



Application Notes for configuring NICE Engage Platform R6.4 to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 using DMCC Service Observation and Single Step Conference - 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 Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0.

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 R6.4 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0. NICE Engage Platform uses Communication Manager's Service Observation feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording on various Communication Manager endpoints, listed in **Section 4**.

Device Media Call Control (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 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 .NET framework and can be used to retrieve telephone conversations from a comprehensive long-term calls database. The NICE Engage Platform uses the Communication Manager feature "Service Observe" to observe a call on an extension; this way the call is recorded and can be played back at a later time. NICE can also conference into the call and record the call using this method. Both methods of call recording use virtual stations on Communication Manager in order to observe or conference into existing calls to record them.

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 in a variety of scenarios using DMCC Service Observation and Single Step Conference with AES and Communication Manager. A range of Avaya endpoints were used in the compliance testing all of which are listed in **Section 4**.

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:

- **Inbound/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **EC500 Calls/Forwarded calls** - Test call recording for calls terminated on Avaya DECT handsets using EC500.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park and Call Pickup.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into one-X® Agent.
- **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. **Conference Call** - An issue arises when using Single Step Conference with Virtual Extensions for NICE call recording for this specific scenario.
 - An unmonitored set calls to a monitored set A.
 - Monitored set A initiates a conference to another monitored set B. (At this point, there are two calls, each with a VE).
 - Monitored set A completes the conference. The recorder drops VE2 and only VE1 remains in the call.
 - Monitored set A drops out of the call, leaving the unmonitored set and monitored set B talking to each other. The recorder drops VE1 and tries to SSC VE2 into the call.
 - The SSC in step 4 does not happen. CM just seems to ignore the SSC request from AES. VE2 is not added to the call and CM does not respond to AES - there is no confirm or failure response. This causes AES to block further TSAPI requests for VE2 until sometime later.

A fix for this issue will be included in CM 7.0.0.3.0 SP (patch 22722), which (as of now) has a GA date of Feb 8th 2016.

2. **Call Park**. The un-parked call is not being recorded. It appears that there are no events being sent for un-parking a call by Communication Manager. Modification Report [**CM-9860**] has been raised with the Communication Manager support team. A fix for this issue will be implemented for release 7.1 of Communication Manager.

Note: When configured for total recording, the un-parked call should be recorded and the call record should appear once Total Recording Service picks up the session.

2.3. Support

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

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Engage Platform with the Avaya solution using DMCC Service Observe and Single Step Conference to record calls. The NICE Application Server is setup for DMCC Service Observe and Single Step Conference mode and connects to the AES.

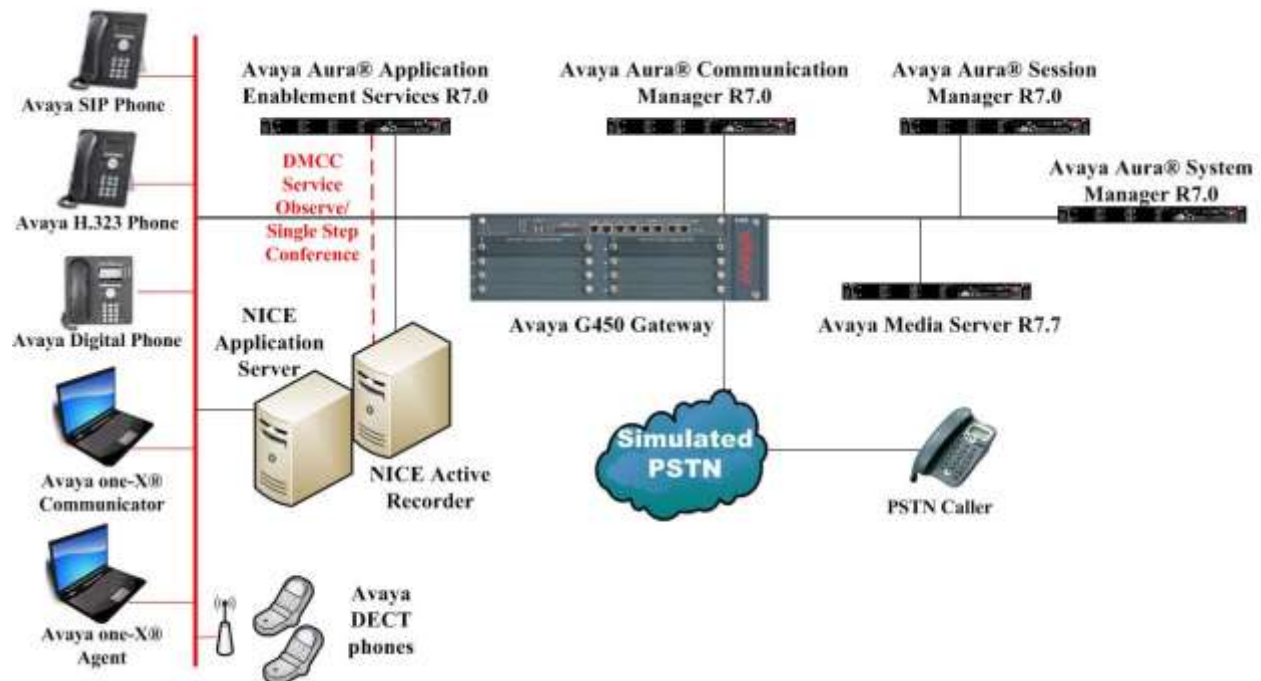


Figure 1: Connection of NICE Engage Platform R6.4 with Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager R7.0 and Avaya Aura® Application Enablement Services R7.0

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 Virtual Server	R7.0.0.0.0 Build 7.0.0.0.16266-7.0.9.9.902 SW Update Revision No. 7.0.0.0.3873
Avaya Aura® Session Manager running on Virtual Server	R7.0.0.0.700007
Avaya Aura® Communication Manager running on Virtual Server	R7.0 Build 017x.00.0.441.0.22477
Avaya Aura® Application Enablement Services running on Virtual Server	R7.0 Build No – 7.0.0.0.0.13-0
Avaya G450 Gateway	37.19.0 /1
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 6.5.0.17
Avaya 9630 SIP Deskphone	R2.6.13.1
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Avaya one-X® Agent	R 2.5.50022.0
Avaya 9408 Digital Deskphone	FW Version 2
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
NICE Engage Platform <ul style="list-style-type: none">- Application Server- Advanced Interactions Recorder	R6.4

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 10**.

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 note 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		
aes63vmpg	10.10.40.16		
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 Communication Manager for Service Observation

Type **display cor x**, where x is the COR number in the screen above, to check the existing Class of Restriction. Ensure that **Can be Service Observed** is set to **y**, if not type **change cor x** to make a change to the Class or Restriction. This value needs to be enabled in order for Service Observe to work for call recording.

```
display cor 1                                     Page 1 of 23
                                     CLASS OF RESTRICTION
COR Number: 1
COR Description:

FRL: 0                                           APLT? y
Can Be Service Observed? y                   Calling Party Restriction: all-toll
Can Be A Service Observer? y                   Called Party Restriction: none
Time of Day Chart: 1                           Forced Entry of Account Codes? n
Priority Queuing? n                             Direct Agent Calling? y
Restriction Override: all                       Facility Access Trunk Test? n
Restricted Call List? n                         Can Change Coverage? n
Unrestricted Call List: 1
Access to MCT? y                               Fully Restricted Service? n
Group II Category For MFC: 7                   Hear VDN of Origin Annc.? n
Send ANI for MFE? n                           Add/Remove Agent Skills? n
MF ANI Prefix:                               Automatic Charge Display? n
Hear System Music on Hold? y PASTE (Display PBX Data on Phone)? n
Can Be Picked Up By Directed Call Pickup? y
Can Use Directed Call Pickup? y
Group Controlled Restriction: inactive
```

Type **change system-parameters features**, on **Page 11** ensure that **Allow Two Observes in Same Call** is set to **y**.

```
change system-parameters features                Page 11 of 19
                                     FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
EAS
Expert Agent Selection (EAS) Enabled? y
Minimum Agent-LoginID Password Length:
Direct Agent Announcement Extension:            Delay:
Message Waiting Lamp Indicates Status For: station

VECTORIZING
Converse First Data Delay: 0                    Second Data Delay: 2
Converse Signaling Tone (msec): 100             Pause (msec): 70
Prompting Timeout (secs): 10
Interflow-qpos EWT Threshold: 2
Reverse Star/Pound Digit For Collect Step? n
Available Agent Adjustments for BSR? n
BSR Tie Strategy: 1st-found
Store VDN Name in Station's Local Call Log? n
SERVICE OBSERVING
Service Observing: Warning Tone? y              or Conference Tone? n
Service Observing/SSC Allowed with Exclusion? n
Allow Two Observers in Same Call? y
```


Type **change feature-access-codes** to access the feature codes on Communication Manager. Scroll to **Page 5** in order to view or change the **Service Observing** access codes. Note the **Service Observing Listen Only Access Code** is **#43**; this will be required in **Section 7.1** during the setup of NICE Engage Platform.

change feature-access-codes	Page 5 of 10
FEATURE ACCESS CODE (FAC)	
Call Center Features	
AGENT WORK MODES	
After Call Work Access Code:	#36
Assist Access Code:	
Auto-In Access Code:	#38
Aux Work Access Code:	#39
Login Access Code:	#40
Logout Access Code:	#41
Manual-in Access Code:	#42
SERVICE OBSERVING	
Service Observing Listen Only Access Code:	#43
Service Observing Listen/Talk Access Code:	#44
Service Observing No Talk Access Code:	
Service Observing Next Call Listen Only Access Code:	
Service Observing by Location Listen Only Access Code:	
Service Observing by Location Listen/Talk Access Code:	
AACC CONFERENCE MODES	
Restrict First Consult Activation:	Deactivation:
Restrict Second Consult Activation:	Deactivation:

5.6. Configure H323 Stations for Service Observation

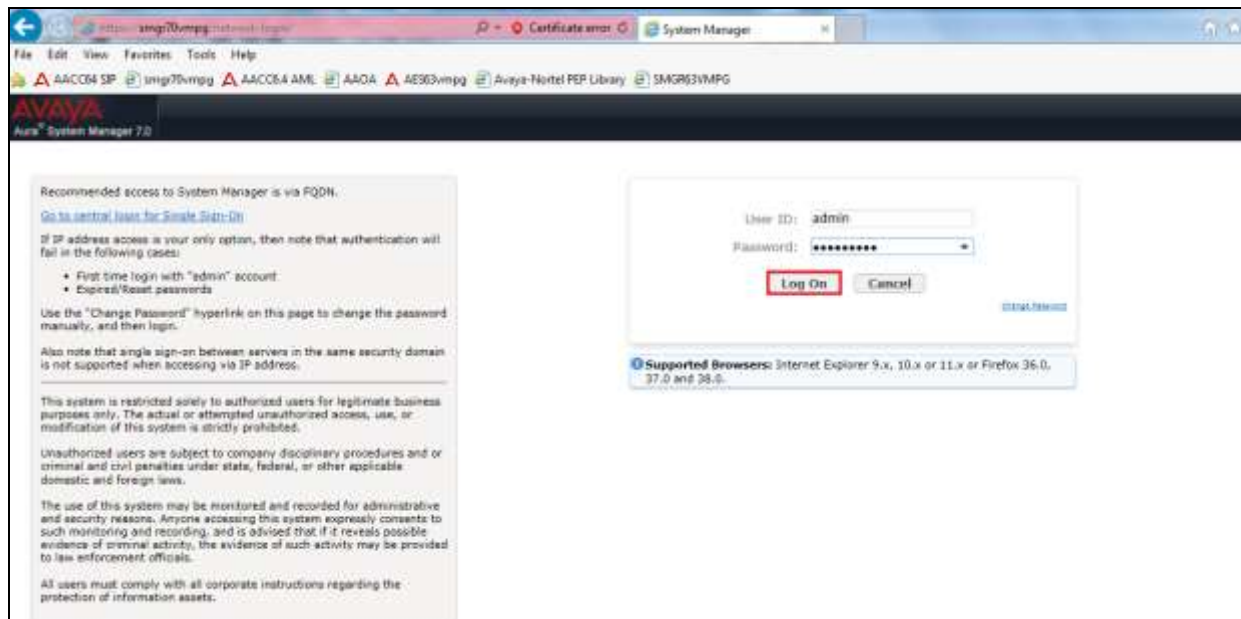
All endpoints that are to be monitored by NICE will need to have IP Softphone set to y. IP Softphone must be enabled in order for DMCC Service Observe and Single Step Conference to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required in **Section 7.1**. 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
Type: 9608	Security Code: 1234
Port: S00101	Coverage Path 1:
Name: Extension	Coverage Path 2:
	Hunt-to Station:
STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
Speakerphone: 2-way	Personalized Ringing Pattern: 1
Display Language: english	Message Lamp Ext: 1591
Survivable GK Node Name:	Mute Button Enabled? y
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? y
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default

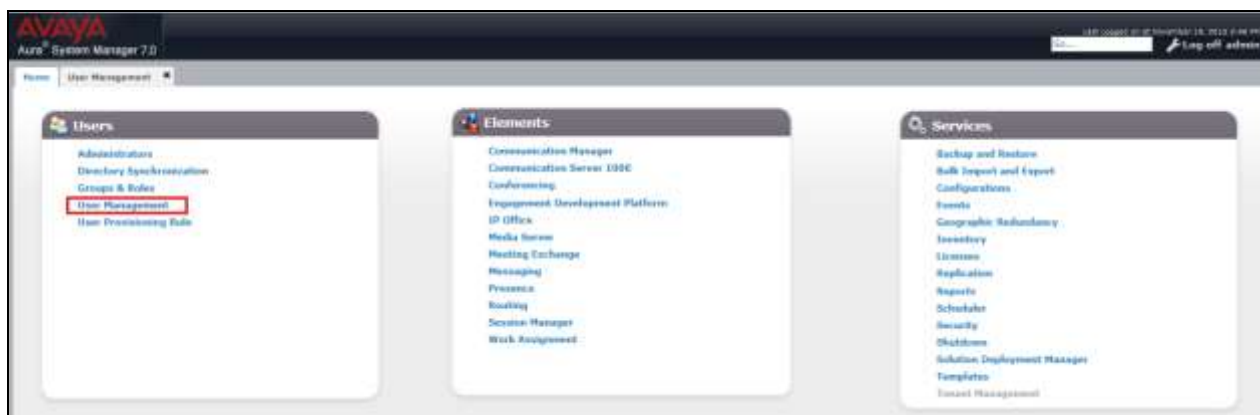
5.7. Configure SIP Stations for Service Observation

Any SIP extension that is to be recorded requires some configuration changes to allow call recording using service observation. 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 a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



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

Search

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

Commit & Continue Commit Cancel

Identity Communication Profile Relationship Contacts

Communication Profile

Communication Profile Password: [REDACTED]

New Cancel

Name: Primary

Select: None

Name: Primary

Default: ☒

Communication Address

New Cancel

Type	Handle	Domain
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. Also that the **Class of Restriction (COR)** is set to that configured in **Section 5.5**.

Edit Endpoint

System: cm70vmpg Extension: 7100
 Template: 9641SIPCC_DEFAULT_CM_7_8 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 Feed (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

* Class of Restriction (COR): 1
 * Emergency Location Ext: 7100
 * Tenant Number: 1
 * SIP Trunk: aar
 Coverage Path 1:
 Lock Message: ☐
 Multibyte Language: Not Applicable

* Class Of Service (COS): 1
 * Message Lamp Ext.: 7100
 Type of 3PCC Enabled: Avaya
 Coverage Path 2:
 Localized Display Name: 7100, SIPExt
 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 Feed (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

Active Station Ringing: single
 MWI Served User Type: signalled
 Per Station CPN - Send Calling Number: none
 IP Phone Group ID:
 Remote Soft Phone Emergency Calls: aar-on-local
 LWC Reception: xps
 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

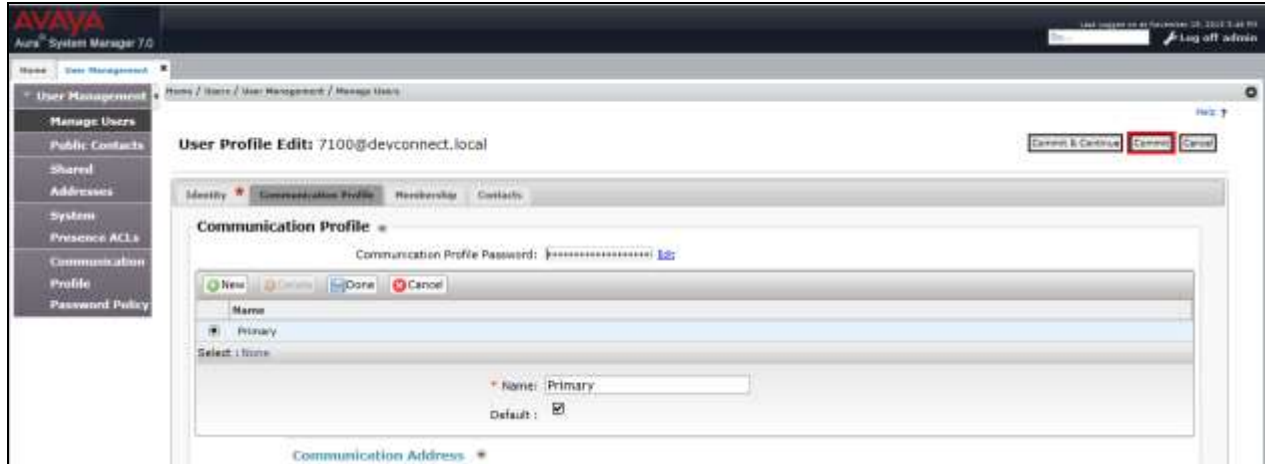
☐ Always Use
☐ IP Audio Hairpinning
☐ Bridged Call Alerting
☐ Bridged Idle Line Preference
☒ Coverage Message Retrieval
☐ Data Restriction
☒ Survivable Trunk Dest
☐ Bridged Appearance Origination Restriction
☒ Restrict Last Appearance

☐ Idle Appearance Preference
☒ IP SoftPhone
☒ LWC Activation
☐ CDR Privacy
☒ Direct IP-IP Audio Connections
☐ H.323 Conversion
☐ IP Video Softphone
☐ Per Button Ring Control

* Required

Done Cancel

Click on **Commit** once this is done to save the changes.



