



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring NICE Engage Platform R6.4 to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 using Passive Station Side VoIP recording - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for the NICE Engage Platform to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0 using Passive Station Side VoIP recording with SMS.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps for the NICE Engage Platform R6.4 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0 and Avaya Aura® Application Enablement Services R7.0. The NICE Engage Platform was setup to use passive station-side VoIP recording with SMS and the Telephony Services API (TSAPI) via the 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 that are to be recorded are plugged into the Avaya 4548GT-PWR layer 3 switch where all of these particular ports are mirrored to one port where the NICE Advanced Interactions server is plugged into. All of the RTP information from all of these phone sets will be delivered to the sniffer port on the NICE Advanced Interactions server. An additional Network Interface Card (NIC) is therefore required on the NICE Advanced Interactions Server. This NIC is not configured to access the IP stack. It will have 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 record.

The NICE Engage Platform is fully integrated into a LAN (Local Area Network), and includes easy-to-use Web based applications (i.e. Nice Application) that works with the Microsoft .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. The NICE Engage Platform uses both the Telephony Services Application Programming Interface (TSAPI) and the System Management Service (SMS) connections on AES. The SMS web service provides the ability to discover the status of resources on Communication Manager.

The NICE Engage Platform contains tools for audio retrieval, centralized system security authorization, system control, and system status monitoring. Also included is a call parameters database (Nice Application Server) that tightly integrates via CTI link PABXs and ACD's including optional advanced audio archive database management, search tools, a wide variety of Recording-on-Demand capabilities, and comprehensive long-term call database for immediate retrieval.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the NICE Engage Platform to carry out call recording in a variety of scenarios using 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.

### 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 one-X® Agent.
- **Serviceability testing** - The behavior of NICE Engage Platform under different simulated failure conditions.

### 2.2. Test Results

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

1. **Call Park.** The un-parked call is not being recorded. It appears that there are no events being sent for un-parking a call by Communication Manager. Modification Report [**CM-9860**] has been raised with the Communication Manager support team. A fix for this issue will be implemented for release 7.1 of Communication Manager.  
**Note:** When configured for total recording, the un-parked call should be recorded and the call record should appear once Total Recording Service picks up the session.

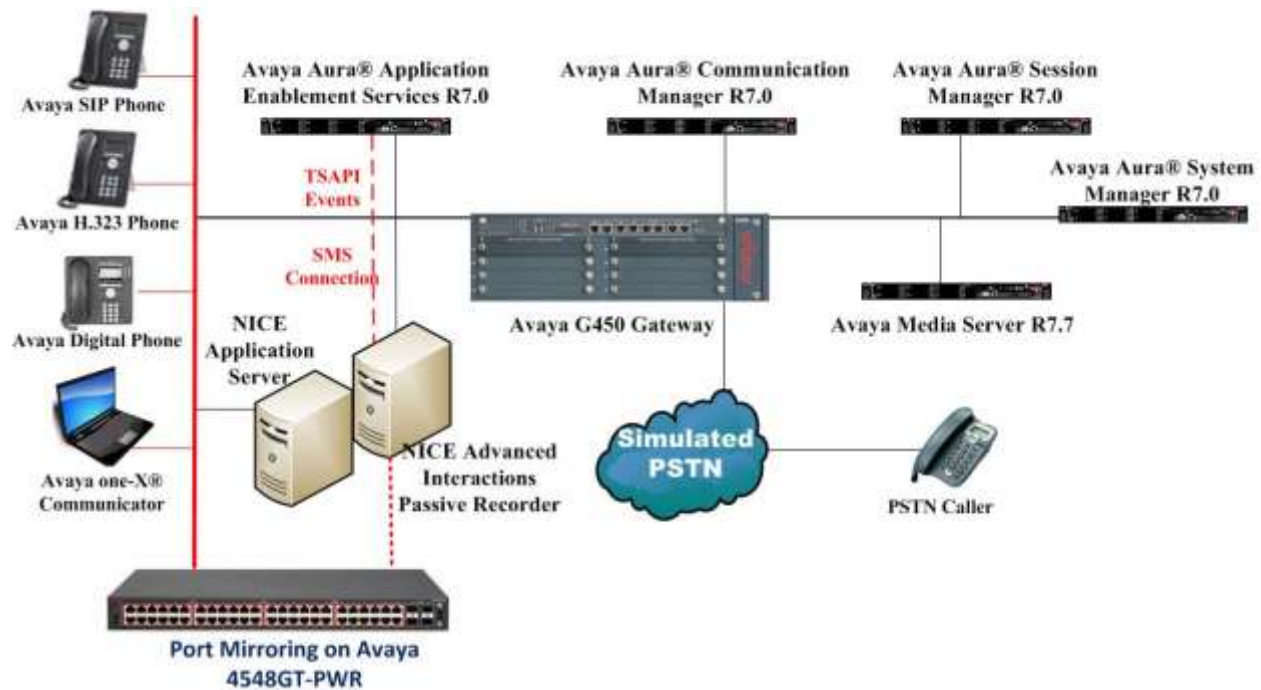
## 2.3. Support

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

## 3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Engage Platform with the Avaya solution using passive recording to record calls. The Avaya 4548GT-PWR switch is configured to mirror ports that the Avaya endpoints are connected to, to one port where the NICE Advanced Interactions recorder sniffer port is connected to.

**Note:** Any data switch that is capable of port mirroring can be used, the data switch shown in the diagram is that which was used for compliance testing.



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

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Virtual Server	R7.0.0.0.0 Build 7.0.0.0.16266-7.0.9.9.902 SW Update Revision No. 7.0.0.0.3873
Avaya Aura® Session Manager running on Virtual Server	R7.0.0.0.700007
Avaya Aura® Communication Manager running on Virtual Server	R7.0 Build 017x.00.0.441.0.22477
Avaya Aura® Application Enablement Services running on Virtual Server	R7.0 Build No – 7.0.0.0.0.13-0
Avaya G450 Gateway	37.19.0 /1
Avaya 4548GT-PWR Ethernet Switch	Boot Image: ver. 5.0.0.9 Diag Image: ver. 5.1.0.8 Agent Image: ver. 5.7.0.009
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 6.5.0.17
Avaya 9630 SIP Deskphone	R2.6.13.1
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Avaya one-X® Agent	R 2.5.50022.0
NICE Engage Platform <ul style="list-style-type: none"><li>- NICE Application Server</li><li>- Advanced Interactions Recorder</li></ul>	R6.4

## 5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

### 5.1. Verify System Features

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

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

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

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

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM100	10.10.40.34		
<b>aes63vmpg</b>	<b>10.10.40.16</b>		
default	0.0.0.0		
g450	10.10.40.15		
<b>procr</b>	<b>10.10.40.13</b>		

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

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

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

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

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

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

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

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

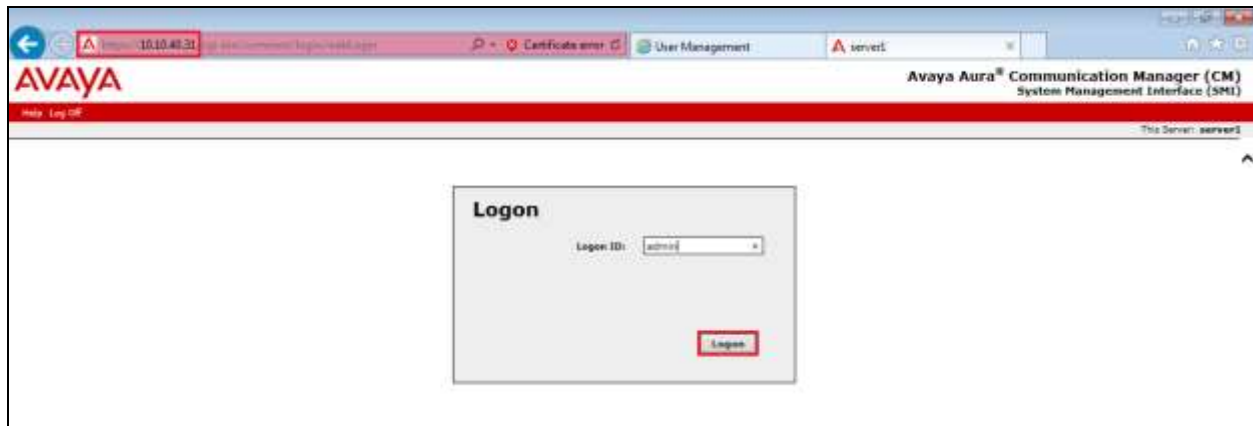
### 5.4. Configure CTI Link for TSAPI Service

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

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

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

This user is created specifically for the SMS connection that NICE utilise 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.

The screenshot displays the Avaya Administration web interface. The top navigation bar includes 'Help' and 'Log Off' links, and the page title is 'Administration'. The left sidebar contains a tree view of system functions, with 'Security' expanded and 'Administrator Accounts' highlighted. The main content area is titled 'Administrator Accounts' and includes a description: 'The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.' Below this, a 'Select Action:' section contains several radio button options. The 'Add Login' option is selected and highlighted with a red box, and the 'Privileged Administrator' sub-option is also selected. Other options include 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. Below these are three radio button options for 'Change Login', 'Remove Login', and 'Lock/Unlock Login', each followed by a 'Select Login' dropdown menu. There are also radio button options for 'Add Group' and 'Remove Group', each followed by a 'Select Group' dropdown menu. At the bottom of the form, there are 'Submit' and 'Help' buttons, with the 'Submit' button highlighted by a red box.

**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**.

The screenshot shows the Avaya Administration web interface. The top navigation bar includes 'Help', 'Log Off', and 'Administration'. Below this, a breadcrumb trail reads 'Administration / Server (Maintenance)'. A left-hand sidebar contains a tree view of configuration categories: 'Server Configuration' (with sub-items like Server Role, Network Configuration, Static Routes, Display Configuration, Time Zone Configuration, NTP Configuration), 'Server Upgrades' (with sub-items like Manage Updates), 'IPSI Firmware Upgrades' (with sub-items like IPSI Version, Download IPSI Firmware, Download Status, Activate IPSI Upgrade, Activation Status), 'Data Backup/Restore' (with sub-items like Backup Now, Backup History, Schedule Backup, Backup Logs, View/Restore Data, Restore History), 'Security' (with sub-items like Administrator Accounts, Login Account Policy, Change Password, Login Reports, Server Access, Syslog Server, Authentication File, Load Authentication File, Firewall, Install Root Certificate, Trusted Certificates, Server/Application Certificates, Certificate Alarms, Certificate Signing Request, SSH Keys, Web Access Mask), and 'Web Access Mask'. The main content area is titled 'Administrator Accounts -- Add Login: privileged Administrator'. Below the title, a descriptive text states: 'This page allows you to add a login that is a member of the USERS group. This login has reduced access privileges.' The form contains several fields: 'Login name' (text input with 'nicecm'), 'Primary group' (text input with 'users'), 'Additional groups (profile)' (dropdown menu with 'prof19'), 'Linux shell' (text input with '/bin/bash'), 'Home directory' (text input with '/var/home/nicecm'), 'Lock this account' (checkbox), 'SAT Limit' (dropdown menu with 'none'), 'Date after which account is disabled-blank to ignore (YYYY-MM-DD)' (text input), 'Select type of authentication' (radio buttons for 'Password' (selected), 'ASG: enter key', and 'ASG: Auto-generate key'), 'Enter password or key' (password input), 'Re-enter password or key' (password input), and 'Force password/key change on next login' (radio buttons for 'Yes' and 'No' (selected)). At the bottom of the form are three buttons: 'Submit', 'Cancel', and 'Help'. Red rectangular boxes highlight the 'Login name' field, the password input fields, and the 'Submit' button.

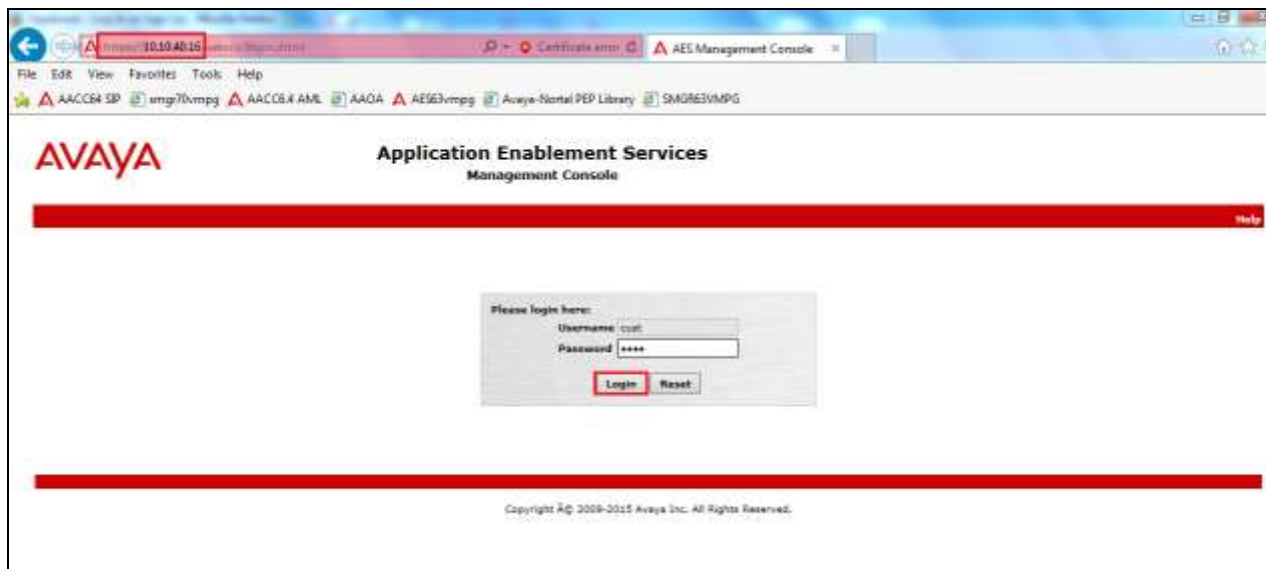
## 6. Configure Avaya Aura® Application Enablement Services

