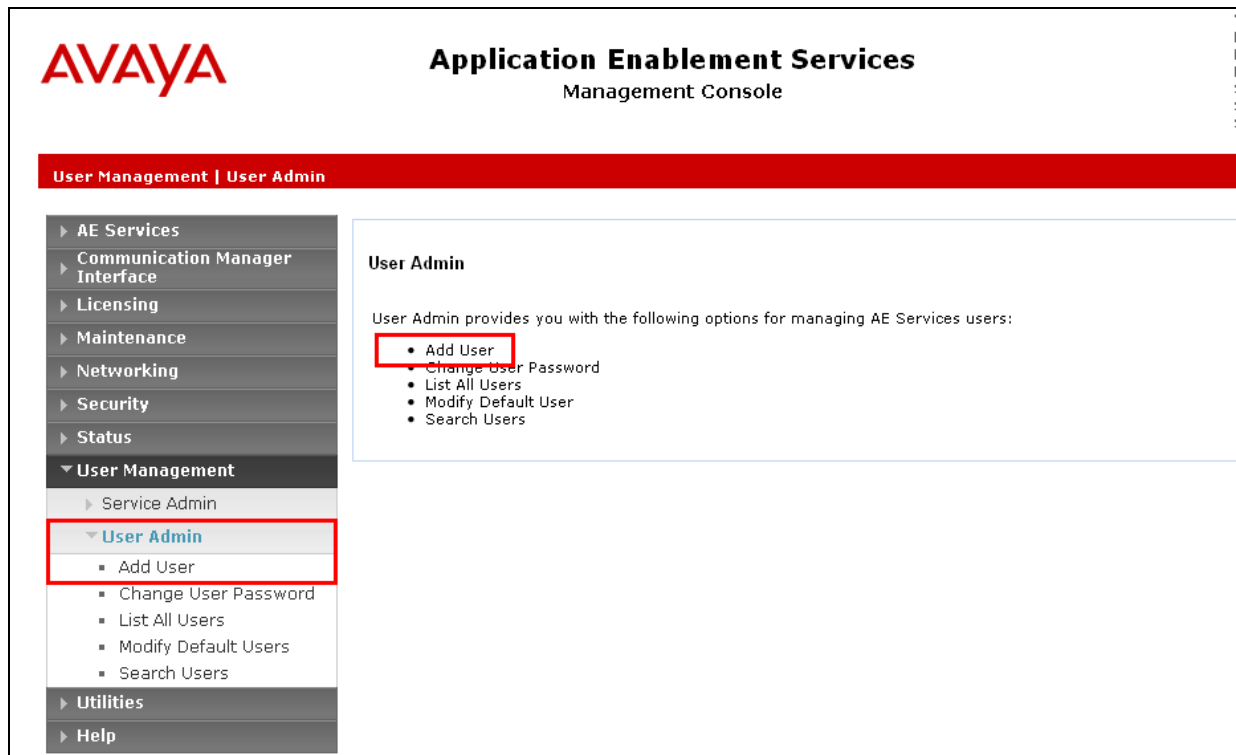
		Enabled	Disabled
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports			
TCP Port Min	1024		
TCP Port Max	1039		
Unencrypted TLINK Ports			
TCP Port Min	<input type="text" value="1050"/>		
TCP Port Max	<input type="text" value="1065"/>		
Encrypted TLINK Ports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

DMCC Server Ports

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

6.5. Create CTI User

A User ID and password needs to be configured for the NICE Engage Platform to communicate 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 NICE Engage Platform setup in **Section 9.1**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with NICE Engage Platform setup in **Section 9.1**.
- **CT User** - Select **Yes** from the drop-down menu.

AVAYA **Application Enablement Services**
Management Console

User Management | User Admin | Add User

Add User

Fields marked with * can not be empty.

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

Scroll down and click on **Apply Changes**.

User Admin	CM License	<input type="text"/>
▪ Add User	CM Home	<input type="text"/>
▪ Change User Password	Css Home	<input type="text"/>
▪ List All Users	CT User	<input type="text" value="Yes"/>
▪ Modify Default Users	Department Number	<input type="text"/>
▪ Search Users	Display Name	<input type="text"/>
► Utilities	Employee Number	<input type="text"/>
► Help	Employee Type	<input type="text"/>
	Enterprise Handle	<input type="text"/>
	Given Name	<input type="text"/>
	Home Phone	<input type="text"/>
	Home Postal Address	<input type="text"/>
	Initials	<input type="text"/>
	Labeled URI	<input type="text"/>
	Mail	<input type="text"/>
	MM Home	<input type="text"/>
	Mobile	<input type="text"/>
	Organization	<input type="text"/>
	Pager	<input type="text"/>
	Preferred Language	<input type="text" value="English"/>
	Room Number	<input type="text"/>
	Telephone Number	<input type="text"/>
	<input type="button" value="Apply Changes"/>	<input type="button" value="Cancel Changes"/>

6.6. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.5** and click on **Edit**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and Search Users. The 'Security Database' category is expanded, showing 'CTI Users' and 'List All Users' (highlighted with a red box). The main content area displays a table of CTI Users with columns: User ID, Common Name, Worktop Name, and Device ID. The table lists several users, with 'nice' selected (radio button) and highlighted with a red box. Below the table are 'Edit' and 'List All' buttons. The top right corner shows system information: Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50, Number of prior failed login attempts: 0, HostName/IP: AES63VMPG/10.10.40.30, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 6.3.3.1.10-0, Server Date and Time: Mon Dec 01 16:05:02 GMT 2014, HA Status: Not Configured. The top navigation bar includes 'Security | Security Database | CTI Users | List All Users' and 'Home | Help | Logout'.

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> asc	asc	NONE	NONE
<input type="radio"/> cube	cube	NONE	NONE
<input type="radio"/> emc	emc	NONE	NONE
<input type="radio"/> jacada	jacada	NONE	NONE
<input checked="" type="radio"/> nice	nice	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

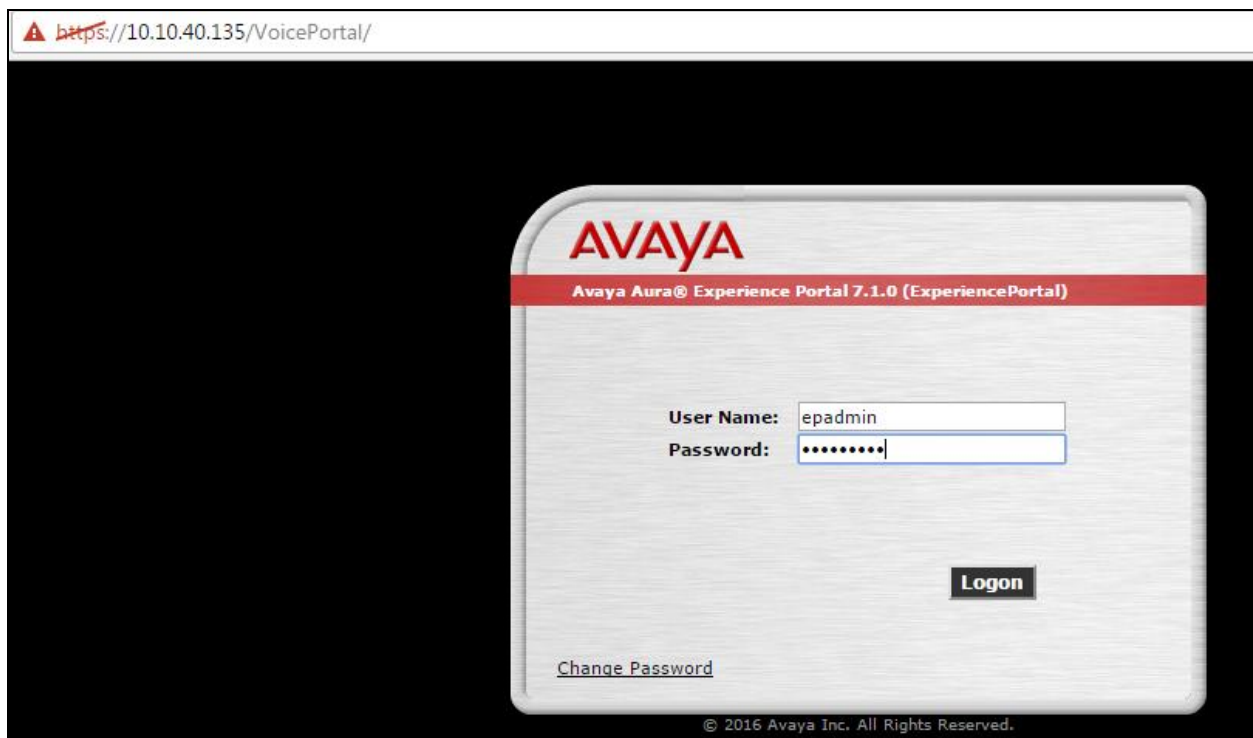
The screenshot shows the 'Edit CTI User' page for the 'nice' user. The left sidebar is the same as the previous screenshot, with 'List All Users' highlighted. The main content area displays the 'Edit CTI User' form. The 'User Profile' section includes fields for User ID, Common Name, Worktop Name, and 'Unrestricted Access' (checked). The 'Call and Device Control' section includes 'Call Origination/Termination and Device Status' (None). The 'Call and Device Monitoring' section includes 'Device Monitoring' (None), 'Calls On A Device Monitoring' (None), and 'Call Monitoring' (checkbox). The 'Routing Control' section includes 'Allow Routing on Listed Devices' (None). At the bottom are 'Apply Changes' and 'Cancel Changes' buttons. The top right corner shows system information: Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50, Number of prior failed login attempts: 0, HostName/IP: AES63VMPG/10.10.40.30, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 6.3.3.1.10-0, Server Date and Time: Mon Dec 01 16:05:37 GMT 2014, HA Status: Not Configured. The top navigation bar includes 'Security | Security Database | CTI Users | List All Users' and 'Home | Help | Logout'.

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

7. Configure Avaya Experience Portal and Avaya Proactive Outreach Manager

Avaya Proactive Outreach Manager is installed on top of an existing Avaya Experience Portal installation. It is assumed that both Experience Portal and Proactive Outreach Manager (POM) are fully installed and configured. This section will go through the changes that are necessary to connect to the POM to Contact Center and to configure both Experience Portal and POM in order to interoperate correctly with NICE.

Open a web browser and navigate to **https://<IPAddressofEP>/VoicePortal/** as shown below, enter the appropriate credentials and click on Logon.



The screenshot shows a web browser window with the address bar displaying <https://10.10.40.135/VoicePortal/>. The main content area features a login interface for the Avaya Aura Experience Portal 7.1.0. The interface includes the Avaya logo at the top, followed by the text "Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal)". Below this, there are two input fields: "User Name:" with the value "epadmin" and "Password:" with a masked password represented by dots. A "Logon" button is positioned to the right of the password field. At the bottom left of the login area, there is a link labeled "Change Password". The footer of the page contains the copyright notice "© 2016 Avaya Inc. All Rights Reserved."

7.1. Configure Proactive Outreach Manager

Select **POM Home** from the bottom of the left window.

AVAYA Welcome, ep
Last logged in Dec 13, 2016 at 5:45:34

Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal) Home ? Help

Expand All | Collapse All

User Management
Roles
Users
Login Options

Real-time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
Application Server
EPM Manager
MPP Manager
Software Upgrade
System Backup

System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

Multi-Media Configuration
Email
HTML
SMS

POM
POM Home
POM Monitor

You are here: Home

Avaya Aura® Experience Portal Manager

Avaya Aura® Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

Installed Components

Media Processing Platform
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

Email Service
Email Service is an Experience Portal feature which provides e-mail capabilities.

HTML Service
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes support for browser based services for mobile devices.

Proactive Outreach Manager
Avaya Proactive Outreach Manager (POM) provides a solution for unified, multichannel, inbound and outbound architecture, with the capability to communicate through different channels of interaction, from Short Message Service (SMS) to e-mail to the traditional voice and video.

SMS Service
SMS Service is an Experience Portal feature which provides SMS capabilities.

Legal Notice

© 2016 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya

Select **Global Configurations** as shown below.

AVAYA Welcome
Last logged in Dec 13, 2016 at 5:45:34

Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal) Home ? Help

Expand All | Collapse All

User Management
Roles
Users
Login Options

Real-time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
Application Server
EPM Manager
MPP Manager
Software Upgrade
System Backup

System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

Multi-Media Configuration
Email
HTML
SMS

POM

Proactive Outreach Manager 3.0 POM Home Campaigns Contacts Configurations

Proactive Outreach Manager is an application for interactive outbound Voice, SMS and E-mail notifications. With Proactive Outreach Manager you can deploy Campaigns that deliver the right information and service over the right media from the right resource at the right time.

Configurations
POM Servers
POM Zone Configuration
POM Zone Licenses
Global Configurations
Purge Schedules
Phone Formats
AACC Configurations

Proactive Outreach Manager

Scroll down to the WFO section and ensure that **WFO** is ticked and the default port of **7999** is selected. The **Nailup call CLID** can be set at any figure but this should be the same as that configured in **Section 8.3**. Click **Apply** at the bottom of the screen.

WFO

Enable WFO☒

WFO port *

Agent settings

Maximum job waiting duration(min) *

Minimum job attachment period(min) *

Nailing retry interval(sec) *

Call queue ☐

Nailup call CLID *

Override PAI for External Consult Calls ☐

ANI for external consult calls ☒ Nailup call CLID ☐ Agent Extension

Miscellaneous

POM poller polling interval(sec) *

Agent script editor auto save time(min) *

Advanced settings

JMS listen port *

Pacer base port *

Router base port *

Agent manager base port *

Campaign batch size *

Maximum concurrent jobs *

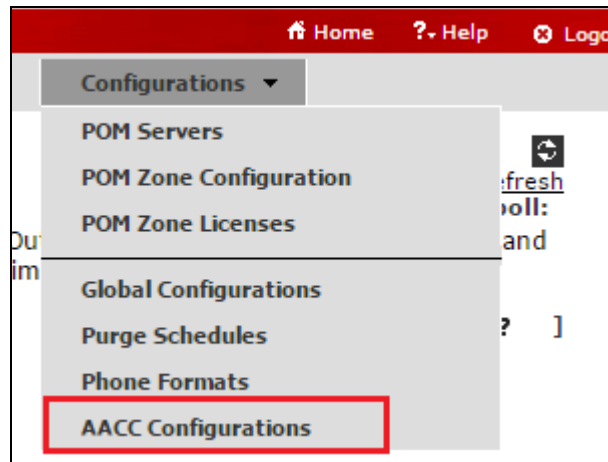
Maximum ports per server *

Apply

Cancel

Help

Select **AACC Configurations** from the **Configurations** menu.



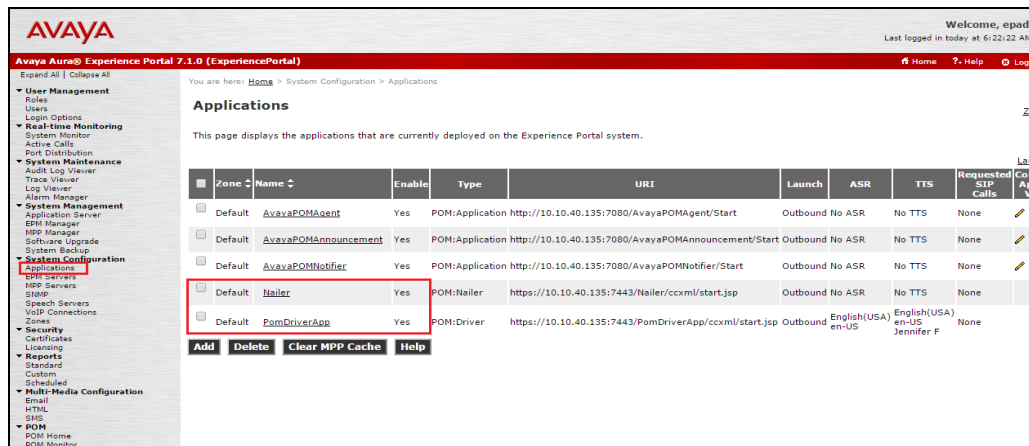
Enter the IP address of the Contact Center Server and the **web service user name** and **password**. Ensure that the **Multicast IP address** is the same as that from **Section 8.4**. Click on **Apply** once the information is filled in correctly.

A screenshot of the 'AACC Configuration' page within the Proactive Outreach Manager 3.0 interface. The page title is 'AACC Configuration' and it includes a subtitle: 'This page allows you to configure AACC Configuration parameters.' Below the subtitle, there is a form with six fields: 'AACC web service IP address' (value: 10.10.40.80), 'AACC web service user name' (value: webadmin), 'AACC web service password' (value: masked with dots), 'AACC Multicast IP address' (value: 234.5.6.84), 'AACC Hostname' (value: AACC70vmpg), and 'AACC Secure Connection' (checkbox, currently unchecked). At the bottom of the form, there are two buttons: 'Apply' and 'Help'.

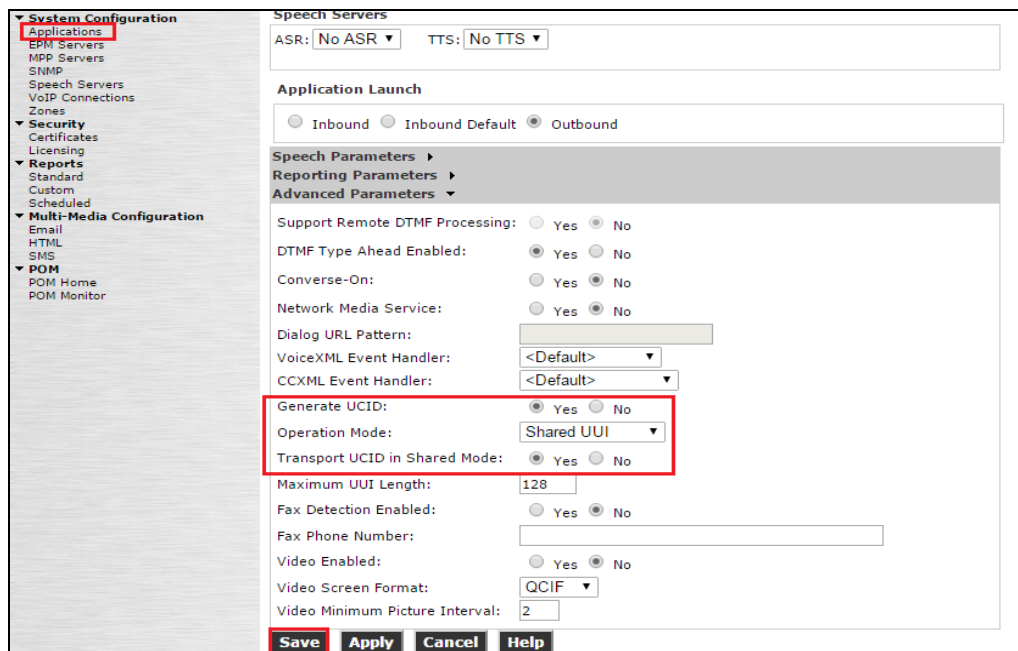
7.2. Configure POM Applications for UCID

Universal Call ID (UCID) is a base feature. UCID assigns a unique number to a call when it enters that call center network. The single UCID can be passed among platforms, and can be used to compile call-related information across platforms and sites. Also available is the user-to-user information (UII) element, which supports the specification of additional information to be passed in external function arguments.

Both the **Nailer** and **PomDriverApp** applications must be configured to pass on the UCID to NICE.



Open the **Nailer** application by clicking on the application. Ensure that **Generate UCID** and **Transport UCID in Shared Mode** are set to **Yes**. **Operation Mode** should be set to **Shared UII**. Click on **Save**.

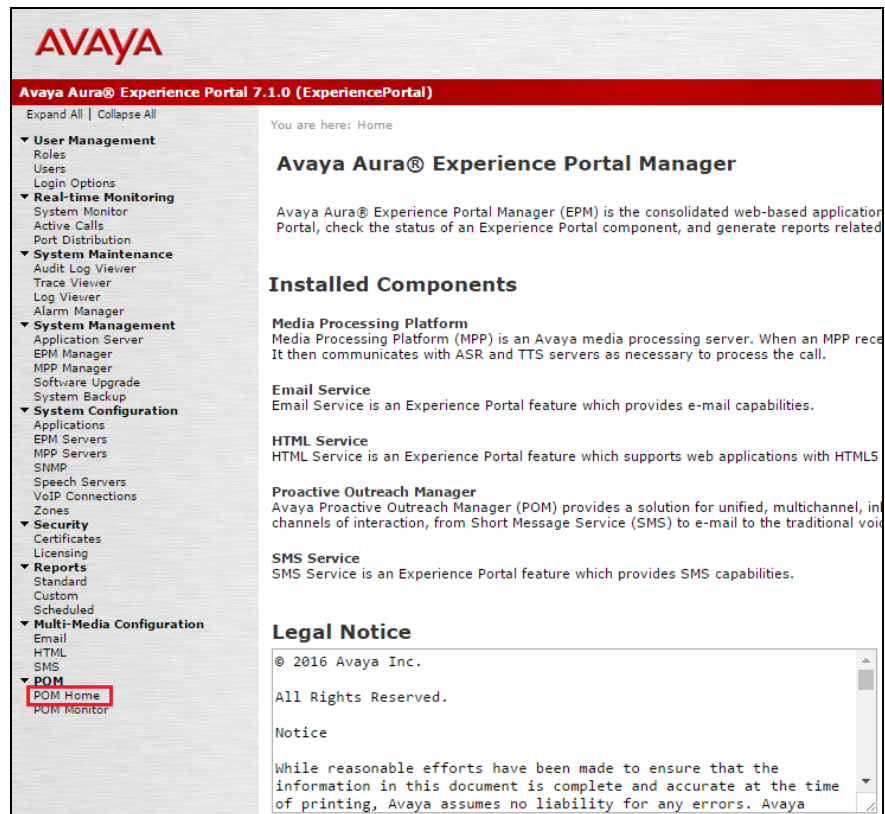


The exact same must be done for the PomDriverApp. Click on this application and scroll down and ensure that **Generate UCID** and **Transport UCID in Shared Mode** are set to **Yes**. **Operation Mode** should be set to **Shared UII**. Click on **Save**.

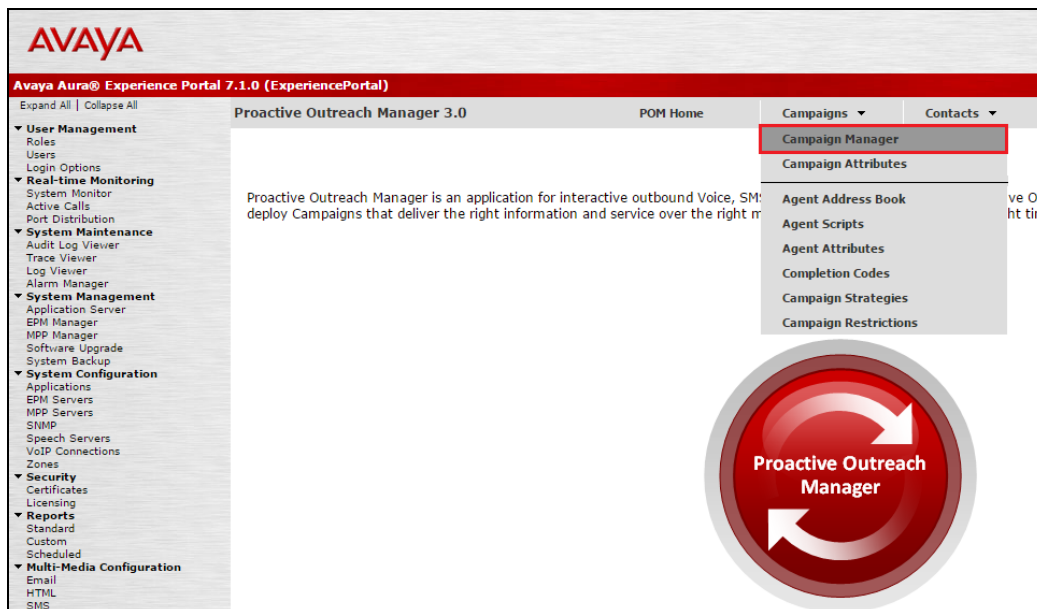
The screenshot shows the 'System Configuration' web interface. On the left is a navigation tree with categories: System Configuration, Security, Reports, and Multi-Media Configuration. Under 'System Configuration', the 'Applications' item is highlighted with a red box. The main content area shows the configuration for the selected application. At the top, there are dropdowns for 'Languages' (English(USA) en-US) and 'Voices' (English(USA) en-US Jennifer F). Below this is the 'Application Launch' section with radio buttons for 'Inbound', 'Inbound Default', and 'Outbound' (selected). The 'Speech Parameters' section is expanded, showing 'Reporting Parameters' and 'Advanced Parameters'. In the 'Advanced Parameters' section, three settings are highlighted with a red box: 'Generate UCID' (radio buttons for Yes and No, with 'Yes' selected), 'Operation Mode' (dropdown menu showing 'Shared UII'), and 'Transport UCID in Shared Mode' (radio buttons for Yes and No, with 'Yes' selected). Other settings include 'Support Remote DTMF Processing' (Yes/No), 'DTMF Type Ahead Enabled' (Yes/No), 'Converse-On' (Yes/No), 'Network Media Service' (Yes/No), 'Dialog URL Pattern' (text field), 'VoiceXML Event Handler' (dropdown), 'CCXML Event Handler' (dropdown), 'Maximum UII Length' (text field with value 128), 'Fax Detection Enabled' (Yes/No), 'Fax Phone Number' (text field), 'Video Enabled' (Yes/No), 'Video Screen Format' (dropdown with value QCIF), and 'Video Minimum Picture Interval' (text field with value 2). At the bottom are buttons for 'Save', 'Apply', 'Cancel', and 'Help', with 'Save' highlighted in red.