5.8. Configure Virtual Stations for Single Step Conference and Service Observation

Add virtual stations to allow NICE Engage Platform record calls using Single Step Conference and Service Observe. Type **add station x** where x is the extension number of the station to be configured also note this extension number for configuration required in **Section 7.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**. Note also the **COR** for the stations, this will be set to that configured in **Section 5.5**.

```
add station 28902                                     Page 1 of 6

                                STATION

Extension: 28902                                         Lock Messages? n          BCC: 0
  Type: 4624                                           Security Code: 1234       TN: 1
  Port: S00101                                         Coverage Path 1:         COR: 1
  Name: Recorder                                       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: 28902
      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
```

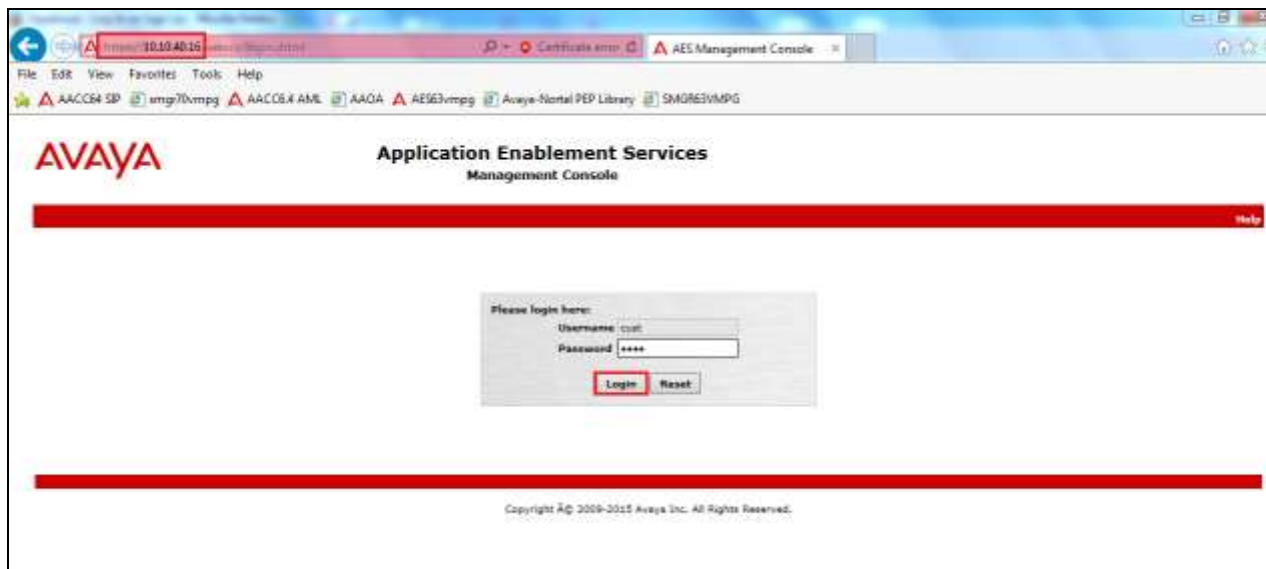
6. Configure Avaya Aura® Application Enablement Services

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

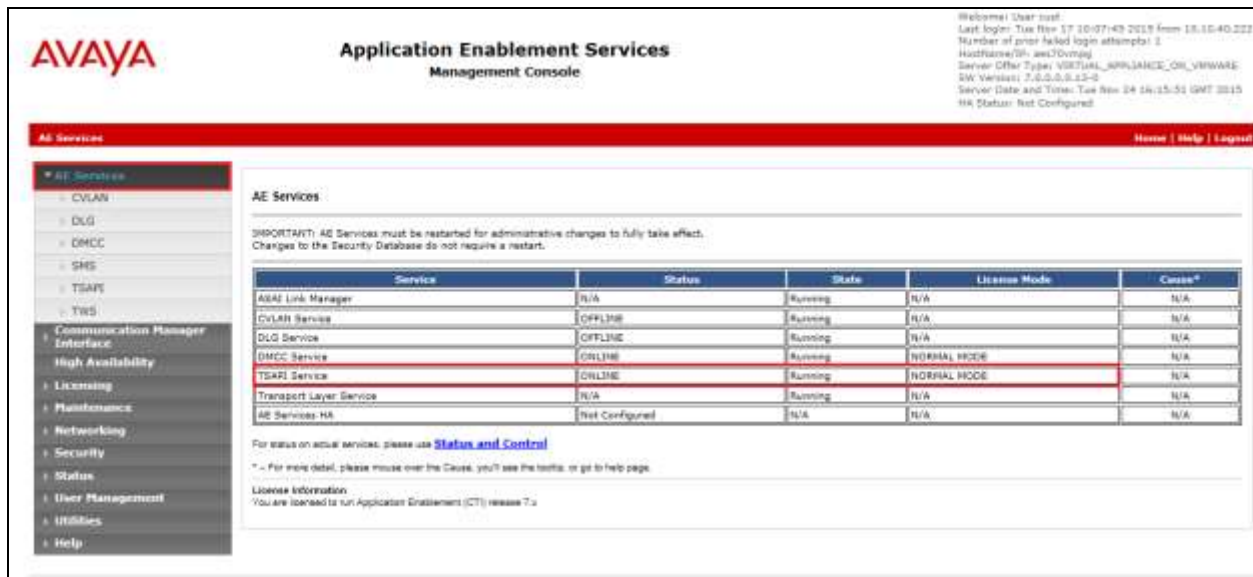
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI and DMCC Ports
- Create CTI User
- Set Up Security Database on AES
- Associate Devices with CTI User

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: root
Last login: Tue Nov 17 10:37:45 2015 from 10.10.40.222
Number of prior failed login attempts: 1
HostName/IP: aes70vmg
Server Offer Type: VIRTUAL_APLIANCE_ON_VMWARE
SW Version: 7.0.0.0.13-0
Server Date and Time: Tue Nov 24 16:15:51 GMT 2015
HA Status: Not Configured

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*
ASAE 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	NORMAL MODE	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 (CT) release 7.0

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: root
Last login: Tue Nov 17 10:37:45 2015 from 10.10.40.222
Number of prior failed login attempts: 1
HostName/IP: aes70vmg
Server Offer Type: VIRTUAL_APLIANCE_ON_VMWARE
SW Version: 7.0.0.0.13-0
Server Date and Time: Tue Nov 24 16:16:56 GMT 2015
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Switch Connections

Enter Name: **Add Connection**

Connection Name	Processor Ethernet	Plug Period	Number of Active Connections
Edit Connection Edit PE/CLAN 3ds 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.

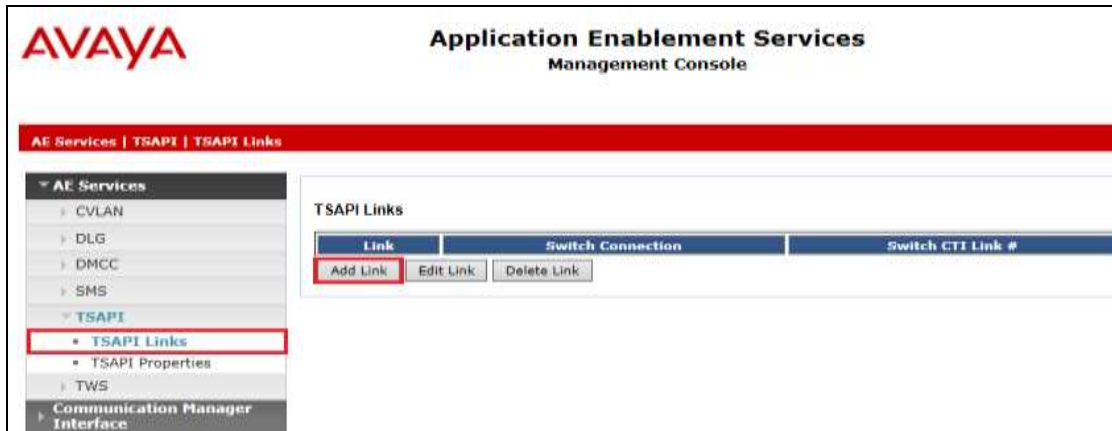
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface (selected), Switch Connections (highlighted with a red box), Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Connection Details - cm70vmpg' 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 - cm70vmpg' and contains a table with the following columns: Name or IP Address. The table has one row with the value '10.10.40.13'. The 'Add/Edit Name or IP' button is highlighted with a red box. There is also a 'Back' button at the bottom left of the table.

6.3. Administer TSAPI link

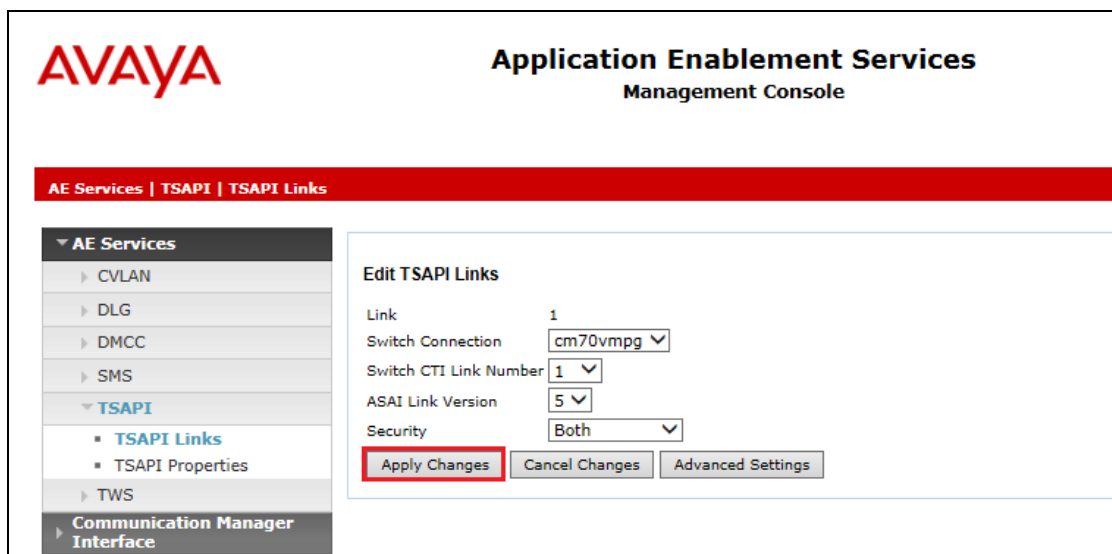
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



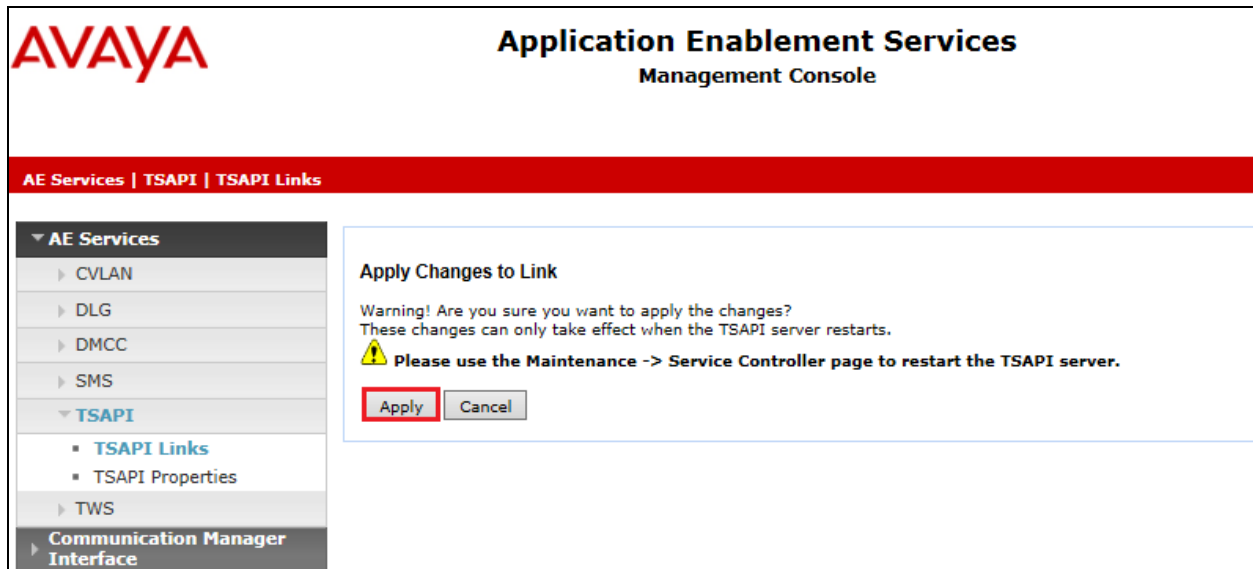
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm70vmppg**, 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**.

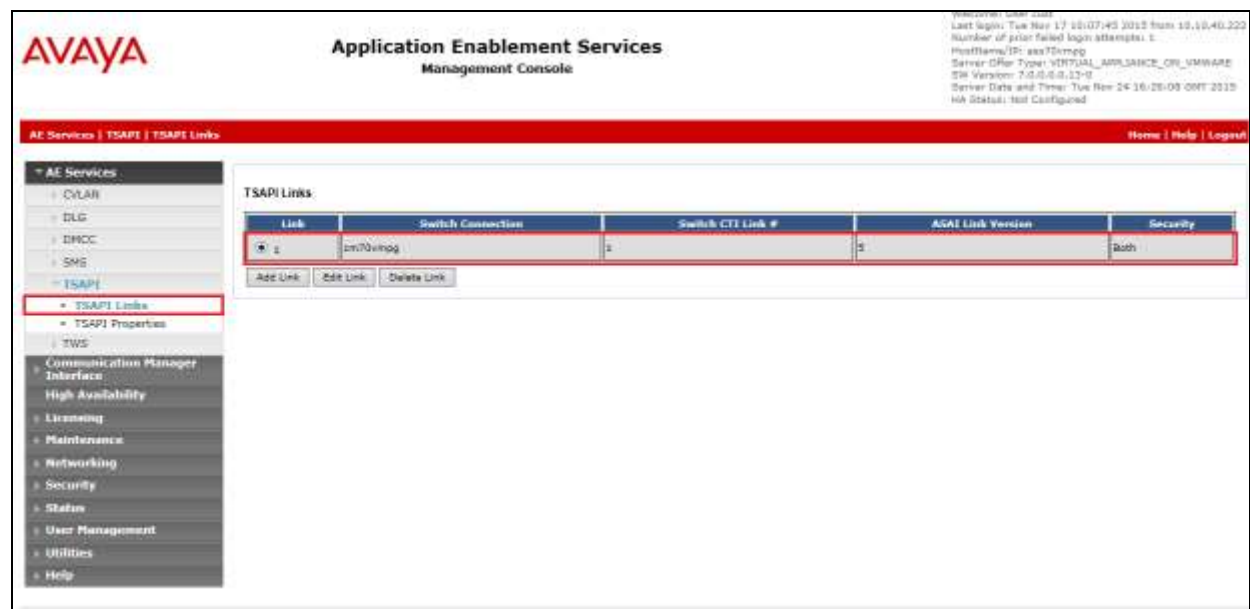
Once completed, select **Apply Changes**.



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



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



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

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. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the NICE Engage Platform in **Section 7.1**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". Below this is a red navigation bar with the text "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security section is expanded, showing sub-items like Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, CTI Users, Devices, Device Groups, Tlinks, Tlink Groups, and Worktops. The "Tlinks" item is highlighted with a red box. The main content area on the right is titled "Tlinks" and contains a "Tlink Name" section. It shows two radio button options: "AVAYA#CM70VMPPG#CSTA#AES70VMPPG" (selected) and "AVAYA#CM70VMPPG#CSTA-S#AES70VMPPG". A "Delete Tlink" button is also present. The selected Tlink name is also highlighted with a red box.

6.5. 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 7.1**.

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

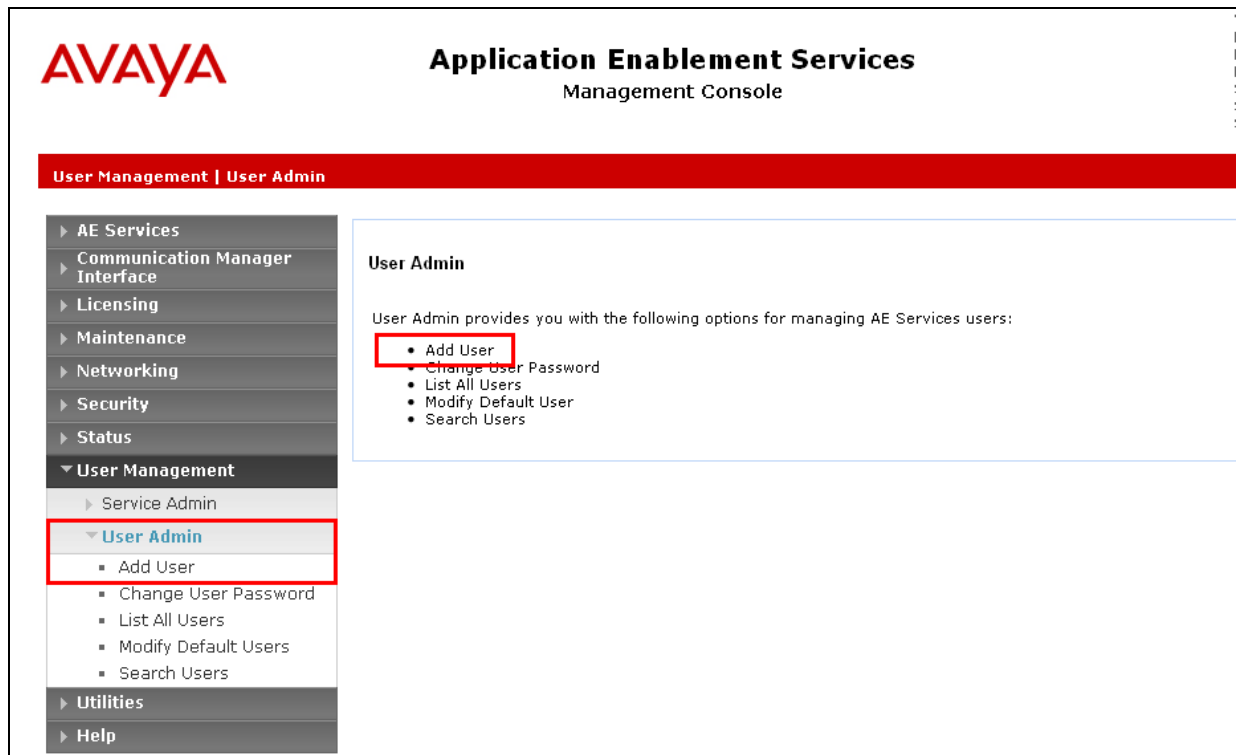
		Enabled Disabled
TSAPI Service Port	450	<input checked="" type="radio"/> <input type="radio"/>
Local TLINK Ports		
TCP Port Min	1024	
TCP Port Max	1039	
Unencrypted TLINK Ports		
TCP Port Min	<input type="text" value="1050"/>	
TCP Port Max	<input type="text" value="1065"/>	
Encrypted TLINK Ports		
TCP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

6.6. 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 7.1**.
- **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 7.1**.
- **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	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	

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

The screenshot displays a web-based user administration interface. On the left, a sidebar menu contains the following items: 'User Admin' (selected), 'Add User', 'Change User Password', 'List All Users', 'Modify Default Users', 'Search Users', 'Utilities', and 'Help'. The main content area is titled 'User Admin' and contains a form with the following fields: 'CM Home', 'Cas Home', 'CT User' (with a dropdown menu showing 'Yes'), 'Department Number', 'Display Name', 'Employee Number', 'Employee Type', 'Enterprise Handle', 'Given Name', 'Home Phone', 'Home Postal Address', 'Initials', 'Labeled URI', 'Mail', 'MM Home', 'Mobile', 'Organization', 'Pager', 'Preferred Language' (with a dropdown menu showing 'English'), 'Room Number', and 'Telephone Number'. At the bottom of the form, there are two buttons: 'Apply Changes' (highlighted with a red box) and 'Cancel Changes'.