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

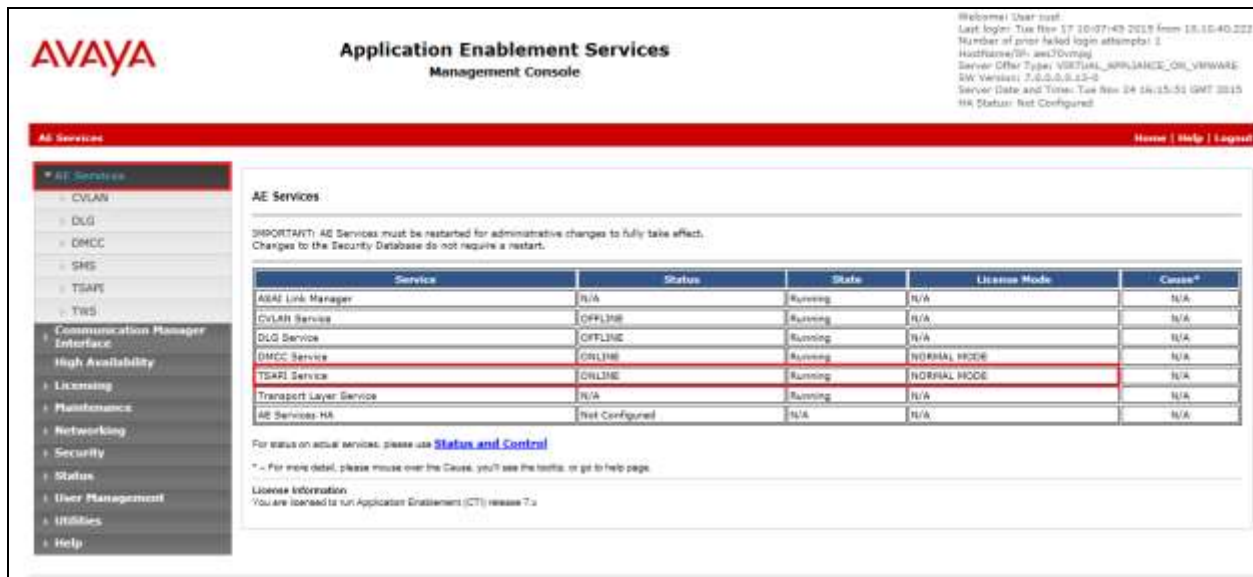
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Set Up Security Database on AES
- Associate Devices with CTI User

### 6.1. Verify Licensing

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



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



**AVAYA** Application Enablement Services Management Console

Welcome! User: root  
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222  
Number of prior failed login attempts: 1  
HostName/IP: ams70vmg  
Server Offer Type: VSEVIRTUAL\_APLIANCE\_OB\_VMWARE  
SW Version: 7.0.0.0.13-0  
Server Date and Time: Tue Nov 24 16:15:51 GMT 2015  
HA Status: Not Configured

**AE Services**

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

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

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

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

License Information:  
You are licensed to run Application Enablement (CT) release 7.0

## 6.2. Create Switch Connection

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



**AVAYA** Application Enablement Services Management Console

Welcome! User: root  
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222  
Number of prior failed login attempts: 1  
HostName/IP: ams70vmg  
Server Offer Type: VSEVIRTUAL\_APLIANCE\_OB\_VMWARE  
SW Version: 7.0.0.0.13-0  
Server Date and Time: Tue Nov 24 16:16:56 GMT 2015  
HA Status: Not Configured

**Communication Manager Interface | Switch Connections**

Switch Connections

Enter Name:  **Add Connection**

Connection Name	Processor Ethernet	Plug Period	Number of Active Connections
<a href="#">Edit Connection</a> <a href="#">Edit PE/CLAN 3ds</a> <a href="#">Edit H.323 Gatekeeper</a> <a href="#">Delete Connection</a> <a href="#">Survivability Hierarchy</a>			

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

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

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

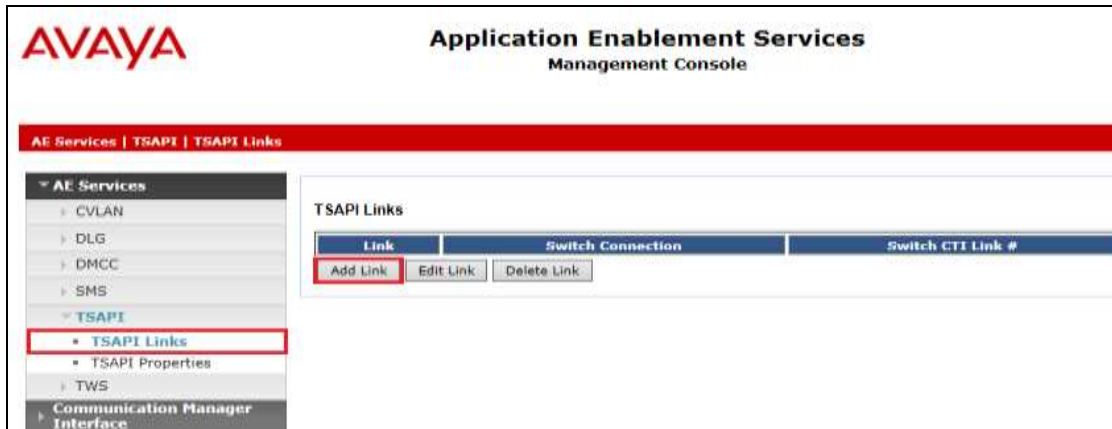
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar is the same as the previous screenshot. The main content area is titled 'Edit Processor Ethernet IP - cm70vmppg'. It contains a text input field with the IP address '10.10.40.13'. To the right of the input field is a button labeled 'Add/Edit Name or IP', which is highlighted with a red box. Below the input field is a table with the following structure:

Name or IP Address
10.10.40.13

At the bottom of the form is a 'Back' button.

### 6.3. Administer TSAPI link

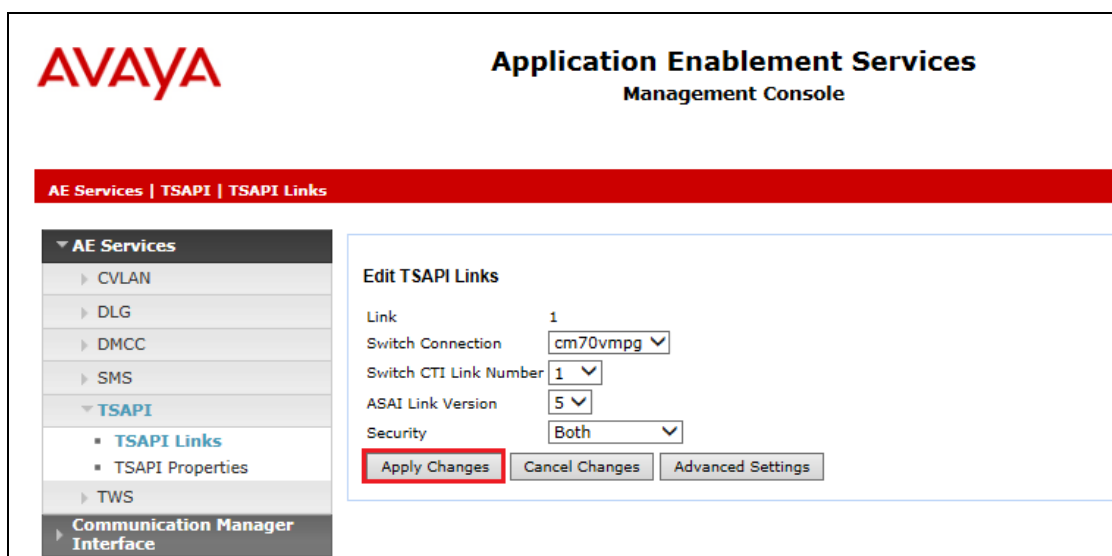
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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 **cm70vmppg**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



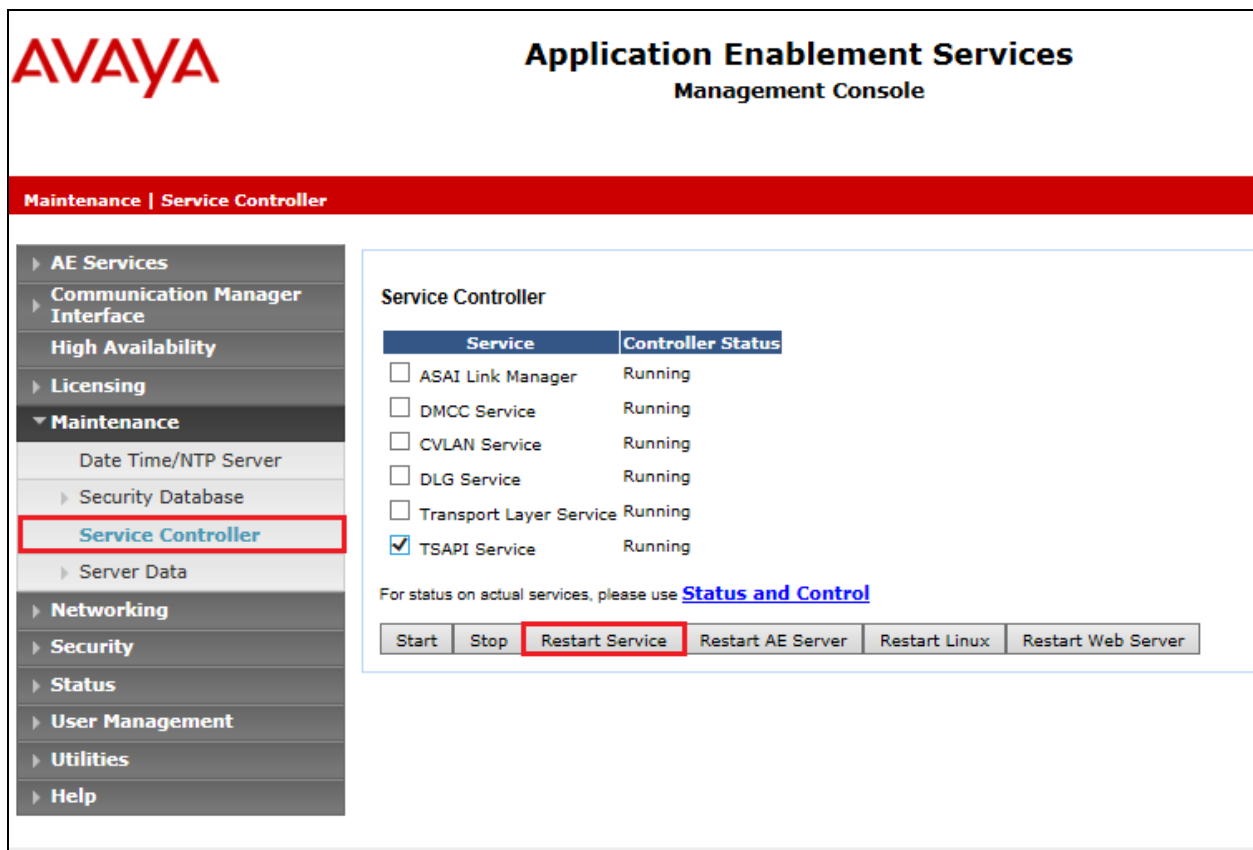
Another screen appears for confirmation of the changes made. Choose **Apply**.

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

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

The screenshot shows the Avaya Application Enablement Services Management Console after the TSAPI link has been applied. The left sidebar is the same as in the previous screenshot, but the 'TSAPI Links' section is now expanded, showing a list of links. The main content area displays a table titled 'TSAPI Links'. The table has five columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. There is one row in the table with the following values: '1', 'cm70vring', '1', '1', and 'Both'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'. In the top right corner, there is a status bar with the following information: 'Hostname/IP: avaya70vring', 'Server OS: Type: VIRTUAL\_APPLIANCE\_OS\_UMWARE', 'SW Version: 7.0.0.0-0.12-0', 'Server Date and Time: Tue Nov 24 16:25:03 GMT 2015', and 'NA Status: Not Configured'.