7.3. Generate an Outbound Campaign

Click on **POM Home** at the bottom of the left window.



Open Campaign Manager.



From the main window, click on **Add**, as shown below, to add a new campaign.

Campaign Manager  [Refresh](#)
Last poll: 12/15/2016 03:44:22 AM

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

  [Advanced](#)

Show | Page: 1/1     

Name	Type	Campaign Strategy	Contact Lists	Last Executed	Actions
------	------	-------------------	---------------	---------------	---------

* In Progress means Campaign job can be in any one of the states - running, pausing, paused, callback, stopping.

Add **Help**

Enter a suitable **Name** for the **New Campaign** and click on **Continue**.

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

Continue **Cancel** **Help**

A new **Campaign Strategy** must be added, click on the “new” icon, highlighted below.

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 creation process. To change optional parameters, click the "Next" button.

Name and Description

NICE_Outbound_Preview

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 current list.

Select   

Campaign type



☒ Finite ☐ Infinite

☐ Do not associate any Contact List at start

Contact List

From the following list select one or more Contact Lists to be used with this Campaign. Click on the icons next to the list to create a new Contact List or refresh the current list.

Default(Default)

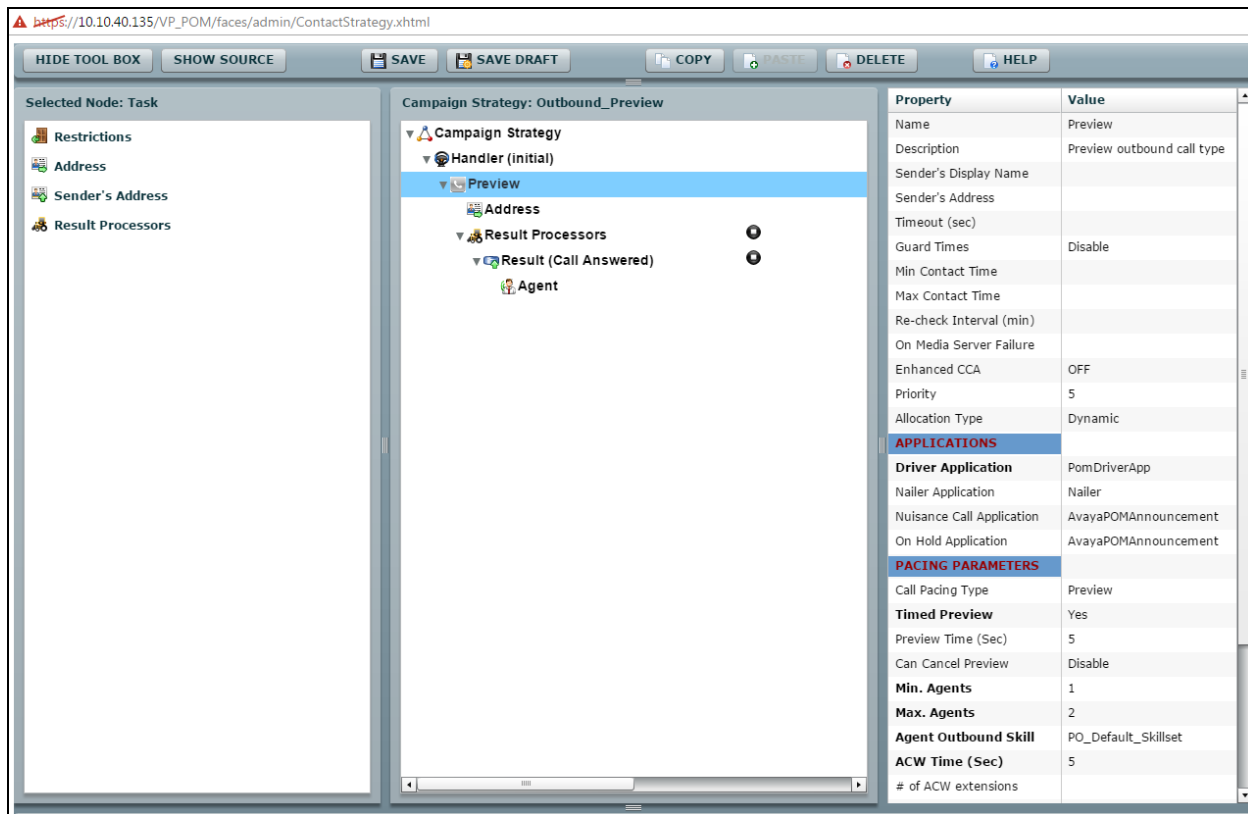
Cancel

Next

Finish

Help

The new strategy is created for the outbound campaign using the drag and drop window as shown below. Click on **Save** once the campaign is complete. For more information on campaigns and creating campaigns please refer to the documentation listed in **Section 12** of these Application Notes.



A list of outbound telephone numbers or “contacts” needs to be added. These are a list in a .csv format and look something like the following.

POMListMixSIP323 - Microsoft Excel						
File Home Insert Page Layout Formulas Data Review View						
Clipboard Font Alignment						
A1 fx ID						
	A	B	C	D	E	F
1	ID	firstname	lastname	phonenumber2	phonenumber1	email
2	1	Rory	McIlroy	92016	92016	wilson1971@avaya.com
3	2	Tiger	Woods	85151	85151	wilson1971@avaya.com
4	3	Jack	Nicklaus	92016	92016	wilson1971@avaya.com
5	4	Gary	Player	85151	85151	wilson1971@avaya.com
6	5	Seve	Ballesteros	92016	92016	wilson1971@avaya.com
7	6	Sam	Snead	85151	85151	wilson1971@avaya.com
8	7	Arnold	Palmer	92016	92016	wilson1971@avaya.com
9	8	Bernhard	Langer	85151	85151	wilson1971@avaya.com
10	9	John	Smith	92016	92016	wilson1971@avaya.com
11	10	Han	Solo	85151	85151	wilson1971@avaya.com
12	11	Luke	Skywalker	92016	92016	wilson1971@avaya.com

Click on the 'new' icon as shown below to add a new contact list.

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 creation process. To change optional parameters, click the "Next" button.

Name and Description

NICE_Outbound_Preview

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 current list.

Outbound_Preview ▾   



Campaign type

☒ Finite ☐ Infinite

☐ Do not associate any Contact List at start


Contact List

From the following list select one or more Contact Lists to be used with this Campaign. Click on the icons next to the list to create a new Contact List or refresh the current list.

Default(Default)  

Cancel Next Finish Help

Enter a suitable **Name** for the outbound list and click on **Save**.

Add New Contact List 

Add New Contact List

This page allows you to add new Contact List.

Name

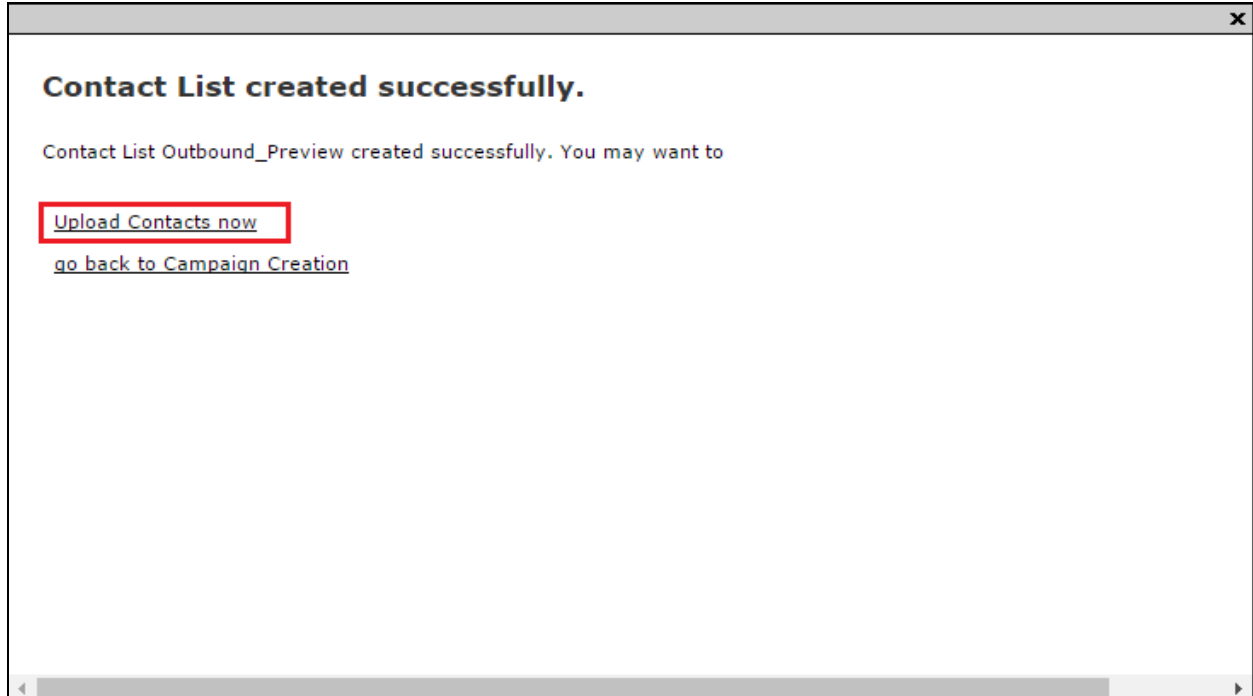
Description

Outbound list

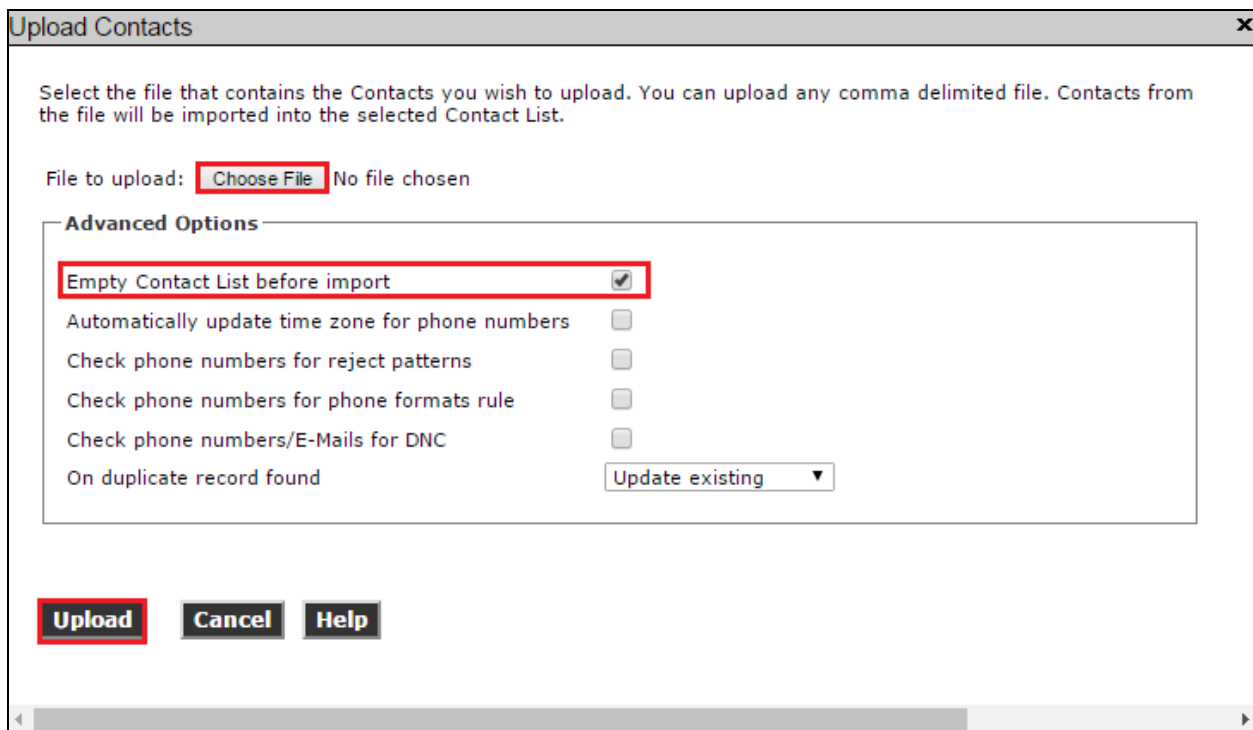
Zone Name

Save Cancel Help

Click on **Upload Contact now**.



The .csv file is then located by clicking on **Choose File**. Ensure that **Empty Contact List before import** is ticked so as the outbound campaign starts from new. Click on **Upload** once this is ready.



Click on **Finish** to complete the campaign with the new **Campaign Strategy** and **Contact List** in place.

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 creation process. To change optional parameters, click the "Next" button.

Name and Description

NICE_Outbound_Preview

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 current list.

Outbound_Preview

Campaign type

☒ Finite ☐ Infinite

☐ Do not associate any Contact List at start

Contact List

From the following list select one or more Contact Lists to be used with this Campaign. Click on the icons next to the list to create a new Contact List or refresh the current list.

Default(Default)
Outbound_Contact_List(Default)

CancelNextFinishHelp

The new campaign can then be started by pressing on the 'play' icon as shown below.

Campaign Manager

Refresh

Last poll: 12/15/2016 03:53:40 AM

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

Show 50 | Page: 1/1

Name	Type	Campaign Strategy	Contact Lists	Last Executed	Actions
NICEout	Finite	OutboundVoice	SIPandQSIG	In Progress	
NICE Outbound Preview	Finite	Outbound_Preview	SIPandQSIG	12/12/2016 06:43:09 AM	

* In Progress means Campaign job can be in any one of the states - running, pausing, paused, callback, stopping.

AddHelp

7.4. Create a POM User for NICE

A user must be created to allow NICE access to web services for call events. This user will be configured during the NICE setup in **Section 9.1**. Click on **Users** in the left window and **Add** in the main window.

AVAYA
Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal)

Expand All | Collapse All

You are here: [Home](#) > User Management > Users

Users

This page displays the list of EPM user accounts. Depending on your user role, you can add, modify, and delete user accounts. You can also configure logins. Configure the parameters under LDAP Settings to enable the EPM to access user accounts in your corporate directory.

Same user (report) has been specified for the Application Reporting web service authentication.

<input type="checkbox"/>	Name	Enable	Type	Assigned Roles/Features	Last Login	Failed Attempts	Locked	Password Longevity (days)
<input type="checkbox"/>	epadmin	Yes	EP (Password)	Administration, Auditor, POM Campaign Manager, POM Administration, User Manager, Web Services	Dec 15, 2016 7:38:12 AM PST			60 (System)
<input type="checkbox"/>	report	Yes	EP (Password)	Reporting	Never			60 (System)
<input type="checkbox"/>	weboutuser	Yes	EP (Password)	Administration, POM Campaign Manager, POM Administration, Web Services	Never			Not enforced

Add **Delete** **Help**

Ensure that **Web Services** is ticked, enter a suitable **Name** and **Password** and click on **Save**.

Change User

Use this page to modify a EPM user account. You can change the user role and password.

Name: nice

Enable: ☒ Yes ☐ No

Roles:

- ☐ Administration
- ☐ Auditor
- ☒ POM Campaign Manager
- ☐ Maintenance
- ☐ Operations
- ☐ POM Administration
- ☐ Privacy Manager
- ☐ Reporting
- ☐ User Manager
- ☒ Web Services

Created: 12/8/16 7:16 AM

Password:

Verify Password:

Enforce Password Longevity: ☐

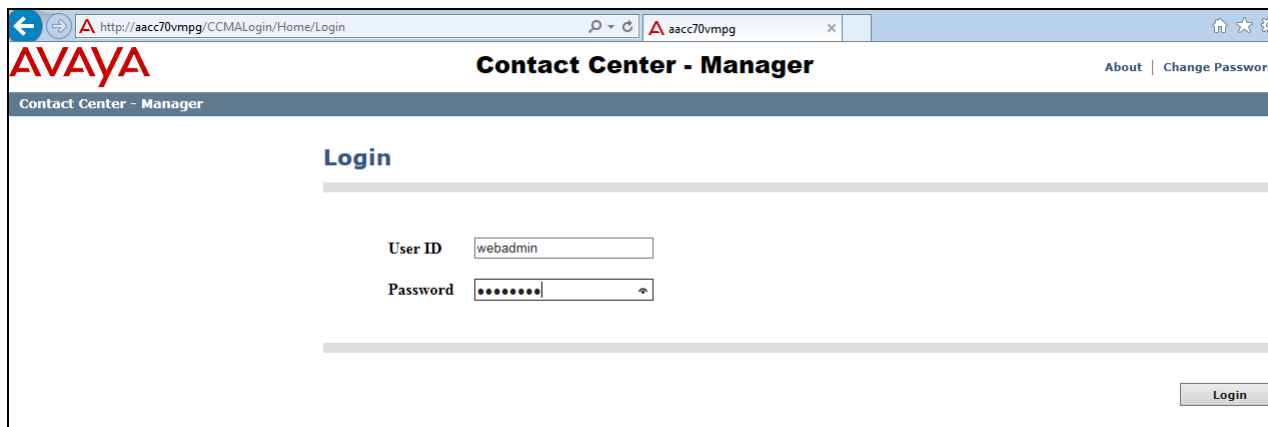
Save **Apply** **Cancel** **Help**

8. Configure Avaya Aura® Contact Center

It is assumed that Contact Center is fully installed and configured. This section will go through the changes that are necessary to connect to the Contact Center to POM and to configure the Contact Center agents and Avaya Aura® Agent Desktop (AAD) in order to interoperate correctly with POM in order to facilitate outbound calls from POM.

Note: Although the configuration steps outlined here are not directly related to the NICE connection with the Avaya solution it is useful to know and it may help with the support of any issues found.

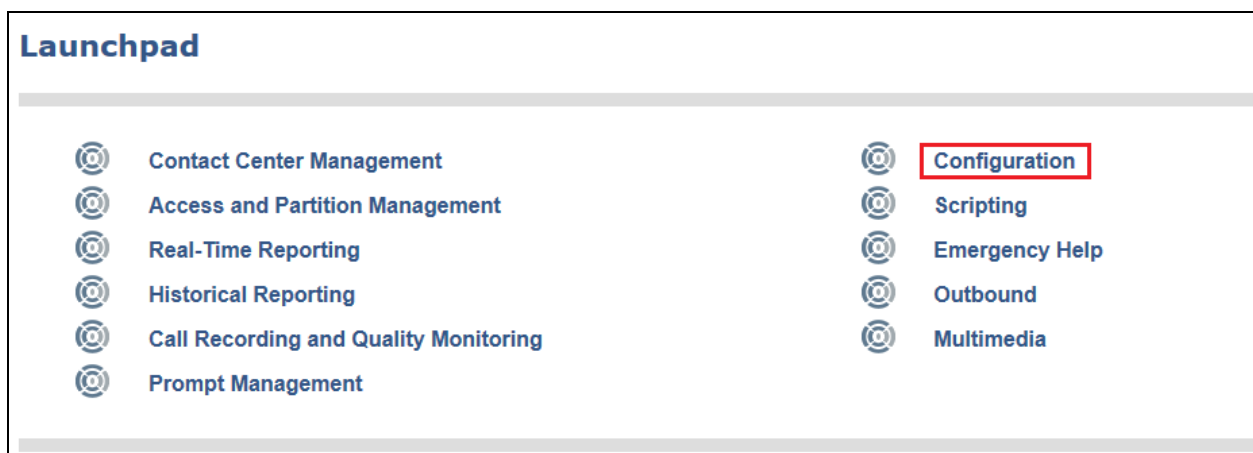
Open a web browser to the Contact Center as shown below, enter the appropriate credentials and click on **Login**.



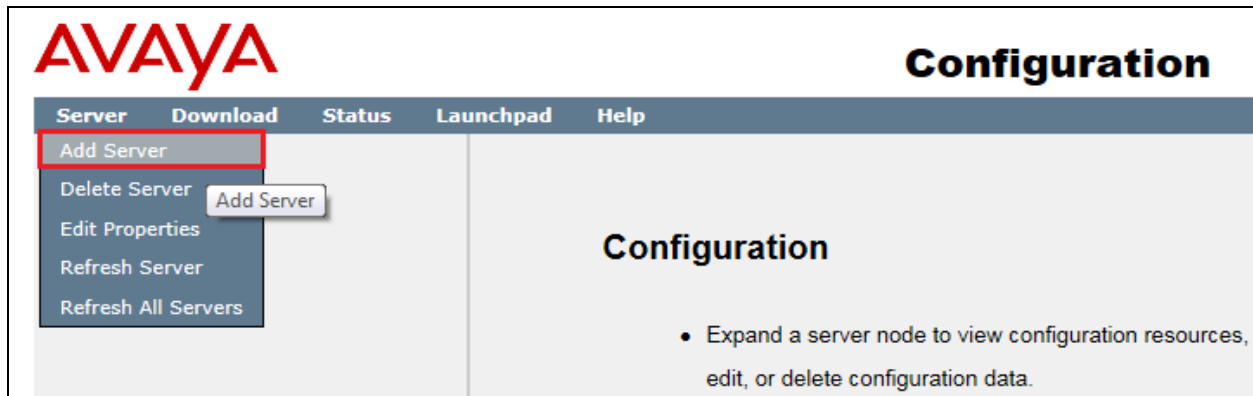
The screenshot shows a web browser window with the URL <http://aacc70vmvg/CCMLogin/Home/Login>. The page title is "Contact Center - Manager". The Avaya logo is in the top left. The main heading is "Login". Below it, there are two input fields: "User ID" with the value "webadmin" and "Password" with masked characters. A "Login" button is at the bottom right.

8.1. Configure POM Server on Contact Center

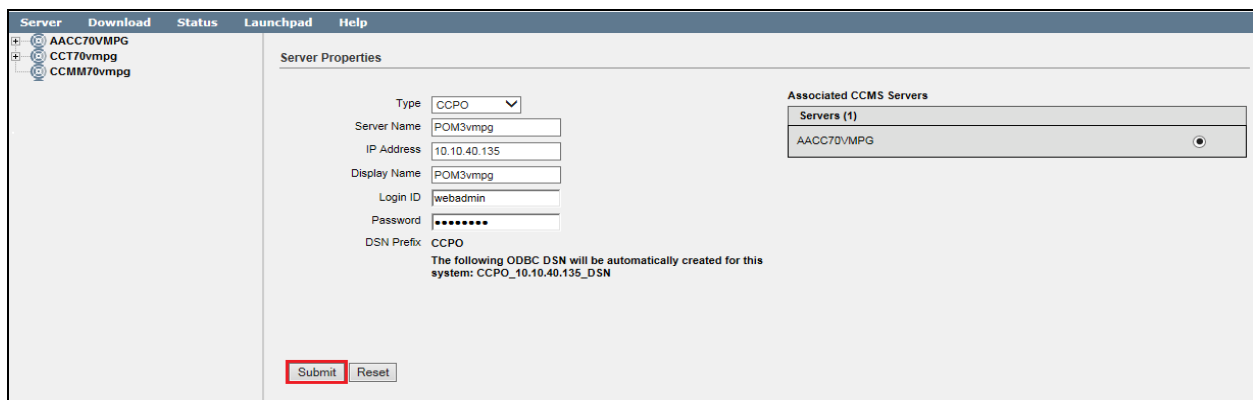
From the Launchpad, click on **Configuration**.



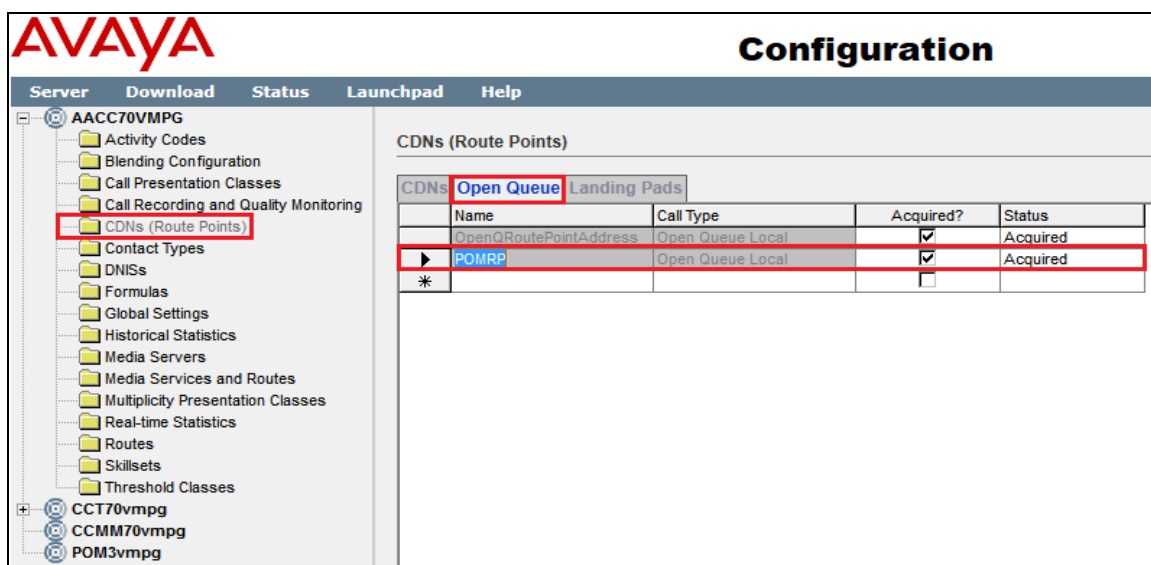
From the top left of the page, click on **Server** and **Add Server**.