6.7. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit Users**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'Security' expanded, showing 'CTI Users' and 'List All Users' (highlighted with a red box). The main content area displays a table of CTI Users. The 'nice' user is selected, and the 'Edit' button is highlighted with a red box.

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

Buttons: **Edit** (highlighted), **List All**

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 'Unrestricted Access' checkbox is checked and highlighted with a red box. The 'Apply Changes' button is also highlighted with a red box.

Section	Field	Value
User Profile:	User ID	nice
	Common Name	nice
	Worktop Name	NONE
Call and Device Control:	Call Origination/Termination and Device Status	NONE
	Device Monitoring	NONE
Call and Device Monitoring:	Calls On A Device Monitoring	NONE
	Call Monitoring	
Routing Control:	Allow Routing on Listed Devices	NONE

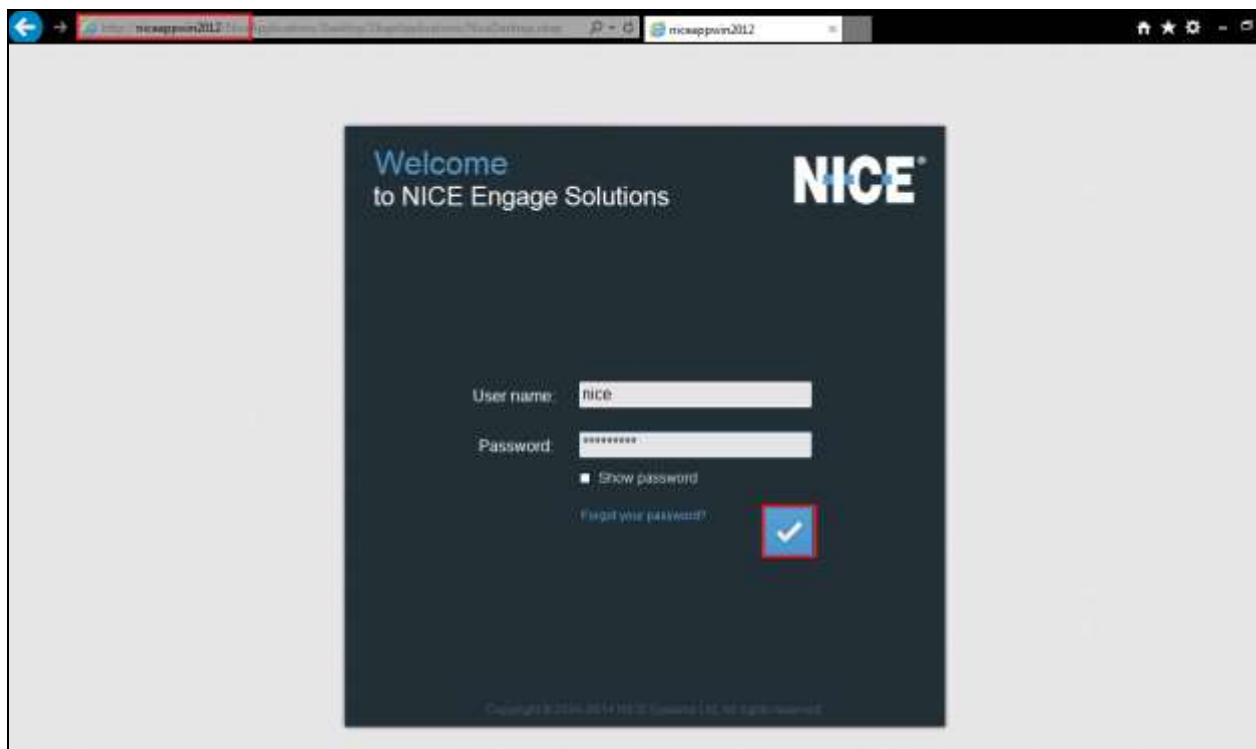
Buttons: **Apply Changes** (highlighted), **Cancel Changes**

7. Configure NICE Engage Platform

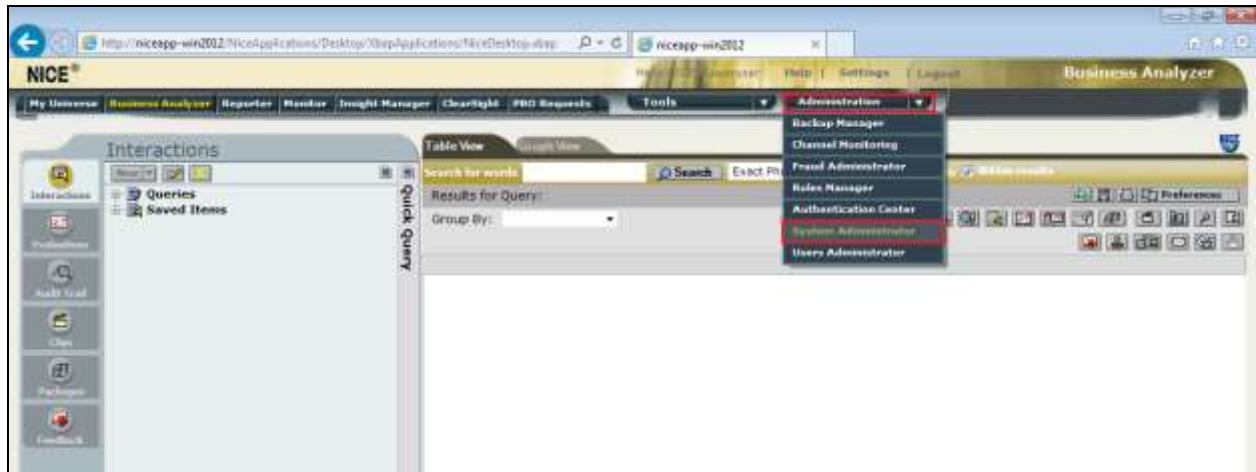
The installation of NICE Engage Platform is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of the NICE Engage Platform contact NICE as per the information provided in Section 2.3.

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

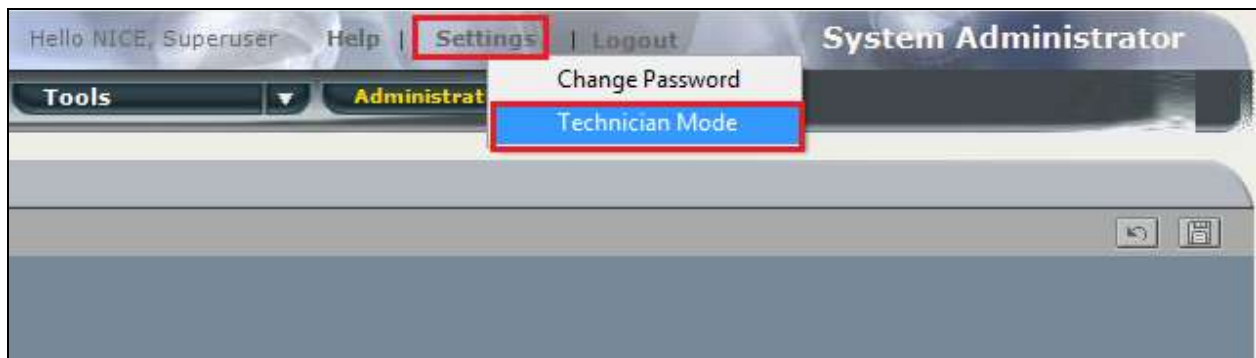
http://<NICEEngageApplicationServerIP>/Nice as shown below and enter the proper credentials and click on **Login**.



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

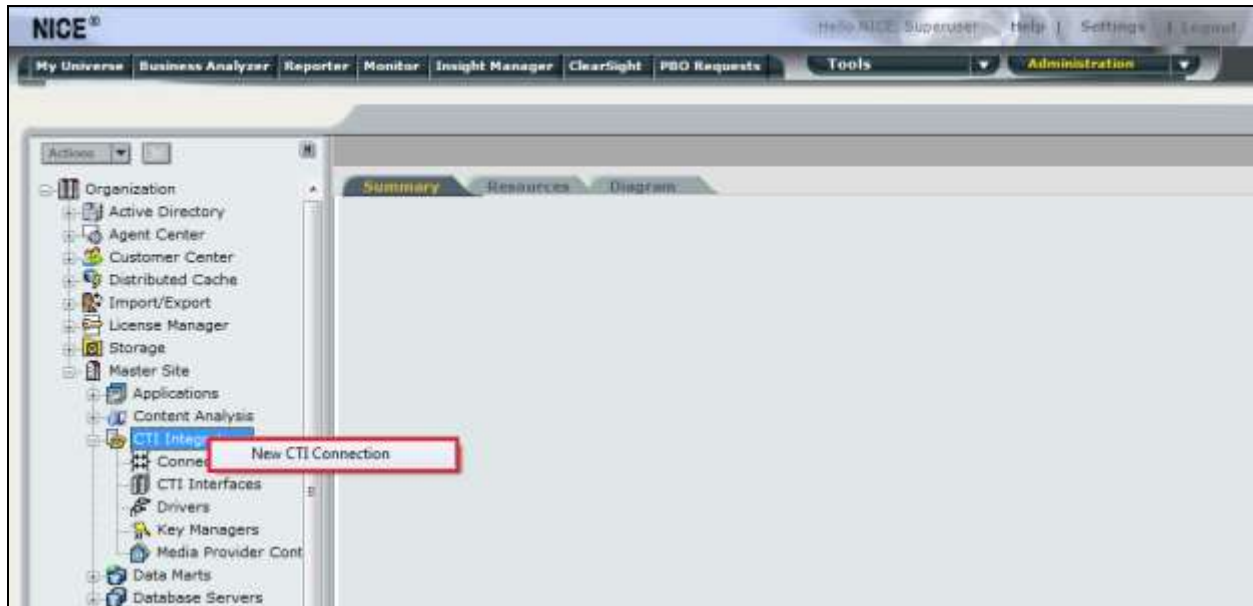


Before any changes can be made, switch to **Technician Mode** by clicking into **Settings** at the top of the screen as shown below.

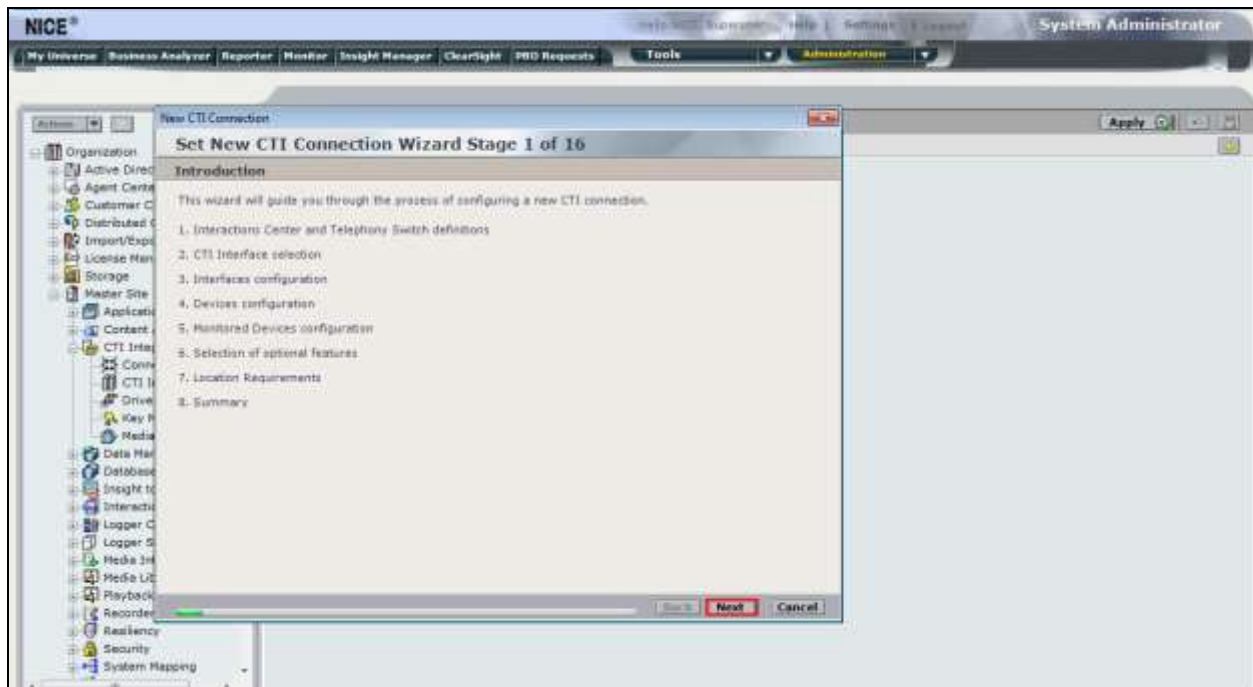


7.1. New CTI Connection

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 16 steps required to setup the connection to the AES for DMCC Service Observe and Single Step Conference type of call recording. Click on **Next** to continue.

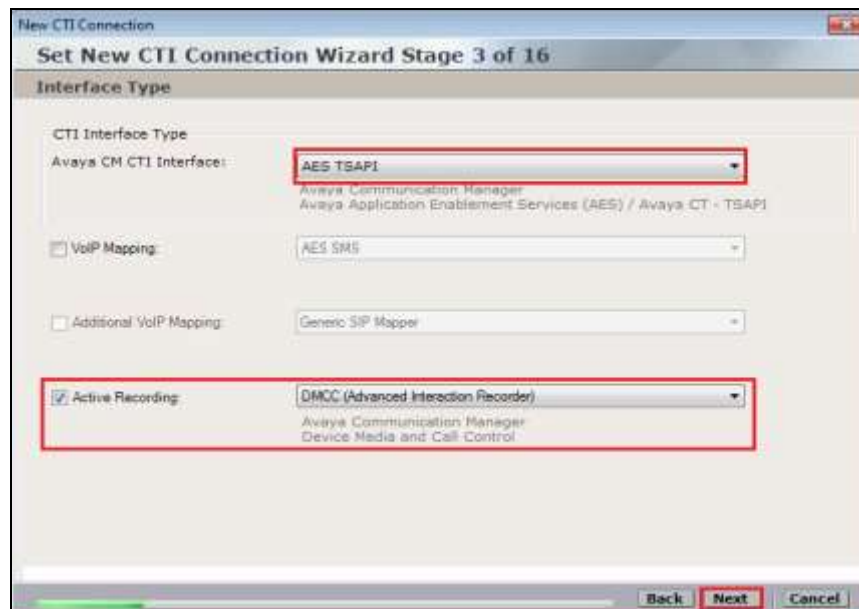


The value for **Regular Interactions Center (IC)** is a value that was already created during the installation of the NICE Engage platform. This value is therefore pre-chosen for the CTI connection being created below.

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.



Select **AES TSAPI** 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.



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

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 16

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	
LoginID	
Password	
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

Back Next Cancel

Double-click on **ServerName** and enter the TSAPI link **Value** from **Section 6.4**.

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 16

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	
LoginID	
Password	
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

Back Next Cancel

Set Parameter Value

Interface Connection Parameter

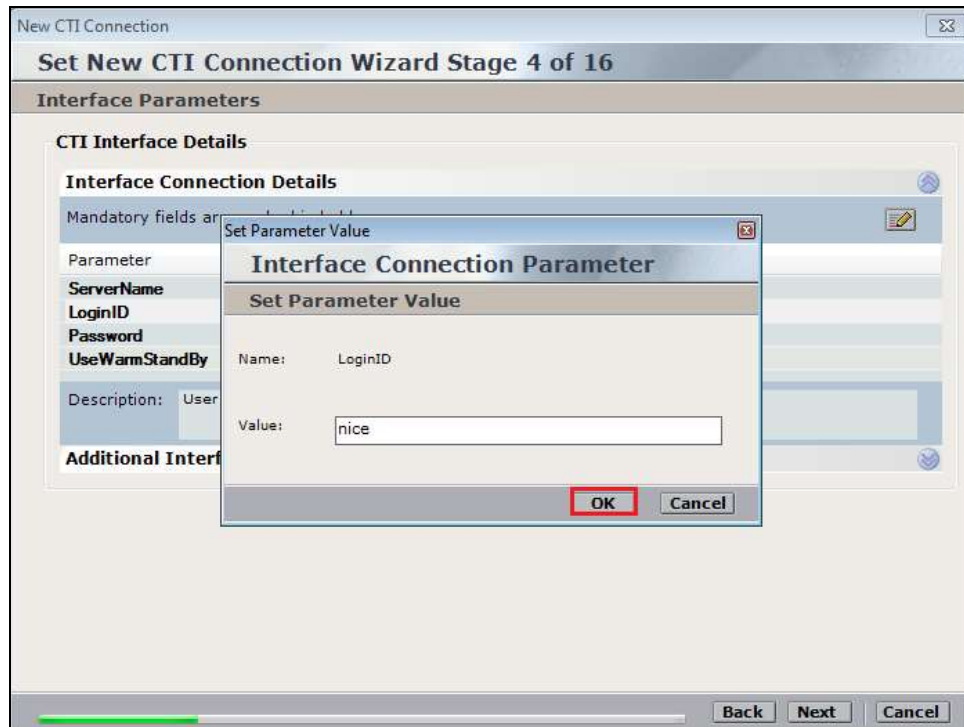
Set Parameter Value

Name: ServerName

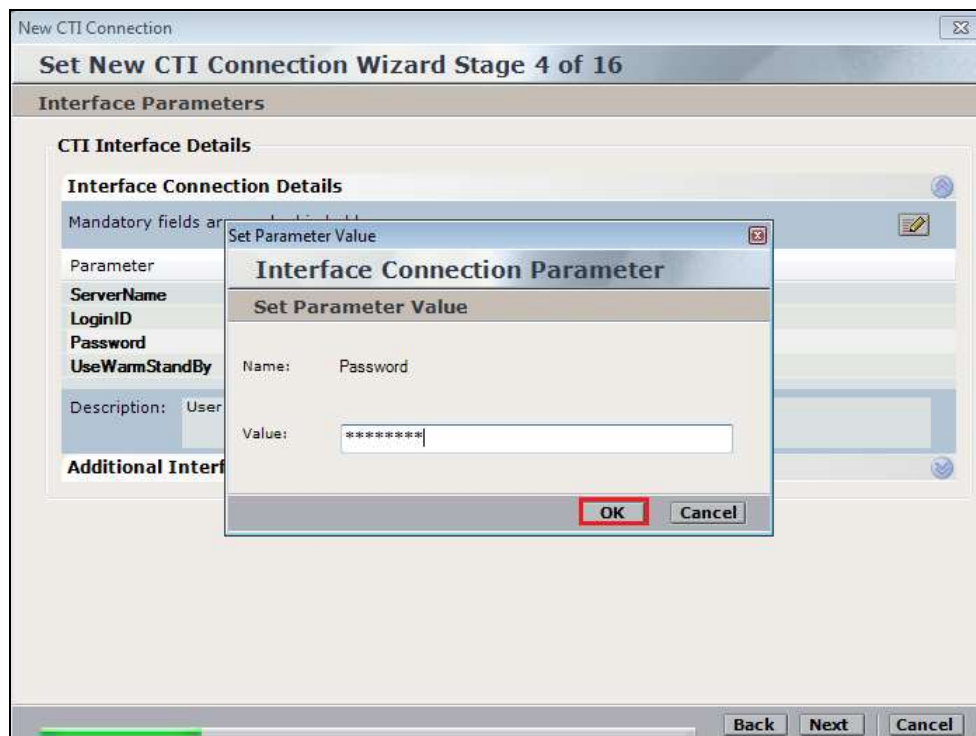
Value: AVAYA#CM70VMGP#CSTA#AES70VMGP

OK Cancel

Double-click on LoginID and enter the username that was created in **Section 6.6**. Click on **OK**.



