



## 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 Passive Station-Side VoIP 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 Passive Station-Side VoIP recording 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. The NICE Engage Platform was set up to use passive station-side VoIP recording with System Management Service (SMS) and the Telephony Services Application Programming Interface (TSAPI) via the Avaya Aura® Application Enablement Services (AES) to capture the audio and call details for call recording on various Communication Manager endpoints, listed in **Section 4**.

Passive station-side VoIP Recording (passive recording) uses port mirroring to record the RTP from each phone set. All phone sets to be recorded are plugged into the data switch, where these particular ports are mirrored to a port connected to the NICE Advanced Interactions Recording server. All of the RTP information from all of these phone sets is delivered to the sniffer port on the NICE Advanced Interactions Recording server. An additional Network Interface Card (NIC) is therefore required on the NICE Advanced Interactions Recording (AIR) server. This NIC is not configured to access the IP stack and has no IP configuration. This NIC connects into the mirrored port network that allows access to the phone network connection. This is effectively a hub environment. The promiscuous port needs to be on the same physical media path as any telephone endpoint that it is going to be recorded.

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 both TSAPI and SMS connections on AES. The TSAPI interface allows NICE Engage to capture the necessary call events and the SMS web service provides the ability to discover the status of resources on Communication Manager.

## 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 passive recording 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.

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. The interface between the SIP phones and Session Manager were also unencrypted to allow NICE to capture the IP address information of the phone sets.

NICE used a “Generic SIP Mapper” interface for media location extraction of the SIP Phones that register to Session Manager. In order for this to operate and avoid configuration of fixed IPs, the signaling must be unencrypted. Any TLS messages on the network need to be decoded by the SIP Mapper and in order to decode these messages all TLS protocols use on the AES needed to be ticked, see **Section 6.5.2**.

**Note:** For Passive Station-Side VoIP recording the RTP is mirrored and sent to NICE Engage platform, therefore any RTP between the Avaya endpoints must not be encrypted.

## 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.
- **Forwarded calls** - Test call recording for calls that were forwarded to various endpoints.
- **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 Avaya Agent for Desktop.
- **Serviceability testing** - The behavior of NICE Engage Platform under different simulated LAN failure conditions.

## **2.2. Test Results**

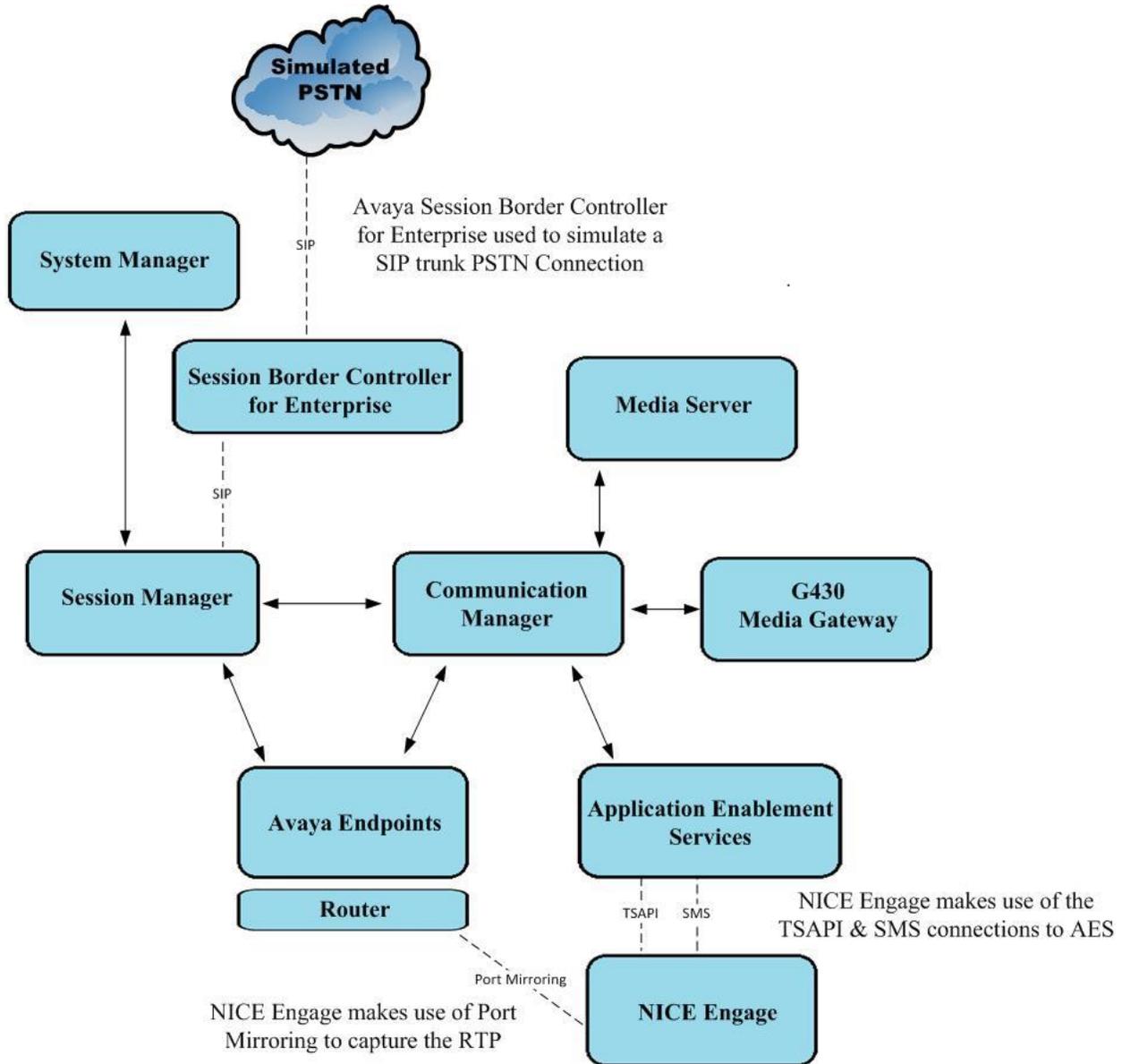
All functionality and serviceability test cases were completed successfully.

## **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 passive recording to record calls. The data switch is configured to mirror ports connected to Avaya endpoints to one port connected to the NICE Advanced Interactions recorder sniffer port.



**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:

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 J100 Series Phones (SIP)	7.1.2.0.14
Avaya J100 Series Phones (H.323)	7.0.14.0.7
Avaya Vantage K175	3.1.1.1
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 Engage Platform - NICE Engage Application Server - NICE Advanced Interactions Recording Server - NICE Engage NDM Server	7.3

All equipment is running on virtual servers on VMware, except the NICE Advanced Interactions Recording Server, which is required to be installed on a server that could be plugged into the data switch and therefore is running on a Dell R610 with two NIC's, one of which connected to the mirrored ports.

## 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 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 5.2**.
- **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