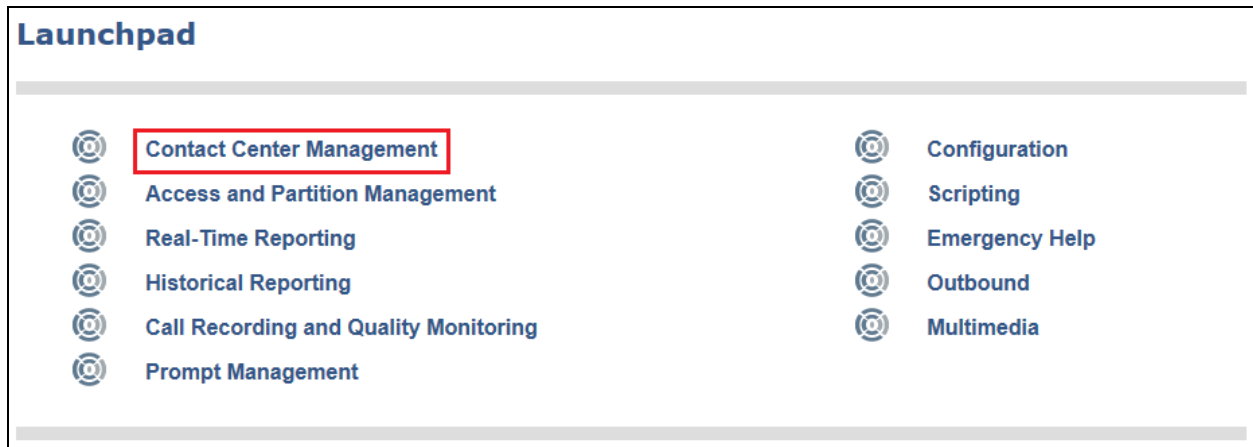
Fill in the details of the POM server, noting that the server Type is **CCPO**. Click on **Submit**.



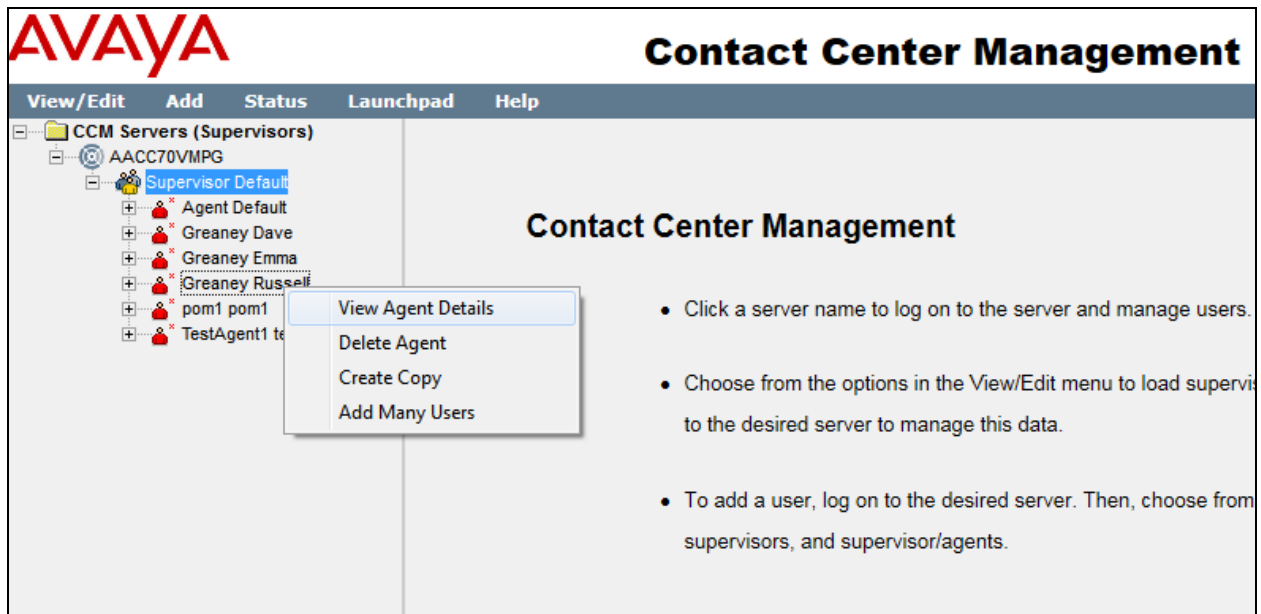
Within **Configuration** click on **CDNs** to add a new CDN for the Outbound campaign. This will later be associated with the POM Skillset in Multimedia.



Back at **Launchpad**, click on **Contact Center Management** in order to update the agents.



Select the agent to be updated and click on **View Agent Details**.



8.2. Configure Contact Center Agent for outbound calls

Add the **POM_Outbound** Contact Type, as shown below and assign a **Priority** to the **PO-Default_Skillset**. The default POM outbound skillset is now associated with this agent and when the agent logs into AAAD, they will also log into POM and should be available for an outbound campaign assuming one is running.

▼ [Agent Information](#)

Primary Supervisor: * Supervisor Default ▼

Call Presentation: CP1 ▼

Login Status

Logged Out

Multiplicity Presentation Class: MPC_Off ▼

Threshold: Agent_Template ▼

▼ [Contact Types](#)

▼ **Contact Type**

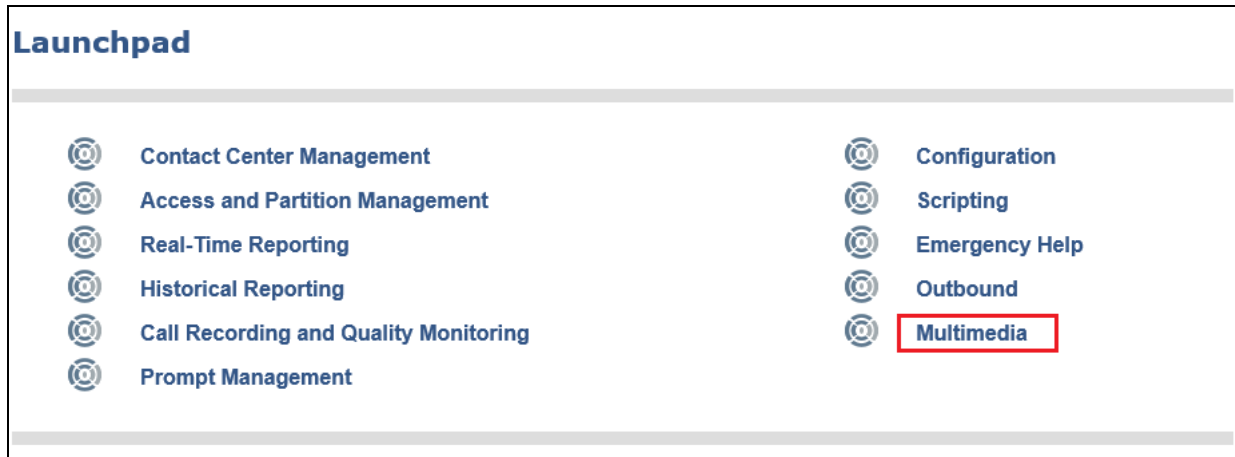
Outbound	<input type="checkbox"/>
POM_Outbound	<input checked="" type="checkbox"/>
Scanned_Document	<input type="checkbox"/>
SMS	<input type="checkbox"/>
Social_Networking	<input type="checkbox"/>
Video	<input type="checkbox"/>

▼ [Skillsets](#)

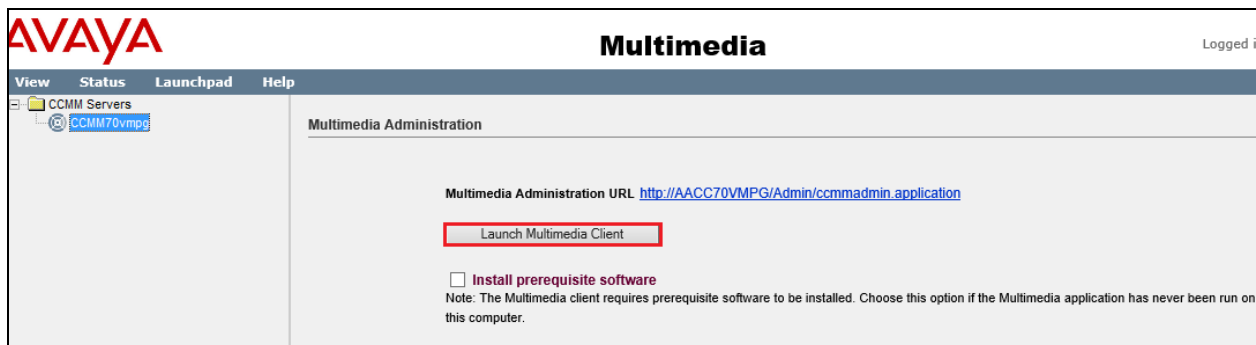
Skillset Name (7) ▼	Contact Type	Priority
Default_Skillset	Voice	Standby ▼
EM_Default_Skillset	EMail	10 ▼
OQ_Default_Skillset	OpenQ	10 ▼
PO_Default_Skillset	POM_Outbound	1 ▼
Sales	Voice	2 ▼
Support	Voice	3 ▼
WC_Default_Skillset	Web_Communications	10 ▼

8.3. Configure Multimedia for POM Integration

The following two sections are configured from the Contact Center server. Open the web browser on the server in order to make changes in multimedia. Once logged in click on **Multimedia**.



Click on **Launch Multimedia Client** as shown below.



Click on **POM** in the left window and enter the **POM voice path CLID**, this should have been set in **Section 7.1**. Click on **Save**.

AVAYA

CCMM Administration

Edit POM Settings

POM Settings

POM voice path CLID: 0000

Save Cancel Help

User: webadmin | Server Time: 12:56 | Status:

Click on **General Administration** in the left window and **Skillset Settings** as shown below. Enter the CDN created in **Section 8.1** opposite the **PO_Default_Skillset**. Click on **Save**.

AVAYA

CCMM Administration

Skillset Name Route Point Auto-Signature Office Hours Chat History Comfort Mes On Hold Mes Max Concurr

PO_Default_Skills	POMRP						
SN_Default_Skills							
VM_Default_Skills							
SM_Default_Skills							
FX_Default_Skills							
SD_Default_Skills							
PR_Default_Skills							
OB_Default_Skills							

Page 1 of 2

Edit Skillset

Skillset:

Auto-Signature:

Route Point:

Office Hours:

Chat History Header:

Comfort Group:

On Hold Group:

Web On Hold Group:

Max Concurrent Chats:

Save Cancel Help

User: webadmin | Server Time: 12:55 | Status:

Click on **Agent Desktop Configuration** in the left window and **User Settings**. Ensure that **Prompt User for Login Details** is ticked as shown below.

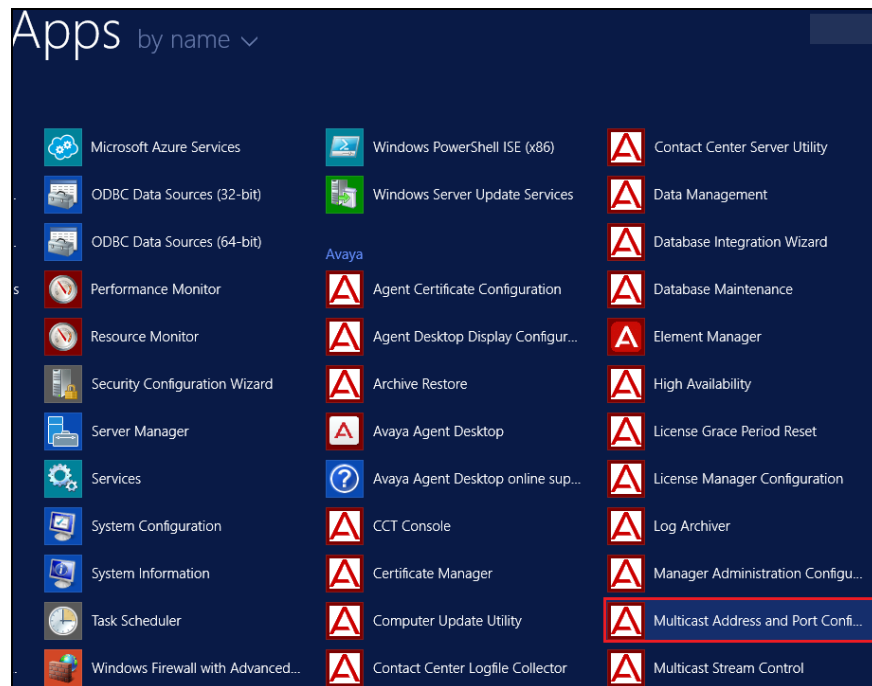
The screenshot displays the 'CCMM Administration' window. On the left, the 'Agent Desktop Configuration' menu is expanded, and 'User Settings' is selected. The main panel, titled 'User Settings', contains the following configuration options:

- Allow Erasing of Call History ☒
- Append Selected Auto Phrase to Existing Text ☒
- Allow Agent Desktop Panel Swap ☒
- Autostart Quality of Service Windows Service ☒
- Enable AAAD System Tray Icon ☒
- Enable AAAD Dashboard ☒
- Password Protect AAAD Dashboard ☒
- Prompt User for Login Details ☒**
- Disallow Duplicate Login ☐
- Enable AAAD Preference Retention ☒
- Enable Localization ☒
- Default Not Ready Reason Code when Rejecting a Contact: 000
- Default Not Ready Reason Code when Pulling a Contact: 0000
- Default Not Ready Reason Code After Max Open Duration: 000
- Home Page Enabled ☐
- Home Page URL: www.avaya.com
- Home Page Name: Avaya Start Page
- Close Multiple Contacts: Agent (dropdown)
- Maximum Number of Calls to Log: 30
- Maximum Number of Speed Dials: 10
- Maximum Number of Favourites: 10

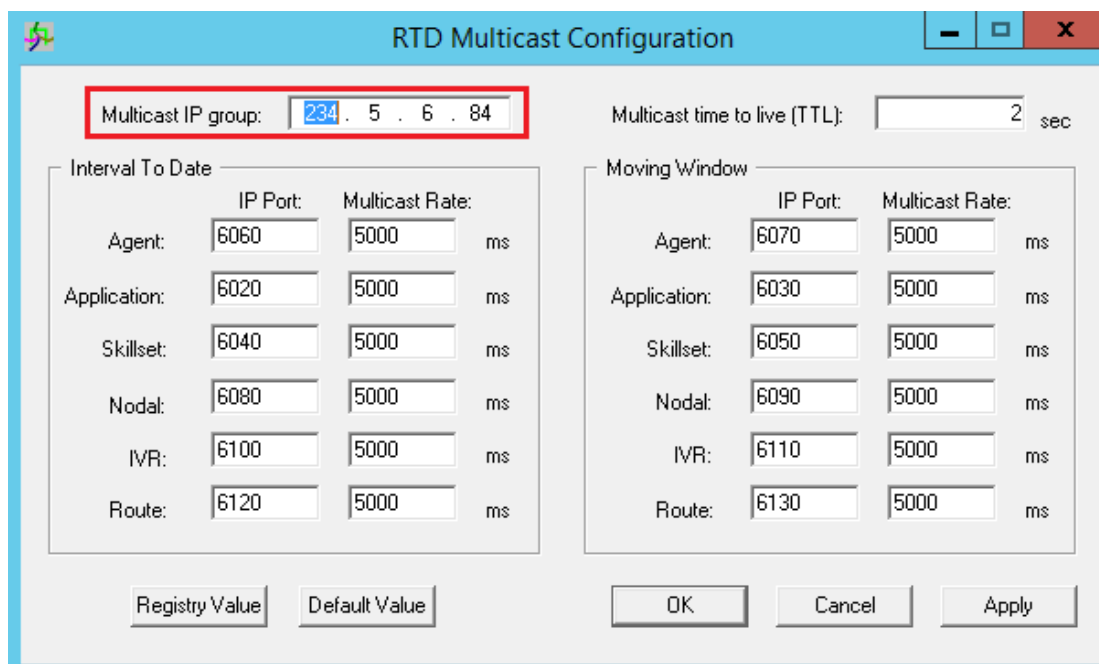
At the bottom right of the main panel are 'Save', 'Cancel', and 'Help' buttons. The status bar at the bottom indicates 'User: webadmin | Server Time: 12:57 | Status:'.

8.4. Configure Multicast IP Address for POM

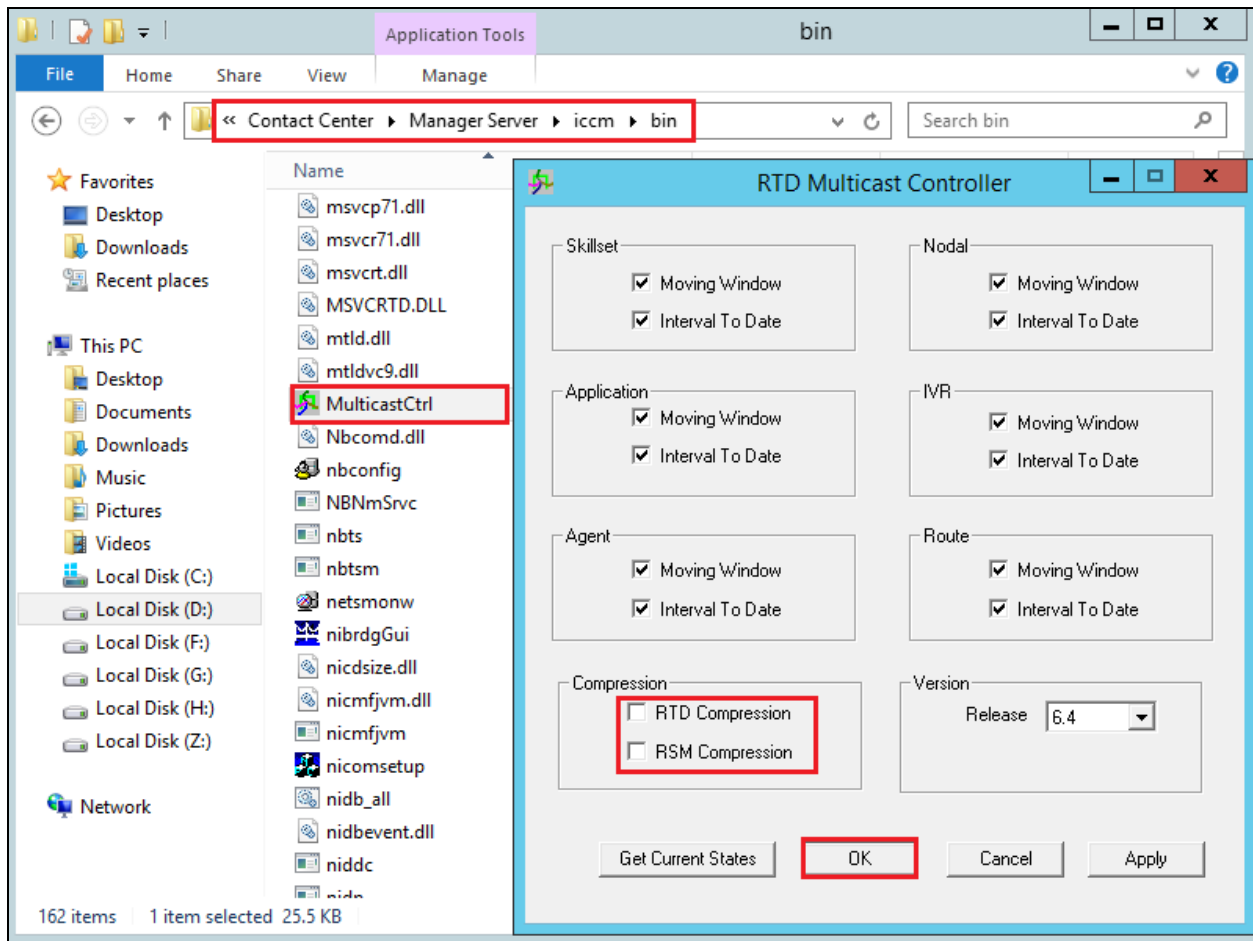
The Multicast address must be noted as this will be required in **Section 7.1** during the POM – AACC integration. Under **Apps** open **Multicast Address and Port Configuration**.



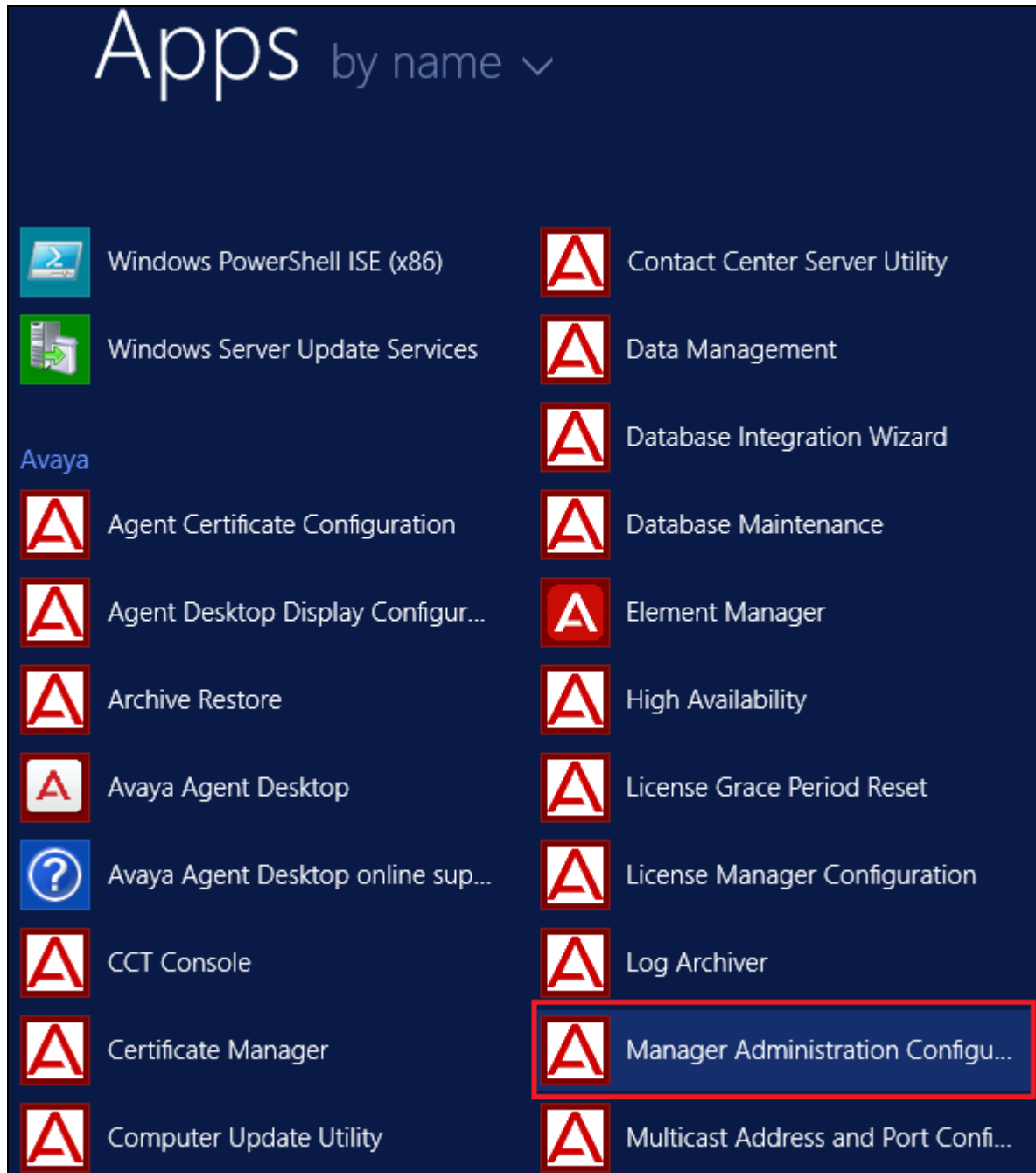
Take note of the Multicast IP address, noting here that it is **234.5.6.84**. This was set to this specific IP address during the Contact Center configuration and it is not the default address.



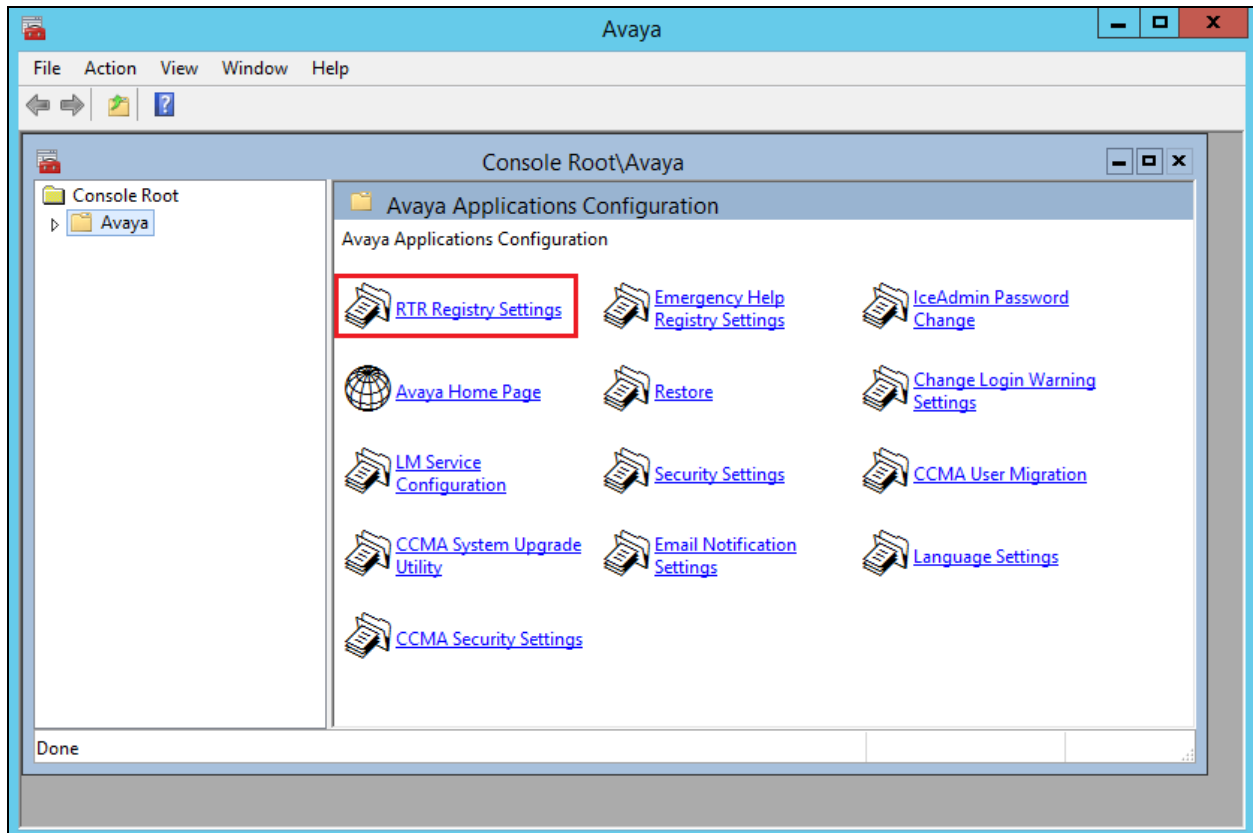
Navigate to **D:/Avaya/Contact Center/Manager Server/iccm/bin** and run the **MulticastCtrl** file as shown and ensure that both **Compression** values are not ticked.