Double-click on password and enter the value for the password that was created in **Section 6.6**.



Click on **Next** once these values are all filled in.

The screenshot shows the 'Set New CTI Connection Wizard Stage 4 of 16' window. The 'Interface Parameters' section is active. Under 'CTI Interface Details', the 'Interface Connection Details' table is shown. The table has two columns: 'Parameter' and 'Value'. The parameters listed are: 'ServerName' (AVAYA#CM70VMPG#CSTA#AES70VMPG), 'LoginID' (nice), 'Password' (*****), and 'UseWarmStandBy' (No). The 'UseWarmStandBy' row is highlighted in blue. Below the table, there is a 'Description' field with the text 'Is warm standby supported?'. At the bottom of the window, there are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red box.

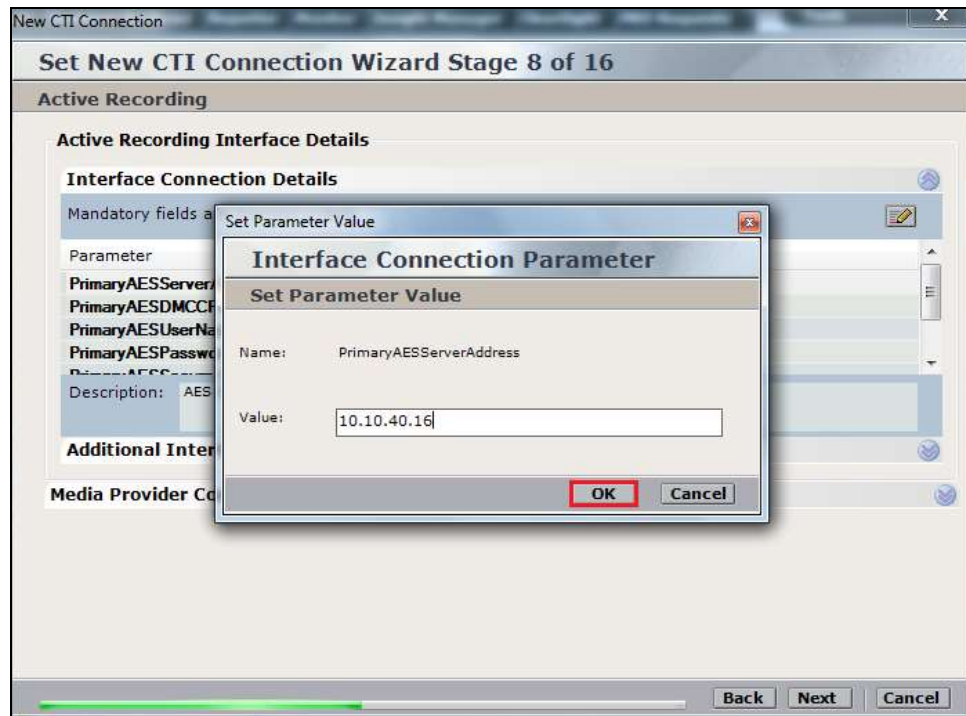
Parameter	Value
ServerName	AVAYA#CM70VMPG#CSTA#AES70VMPG
LoginID	nice
Password	*****
UseWarmStandBy	No

The values below must be filled in by double-clicking on each **Parameter**.

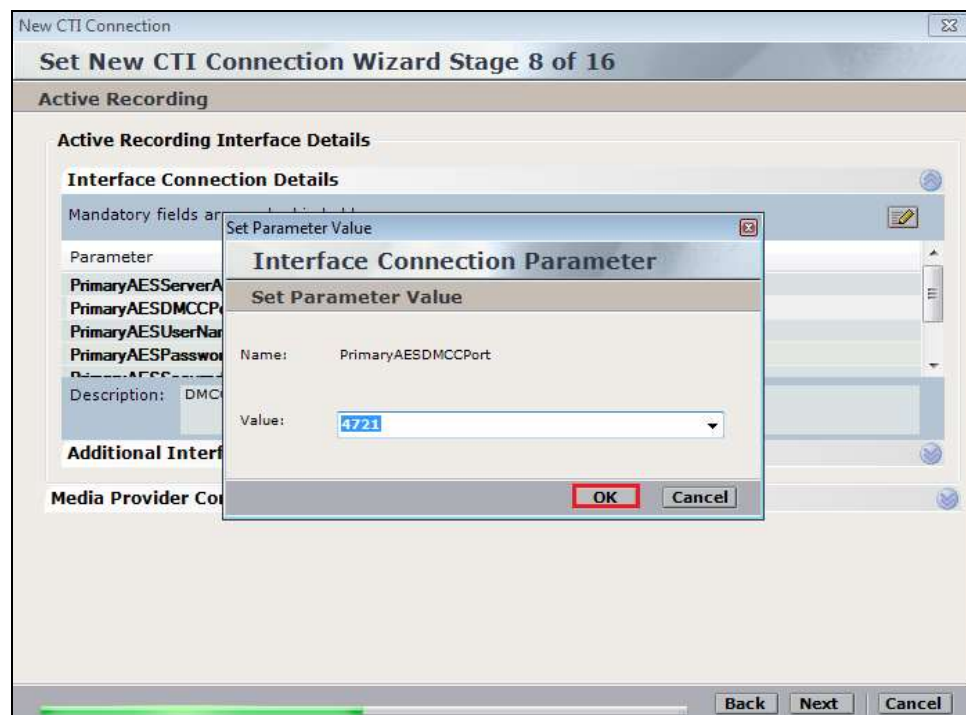
The screenshot shows the 'Set New CTI Connection Wizard Stage 8 of 16' window. The 'Active Recording' section is active. Under 'Active Recording Interface Details', the 'Interface Connection Details' table is shown. The table has two columns: 'Parameter' and 'Value'. The parameters listed are: 'PrimaryAESServerAddress', 'PrimaryAESDMCCPort' (4722), 'PrimaryAESUserName', 'PrimaryAESPassword', and 'PrimaryAESSendConnection' (TRUE). The 'PrimaryAESSendConnection' row is highlighted in blue. Below the table, there is a 'Description' field. At the bottom of the window, there are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red box.

Parameter	Value
PrimaryAESServerAddress	
PrimaryAESDMCCPort	4722
PrimaryAESUserName	
PrimaryAESPassword	
PrimaryAESSendConnection	TRUE

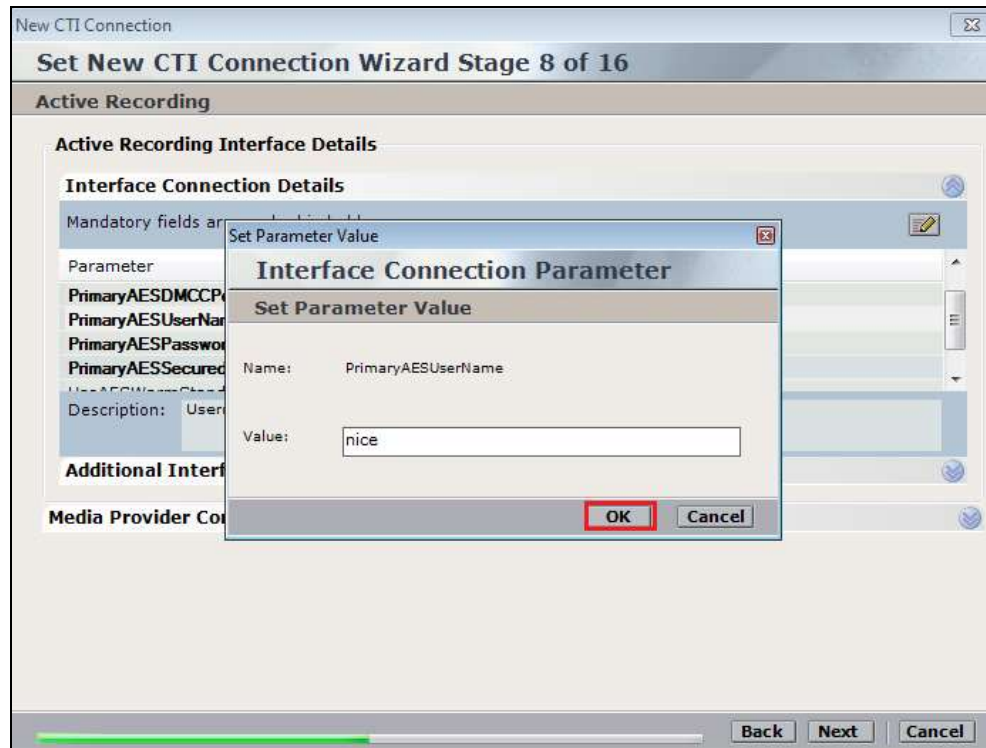
Enter the **Value** for the **AESServerAddress**, note this is the IP address of the AES server. Click on **OK**.



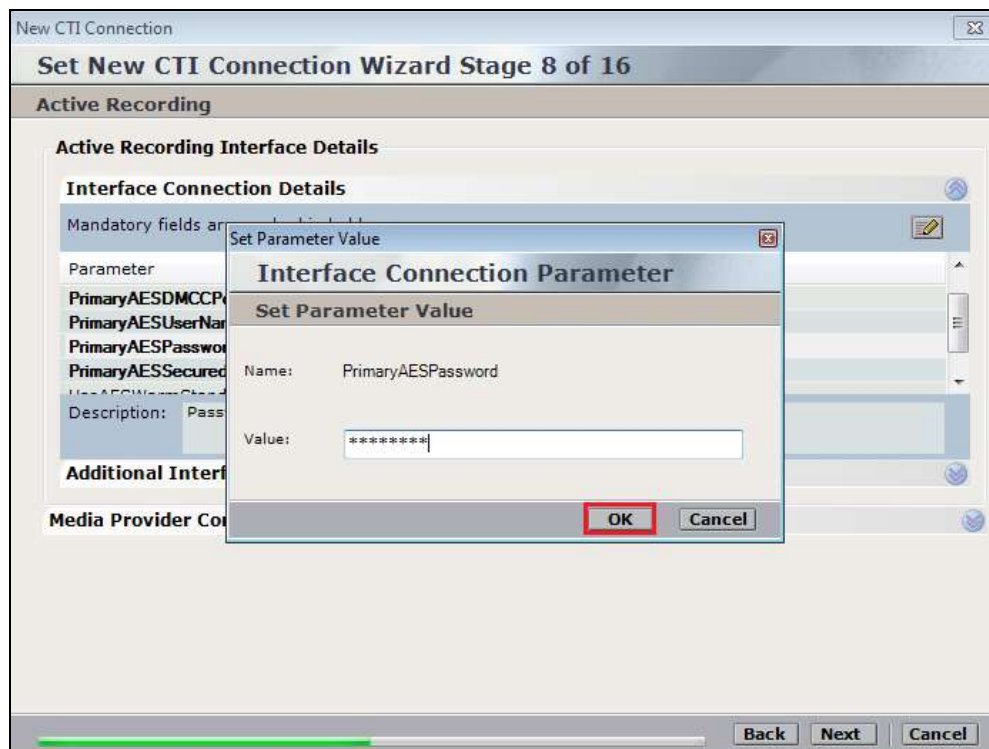
Enter the **Value** for the **AESDMCCPort**, note this will be the same port that was configured in **Section 6.5**. In this example the unencrypted port **4721** is entered.



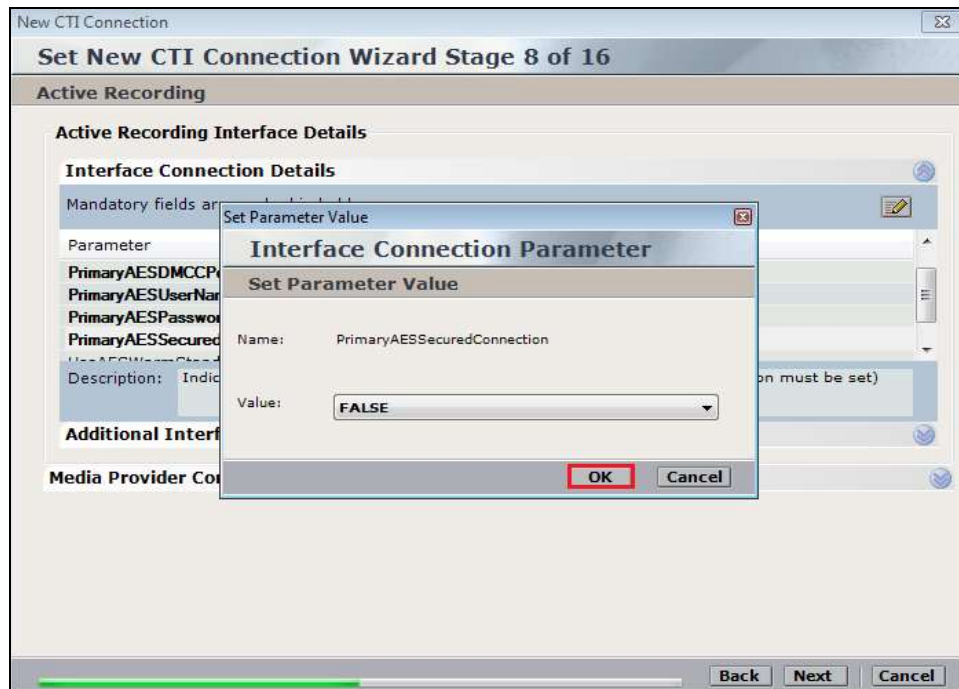
As before enter the username that was created in **Section 6.6** and click on **OK**.



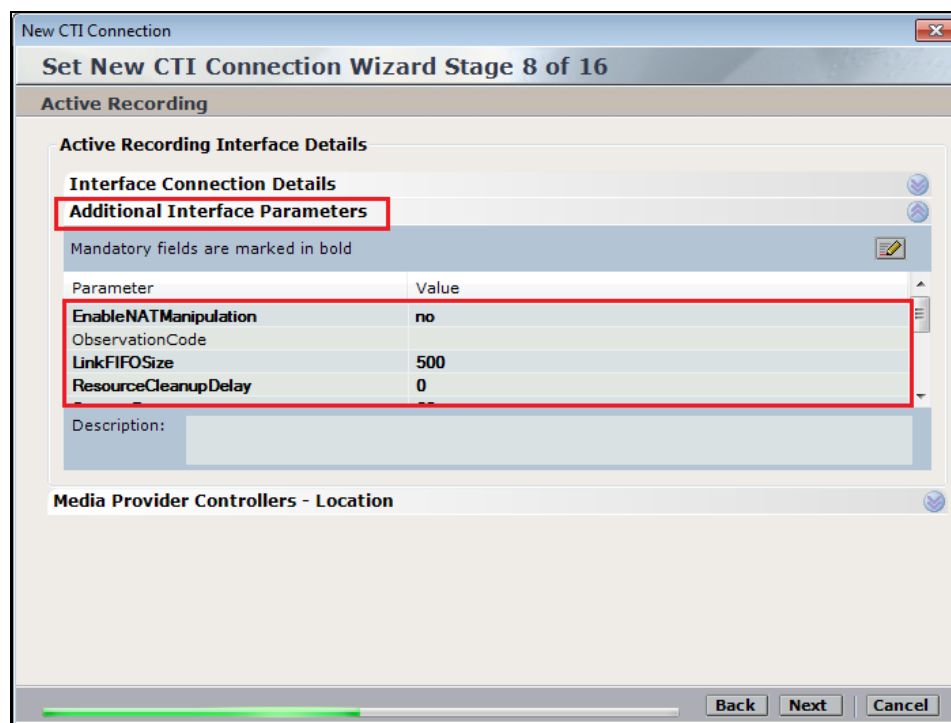
Enter the password that was created in **Section 6.6** and click on **OK**.



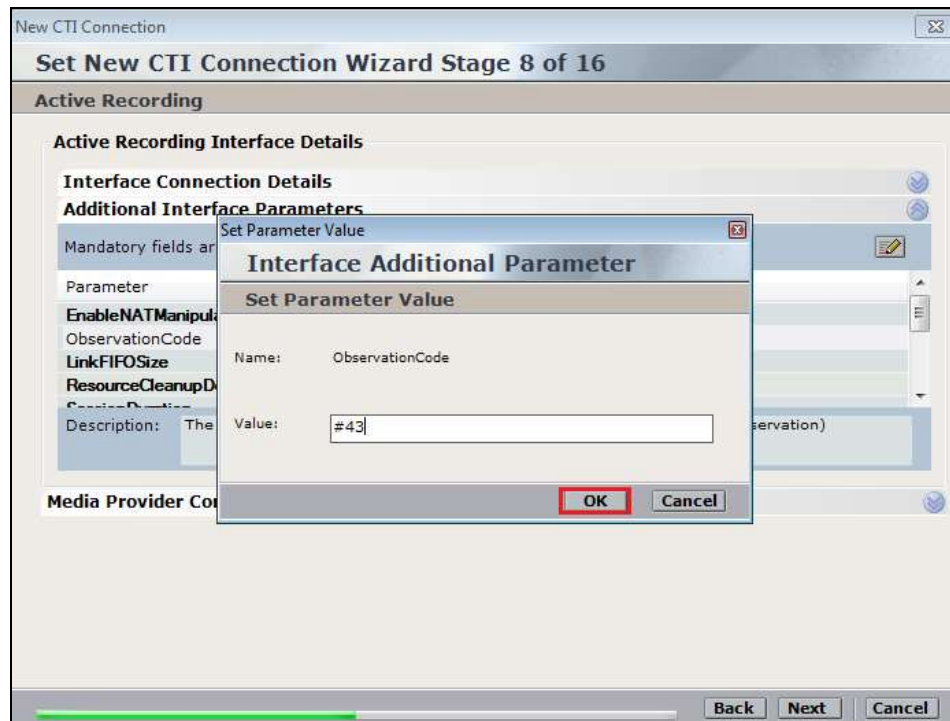
Because the unencrypted port was chosen select **False** for the **AESSecuredConnection**. Click on **OK** and then **Next** (not shown) to continue.