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



**AVAYA** Application Enablement Services Management Console

Maintenance | Service Controller

Service Controller

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

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

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



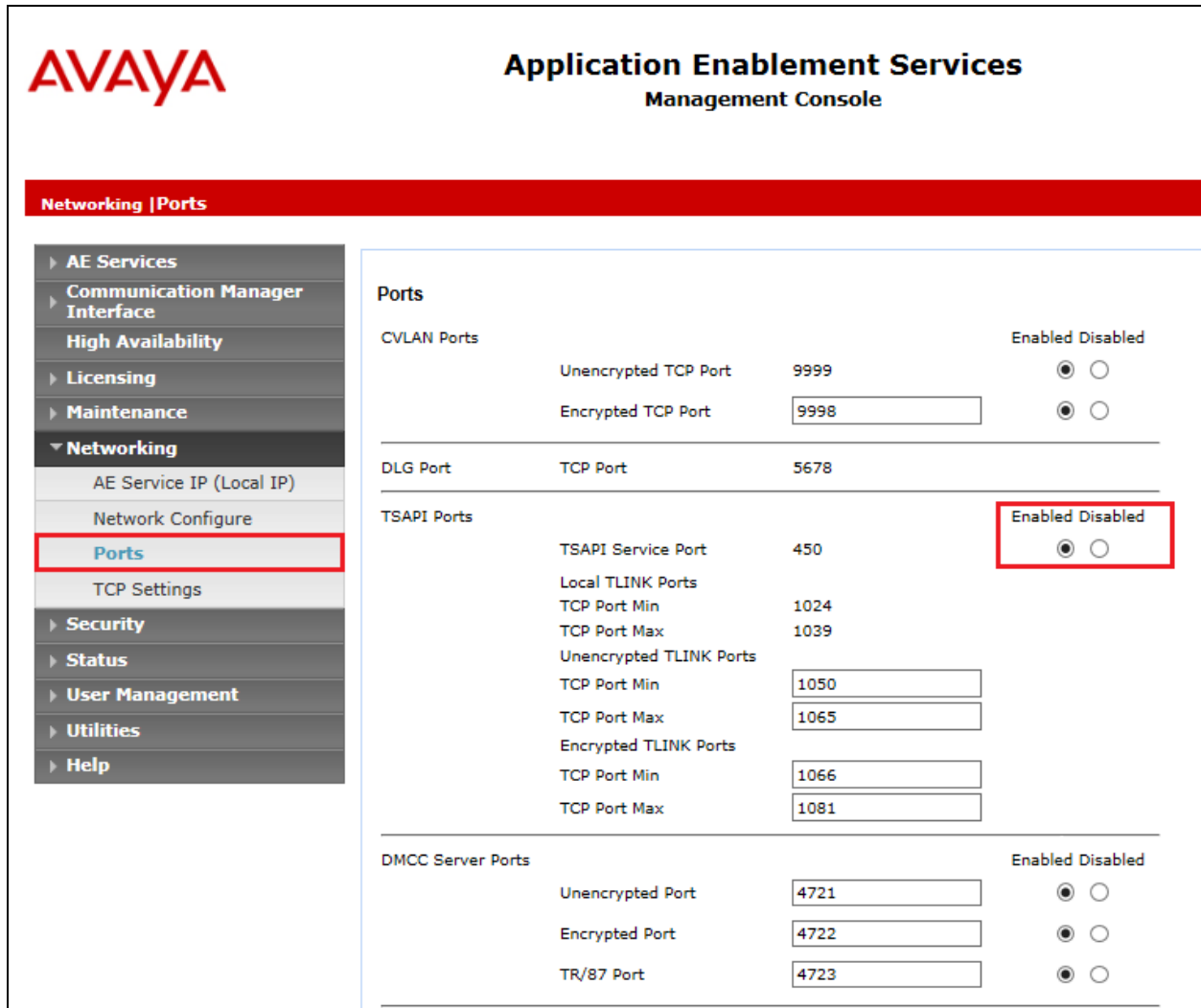
## 6.4. Identify Tlinks

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

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

## 6.5. 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.



**AVAYA** Application Enablement Services Management Console

**Networking | Ports**

**Ports**

CVLAN Ports

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

DLG Port

TCP Port	5678	

TSAPI Ports

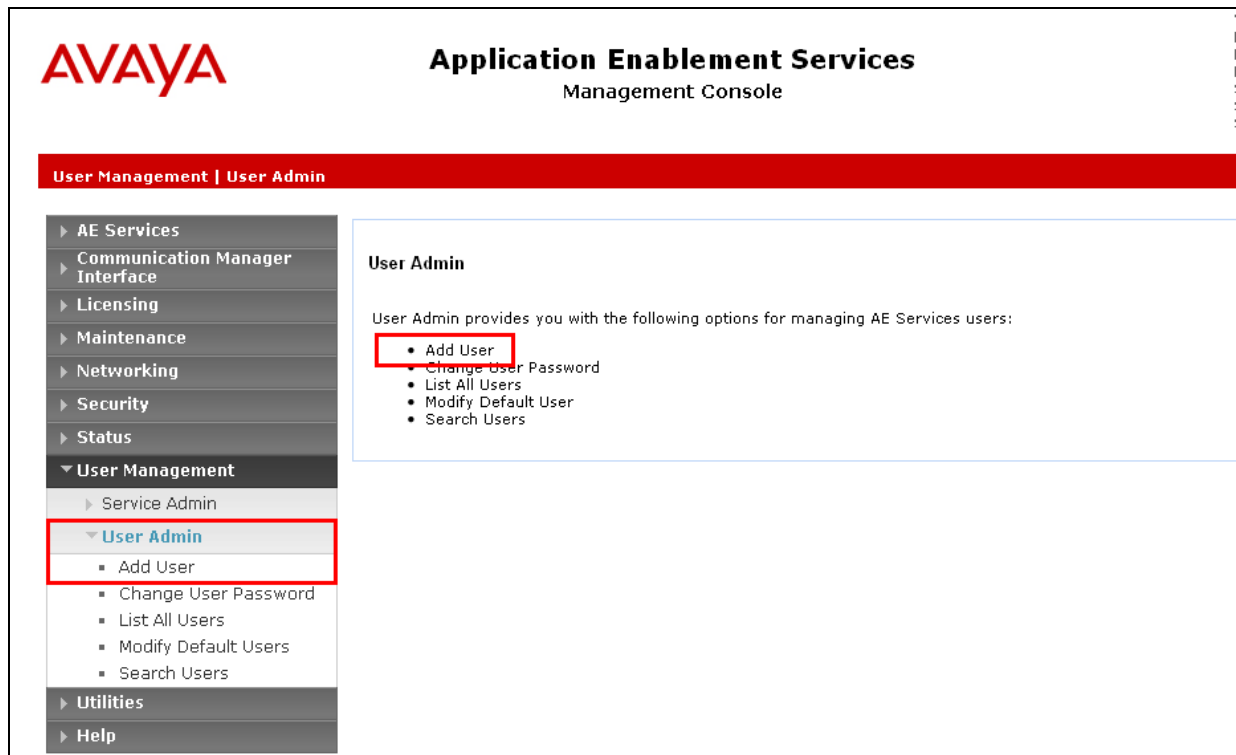
			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK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

DMCC Server Ports

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

## 6.6. Create CTI User

A User ID and password needs to be configured for the NICE Engage Platform to communicate with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the NICE Engage Platform setup in **Section 7.1**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with NICE Engage Platform setup in **Section 7.1**.
- **CT User** - Select **Yes** from the drop-down menu.

**AVAYA** **Application Enablement Services**  
Management Console

User Management | User Admin | Add User

**Add User**

Fields marked with \* can not be empty.

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

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

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

## 6.7. Associate Devices with CTI User

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

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

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

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

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

The screenshot shows the 'Edit CTI User' page for the 'nice' user. The 'Unrestricted Access' checkbox is checked and highlighted with a red box. The 'Apply Changes' button is also highlighted with a red box.

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

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

## 6.8. 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**.
- **SMS Logging** — Use the default setting **NORMAL** unless debugging.
- **SMS Log Destination** — Use the default **apache**, unless debugging.
- **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**.
- **Proxy Shutdown Timer** — Use the default **1800** seconds.
- **SAT Login Keepalive** — Use the default **180** seconds.
- **CM Terminal Type** — Use the default **OSSIZ**.
- **Proxy Log Destination** — Use the default destination **/var/log/avaya/aes/ossicm.log** for the CM Proxy Trace logs on the AE Server.

**AE Services**

- CVLAN
- DLG
- DMCC
- SMS**
  - SMS Properties**
  - TSAPI
  - TWS
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security

**SMS Properties**

Default CM Host Address: 10.10.40.31

Default CM Admin Port: 5022

CM Connection Protocol: SSH

SMS Logging: NORMAL

SMS Log Destination: apache

CM Proxy Trace Logging: NONE

Max Sessions per CM: 5

Proxy Shutdown Timer: 1800 seconds

SAT Login Keepalive: 180 seconds

CM Terminal Type: OSSIZ

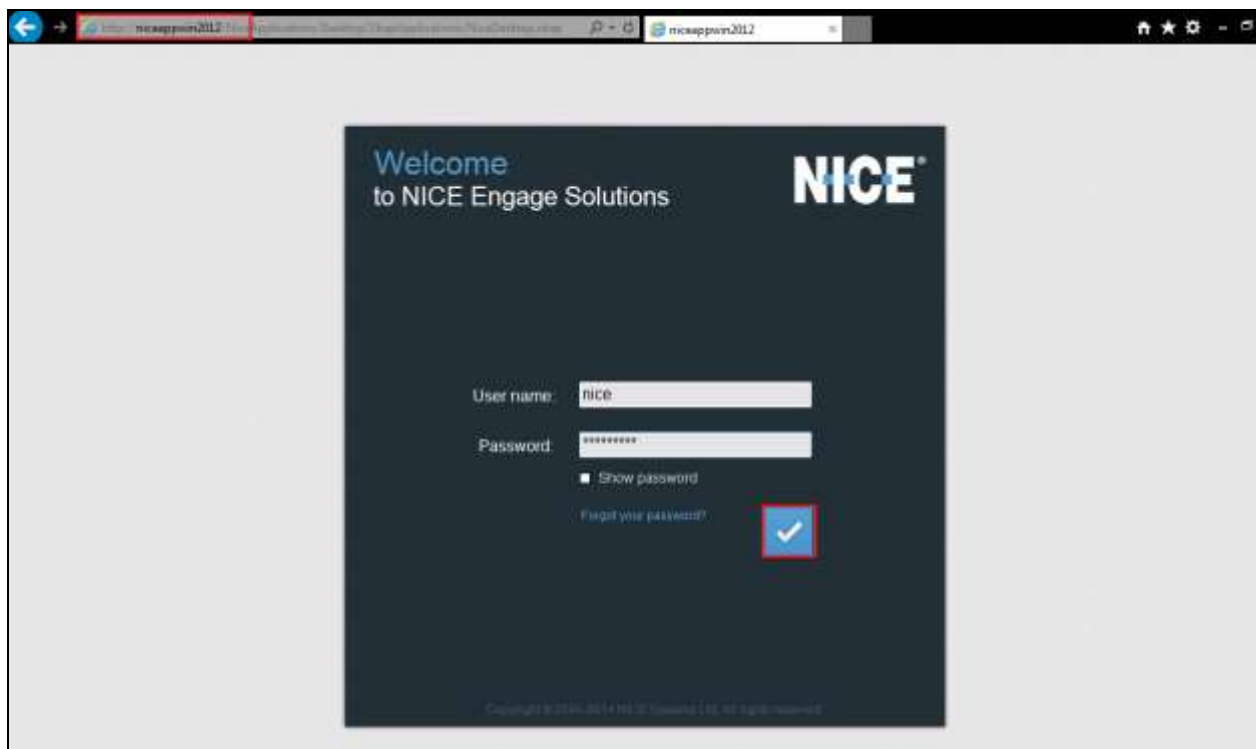
Proxy Log Destination: /var/log/avaya/aes/ossicm.log

Apply Changes Restore Defaults Cancel

## 7. Configure NICE Engage Platform

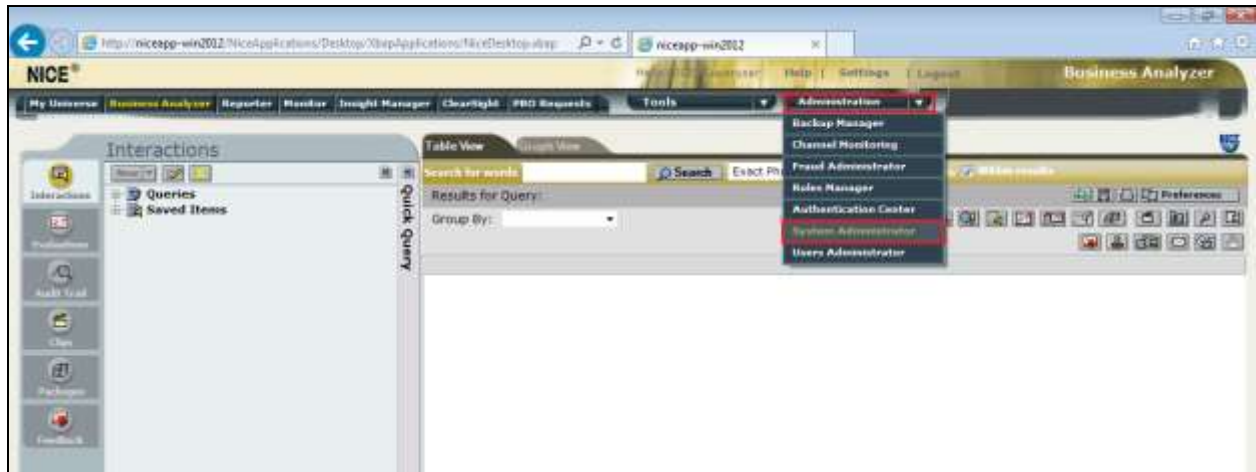
The installation of NICE Engage Platform is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of the NICE Engage Platform contact NICE as per the information provided in **Section 2.3**.

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**.

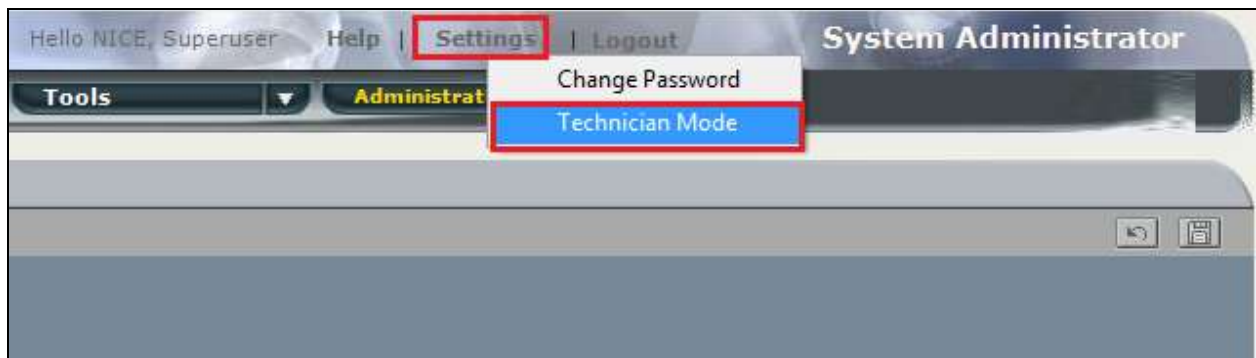




Once logged in expand the **Administration** dropdown menu and click on **System Administrator** as highlighted.



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

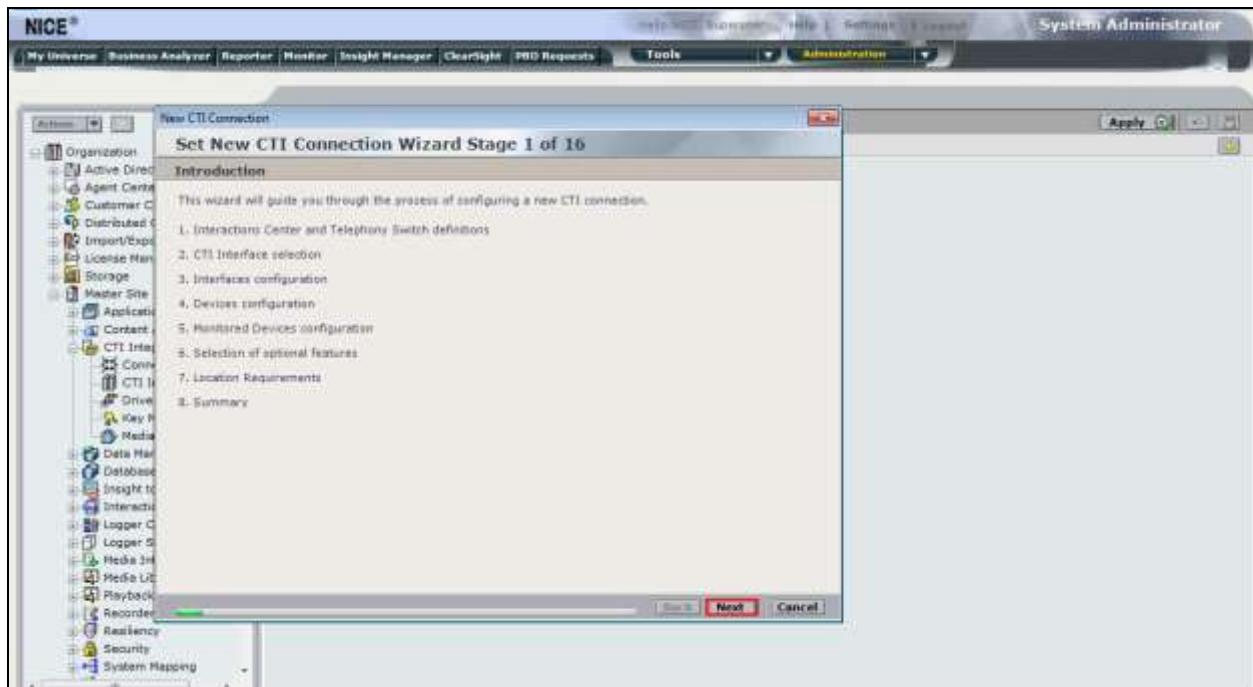


## 7.1. New CTI Connection

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



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

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

New CTI Connection

Set New CTI Connection Wizard Stage 2 of 16

Interactions Center Switch

Attach CTI to Interactions Center Server:

- ☒ Regular Interactions Center: IC
- ☐ Interactions Center Cluster:
- ☐ Use existing Telephony Switch: Avaya CM
- ☒ Define new Telephony Switch:

Switch Type: Avaya CM

Switch Name: Avaya CM Passive

Advanced >>

Back Next Cancel

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

New CTI Connection

Set New CTI Connection Wizard Stage 3 of 16

Interface Type

CTI Interface Type

Avaya CM CTI Interface: AES TSAPI

Avaya Communication Manager  
Avaya Application Enablement Services (AES) / Avaya CT - TSAPI

☒ VoIP Mapping: AES SMS

Avaya Communication Manager  
IP address mapping (AES SMS)

☐ Additional VoIP Mapping: Generic SIP Mapper

☐ Active Recording: DMCC (Advanced Interaction Recorder)

Back Next Cancel

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
<b>ServerName</b>	
<b>LoginID</b>	
<b>Password</b>	
<b>UseWarmStandBy</b>	No

Description: Server connection name.