Run the **Manager Administration Configuration** application as shown below.



Run the **RTR Registry Settings** program highlighted below.



Note that the **IP Receive Address** is set to the same IP Address as above and the **Compress Realtime Data Packets** is ticked off.

RTR Properties

RTR Settings

IP Receive Address: 234 . 5 . 6 . 84

IP Send Address: 234 . 5 . 6 . 2

Output Rate: 5000 milliseconds

Transform Rate: 1000 milliseconds

OAM Timeout: 120000 milliseconds

☐ Restart Real Time Reporting Service

Transmission Options

☐ Multicast

☐ Unicast

☒ Multicast and Unicast

Maximum Unicast Sessions: 100

WARNING: It is important to consult your engineering guidelines before modifying the number of unicast sessions or the output rate.

☐ Compress Realtime Data Packets

OK Cancel

From the Multimedia Client (see **Section 8.3** to log in), navigate to **General Administration** in the left window and then **General Settings** and ensure that the **Multicast IP** address is set correctly.

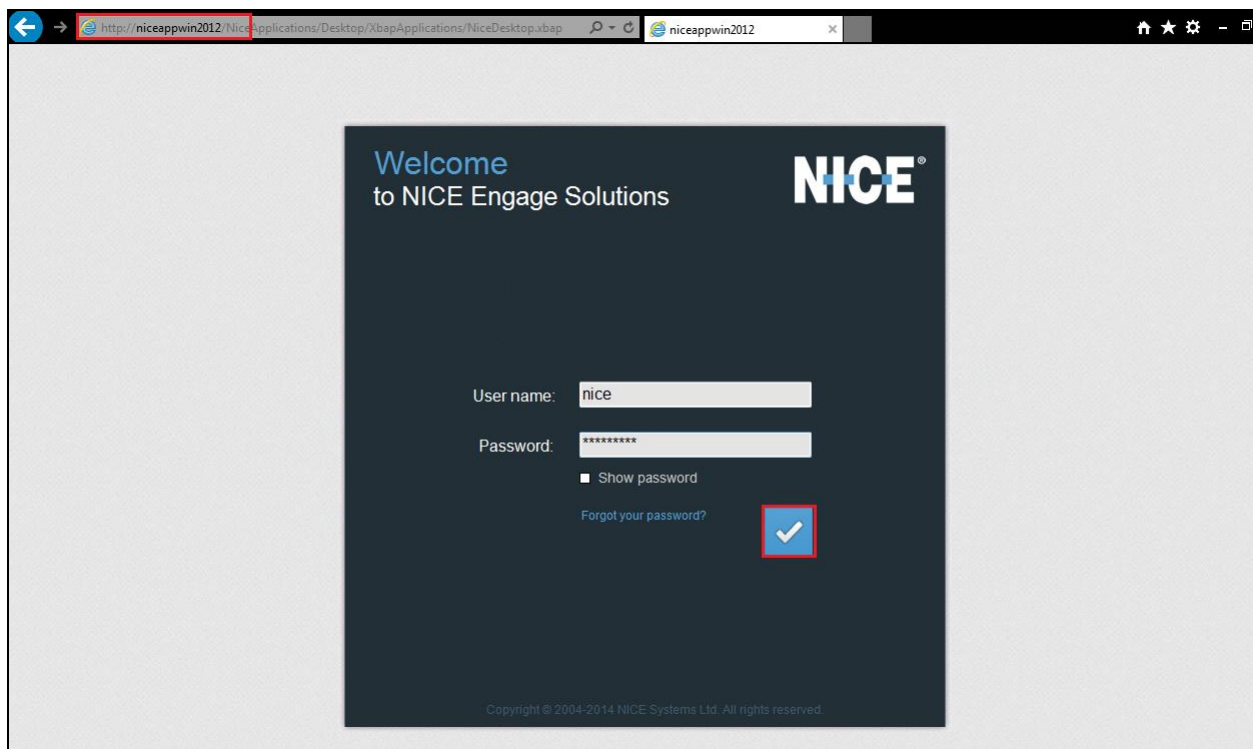
The screenshot displays the 'CCMM Administration' window with the 'Edit General Settings' tab active. The left sidebar shows the 'General Administration' menu, with 'General Settings' highlighted. The main content area is divided into three sections: 'System License' with a 'License Type' dropdown set to 'NODAL'; 'RTD Multicast Configuration' with a 'Multicast IP' field set to '234.5.6.84' and a 'Port' field set to '6050'; and 'Reporting Credentials' with a 'Reporting Account Password Reset' section containing 'Account ID' (mmReport), 'Set Password' (checkbox), 'New Password', and 'Confirm Password' fields. The 'Save' button is highlighted with a red box. The bottom status bar shows 'User: webadmin | Server Time: 10:33 | Status:'.

9. Configure NICE Engage Platform

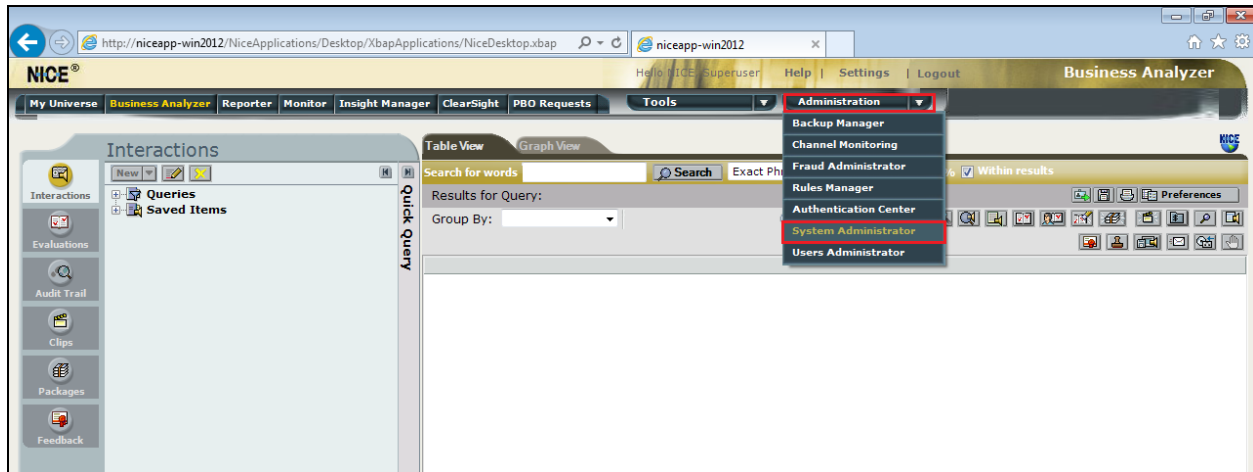
The installation of NICE Engage Platform is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of the NICE Engage Platform contact NICE as per the information provided in **Section 2.3**.

The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya Solution. All configuration of the NICE Engage Platform for connection with the AES is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser as shown navigate to

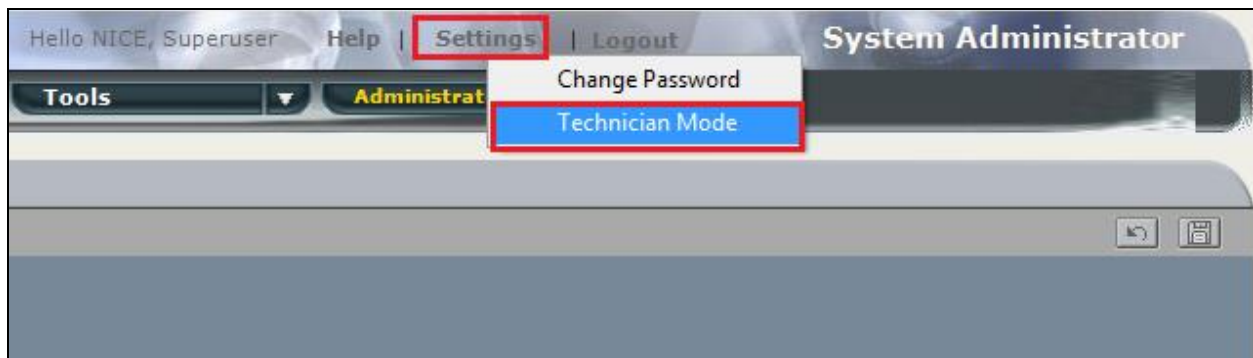
http://<NICEEngageApplicationServerIP>/Nice as shown below and enter the proper credentials and click on **Login**.



Once logged in expand the **Administration** dropdown menu and click on **System Administrator** as highlighted.

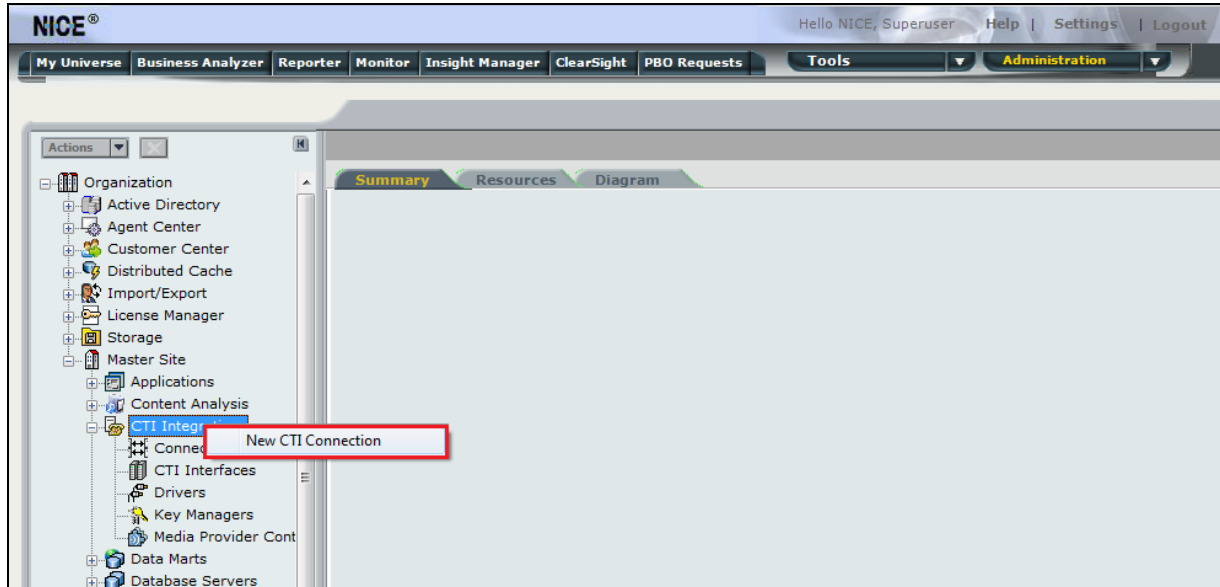


Before any changes can be made, switch to **Technician Mode** by clicking into Settings at the top of the screen as shown below.

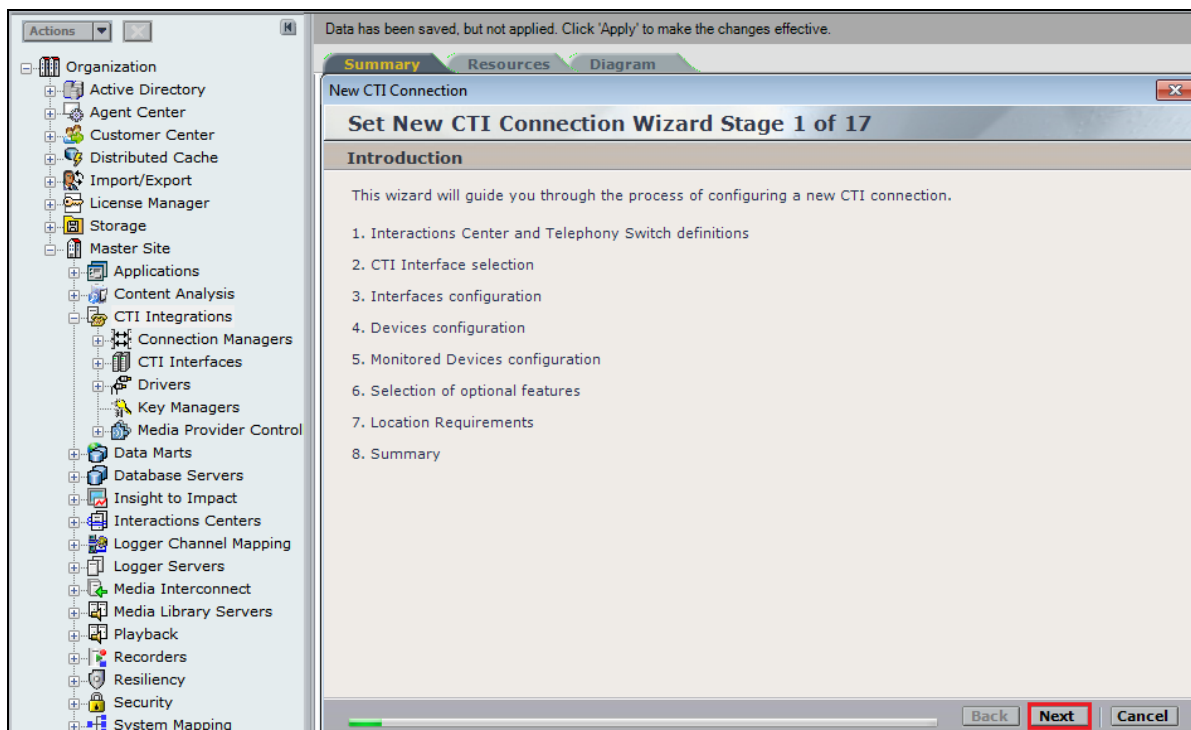


9.1. New CTI Connection

Navigate to **Master Site** → **CTI Integration** in the left window then right-click on CTI Integration and select **New CTI Connection** as shown below.



The **New CTI Connection Wizard** is opened and this will go through the 17 steps required to setup the connection to both the POM server for events and the AES for DMCC Multi-Registration type of call recording. Click on **Next** to continue.



The value for **Regular Interactions Center** is a value that was already created during the installation of the NICE Engage platform. This value is therefore pre-chosen for the CTI connection being created below.

The **Telephony Switch** must be selected and this will be **Avaya CM**. Enter a suitable name for this **Switch Name**. Click on **Next** to continue.

New CTI Connection
Set New CTI Connection Wizard Stage 2 of 17
Interactions Center Switch

Attach CTI to Interactions Center Server:

- ☒ Regular Interactions Center: NICE-AppSvr
- ☐ Interactions Center Cluster:
- ☐ Use existing Telephony Switch: Avaya POM
- ☒ Define new Telephony Switch:

Switch Type: Avaya CM

Switch Name: Avaya CM

Advanced >>

Back Next Cancel

Select **POM Server** for the **Avaya CM CTI Interface**, ensure that **Active Recording** is ticked and select the **DMCC (Advanced integration Recorder)** from the dropdown menu. Click on **Next** to continue.

New CTI Connection
Set New CTI Connection Wizard Stage 3 of 17
Interface Type

CTI Interface Type

Avaya CM CTI Interface: POM Server
Avaya Communication Manager
POM Server

☐ VoIP Mapping: AES SMS

☐ Additional VoIP Mapping: AES SMS

☒ Active Recording: DMCC (Advanced Interaction Recorder)
Avaya Communication Manager
Device Media and Call Control

Back Next Cancel

Each of the values for the POM Server must be filled in below. Double-click on each **Parameter** to enter a value for that parameter.

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 17

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
POM Server Address	
POM Server Username	
POM Server Password	
POM WFO Port ID	7999
POM WFO Port ID	FALSE

Description:

Additional Interface Parameters

Back Next Cancel

Enter the IP address for the POM server and click on **OK**.

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 17

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
POM Server Address	
POM Server Username	
POM Server Password	
POM WFO Port ID	7999
POM WFO Port ID	FALSE

Description: POM

Additional Interface Parameters

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

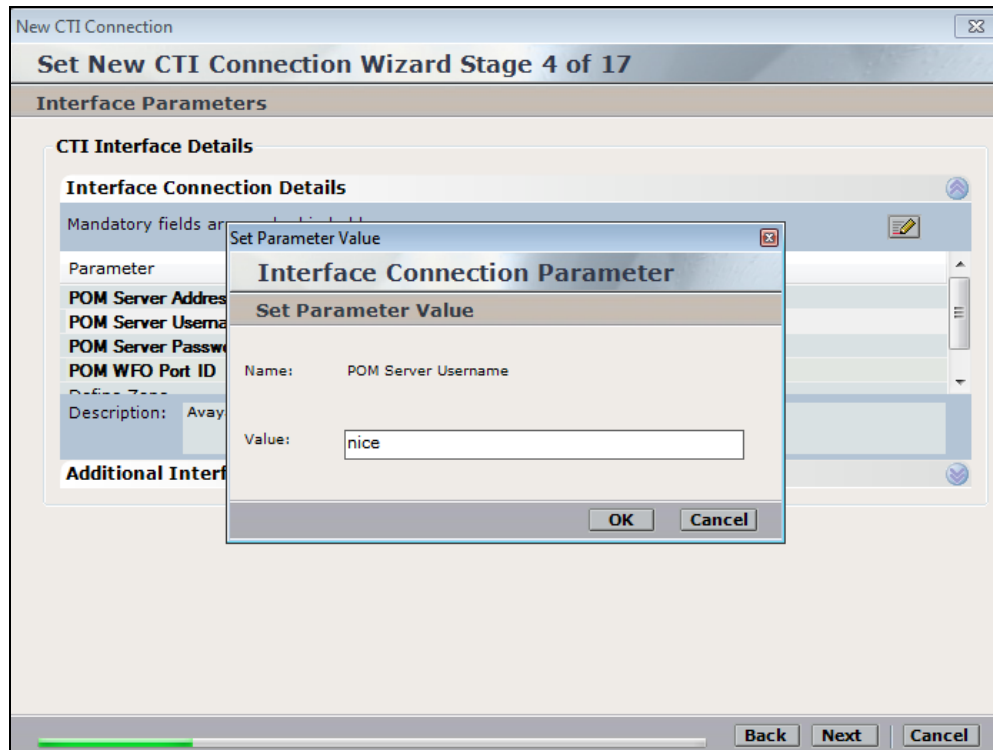
Name: POM Server Address

Value: 10.10.40.135

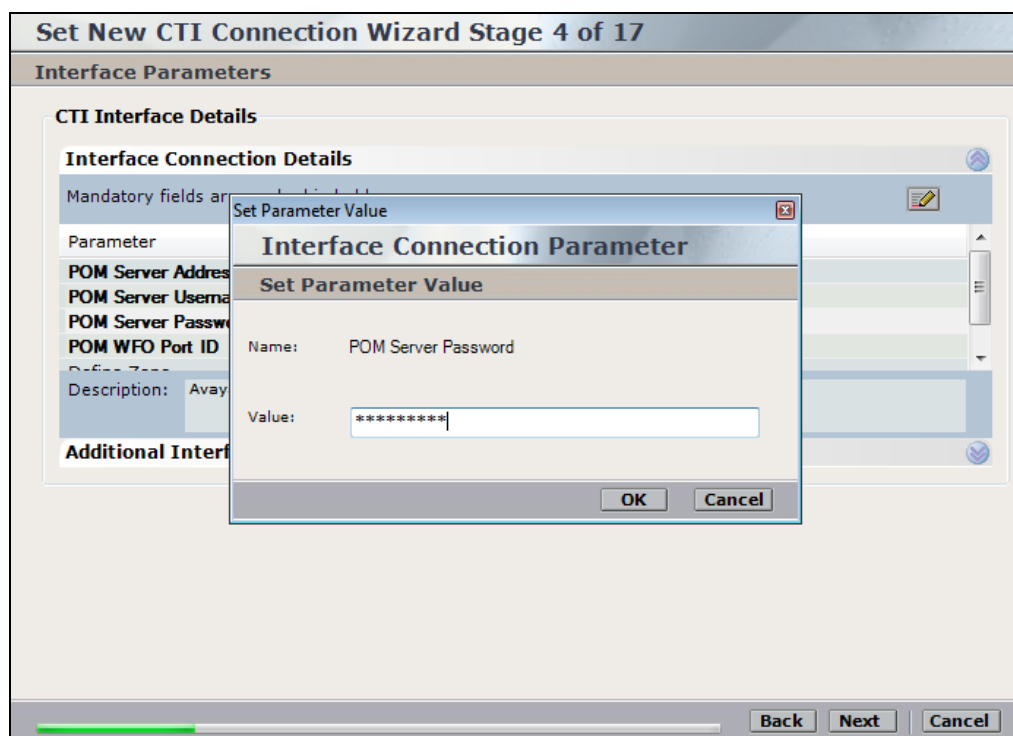
OK Cancel

Back Next Cancel

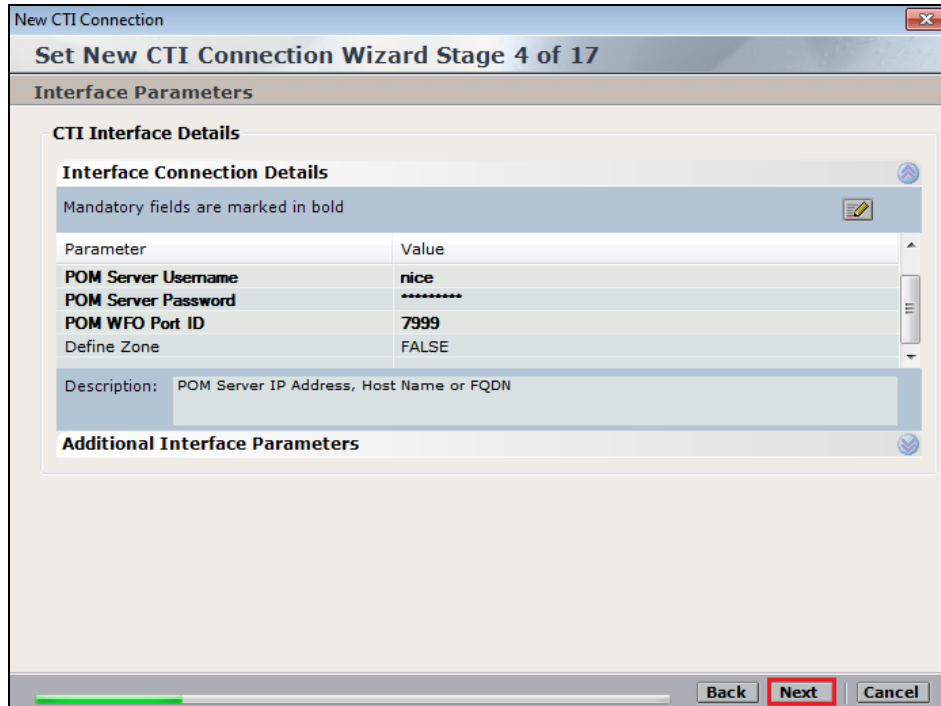
Enter the **POM Server Username** and click on **OK**.



Enter the **POM Server Password** and click on **OK**.



The other values can be left as default and click on **Next** to continue.