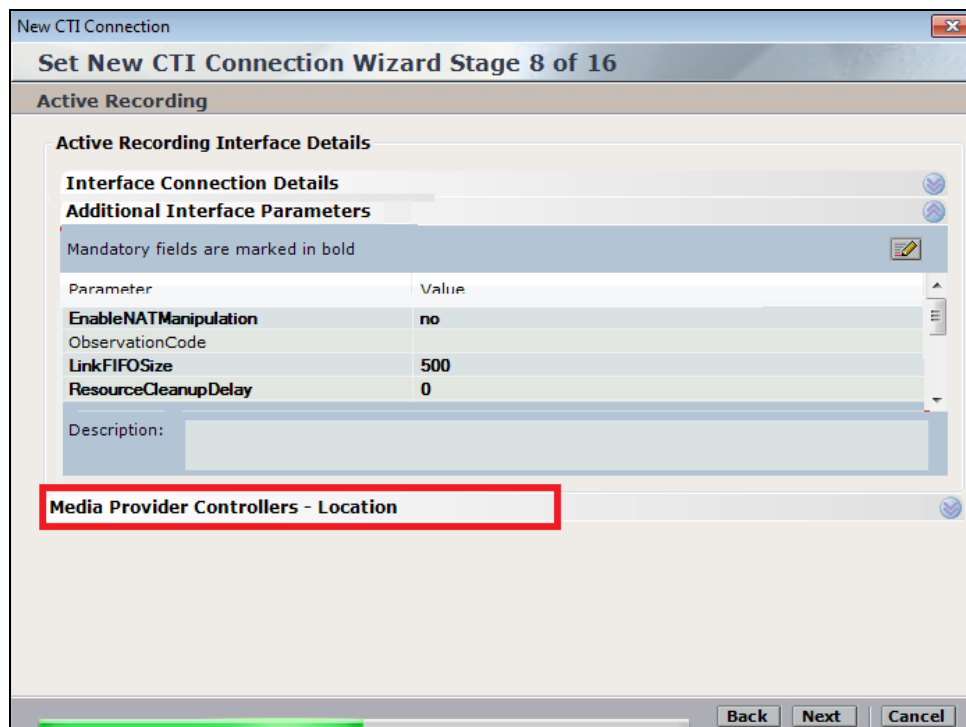
Click on **Additional Interface Parameters**, then to change the Service Observation Code double-click on **ObservationCode**.



Enter the **Value** that was created in **Section 5.5**. This was the Service Observing Listen Only Access Code **#43**. Click on **OK** to continue.



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



Enter the **IP/Hostname** of the Nice Advanced Interactions Server, then click on the + 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.

New CTI Connection
Set New CTI Connection Wizard Stage 10 of 16

Devices

Available Devices
Provide telephony switch available devices
0 devices

Device Number/IP	CTI Trunk ID	Type

The **Device Type** should be **Extension** and insert the extension number of a phoneset that is to be recorded the example below showing extension **2001**. Expand **Advanced Device Parameters** and ensure that the **Value** for **Observation Type** is set to **Resourced-Based**. Click on **OK** to continue.

New CTI Connection
Set New CTI Connection Wizard Stage 10 of 16

Devices

Available Devices
Provide telephony switch available devices
0 devices

Device Number/IP	CTI Trunk ID	Type

Add Device

Name:

Device Type: *

Device Number: *

IP:

Advanced Device Parameters

☐ Display Read Only Information

Name	Value
Observation Type	Resource-Based

Description: Observation Type. Non-Resource-Based - can be recorded without the

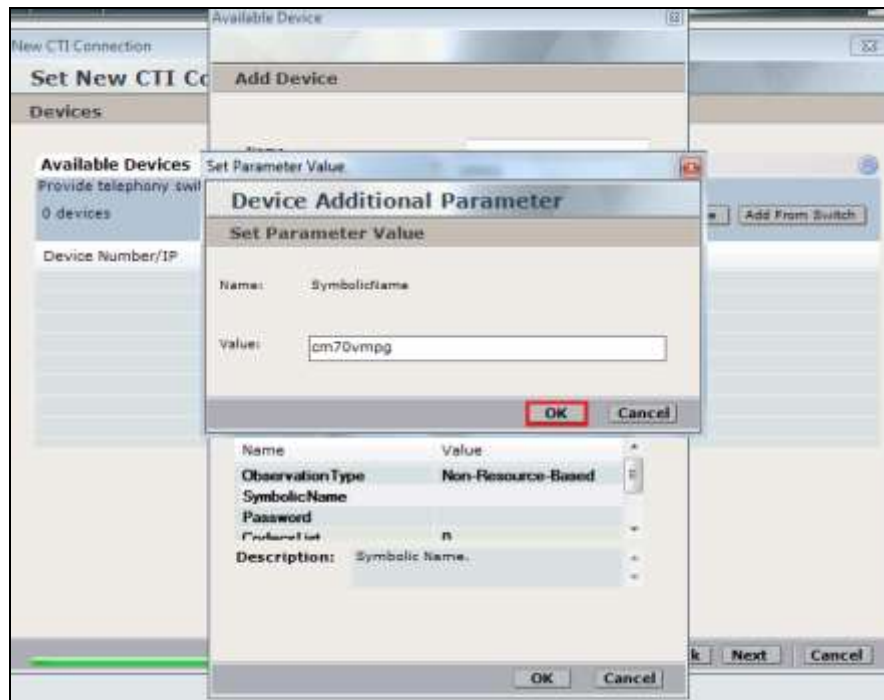
For Service Observe and Single Step Conference virtual extensions need to be added. These are the virtual extensions that were created in **Section 5.7**. Ensure that **Device Type** is set to **Virtual Extension** and add the correct extension for **Device Number**. Each of the **Parameters** highlighted at the bottom of the screen need to be configured and these are done by double-clicking on each parameter.

The screenshot shows a window titled "Available Device" with a sub-header "Add Device". In the "Add Device" section, there is a "Name" text box, a "Device Type" dropdown menu set to "Virtual Extension", and a "Device Number" text box containing "28902". These three fields are enclosed in a red rectangular box. Below this is the "Advanced Device Parameters" section, which includes a checkbox for "Display Read Only Information" and a table with two columns: "Name" and "Value". The table has four rows: "ObservationType" with value "None", "SymbolicName", "Password", and "ConferenceList" with value "n". The first three rows are enclosed in a red rectangular box. Below the table is a "Description" field with the text "Observation Type. Non-Resource-Based - can be recorded without the". At the bottom of the window are "OK" and "Cancel" buttons.

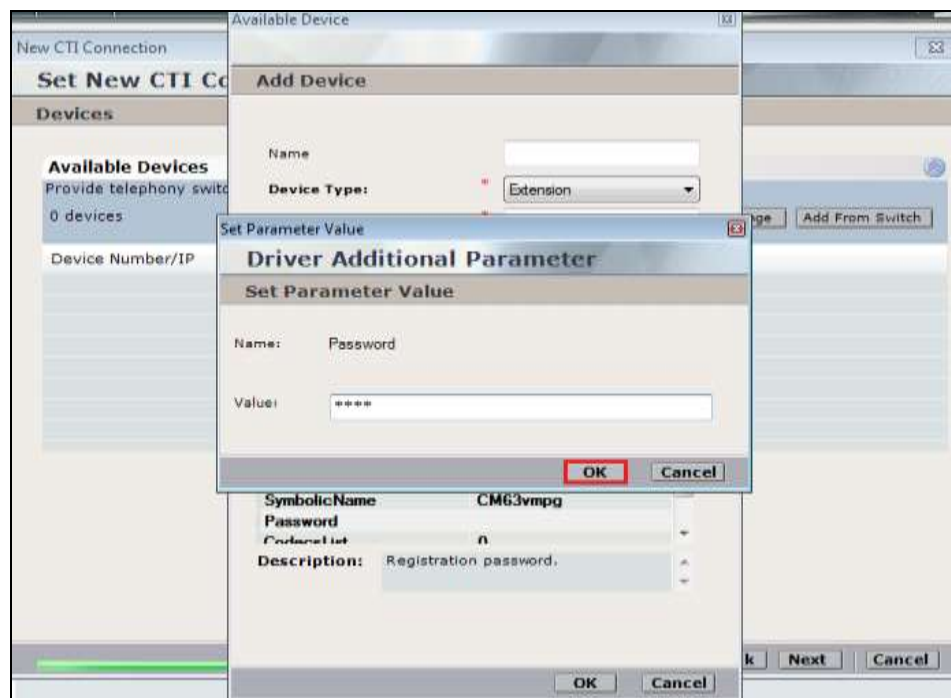
Name	Value
ObservationType	None
SymbolicName	
Password	
ConferenceList	n

Description: Observation Type. Non-Resource-Based - can be recorded without the

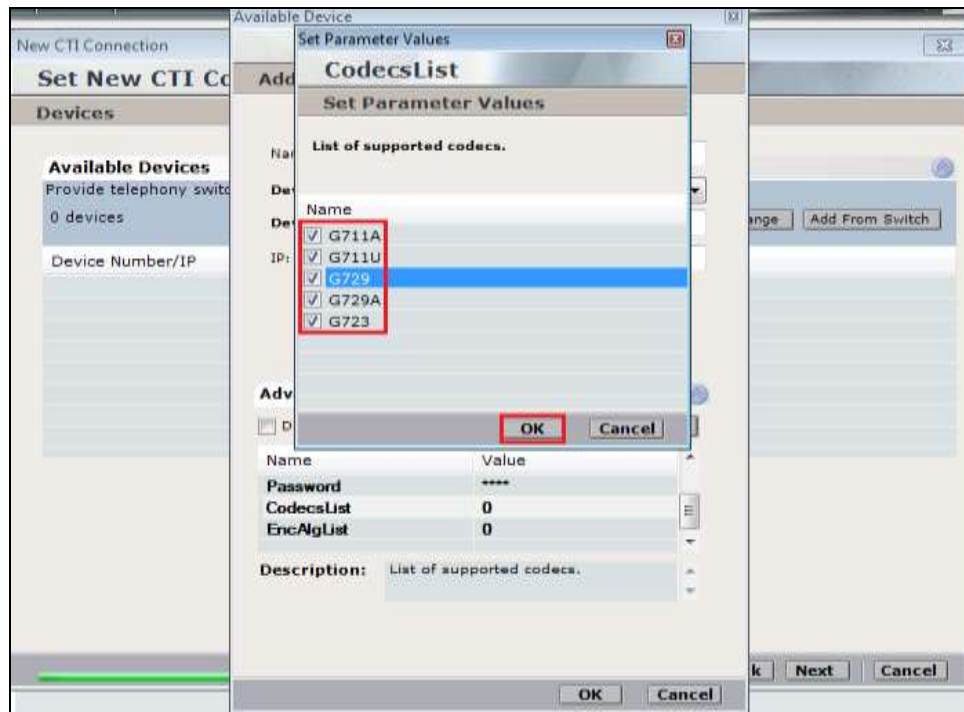
Enter the correct **Value** for **SymbolicName**. Double-click on **SymbolicName** to set the value. This should be the same as the switch name entered in **Section 6.2**.



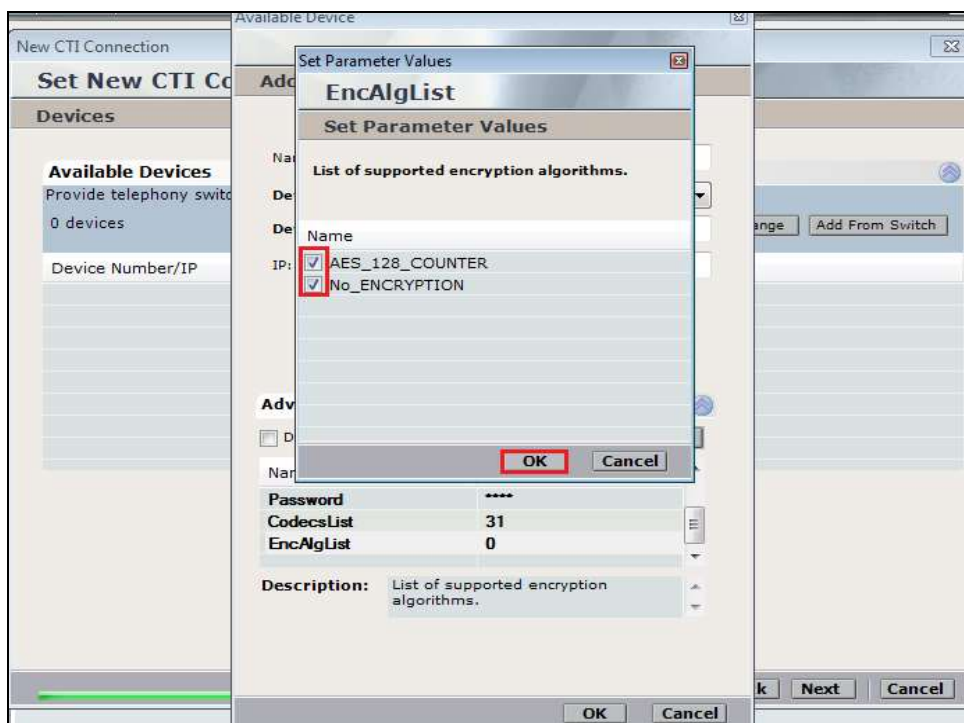
Enter the correct **Password** and note this is the password for the extension that is being added here. This is the station password which was entered during the creation of the station. A printout of an extension can be found in **Section 5.5** of these Application Notes.



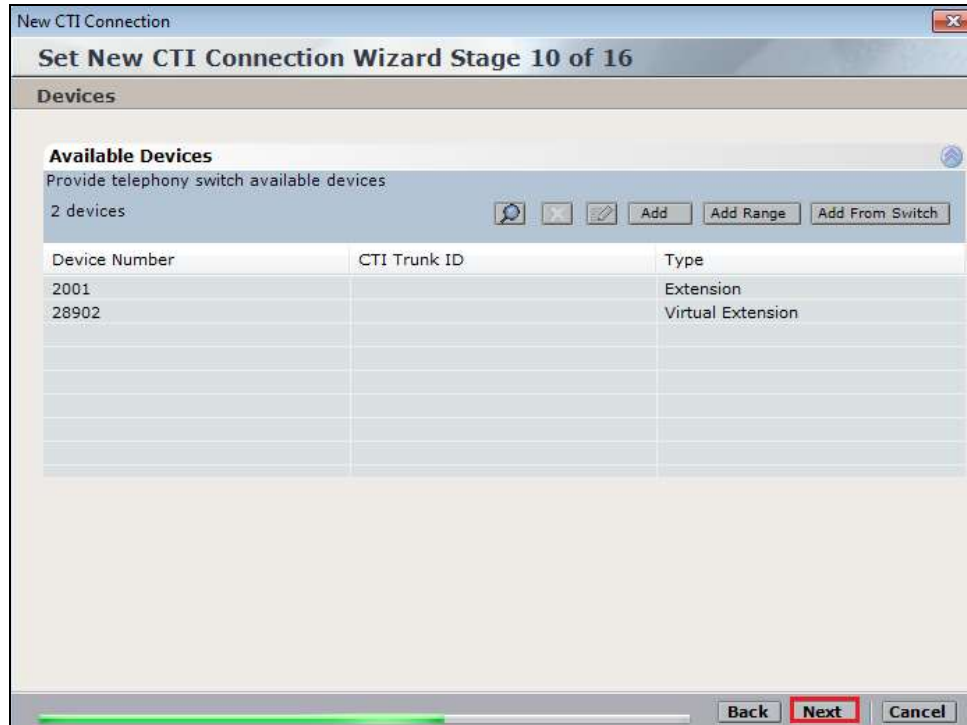
Double-click on **CodecsList** and ensure that all the values are ticked as shown below. Click on **OK** to continue.



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



Click on **Next** to continue.



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 of 2 devices. The 'Next' button is highlighted with a red box.

Device Number	CTI Trunk ID	Type
2001		Extension
28902		Virtual Extension

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



The screenshot shows the 'Set New CTI Connection Wizard Stage 11 of 16' window. The 'Monitor' section is active, displaying 'Available Devices' (0 devices) and 'Monitored Devices' (1 device). The 'Next' button is highlighted with a red box.

Device	Type
2001	Extension

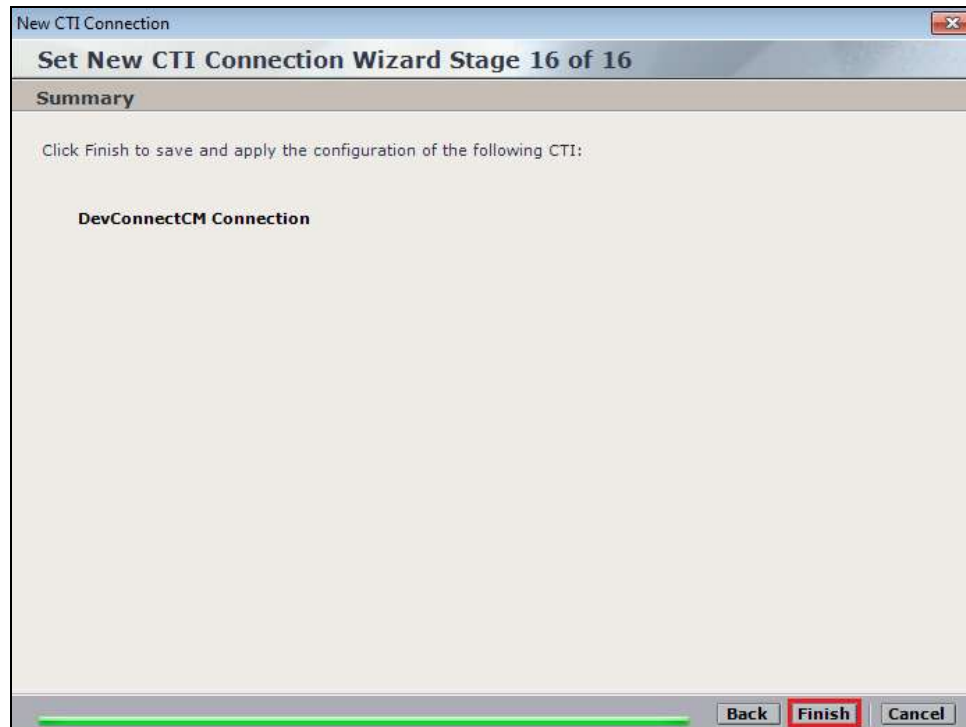
It is optional, but for better analysis tick on **Call Flow Analysis** and click on **Next** to continue.

The screenshot shows a window titled "New CTI Connection" with a subtitle "Set New CTI Connection Wizard Stage 12 of 16". The main section is labeled "Optional" and contains the text: "Select optional features relevant to integration. Some options may require further configuration." Below this text are four checkboxes: "SIP Trunk Correlation", "Rejected Devices", "Filter Calls", and "Call Flow Analysis". The "Call Flow Analysis" checkbox is checked and highlighted with a red rectangle. At the bottom right, there are three buttons: "Back", "Next" (highlighted with a red rectangle), and "Cancel". A green progress bar is visible at the bottom left.

