



Avaya Solution & Interoperability Test Lab

Application Notes for NICE Engage Platform R7.3 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using DMCC Multiple Registration for Stereo Recording - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the NICE Engage Platform to interoperate with Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1, and Avaya Aura® Application Enablement Services R10.1 using DMCC Multiple Registration to record telephone calls.

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 R7.3 to interoperate with Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1, and Avaya Aura® Application Enablement Services R10.1. NICE Engage Platform uses Avaya Aura® Communication Manager Multiple Registration feature via the Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services Application Programming Interface (TSAPI) to capture the audio and call details for call recording on various Communication Manager H.323, SIP and Digital endpoints, listed in **Section 4**.

Device Media Call Control (DMCC) allows 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.

NICE Engage Platform provides the ability to record multi-channel interactions across the organization for regulatory compliance and to utilize these interactions for multiple business applications in order to extract insights and gain value. The platform tightly integrates with the telephony environment via CTI, APIs and SIP and stores the metadata in a single recording platform to ensure regulatory adherence and standardized workforce optimization processes across multiple channels. It provides comprehensive search tools and media retrieval, as well as a wide variety of Real-Time capabilities for PCI compliance and advanced applications.

The NICE Engage Platform uses the Multiple Registration method to record the calls, using the TSAPI connection to monitor the events necessary to start and stop the recordings. The application uses the AES 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 streams via the recording device and records the call, in stereo.

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 Multiple Registration. 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with these Application Notes, the interface between Avaya systems and NICE Engage Platform did not include use of any specific encryption features as requested by NICE.

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.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park, Call Pickup, Bridged Appearance and Service Observing.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into Avaya Agent for Desktop.
- **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 observations were noted.

- Observing a station/user/extension that is not monitored from a station/user/extension that is monitored can cause no CTI events on the observer. Recordings will appear in NICE Business Analyser (NBA), according to pre-configured Total Recording Solution (TRS) insertion time out (default 5h). During testing, NICE decreased time out to get stored recordings.
- An issue was observed with calling from a SIP phone with a Bridged Appearance call button configured. There were no call start events from TSAPI to allow the call to be logged. This only happens with Bridged Appearance from a SIP phone, if a Bridged Appearance was configured on a H.323 phone the events were sent and the call was recorded. Since the call was recorded, a workaround is to have TRS applied similar to above. Avaya are aware of the issue, and this has been raised previously.

2.3. Support

Technical support can be obtained for NICE Engage Platform from the website <https://www.nice.com/contact-us>

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Engage Platform with the Avaya solution using DMCC Multiple Registration to record calls. The NICE Application Server is set up for DMCC Multiple Registration and connects to AES.

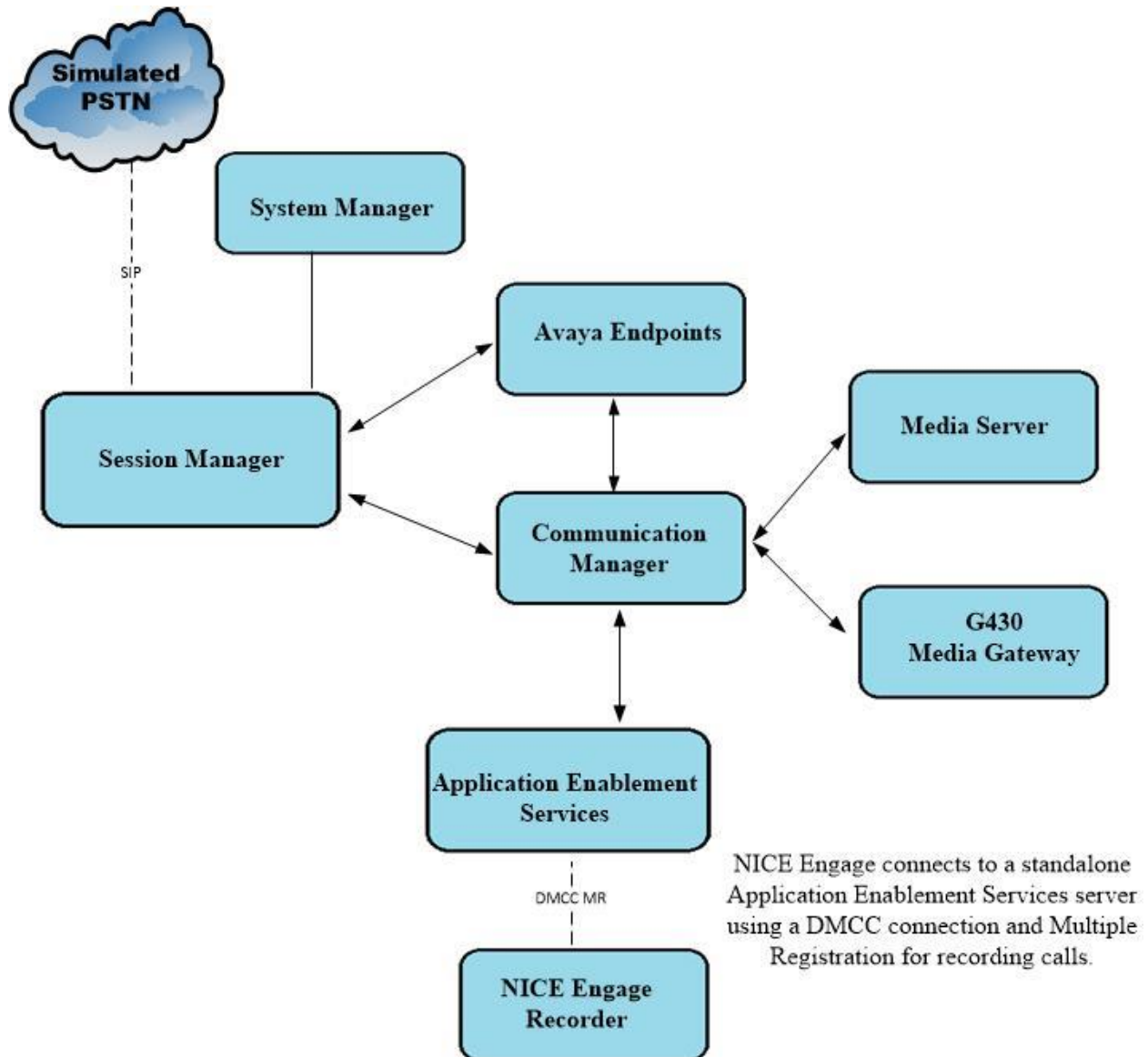


Figure 1: Connection of NICE Engage Platform R7.3 with Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1 and Avaya Aura® Application Enablement Services R10.1

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Equipment / Software	Release / Version
Avaya Aura® System Manager	System Manager 10.1.0.2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Service Pack 2
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0.2.0 – SP2 R020x.01.0.974.0 Update ID 01.0.974.0-27607
Avaya Aura® Application Enablement Services	10.1.0 Build 10.1.0.2.0.12-0
Avaya Aura® Media Server	10.1.0.101
Avaya G430 Media Gateway	42.7.0 /2
Avaya 9404 Digital Phones	17.0
Avaya J100 Series Phones (SIP)	7.1.2.0.14
Avaya J100 Series Phones (H.323)	7.0.14.0.7
Avaya Agent for Desktop (SIP)	2.0.6.23.3005
Avaya Workplace (SIP)	3.26.0.64
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	10.1.0
NICE Equipment / Software	Release / Version
NICE Engage Platform <ul style="list-style-type: none"> - NICE Engage Application Server - NICE Advanced Interactions Recording Server - NICE Engage NDM Server 	7.3

All Equipment is running on virtual servers on VMware.

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 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options	Page	4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? y	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? y	DS1 Echo Cancellation? y	
Attendant Vectoring? y		
(NOTE: You must logoff & login to effect the permission changes.)		

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

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

display node-names ip	Page	1 of 2
IP NODE NAMES		
Name	IP Address	
SM100	10.10.40.12	
aespri101x	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 0**.
- **Local Port:** Retain the default value of **8765**.

change ip-services						Page	1 of	4
IP SERVICES								
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 **aespri101x**.
- **Password:** Enter a password to be administered on AES.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on AES 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:	aespri101x	*****	y	in use			
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: 1990				
Type: ADJ-IP				
		COR: 1		
Name: aespri101x				

5.5. Configure H.323 Stations for Multiple Registration

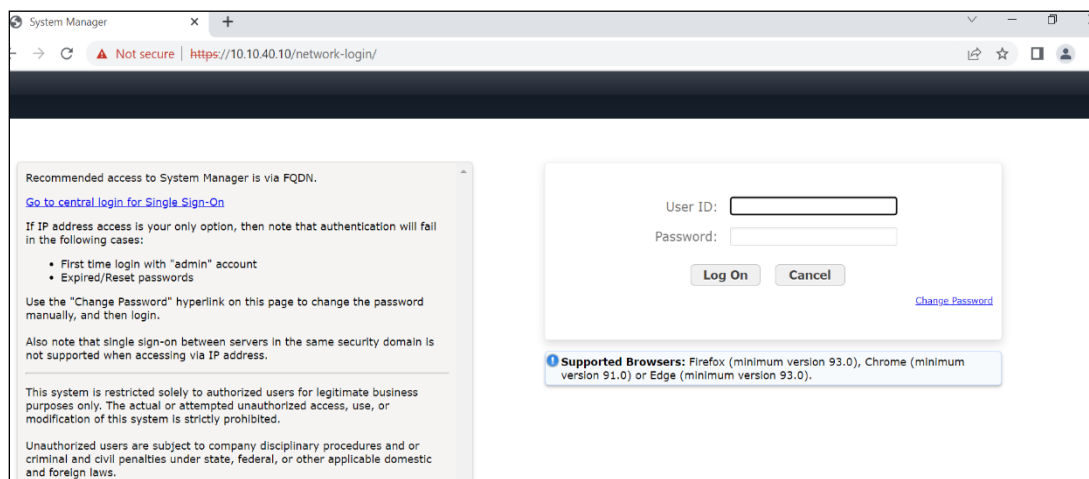
All endpoints that are to be monitored by NICE will need to have **IP Softphone** set to y. IP Softphone must be enabled for Multiple Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required during the NICE Recorder setup in **Section 7.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to y.

change station 1001	Page 1 of 6	
STATION		
Extension: 1001	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: 1001	
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	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

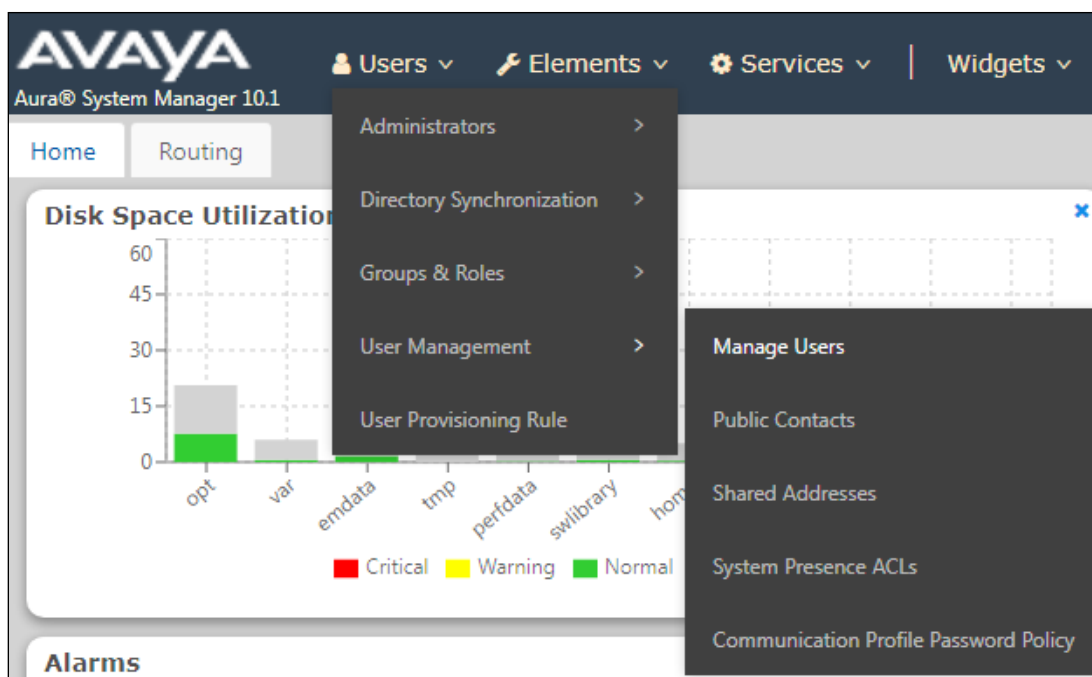
5.6. Configure SIP Stations for Multiple Registration

Each Avaya SIP endpoint or station that needs to be monitored for call recording will need to have “Type of 3PCC Enabled” set to “Avaya” and “Softphone” set to “Yes”. Changes to SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN>/network-login**, where <FQDN> is the fully qualified domain name of System Manager or the IP address of System Manager can be used as an alternative to the FQDN. Log in using appropriate credentials.

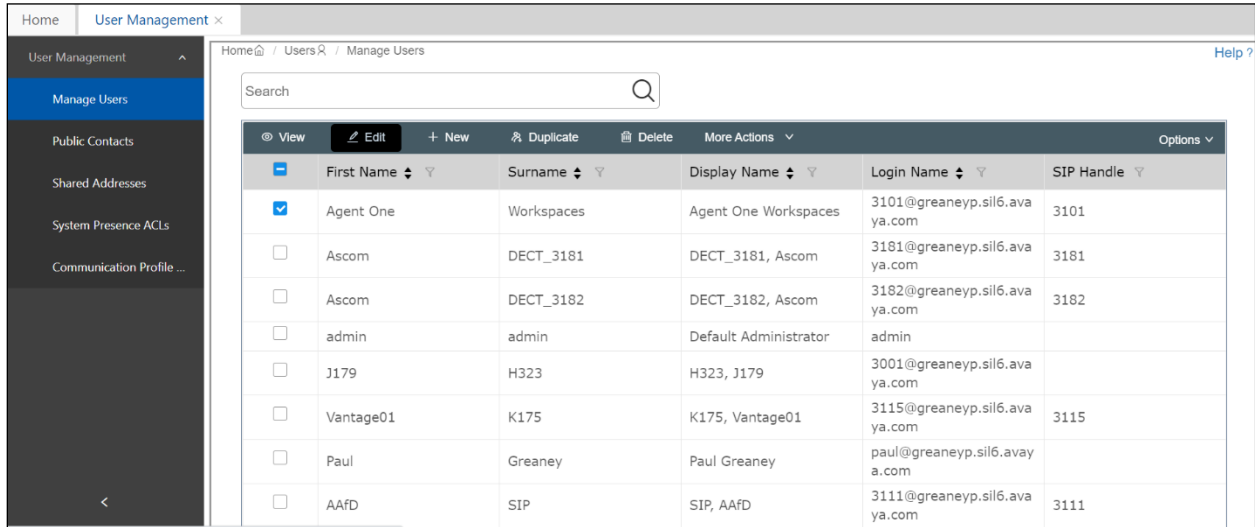
Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



From the home page, click on **Users → User Management → Manage Users**, as shown below.



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



Home / User Management x

User Management

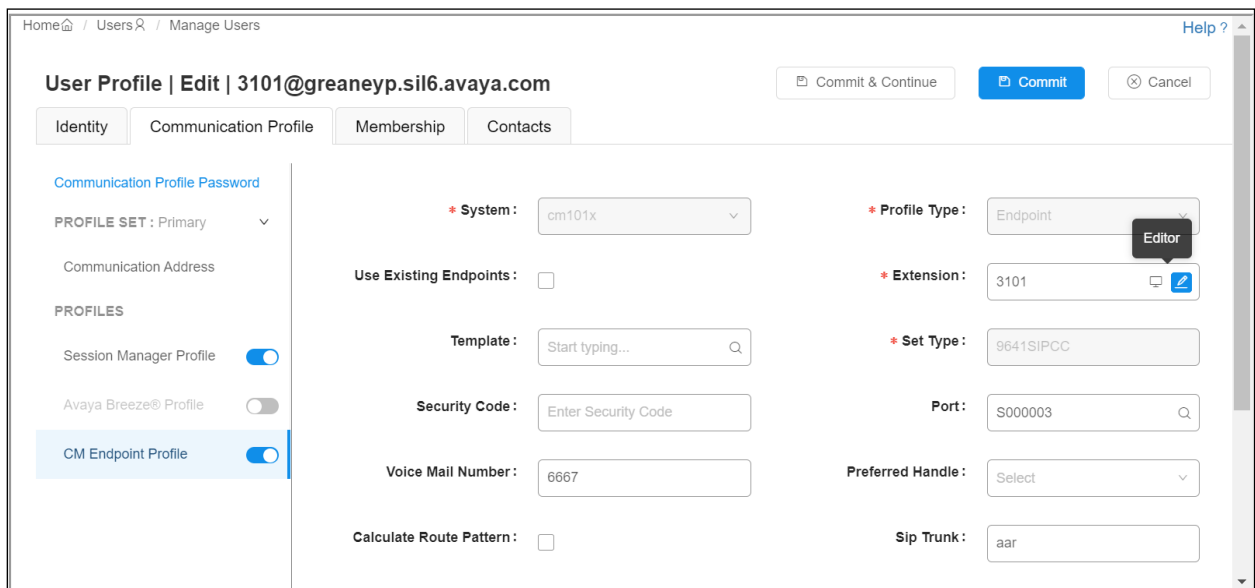
- Manage Users
- Public Contacts
- Shared Addresses
- System Presence ACLs
- Communication Profile ...