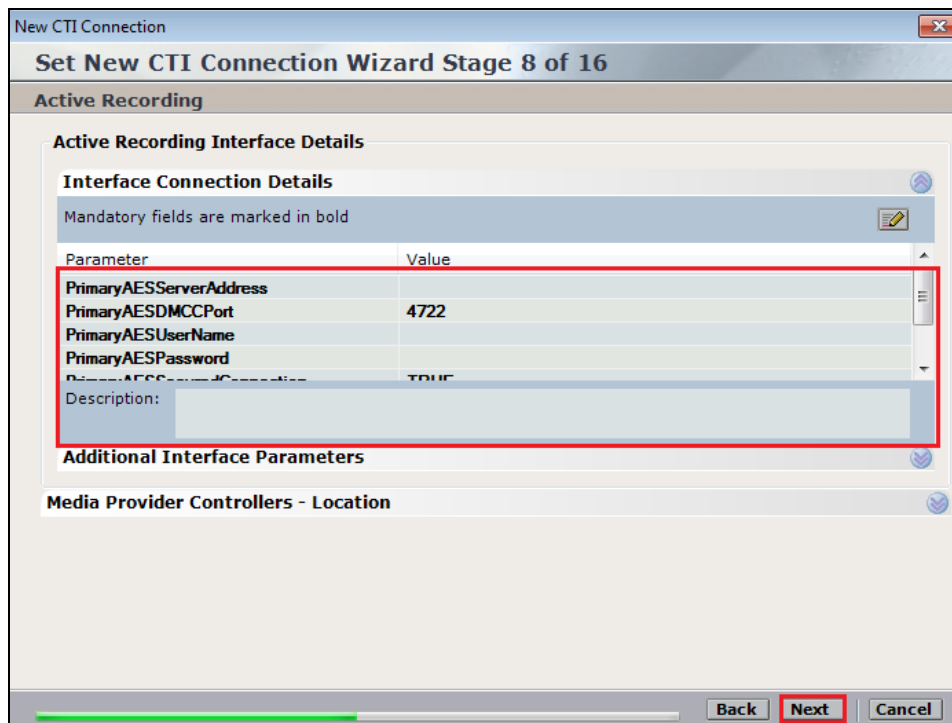


The screenshot shows the 'Set New CTI Connection Wizard Stage 4 of 17' window. The 'Interface Parameters' section is active. Under 'CTI Interface Details', the 'Interface Connection Details' table lists parameters: POM Server Username (nice), POM Server Password (masked), POM WFO Port ID (7999), and Define Zone (FALSE). A description field contains 'POM Server IP Address, Host Name or FQDN'. The 'Additional Interface Parameters' section is empty. The 'Next' button is highlighted with a red box.

Parameter	Value
POM Server Username	nice
POM Server Password	*****
POM WFO Port ID	7999
Define Zone	FALSE

Description: POM Server IP Address, Host Name or FQDN

The value for the connection to the AES for DMCC recording must now be filled in as well. Each of the values below must be filled in. Double-click on each **Parameter** to enter a value for that parameter.

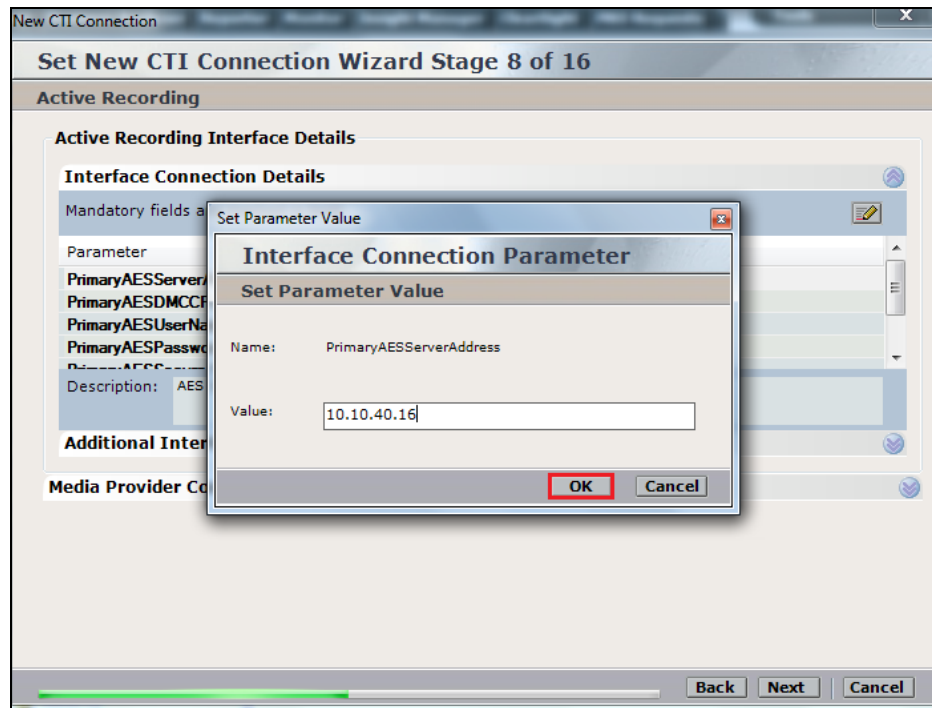


The screenshot shows the 'Set New CTI Connection Wizard Stage 8 of 16' window. The 'Active Recording' section is active. Under 'Active Recording Interface Details', the 'Interface Connection Details' table lists parameters: PrimaryAESServerAddress, PrimaryAESDMCCPort (4722), PrimaryAESUserName, PrimaryAESPassword, and PrimaryAESSoundGeneration (TRUE). A description field is empty. The 'Additional Interface Parameters' section is empty. The 'Media Provider Controllers - Location' section is also empty. The 'Next' button is highlighted with a red box.

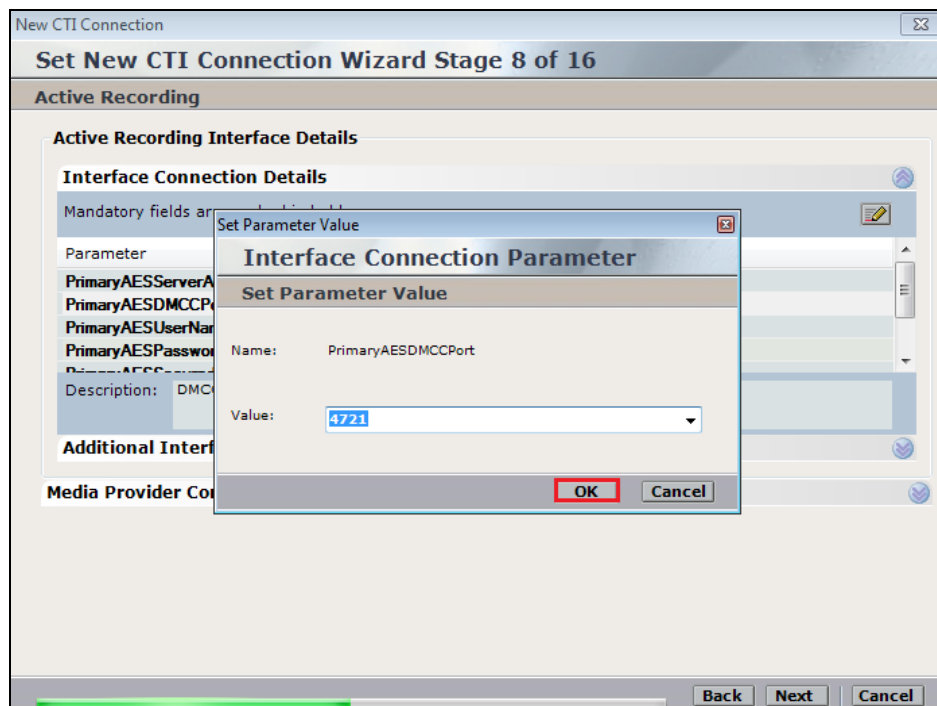
Parameter	Value
PrimaryAESServerAddress	
PrimaryAESDMCCPort	4722
PrimaryAESUserName	
PrimaryAESPassword	
PrimaryAESSoundGeneration	TRUE

Description:

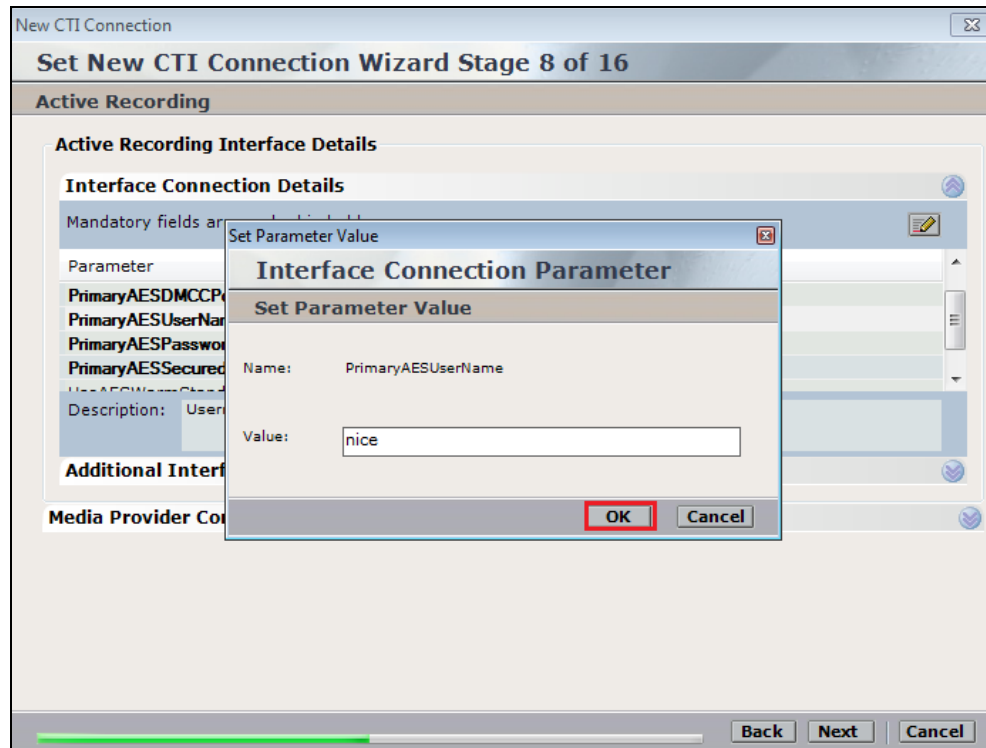
Enter the **Value** for the **AESServerAddress**, note this is the IP address of the AES server. Click on **OK**.



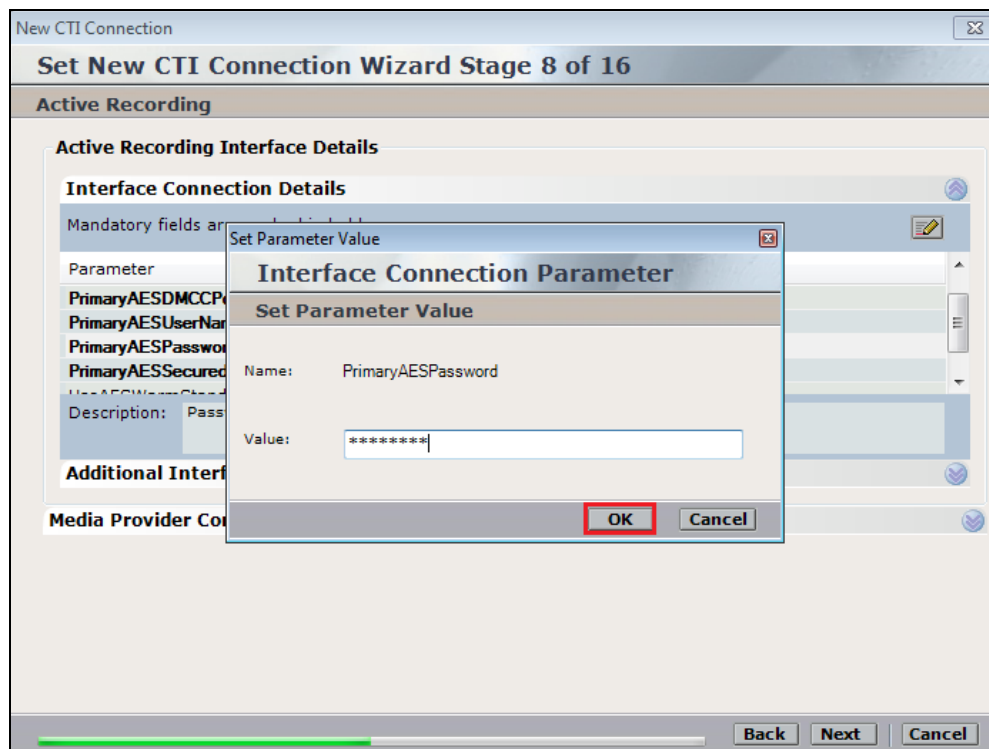
Enter the **Value** for the **AESDMCCPort**, note this will be the same port that was configured in **Section 6.4**. In this example the unencrypted port **4721** is entered.



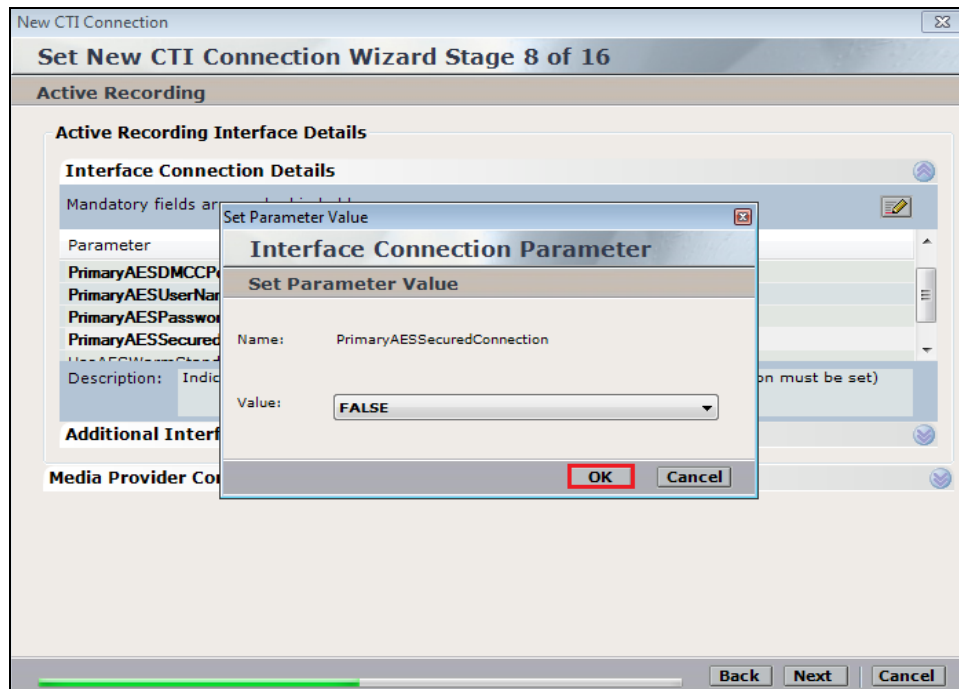
Enter the username that was created in **Section 6.5** and click on **OK**.



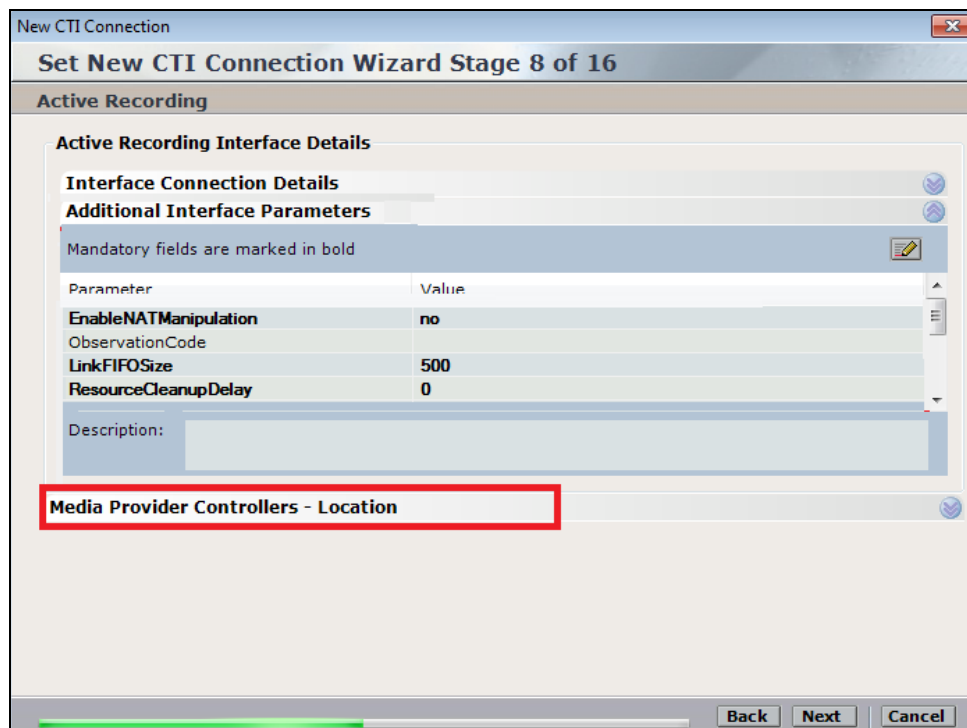
Enter the password that was created in **Section 6.5** and click on **OK**.



Because the unencrypted port was chosen select **False** for the **AESSecuredConnection**. Click on **OK** and then **Next** to continue.



Click on **Media Provider Controllers – Location** to expand this.



Enter the **IP/Hostname** of the Nice Advanced Interactions Server. Click on in + icon to add this.

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Additional Interface Parameters

Media Provider Controllers - Location

Media Provider Location

Server IP/Hostname: NICEActive2012

Connection Manager Port: 62094

Media Provider Controllers:

IP/Hostname	CM Port

Back Next Cancel

Click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Additional Interface Parameters

Media Provider Controllers - Location

Media Provider Location

Server IP/Hostname:

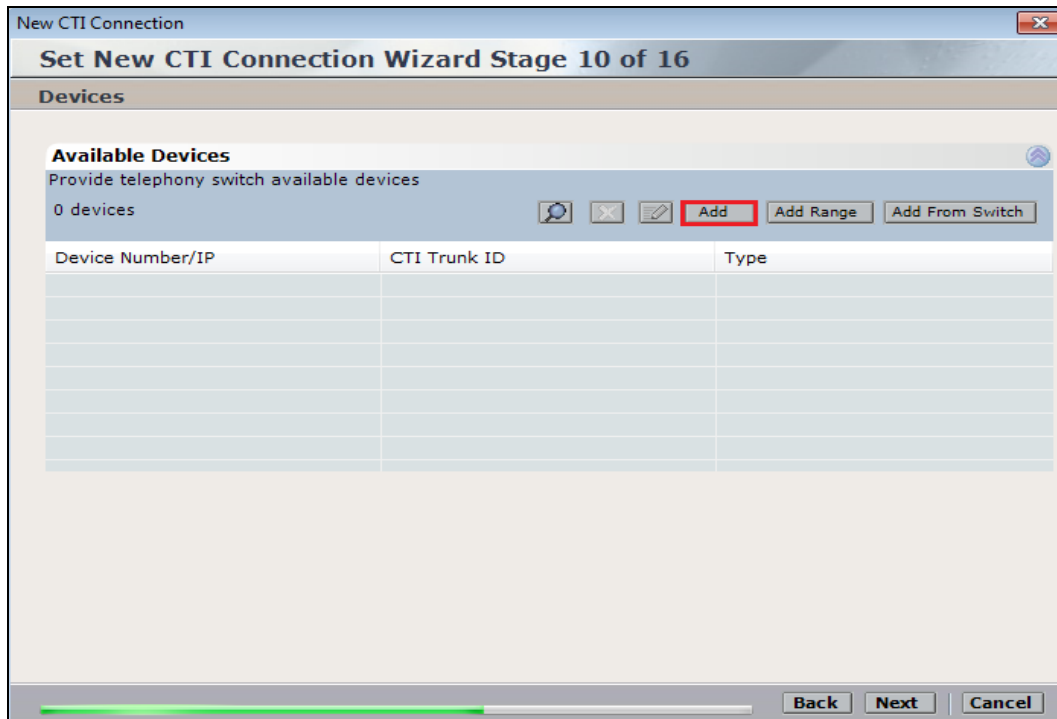
Connection Manager Port: 62094

Media Provider Controllers:

IP/Hostname	CM Port
NICEActive2012	62094

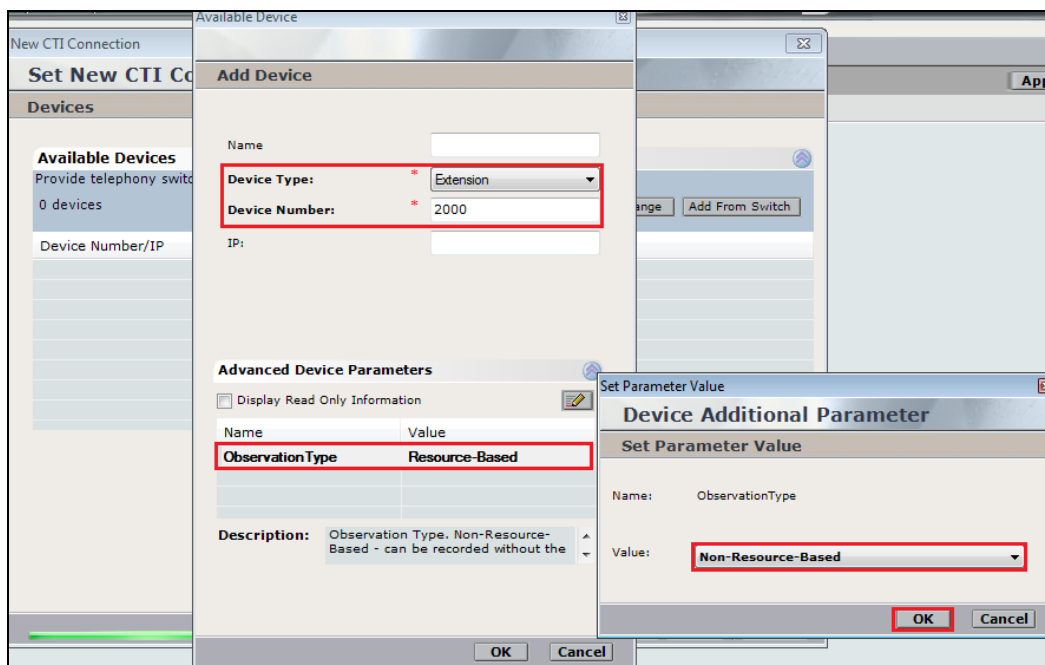
Back Next Cancel

On the following screen, click on **Add**, to add the Communication Manager devices.



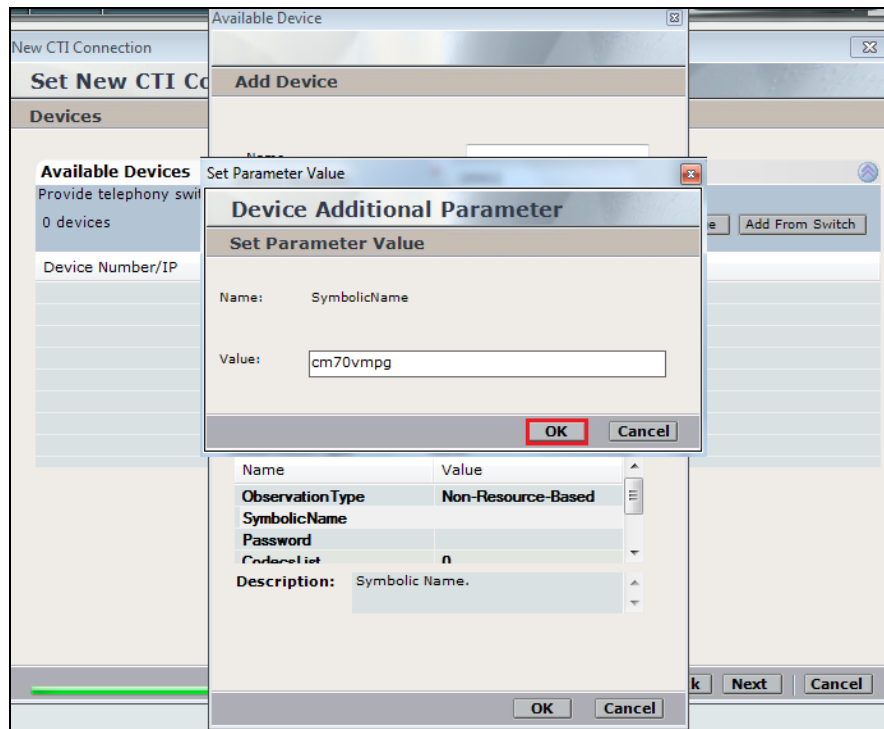
The screenshot shows the 'Set New CTI Connection Wizard Stage 10 of 16' window. The 'Devices' section is active, displaying 'Available Devices' with a table for 'Device Number/IP', 'CTI Trunk ID', and 'Type'. The table is currently empty. Above the table, there are buttons for 'Add', 'Add Range', and 'Add From Switch'. The 'Add' button is highlighted with a red box. At the bottom of the window, there are 'Back', 'Next', and 'Cancel' buttons.

The **Device Type** should be **Extension** and insert the correct extension number. Expand **Advanced Device Parameters** and ensure that the **Value** for **Observation Type** is set to **Non-Resourced-Based**. Click on **OK** to continue.

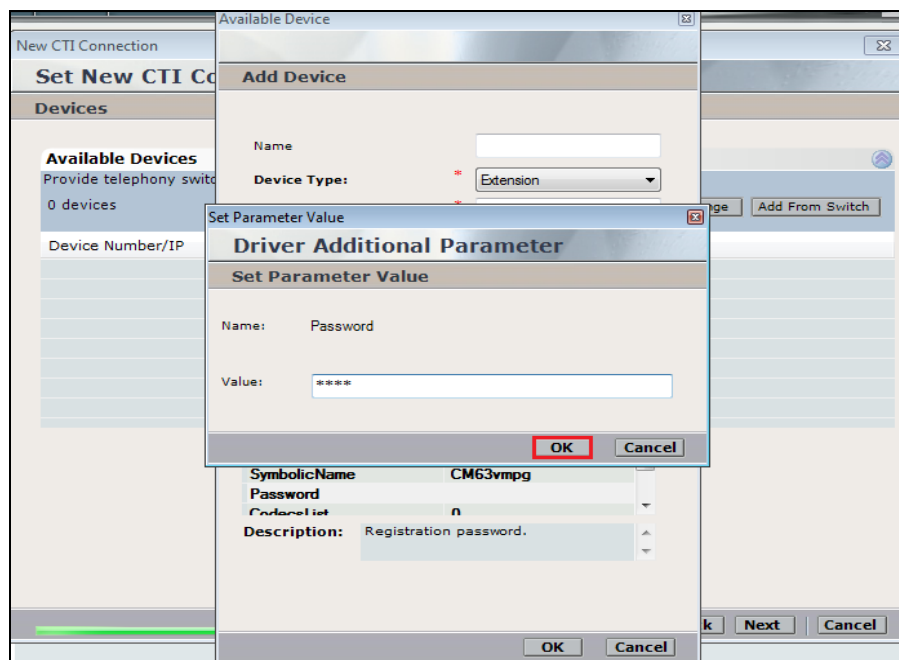


The screenshot shows the 'Set New CTI Connection Wizard Stage 10 of 16' window with the 'Add Device' sub-window open. The 'Device Type' is set to 'Extension' and the 'Device Number' is '2000'. The 'Advanced Device Parameters' section is expanded, showing 'Observation Type' set to 'Resource-Based'. A 'Set Parameter Value' dialog box is open, showing 'ObservationType' with a value of 'Non-Resource-Based'. The 'OK' button in the dialog box is highlighted with a red box.