Additional Interface Parameters

Back Next Cancel

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

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 16

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
<b>ServerName</b>	
<b>LoginID</b>	
<b>Password</b>	
<b>UseWarmStandBy</b>	No

Description: Server connection name.

Additional Interface Parameters

Back Next Cancel

Set Parameter Value

Interface Connection Parameter

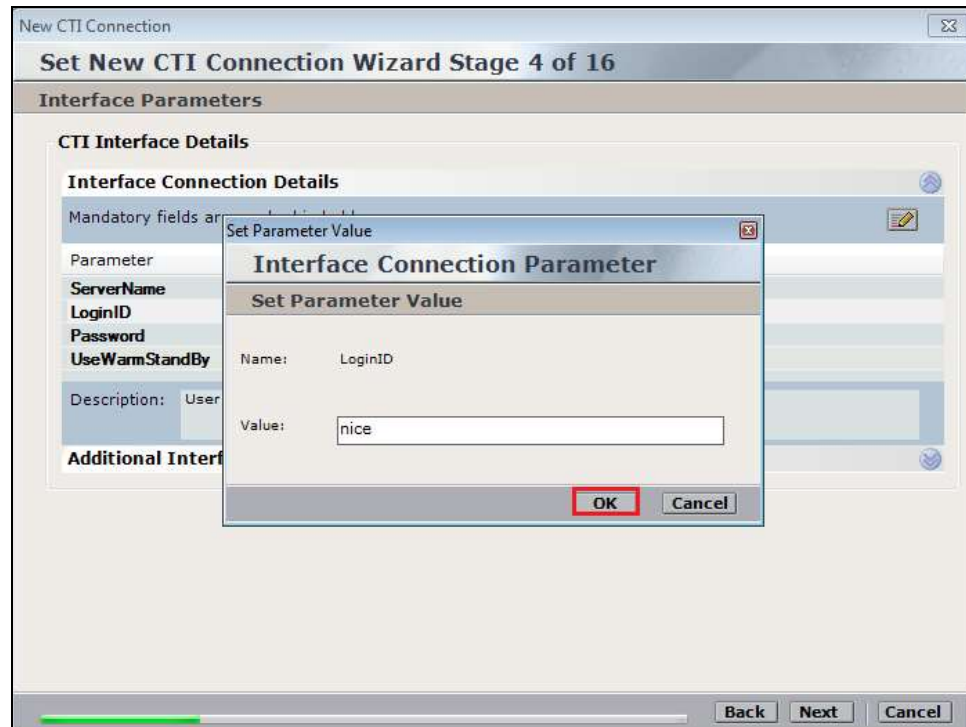
Set Parameter Value

Name: ServerName

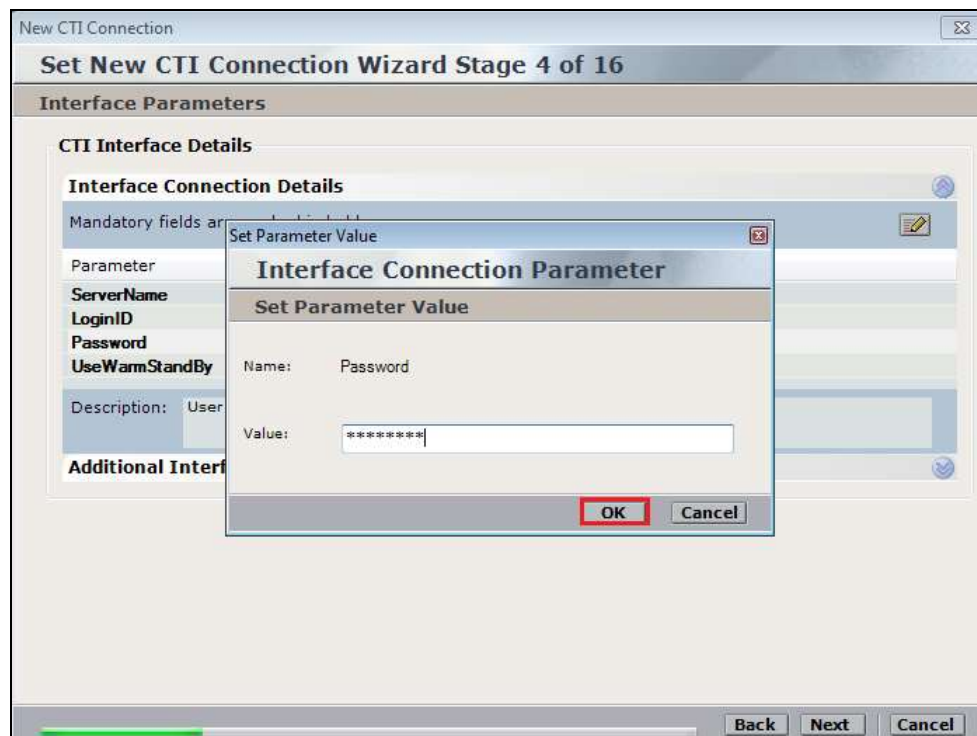
Value: AVAYA#CM70VMPG#CSTA#AES70VMPG

OK Cancel

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



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



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

The screenshot shows the 'Set New CTI Connection Wizard Stage 4 of 16' window. The 'Interface Parameters' section is active, displaying 'CTI Interface Details'. A table lists parameters with their values, where mandatory fields are in bold. The 'UseWarmStandBy' parameter is highlighted in blue. The 'Next' button at the bottom is also highlighted in blue.

Parameter	Value
<b>ServerName</b>	AVAYA#CM70VMPG#CSTA#AES70VMPG
<b>LoginID</b>	nice
<b>Password</b>	*****
<b>UseWarmStandBy</b>	No

Description: Is warm standby supported?

Additional Interface Parameters

Back Next Cancel

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

The screenshot shows the 'Set New CTI Connection Wizard Stage 5 of 16' window. The 'VoIP Mapping' section is active, displaying 'VoIP Mapping Interface Details'. A table lists parameters with their values, where mandatory fields are in bold. The 'AESVersion' parameter is highlighted in blue. The 'Next' button at the bottom is also highlighted in blue.

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

Description: AES Version.

Additional Interface Parameters

Back Next Cancel



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

New CTI Connection

**Set New CTI Connection Wizard Stage 5 of 16**

VoIP Mapping

**VoIP Mapping Interface Details**

**Interface Connection Details**

Mandatory fields are marked in bold

Parameter

**AESVersion**

**SmsHostIpAddress**

**SmsSessionMode**

SmsRequestTimeoutInSec 30

Description: AES Version.

**Additional Interface Parameters**

**Interface Connection Parameter**

**Set Parameter Value**

Name: AESVersion

Value: 4.1 and Above

OK Cancel

Back Next Cancel

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

New CTI Connection

**Set New CTI Connection Wizard Stage 5 of 16**

VoIP Mapping

**VoIP Mapping Interface Details**

**Interface Connection Details**

Mandatory fields are marked in bold

Parameter

**AESVersion**

**SmsHostIpAddress**

**SmsSessionMode**

SmsRequestTimeoutInSec 30

Description: The IP of the Avaya AES server.

**Additional Interface Parameters**

**Interface Connection Parameter**

**Set Parameter Value**

Name: PrimaryAESServerAddress

Value: 10.10.40.16

OK Cancel

Back Next Cancel

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

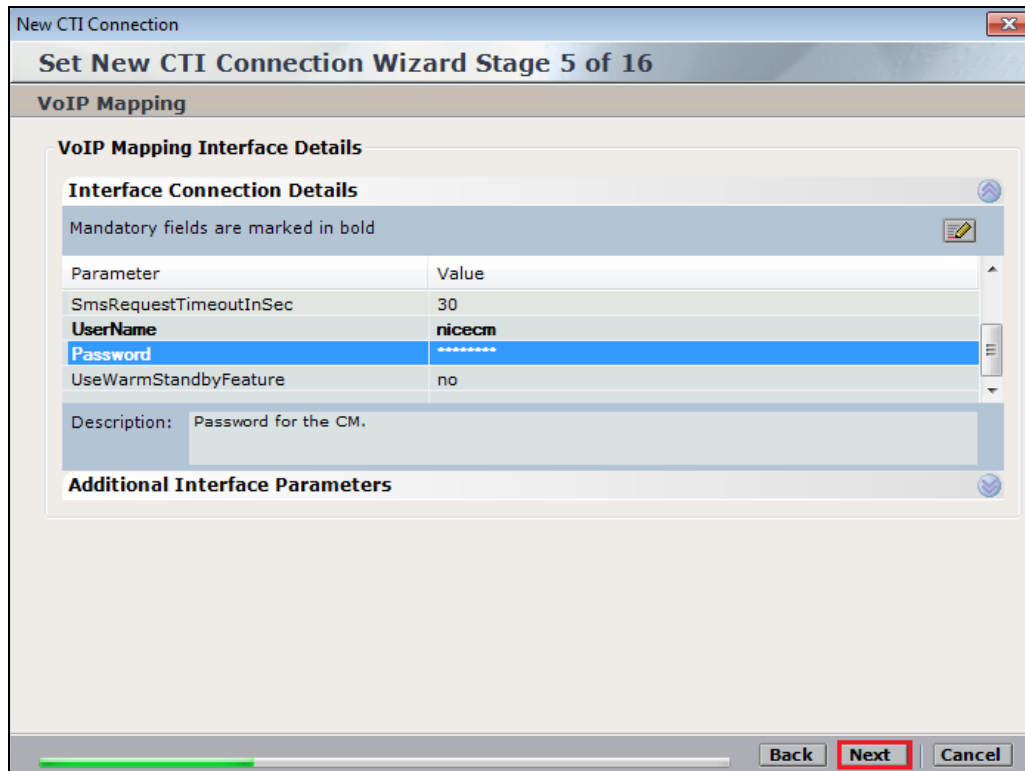
The image shows two overlapping windows from a software application. The background window is titled 'New CTI Connection' and contains a 'Set New CTI Connection Wizard'. It has a 'VoIP Mapping' tab selected. Under 'Interface Connection Details', a list of parameters is shown, with 'UserName' highlighted by a red rectangle. The foreground window is titled 'Set Parameter Value' and 'Interface Connection Parameter'. It has a 'Set Parameter Value' tab. The 'Name' field is labeled 'Username' and the 'Value' field contains the text 'nicecm'. Both the 'OK' and 'Cancel' buttons in the foreground window are highlighted with red rectangles.

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

The image shows the same two overlapping windows as the previous screenshot. In the background 'Set New CTI Connection Wizard' window, the 'Password' parameter is now highlighted with a red rectangle. In the foreground 'Set Parameter Value' window, the 'Name' field is labeled 'Password' and the 'Value' field contains masked characters (seven asterisks). The 'OK' button in the foreground window is highlighted with a red rectangle.



Click on **Next** to continue.

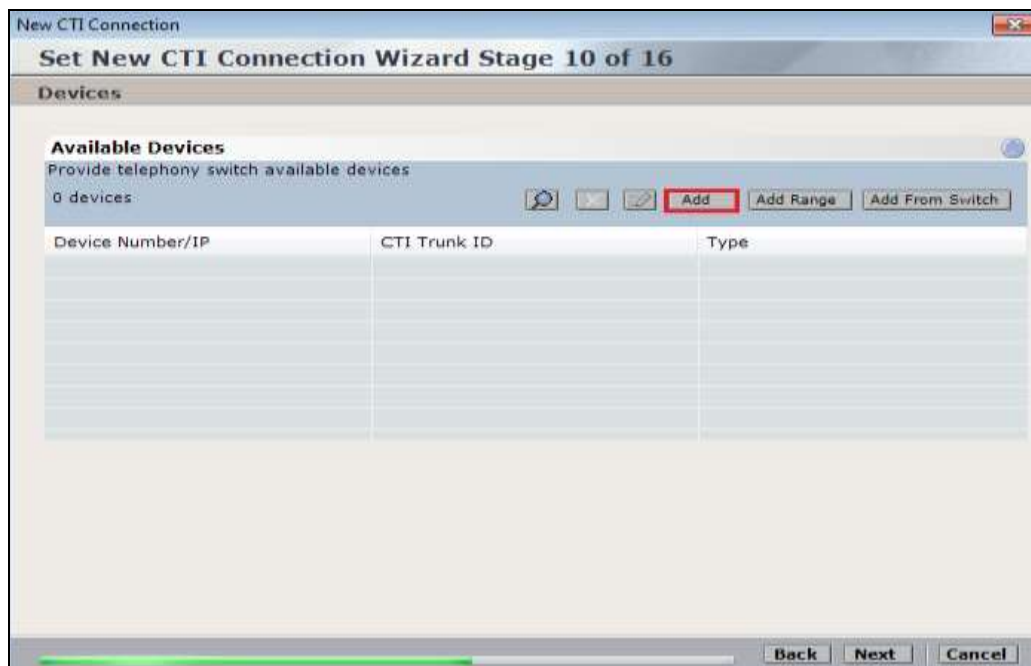


The screenshot shows the 'Set New CTI Connection Wizard Stage 5 of 16' window. The title bar says 'New CTI Connection'. The main heading is 'Set New CTI Connection Wizard Stage 5 of 16'. Below it is the 'VoIP Mapping' section. The 'VoIP Mapping Interface Details' section is expanded, showing 'Interface Connection Details'. A note states 'Mandatory fields are marked in bold'. A table lists parameters: 'SmsRequestTimeoutInSec' (30), 'UserName' (nicecm), 'Password' (masked with asterisks), and 'UseWarmStandbyFeature' (no). The 'Password' row is highlighted in blue. Below the table is a 'Description' field with the text 'Password for the CM.'. The 'Additional Interface Parameters' section is collapsed. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red box.

Parameter	Value
SmsRequestTimeoutInSec	30
<b>UserName</b>	<b>nicecm</b>
<b>Password</b>	*****
UseWarmStandbyFeature	no

Description: Password for the CM.