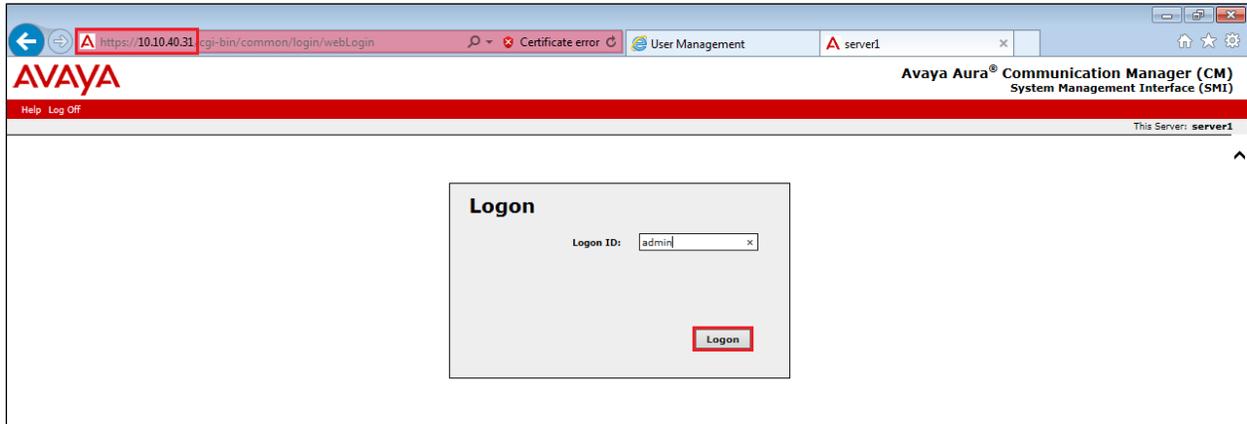
Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1 Page 1 of 3
```

CTI LINK	
CTI Link: 1	
Extension: 1990	
Type: ADJ-IP	
Name: aespri101x	COR: 1

## 5.5. Configure System Management Service user on Avaya Aura® Communication Manager

This user is created specifically for the SMS connection that NICE utilises for this specific type of call recording. Using a web browser navigate to the Communication Manager IP Address. Enter the proper credentials and click on Logon.



Once logged in click on **Administration** at the top of the page and select **Server (Maintenance)** from the drop-down menu.



In the left window navigate to **Security** → **Administrator Accounts**. In the main window select **Add Login** and **Privileged Administrator** as shown below. Click on **Submit** when finished.

**AVAYA**

Help Log Off Administration

Administration / Server (Maintenance)

**Administrator Accounts**

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

**Select Action:**

- Add Login
- Privileged Administrator
- Unprivileged Administrator
- SAT Access Only
- Web Access Only
- CDR Access Only
- Business Partner Login (dadmin)
- Business Partner Craft Login
- Custom Login

Change Login  ▼

Remove Login  ▼

Lock/Unlock Login  ▼

Add Group

Remove Group  ▼

**Submit** Help

Enter a suitable **Login name** and enter a suitable **password**, then click on **Submit** as all other settings can be left as default. Note this name and password will be needed in **Section 7.1**.

**AVAYA**

Help Log Off Administration

Administration / Server (Maintenance)

**Administrator Accounts -- Add Login: privileged Administrator**

This page allows you to add a login that is a member of the **USERS** group. This login has reduced access privileges.

Login name:

Primary group:

Additional groups (profile):

Linux shell:

Home directory:

Lock this account:

SAT Limit:

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Select type of authentication:

- Password
- ASG: enter key
- ASG: Auto-generate key

Enter password or key:

Re-enter password or key:

Force password/key change on next login:

- Yes
- No

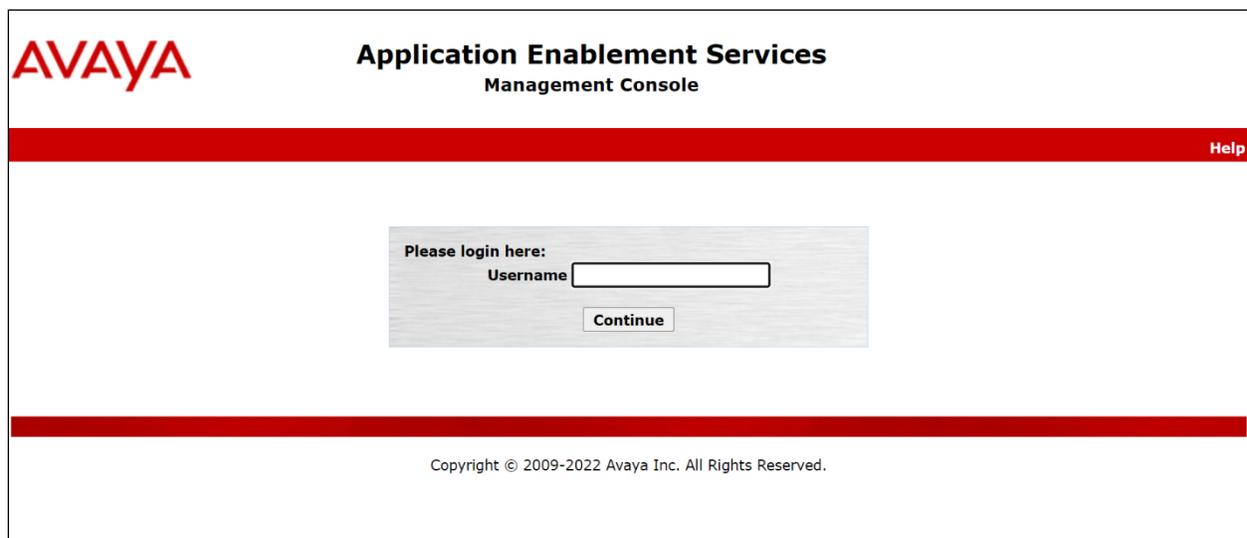
## 6. Configure Avaya Aura® Application Enablement Services

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 Ports
- Create CTI User
- Configure Security
- Restart AE Server
- Configure the System Management Service on Avaya Aura® Application Enablement Services

### 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. The title "Application Enablement Services Management Console" is centered at the top. A red horizontal bar spans the width of the page, with the word "Help" in the top right corner. In the center, there is a light gray login box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. 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 Service** is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

**AVAYA** Application Enablement Services Management Console

Welcome: User cust  
 Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222  
 Number of prior failed login attempts: 1  
 HostName/IP: aes70vmpg  
 Server Offer Type: VIRTUAL\_APPLIANCE\_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

Home | Help | Logout

AE Services

AE Services

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

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

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

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

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

The TSAPI license is a 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.

**Licensing**

AE Services  
 Communication Manager Interface  
 High Availability  
**Licensing**  
 WebLM Server Address  
**WebLM Server Access**  
 Reserved Licenses  
 Maintenance  
 Networking  
 Security  
 Status  
 User Management  
 Utilities  
 Help

**Licensing**

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