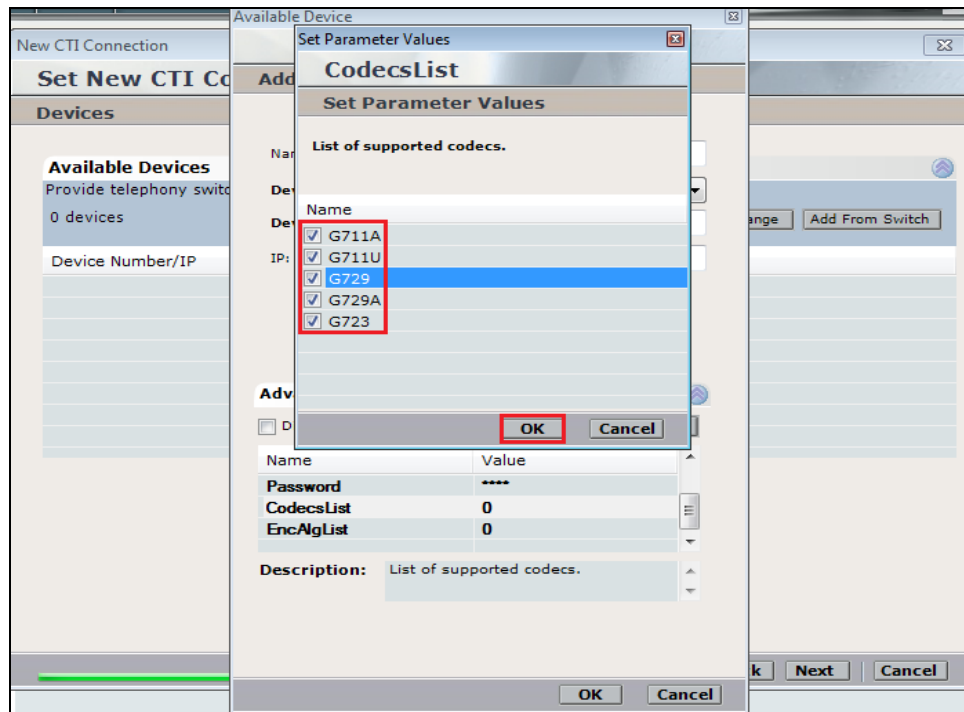
Next enter the correct **Value** for **SymbolicName**. Double-click on **SymbolicName** to set the value. This should be the same as the switch name entered in **Section 6.2**.



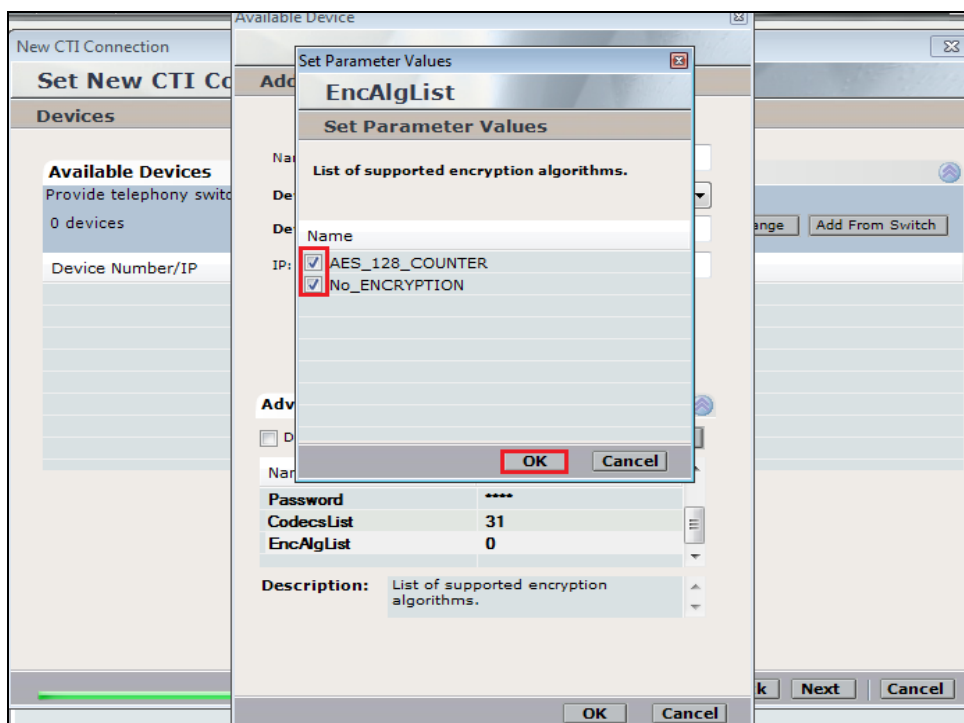
Enter the correct **Password** and note this is the password for the extension that is being added here. This is the station password which was entered during the creation of the station. A printout of an extension can be found in **Section 5.5** of these Application Notes.



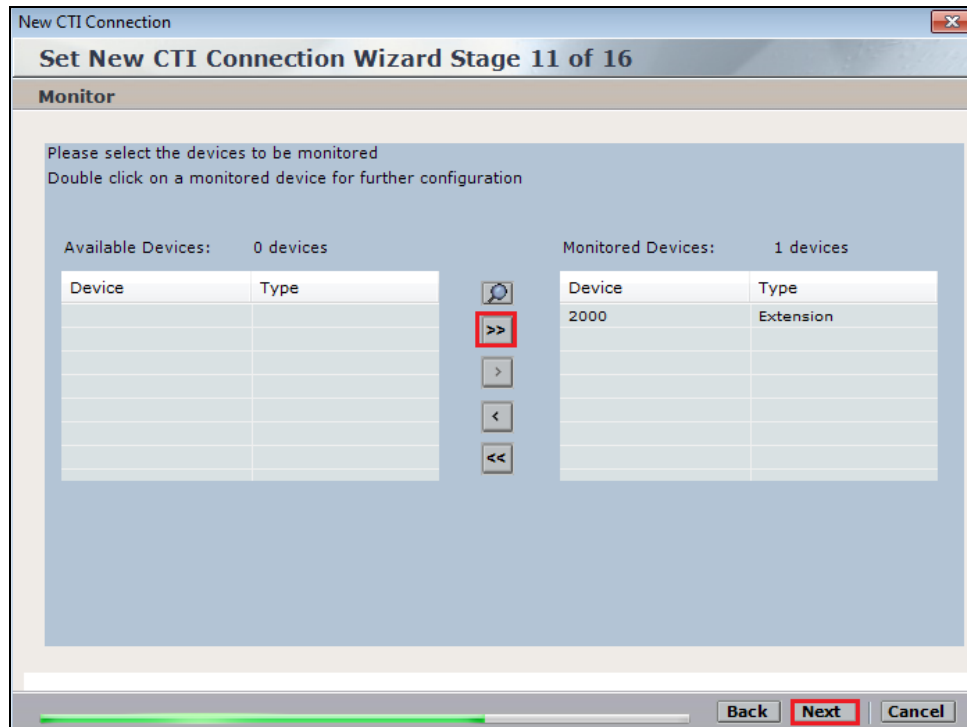
Double-click on **CodecsList** and ensure that all the values are ticked as shown below. Click on **OK** to continue.



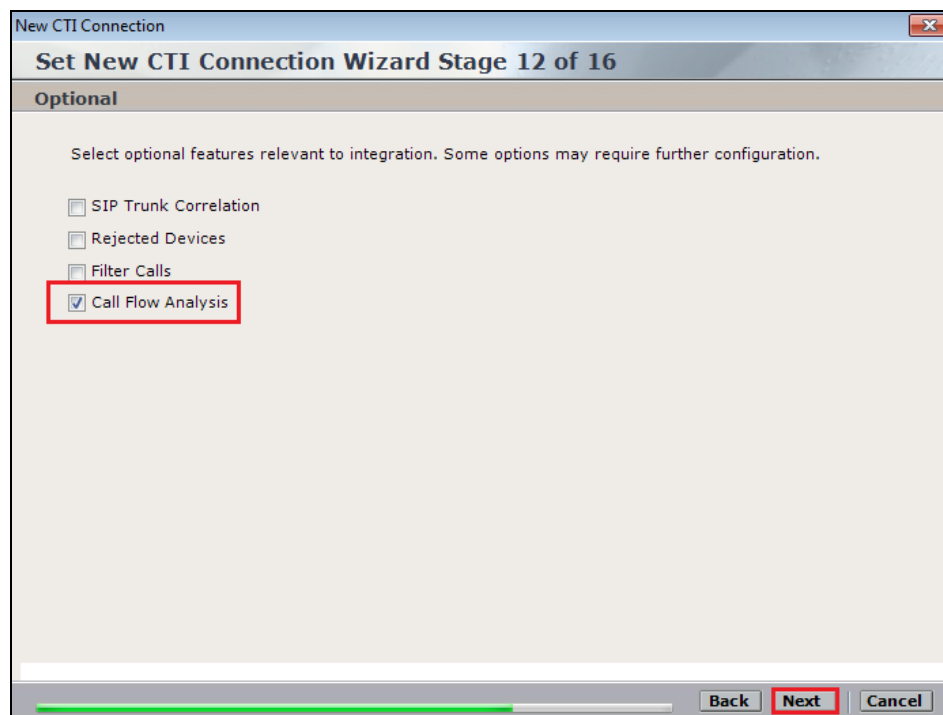
Double-click on **EncAlgList** and ensure both options are ticked as shown below. Click on **OK** to continue.



Select the new extension and click on the >> icon as shown. Click on **Next** to continue.



This is optional, but for better analysis tick on **Call Flow Analysis** and click on **Next** to continue.



Select a different **Port** number as shown below. Port **62095** is chosen simply because **62094** was already in use.

New CTI Connection

Set New CTI Connection Wizard Stage 15 of 16

Requirements

The Interactions Center server selected already has a Connection Manager.
Create a new Connection Manager, or select an existing one.

☒ Create a new Connection Manager

Port: 62095

☐ Select available Connection Manager

Ports in use:

62094

Back Next Cancel

Click on **Finish** to complete the **New CTI Wizard**.

New CTI Connection

Set New CTI Connection Wizard Stage 16 of 16

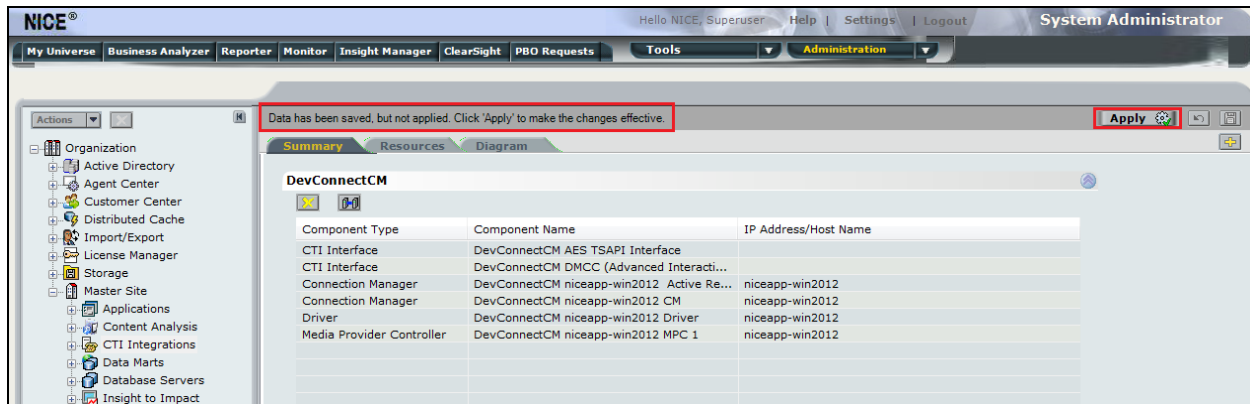
Summary

Click Finish to save and apply the configuration of the following CTI:

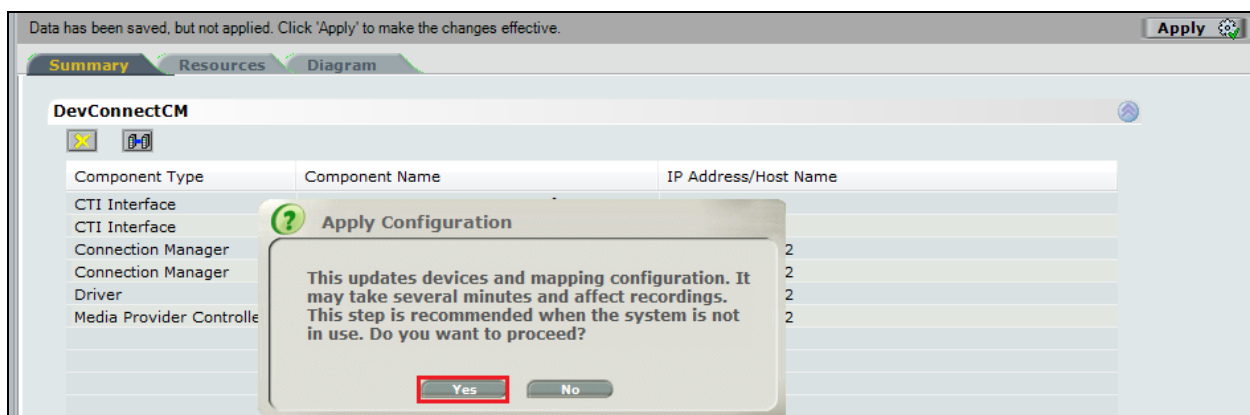
DevConnectCM Connection

Back Finish Cancel

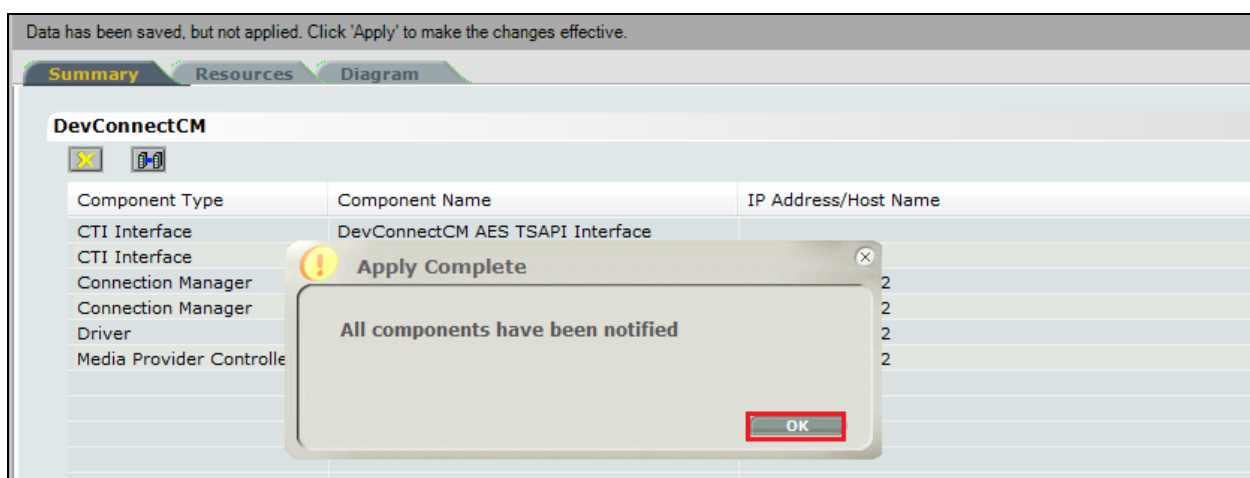
Click on **Apply** at the top right of the screen to save the new connection.



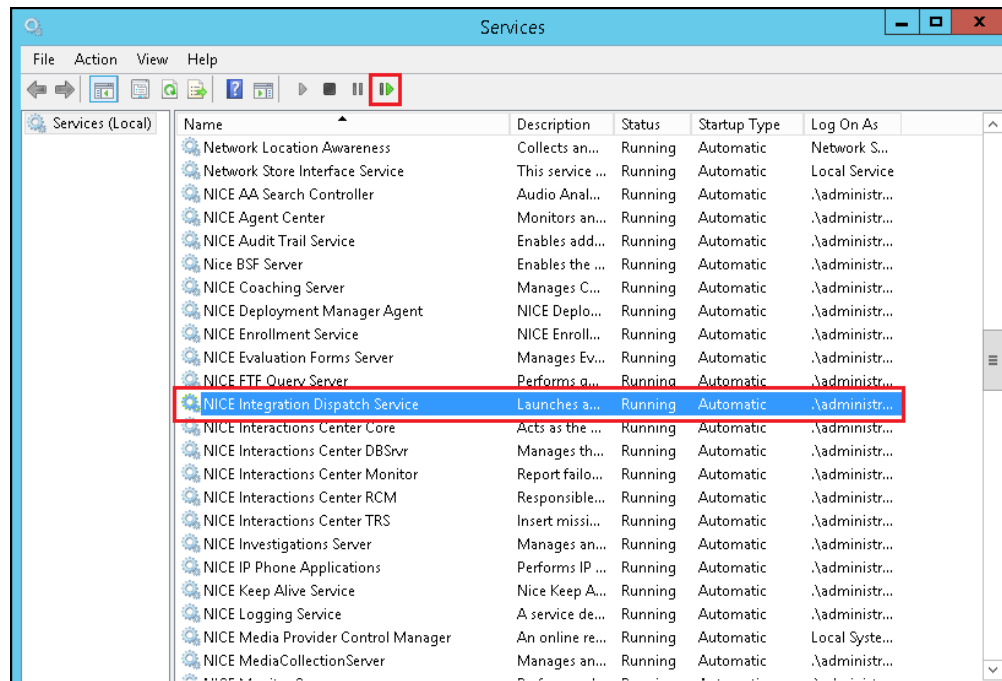
Click on **Yes** to proceed.



The following shows that the save was successful. Click on **OK** to continue.

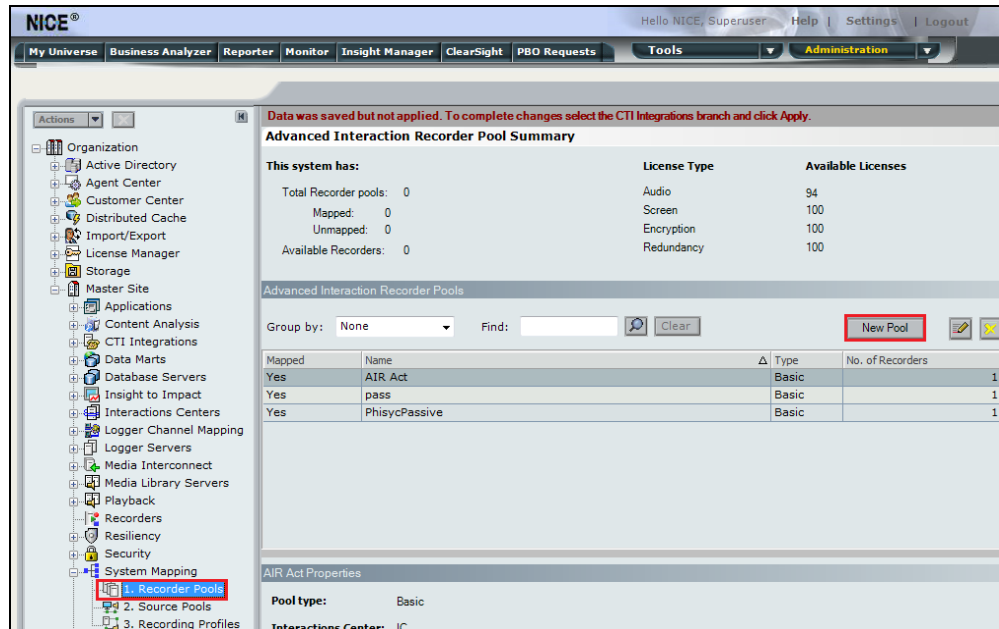


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

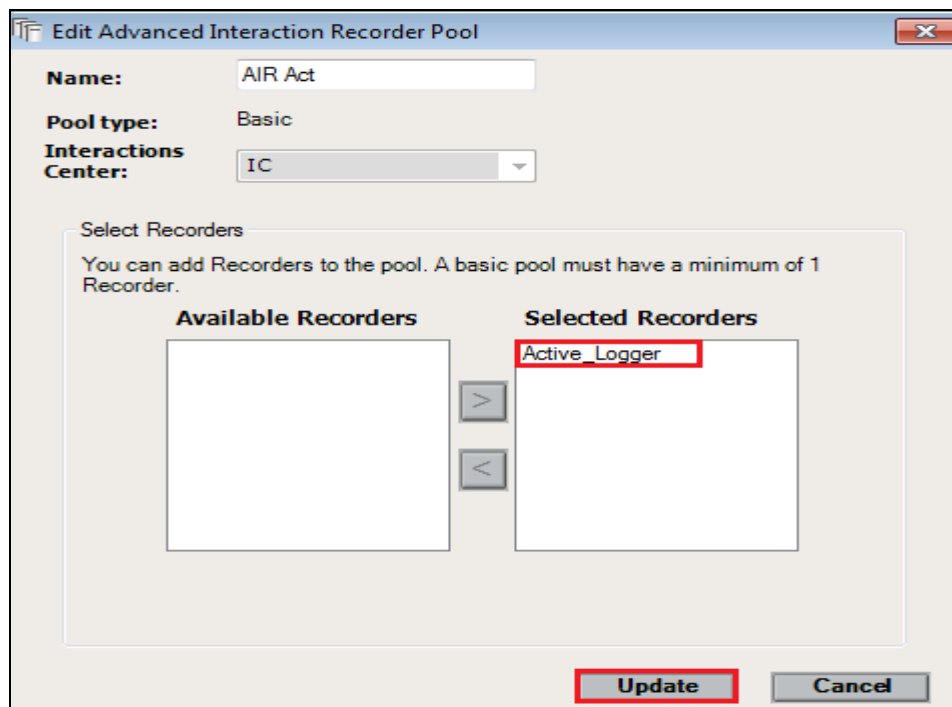


9.2. System Mapping

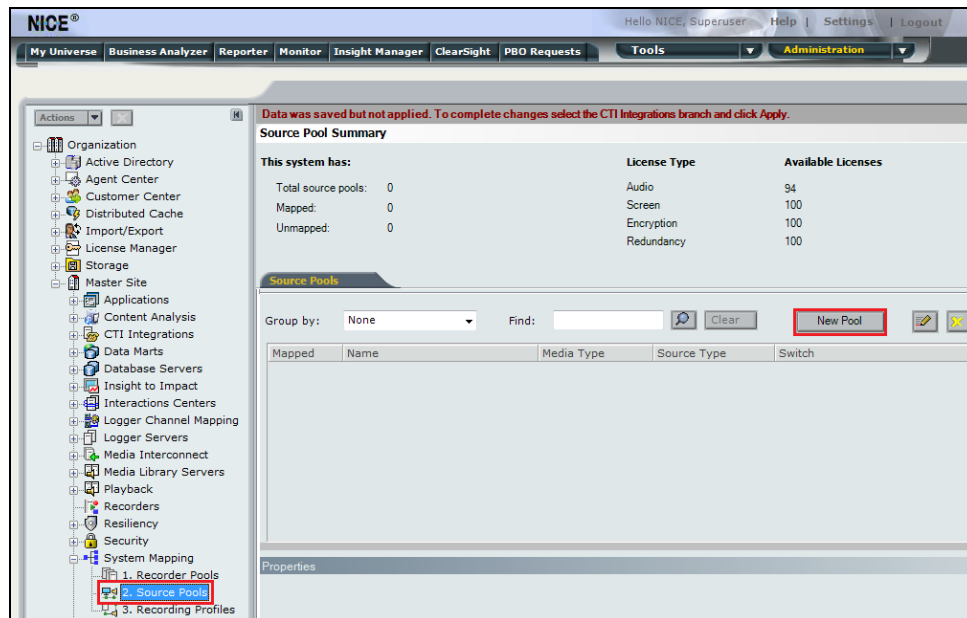
From the web browser navigate to **Master Site → System Mapping → Recorder Pools** and in the main window click on **New Pool**.