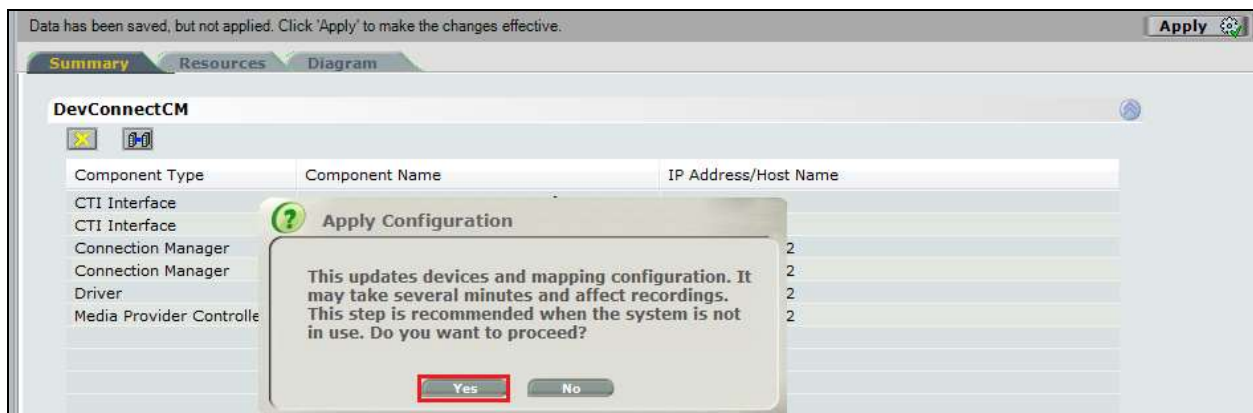
Select a different **Port** number as shown below **62095** is chosen simply because **62094** was already in use.

The screenshot shows a window titled "New CTI Connection" with a subtitle "Set New CTI Connection Wizard Stage 15 of 16". The main section is labeled "Requirements" and contains the text: "The Interactions Center server selected already has a Connection Manager. Create a new Connection Manager, or select an existing one." Below this text are two radio button options. The first option, "Create a new Connection Manager", is selected and highlighted with a red rectangle. It includes a "Port:" label and a text box containing "62095". The second option, "Select available Connection Manager", is unselected. Below it, there is a "Ports in use:" label and a text box containing "62094". At the bottom right, there are three buttons: "Back", "Next" (highlighted with a red rectangle), and "Cancel". A green progress bar is visible at the bottom left.

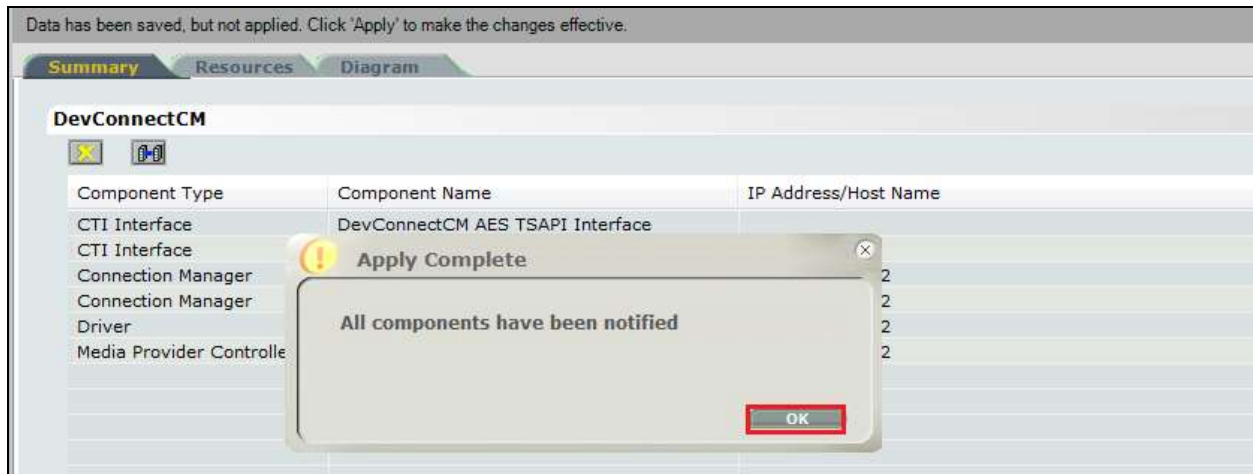
Click on **Finish** to complete the New CTI Wizard.



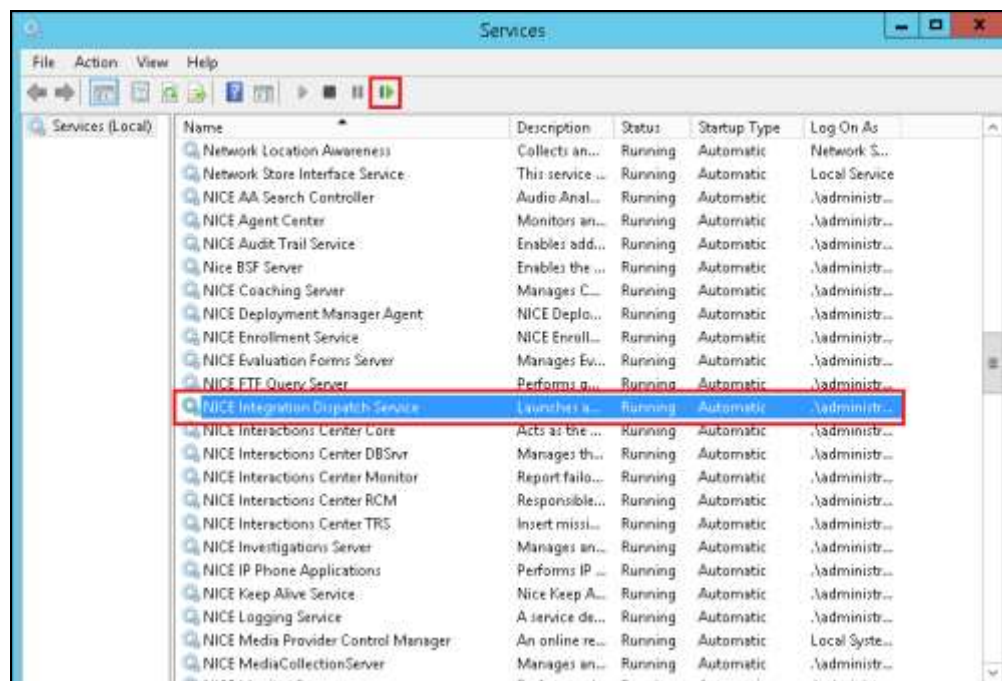
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed



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

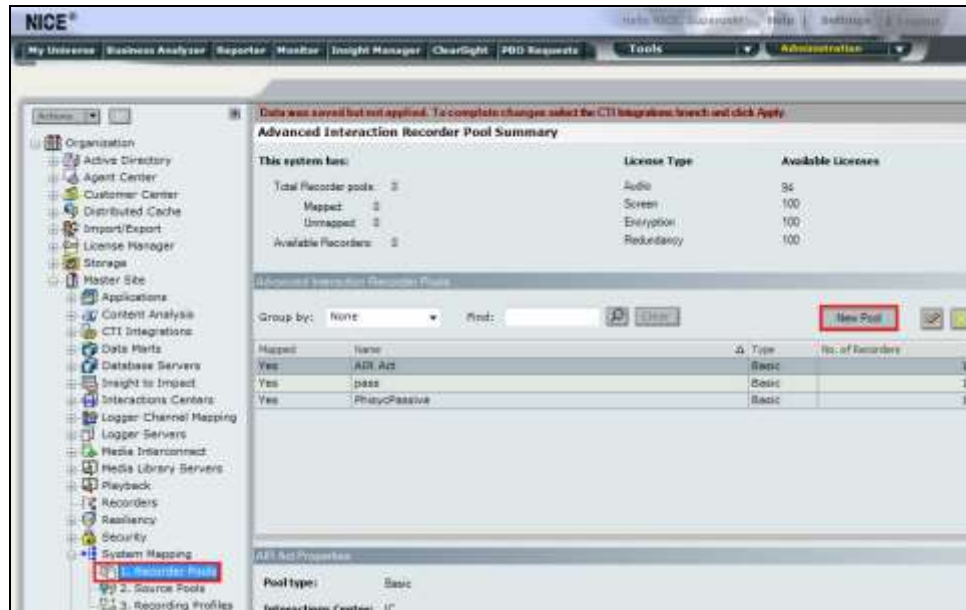


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

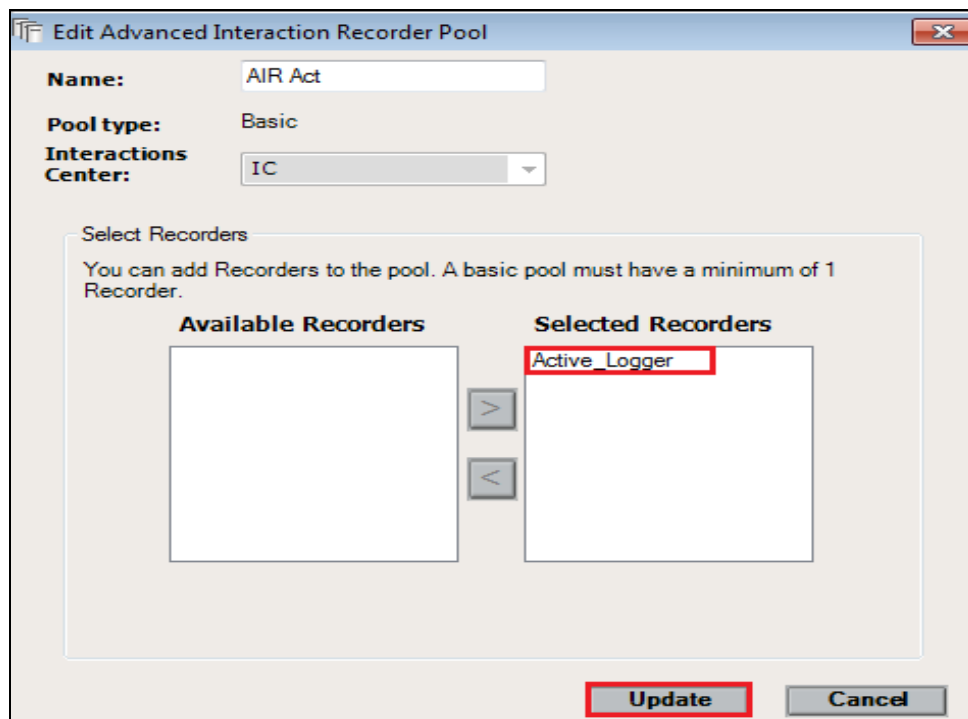


7.2. System Mapping

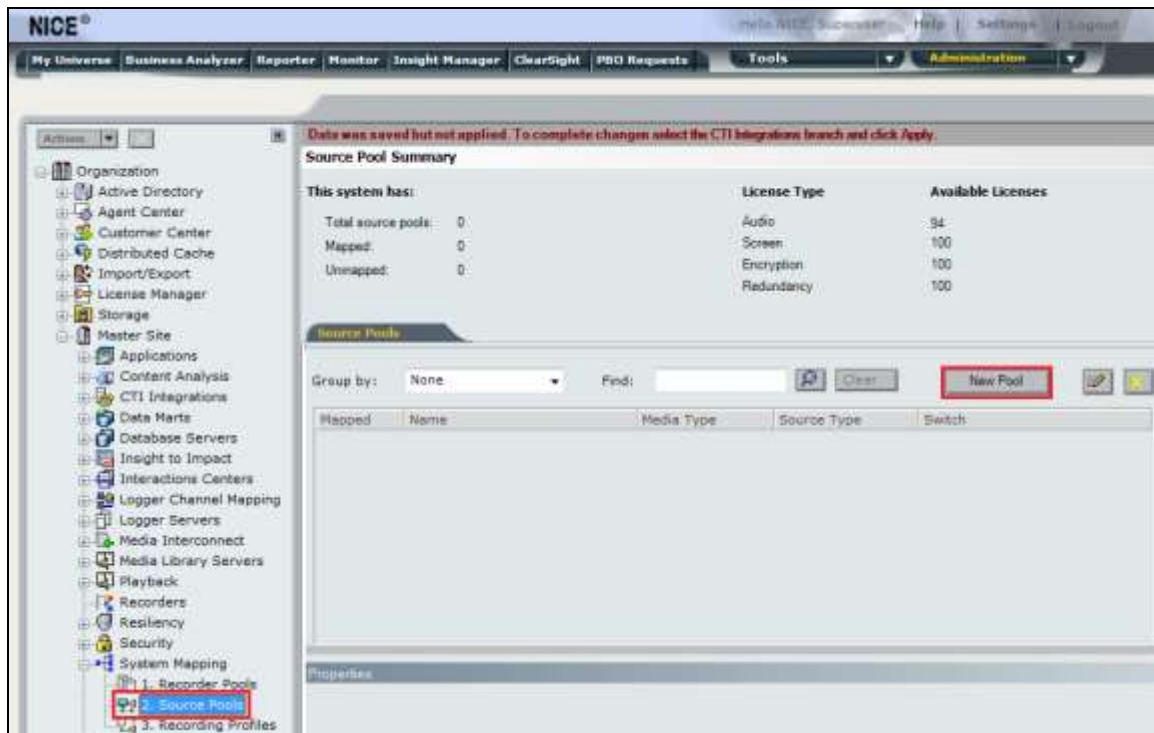
From the web browser navigate to **Master Site → System Mapping → Recorder Pools**. In the main window click on **New Pool**.



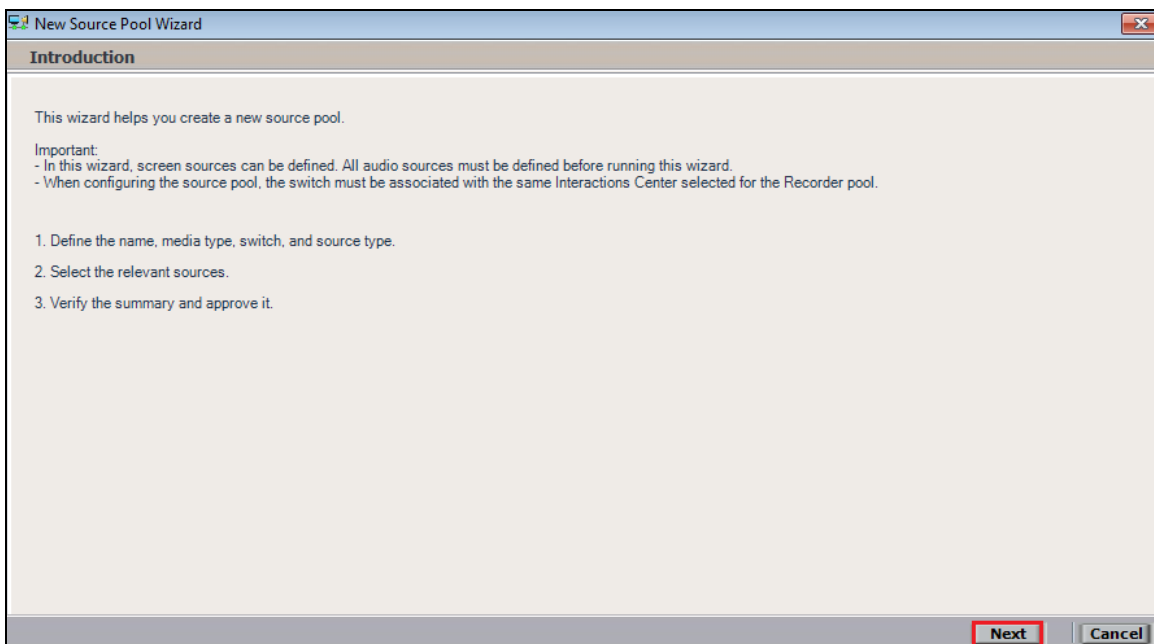
Enter a suitable **Name** for the **Recorder Pool** and select the **Active_Logger** from the list of **Available Recorders** and click on **Update** to continue.



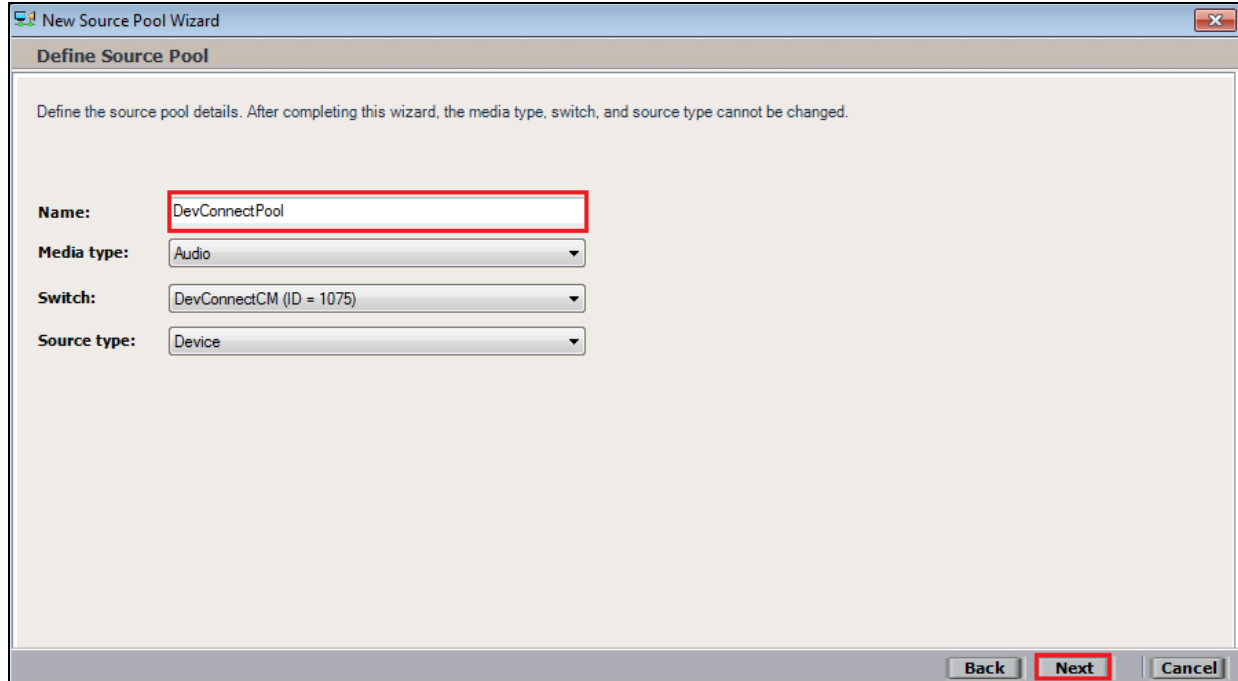
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



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 main heading is 'Define Source Pool'. Below the heading 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, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red border.