**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** users.

The screenshot shows the 'Application Enablement' section in the Management Console. A red box highlights the 'Application Enablement' menu item, which includes options like 'View by feature', 'View by local WebLM', and 'Enterprise configuration'. The main area displays a table of license features and their capacities.

Feature (License Keyword)	License Capacity	Currently available	
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000	
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16	
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000	
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3	
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3	3	
DLG (VALUE_AES_DLG)	16	16	
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	997	
Product Notes (VALUE_NOTES)	<p>SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer            MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_8832_vm;CtiMediumServer            LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer            TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; AACC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CE_AGENT_STATES_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; TP_CIFINT_001, BasicUnrestricted, AgentEvents; FXT_CIFINT_001, ...</p>		Not counted

## 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.

The screenshot shows the 'Application Enablement Services Management Console' interface. The top navigation bar includes 'Communication Manager Interface | Switch Connections' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'Switch Connections' selected. The main content area displays the 'Switch Connections' configuration page, which includes a table of existing connections and an 'Add Connection' button.

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

Buttons below the table: 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 5.3**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button. In the resulting screen, enter the IP address of the procr as shown in **Section Error! Reference source not found**. that will be used for the AES connection and select the **Add/Edit Name or IP** button.

Name or IP Address	Status
10.10.40.13	In Use

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: 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. The main navigation bar includes 'Communication Manager Interface | Switch Connections' and 'Home | Help | Logout'. The left sidebar lists 'AE Services', 'Communication Manager Interface', 'Switch Connections', 'Dial Plan', 'High Availability', 'Licensing', 'Maintenance', and 'Networking'. The main content area shows a table of 'Switch Connections' with columns for 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'. A table with one row is visible, showing 'cm101x' with 'Yes' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit Signaling Details', 'Delete Connection', and 'Survivability Hierarchy'.

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

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

The screenshot shows the 'Edit H.323 Gatekeeper - cm101x' page. The top navigation bar is 'Communication Manager Interface | Switch Connections'. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Switch Connections' and contains a form for editing the H.323 Gatekeeper. The form has a header 'Edit H.323 Gatekeeper - cm101x' and a text input field with an 'Add Name or IP' button. Below the input field is the label 'Name or IP Address' and a radio button selected next to the IP address '10.10.40.13'. There is also a 'Delete IP' button.

### 6.3. Administer TSAPI link

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



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

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

Link 1

Switch Connection cm101x ▼

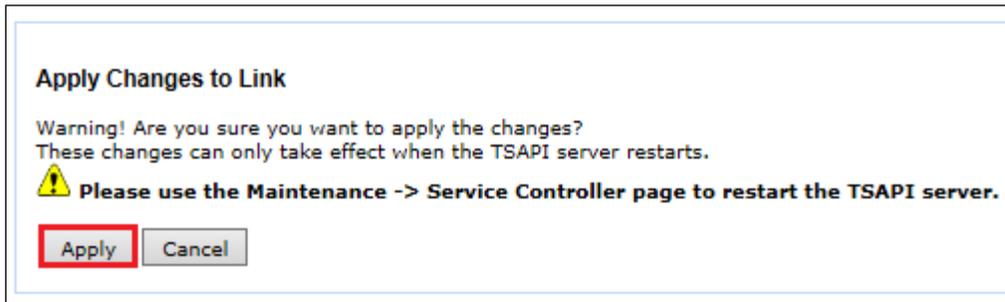
Switch CTI Link Number 1 ▼

ASAI Link Version 12 ▼

Security Both ▼

Apply Changes Cancel Changes Advanced Settings

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



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 the NICE Engage Platform in **Section 7.1**. The Tlink for the unencrypted TSAPI link was used.