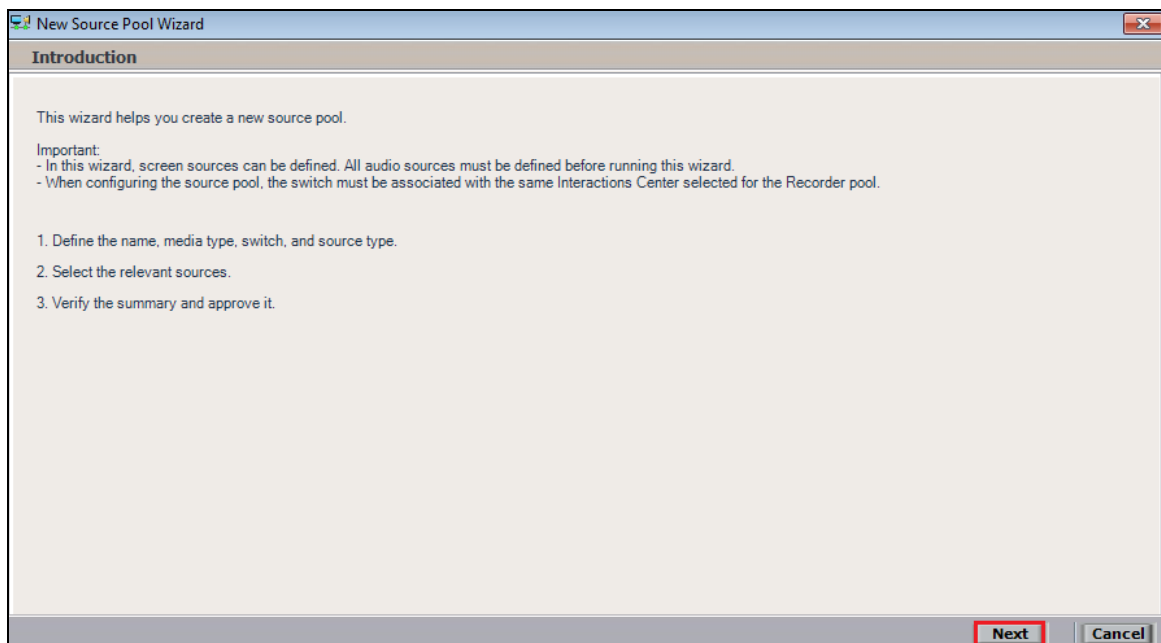
Enter a suitable **Name** for the **Recorder Pool** and select the **Active_Logger** from the list of **Available Recorders** and click on **Update** to continue.



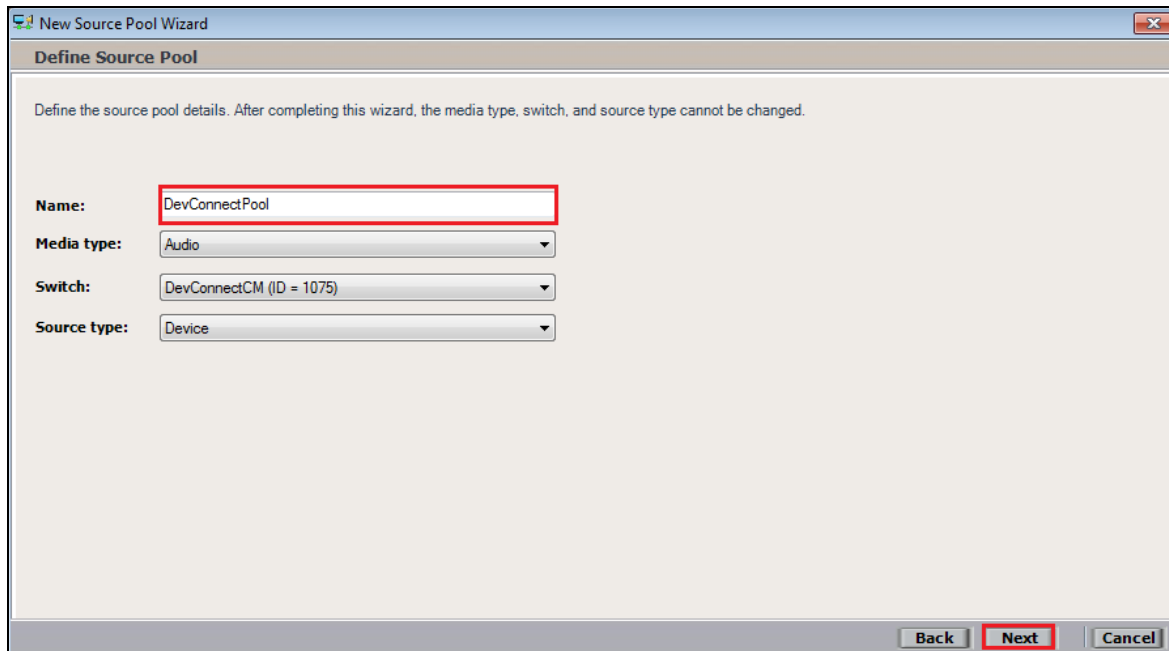
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



Click on **Next** to continue to add a new **Source Pool**.

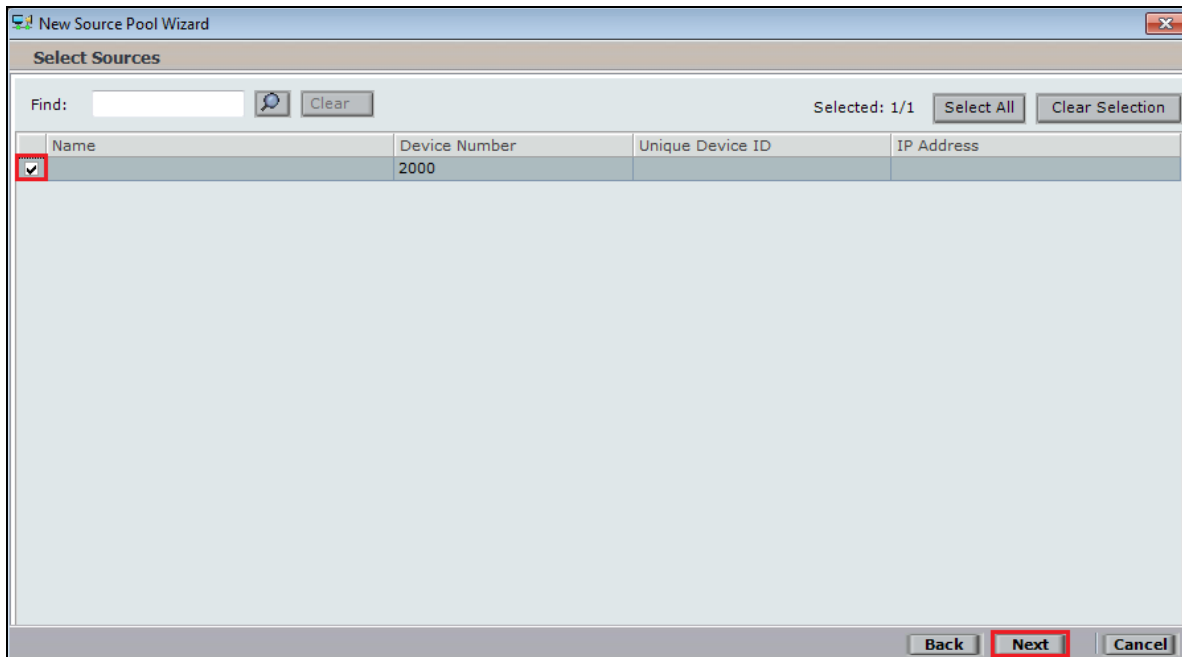


Enter a suitable **Name** and the other values were left as default. Click on **Next** to continue.



The screenshot shows the 'Define Source Pool' step of the 'New Source Pool Wizard'. The window title is 'New Source Pool Wizard'. The subtitle is 'Define Source Pool'. Below the subtitle is a note: 'Define the source pool details. After completing this wizard, the media type, switch, and source type cannot be changed.' There are four input fields: 'Name' with the value 'DevConnectPool', 'Media type' with the value 'Audio', 'Switch' with the value 'DevConnectCM (ID = 1075)', and 'Source type' with the value 'Device'. At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red box.

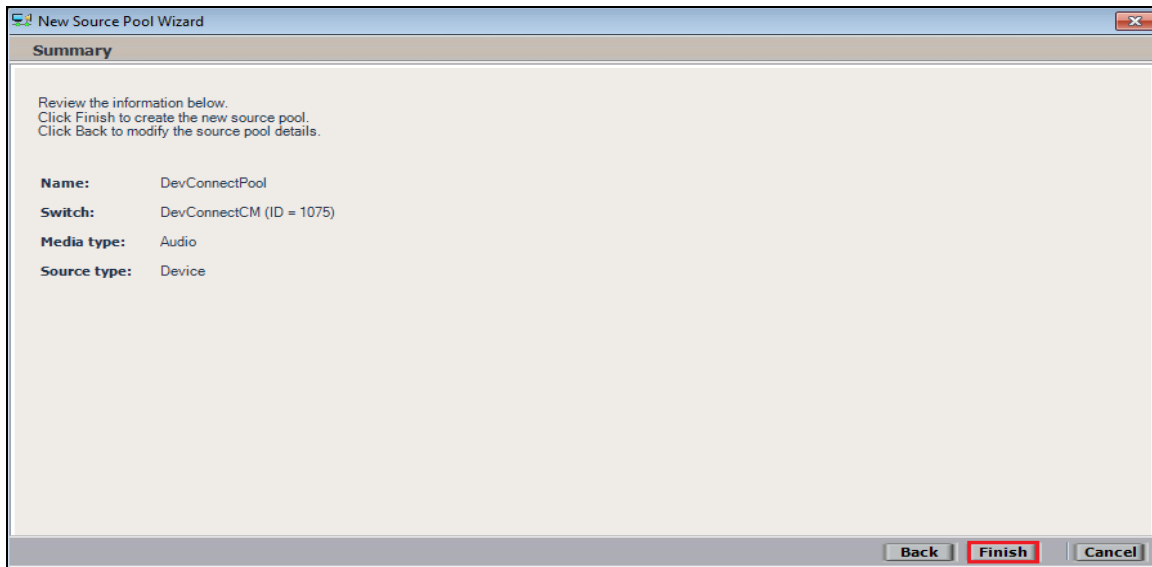
Select the extensions that were added in **Section 9.1**, note only one extension number is shown in the example below but this is not typical. Click on **Next** to continue.



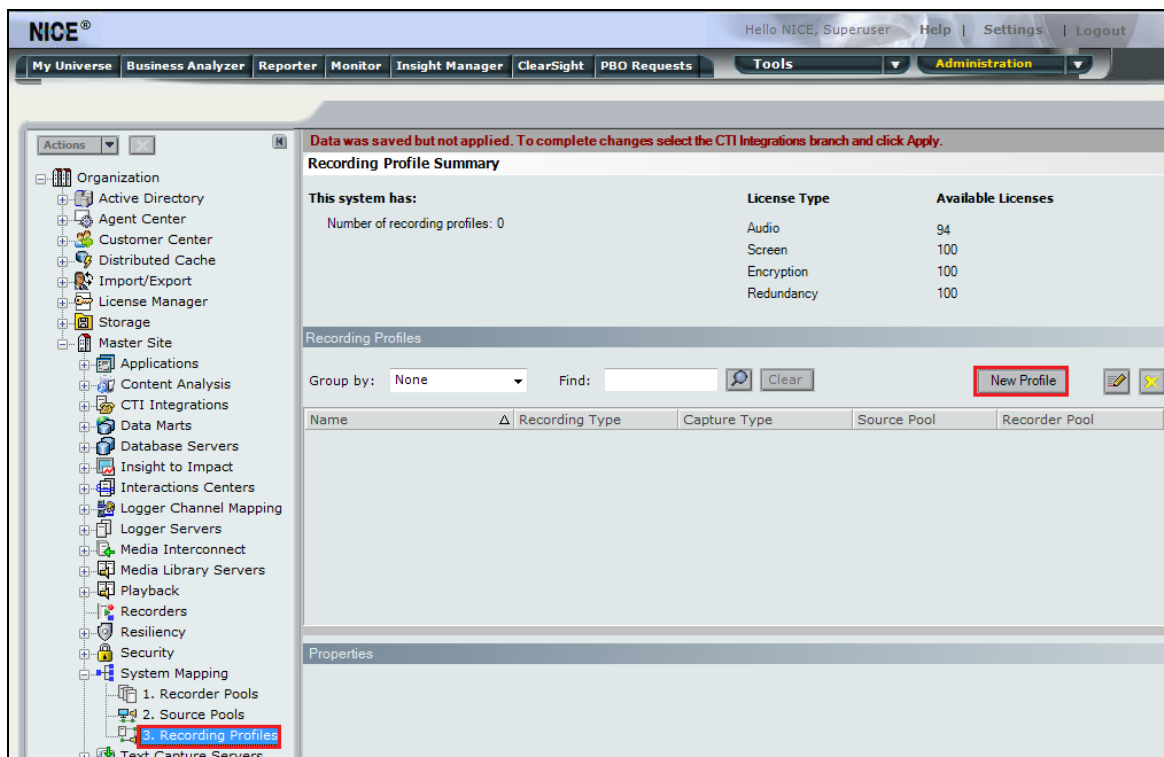
The screenshot shows the 'Select Sources' step of the 'New Source Pool Wizard'. The window title is 'New Source Pool Wizard'. The subtitle is 'Select Sources'. There is a 'Find:' text box with a search icon and a 'Clear' button. To the right, it says 'Selected: 1/1' with 'Select All' and 'Clear Selection' buttons. Below this is a table with four columns: 'Name', 'Device Number', 'Unique Device ID', and 'IP Address'. The first row has a checked checkbox in the 'Name' column, and the 'Device Number' is '2000'. At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red box.

	Name	Device Number	Unique Device ID	IP Address
<input checked="" type="checkbox"/>		2000		

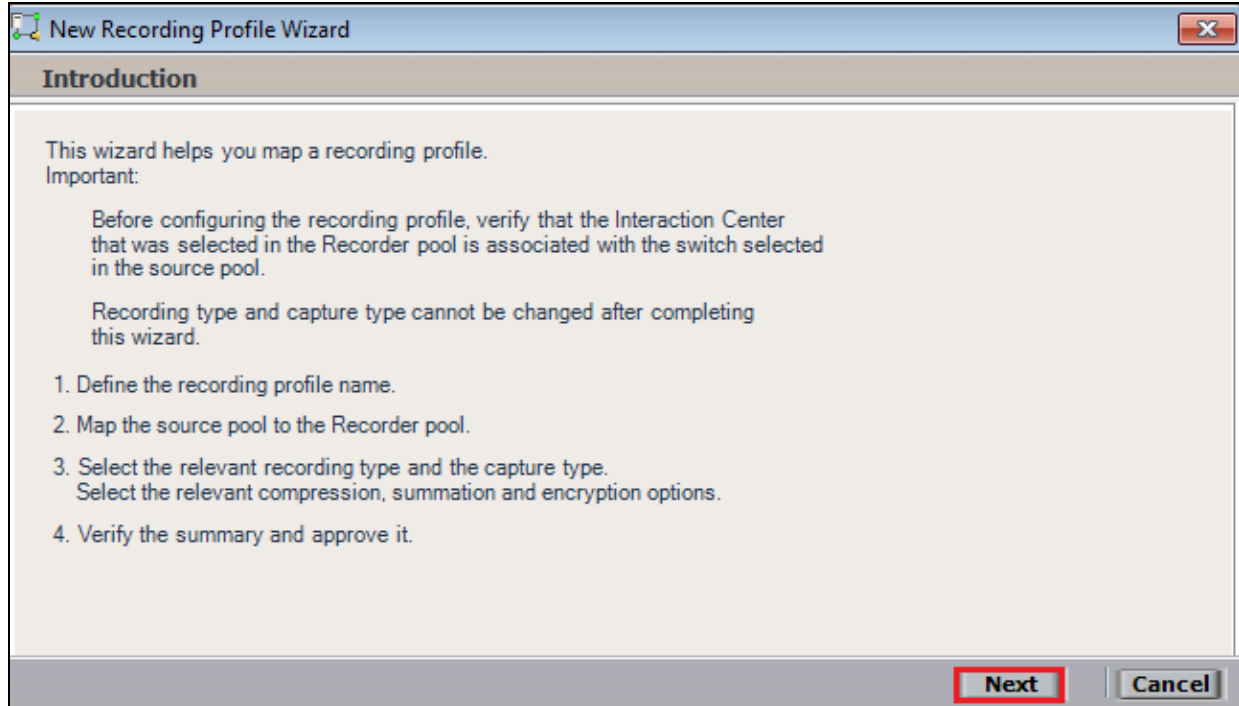
Click on **Finish** to complete the New Source Pool Wizard.



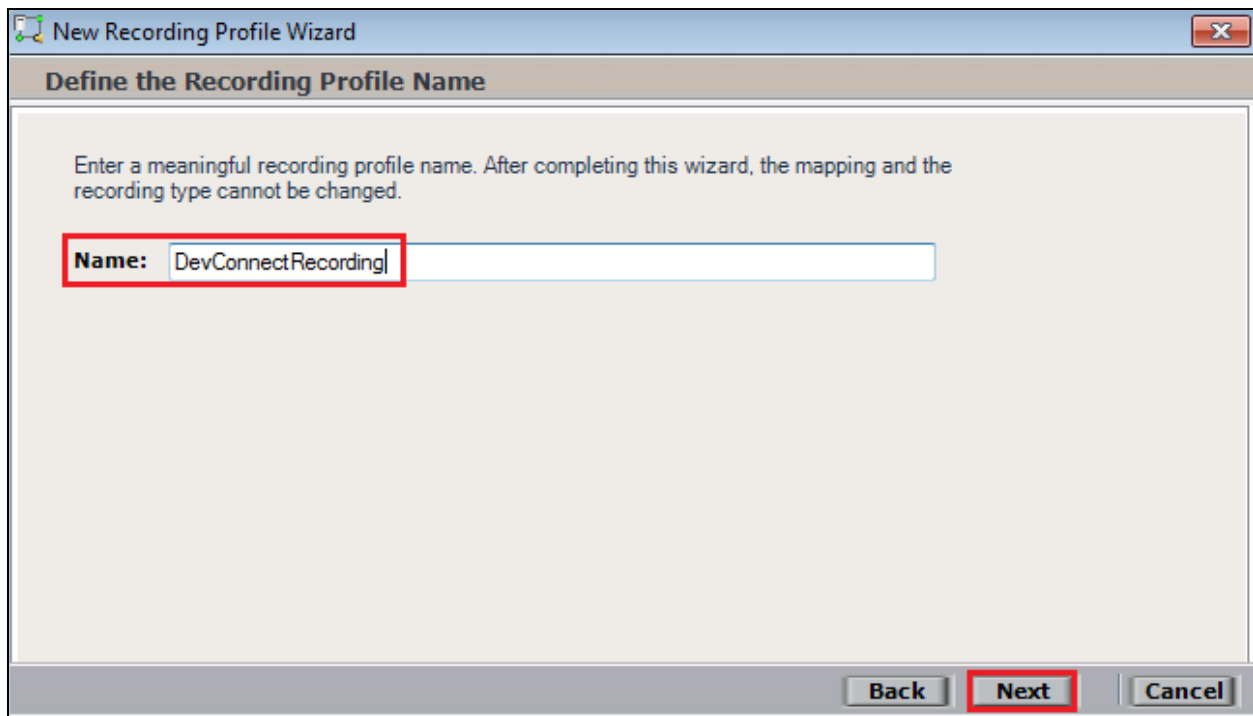
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



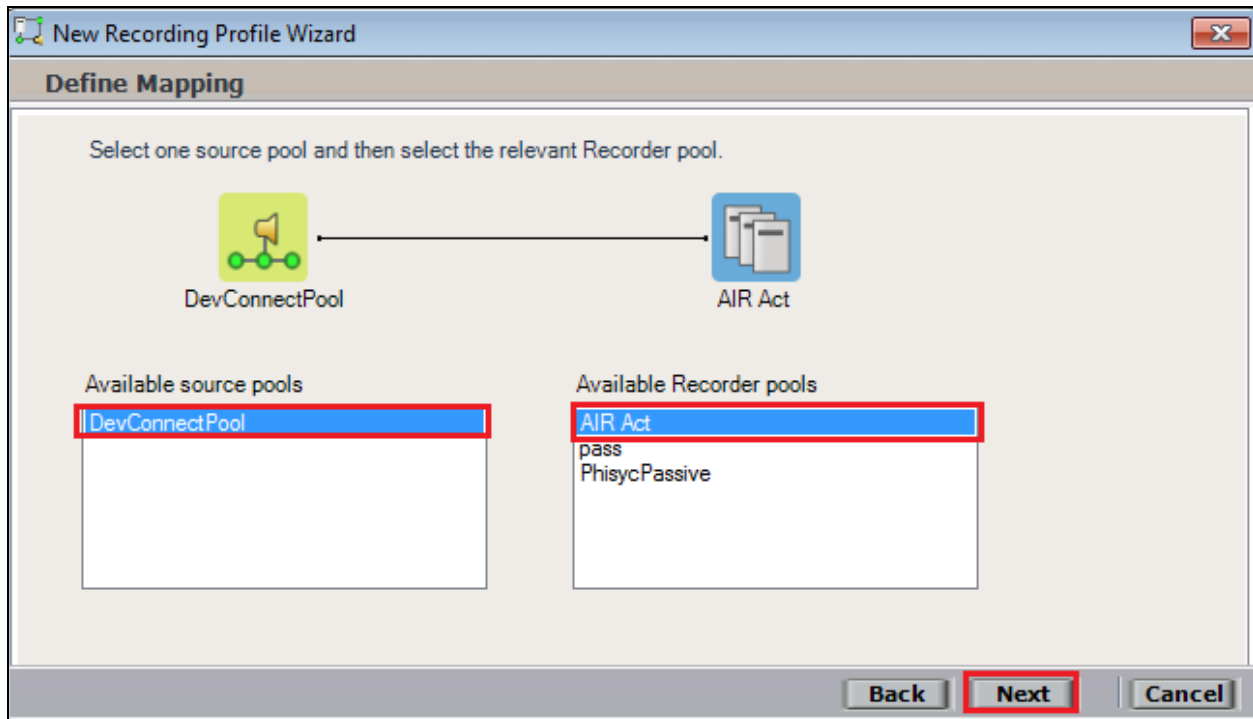
Click on **Next** to continue with the **New Recording Profile Wizard**.



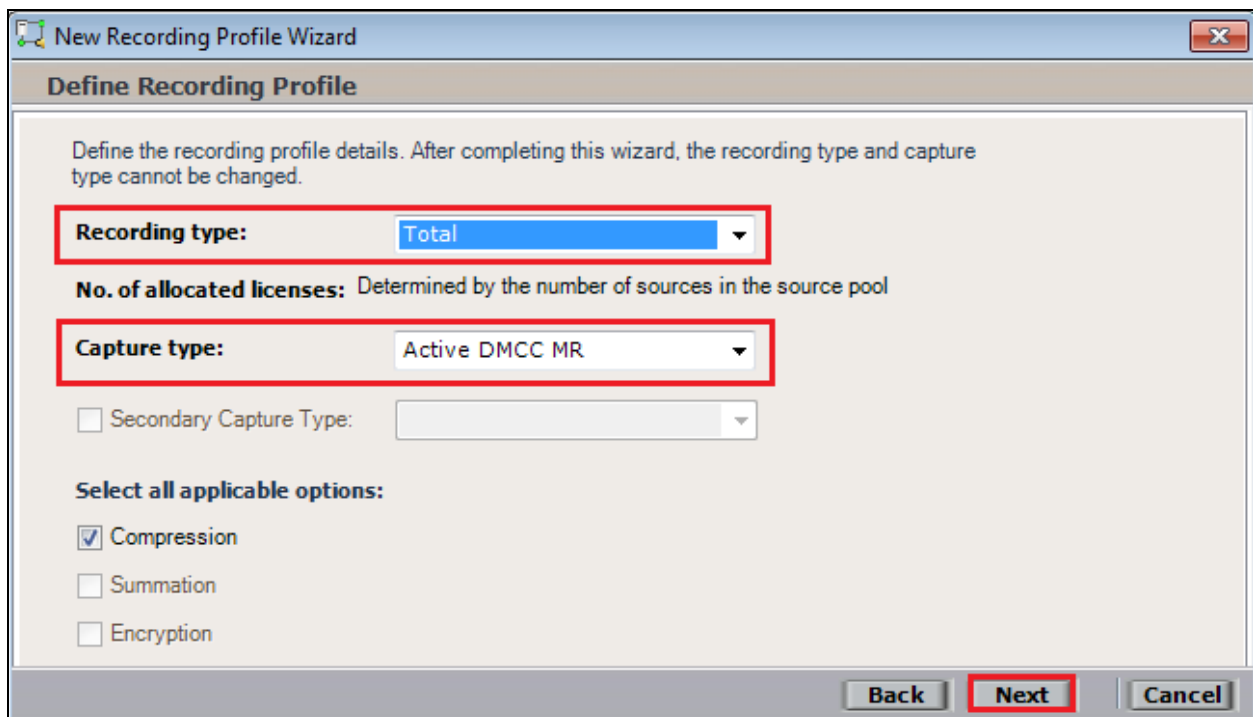
Enter a suitable **Name** for the Recording profile.