Home / Users / Manage Users

Search

View	Edit	New	Duplicate	Delete	More Actions	Options
First Name	Surname	Display Name	Login Name	SIP Handle		
<input checked="" type="checkbox"/>	Agent One	Workspaces	Agent One Workspaces	3101@greanep.sil6.ava ya.com	3101	
<input type="checkbox"/>	Ascom	DECT_3181	DECT_3181, Ascom	3181@greanep.sil6.ava ya.com	3181	
<input type="checkbox"/>	Ascom	DECT_3182	DECT_3182, Ascom	3182@greanep.sil6.ava ya.com	3182	
<input type="checkbox"/>	admin	admin	Default Administrator	admin		
<input type="checkbox"/>	J179	H323	H323, J179	3001@greanep.sil6.ava ya.com		
<input type="checkbox"/>	Vantage01	K175	K175, Vantage01	3115@greanep.sil6.ava ya.com	3115	
<input type="checkbox"/>	Paul	Greaney	Paul Greaney	paul@greanep.sil6.ava ya.com		
<input type="checkbox"/>	AAFD	SIP	SIP, AAFD	3111@greanep.sil6.ava ya.com	3111	

Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.



Home / Users / Manage Users

User Profile | Edit | 3101@greanep.sil6.ava.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System : cm101x

* Profile Type : Endpoint

Use Existing Endpoints : ☐

* Extension : 3101

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000003

Voice Mail Number : 6667

Preferred Handle : Select

Calculate Route Pattern : ☐

Sip Trunk : aar

Editor

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below. Click on **Done**, at the bottom of the screen, once this is set, (not shown).

System	cm101x	Extension	3101
Template	Select	Set Type	9641SIPCC
Port	S000003	Security Code	
Name	Agent One Workspaces		

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	3101	* Message Lamp Ext.	3101
* Tenant Number	1		
* SIP Trunk	Qaar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	<input type="checkbox"/>	Localized Display Name	Agent One Workspaces
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

SIP URI

Primary Session Manager

IPv4: 10.10.40.12 **IPv6:**

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	Auto Answer	none
MWI Served User Type	None	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
IP Phone Group ID		Hunt-to Station	
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
AUDIX Name	None	Time of Day Lock Table	None
Short/Prefixed Registration Allowed	default		
Voice Mail Number	6667	Music Source	
Bridging Tone for This Extension	no		

Features

<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference
<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting

The buttons were set as shown below but these are not critical to the overall operation of the call recording. Click on **Done** at the bottom of the screen (not shown).

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

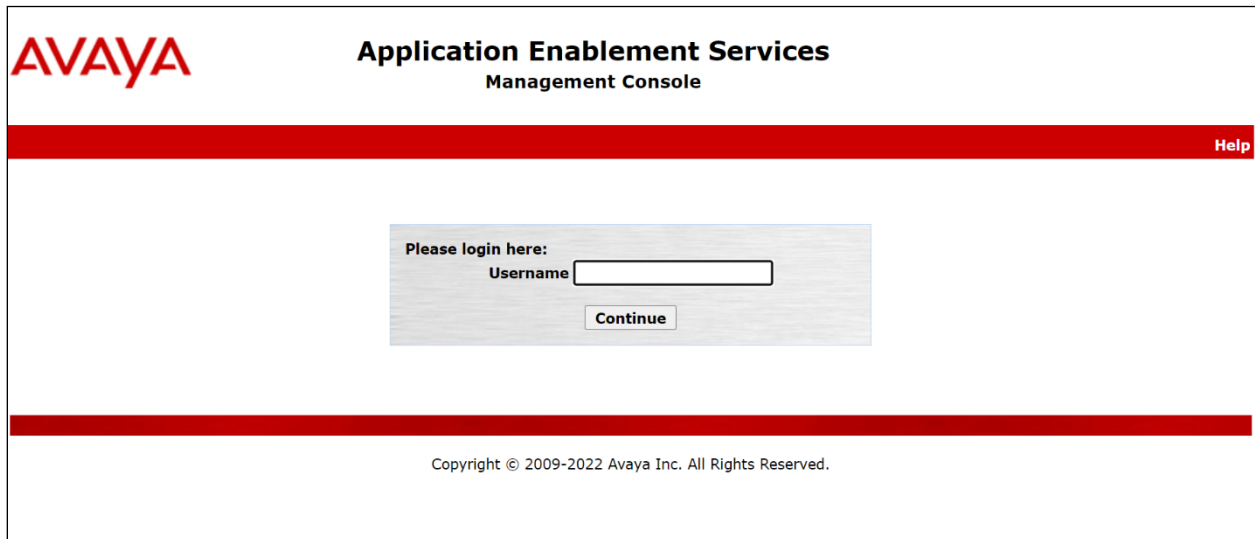
6. Configure Avaya Aura® Application Enablement Services

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
- Configure Networking Ports
- Create CTI User
- Configure Security
- Restart AE Server

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 screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a login box with the text "Please login here:" and "Username" followed by a text input field. A "Continue" button is located below the input field. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot shows the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is selected. The main content area displays a table of services and their status.

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	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

Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. A tooltip message states: '* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.' At the bottom, 'License Information' indicates: 'You are licensed to run Application Enablement (CTI) release 8.x'.

The TSAPI and DMCC licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

The screenshot shows the 'Licensing' management console. The left navigation menu has 'Licensing' selected. The main content area is titled 'Licensing' and provides instructions for setting up and maintaining the WebLM. It lists three scenarios: setting up/maintaining WebLM, importing/setting up/maintaining the license, and administering reserved licenses. A red note at the bottom states: 'NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page'.

The following screen shows the available licenses for **TSAPI** and **DMCC** users.

▼ Application_Enablement

View license capacity

View peak usage

ASBCE

▶ Session_Border_Controller_E_AE

AVAYA_OCEANA

▶ Avaya_Oceana

CCTR

▶ ContactCenter

CE

▶ COLLABORATION_ENVIRONMENT

COLLABORATION_DESIGNER

▶ Collaboration_Designer

COLLABORATIVE_BROWSING_SNAP-IN

▶ Collaborative_Browsing_Snap_In


COMMUNICATION_MANAGER

▶ Call_Center

▶ Communication_Manager

License File Host IDs:

Licensed Features

10 Items  Show All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

6.2. Create Switch Connection

Typically, the connection between the AES and Communication Manager is set up as part of the initial installation and would not usually be outlined in these Application Notes. Due to the nature of this particular setup with two connections from Communication Manager to two separate AES's the switch connection will be displayed on this section. From the AES Management Console navigate to **Communication Manager Interface → Switch Connections**, the connection to Communication Manager should be present as shown below but if one is not present one can be added by clicking on **Add Connection**.

Application Enablement Services

Management Console

Welcome: User cust
Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Sep 20 15:52:43 IST 2022
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

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
cm101x	Yes	30	1

Edit Connection
Edit PE/CLAN IPs
Edit Signaling Details
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 Error! Reference source not found.** A connection from the NICE server to the AES could not be made with **Secure H323 Connection** ticked and so this was left unticked, as shown below. Click **Apply** to save changes.

Communication Manager Interface | Switch Connections

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Networking

Security

Status

User Management

Connection Details - cm101x

Switch Password

.....

Confirm Switch Password

.....

Msg Period

30

Minutes (1 - 72)

Provide AE Services certificate to switch

☒

Secure H323 Connection

☐

Processor Ethernet

☒

Enable TLS Certificate Validation

☐

Apply

Cancel

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 0** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

Communication Manager Interface | Switch Connections

Home | Help | Logout

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Edit Processor Ethernet IP - cm101x


10.10.40.13

Add/Edit Name or IP

Name or IP Address	Status
10.10.40.13	In Use

Back

Clicking on **Edit Signaling Details** below brings up the H.323 Gatekeeper page.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Sep 20 15:52:43 IST 2022
HA Status: Not Configured

Communication Manager Interface | Switch ConnectionsHome | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm101x	Yes	30	1

The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.

Communication Manager Interface | Switch Connections

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

Switch Connections

Edit H.323 Gatekeeper - cm101x

Name or IP Address

☒ 10.10.40.13

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.

The screenshot shows the 'AE Services | TSAPI | TSAPI Links' management console. On the left is a navigation menu with 'AE Services' expanded, showing options like CVLAN, DLG, DMCC, SMS, and 'TSAPI' (which is further expanded to show 'TSAPI Links' and 'TSAPI Properties'). The main content area is titled 'TSAPI Links' and contains a table with two columns: 'Link' and 'Switch Connection'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

Link	Switch Connection
------	-------------------

[Add Link](#) [Edit Link](#) [Delete Link](#)

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 **cm101x**, 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:** **12** was used for compliance testing but the latest version available can be chosen).
- **Security:** This can be left at the default value of **both**. An unencrypted TSAPI link was used.

Once completed, select **Apply Changes**.

AE Services | TSAPI | TSAPI Links

▼ **AE Services**

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ **TSAPI**

▪ **TSAPI Links**

▪ TSAPI Properties

▶ TWS

▶ **Communication Manager Interface**

Edit TSAPI Links

Link1

Switch Connectioncm101x ▼


Switch CTI Link Number1 ▼

ASAI Link Version12 ▼

SecurityBoth ▼

Apply ChangesCancel ChangesAdvanced Settings

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

Apply Changes to Link
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.**

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

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm101x	1	12	Both

6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure NICE Inform Recorder in **Section 7.1**. The Tlink for the unencrypted TSAPI link was used.

Security | Security Database | Tlinks

▶ **AE Services**

▶ **Communication Manager Interface**

High Availability

▶ **Licensing**

▶ **Maintenance**

▶ **Networking**

▼ **Security**

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ **Security Database**

▪ Control

⊕ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

▪ Tlink Groups

▪ Worktops

Tlinks

Tlink Name

☒ AVAYA#CM101X#CSTA#AESPRI101X

☐ AVAYA#CM101X#CSTA-S#AESPRI101X

Delete Tlink

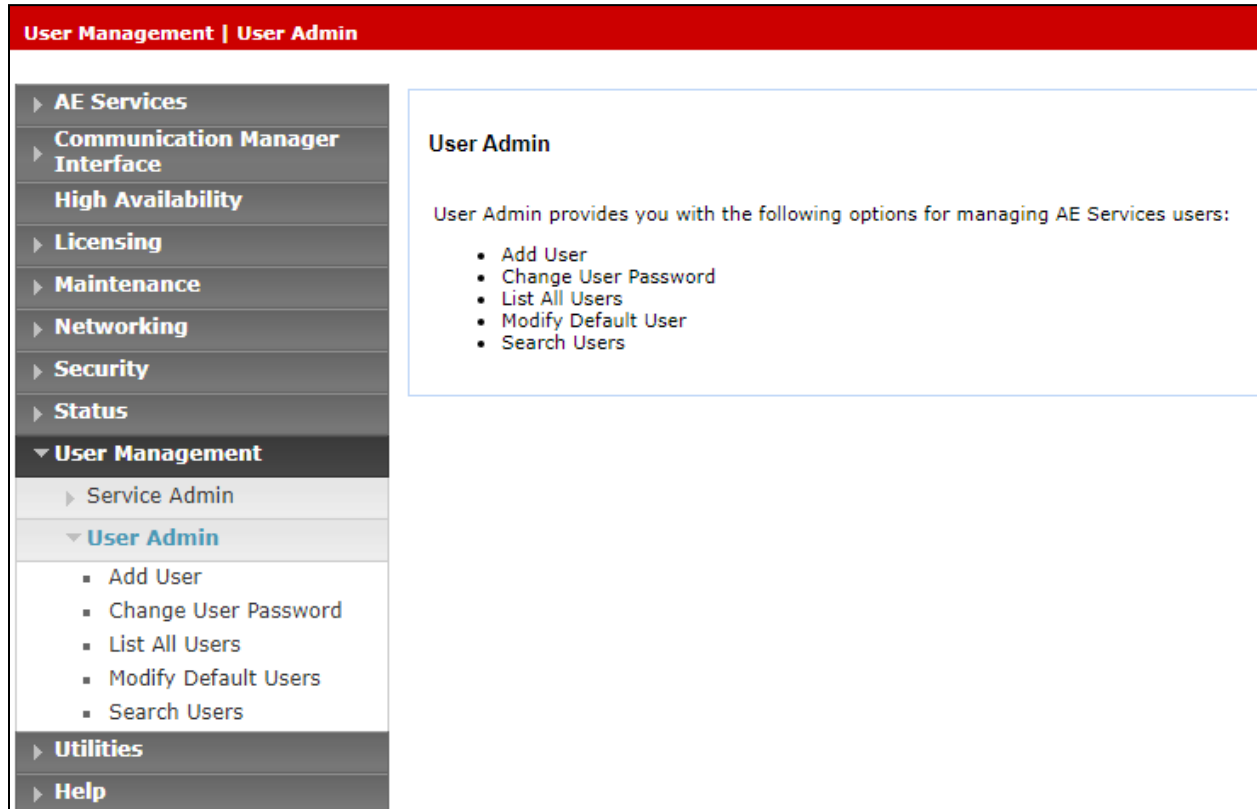
6.5. Configure Networking Ports

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**.

Networking Ports				
<ul style="list-style-type: none"> AE Services Communication Manager Interface High Availability Licensing Maintenance Networking AE Service IP (Local IP) Network Configure Ports TCP/TLS Settings Security Status User Management Utilities Help 	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"/>	
H.323 Ports				
TCP Port Min	<input type="text" value="20000"/>			
TCP Port Max	<input type="text" value="29999"/>			
Local UDP Port Min	<input type="text" value="20000"/>			
Local UDP Port Max	<input type="text" value="29999"/>			
			Enabled Disabled	
Server Media		<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.

High Availability	* User Id	nice1
▶ Licensing	* Common Name	nice1
▶ Maintenance	* Surname	nice1
▶ Networking	User Password
▶ Security	Confirm Password
▶ Status	Admin Note	
▼ User Management	Avaya Role	None ▼
▶ Service Admin	Business Category	
▼ User Admin	Car License	
▪ Add User	CM Home	
▪ Change User Password	Css Home	
▪ List All Users	CT User	Yes ▼
▪ Modify Default Users	Department Number	
▪ Search Users	Display Name	
▶ Utilities	Employee Number	
▶ Help	Employee Type	
	Enterprise Handle	

Scroll down and click on **Apply Changes** (not shown).

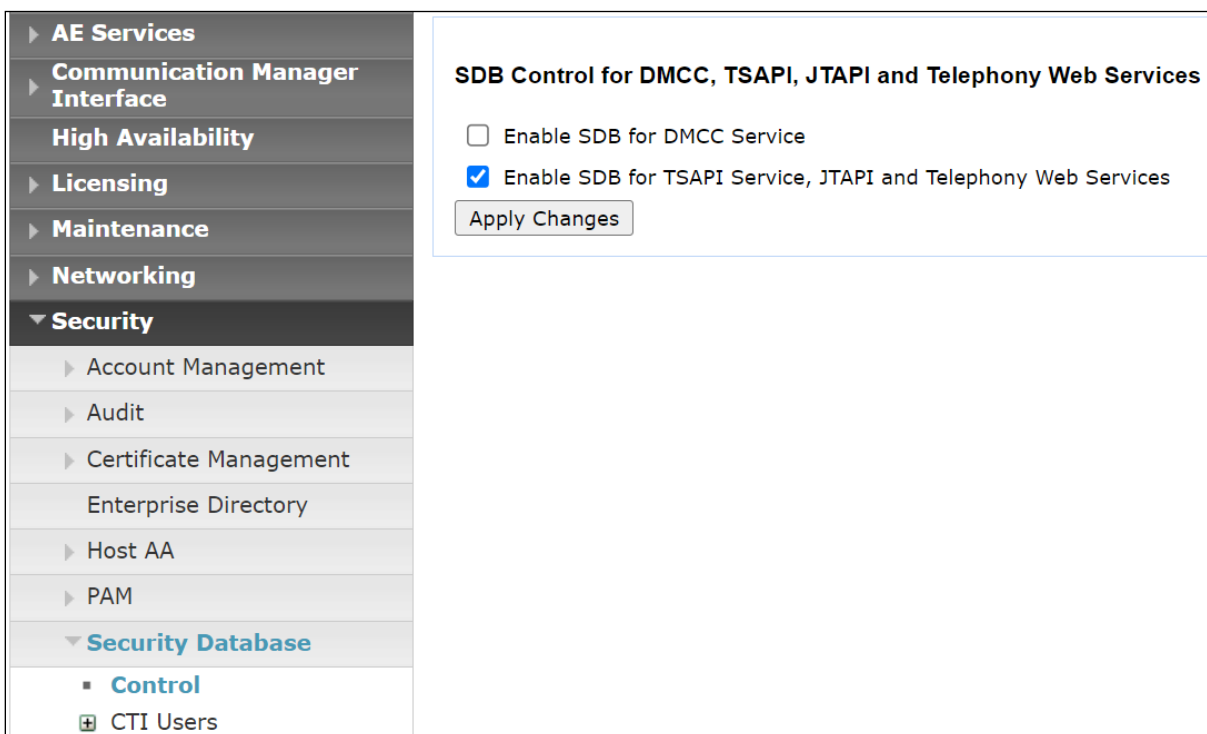
6.7. Configure Security

The CTI user permissions and the database security are set under **Security Database**.