The screenshot shows the 'Security | Security Database | Tlinks' configuration page. 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, CTI Users, Devices, Device Groups, Tlinks (highlighted), Tlink Groups, and Worktops. The main content area is titled 'Tlinks' and displays two radio button options for 'Tlink Name': 'AVAYA#CM101X#CSTA#AESPRI101X' (selected) and 'AVAYA#CM101X#CSTA-S#AESPRI101X'. A 'Delete Tlink' button is located below the options.

## 6.5. Configure Networking Ports

Navigate to **Networking** in the left window, both the TSAPI and TLS port configurations can be observed from here.

### 6.5.1. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking** → **Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

**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"/>

---

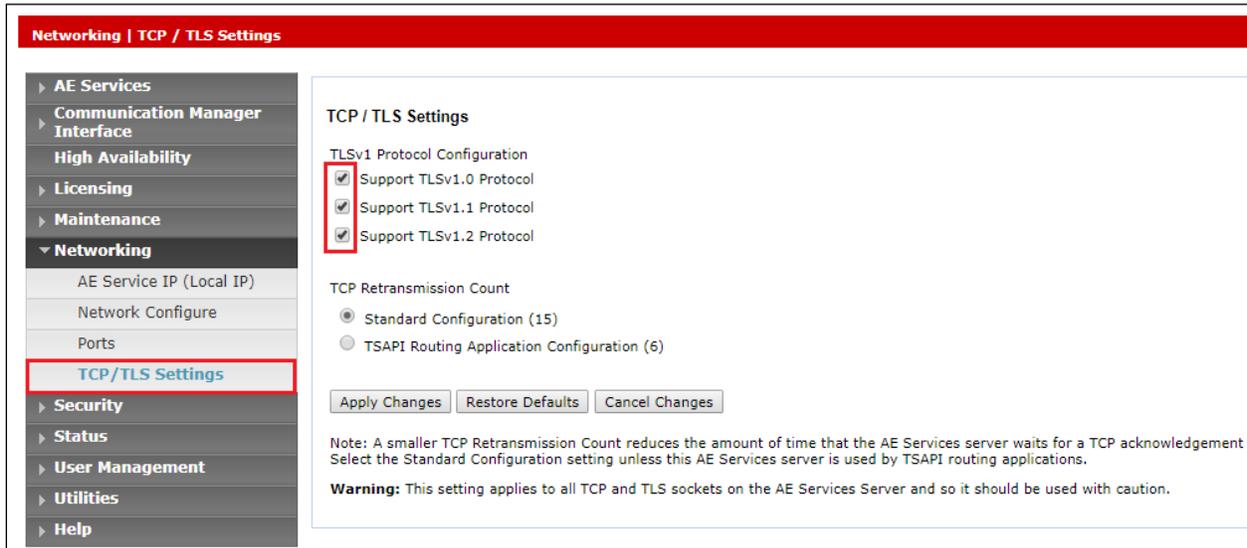
**H.323 Ports** Enabled Disabled

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"/>	
Server Media		<input checked="" type="radio"/> <input type="radio"/>

## 6.5.2. Enable TLS Ports

In order to allow the NICE Generic SIP Mapper to decode TLS messages support for all three TLS protocols needed to be ticked.

Navigate to **TCP/TLS Settings** as shown. To ensure that all TLS protocols are supported, tick the boxes as shown below. Click on **Apply Changes**.



The screenshot shows a web interface for configuring TCP/TLS settings. On the left is a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The 'Networking' section is expanded, and 'TCP/TLS Settings' is highlighted with a red box. The main content area is titled 'TCP / TLS Settings' and contains the following options:

- TLSv1 Protocol Configuration:** Three checkboxes are present, all of which are checked and highlighted with a red box:
  - Support TLSv1.0 Protocol
  - Support TLSv1.1 Protocol
  - Support TLSv1.2 Protocol
- TCP Retransmission Count:** Two radio button options:
  - Standard Configuration (15)
  - TSAPI Routing Application Configuration (6)

Below the settings are three buttons: 'Apply Changes', 'Restore Defaults', and 'Cancel Changes'. A note at the bottom states: 'Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement. Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.' A warning below the note reads: 'Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution.'

## 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.

The screenshot displays the 'User Management | User Admin' interface. On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Add User, Change User Password, List All Users, Modify Default Users, Search Users, Utilities, and Help. The 'User Admin' section is highlighted in blue. The main content area on the right is titled 'User Admin' and contains the text: 'User Admin provides you with the following options for managing AE Services users:' followed by a bulleted list: Add User, Change User Password, List All Users, Modify Default User, and Search Users.

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.

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

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 Error! Reference source not found.**, these values set here do not impact the overall setup.

The screenshot shows a navigation pane on the left 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" and contains two checkboxes: "Enable SDB for DMCC Service" (unchecked) and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services" (checked). An "Apply Changes" button is located below the checkboxes.

**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

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:

---

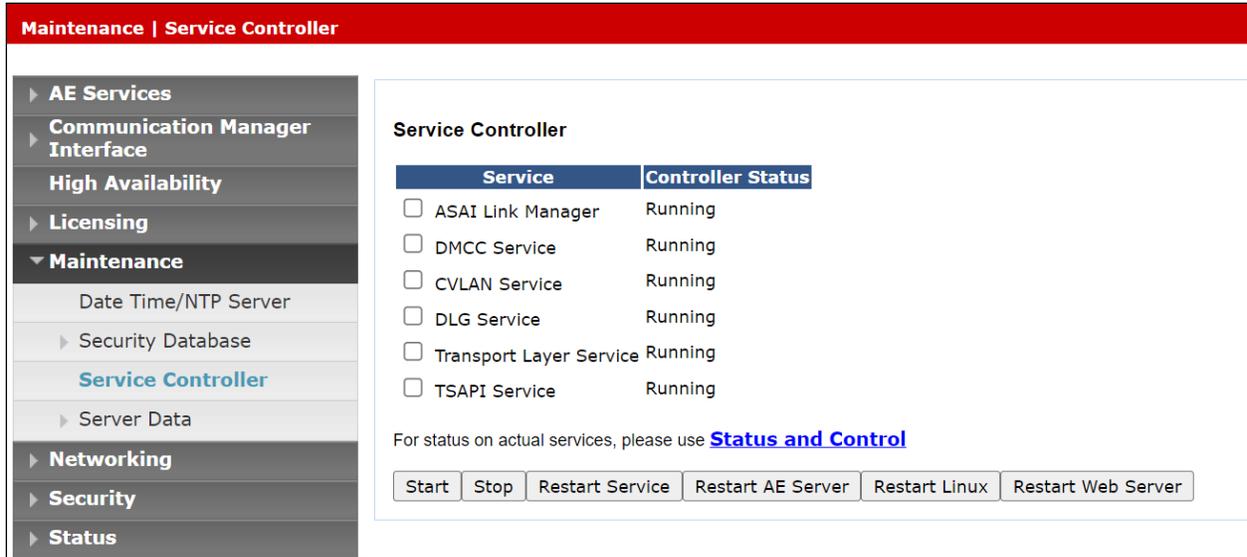
Routing Control:

- 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

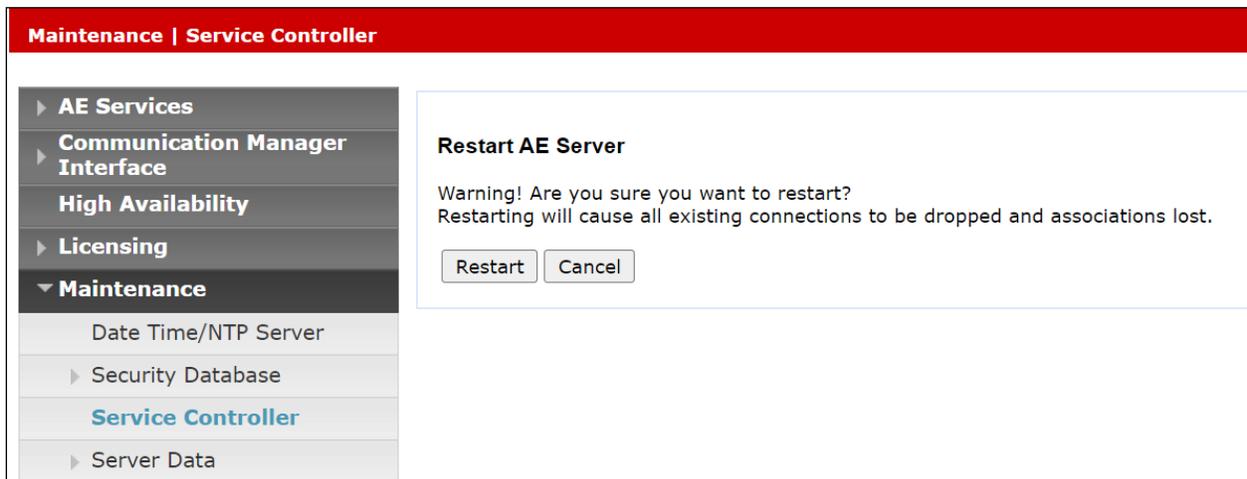
Service Controller

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

## 6.9. Configure the System Management Service on Avaya Aura® Application Enablement Services

From the AE Services Management Console main menu, select **AE Services** → **SMS** → **SMS Properties**. The following list describes the SMS configuration settings and provides guidelines for configuring SMS.