Name: DevConnectPool

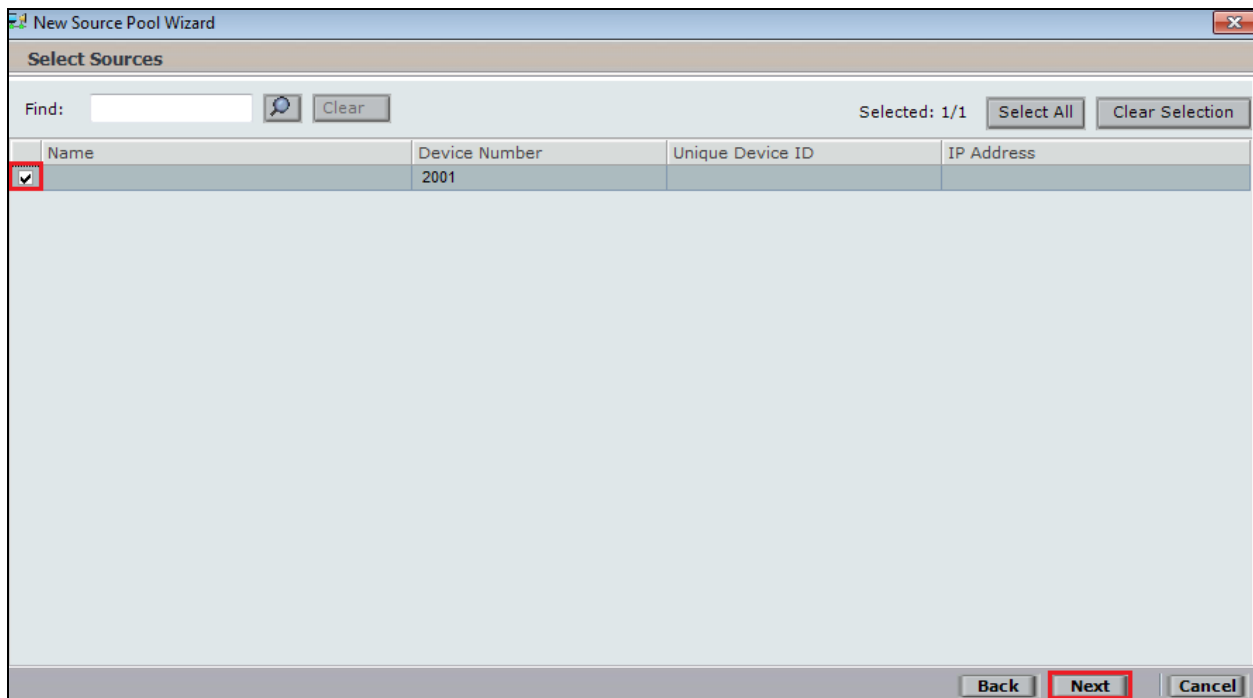
Media type: Audio

Switch: DevConnectCM (ID = 1075)

Source type: Device

Back Next Cancel

Select the extensions that were created in **Section 7.1**, 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 main heading is 'Select Sources'. There is a search bar with the text 'Find:' and a 'Clear' button. To the right of the search bar, it says 'Selected: 1/1' and there are '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 of the table has a checked checkbox in the 'Name' column, and the 'Device Number' is '2001'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red border.

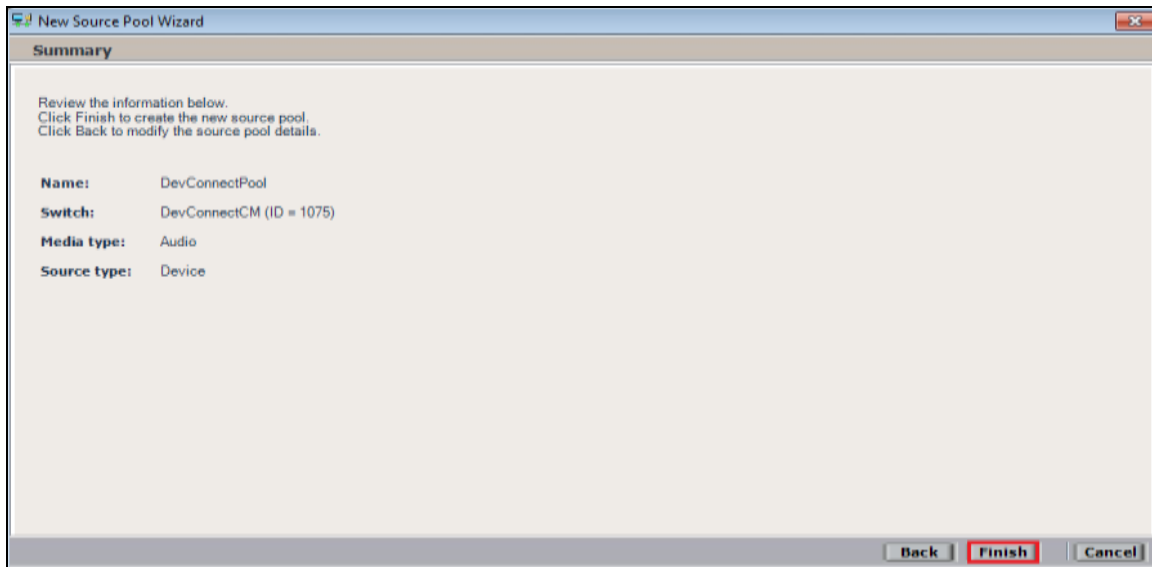
Find: [Search] Clear

Selected: 1/1 Select All Clear Selection

Name	Device Number	Unique Device ID	IP Address
<input checked="" type="checkbox"/>	2001		

Back Next Cancel

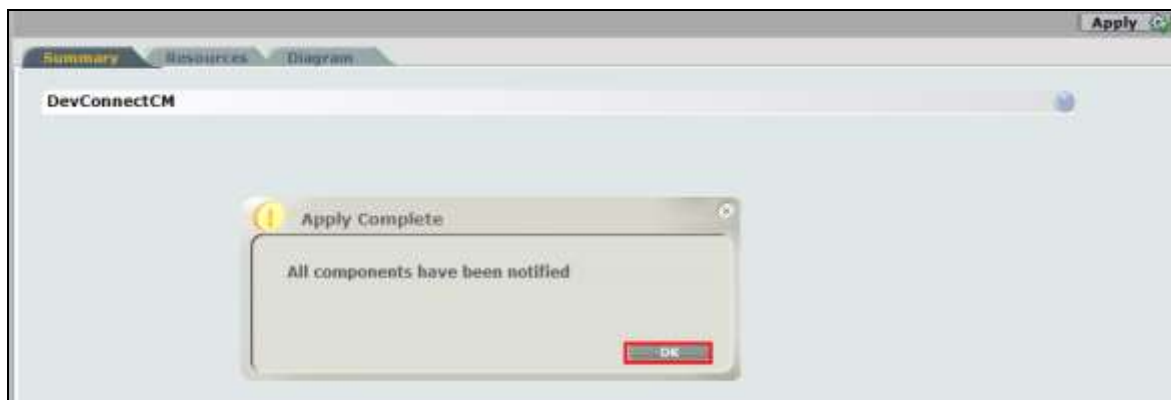
Click on **Finish** to complete the New Source Pool Wizard.



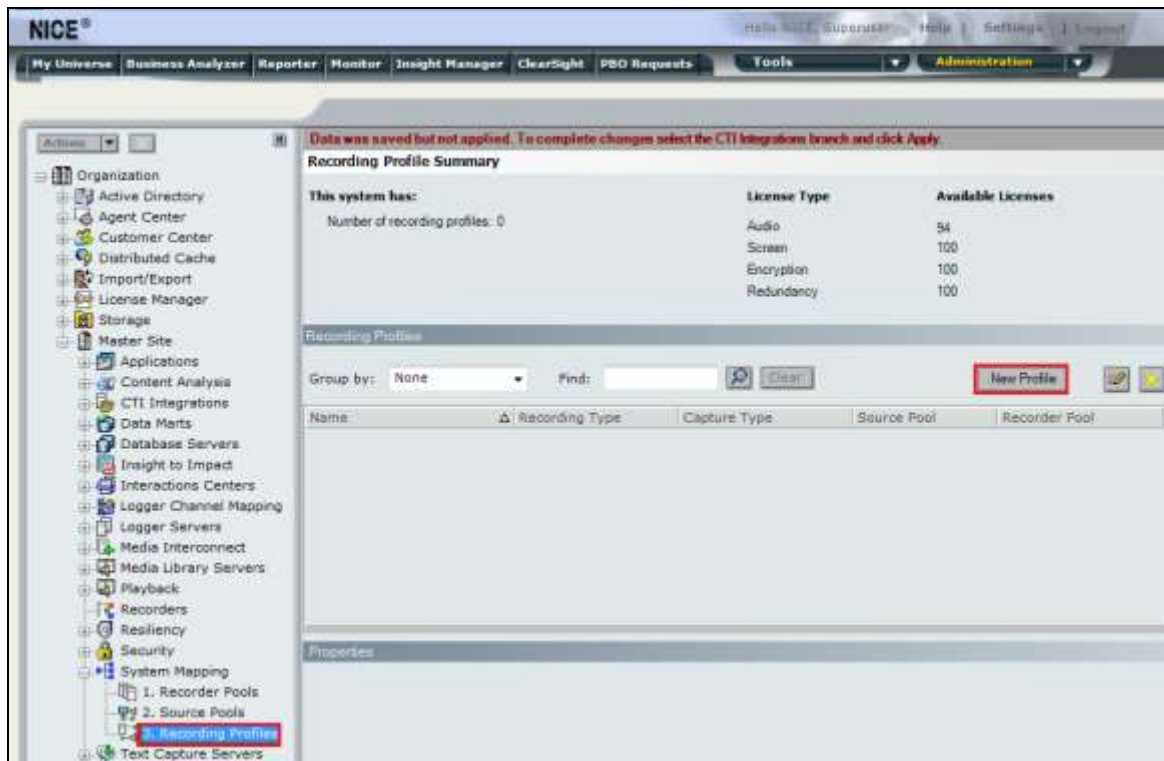
To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.



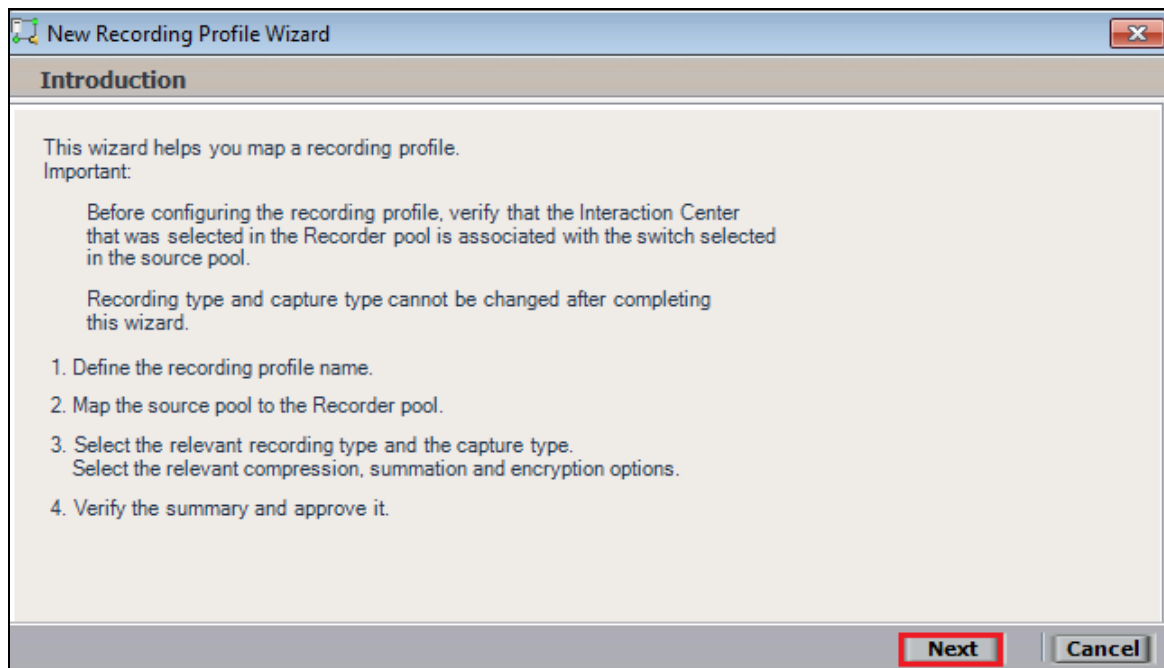
The following screen shows the changes were saved correctly. Click on **OK** to continue.



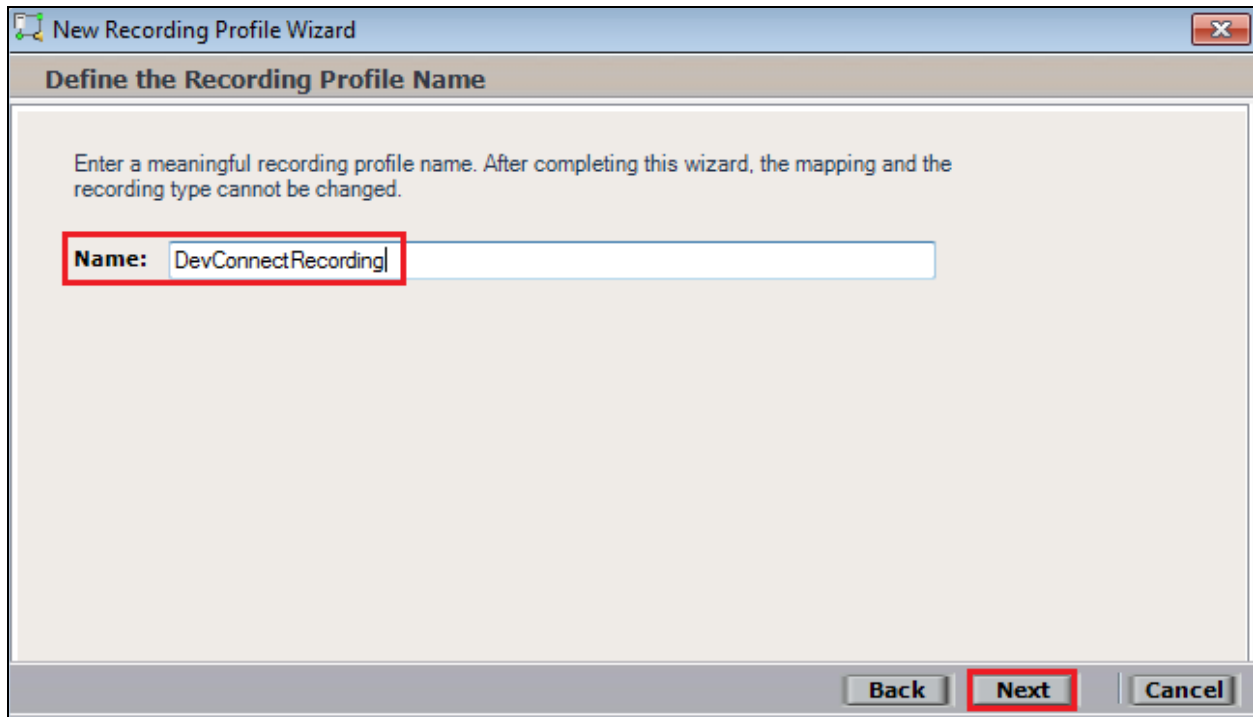
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



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

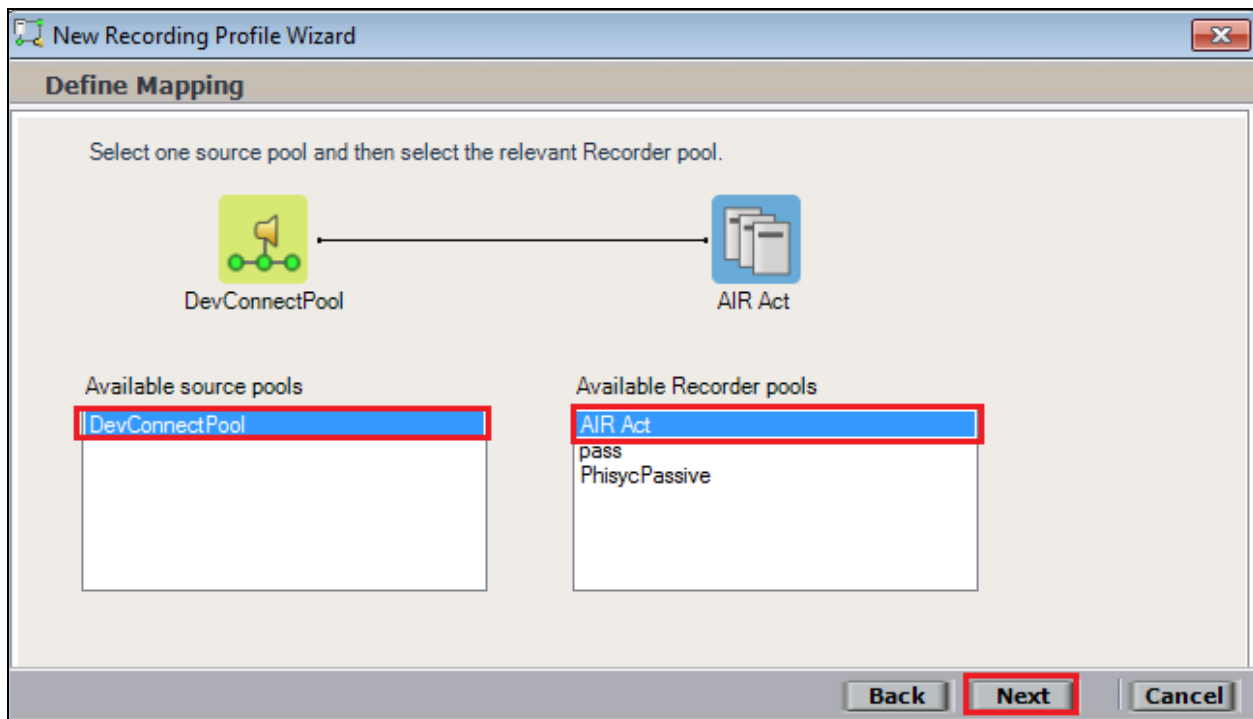


Enter a suitable **Name** for the Recording profile.



The screenshot shows the 'New Recording Profile Wizard' window with the title 'Define the Recording Profile Name'. The instruction text reads: 'Enter a meaningful recording profile name. After completing this wizard, the mapping and the recording type cannot be changed.' Below this, there is a text input field labeled 'Name:' containing the text 'DevConnectRecording'. The 'Next' button at the bottom right is highlighted with a red box.

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



The screenshot shows the 'New Recording Profile Wizard' window with the title 'Define Mapping'. The instruction text reads: 'Select one source pool and then select the relevant Recorder pool.' The interface displays two icons at the top: 'DevConnectPool' (a green icon with a yellow flag) and 'AIR Act' (a blue icon with a stack of papers). Below these icons are two list boxes. The 'Available source pools' list box contains 'DevConnectPool', which is highlighted with a blue selection bar and a red border. The 'Available Recorder pools' list box contains 'AIR Act', 'pass', and 'PhisycPassive', with 'AIR Act' highlighted by a blue selection bar and a red border. The 'Next' button at the bottom right is highlighted with a red box.

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

New Recording Profile Wizard

Define Recording Profile

Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.

Recording type: Total

No. of allocated licenses: Determined by the number of sources in the source pool

Capture type: Active DMCC VE By Device

☐ Secondary Capture Type:

Select all applicable options:

☒ Compression

☐ Summation

☐ Encryption

Back Next Cancel

Note: The only difference in the setup for Single Step Conference is with both the choice of **Recording type** which is set to **Interaction-based** and **Capture type** which will be **Active DMCC VE By Call** as shown below.

New Recording Profile Wizard

Define Recording Profile

Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.