6.7.1. Configure Database Control

The security database can be set differently depending on the requirements of the customer in question. For compliance testing, the DevConnect lab was setup as shown below, however this may be changed by opening **Control** and ticking the boxes shown.

Note: Since the CTI user was given unrestricted access, as per **Section 6.7.2**, these values set here do not impact the overall setup.



The screenshot shows a web-based configuration interface. On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' (unchecked) and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services' (checked). Below the checkboxes is an 'Apply Changes' button.

Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section** Error! Reference source not found. for more information on this.

6.7.2. 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**.

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> nice1	nice1	NONE	NONE
<input type="radio"/> paul1	paul1	NONE	NONE
<input type="radio"/> paul2	paul2	NONE	NONE
<input type="radio"/> sytel	Sytel	NONE	NONE

[Edit](#) [List All](#)

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

Edit CTI User

User Profile:

User ID: nice1
Common Name: nice1
Worktop Name: NONE
Unrestricted Access: ☒

Call and Device Control:

Call Origination/Termination and Device Status: None

Call and Device Monitoring:

Device Monitoring: None
Calls On A Device Monitoring: None
Call Monitoring: ☐

Routing Control:

Allow Routing on Listed Devices: None

[Apply Changes](#) [Cancel Changes](#)

6.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

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 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

A message confirming the restart will appear, click on **Restart** to proceed.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

Restart AE Server

Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

Restart

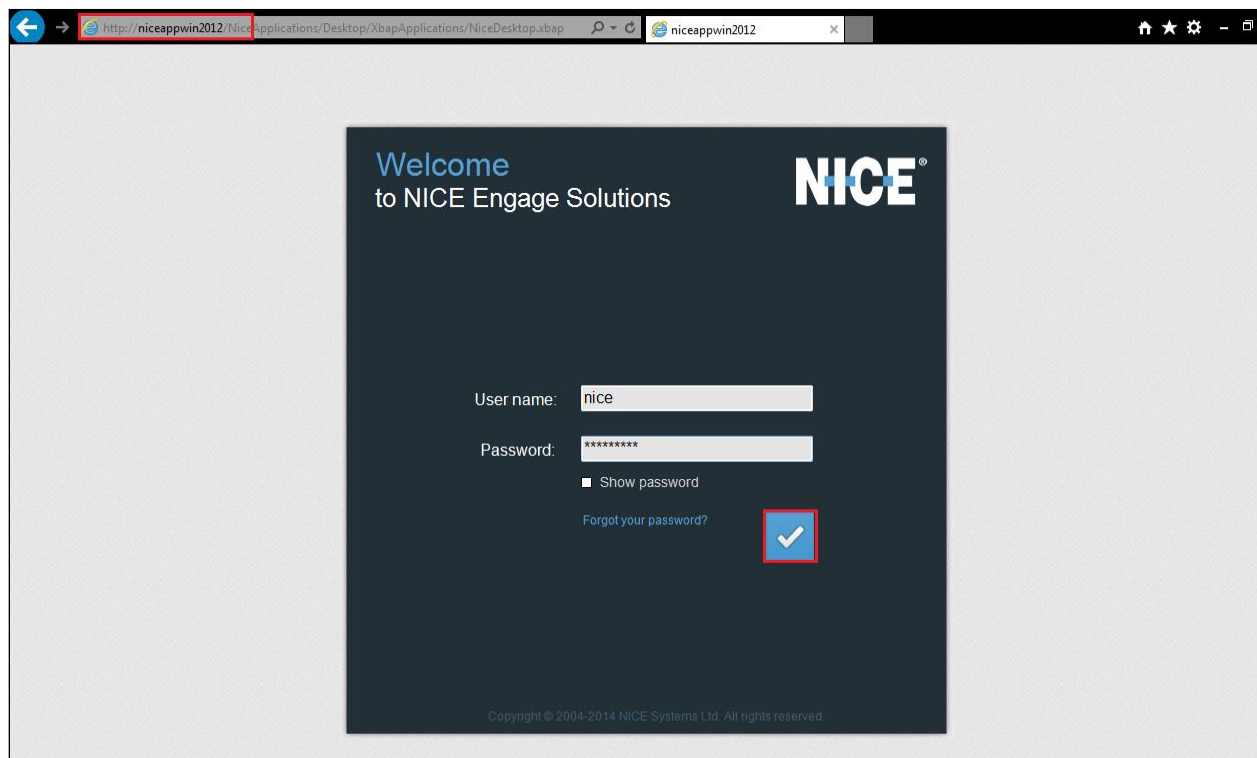
Cancel

7. Configure NICE Engage Platform

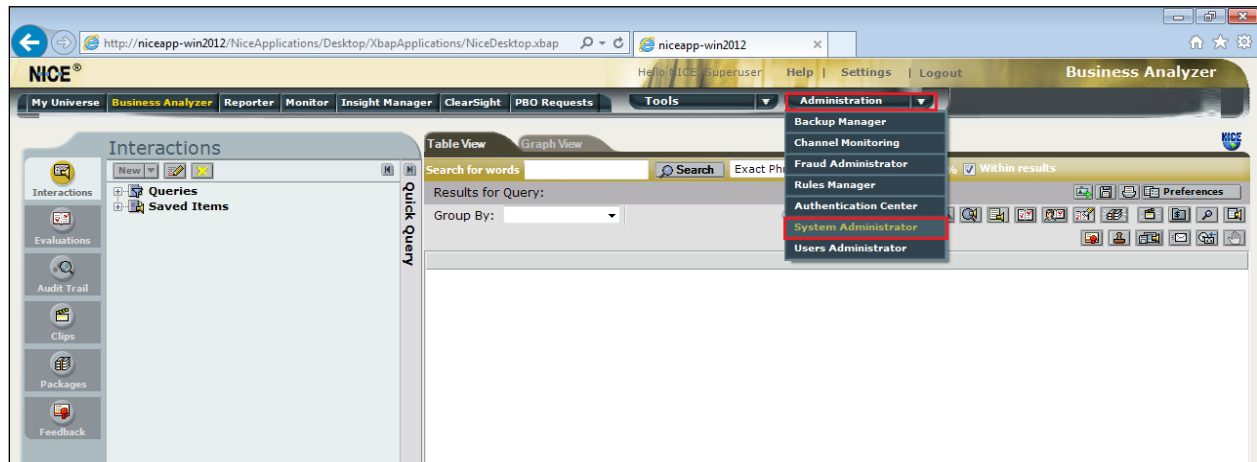
The installation of NICE Engage Platform is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of the NICE Engage Platform, contact NICE as per the information provided in **Section 2.3**.

The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya Solution.

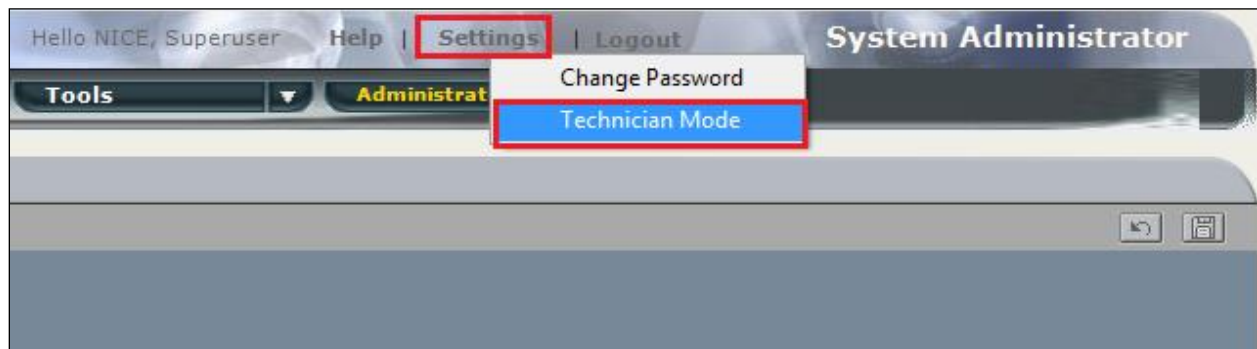
All configuration of the NICE Engage Platform for connection with the AES is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser as shown navigate to **http://<NICEEngageApplicationServerIP>/Nice** as shown below and enter the proper credentials and click on **Login**.



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

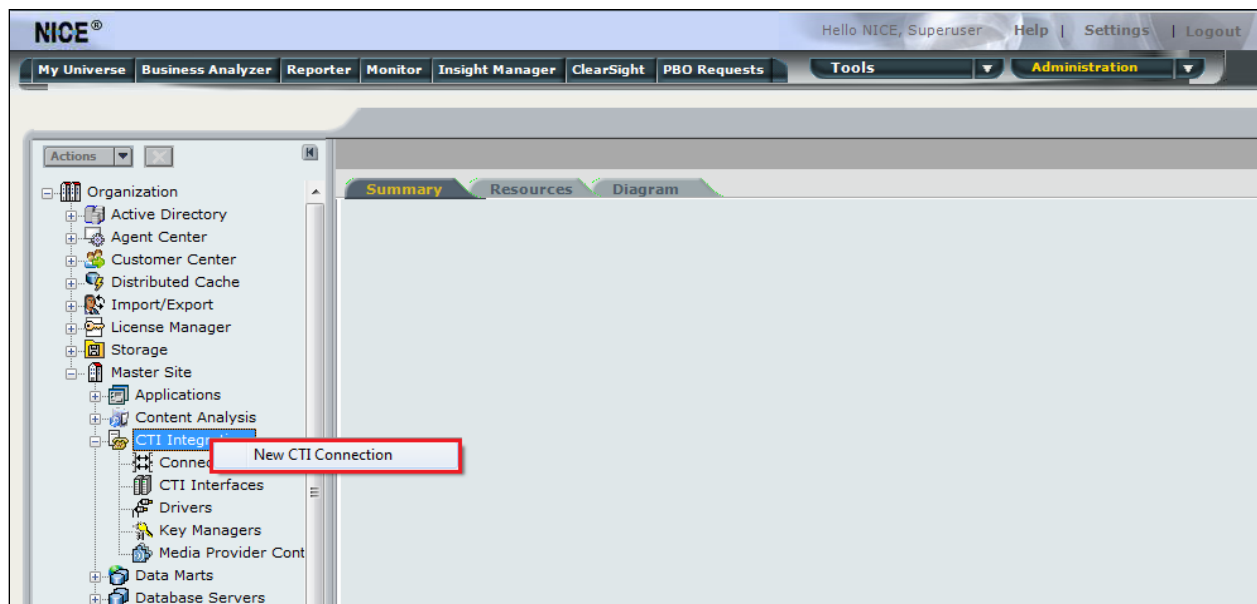


Before any changes can be made, switch to **Technician Mode** by clicking into **Settings** at the top of the screen as shown below.



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.

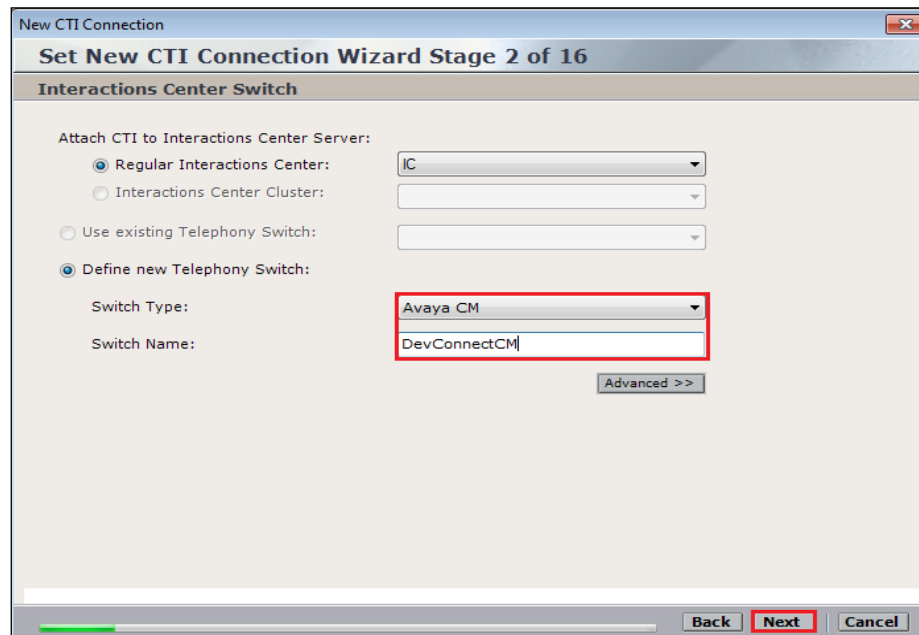


The **New CTI Connection Wizard** is opened, and this will go through the 16 steps required to set up the connection to the AES for DMCC Multiple Registration type of call recording. Click on **Next** to continue.

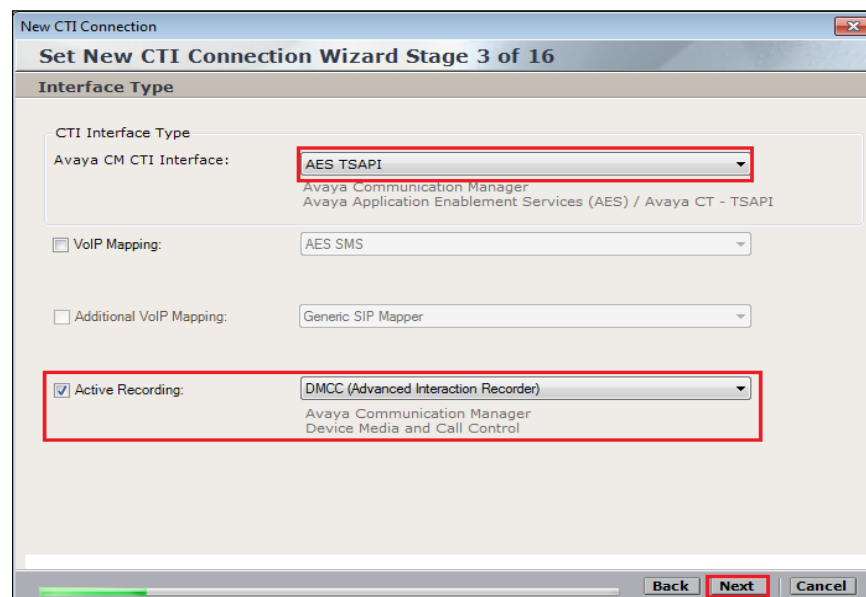


The value for **Regular Interactions Center (IC)** is a value that was already created during the installation of the NICE Engage platform. This value is therefore pre-chosen for the CTI connection being created below.

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 **Avaya CM CTI Interface**, ensure that **Active Recording** is ticked and select the **DMCC (Advanced Interaction 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 Tlink **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

ServerName

LoginID

Password

UseWarmStandBy

Description: Name: ServerName

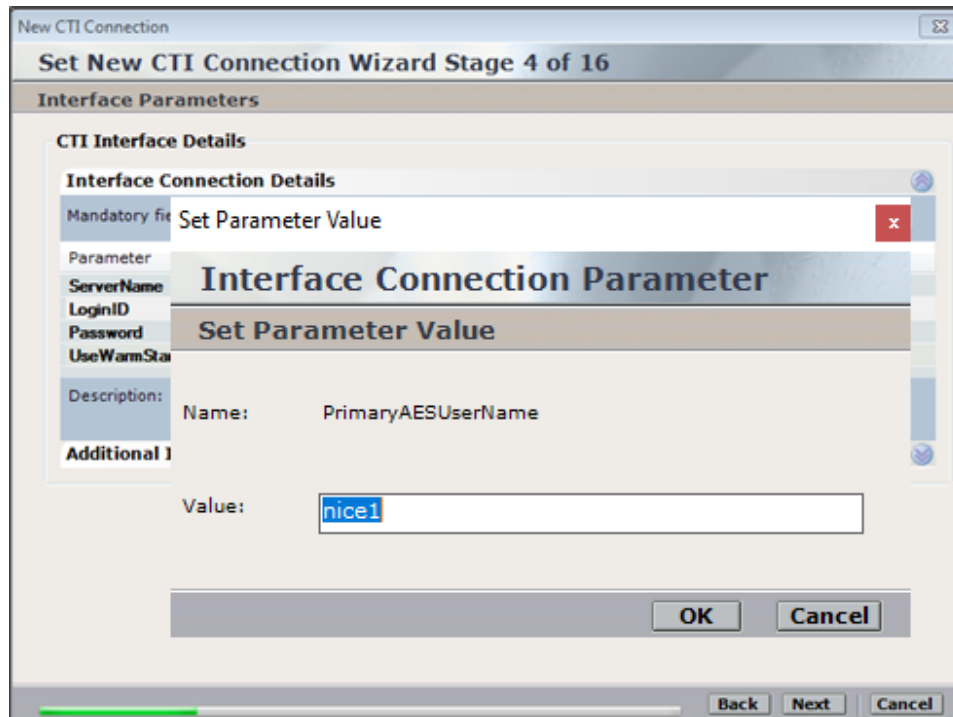
Additional Interface Parameters

Value: AVAYA#CM101X#CSTA#AESPRI101X

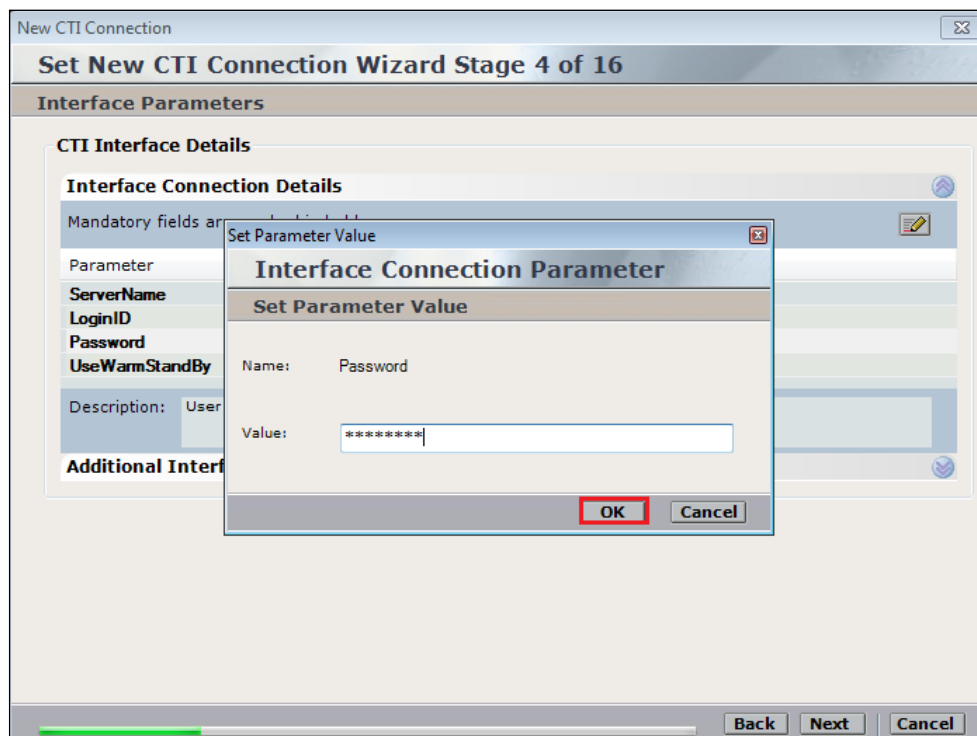
OK Cancel

Back Next 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.