- **Default CM Host Address** — SMS will attempt to connect to this Communication Manager host address, as long as no host address is explicitly specified in the authorization header of a client request. If this field is blank, all SMS requests must explicitly include the target Communication Manager host address.
- **Default CM Admin Port** — By default the System Management Service will use **5022** to connect to a Communication Manager server.
- **CM Connection Protocol** — Use the default **SSH** port. The default TUI (or SAT) ports on Communication Manager are **SSH Port=5022 Telnet Port=5023**.
- **CM Proxy Trace Logging** — Use the default **NONE**, unless debugging.
- **Max Sessions per CM** — This is a safety setting that prevents SMS from consuming all of the TUI processes on Communication Manager. By default, the setting is **5**.

Use default settings for all other fields, as shown below.

The screenshot displays the 'SMS Properties' configuration page within the Avaya Aura AE Services Management Console. The page title is 'AE Services | SMS | SMS Properties'. On the left, a navigation menu shows 'AE Services' expanded, with 'SMS Properties' selected under the 'SMS' section. The main content area contains the following configuration fields:

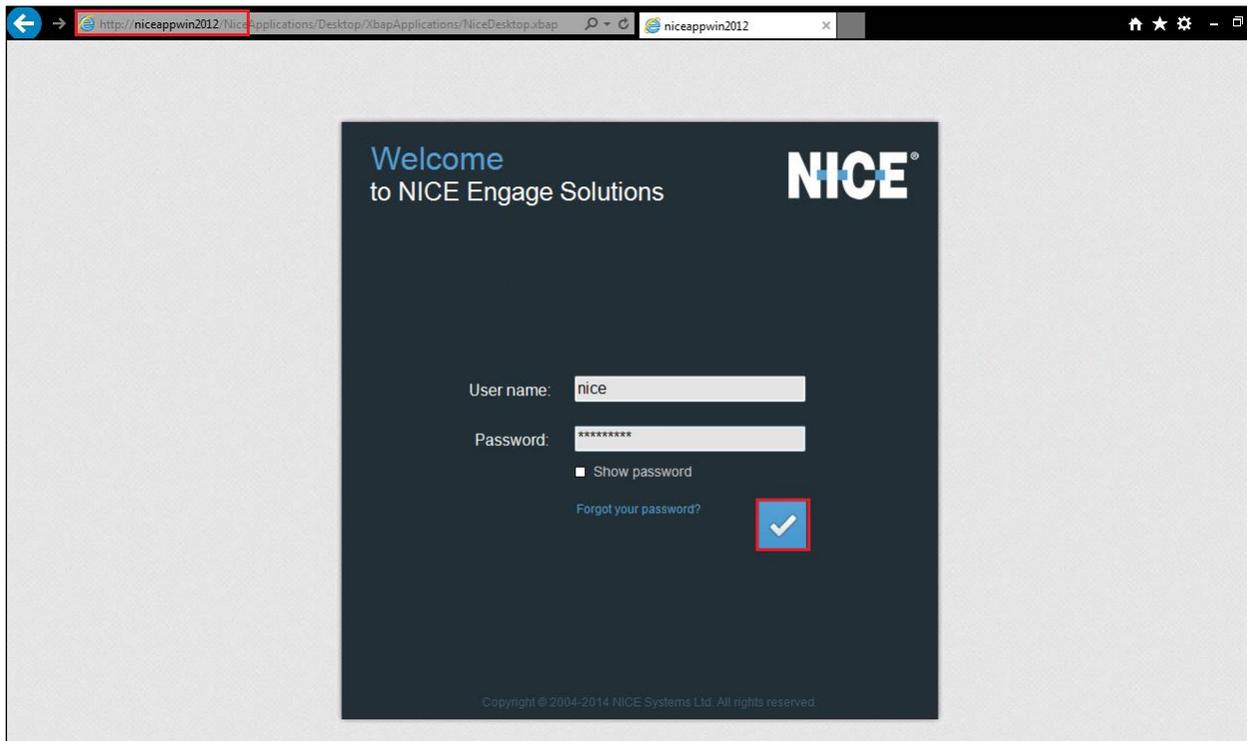
SMS Properties	
Default CM Host Address	<input type="text" value="10.10.40.13"/>
Default CM Admin Port	<input type="text" value="5022"/>
CM Connection Protocol	<input type="text" value="SSH"/>
SMS Logging	<input type="text" value="NORMAL"/>
SMS Log Destination	<input type="text" value="apache"/>
CM Proxy Trace Logging	<input type="text" value="NONE"/>
Max Sessions per CM	<input type="text" value="5"/>
Proxy Shutdown Timer	<input type="text" value="1800"/> seconds
SAT Login Keepalive	<input type="text" value="180"/> seconds
CM Terminal Type	<input type="text" value="OSSIZ"/>
Proxy Log Destination	<input type="text" value="/var/log/avaya/aes/ossicm.log"/>

At the bottom of the configuration area, there are three buttons: 'Apply Changes', 'Restore Defaults', and 'Cancel'.

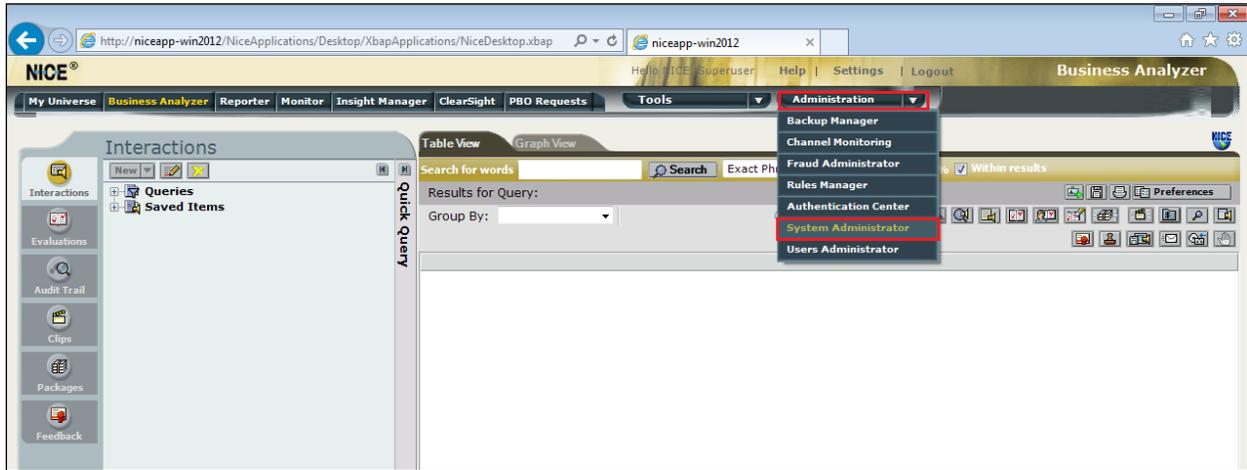
## 7. Configure NICE Engage Platform

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**.

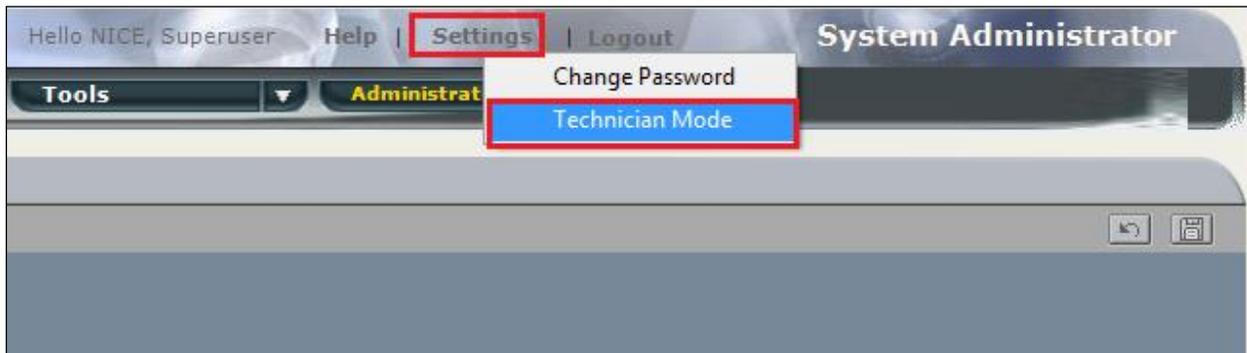
The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya solution. All configuration of the NICE Engage Platform for connection with the AES is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser as shown navigate to **Error! Hyperlink reference not valid.** 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.

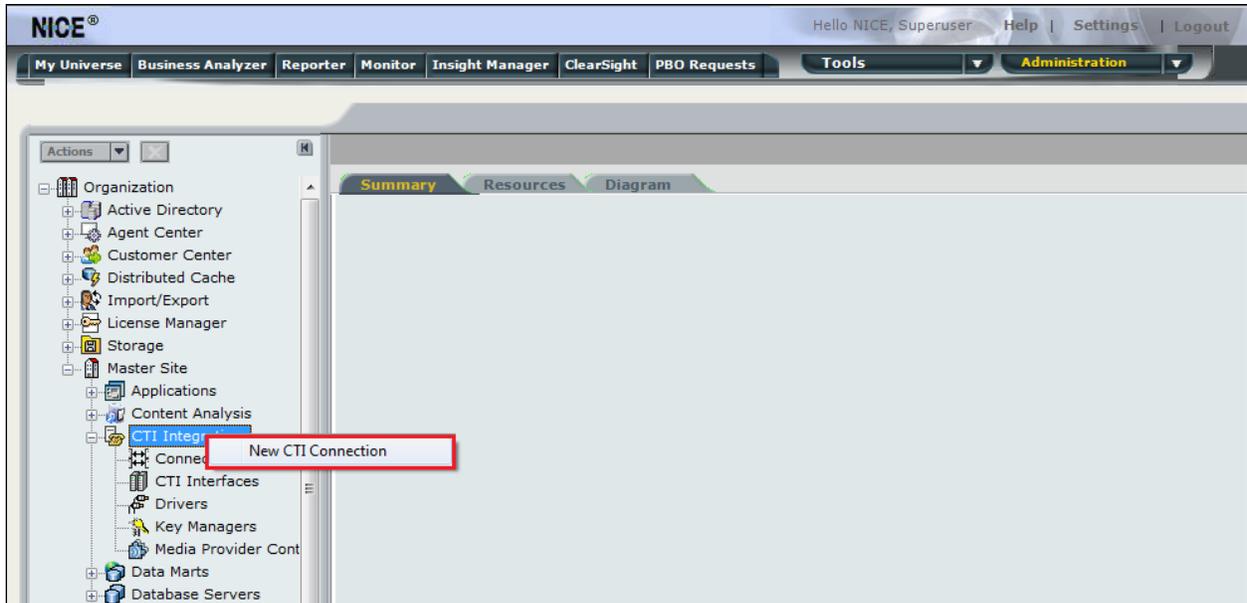


Before any changes can be made, switch to **Technician Mode** by clicking into **Settings** at the top of the screen as shown below.

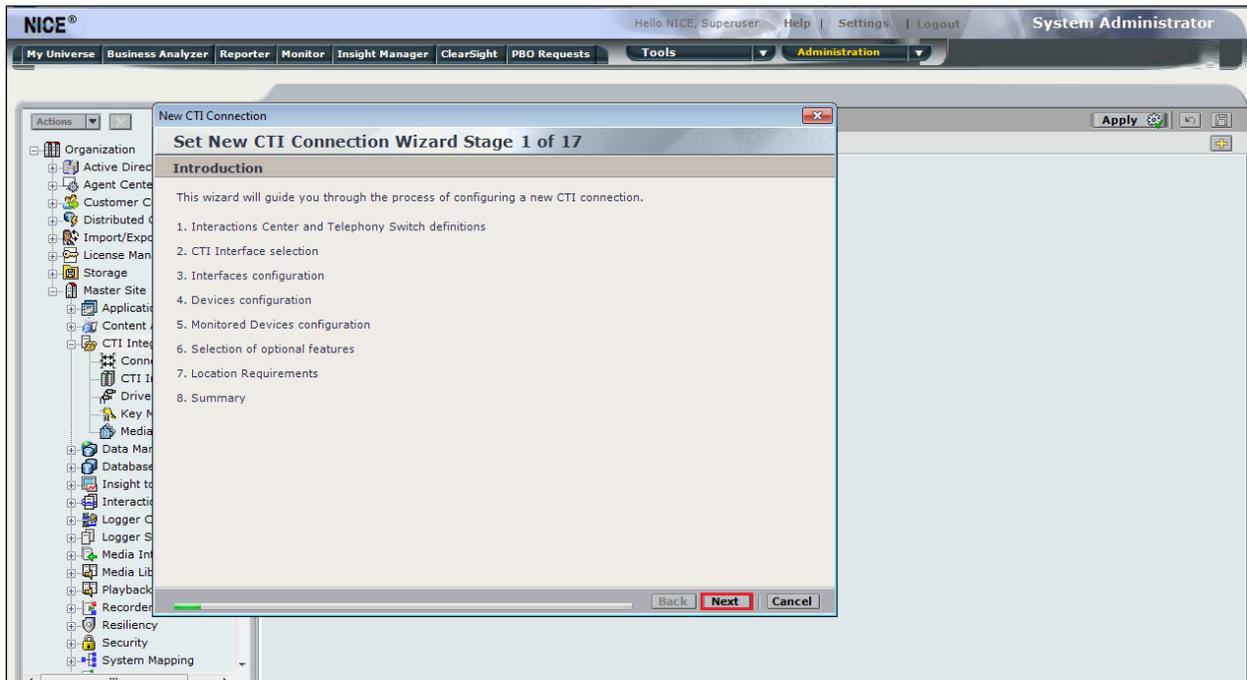


## 7.1. New CTI Connection

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 17 steps required to set up the connection to the AES for Passive Station Side VoIP recording. Click on **Next** to continue.



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

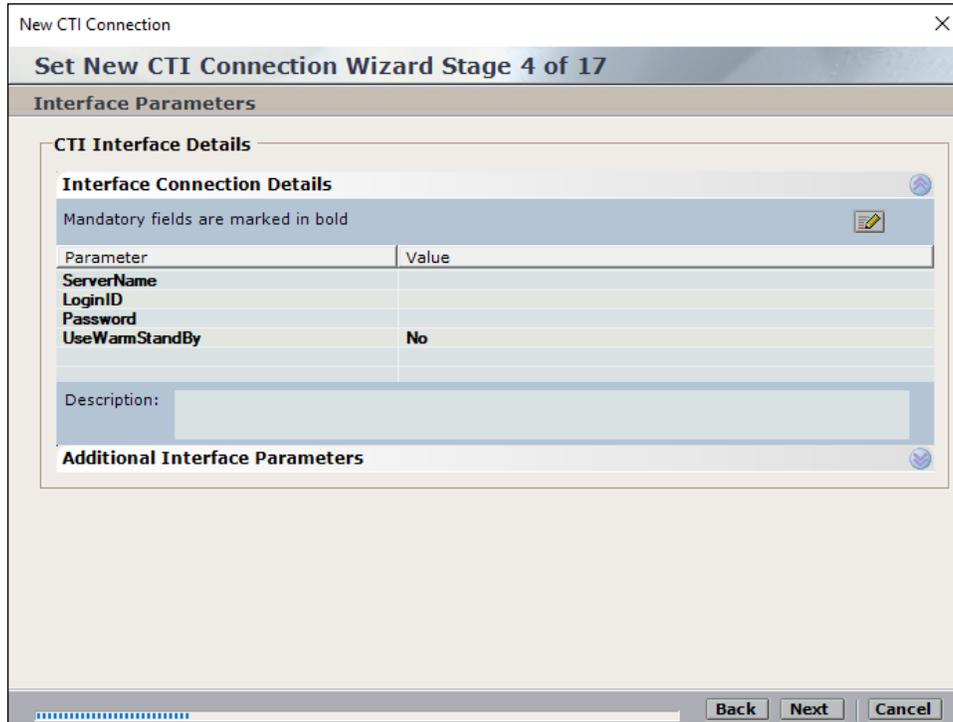
The **Telephony Switch** must be selected, and this will be **Avaya CM**. Enter a suitable name for this **Switch Name**. Click on **Next** to continue.

The screenshot shows the 'Set New CTI Connection Wizard Stage 2 of 17' window. The 'Interactions Center Switch' section is active. Under 'Attach CTI to Interactions Center Server:', the 'Regular Interactions Center' radio button is selected, with a dropdown menu showing 'IC (nice-app)'. The 'Interactions Center Cluster' dropdown is empty. Under 'Use existing Telephony Switch:', the 'Avaya CM' dropdown is selected. Under 'Define new Telephony Switch:', the 'Switch Type' dropdown is set to 'Avaya CM' and the 'Switch Name' text box contains 'Avaya CM Passive'. An 'Advanced <<' button is visible. Below, the 'Agent Logon Mode' section has three checked options: 'To the same station again', 'To more than one station', and 'To a station another agent is logged into'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