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



The screenshot shows the 'Set New CTI Connection Wizard Stage 10 of 16' window. The title bar says 'New CTI Connection'. The main heading is 'Set New CTI Connection Wizard Stage 10 of 16'. Below it is the 'Devices' section. The 'Available Devices' section is expanded, showing 'Provide telephony switch available devices'. It states '0 devices'. There are buttons for 'Add', 'Add Range', and 'Add From Switch'. The 'Add' button is highlighted with a red box. Below the buttons is a table with columns 'Device Number/IP', 'CTI Trunk ID', and 'Type'. The table is empty. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Device Number/IP	CTI Trunk ID	Type
------------------	--------------	------

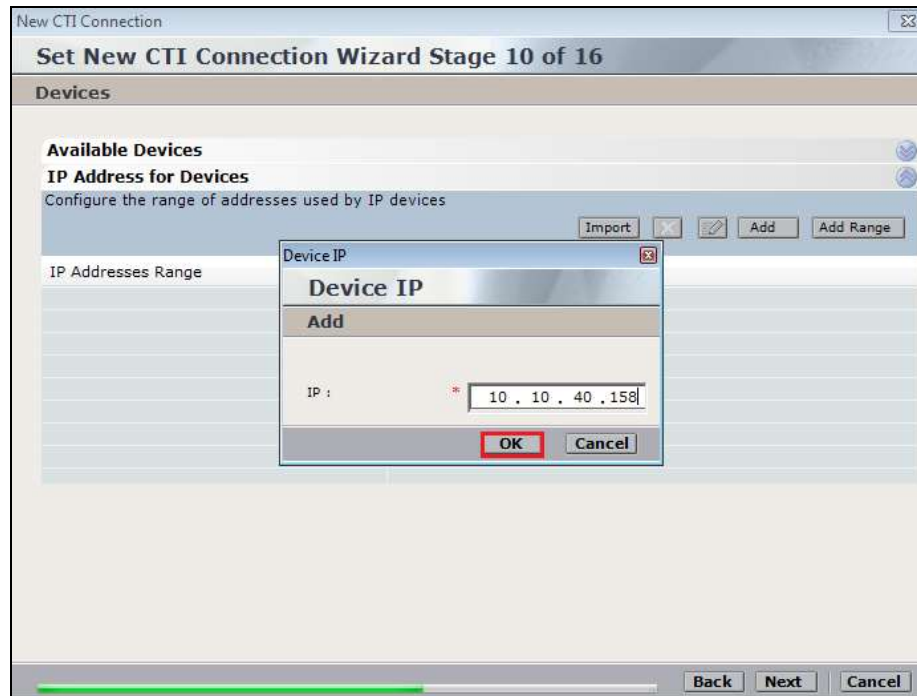
The **Device Type** should be **Extension** and insert the correct extension number. Also the IP Address of the extension must be added to IP. Click on **OK** to continue.

The screenshot shows the 'Add Device' dialog box within the 'Set New CTI Connection Wizard'. The dialog has a 'Name' field, a 'Device Type' dropdown menu set to 'Extension', a 'Device Number' field containing '2000', and an 'IP' field containing '10.10.40.158'. These four fields are grouped together and highlighted with a red rectangular border. Below this group is the 'Advanced Device Parameters' section, which includes a checkbox for 'Display Read Only Information' and a table with 'Name' and 'Value' columns. At the bottom of the dialog is a 'Description' text area and two buttons: 'OK' and 'Cancel'. The 'OK' button is also highlighted with a red rectangular border. In the background, the 'Available Devices' list in the wizard is visible, showing '0 devices'.

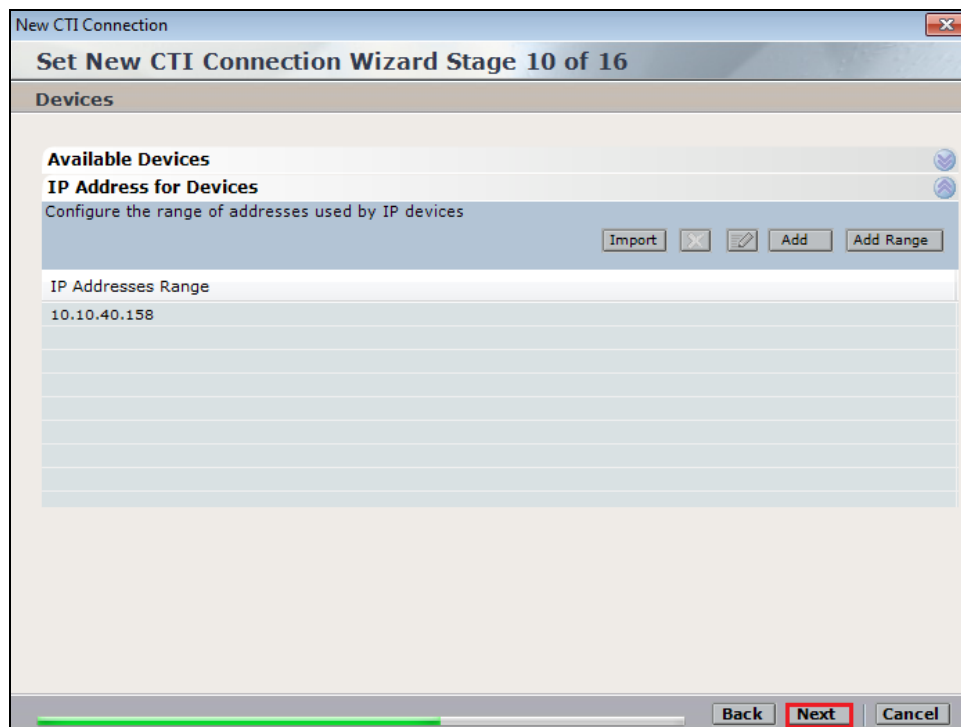
Click on **Add** to add the **IP Address** of the device. Note a range of devices can be added here also by clicking on **Add Range**.

The screenshot shows the 'IP Address for Devices' section of the 'Set New CTI Connection Wizard', specifically 'Stage 10 of 16'. The section is titled 'Available Devices' and 'IP Address for Devices'. Below the title is the instruction 'Configure the range of addresses used by IP devices'. There are three buttons: 'Import', 'Add', and 'Add Range'. The 'Add' button is highlighted with a red rectangular border. Below the buttons is a table with the header 'IP Addresses Range' and two empty columns. At the bottom of the wizard window are 'Back', 'Next', and 'Cancel' buttons.

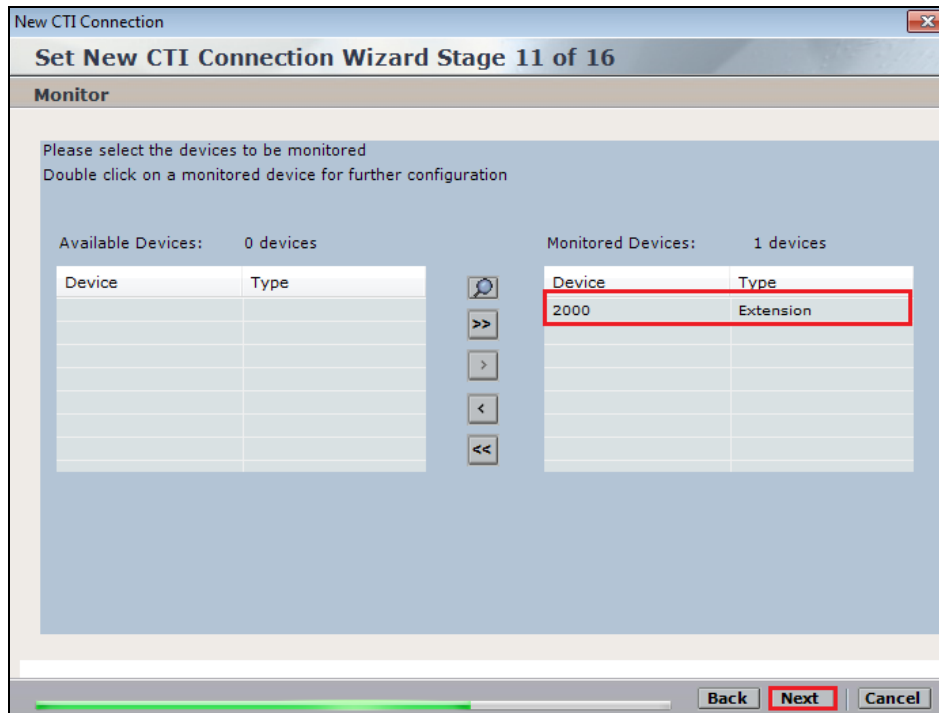
Enter the correct **IP** for the phone set extension.



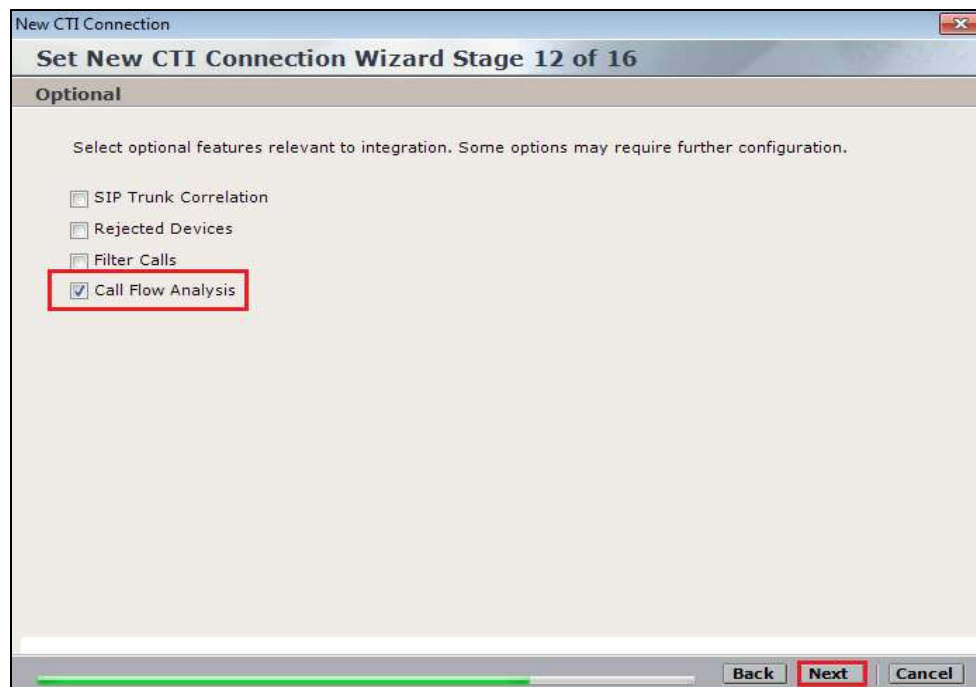
Enter the IP addresses for all devices that are to be recorded and click on **Next** to continue.



Select the new extension and click on the >> icon 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.

New CTI Connection

**Set New CTI Connection Wizard Stage 15 of 16**

**Requirements**

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

☒ Create a new Connection Manager

Port: 62095

☐ Select available Connection Manager

Ports in use:

62094

Back Next Cancel

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

New CTI Connection

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

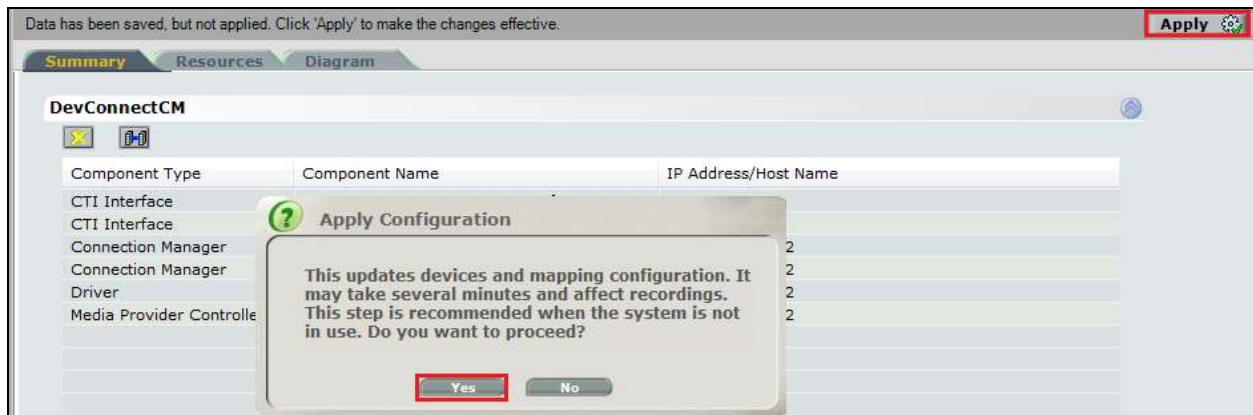
**Summary**

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

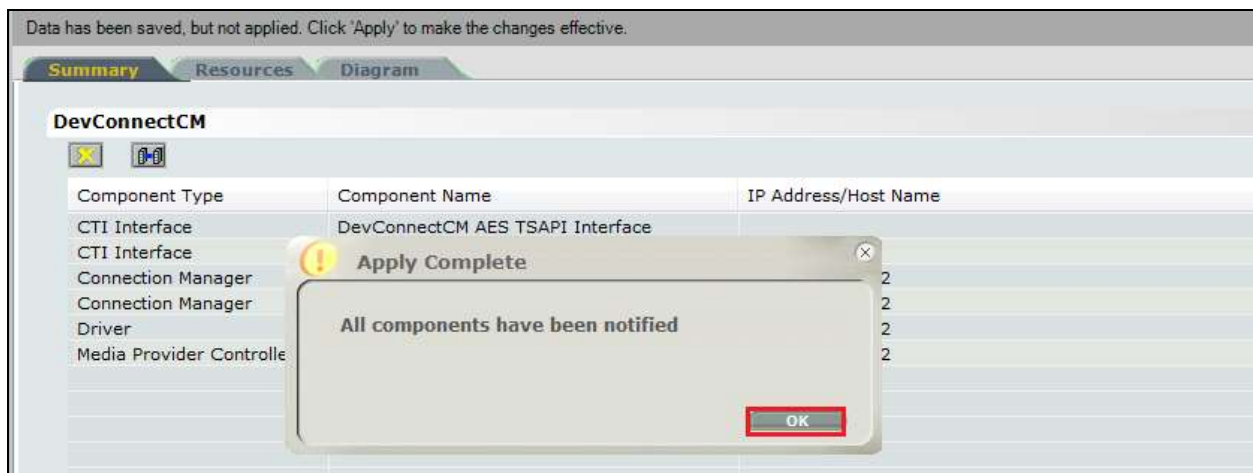
**DevConnectCM Connection**

Back Finish Cancel

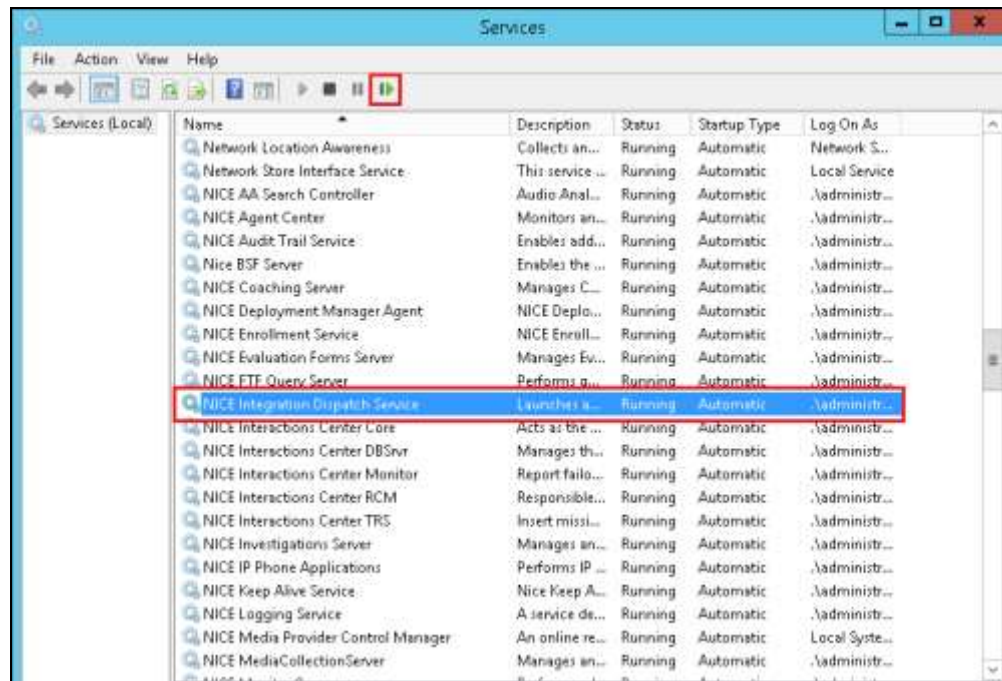
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed.