General Interface Info

Interface Connection Details

☐ Display Read Only Information Mandatory fields are marked in bold [X] [Pencil] [Add]

Parameter	Value
ServerName	AVAYA#CM101X#CSTA#AESPRI101X
LoginID	nice1
Password
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

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

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
PrimaryAESServerAddress	
PrimaryAESDMCCPort	
PrimaryAESUserName	
PrimaryAESPassword	
PrimaryAESConnectToCTI	TRUE

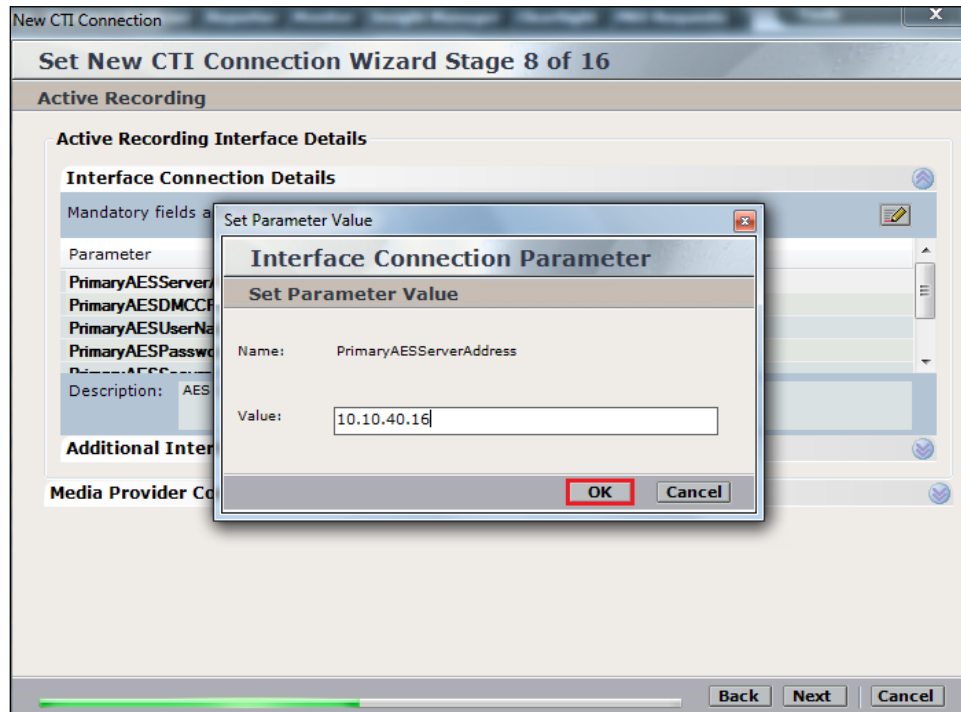
Description:

Additional Interface Parameters

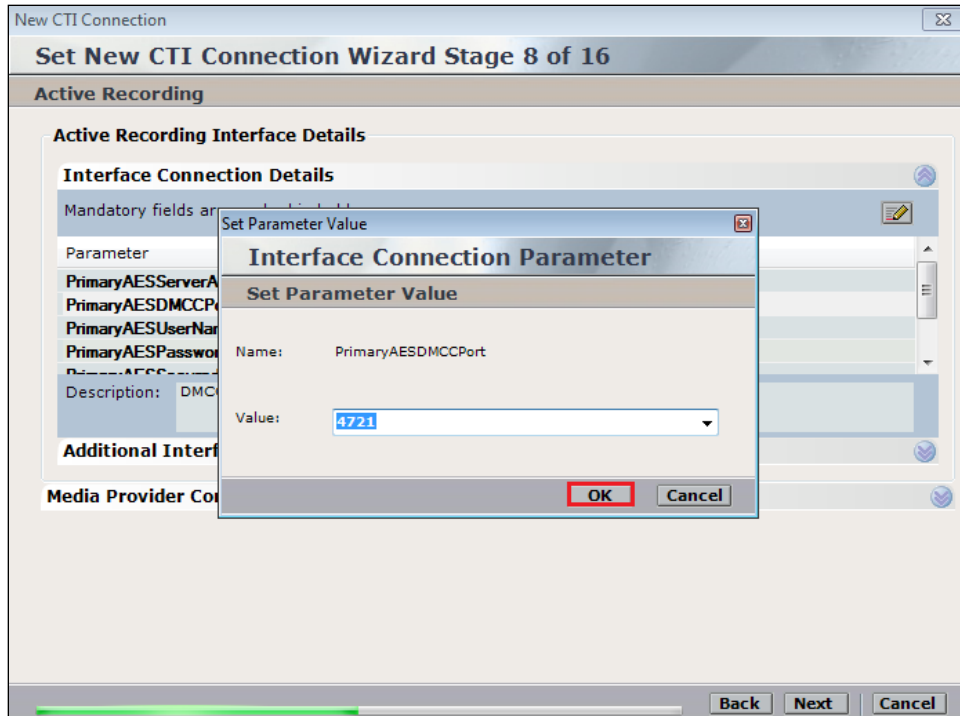
Media Provider Controllers - Location

[Back] **[Next]** [Cancel]

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



Enter the **Value** for the **PrimaryAESDMCCPort**, note this will be the same port that was configured in **Section Error! Reference source not found..** 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**.

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Mandatory fields are:

Parameter

- PrimaryAESDMCCP
- PrimaryAESUserName
- PrimaryAESPassword
- PrimaryAESSecure
- UseAESVoiceClass

Description: User

Additional Interf

Media Provider Co

Value: nice1

OK Cancel

Back Next Cancel

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

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Mandatory fields are:

Parameter

- PrimaryAESDMCCP
- PrimaryAESUserName
- PrimaryAESPassword
- PrimaryAESSecure
- UseAESVoiceClass

Description: Pass

Additional Interf

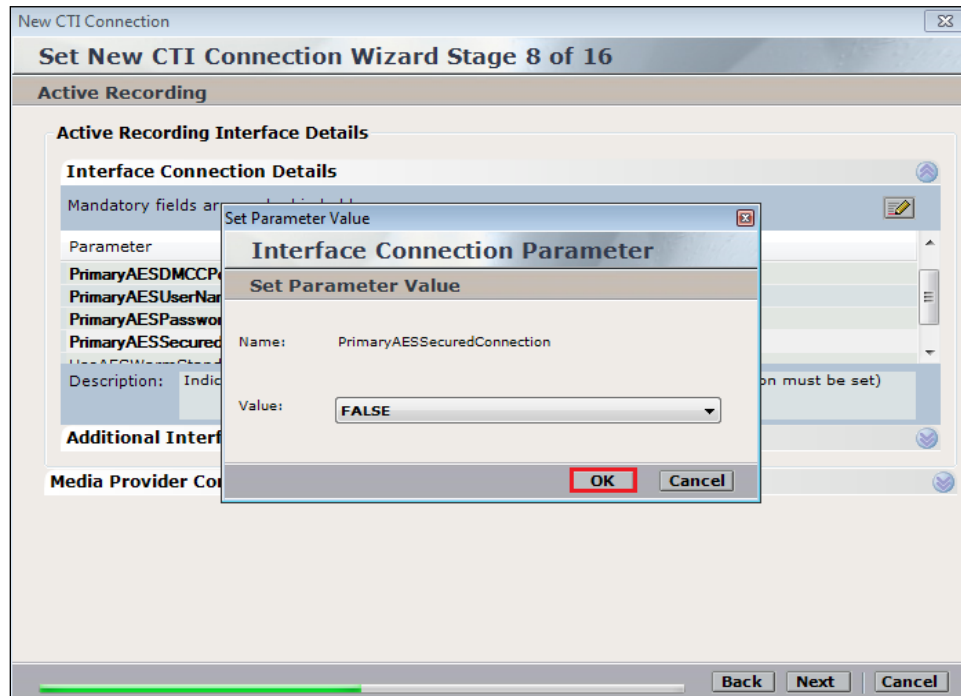
Media Provider Co

Value: *****

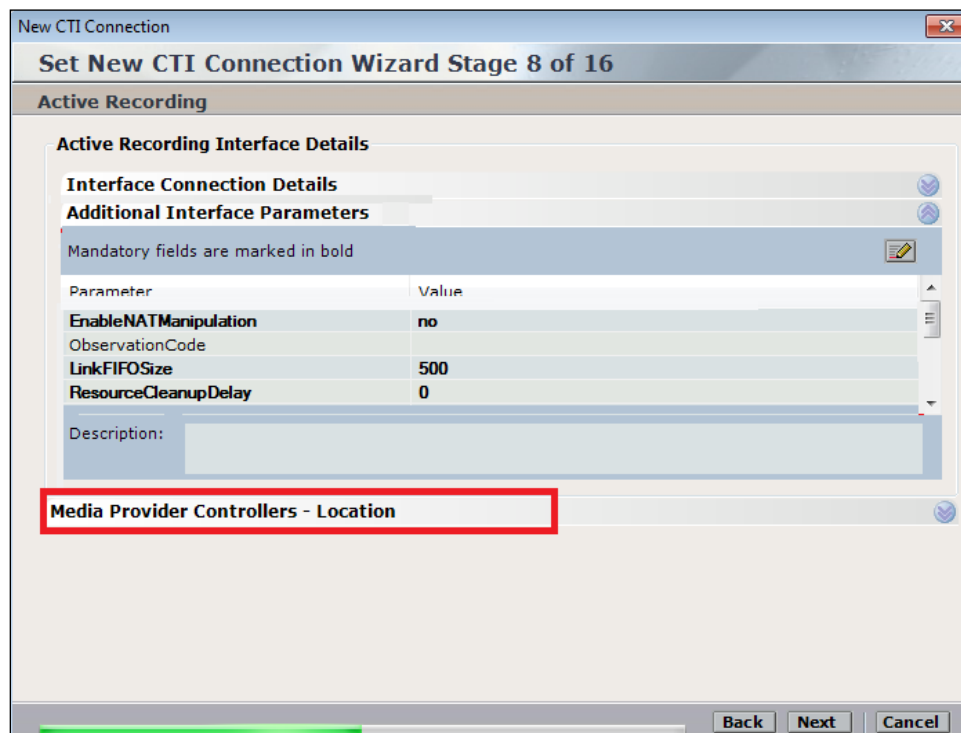
OK Cancel

Back Next Cancel

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



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



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

Buttons: Add (highlighted), Add Range, Add From Switch

Device Number/IP	CTI Trunk ID	Type

Buttons: Back, Next, Cancel

The **Device Type** should be **Extension** and insert the extension number of a phoneset that is to be recorded the example below showing extension **1001**. Expand **Advanced Device Parameters** and ensure that the **Value** for **Observation Type** is set to **Non-Resourced-Based**. Click on **OK** to continue.

New Switch

Available Device

Set New CTI In

Switch Devices Con

Add Device

Set Devices

Available Devices
Provide telephony sv
0 devices

Device Number

Name

Device Type: * Extension

Device Number: * 1001

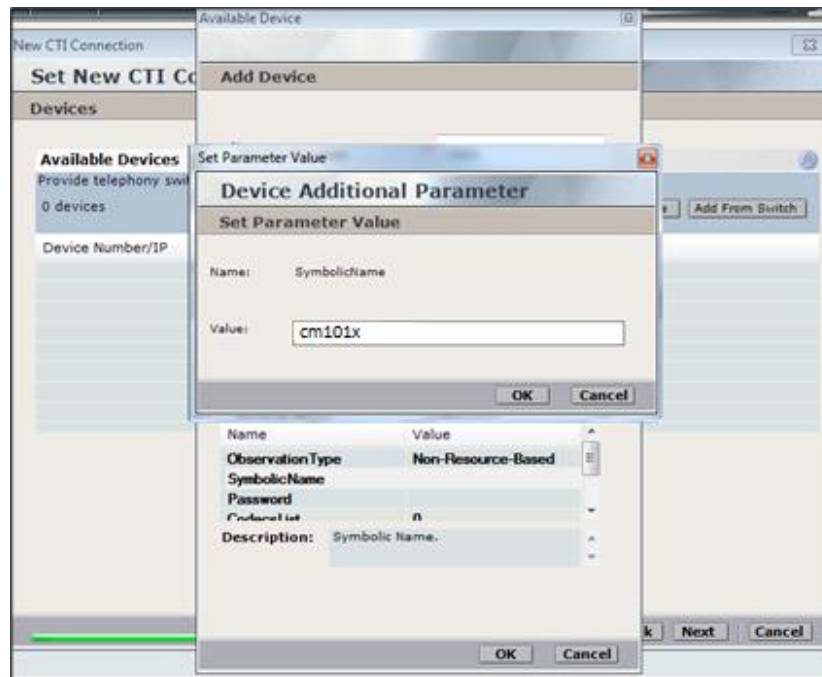
Advanced Device Parameters

☐ Display Read Only Information

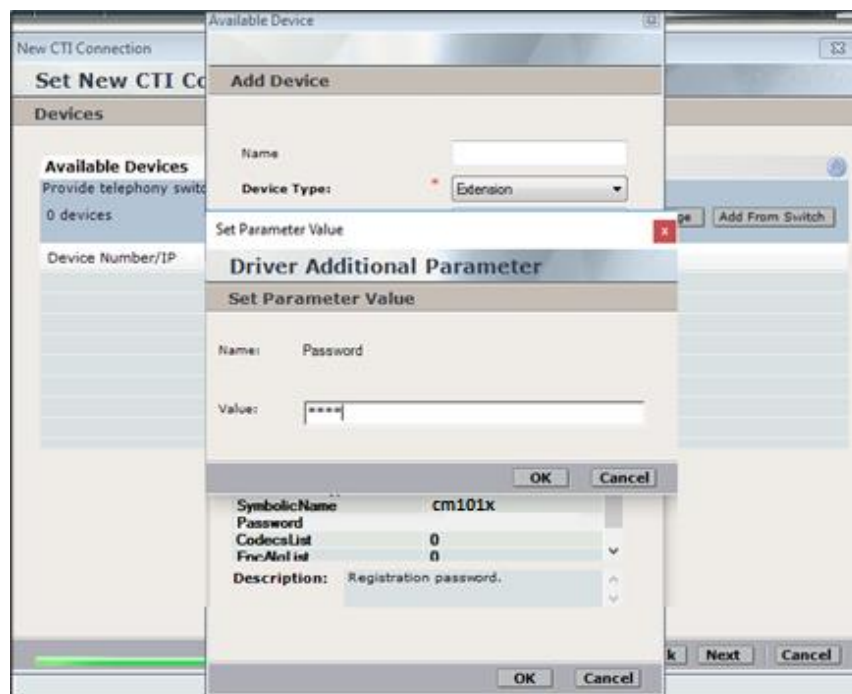
Name	Value
ObservationType	Non-Resource-Based
SymbolicName	
Password	
CodecsList	0
FuncAln list	0
Description:	Observation Type. Non-Resource-Based - can be recorded without the

Buttons: OK, Cancel, Cancel

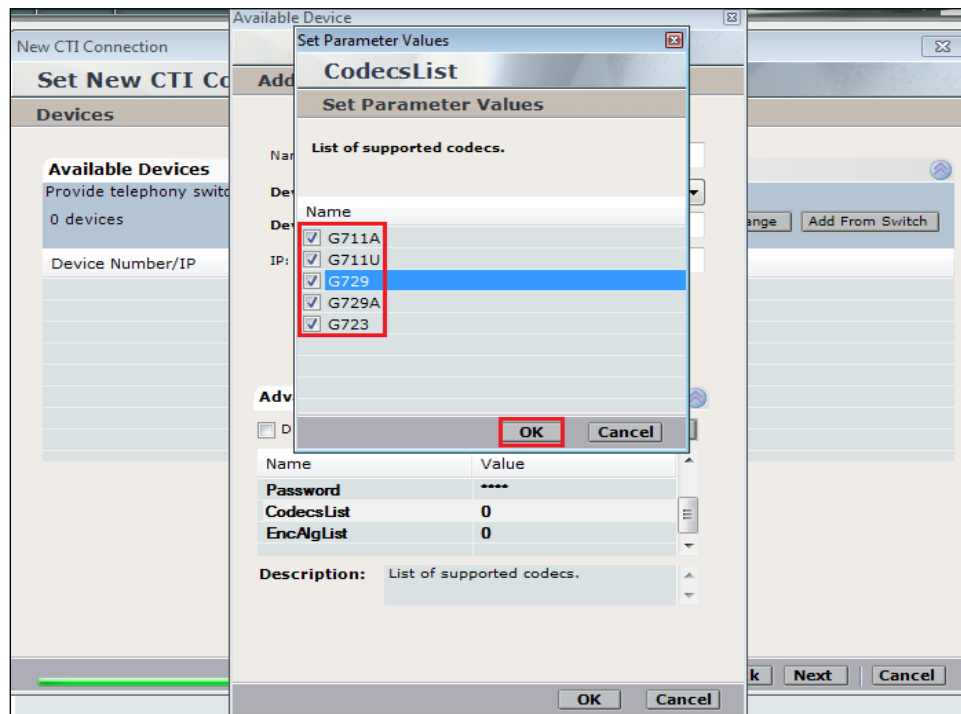
Enter the correct **Value** for **SymbolicName**. Double-click on **SymbolicName** to set the value. This should be the same as the switch name entered in **Section 6.2**.