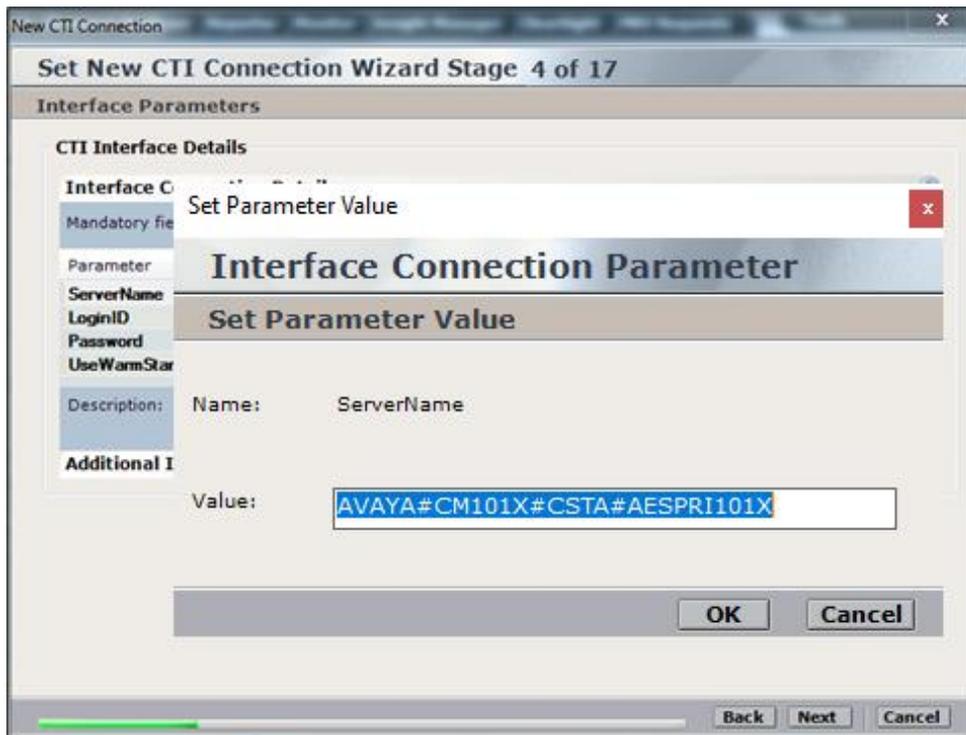
Select **AES TSAPI** for the **Avaya CM CTI Interface**, ensure that **VoIP Mapping** is ticked and select the **AES SMS** from the dropdown menu. Ensure that **Additional VoIP Mapping** is ticked, and that **Generic SIP Mapper** is chosen from the dropdown. Click on **Next** to continue.

The screenshot shows the 'Set New CTI Connection Wizard Stage 3 of 17' window. The 'Interface Type' section is active. Under 'CTI Interface Type', the 'Avaya CM CTI Interface' dropdown is set to 'AES TSAPI', with subtext 'Avaya Communication Manager' and 'Avaya Application Enablement Services (AES) / Avaya CT - TSAPI'. The 'VoIP Mapping' checkbox is checked, with a dropdown set to 'AES SMS' and subtext 'Avaya Communication Manager' and 'IP address mapping (AES SMS)'. The 'Additional VoIP Mapping' checkbox is checked, with a dropdown set to 'Generic SIP Mapper' and subtext 'Avaya Communication Manager' and 'Generic SIP Mapper'. The 'Active Recording' checkbox is unchecked, with a dropdown set to 'DMCC (Advanced Interaction Recorder)'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

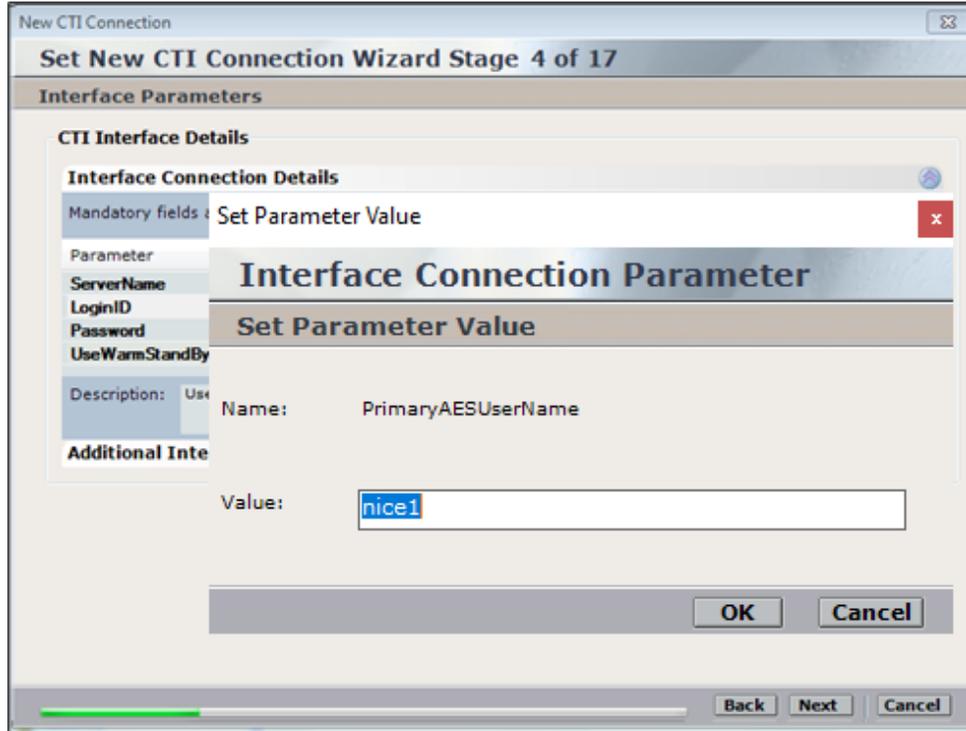
Each of the values below must be filled in. Double-click on each **Parameter** to enter a value for that parameter.



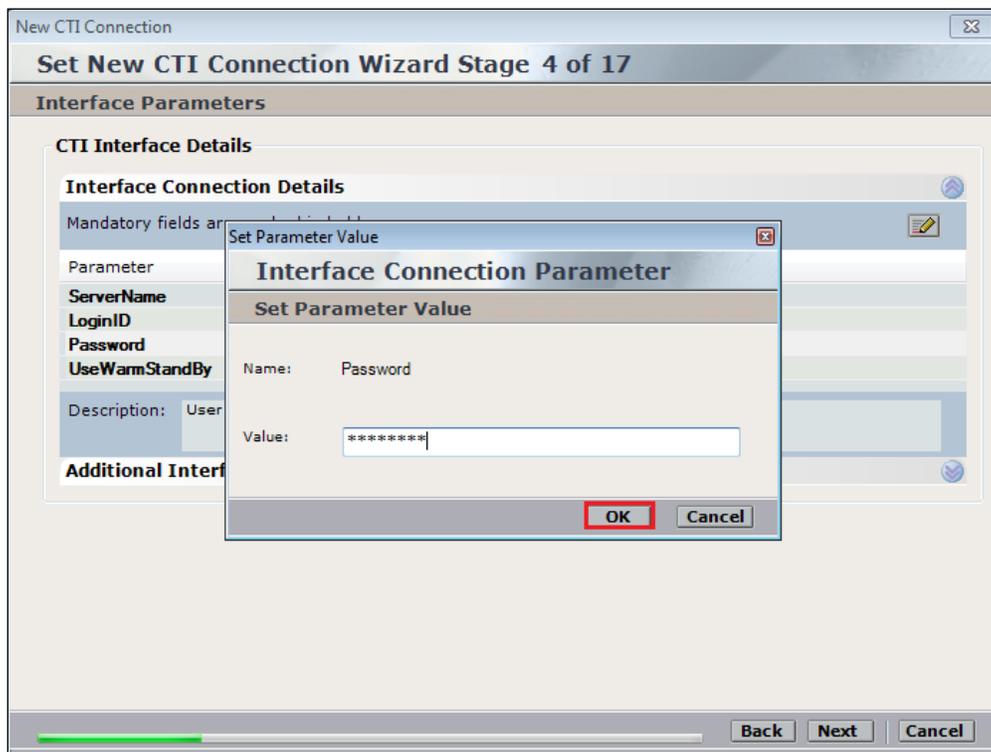
Double-click on **ServerName** and enter the TSAPI Tlink **Value** from **Section 6.4**.



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

Parameter	Value
<b>ServerName</b>	<b>AVAYA#CM101X#CSTA#AESPRI101X</b>
<b>LoginID</b>	<b>nice1</b>
<b>Password</b>	<b>*****</b>
<b>UseWarmStandBy</b>	<b>No</b>

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 4 of 17**

**VoIP Mapping**

**VoIP Mapping Interface Details**

**Interface Connection Details**

Mandatory fields are marked in bold

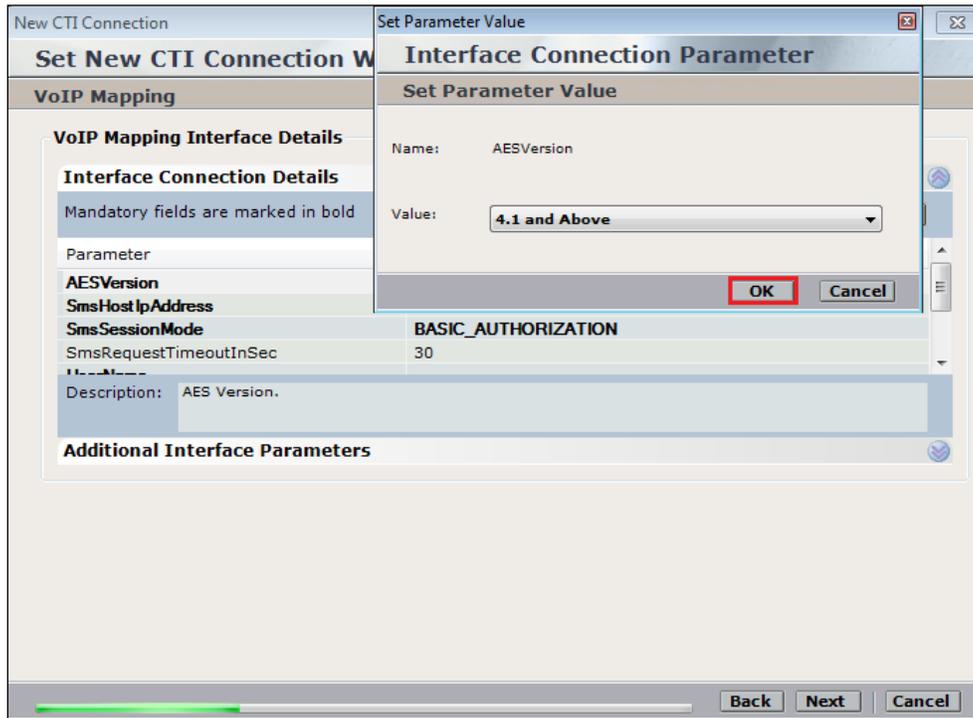
Parameter	Value
<b>AESVersion</b>	<b>Below 4.1</b>
<b>SmsHostIpAddress</b>	
<b>SmsSessionMode</b>	<b>BASIC_AUTHORIZATION</b>
<b>SmsRequestTimeoutInSec</b>	<b>30</b>

Description: AES Version.

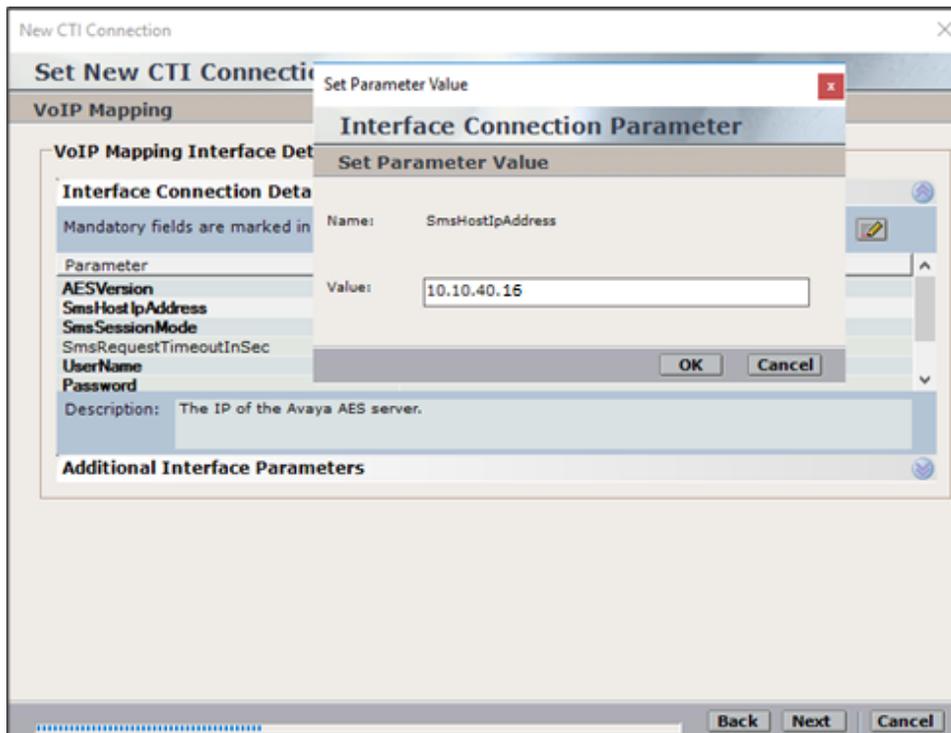
**Additional Interface Parameters**

Back    Next    Cancel

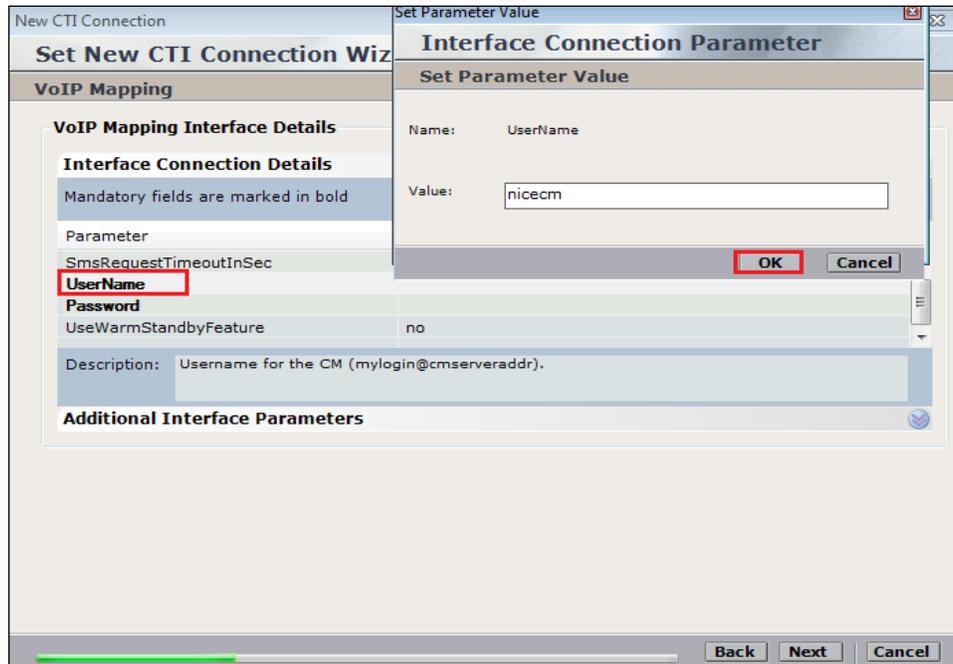
Enter the **Value** for the **AESVersion**. Click on **OK**.



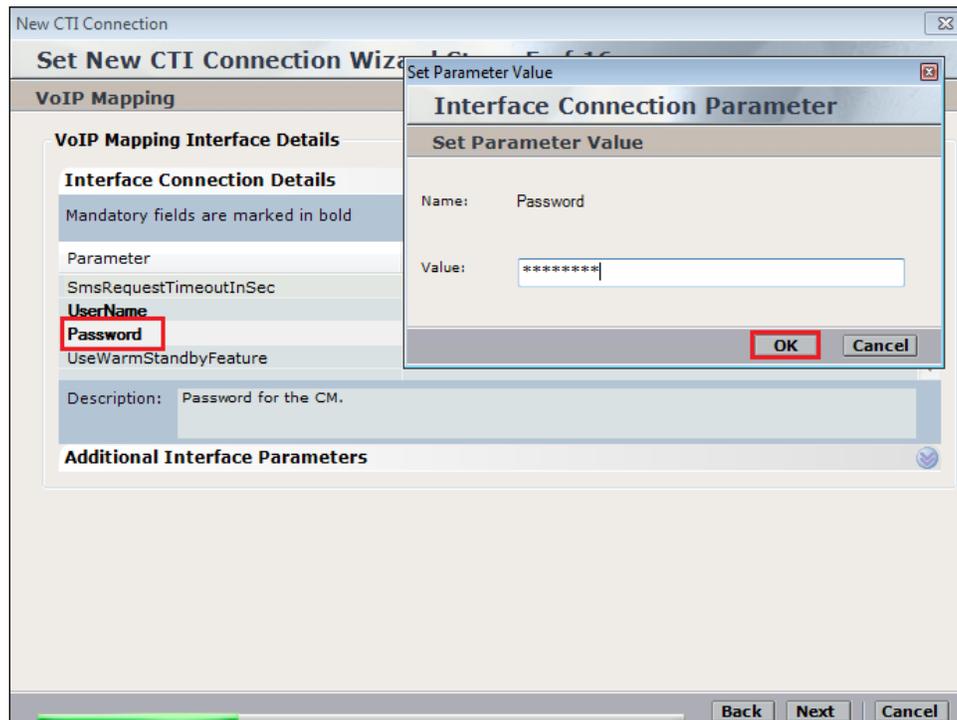
Enter the **Value** for the **SmsHostIpAddress**, note this will be the IP address of the AES in the solution. Click on **OK** to continue.



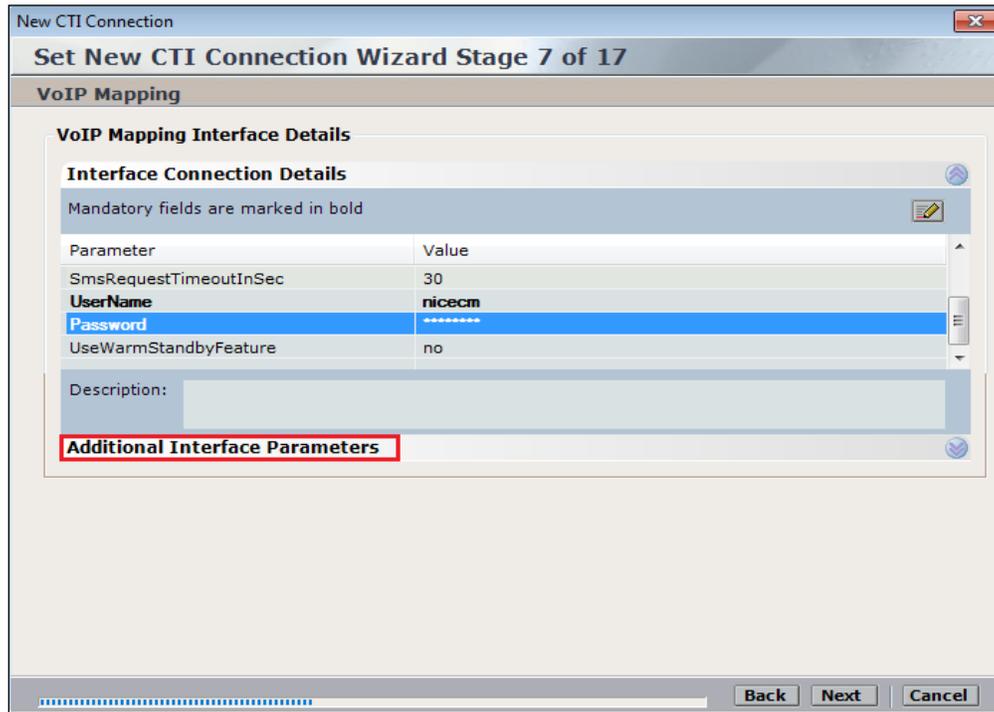
As before, enter the username that was created in **Section 5.5** and click on **OK**. The username can be entered as shown below when one Communication Manager has been associated on the SMS properties, see **Section 6.8**. However, if there are multiple Communication Manager on site then the username must be in the form login@CMIPADDRESS:port



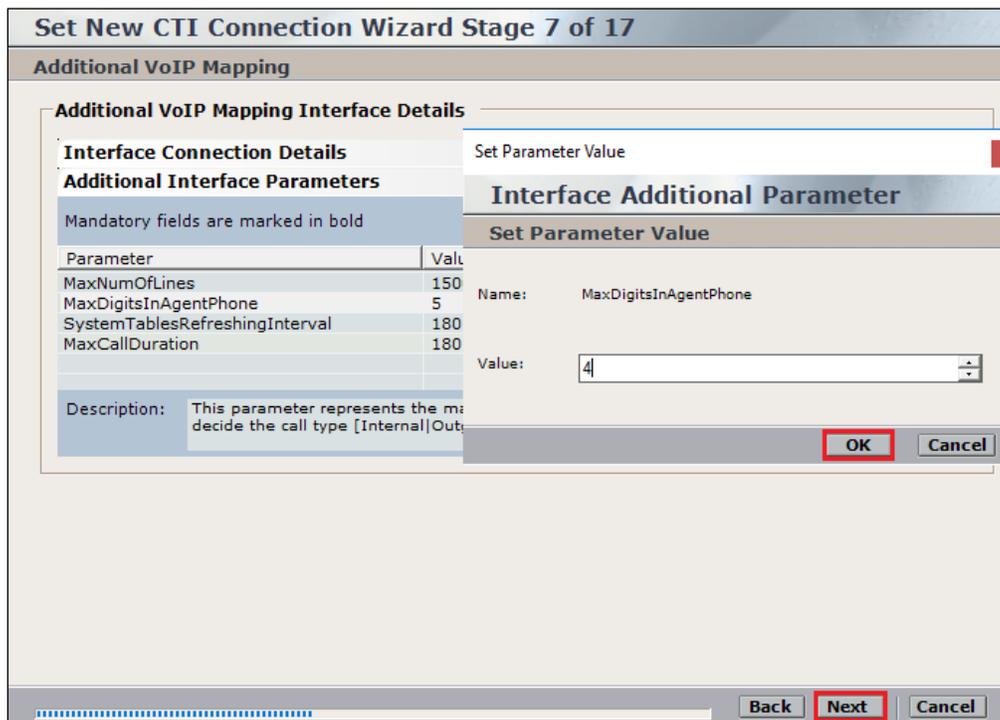
Enter the password that was created in **Section 5.5** and click on **OK**.



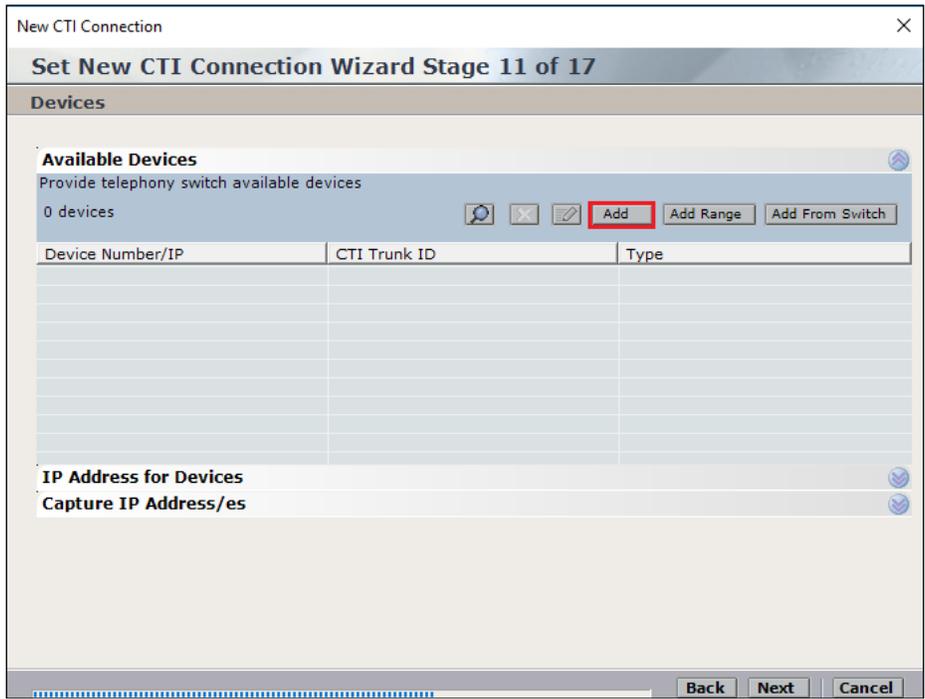
Click on **Additional Interface parameters** to continue.



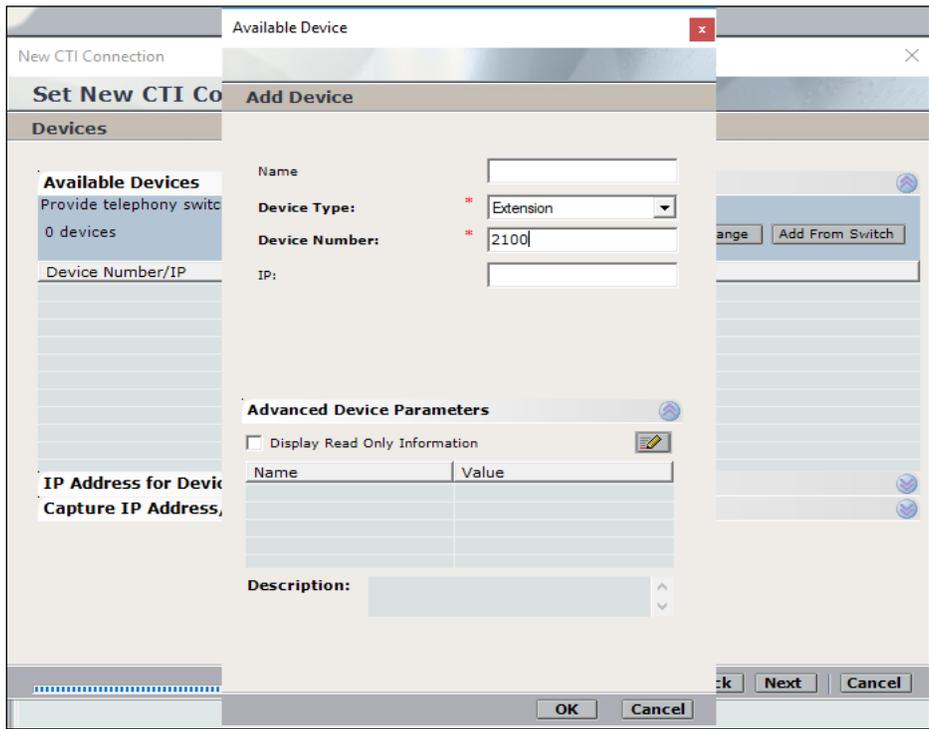
Double-click on **MaxDigitsInAgentPhone** and change the **Value** to **4** as shown below. Click on **Next** at the bottom of the screen.



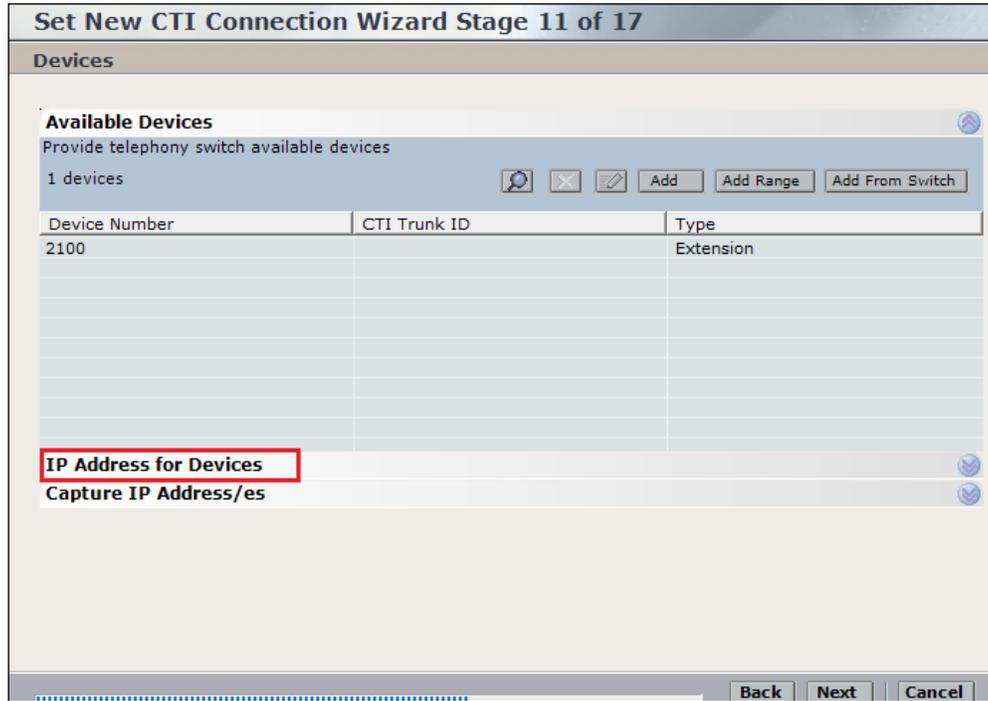
On the following screen, click on **Add**, to add the Communication Manager devices.



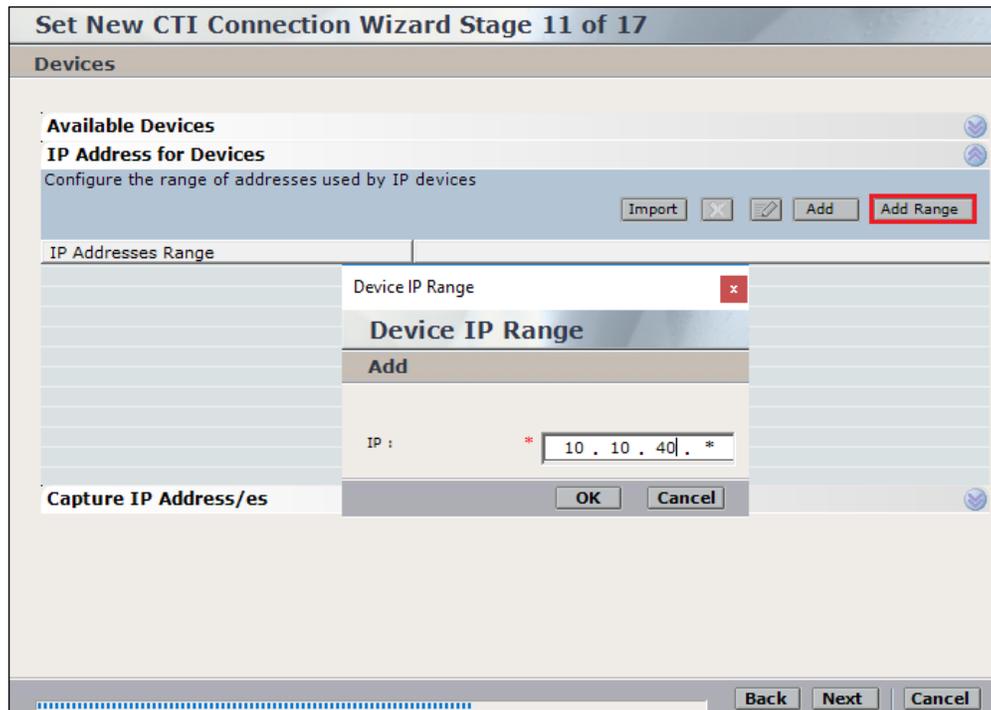
The **Device Type** should be **Extension** and insert the correct extension number. The IP can be left blank if the Generic SIP mapper or the SMS connection will be used to determine the IP address. Click on **OK** to continue.



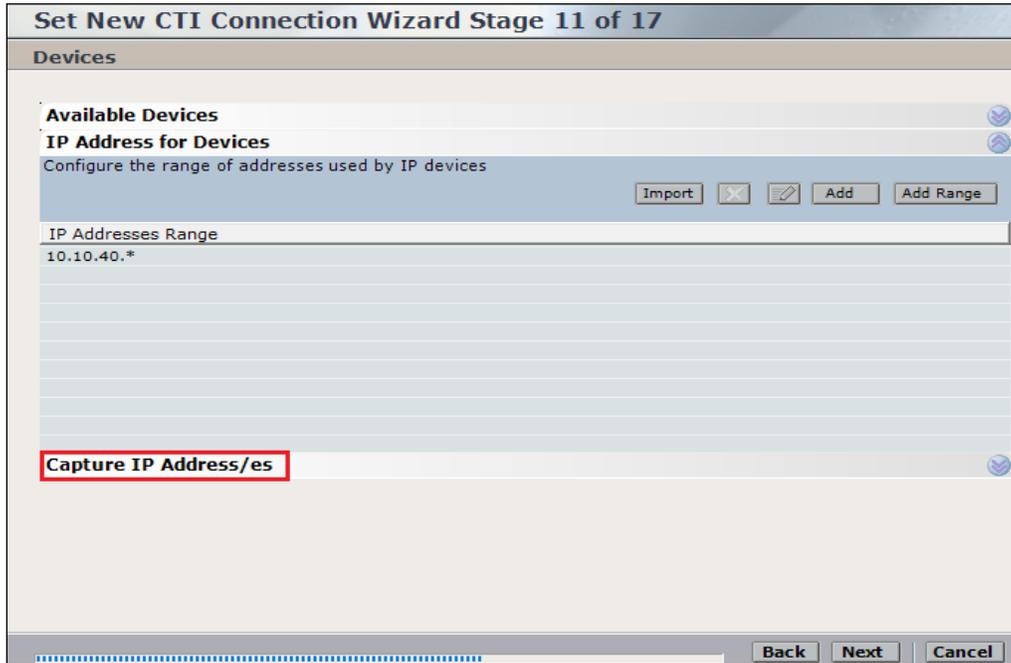
Click on **IP Address for Devices**. This will add the address range for the IP addresses picked up from the SMS connection to the AES.



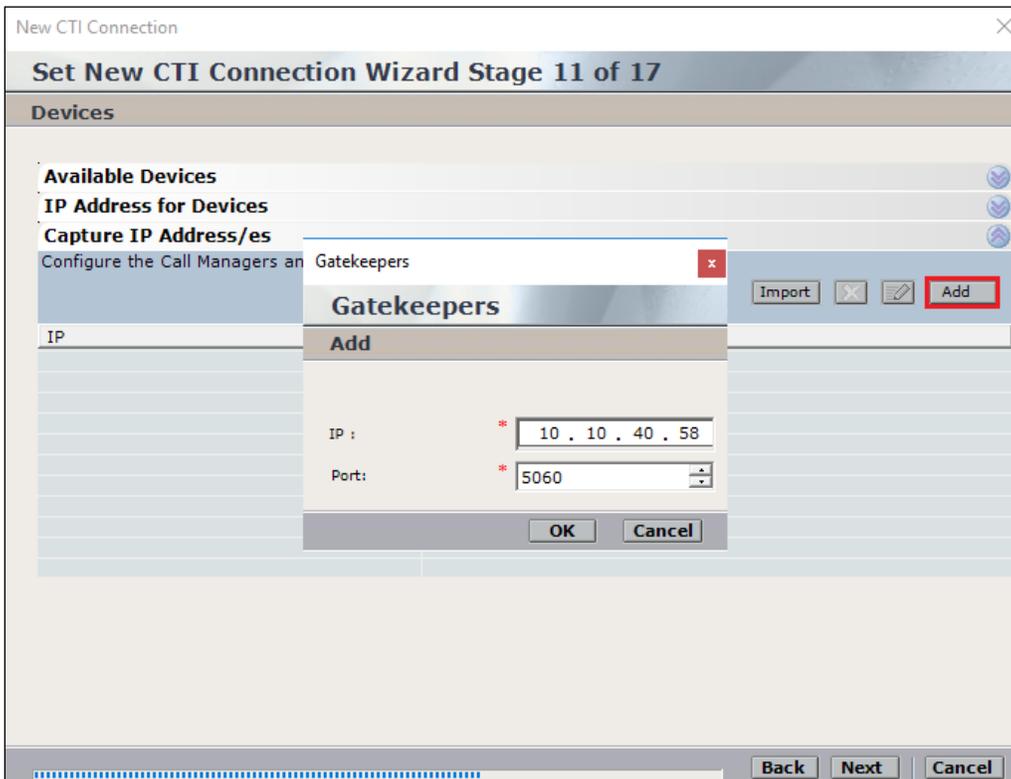
Click on **Add Range** to add the **Device IP Range**. The range is added in the form of x.x.x.\* as shown below where the range is from 10.10.40.1 to 10.10.40.254. Click on **OK**.



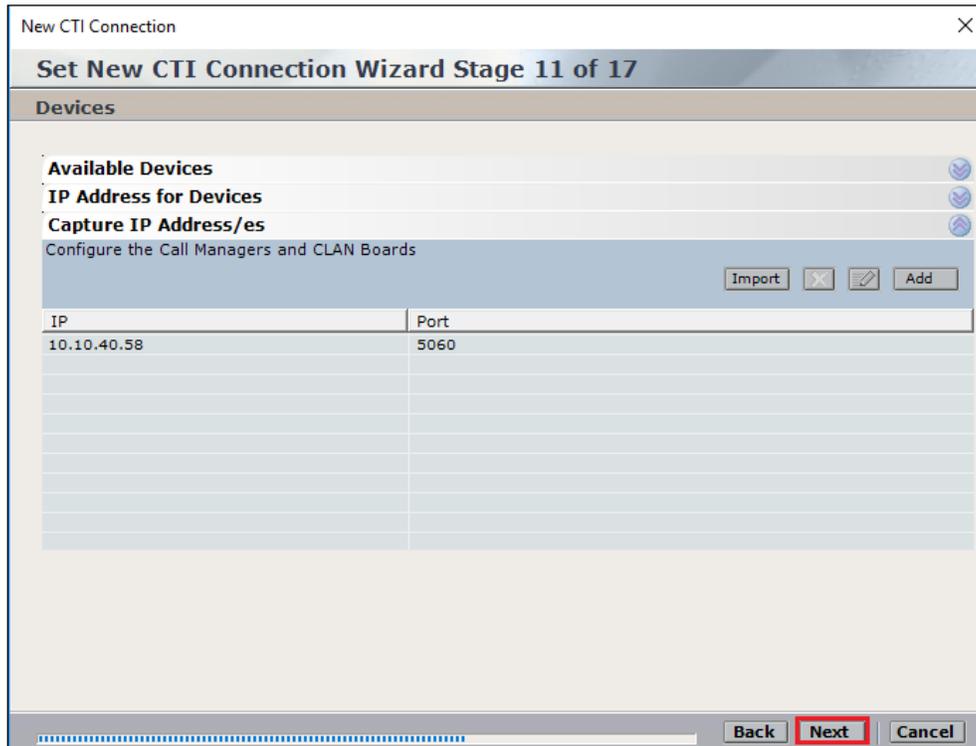