Recording type: Interaction-based

No. of allocated licenses: 1

Capture type: Active DMCC VE By Call

☐ Secondary Capture Type:

Select all applicable options:

☒ Compression

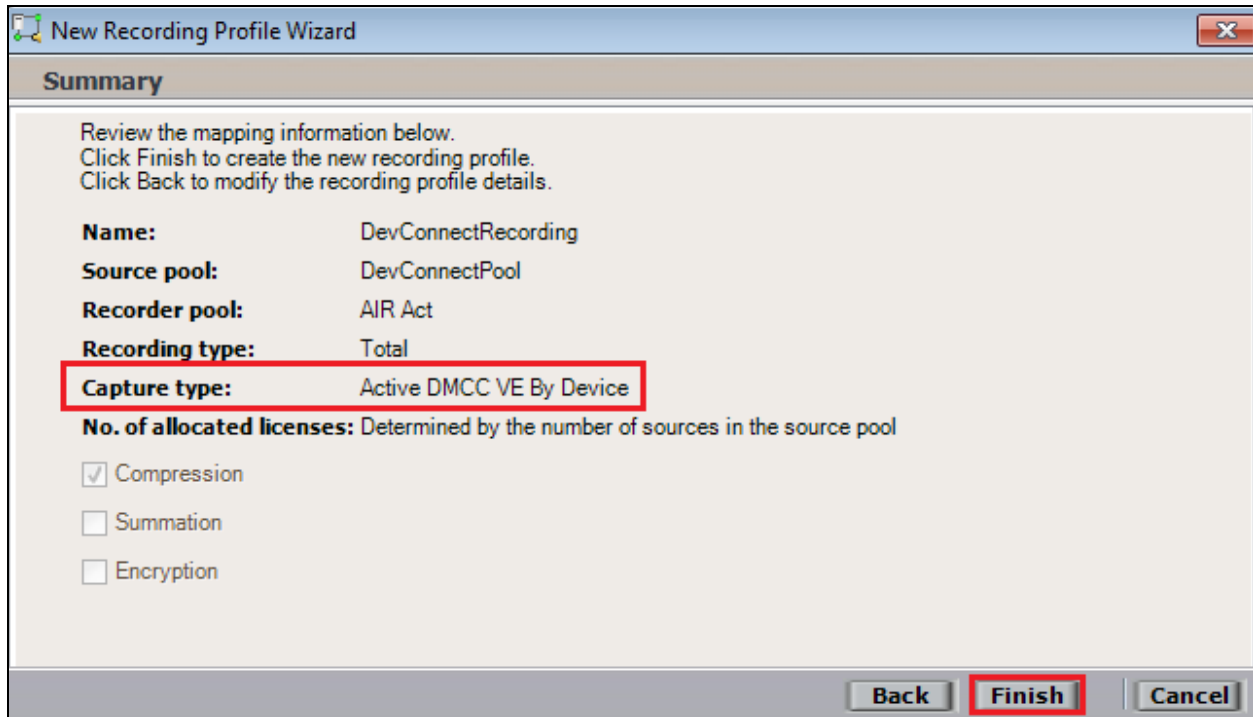
☐ Summation

☐ Encryption

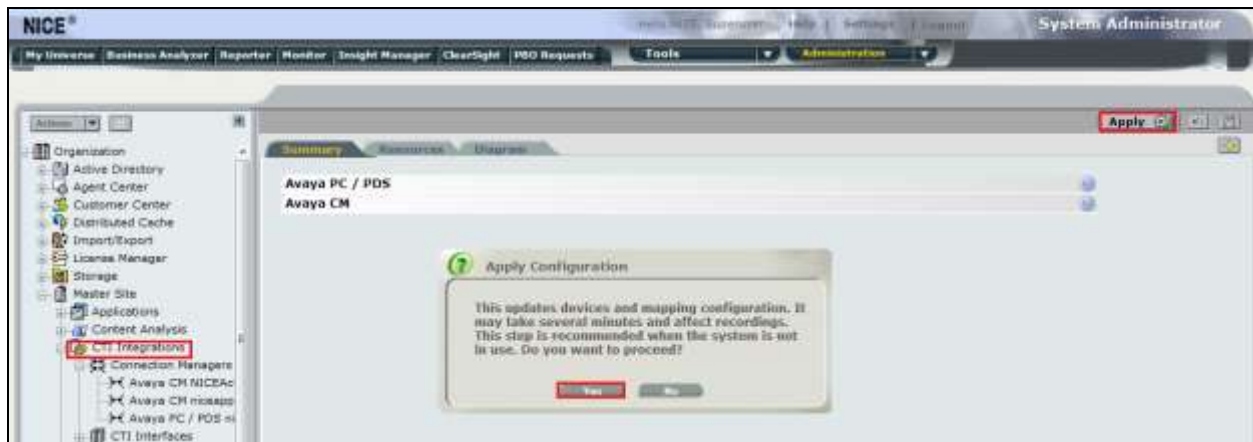
Back Next Cancel

Depending on number of Virtual Extensions

Click on **Finish** to complete the **New Recording Profile Wizard**. The screen below shows that for Service Observe.



Navigate to **Master Site** → **CTI Integrations** and from the main window click on **Apply**. Then click on **Yes** to proceed.



This concludes the setup of the NICE Application Server for DMCC Service Observe and Single Step Conference recording.

8. 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.

8.1. Verify Avaya Aura® Communication Manager CTI Service State

Before the connection between the NICE Engage Platform and the AES is check the connection between Communication Manager and AES can be check 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	4	no	aes70vmpg	established	18	18

8.2. Verify TSAPI Link

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The main area displays the 'TSAPI Link Details' screen. At the top, there's a header with the Avaya logo and 'Application Enablement Services Management Console'. Below this, a red banner indicates 'Status | Status and Control | TSAPI Service Summary'. The main content area shows a table with columns: Link, Switch Name, Switch CTI Link ID, Status, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period. The table has one row with the following values: Link 1, Switch Name cm70vmpg, Switch CTI Link ID 1, Status Talking, State Online, Switch Version 17, Associations 4, Msgs to Switch 15, Msgs from Switch 15, and Msgs Period 30. Below the table, there are buttons for 'Online' and 'Offline'. At the bottom, there's a section for 'For service-side information, choose one of the following:' with buttons for 'TSAPI Service Status', 'Link Status', and 'User Status'.

8.3. 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: 991-aea/0vrrag/10.10.40.126
Server Offer Type: VIRTUAL_APP_SAME_ORL_VMWARE
SW Version: 7.0.0.0.12
Server Date and Time: Tue Dec 13 14:45:11 GMT 2016
HA Status: Not Configured

Status | Status and Control | DMCC Service Summary

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 13 14:45:11 GMT 2016

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"/>	LC06ED1F86D6A1627 7F0F0B05747B4AF-0	NICE		10.10.40.126	XML Unencrypted	3

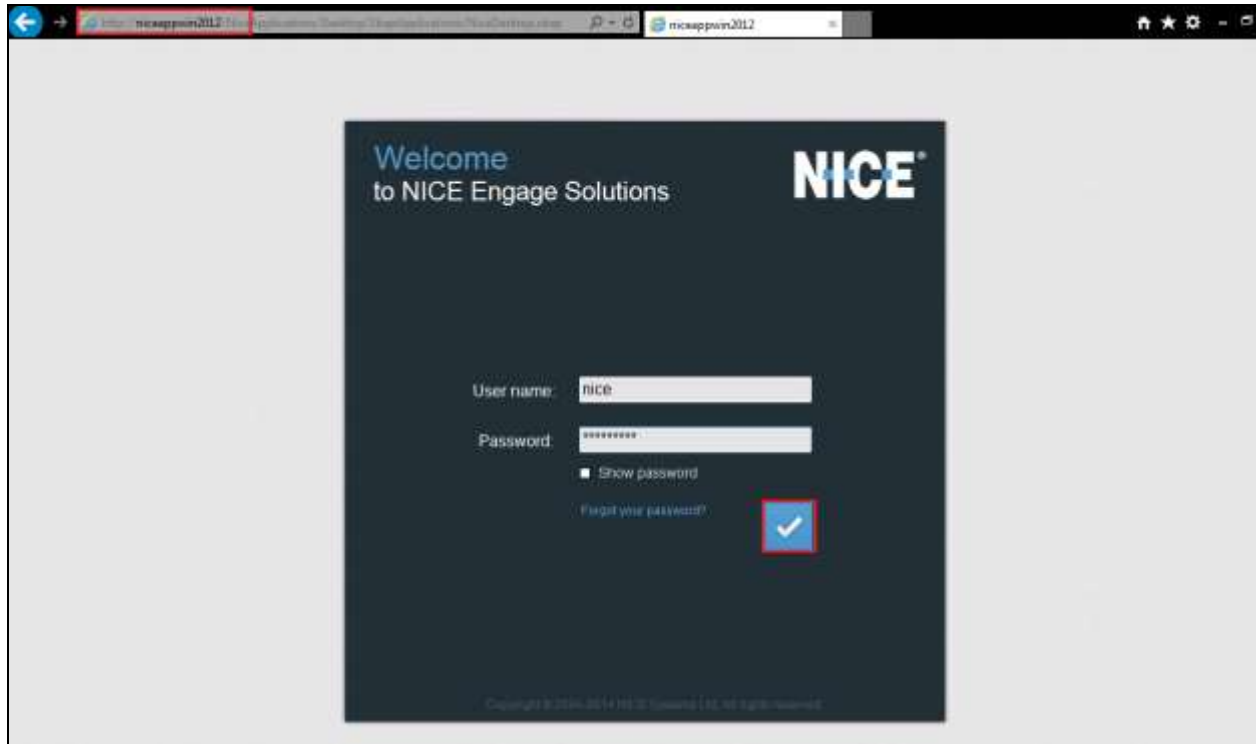
Terminate Sessions | Show Terminated Sessions

Item 1 of 1
1 Go

8.4. 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.

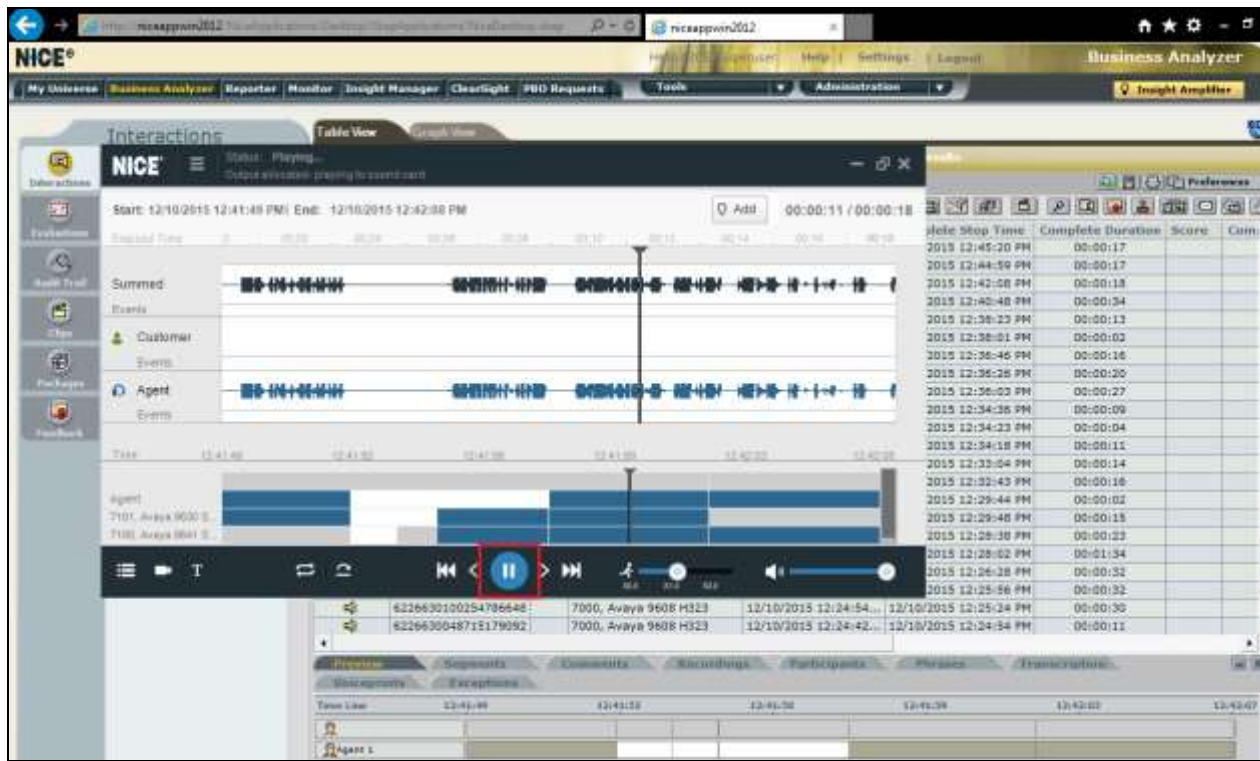
Open a browser session to the NICE Application Server as is shown below. Enter the proper credentials and click on **Login**.



The screenshot displays the NICE Business Analyzer web application. The top navigation bar includes the NICE logo, user information (John J. Cooper), and links for Help, Settings, and Logout. The main menu contains tabs for My Universe, Business Analyzer (selected), Reporter, Monitor, Insight Manager, Clearlight, and PBO Requests. The Business Analyzer tab is active, showing a left sidebar with icons for Interactions, Reports, Audit Trail, Cases, Mailboxes, and Feedback. The Interactions section is expanded, revealing a 'Queries' folder with a list of queries: Complete - Last 24 hours, Complete - Last 7 days, Segment - Calls to calibrate, Segment - Last 24 hours, Segment - Last 7 days, Segment - Last 7 days Calls not eval, and Private. A 'Saved Themes' section is also visible. The main content area shows a 'Table View' of query results, with a search bar and a list of results for the 'Complete - Last 24 hours' query.

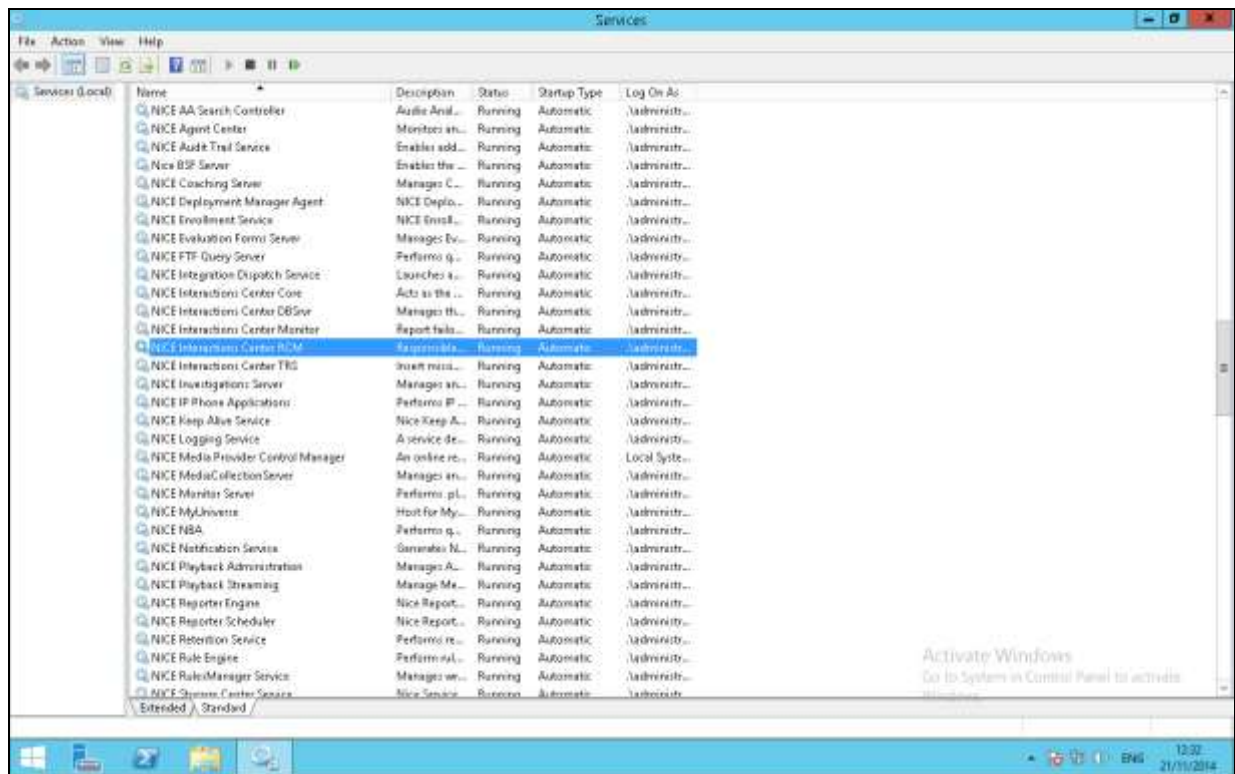
The screenshot displays the NICE Business Analyzer interface. On the left, a sidebar contains icons for 'Interactions', 'Queries', 'Reports', 'Monitor', 'Insight Manager', 'Clearlight', 'MRQ Requests', 'Tools', and 'Administration'. The 'Interactions' icon is highlighted with a red box. The main window shows a 'Table View' of interaction data. At the top, there's a search bar with 'Search' and 'Exact Phras' buttons. Below the search bar, the text 'Results for Query: Complete - Last 24 hours' is visible. The table has columns: Type, Flag, Full Name, Complete ID, Complete Start Time, Complete Stop Time, Complete Duration, and Complete. The table lists various user interactions, with some rows highlighted in red. The bottom of the screen shows a status bar with '150 Records found'.

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.



8.5. 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.



9. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0 to connect to using DMCC Service Observation and Single Step Conference to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

10. 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] *Avaya Aura® Session Manager Overview*, Doc # 03603323 *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 one-X® Agent Softphone

This is a printout of the Avaya one-X® Agent softphone used during compliance testing.

display station 2100	Page 1 of 5	
STATION		
Extension: 2100	Lock Messages? n	BCC: 0
Type: 9630	Security Code: *	TN: 1
Port: S00031	Coverage Path 1:	COR: 1
Name: one-X Agent1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 2100	
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: default	
	Customizable Labels? Y	

display station 2100	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:	Display Client Redirection? n	
AUDIX Name:	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: 2100	Always Use? n IP Audio Hairpinning? n	

display station 2100 Page 3 of 5

STATION

```

Conf/Trans on Primary Appearance? n
Bridged Appearance Origination Restriction? 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: 1000		n
External Calls To: 1000		n
Busy For Internal Calls To:		n
External Calls To:		n
No Reply For Internal Calls To:		n
External Calls To:		n

SAC/CF Override: n

display station 2100 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: manual-in          Grp:
2: call-appr          6: after-call          Grp:
3: call-appr          7: aux-work          RC:  Grp:
4: auto-in            Grp:          8:

```

voice-mail

Avaya 9608 H.323 Deskphone

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

display station 2001	Page 1 of 5	
STATION		
Extension: 2001	Lock Messages? n	BCC: 0
Type: 9608	Security Code: *	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: Ext2001	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: 2001	
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 2001	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: 2001	Always Use? n IP Audio Hairpinning? n

©2016 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.