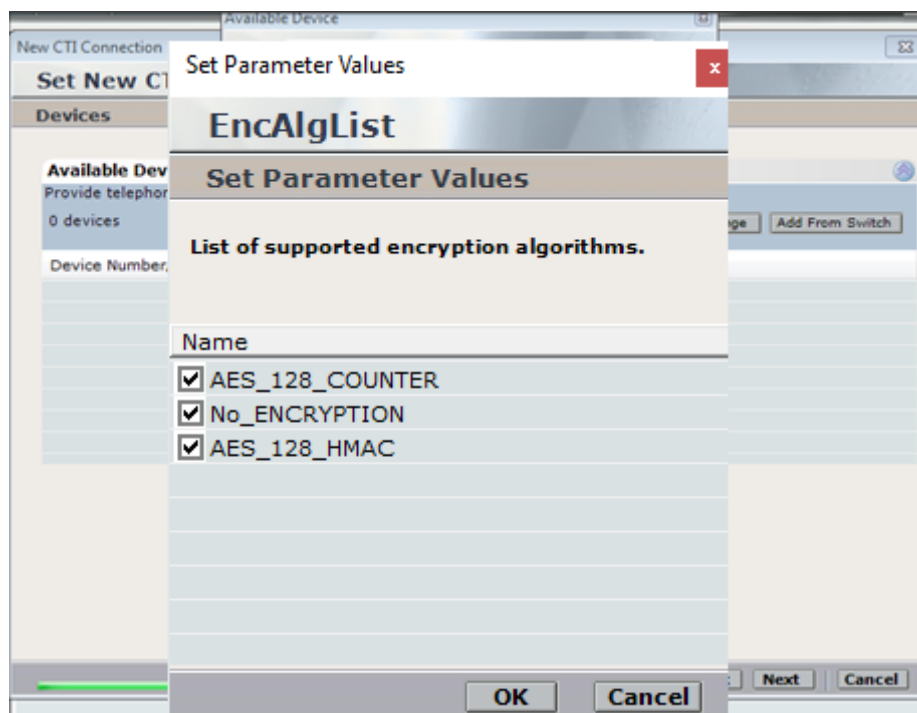
Enter the correct **Password** and note this is the password for the extension that is being added here. This is the station password which was entered during the creation of the station found in **Section 5.5** of these Application Notes.



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



Double-click on **EncAlgList**. To cover all options, all types of encryptions were ticked. 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'. It prompts the user to 'Provide telephony switch available devices' and shows '2 devices'. There are buttons for 'Add', 'Add Range', and 'Add From Switch'. A table lists the available devices:

Device Number	CTI Trunk ID	Type
1001		Extension
1050		Extension
1101		Extension
1110		Extension

At the bottom, there are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red box.

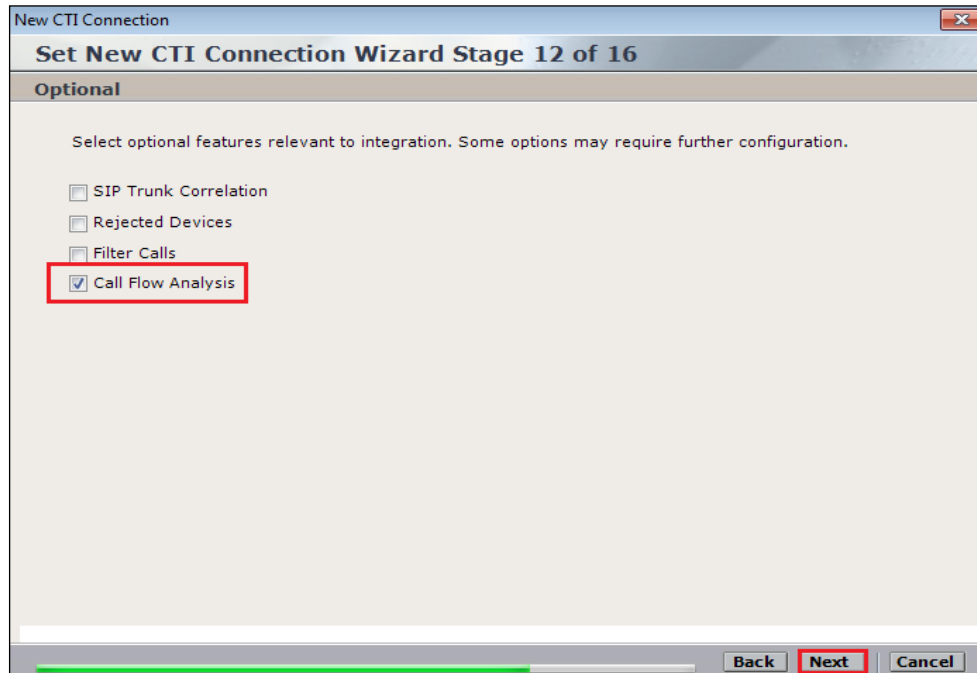
Select the new extension and click on the >> icon as shown. Click on **Next** to continue.

The screenshot shows the 'Set New CTI Connection Wizard Stage 11 of 16' window. The 'Monitor' section is active, prompting the user to 'Please select the devices to be monitored' and 'Double click on a monitored device for further configuration'. It shows 'Available Devices: 0 devices' and 'Monitored Devices: 1 devices'. There are buttons for '>>', '>', '<', and '<<'. A table lists the monitored devices:

Device	Type
1001	Extension

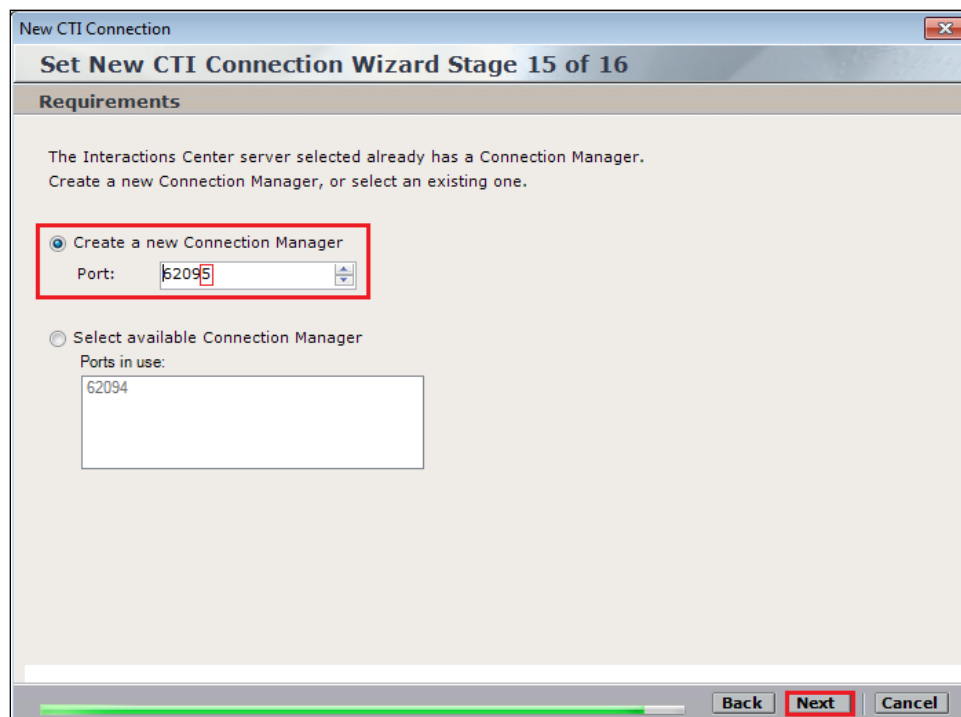
At the bottom, there are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red box.

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



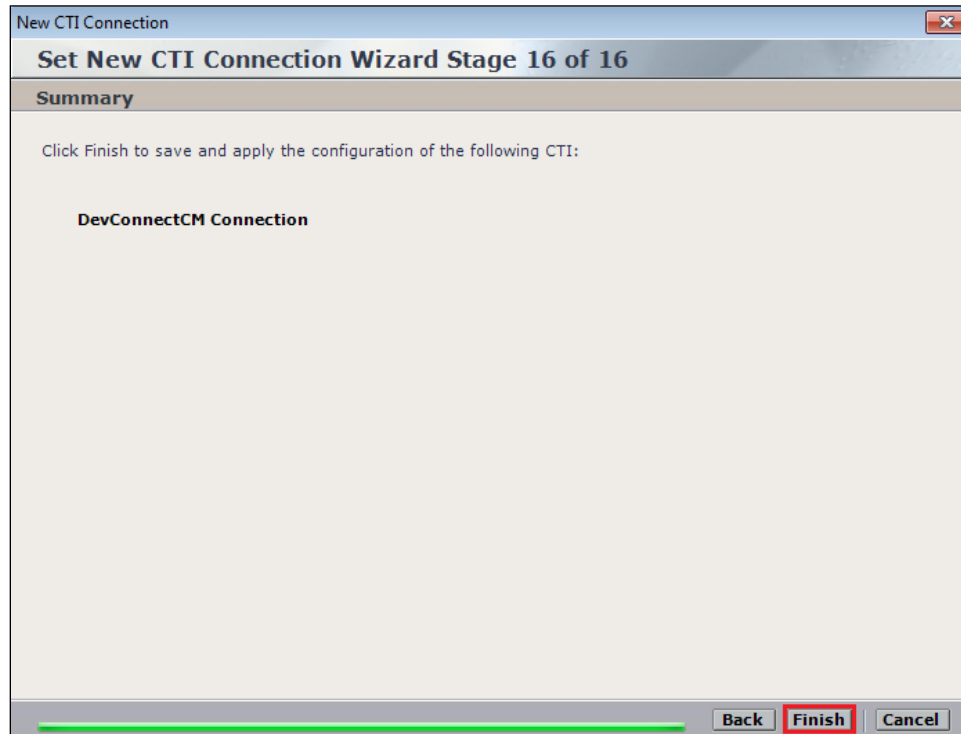
The screenshot shows a window titled "New CTI Connection" with a subtitle "Set New CTI Connection Wizard Stage 12 of 16". The main section is labeled "Optional" and contains the text: "Select optional features relevant to integration. Some options may require further configuration." Below this text are 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 of the window, there are three buttons: "Back", "Next" (highlighted with a red rectangle), and "Cancel". A 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.

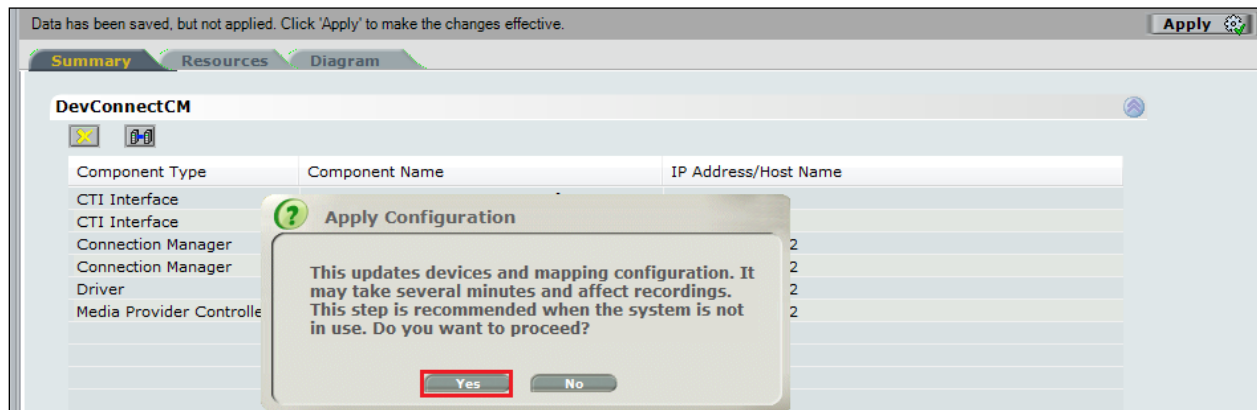


The screenshot shows a window titled "New CTI Connection" with a subtitle "Set New CTI Connection Wizard Stage 15 of 16". The main section is labeled "Requirements" and contains the text: "The Interactions Center server selected already has a Connection Manager. Create a new Connection Manager, or select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

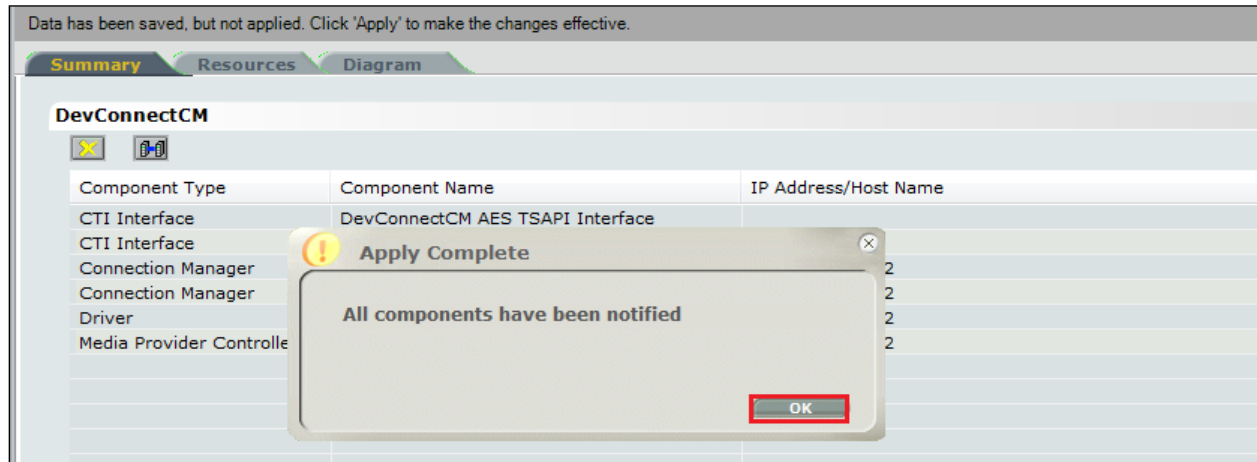
Click on **Finish** to complete the **New CTI Wizard**.