Select **Capture IP Address/es**. This will add the information required for the Generic SIP mapper to capture the IP addresses information of the SIP phones.



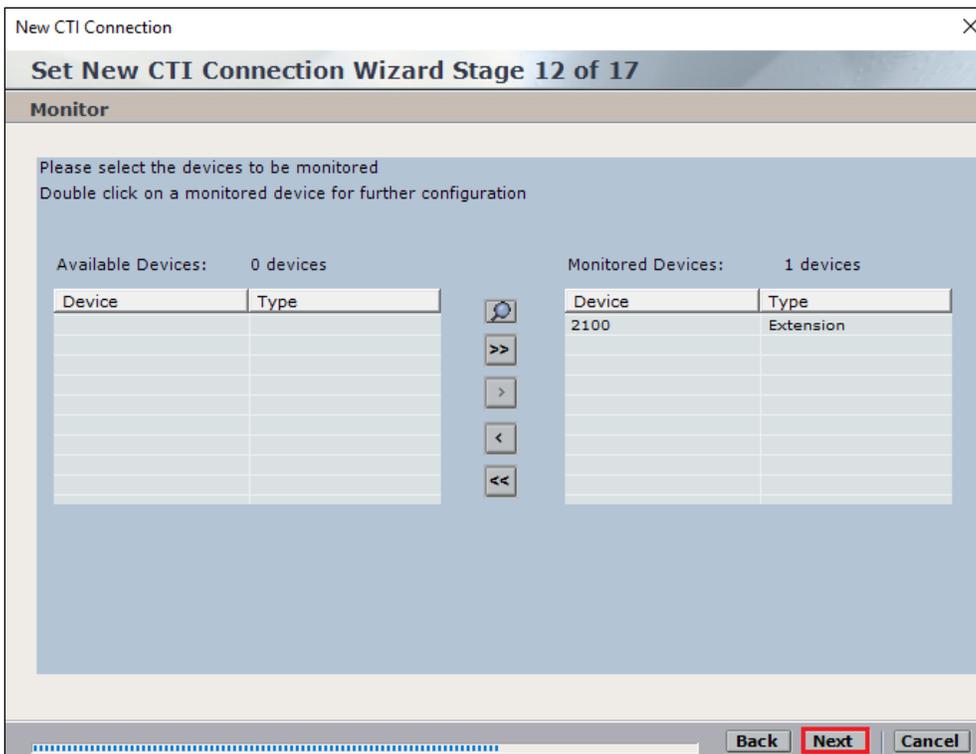
Click on **Add** and enter the Session Manager's IP address and the SIP Port **5060**.



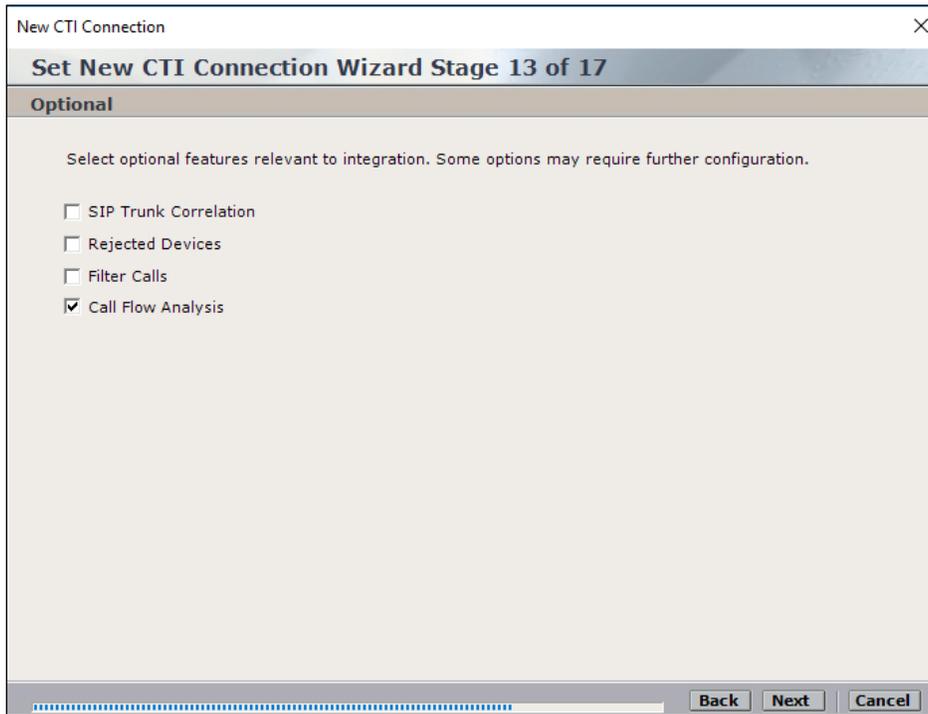
Click on **Next** to continue.



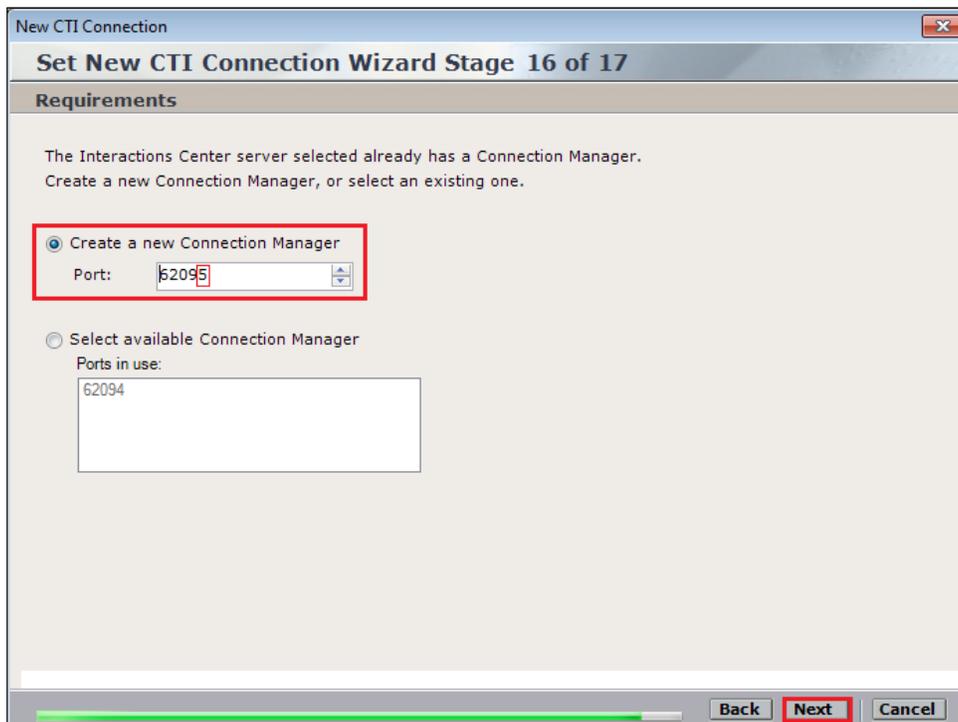
Select the new extension and click on the >> button as shown. Click on **Next** to continue.



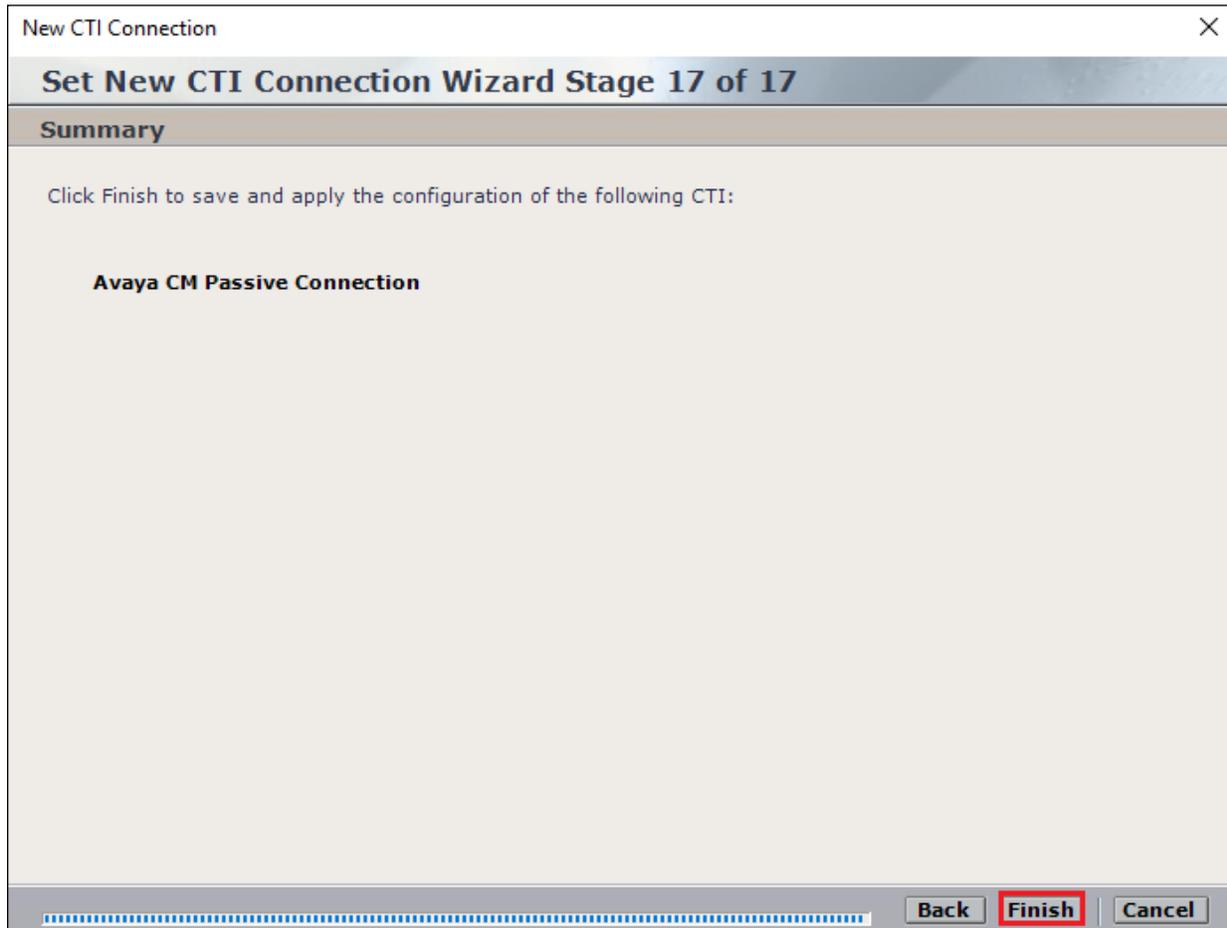
It is optional, but for better analysis tick on **Call Flow Analysis** and click on **Next** to continue.



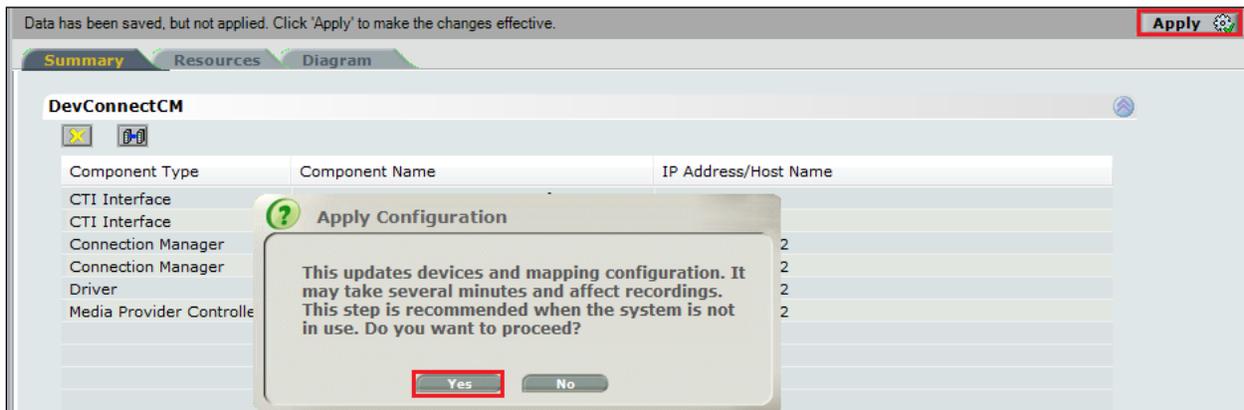
Select a different **Port** number as shown below **62095** is chosen simply because **62094** is already in use.



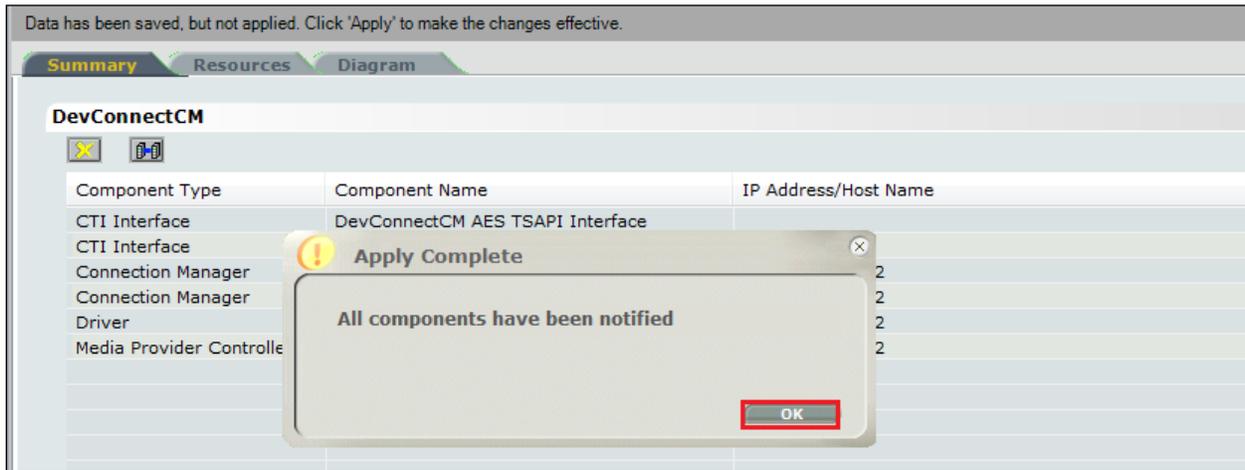
Click on **Finish** to complete the New CTI Wizard.



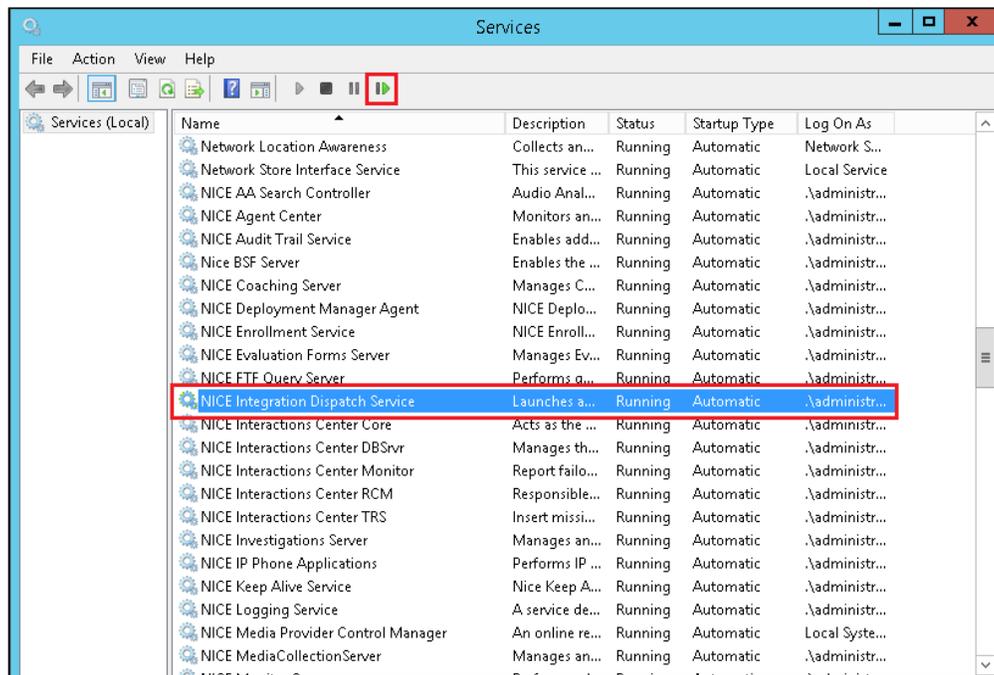
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed.



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

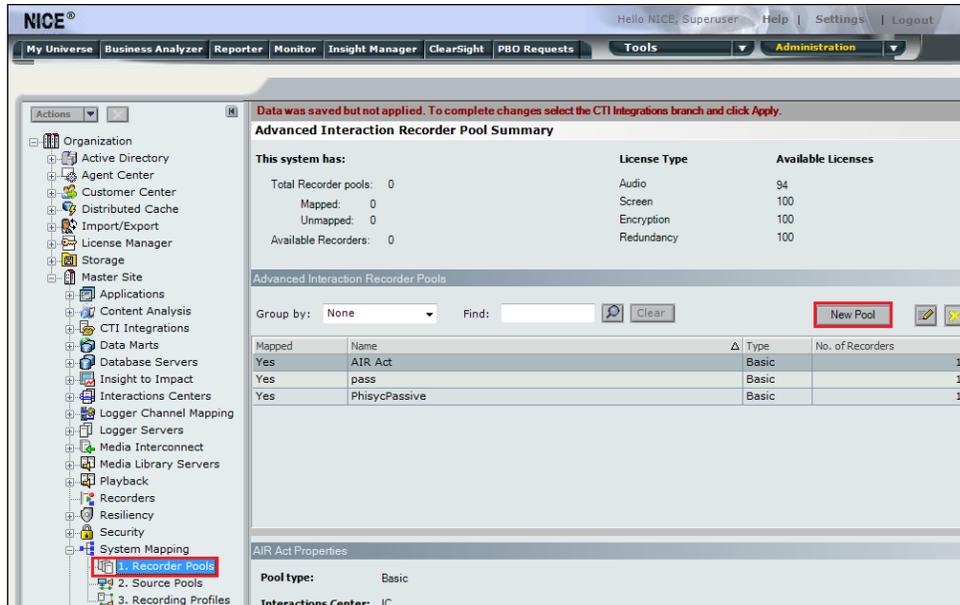


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

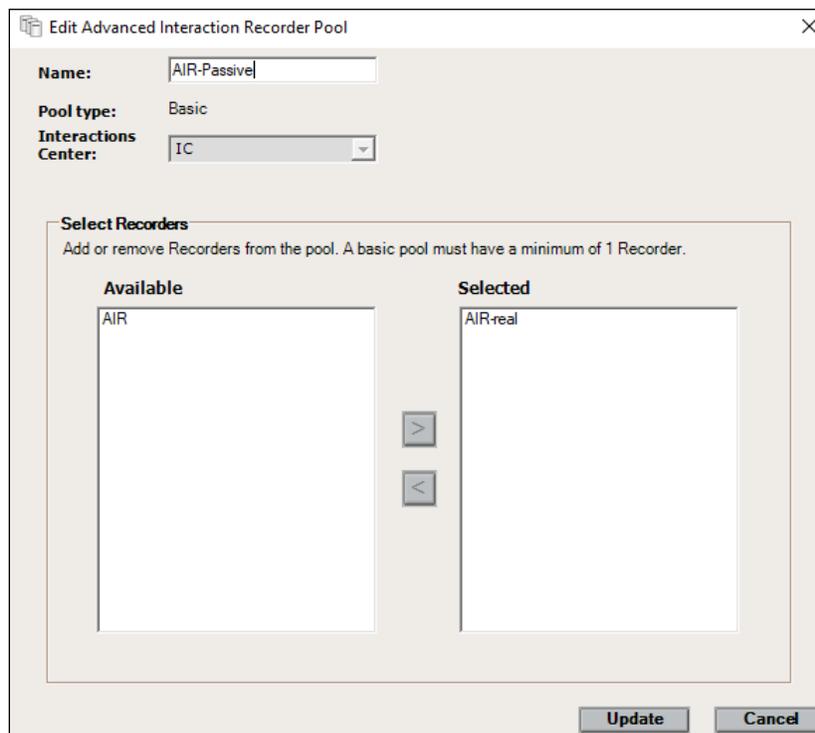


## 7.2. System Mapping

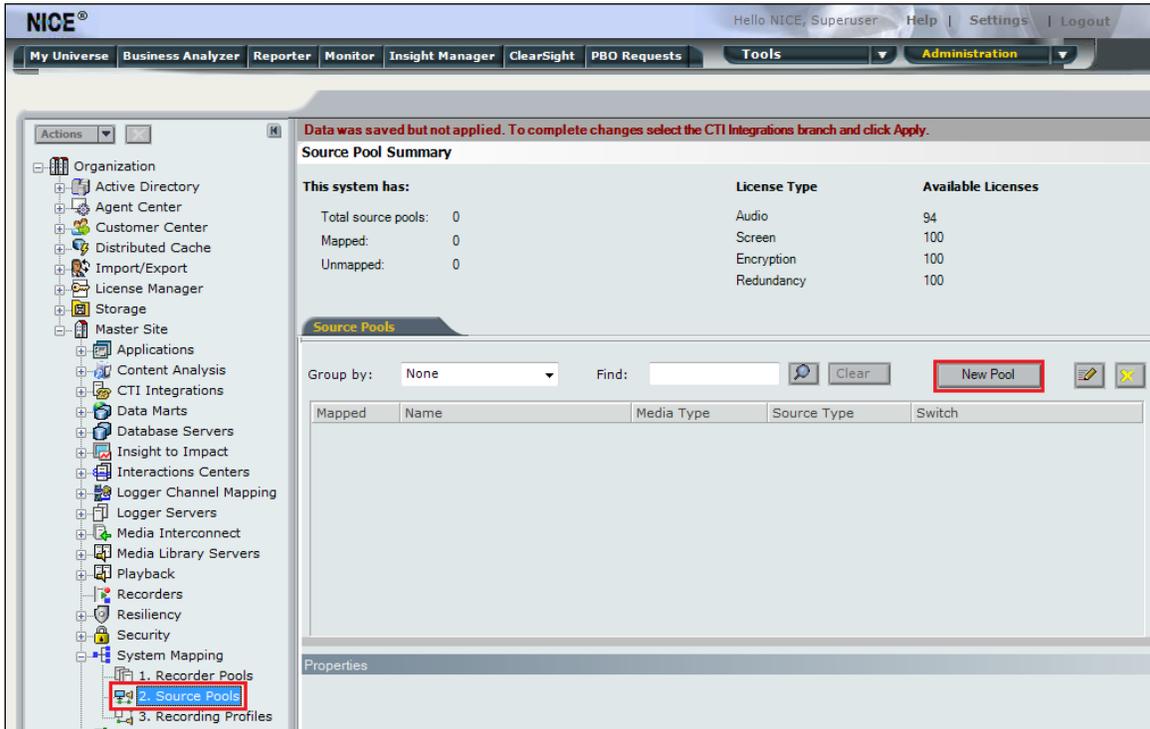
From the web browser navigate to **Master Site** → **System Mapping** → **Recorder Pools**. In the main window click on **New Pool**.



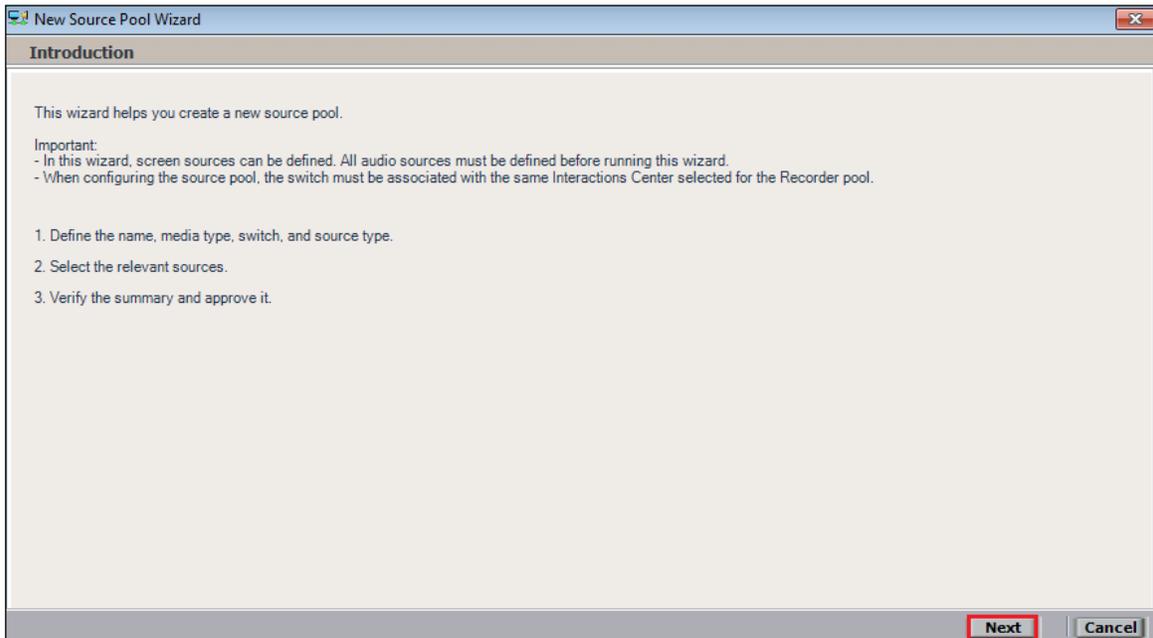
Enter a suitable **Name** for the **Recorder Pool** and select the **AIR-real** from the list of **Available Recorders** and click on **Update** to continue.



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' set to 'Audio', 'Switch' set to 'DevConnectCM (ID = 1075)', and 'Source type' set to 'Device'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red box.

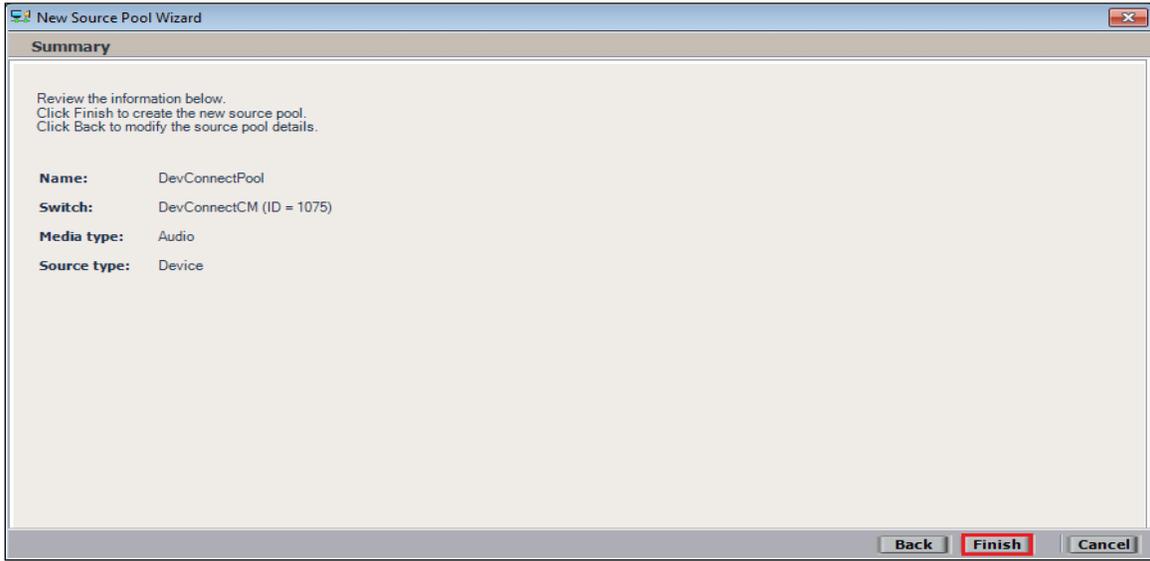
Select the extensions that were created in **Section 7.1**, note only one extension number is shown in the example below but this is not typical. Click on **Next** to continue.

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 'Find:' and a 'Clear' button. To the right, it says 'Selected: 1/1' with 'Select All' and 'Clear Selection' buttons. Below is a table with the following data:

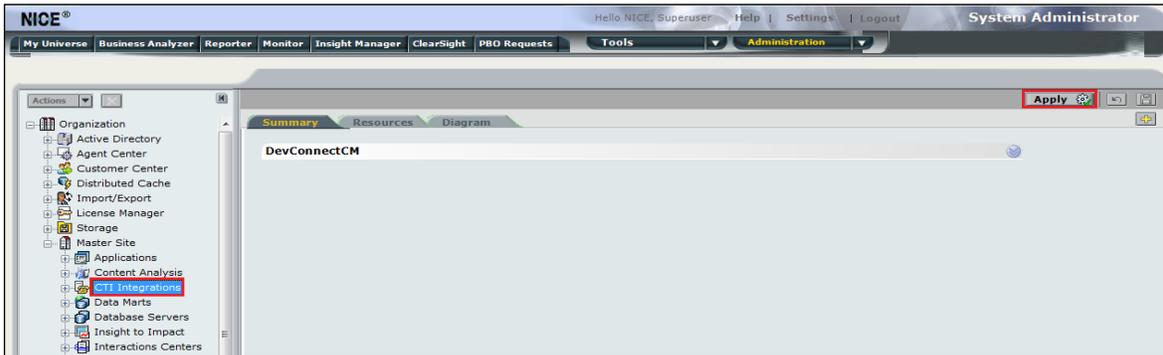
	Name	Device Number	Unique Device ID	IP Address
<input checked="" type="checkbox"/>		2001		

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

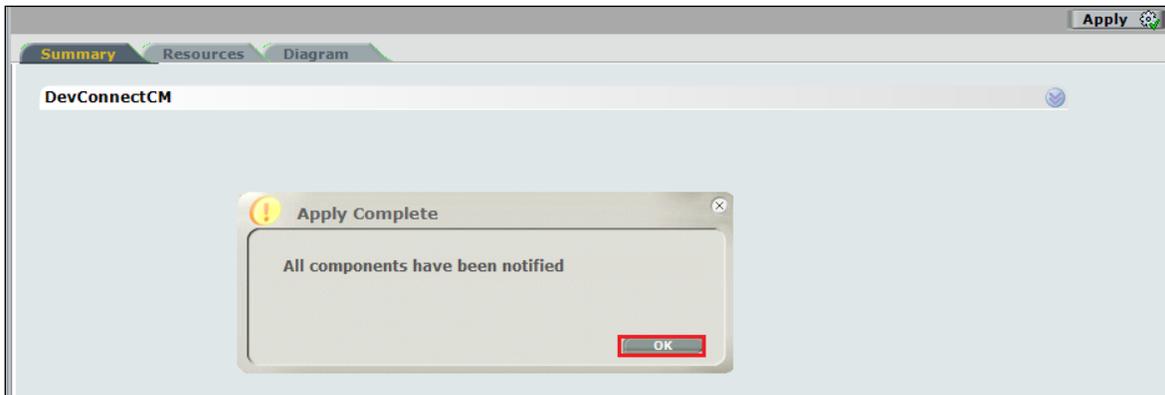
Click on **Finish** to complete the **New Source Pool Wizard**.



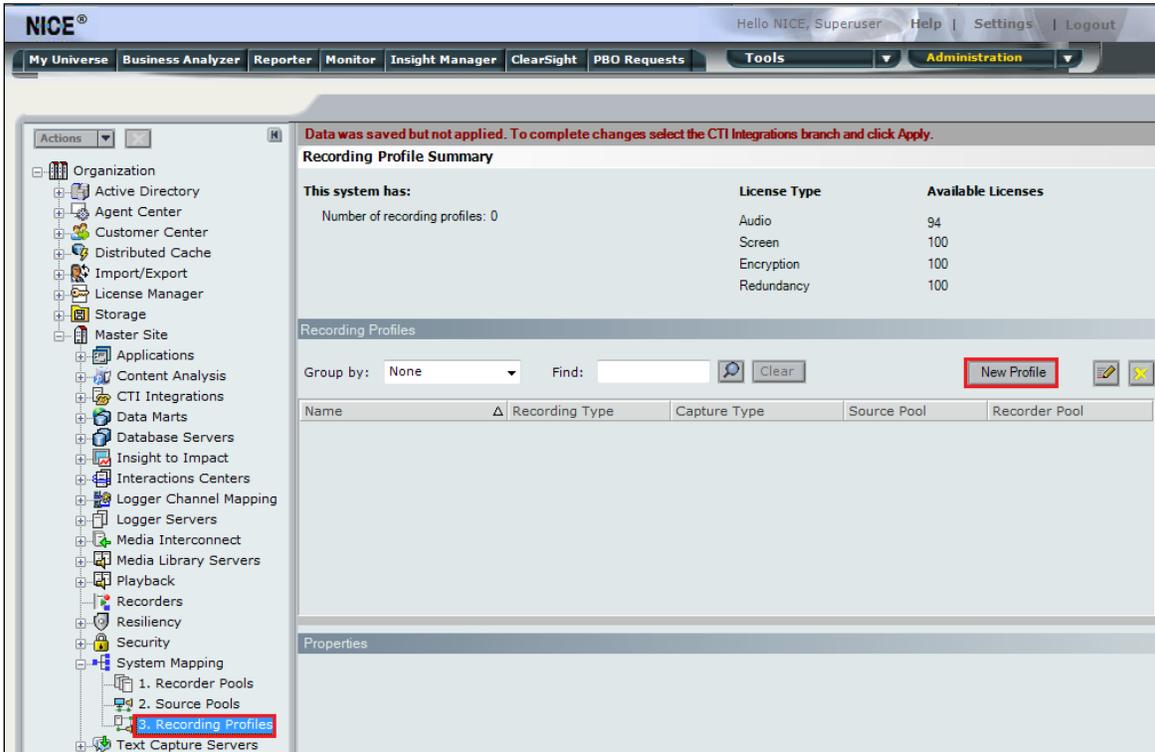
To implement these new changes, navigate to **Master Site** → **CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.



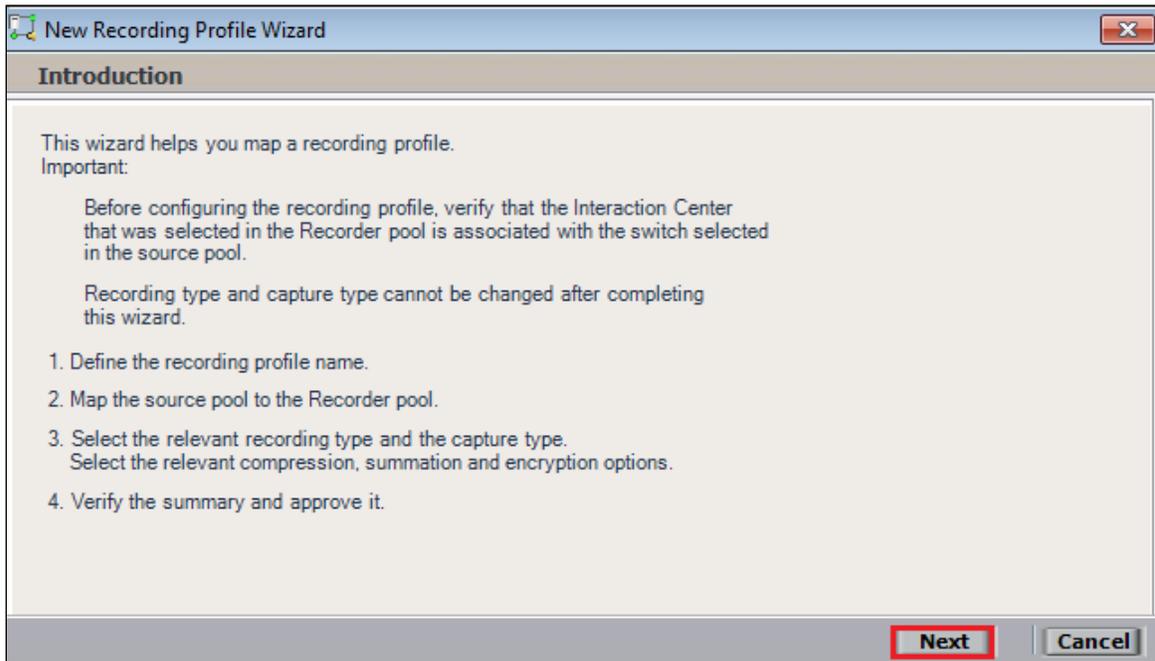
The following screen shows the changes were saved correctly. Click on **OK** to continue.



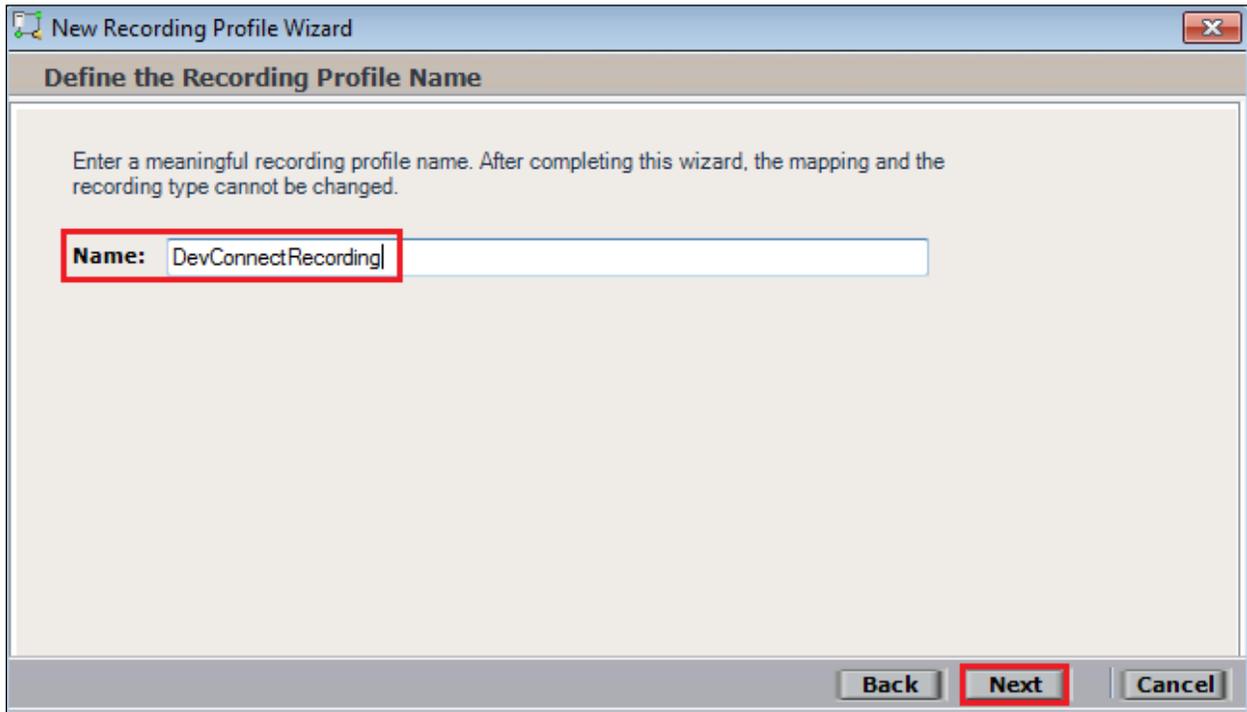
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



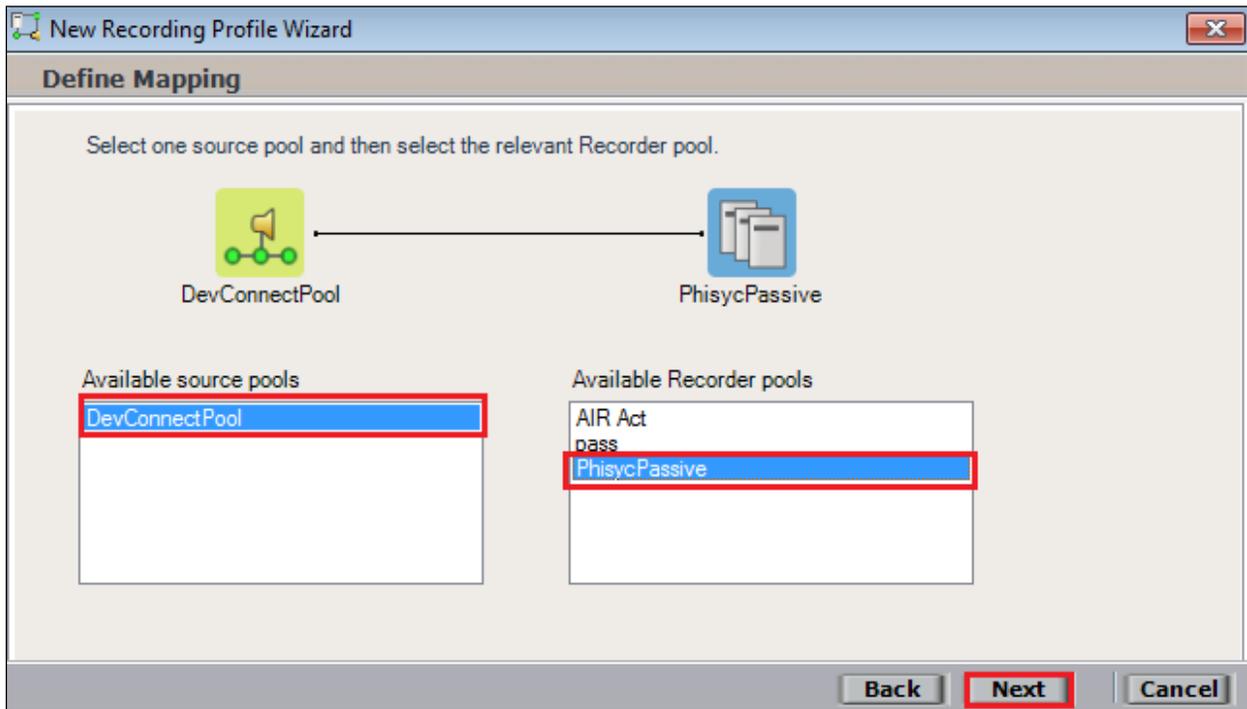
Click on **Next** to continue with the **New Recording Profile Wizard**.



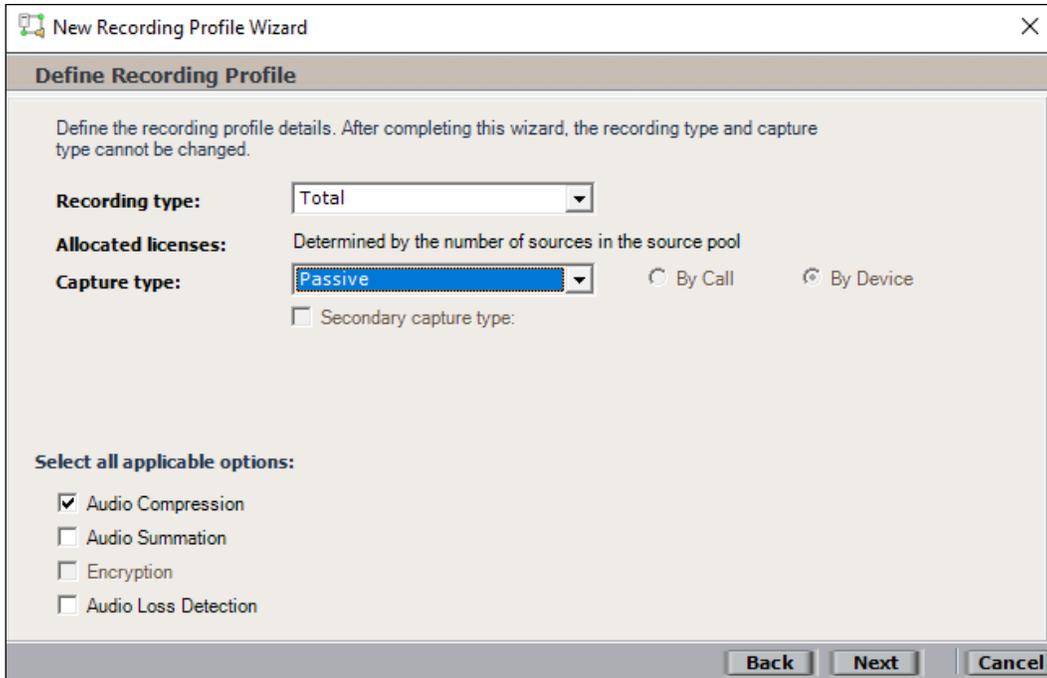
Enter a suitable **Name** for the Recording profile.



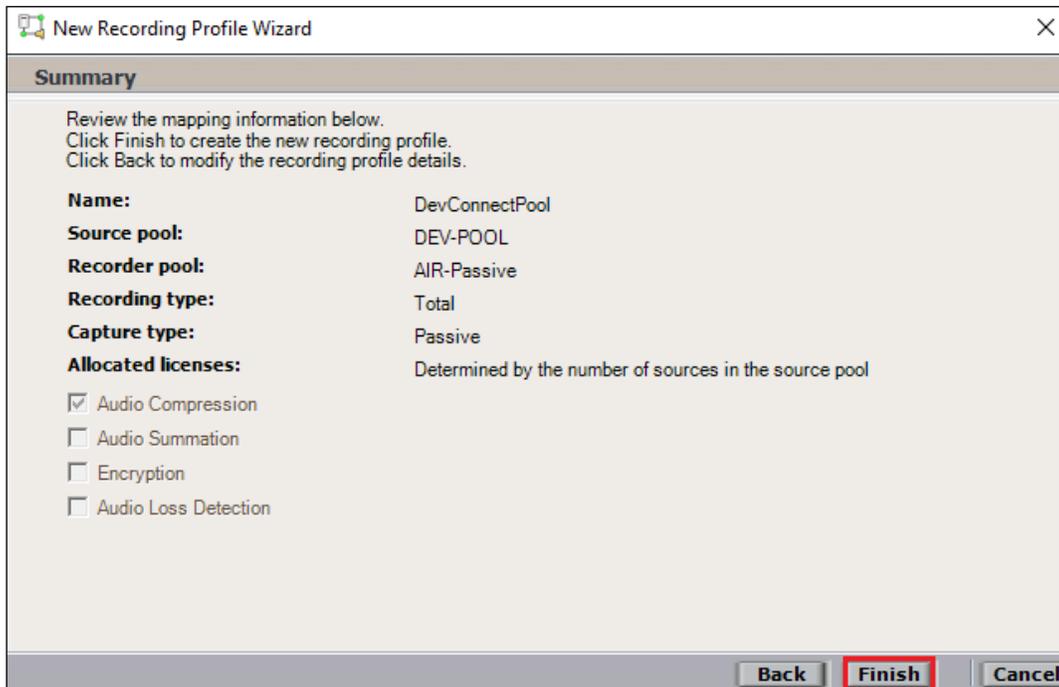
Select the correct **source pool** and **Recorder pool**, click **Next** to continue. The recorder pool below shows **Phisyc Passive**, but this should be the Recorder pool that was created above and, in this case, will be **pass**.



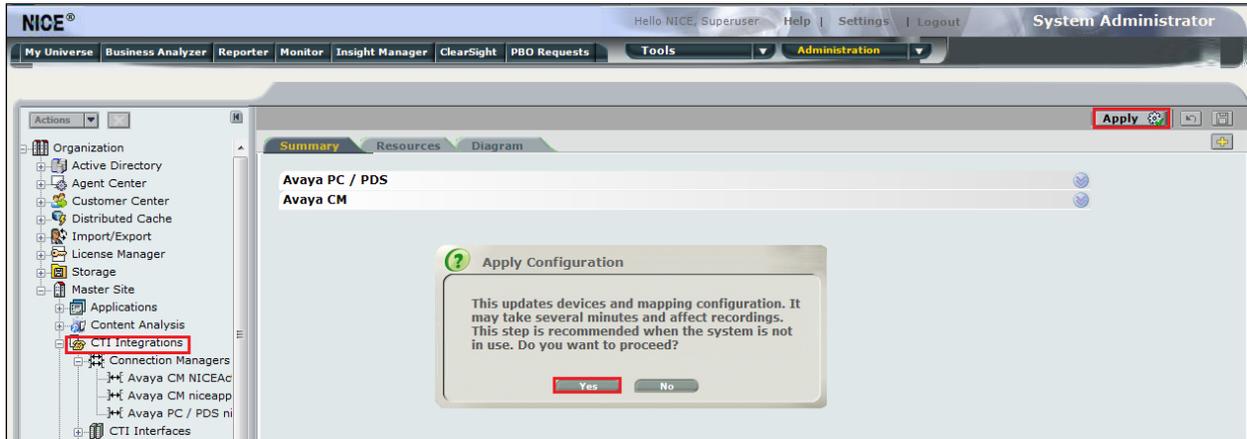
For total recording i.e., the recording of all calls, select **Total** as the **Recording type**. For **Capture type**, ensure that **Passive** is selected from the drop-down box. **Audio Compression** is selected as default and can be left like this. Click on **Next** to continue.



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

## 8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the NICE Engage Platform, Avaya Aura® Communication Manager, 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 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 aevcs cti-link`. Verify the **Service State** of the CTI link is **established**.