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

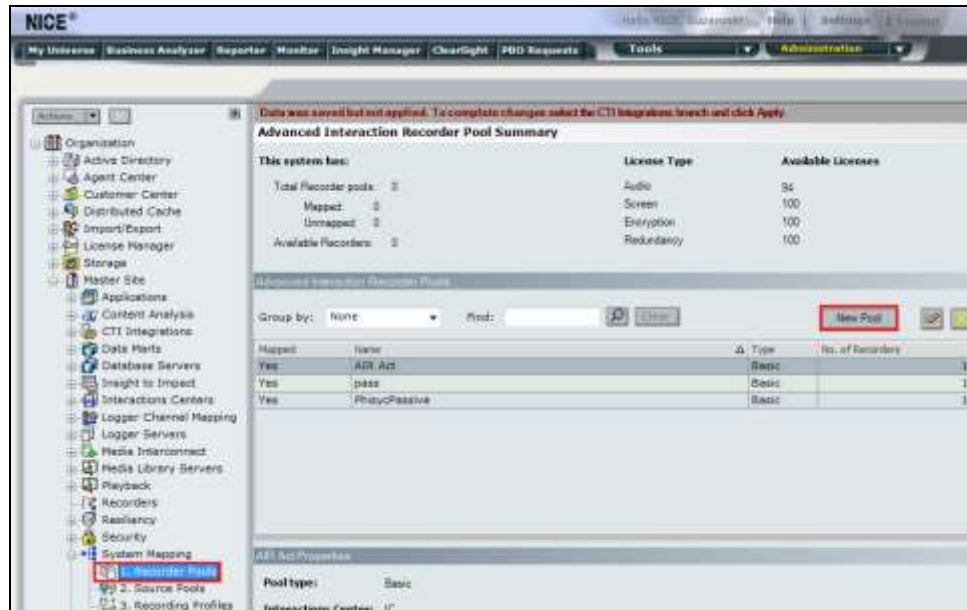


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

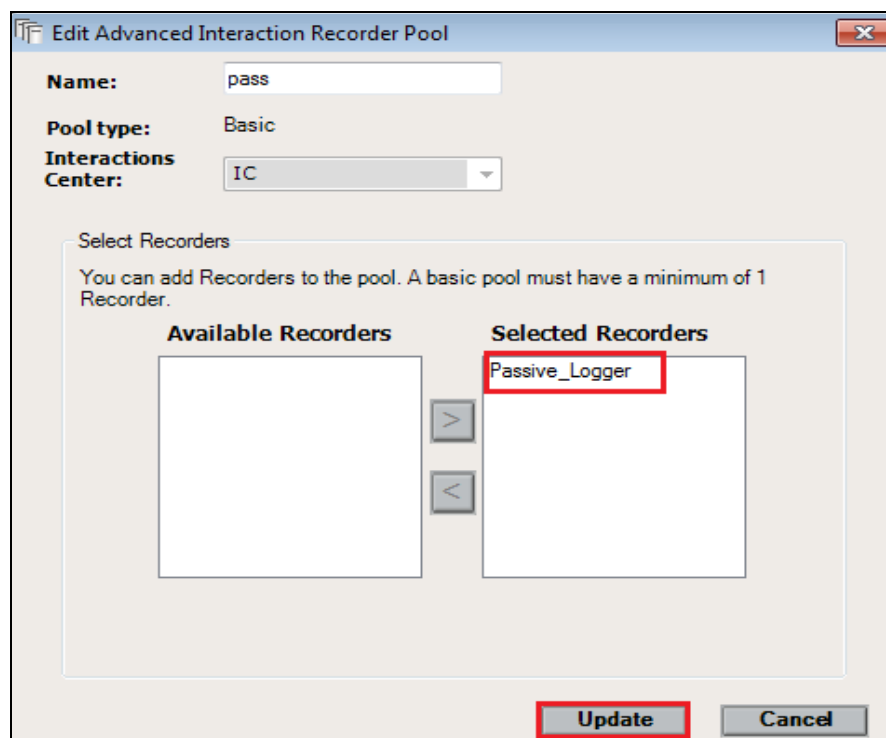


## 7.2. System Mapping

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

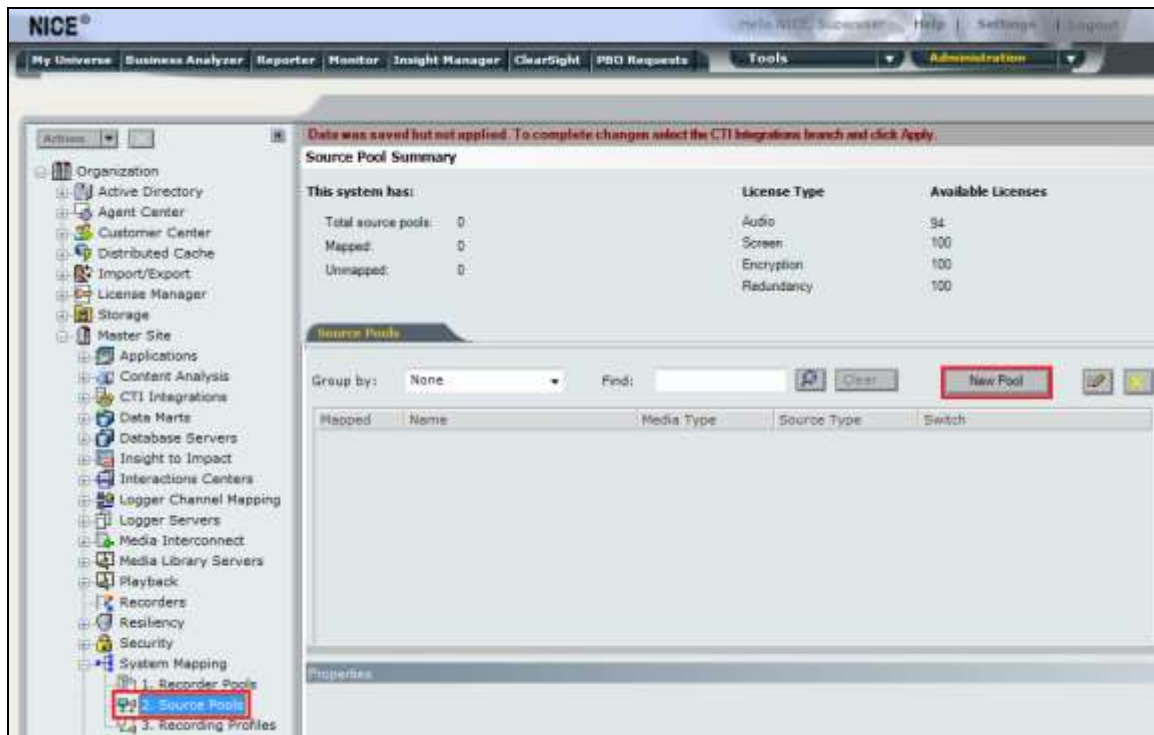


Enter a suitable **Name** for the **Recorder Pool** and select the **Passive\_Logger** from the list of **Available Recorders** and click on **Update** to continue.

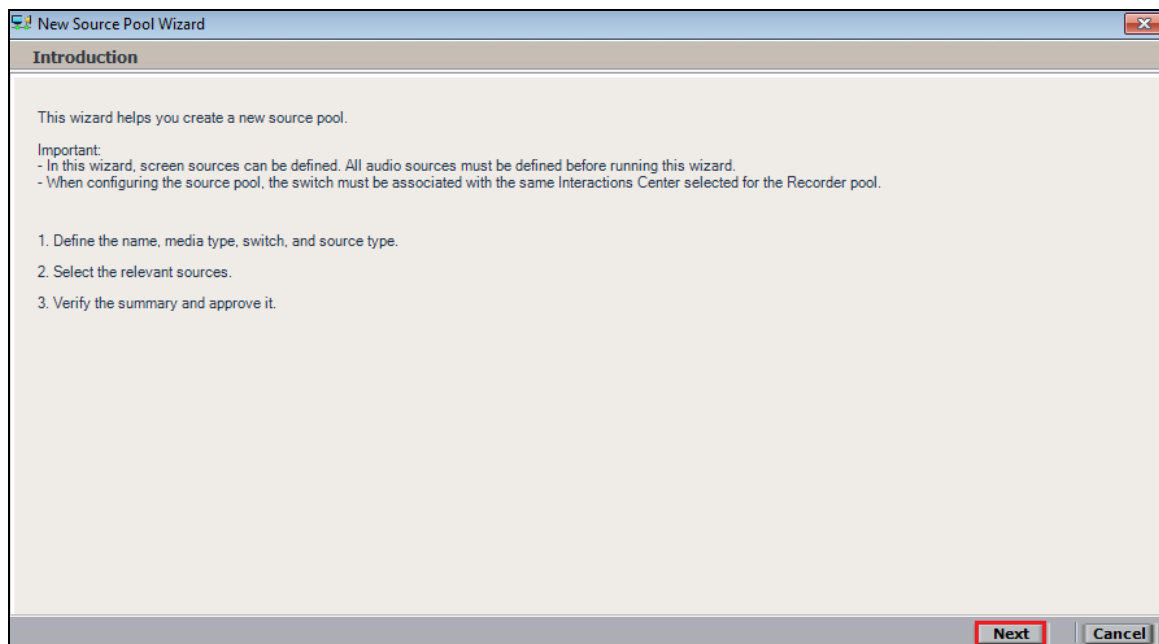




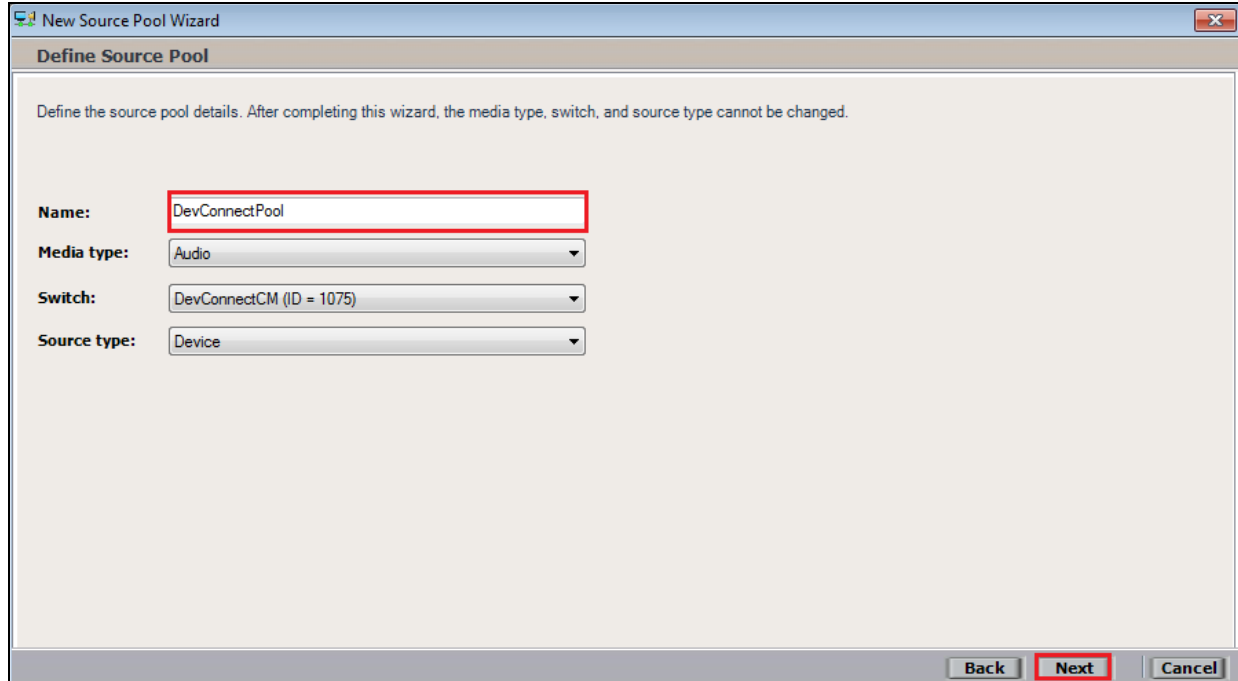
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



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



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



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

Name: DevConnectPool

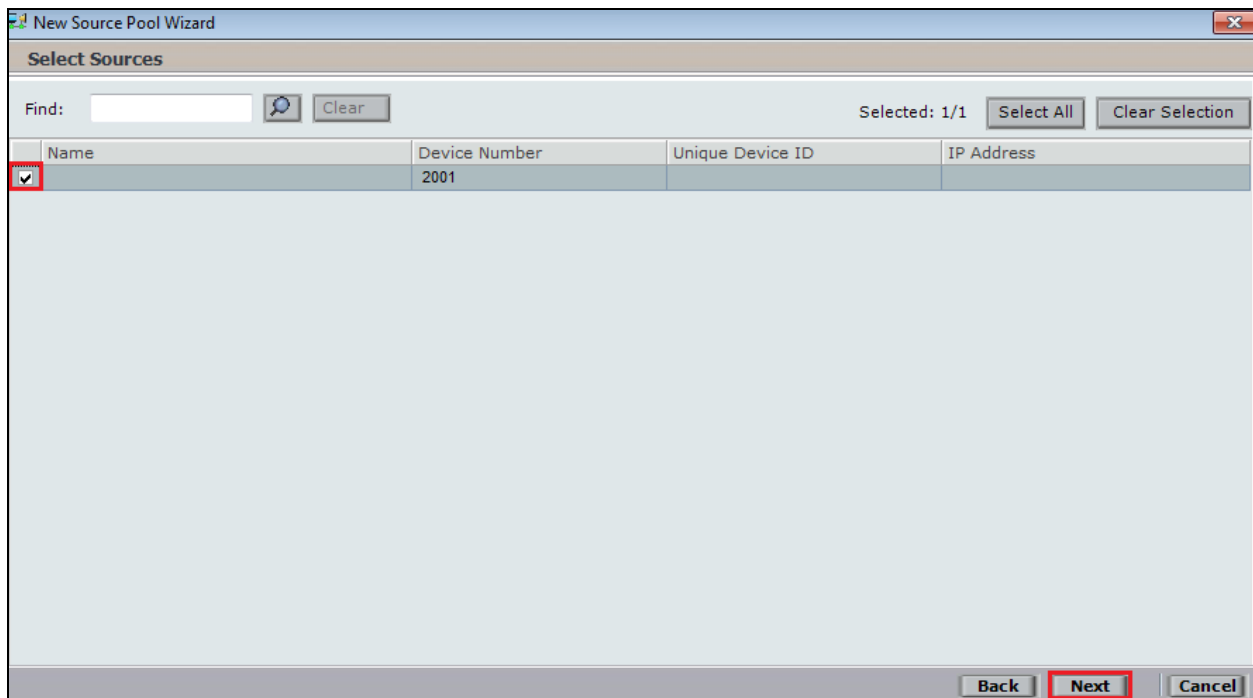
Media type: Audio

Switch: DevConnectCM (ID = 1075)

Source type: Device

Back Next Cancel

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



The screenshot shows the 'Select Sources' step of the 'New Source Pool Wizard'. The window title is 'New Source Pool Wizard'. The main heading is 'Select Sources'. There is a search bar with the text 'Find:' and a 'Clear' button. To the right of the search bar, it says 'Selected: 1/1' and there are 'Select All' and 'Clear Selection' buttons. Below this is a table with four columns: 'Name', 'Device Number', 'Unique Device ID', and 'IP Address'. The first row of the table has a checked checkbox in the 'Name' column, and the 'Device Number' is '2001'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red border.