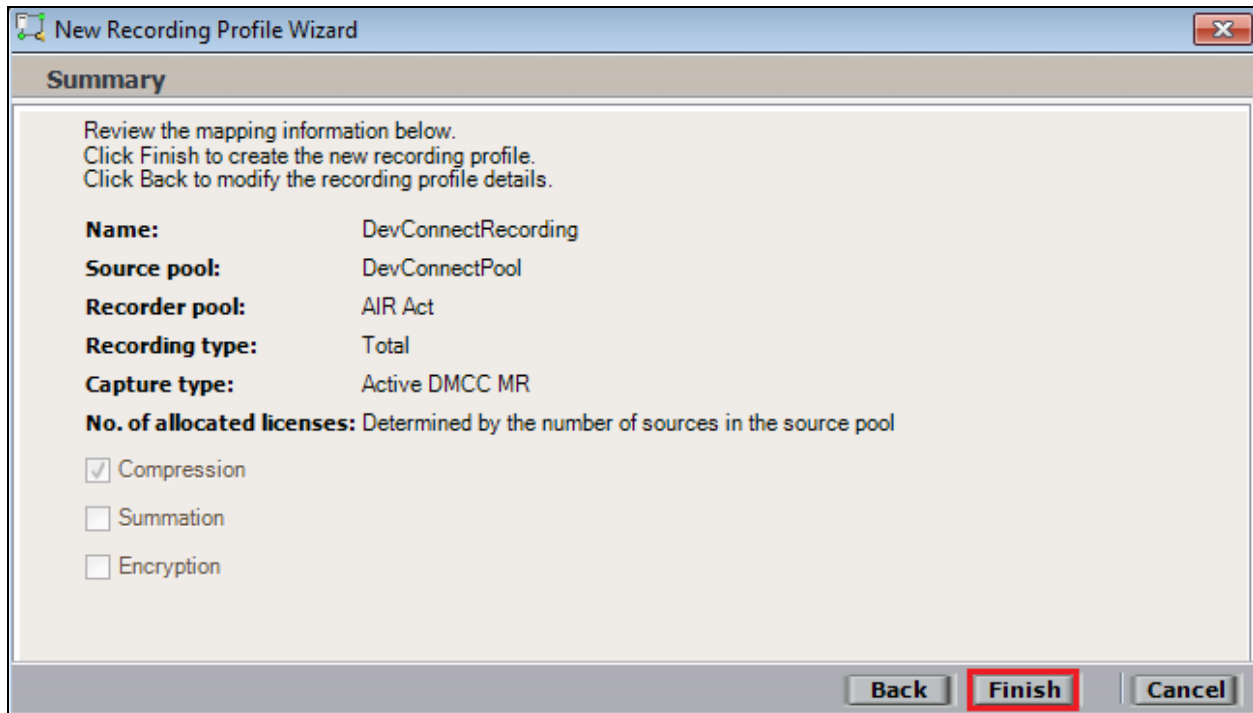
Select the correct **source pool** and **Recorder pool**, and then click **Next** to continue.



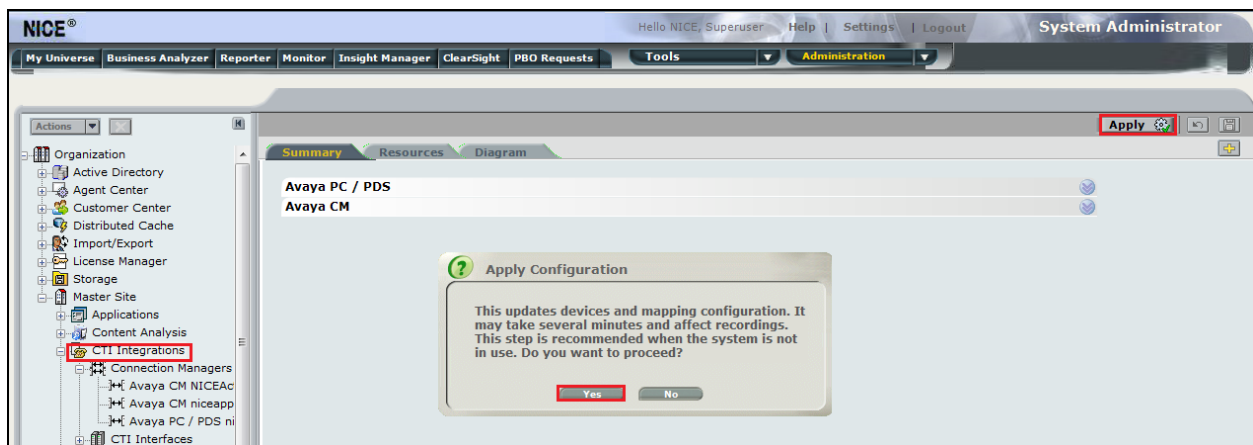
For total recording i.e., the recording of all calls, select **Total** as the **Recording type**. For **Capture type** ensure that **Active DMCC MR** is selected from the drop-down box. Compression is selected as default and can be left like this. Click on **Next** to continue.



Click on **Finish** to complete the **New Recording Profile Wizard**.



To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window. Then click on **Yes** to proceed.



This concludes the setup of the NICE Application Server for DMCC Multi-Registration recording, connecting to POM for call events.

10. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the NICE Engage Platform and Avaya Aura® Application Enablement Services.

10.1. Verify Avaya Aura® Communication Manager CTI Service State

Before checking the connection between the NICE Engage Platform and AES, check the connection between Communication Manager and AES to ensure it is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	5	no	aes70vmpg	established	18	18

10.2. Verify DMCC link on AES

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** to display the **DMCC Service Summary – Session Summary** screen. The screen below shows that the user **NICE** is connected from the IP address **10.10.40.126**, which is the NICE Application server.

AVAYA

Application Enablement Services
Management Console

Number of prior failed login attempts: 1
HostName/IP: aes70vmpg/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Dec 15 14:45:11 GMT 2015
HA Status: Not Configured

Status | Status and Control | DMCC Service SummaryHome | Help | Logo

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

User Management

Utilities

Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Dec 15 14:45:11 GMT 2015

Service Uptime: 1 days, 0 hours 46 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 1

Number of Existing Devices: 3

Number of Devices Created Since Service Boot: 11

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	1C06ED1F66D641627 7F0F0B05747B4AF-0	NICE		10.10.40.126	XML Unencrypted	3

Item 1-1 of 1

1 Go

Terminate Sessions Show Terminated Sessions

By clicking on **POM Monitor** at the bottom of the left window, it will show the campaigns that are running.

Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal)

Expand All Collapse All

User Management

Roles

Users

Login Options

Real-time Monitoring

System Monitor

Active Calls

Port Distribution

System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

System Management

Application Server

EPM Manager

MPP Manager

Software Upgrade

System Backup

System Configuration

Applications

EPM Servers

MPP Servers

SNMP

Speech Servers

VoIP Connections

Zones

Security

Certificates

Licensing

Reports

Standard

Custom

Scheduled

Multi-Media Configuration

Email

HTML

SMS

POM

POM Home

POM Monitor

Proactive Outreach Manager 3.0

POM Home

Campaigns

Contacts

Configurations

Active Campaigns

	Campaign Name	Campaign Type	Job ID	Status	Contact List(s)	Organization	Start Time	Total Contacts	Processed
	NICEout	finite	12	Running	SIPandQSIG		12/13/2016 1:4...	31	1

The **Application Server** can be checked as follows.

Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal)

Expand All | Collapse All

User Management

Roles

Users

Login Options

Real-time Monitoring

System Monitor

Active Calls

Port Distribution

System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

System Management

Application Server

EPM Manager

MPP Manager

Software Upgrade

System Backup

System Configuration

Applications

EPM Servers

MPP Servers

You are here: [Home](#) > System Management > Application Server

Application Server (Dec 15, 2016 3:54:48 AM PST)

Use this page to start and stop the application server co-resident with the p deploy, undeploy, start and stop applications on the application server.

<input type="checkbox"/>	Host Address	State
<input type="checkbox"/>	POM3vmpg	Running

State Commands

Start

Stop

Help

The **EPM Manager** can be checked as follows.

Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal)

Expand All | Collapse All

You are here: [Home](#) > System Management > EPM Manager

EPM Manager (Dec 15, 2016 3:55:15 AM PST)

This page displays the current state of each EPM in the Experience Portal system. To enable the selected EPMs must also be stopped.

Last Poll: Dec 15, 2016 3:54:59 AM PST

<input type="checkbox"/>	Zone	Server Name	Type	Mode	State	Config
<input type="checkbox"/>	Default EPM		Primary	Online	Running	OK

State Commands

[Start](#) [Stop](#) [Restart](#) [Reboot](#) [Halt](#)

Mode Commands

[Offline](#) [Online](#)

[Help](#)

The **MPP Manager** can be checked as follows.

Avaya Aura® Experience Portal 7.1.0 (ExperiencePortal)

Expand All | Collapse All

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (Dec 15, 2016 3:56:14 AM PST)

This page displays the current state of each MPP in the Experience Portal system. To enable the selected MPPs must also be stopped.

Last Poll: Dec 15, 2016 3:56:08 AM PST

<input type="checkbox"/>	Zone	Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
							Today	Recurring	In	Out
<input type="checkbox"/>	Default	LocalMPP	Online	Running	OK	Yes	No	None	0	0

State Commands

[Start](#) [Stop](#) [Restart](#) [Reboot](#) [Halt](#) [Cancel](#)

Mode Commands

[Offline](#) [Test](#) [Online](#)

Restart/Reboot Options

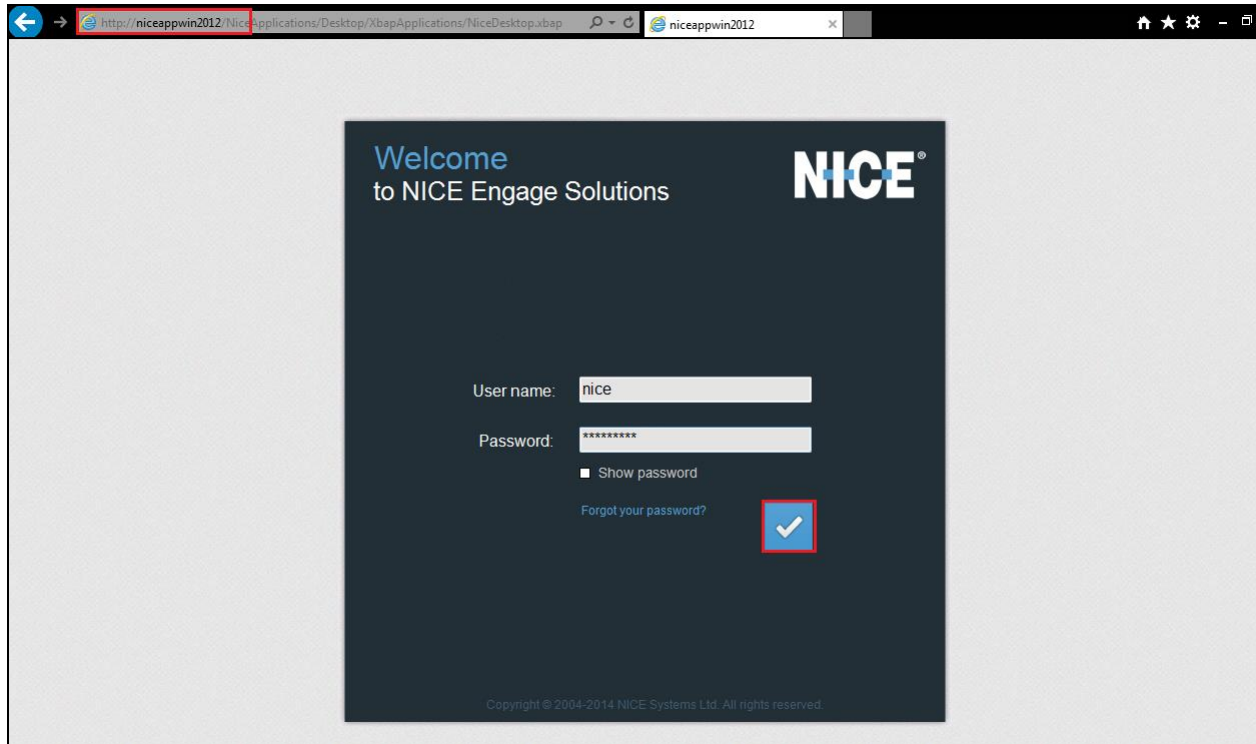
☒ One server at a time
☐ All servers

[Help](#)

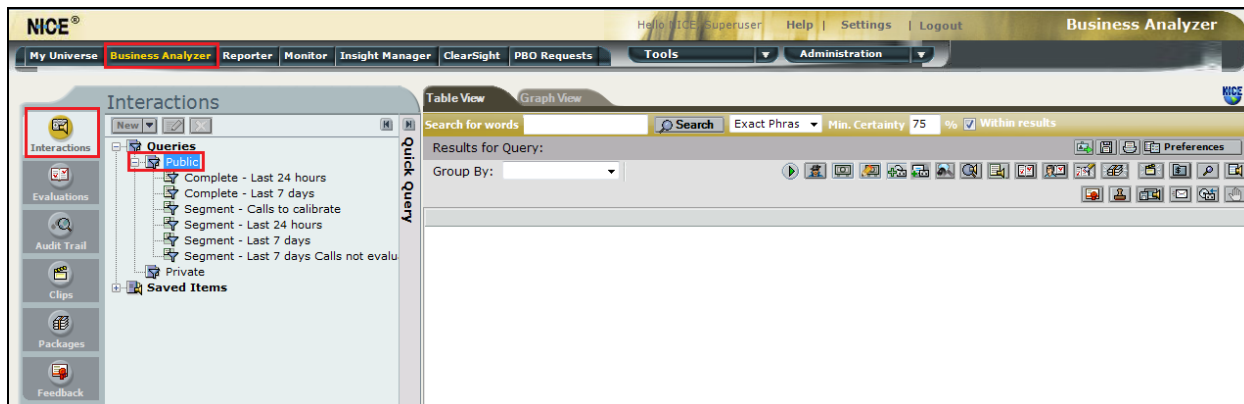
10.4. Verify calls are being recorded

From any of the monitored Avaya endpoints make a series of inbound and outbound calls. Once these calls are completed they should be available for playback through a web browser to the NICE Application Server.

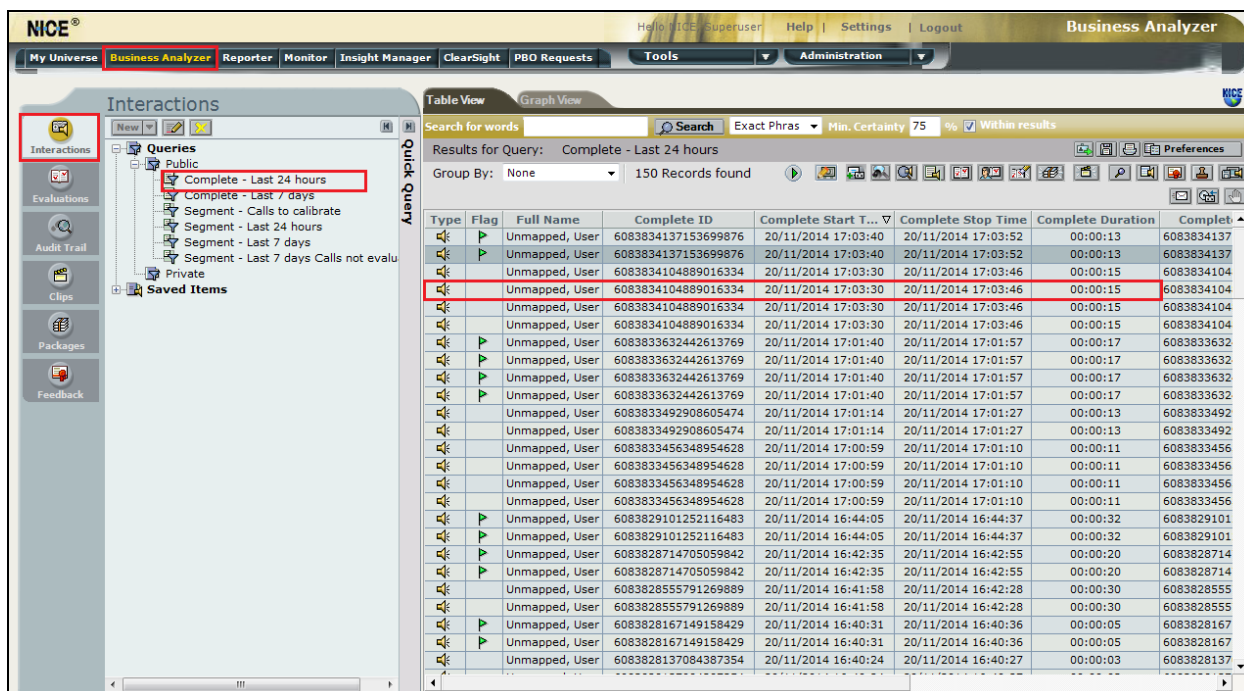
Open a browser session to the NICE Application Server as is shown below. Enter the proper credentials and click on **Login**.



Click on **Business Analyser** at the top of the screen. Select **Interactions** from the left window and then navigate to **Queries** → **Public**.



Click on **Complete – Last 24 hours**. This should reveal all the recordings that took place over the previous 24 hours. Select the required recording from the list and double-click on this to play the recording.



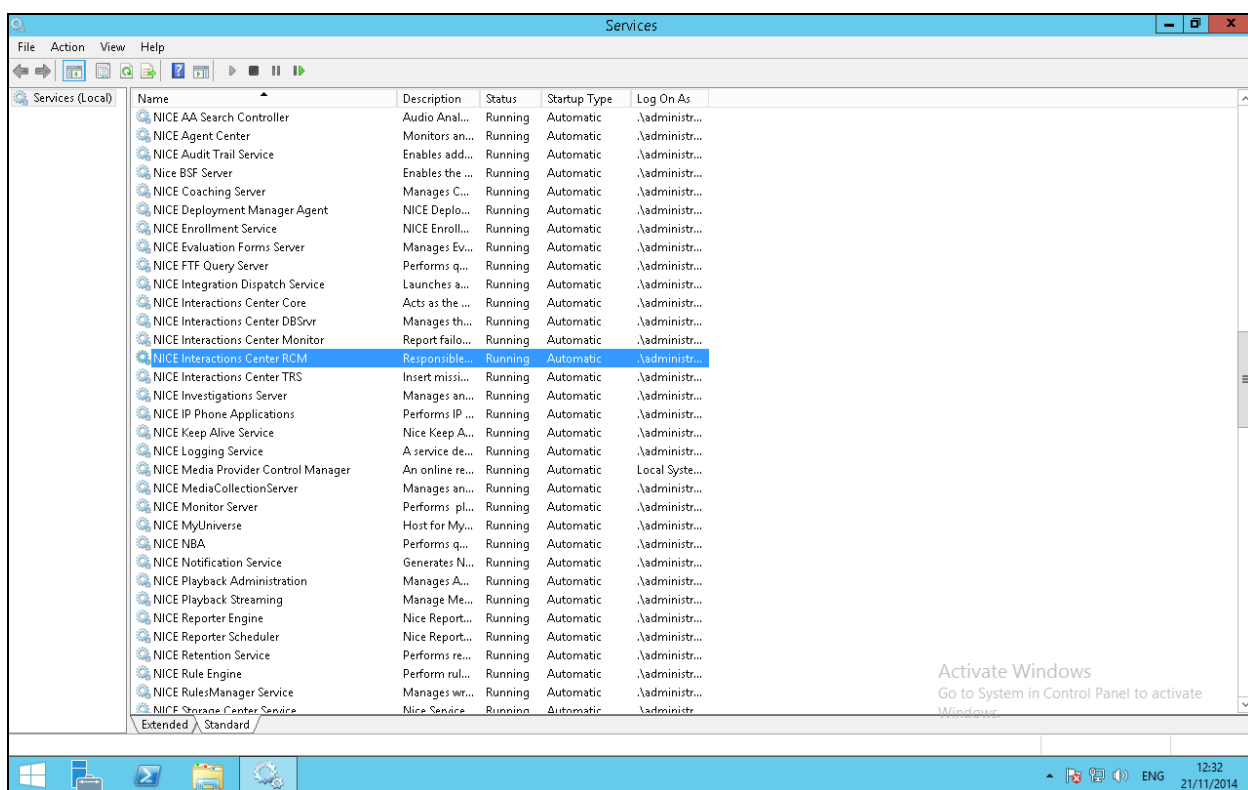
The NICE player is opened and the recording is presented for playback. Click on the **Play/Pause** icon highlighted below to play back the recording.

The screenshot displays the NICE Business Analyzer web application. The main window shows a recording playback interface. At the top, there's a navigation bar with tabs like 'My Universe', 'Business Analyzer', 'Reporter', 'Monitor', 'Insight Manager', 'ClearSight', 'PBO Requests', 'Tools', and 'Administration'. Below this, the 'Interactions' section is active, showing a timeline from 12:41:49 PM to 12:42:08 PM. The timeline includes a waveform and a table of events. The playback control bar at the bottom center has a red square highlighting the Play/Pause button. The table below the timeline lists events with columns for Time, Agent, and other details.

Time	Agent	Event
12:41:49	7101, Avaya 9630 S...	
12:41:52	7100, Avaya 9641 S...	
12:41:56		
12:41:59		
12:42:03		
12:42:08		

10.5. Verify NICE Services

If these recordings are not present or cannot be played back, the NICE services may not be running or may need to be restarted. There are two separate servers as a part of this NICE Engage Platform. The NICE Application Server and the NICE Advanced Interactions Server can be logged into and checked to ensure all services beginning with NICE are running correctly. As a last resort both servers may need a reboot after the initial configuration.



11. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform to successfully interoperate with Avaya Proactive Outreach Manager R3.0, Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0 to connect to using DMCC Multi-Registration to record outbound campaign calls. All feature functionality and serviceability test cases were completed successfully with some observations noted in **Section 2.2**.

12. Additional References

This section references the Avaya and NICE product documentation that are relevant to these Application Notes.

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

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 7.0
- [4] *Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment* Release 7.1 Issue 1
- [5] *Implementing Proactive Outreach Manager* Release 3.0.3 Issue 2
- [6] *Avaya Aura® Contact Centre SIP Commissioning*, Doc # NN44400-511, Release 7.0

Product documentation for NICE products may be found at: <http://www.extranice.com/>

Appendix

Avaya 9608 H.323 Deskphone

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

display station 7000	Page 1 of 5	
STATION		
Extension: 7000	Lock Messages? n	BCC: 0
Type: 9608	Security Code: 1234	TN: 1
Port: S00000	Coverage Path 1:	COR: 1
Name: EXT7000	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 7000	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: yes	
	Customizable Labels? Y	

display station 7000	Page 2 of 5	
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance?	n
LWC Activation? y	Coverage Msg Retrieval?	y
LWC Log External Calls? n	Auto Answer:	none
CDR Privacy? n	Data Restriction?	n
Redirect Notification? y	Idle Appearance Preference?	n
Per Button Ring Control? n	Bridged Idle Line Preference?	n
Bridged Call Alerting? n	Restrict Last Appearance?	y
Active Station Ringing: single		
	EMU Login Allowed?	n
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State:	enabled
Multimedia Mode: enhanced	Audible Message Waiting?	n
MWI Served User Type: sip-adjunct	Display Client Redirection?	n
	Select Last Used Appearance?	n
	Coverage After Forwarding?	s
	Multimedia Early Answer?	n
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections?	y
Emergency Location Ext: 7000	Always Use? n IP Audio Hairpinning?	n

display station 7000 Page 3 of 5

STATION

```

Conf/Trans on Primary Appearance? n
Bridged Appearance Origination Restriction? n    Offline Call Logging? y
Require Mutual Authentication if TLS? n

```

```

Call Appearance Display Format: disp-param-default
IP Phone Group ID:
Enhanced Callr-Info Display for 1-Line Phones? n

```

ENHANCED CALL FORWARDING

				Forwarded Destination	Active
Unconditional For	Internal Calls To:	4980			n
	External Calls To:	4980			n
Busy For	Internal Calls To:	4980			n
	External Calls To:	4980			n
No Reply For	Internal Calls To:	4980			n
	External Calls To:	4980			n

SAC/CF Override: n

display station 7000 Page 4 of 5

STATION

SITE DATA

```

Room:                               Headset? n
Jack:                               Speaker? n
Cable:                             Mounting: d
Floor:                             Cord Length: 0
Building:                           Set Color:

```

ABBREVIATED DIALING

```
List1:      List2:      List3:
```

BUTTON ASSIGNMENTS

```

1: call-appr          5: aux-work      RC:      Grp:
2: call-appr          6: manual-in      Grp:
3: call-appr          7: extnd-call
4: auto-in            Grp:      8:

```

voice-mail

Avaya 9641 SIP Deskphone

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

display station 7100	Page 1 of 6	
STATION		
Extension: 7100	Lock Messages? n	BCC: 0
Type: 9641SIP	Security Code: 1234	TN: 1
Port: S00003	Coverage Path 1: 1	COR: 1
Name: 7100, SIPExt	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Message Lamp Ext: 7100	
Display Language: english	Button Modules: 0	
Survivable COR: internal		
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

display station 7100	Page 2 of 6
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Coverage Msg Retrieval? y
LWC Activation? y	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Per Button Ring Control? n	Idle Appearance Preference? n
Bridged Call Alerting? n	Bridged Idle Line Preference? n
Active Station Ringing: single	Restrict Last Appearance? y
H.320 Conversion? n	Per Station CPN - Send Calling Number?
	EC500 State: enabled
MWI Served User Type: sip-adjunct	
	Coverage After Forwarding? s
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y
Emergency Location Ext: 7100	Always Use? n IP Audio Hairpinning? n

display station 7100Page 3 of 6

STATION

Bridged Appearance Origination Restriction? n Offline Call Logging? y

IP Phone Group ID:

ENHANCED CALL FORWARDING

	Forwarded Destination	Active
Unconditional For Internal Calls To:		n
External Calls To:		n
Busy For Internal Calls To:	95120	y
External Calls To:	95120	y
No Reply For Internal Calls To:		n
External Calls To:		n

SAC/CF Override: n

display station 7100Page 4 of 6

STATION

SITE DATA

Room:	Headset? n
Jack:	Speaker? n
Cable:	Mounting: d
Floor:	Cord Length: 0
Building:	Set Color:

ABBREVIATED DIALING

List1:	List2:	List3:
--------	--------	--------

BUTTON ASSIGNMENTS

1: call-appr	5: call-fwd	Ext:
2: call-appr	6:	
3: call-park	7:	
4: extnd-call	8:	

display station 7100Page 6 of 6

STATION

SIP FEATURE OPTIONS

Type of 3PCC Enabled: Avaya

SIP Trunk: aar

Enable Reachability for Station Domain Control: s

©2017 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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