```
status aevcs 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	<b>established</b>	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**.

**TSAPI Link Details**

Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	cm101x	1	Talking	Wed Sep 14 18:19:00 2022	Online	20	6	21	23	30

Online Offline

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

TSAPI Service Status TLink Status User 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

### 8.2.1. Verify SMS link

Open a web page to <https://<AESIP>/sms/sms-test.php>, as shown below. Enter the Communication Manager login details and a **Request**, such as List Agent, is entered as shown below, this should return a **Response** as shown.

The screenshot shows a web browser window with the URL [https://10.10.40.16/sms/sms\\_test.php](https://10.10.40.16/sms/sms_test.php). The page title is "String Based - Web Service Request Form".

**SMS Resources**

- Model Documentation
- Model Doc (No-Frames)
- SMS WSDL

**Connection Information**

CM Login ID:  login@<[IPv6]:port|hostname:port>  
 Password:   
 SOAP Request Timeout (Seconds):

**Request Parameters**

Model:  ...  
 Operation:   
 Objectname:   
 Qualifier:   
 Fields:

**Session Recording**

Record SMS Request  
 Record Result Data

**Last Request Response**

Session ID:  [Duplicate Session](#)

Response:

```

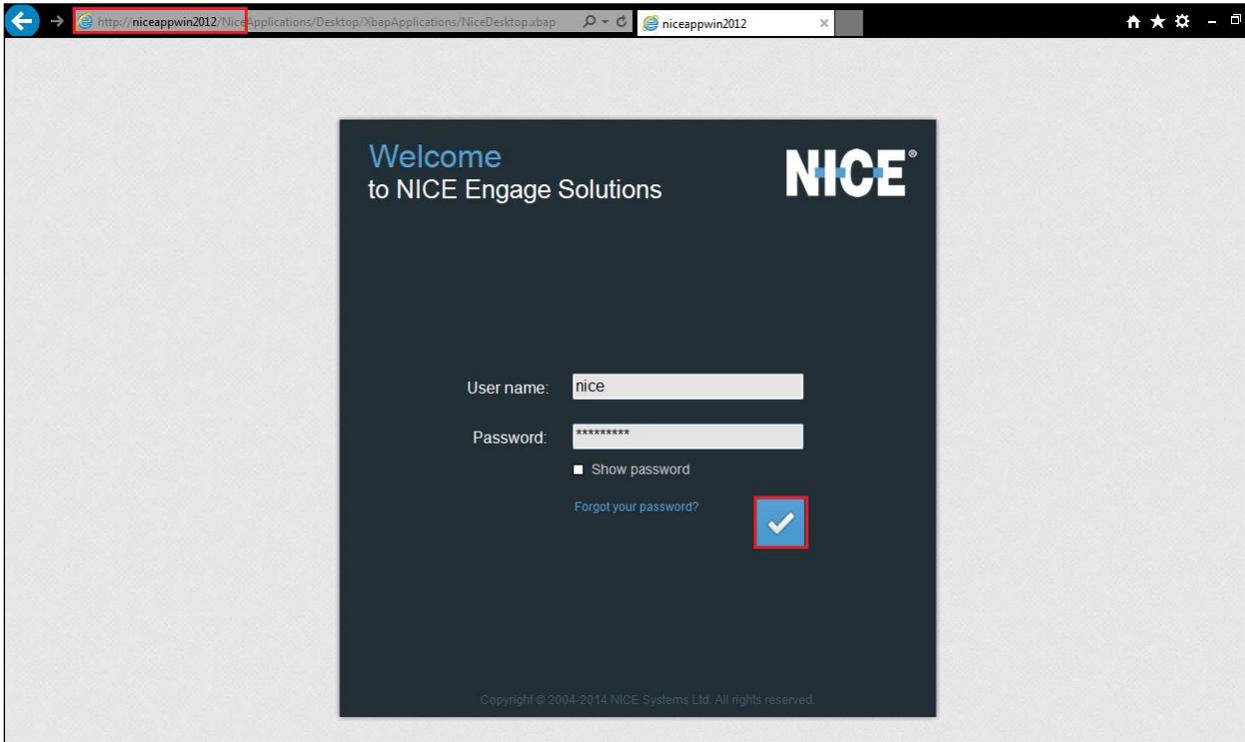
Response {
  var $result_code = 0
  var $result_data = 'Login_ID[0]=3401|Login_ID[1]=3402|Name[0]=Agent
One|Name[1]=Agent
Two|Extension[0]=unstaffed|Extension[1]=unstaffed|Direct_Agent_Skill[0]=|Direct_Age
nt_Skill[1]=|AAS[0]=n|AAS[1]=n|AUDIX[0]=n|AUDIX[1]=n|COR[0]=1|COR[1]=1|Call_Handlin
g_Preference[0]=skill-level|Call_Handling_Preference[1]=skill-
level|Service_Objective[0]=n|Service_Objective[1]=n|SN[0]=|SN[1]=|SL[0]=|SL[1]='

```

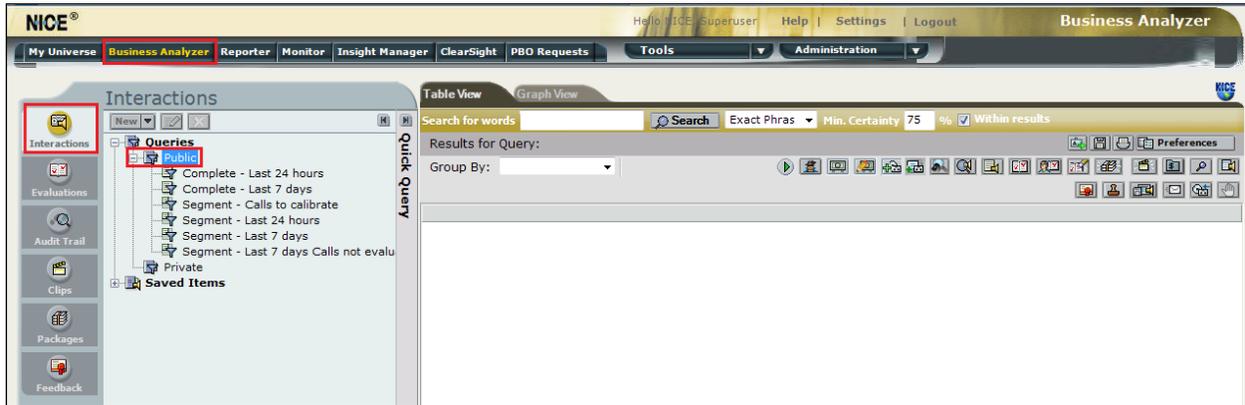
### 8.3. Verify Calls are being Recorded

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

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



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



Click on **Complete – Last 24 hours**. This should reveal all the recordings that took place over the previous 24 hours. Select the required recording from the list and double-click on this to play the recording. The NICE player is opened, and the recording is presented for playback. Click on the **Play/Pause** icon highlighted below to play back the recording.

Results for Query: Complete - Last 24 hours  
Group By: None 25 Records found

Type	Flag	Full Name	Complete ID	Complete Start Time	Complete Stop Time	Complete Dur...	Comple...	Direction Ty...	HangUp Side Description	Participant Phone Number
		SIP, 3101	7197848976168648969	08/02/2023 18:10:15	08/02/2023 18:11:22	00:01:08	2	Outgoing	CUSTOMER	35391847001
		H323, 3001	7197848568146755843	08/02/2023 18:08:43	08/02/2023 18:10:00	00:01:17	2	Outgoing	AGENT	35391847001
		Workplace, 3110	7197847215232057598	08/02/2023 18:03:22	08/02/2023 18:03:44	00:00:21	2	Outgoing	CUSTOMER	35391847001
		H323, 3001	7197847069203169522	08/02/2023 18:02:56	08/02/2023 18:03:33	00:00:37	2	Outgoing	CUSTOMER	5321
		SIP, 3101	7197847090678006006	08/02/2023 18:02:56	08/02/2023 18:03:31	00:00:36	2	Outgoing	CUSTOMER	5350
		Workplace, 3110	7197846596756766959	08/02/2023 18:00:58	08/02/2023 18:01:10	00:00:13	2	Outgoing	AGENT	35391847001
		SIP, 3101	7197846437842877004	08/02/2023 18:00:25	08/02/2023 18:00:41	00:00:16	2	Outgoing	AGENT	35391847001
		H323, 3001	7197846339058729193	08/02/2023 18:00:02	08/02/2023 18:00:17	00:00:15	2	Outgoing	AGENT	35391847001
		H323, 3001	7197845862317359333	08/02/2023 17:58:09	08/02/2023 17:58:23	00:00:14	2	Incoming	AGENT	35391847001
		SIP, 3101	7197845793597882595	08/02/2023 17:57:50	08/02/2023 17:58:00	00:00:10	2	Incoming	AGENT	35391847001
		Workplace, 3110	7197845793597882595							35391847001
		Workplace, 3110	7197845793597882595							35391847001
		SIP, 3101	7197845793597882595							35391847001
		H323, 3001	7197845793597882595							35391847001
		SIP, 3101	7197845793597882595							35391847001
		H323, 3001	7197845793597882595							35391847001
		SIP, 3101	7197845793597882595							35391847001
		Workplace, 3110	7197845793597882595							35391847001
		Workplace, 3110	7197845793597882595							35391847001
		SIP, 3101	7197845793597882595							35391847001
		H323, 3001	7197845793597882595							35391847001
		SIP, 3101	7197845793597882595							35391847001
		Workplace, 3110	7197845793597882595							35391847001
		Workplace, 3110	7197845793597882595							35391847001
		SIP, 3101	7197845793597882595							35391847001
		H323, 3001	7197845793597882595							35391847001

Start: 08/02/2023 18:10:15 | End: 08/02/2023 18:11:22 | Add | 00:00:00/00:01:07

Elapsed Time: 0 00:10 00:20 00:30 00:40 00:50 01:00

Summed Events

Customer Events

Agent Events

Time: 18:10:15 18:10:28 18:10:41 18:10:55 18:11:08 18:11:22

Customer SIP, 3101

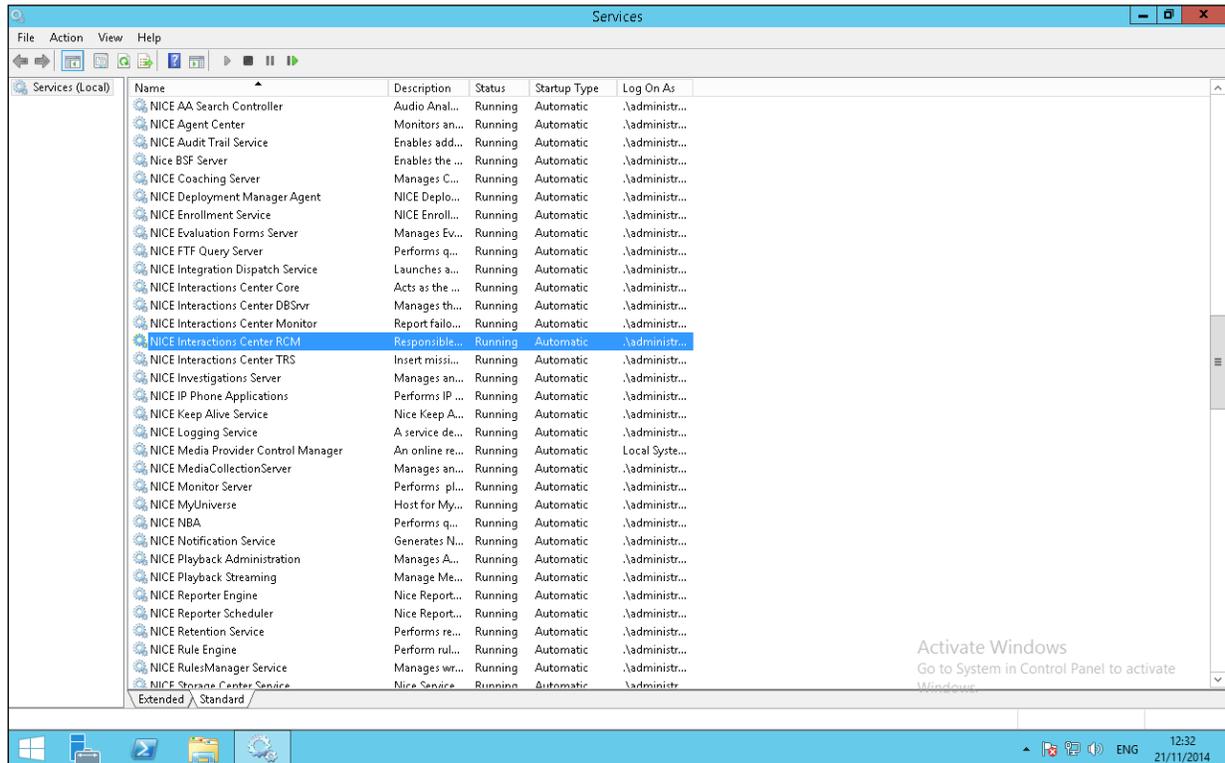
Preview Segments

Type	Flag	Full Name	Segment ID	Segment Start Time	Segment Stop Time	Segment Duration	Participant Station	Direction Type Description	Participant Phone Number	Segment Dialed Number
		SIP, 3101	719784899053550858	08/02/2023 18:10:15	08/02/2023 18:11:22	00:01:08	3101	Outgoing	35391847001	35391847001
		SIP, 3101	719784899053550858	08/02/2023 18:10:15	08/02/2023 18:11:22	00:01:08		Outgoing	35391847001	35391847001

**Note:** If call recordings are not shown up here, Wireshark could be opened on the NICE Passive server, using the interface connected to the Mirrored Port to check that RTP is coming to that port.

## 8.4. 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 Passive Logger, both servers 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 Passive Station-Side VoIP with SMS to record calls. All feature functionality and serviceability test cases were completed successfully with no issues or 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](mailto:devconnect@avaya.com).