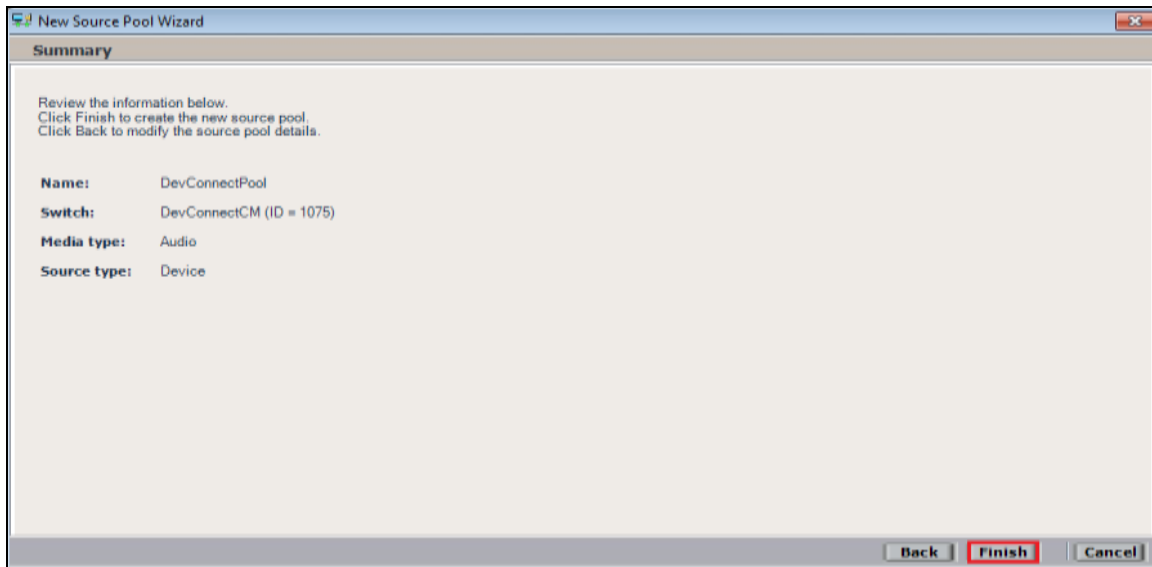
Find: [Search] Clear

Selected: 1/1 Select All Clear Selection

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

Back Next Cancel

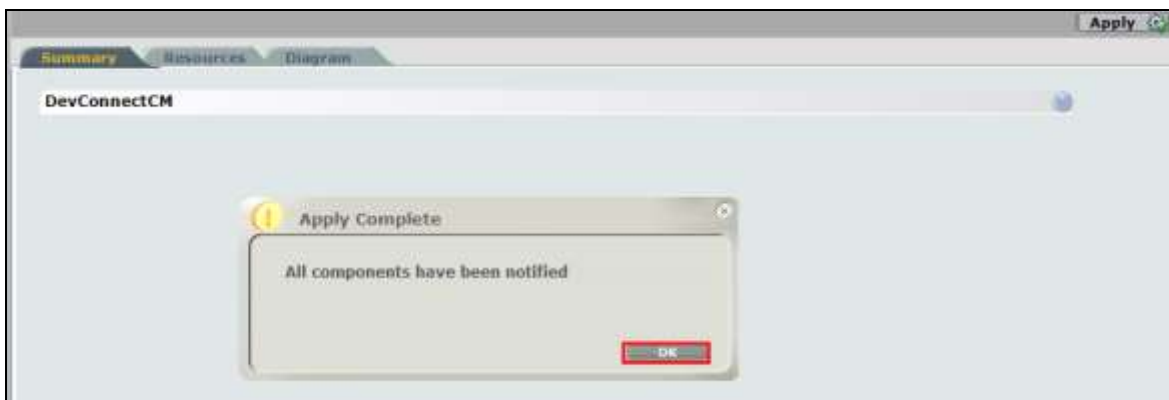
Click on **Finish** to complete the New Source Pool Wizard.



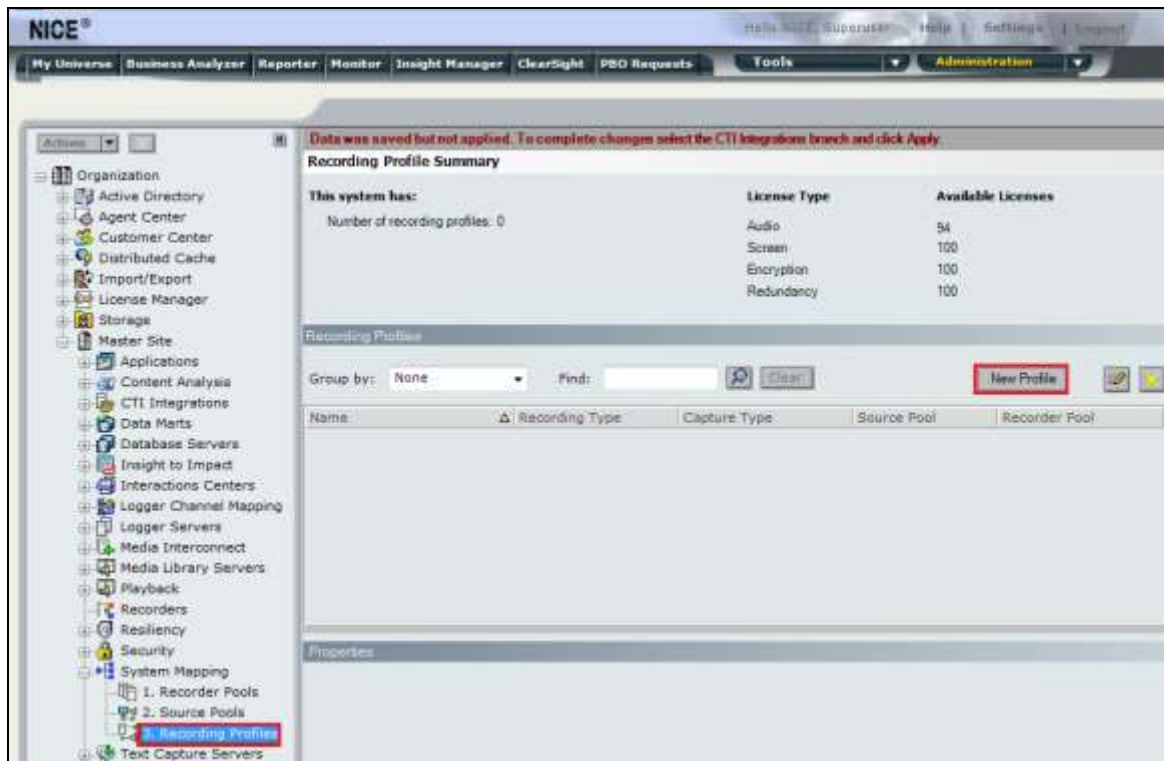
To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.



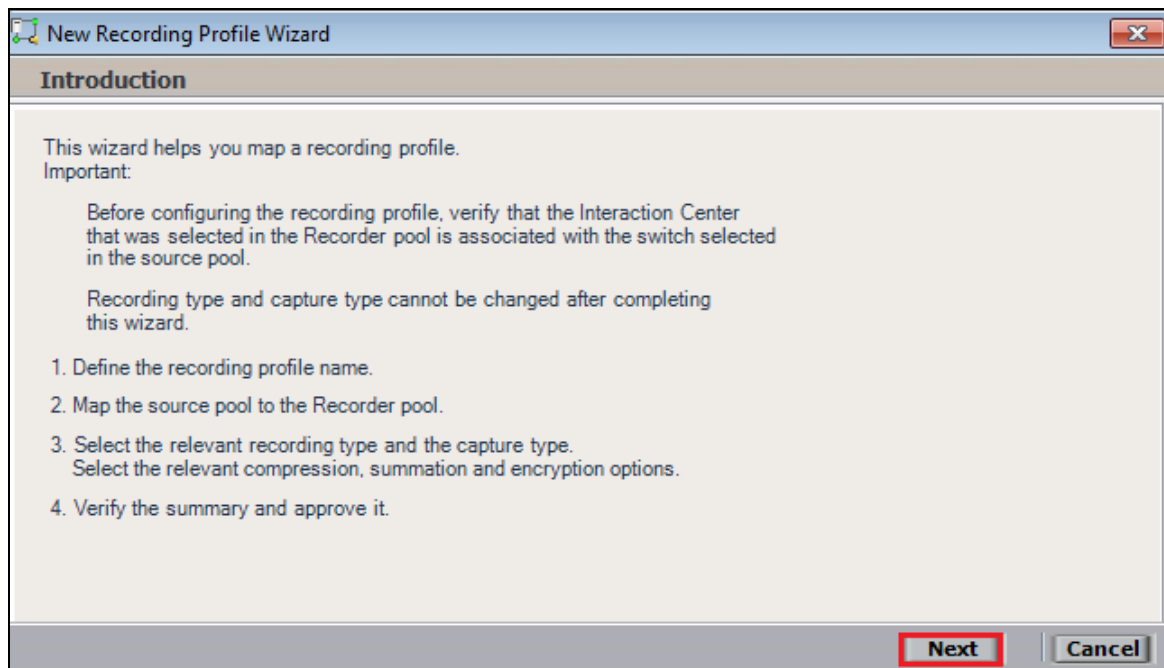
The following screen shows the changes were saved correctly. Click on **OK** to continue.



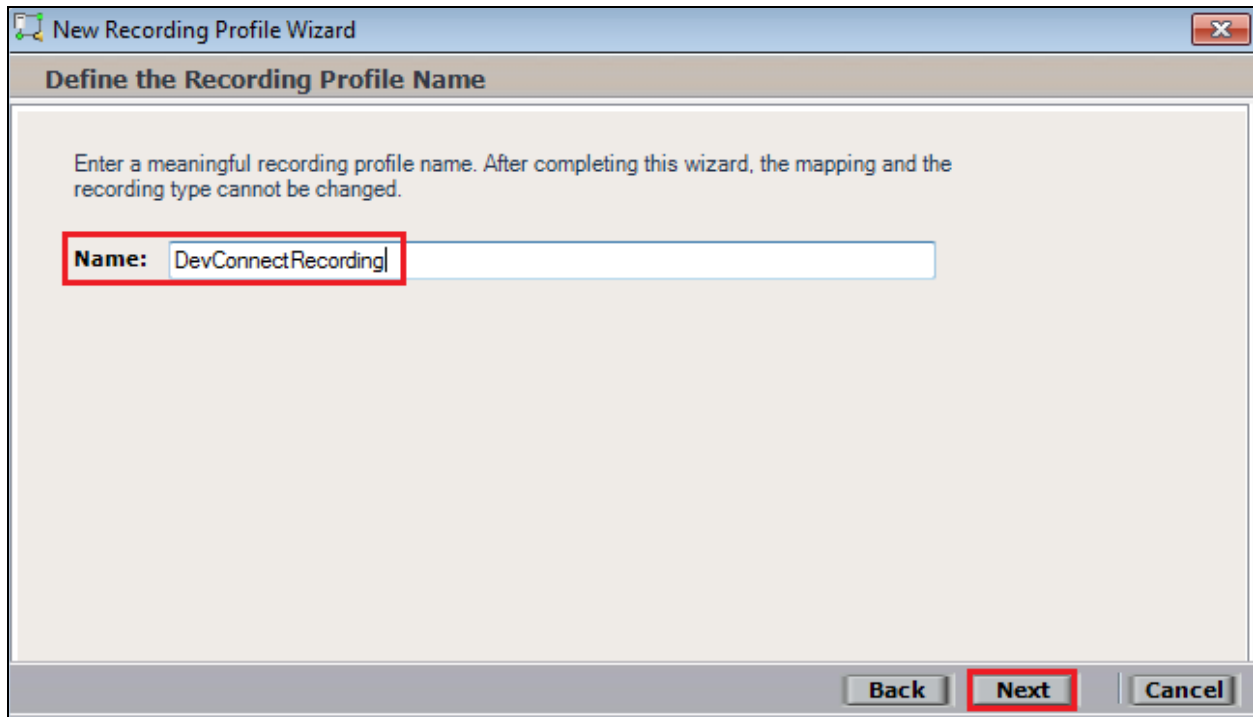
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



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

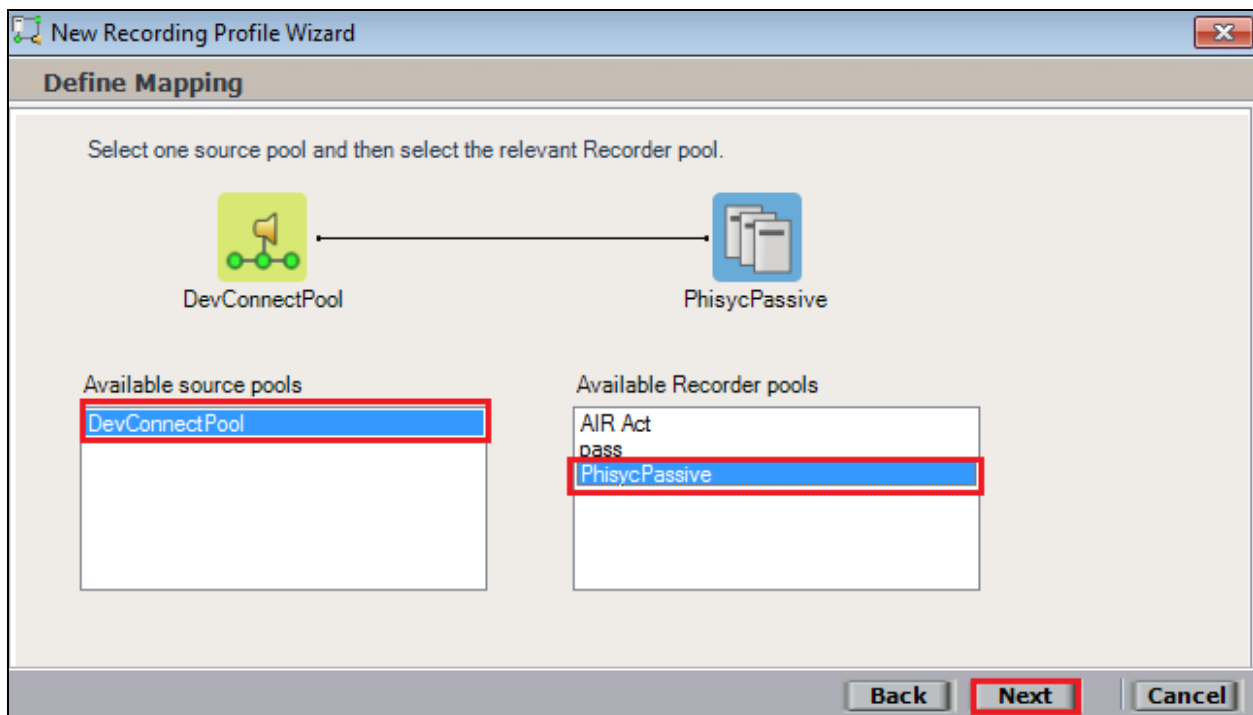


Enter a suitable **Name** for the Recording profile.