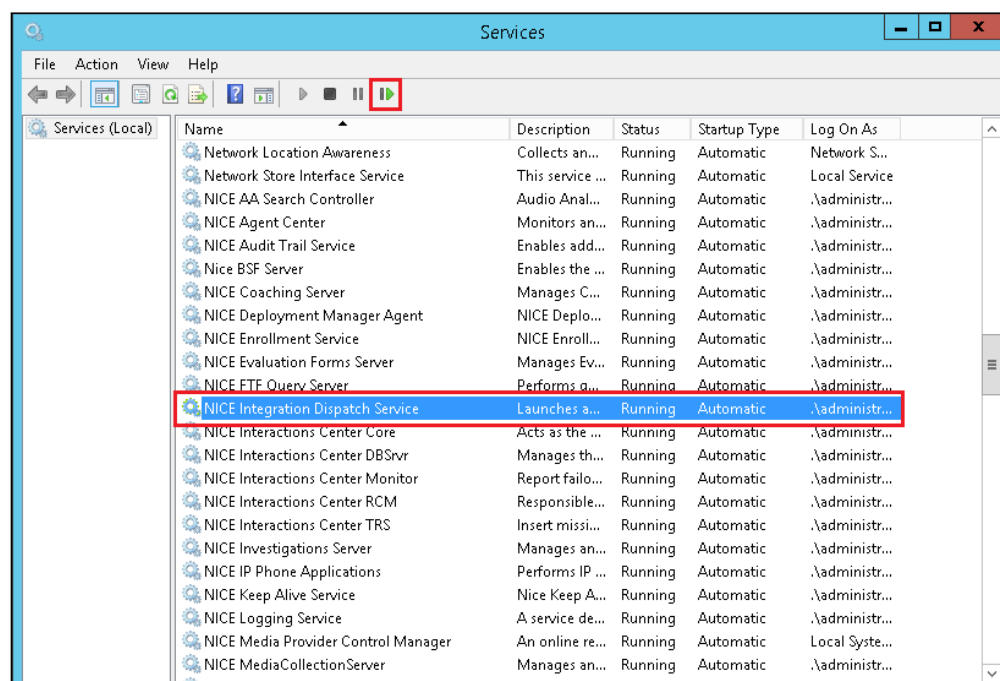
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed



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

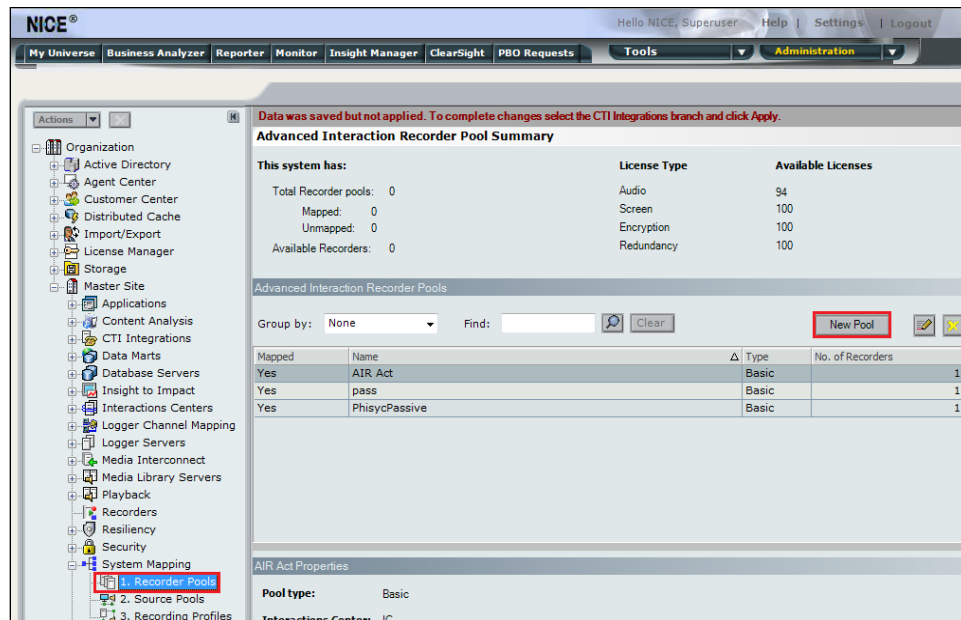


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

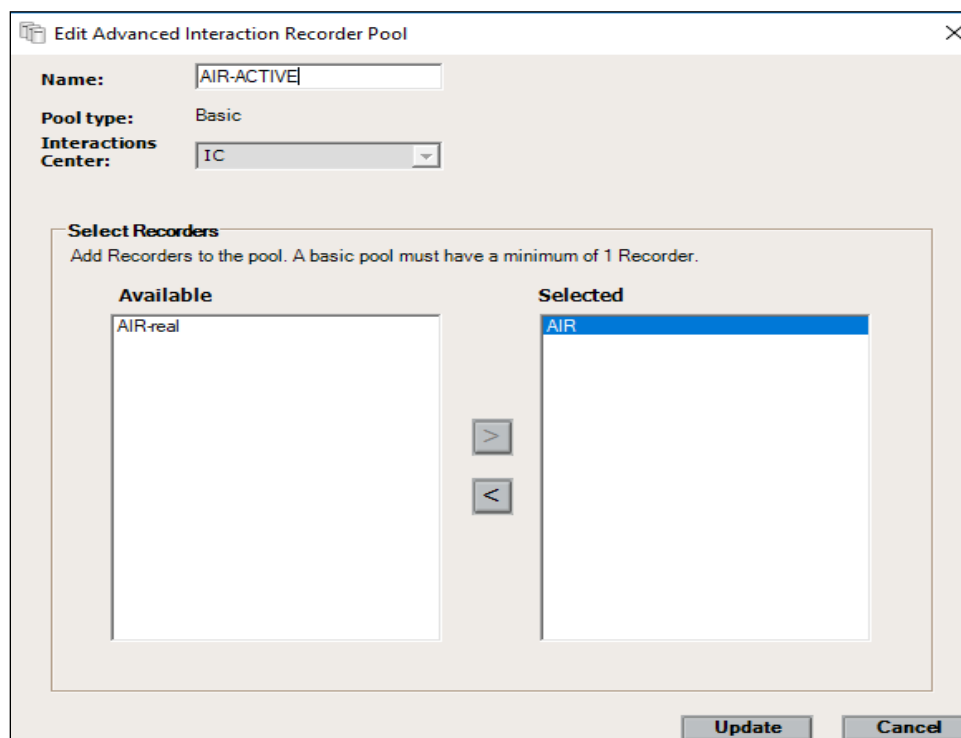


7.2. System Mapping

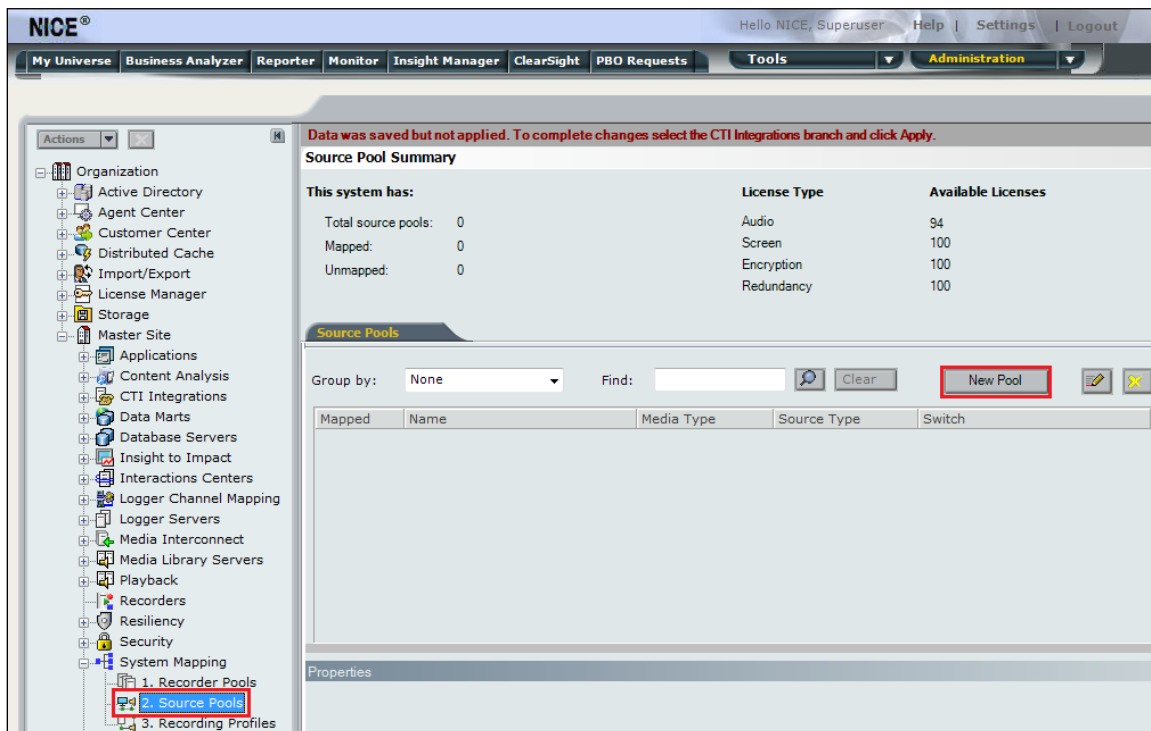
From the web browser navigate to **Master Site → System Mapping → Recorder Pools**. In the main window click on **New Pool**.



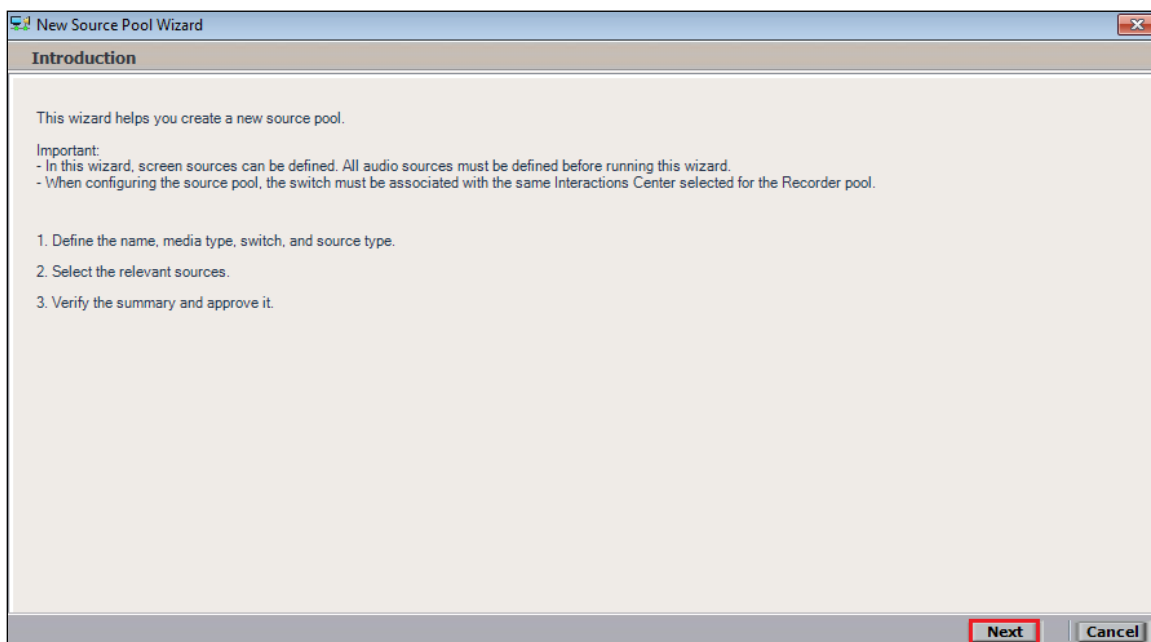
Enter a suitable **Name** for the **Recorder Pool** and select the **AIR** from the list of **Available Recorders** and click on **Update** to continue.



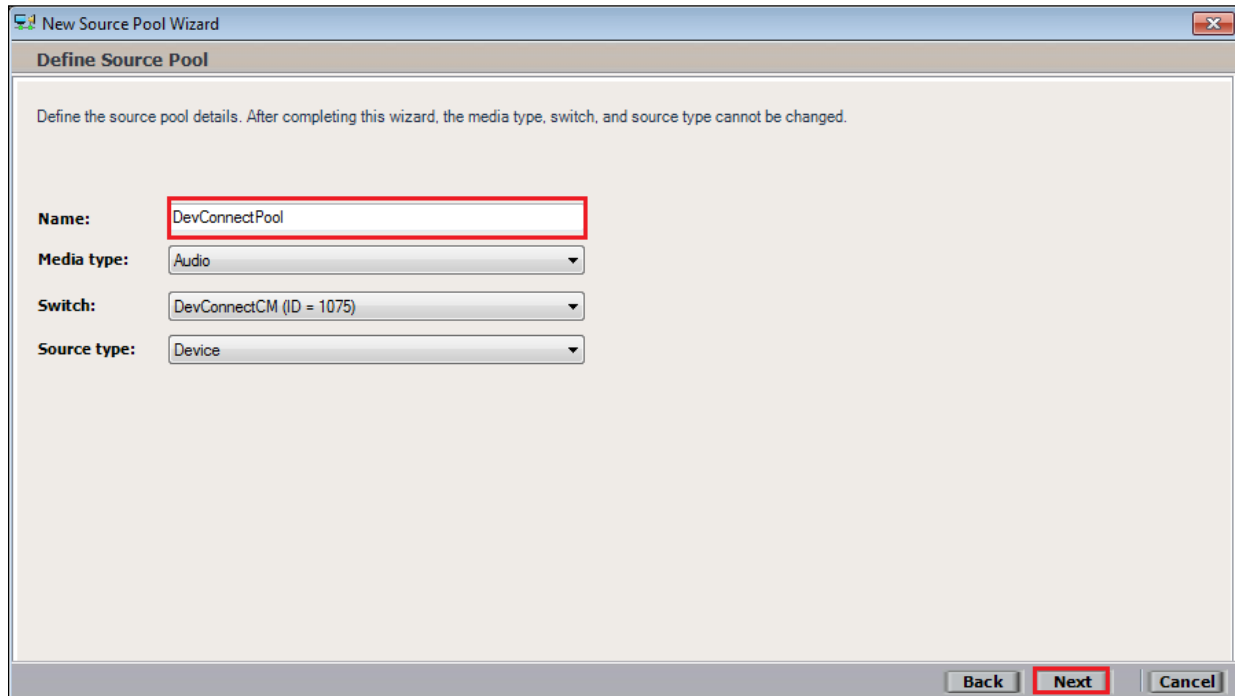
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



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

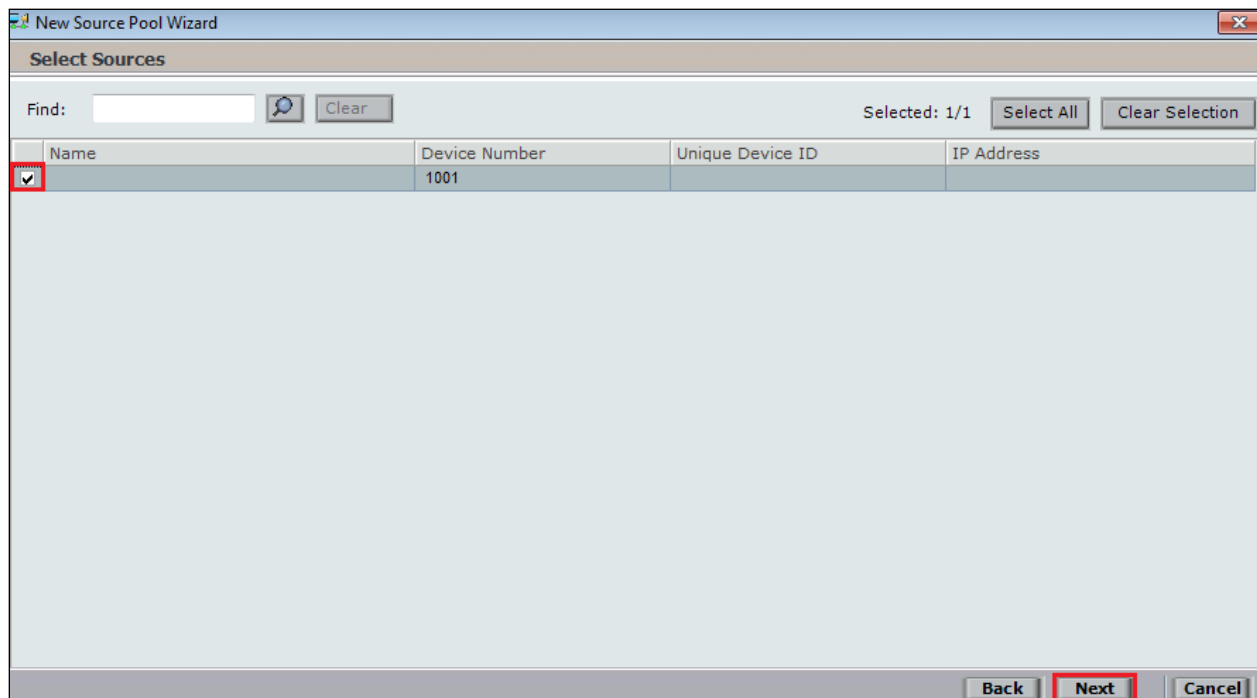
Media type: Audio

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 'Find:' search bar with a magnifying glass 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 '1001'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red border.

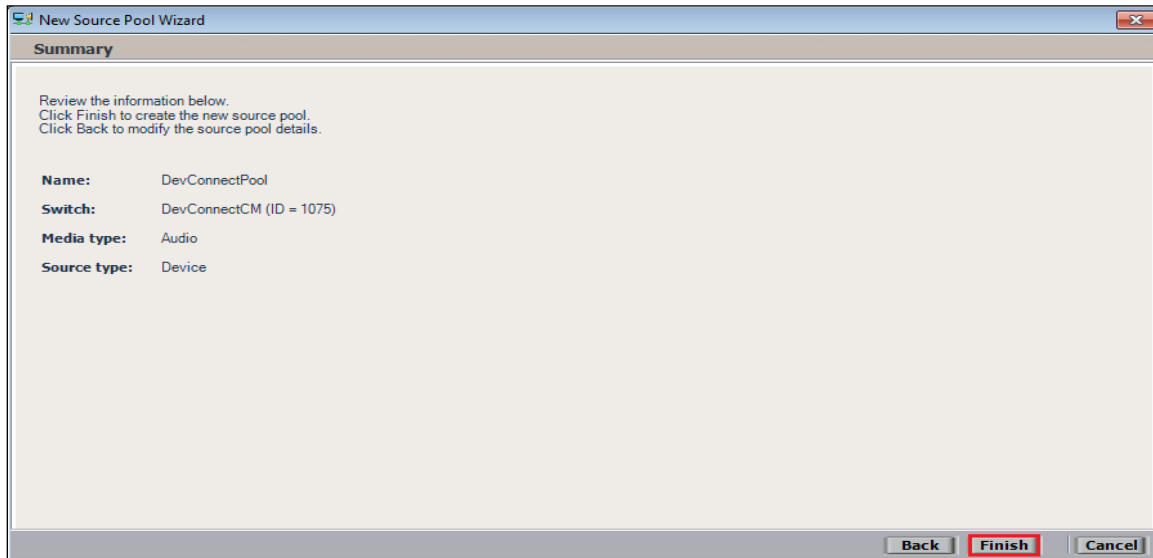
Find: [Search Bar] Clear

Selected: 1/1 Select All Clear Selection

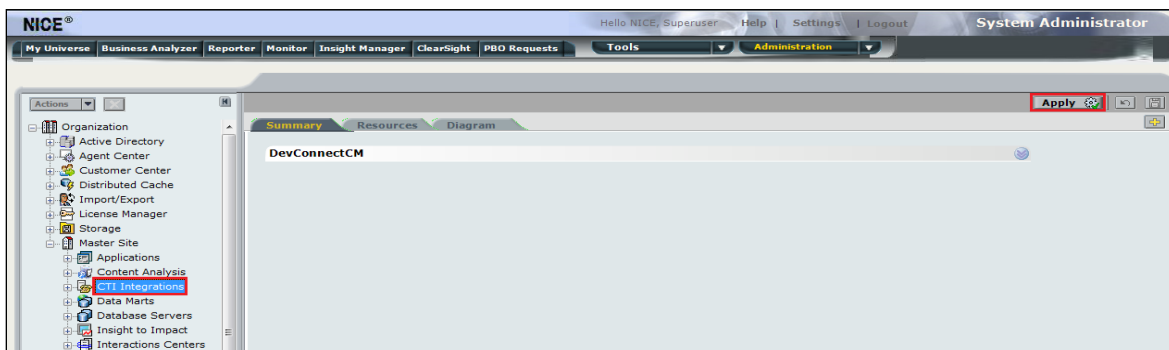
Name	Device Number	Unique Device ID	IP Address
<input checked="" type="checkbox"/>	1001		

Back Next Cancel

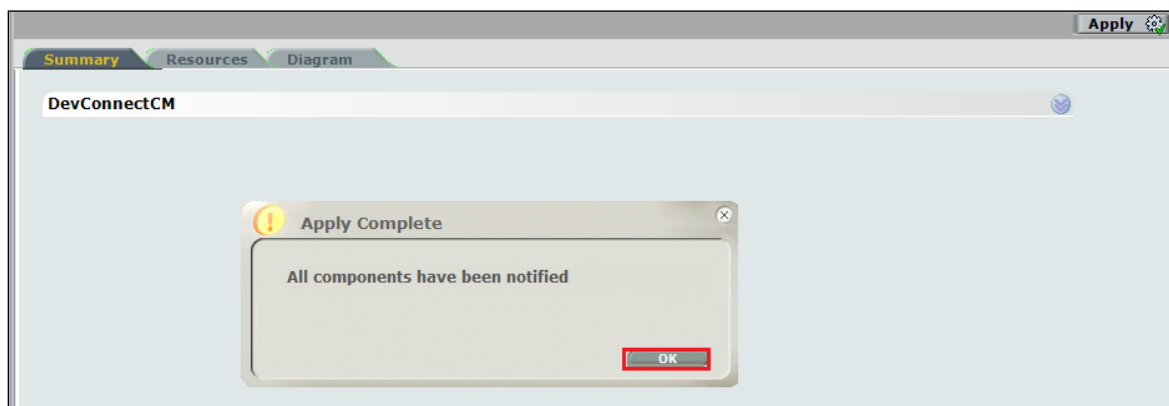
Click on **Finish** to complete the New Source Pool Wizard.



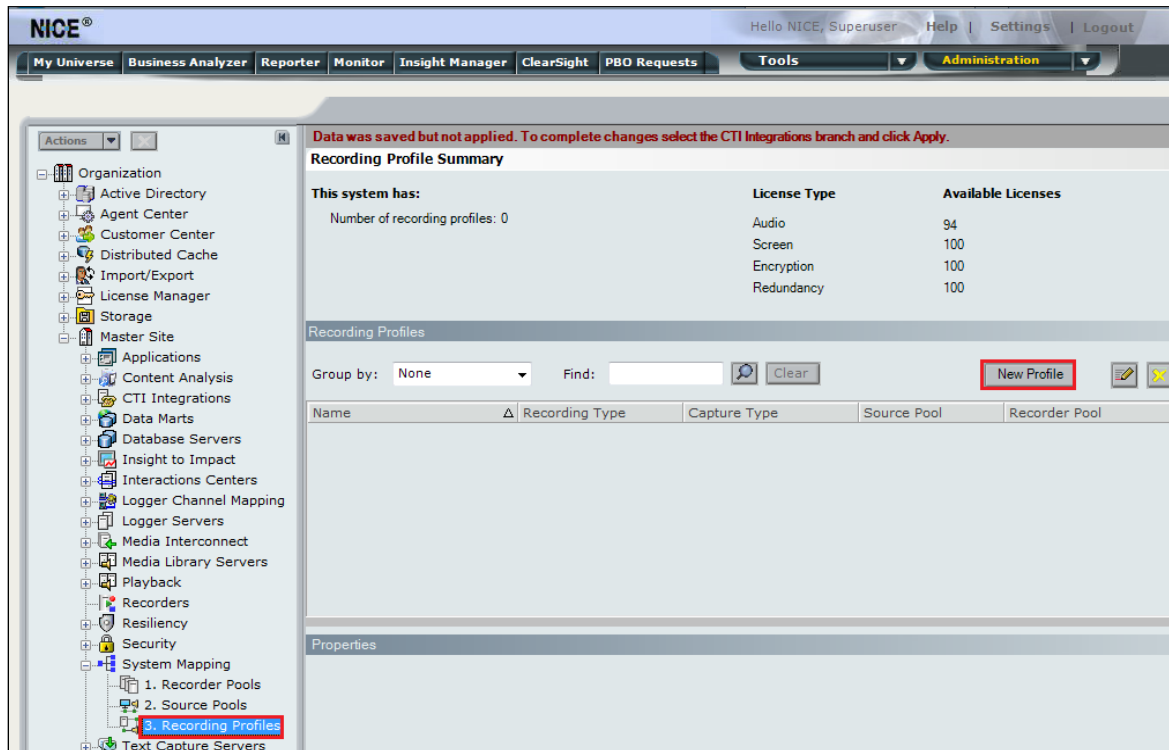
To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.



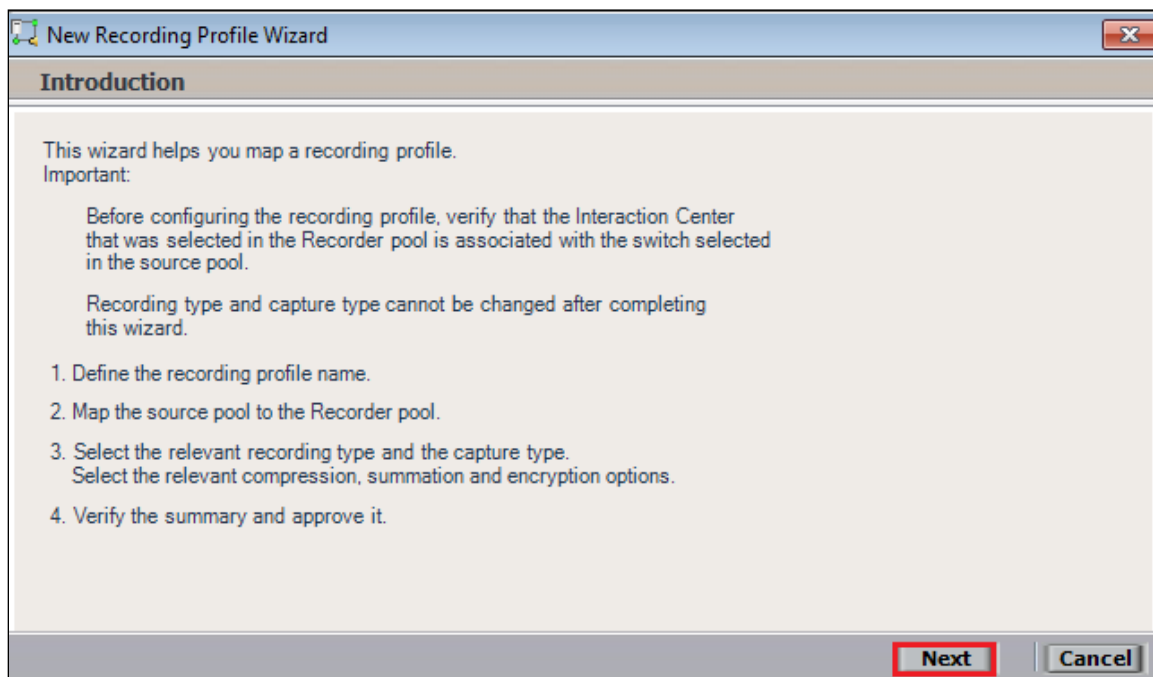
The following screen shows the changes were saved correctly. Click on **OK** to continue.



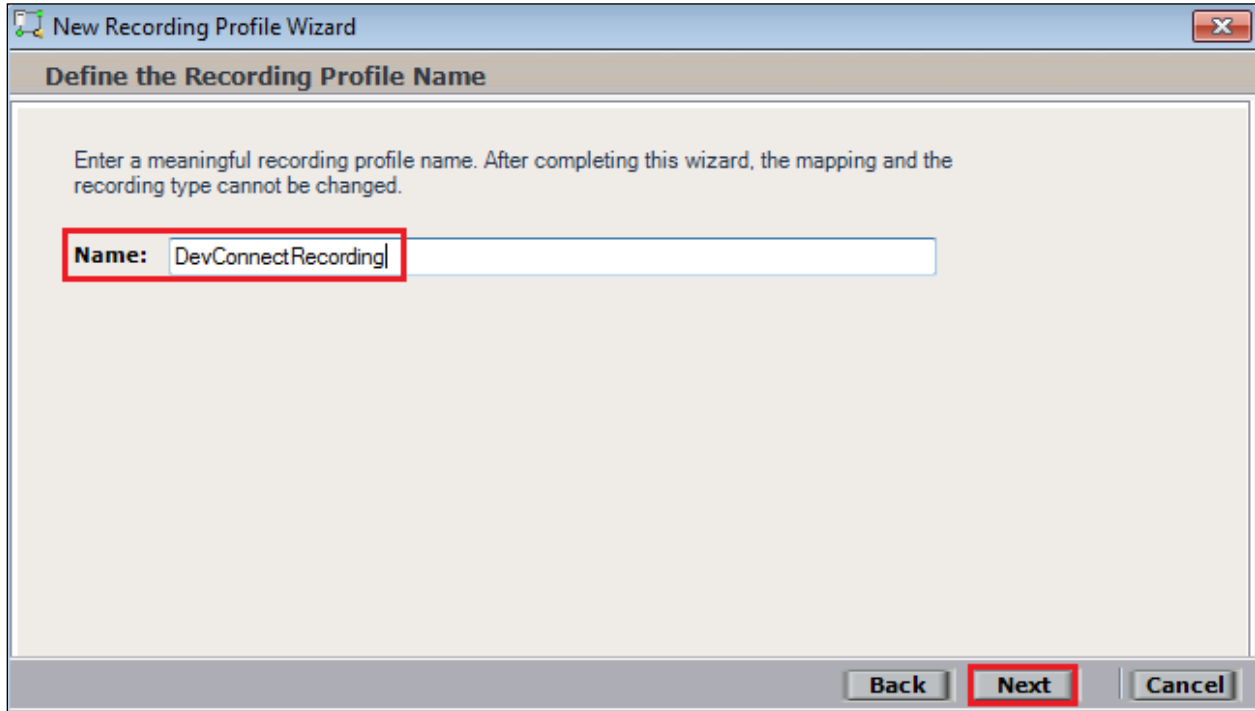
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



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

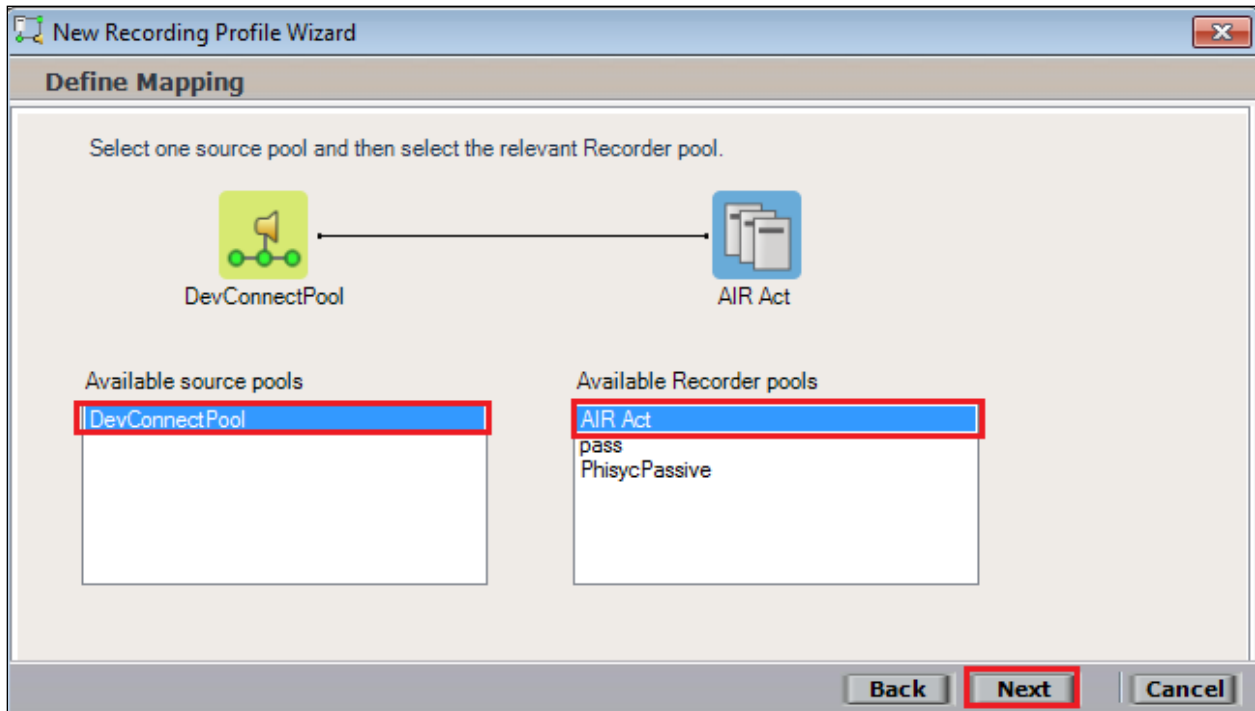


Enter a suitable **Name** for the Recording profile.



The screenshot shows the 'New Recording Profile Wizard' window, specifically the 'Define the Recording Profile Name' step. The window has a title bar with a close button. Below the title bar is a section header 'Define the Recording Profile Name'. The main area contains a text box with the instruction: 'Enter a meaningful recording profile name. After completing this wizard, the mapping and the recording type cannot be changed.' Below this is a text input field with the label 'Name:' and the text 'DevConnectRecording' entered. The input field is highlighted with a red border. At the bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red border.

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



The screenshot shows the 'New Recording Profile Wizard' window, specifically the 'Define Mapping' step. The window has a title bar with a close button. Below the title bar is a section header 'Define Mapping'. The main area contains a text box with the instruction: 'Select one source pool and then select the relevant Recorder pool.' Below this is a diagram showing a mapping from 'DevConnectPool' (represented by a green icon with a flag) to 'AIR Act' (represented by a blue icon with a document). Below the diagram are two lists: 'Available source pools' and 'Available Recorder pools'. The 'Available source pools' list contains 'DevConnectPool', which is highlighted with a blue background and a red border. The 'Available Recorder pools' list contains 'AIR Act', 'pass', and 'PhisycPassive', with 'AIR Act' highlighted with a blue background and a red border. At the bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red border.

For total recording i.e., the recording of all calls, select **Total** as the **Recording type**. For **Capture type** ensure that **Active DMCC MR Stereo** and **By Device** is selected beside it. **Audio 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

Allocated licenses: Determined by the number of sources in the source pool

Capture type: Active DMCC MR Stereo

☐ By Call ☒ By Device

☐ Secondary capture type:

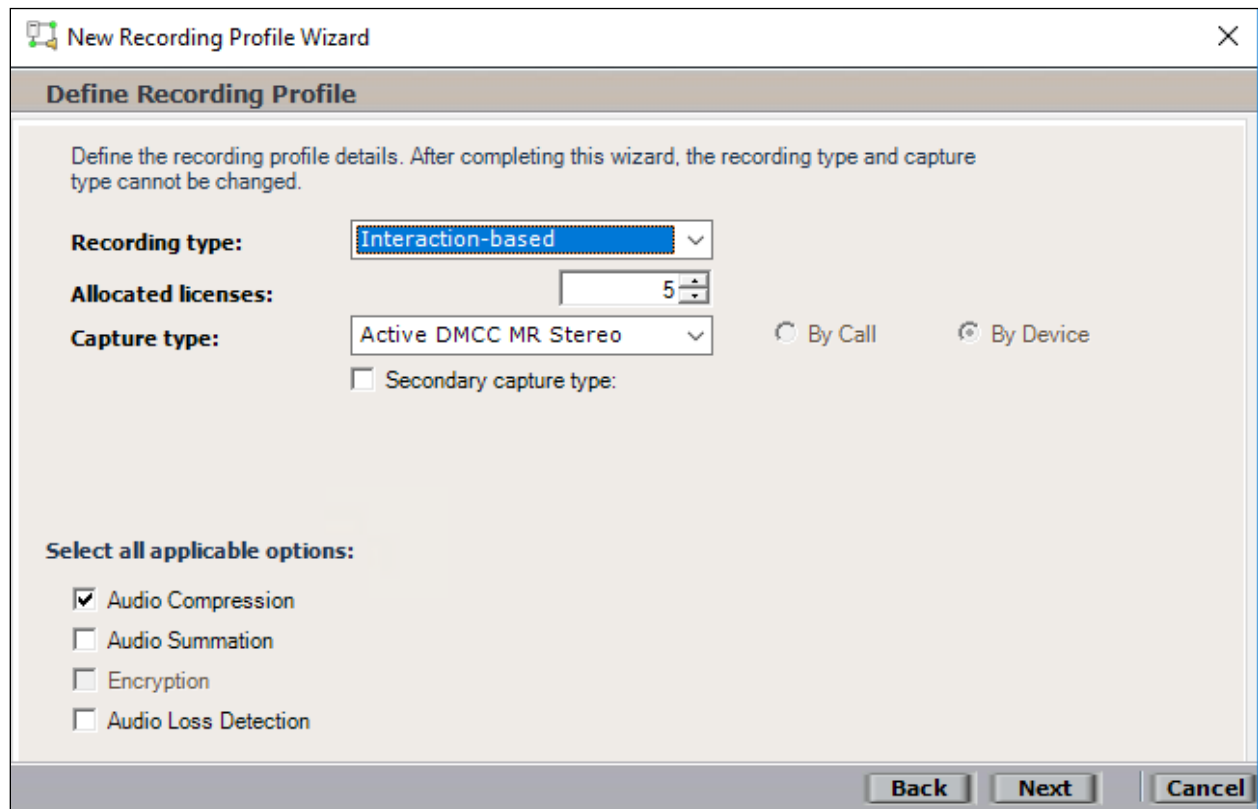
Select all applicable options:

- ☒ Audio Compression
- ☐ Audio Summation
- ☐ Encryption
- ☐ Audio Loss Detection

Back Next Cancel

Note: Avaya would recommend that **Total** “recording type” is used as it is not recommended to have recorders registering and unregistering to cope with an “interaction-based” type of recording.

Interaction-based recording can be configured by selecting **Interaction-based** as the **Recording type** and **Active DMCC MR Stereo** as the **Capture type** and **By Device** is selected beside it. **Audio Compression** is selected as default and can be left like this. Click on **Next** to continue.



The image shows a 'New Recording Profile Wizard' dialog box with a title bar containing a green icon and a close button. The main title is 'Define Recording Profile'. Below this, a note states: 'Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.' The configuration options are as follows:

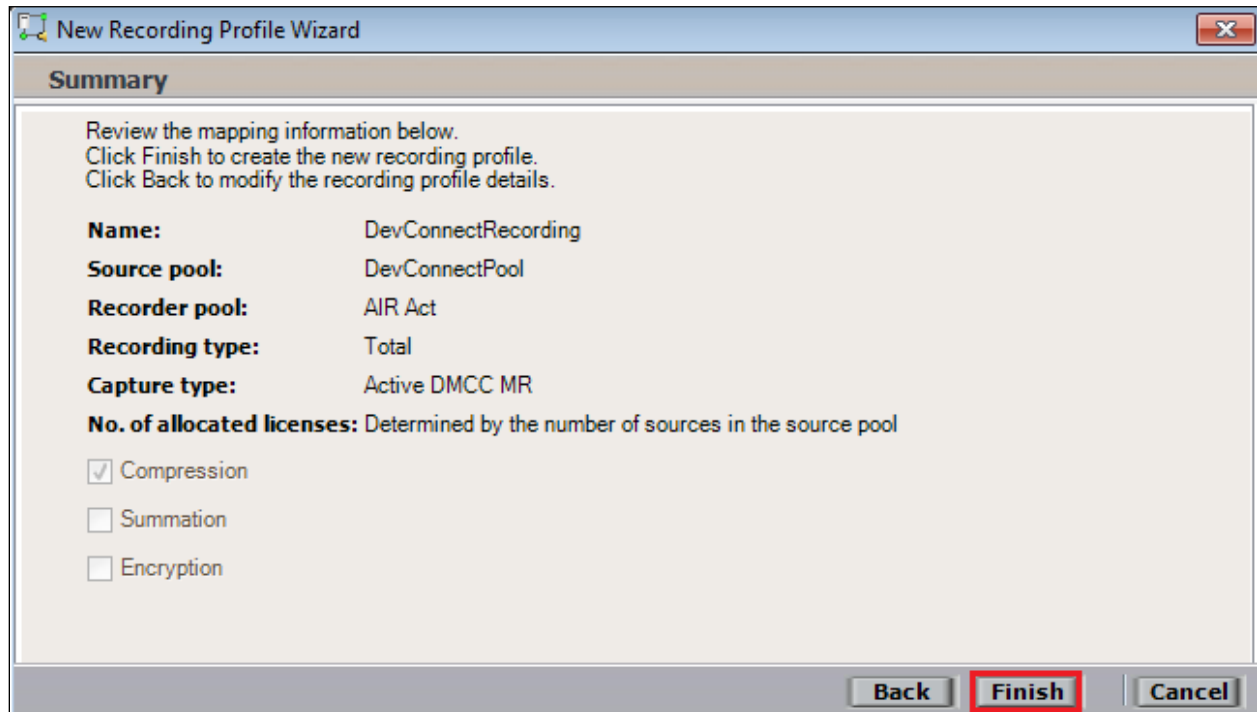
- Recording type:** A dropdown menu with 'Interaction-based' selected.
- Allocated licenses:** A numeric spinner box set to '5'.
- Capture type:** A dropdown menu with 'Active DMCC MR Stereo' selected.
- Two radio buttons: 'By Call' (unselected) and 'By Device' (selected).
- A checkbox for 'Secondary capture type:' which is unchecked.

Below these options, a section titled 'Select all applicable options:' contains four checkboxes:

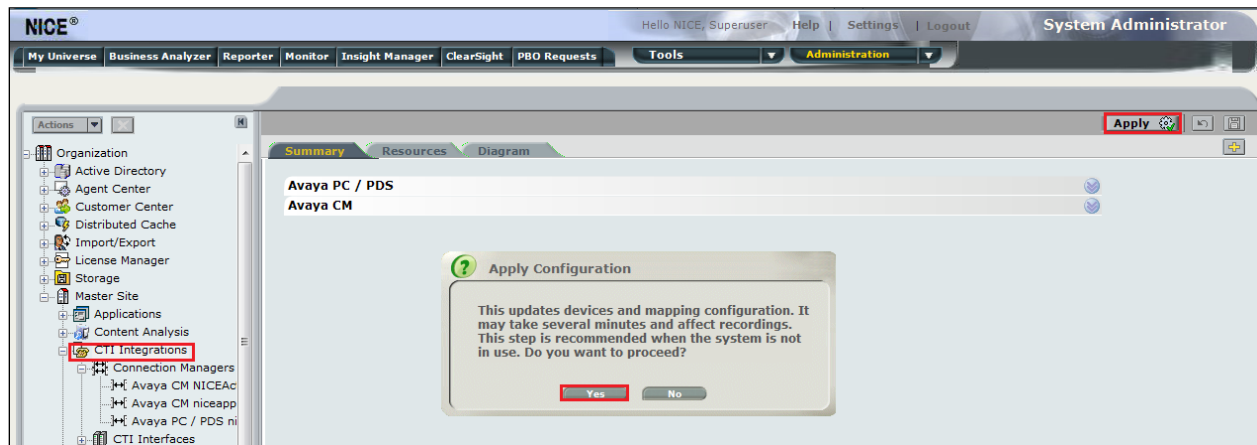
- ☒ Audio Compression
- ☐ Audio Summation
- ☐ Encryption
- ☐ Audio Loss Detection

At the bottom of the dialog are three buttons: 'Back', 'Next', and 'Cancel'.

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



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



This concludes the setup of the NICE Application Server for DMCC Multiple Registration recording.

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the NICE Engage Platform, Communication Manager, and 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 checked, 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	12	no	aespri101x	established	865	865

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**.

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm101x	1	Talking	Wed Sep 14 18:19:00 2022	Online	20	6	21	23	30

OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

Clicking on **User Status** from the screen on the previous page should display something similar to that shown below, where the NICE user and corresponding **Tlink Name** are shown.

CTI User Status

☐ Enable page refresh every seconds

CTI Users

Open Streams 3
 Closed Streams 24

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Fri 09 Sep 2022 06:27:34 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Fri 09 Sep 2022 06:27:34 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
nice1	Wed 14 Sep 2022 06:26:31 PM IST		AVAYA#CM101X#CSTA#AESPRI101X

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.

Status | Status and Control | DMCC Service Summary
 Home | Help | Logout

AE Services
 Communication Manager
 Interface
 High Availability
 Licensing
 Maintenance
 Networking
 Security
Status
 Alarm Viewer
 Logs
 Log Manager
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 seconds
 Session Summary **Device Summary**
 Generated on Wed Feb 08 18:22:56 GMT 2023
 Service Uptime: 5 days, 23 hours 7 minutes
 Number of Active Sessions: 1
 Number of Sessions Created Since Service Boot: 2
 Number of Existing Devices: 10
 Number of Devices Created Since Service Boot: 316

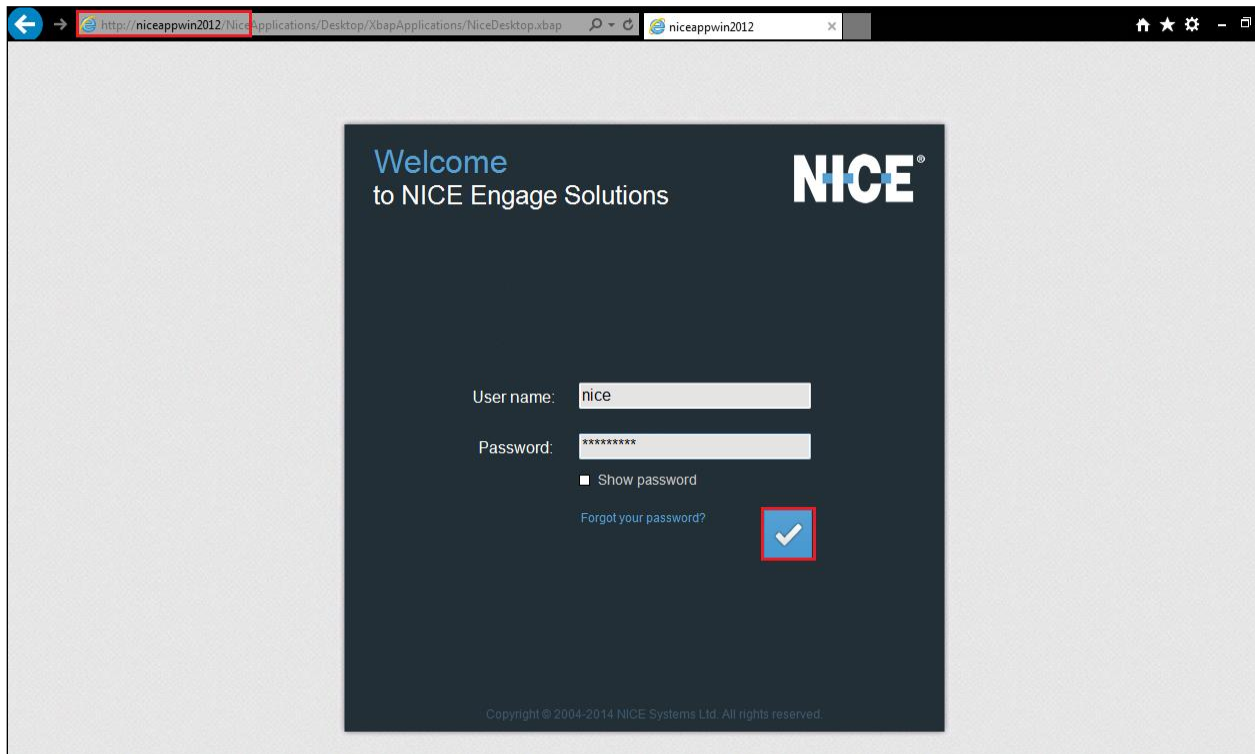
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	36EC35B84917CF010 3E3957E5DD007DC-1	nice1		10.10.40.126	XML Unencrypted	10

Item 1-1 of 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**.

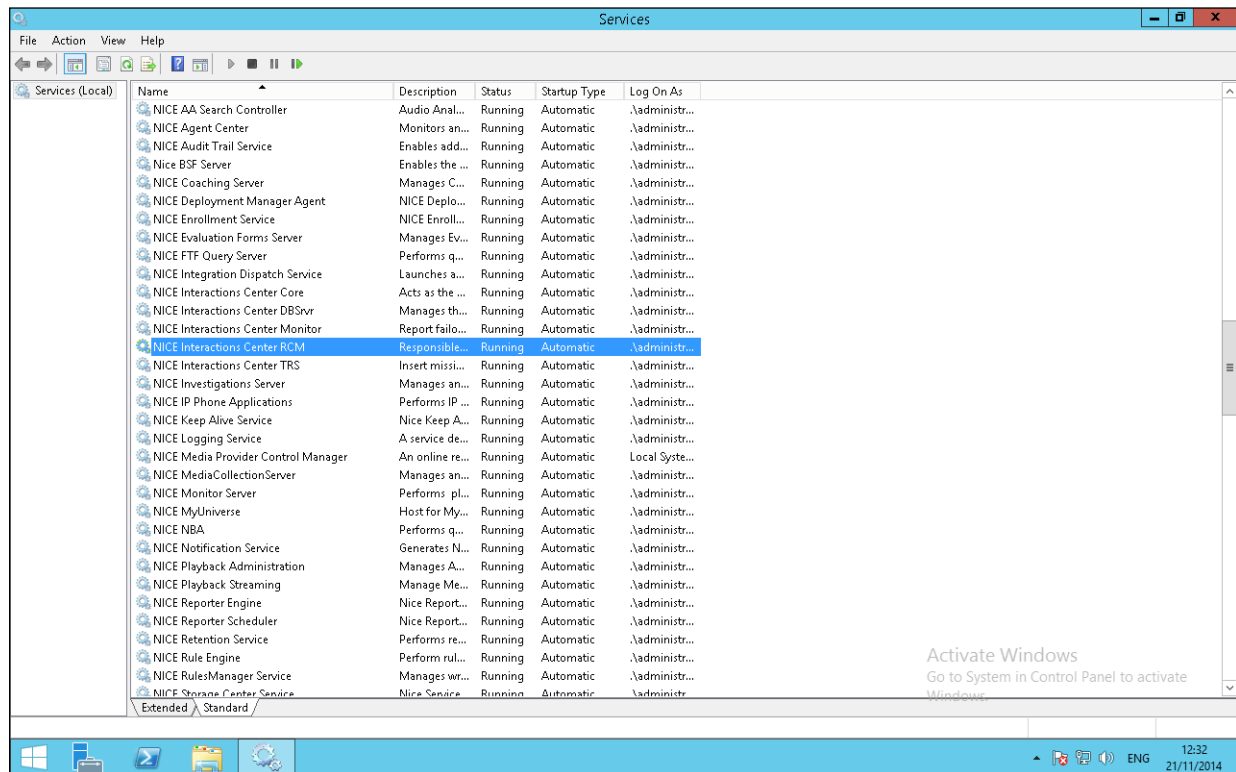


Note: The recording below shows two separate streams in stereo, with the **Customer** on one side and the **Agent** on the other.

PG; Reviewed: Solution & Interoperability Test Lab Application Notes 59 of 62
SPOC 4/13/2023 ©2023 Avaya Inc. All Rights Reserved. NICE73AES101MR

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 Recorder 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 R7.3 to successfully interoperate with Avaya Aura® Communication Manager R10.1 using Avaya Aura® Application Enablement Services R10.1 to connect to using DMCC Multiple Registration to record calls in stereo. All feature functionality and serviceability test cases were completed successfully with 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® System Manager*. Release 10.1.x, Issue 6, June 2022.
- [2] *Administering Avaya Aura® Session Manager*. Release 10.1.x, Issue 3, April 2022.
- [3] *Administering Avaya Aura® Communication Manager*. Release 10.1, Issue 1, December 2021.
- [4] *Administering Avaya Aura® Application Enablement Services*. Release 10.1.x, Issue 4, April 2022.
- [5] *Implementing and Administering Avaya Aura® Media Server*. Release 10.1.x, Issue 2, July 2022.
- [6] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [7] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

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

©2023 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.