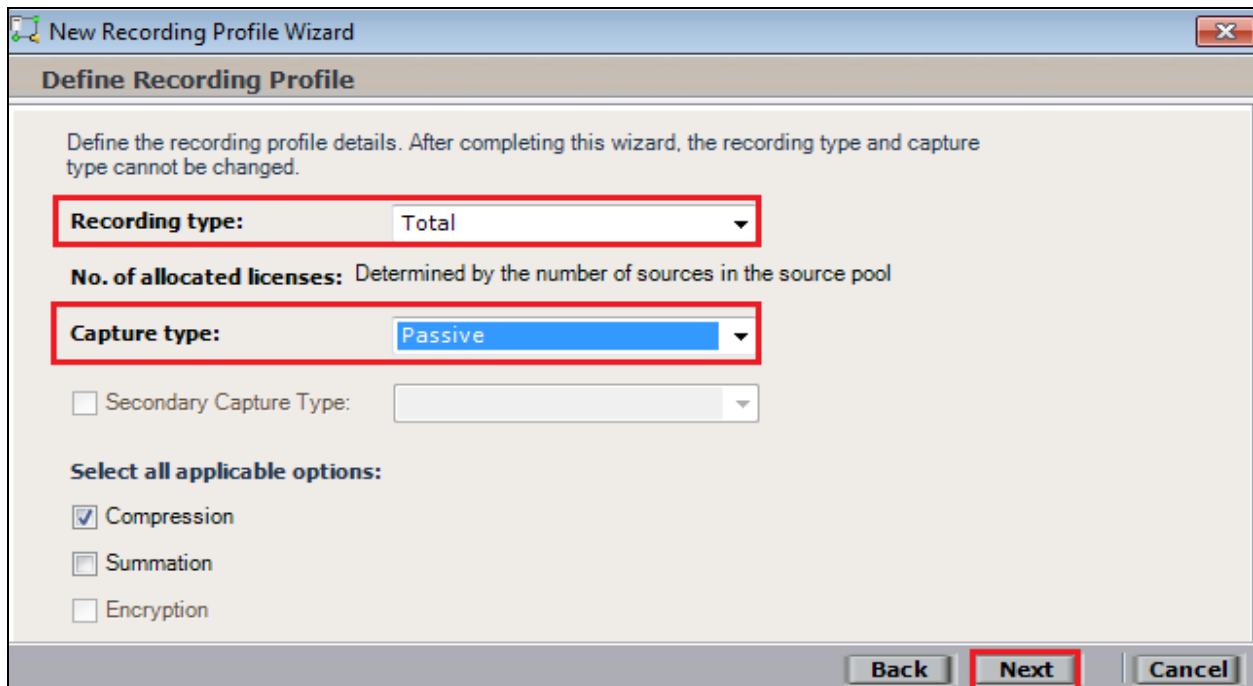
The screenshot shows the 'New Recording Profile Wizard' window with the title 'Define the Recording Profile Name'. The instruction text reads: 'Enter a meaningful recording profile name. After completing this wizard, the mapping and the recording type cannot be changed.' Below this, there is a text input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

Select the correct **source pool** and **Recorder pool**, 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**.



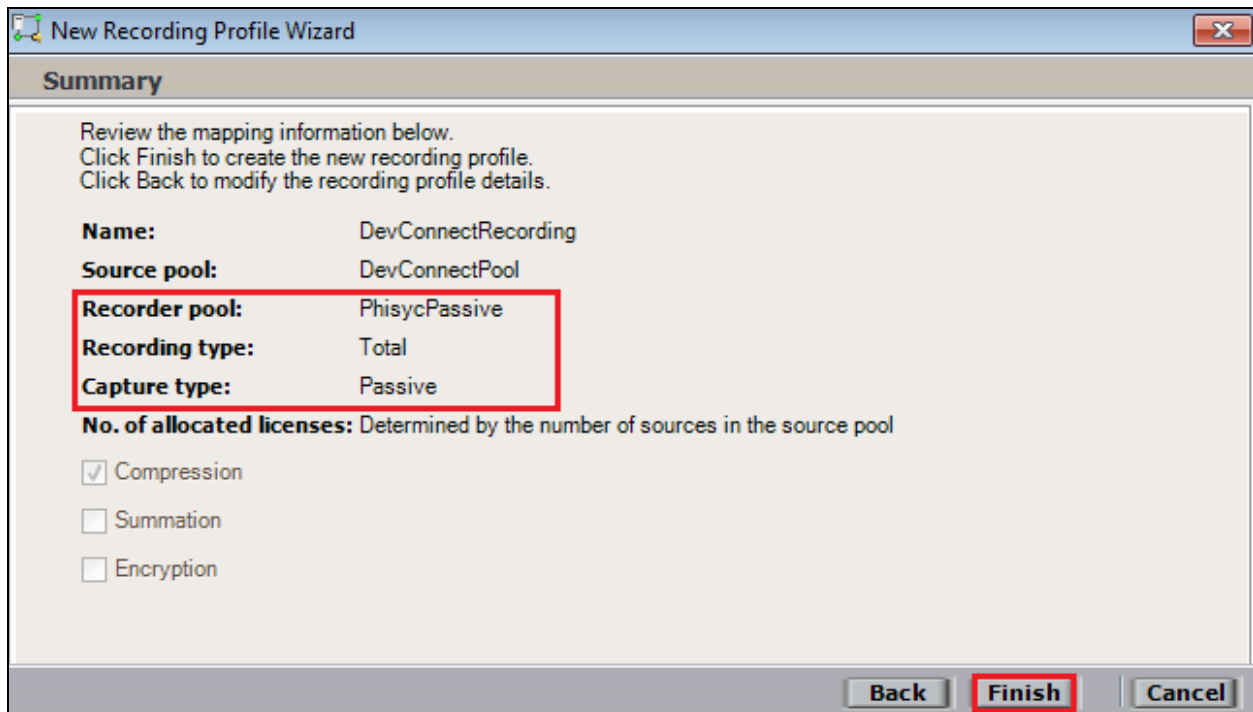
The screenshot shows the 'New Recording Profile Wizard' window with the title 'Define Mapping'. The instruction text reads: 'Select one source pool and then select the relevant Recorder pool.' Above the selection lists, there is a diagram showing a source pool icon (DevConnectPool) connected by a double-headed arrow to a recorder pool icon (PhisycPassive). Below the diagram, there are two list boxes. The 'Available source pools' list has 'DevConnectPool' selected and highlighted with a red box. The 'Available Recorder pools' list has 'AIR Act', 'pass', and 'PhisycPassive' listed, with 'PhisycPassive' selected and highlighted with a red box. The 'Next' button at the bottom right is highlighted with a red box.

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



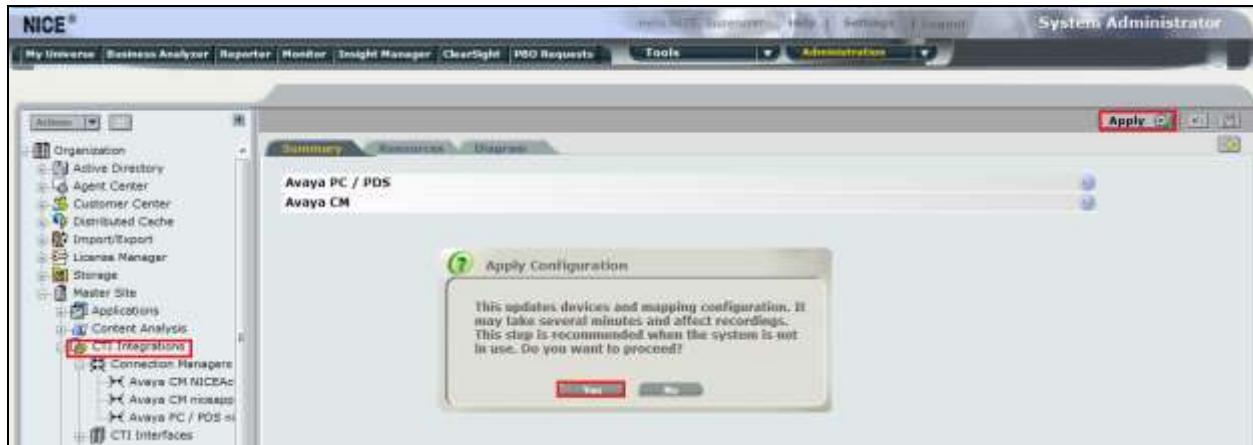
The screenshot shows the 'Define Recording Profile' step of the 'New Recording Profile Wizard'. The window title is 'New Recording Profile Wizard'. The main heading is 'Define Recording Profile'. Below the heading, there is a note: 'Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.' The 'Recording type' dropdown is set to 'Total' and is highlighted with a red box. Below it, the text 'No. of allocated licenses: Determined by the number of sources in the source pool' is displayed. The 'Capture type' dropdown is set to 'Passive' and is also highlighted with a red box. Below this, there is a checkbox for 'Secondary Capture Type' which is unchecked. Under the heading 'Select all applicable options:', there are three checkboxes: 'Compression' (checked), 'Summation' (unchecked), and 'Encryption' (unchecked). At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red box), and 'Cancel'.

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



The screenshot shows the 'Summary' step of the 'New Recording Profile Wizard'. The window title is 'New Recording Profile Wizard'. The main heading is 'Summary'. Below the heading, there is a note: 'Review the mapping information below. Click Finish to create the new recording profile. Click Back to modify the recording profile details.' The summary table shows the following information: Name: DevConnectRecording, Source pool: DevConnectPool, Recorder pool: PhisycPassive (highlighted with a red box), Recording type: Total (highlighted with a red box), and Capture type: Passive (highlighted with a red box). Below the table, the text 'No. of allocated licenses: Determined by the number of sources in the source pool' is displayed. Under the heading 'Select all applicable options:', there are three checkboxes: 'Compression' (checked), 'Summation' (unchecked), and 'Encryption' (unchecked). At the bottom right, there are three buttons: 'Back', 'Finish' (highlighted with a red box), and 'Cancel'.

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



This concludes the setup of the NICE Application Server for 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 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 aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	aes70vmpg	established	18	18

### 8.2. Verify TSAPI Link

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

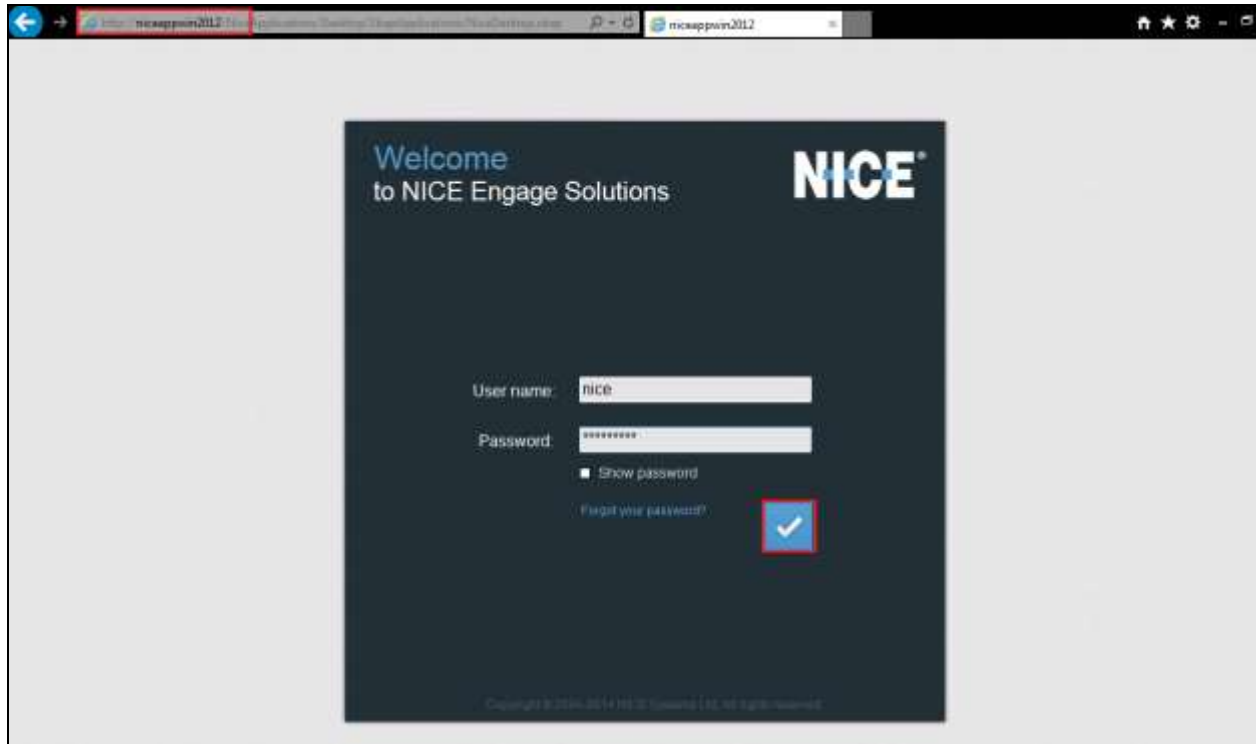
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The 'Status' section is expanded, showing 'Status and Control' and 'TSAPI Service Summary'. The main area displays the 'TSAPI Link Details' screen, which includes a table with columns for Link, Switch Name, Switch CTI Link ID, Status, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period. The table shows a single entry with Link ID 1, Switch Name cm70vmpg, Switch CTI Link ID 1, Status Talking, and State Online. Below the table, there are buttons for 'Online' and 'Offline', and a section for 'For service-side information, choose one of the following:' with buttons for 'TSAPI Service Status', 'Link Status', and 'User Status'.



### 8.3. Verify calls are being recorded

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

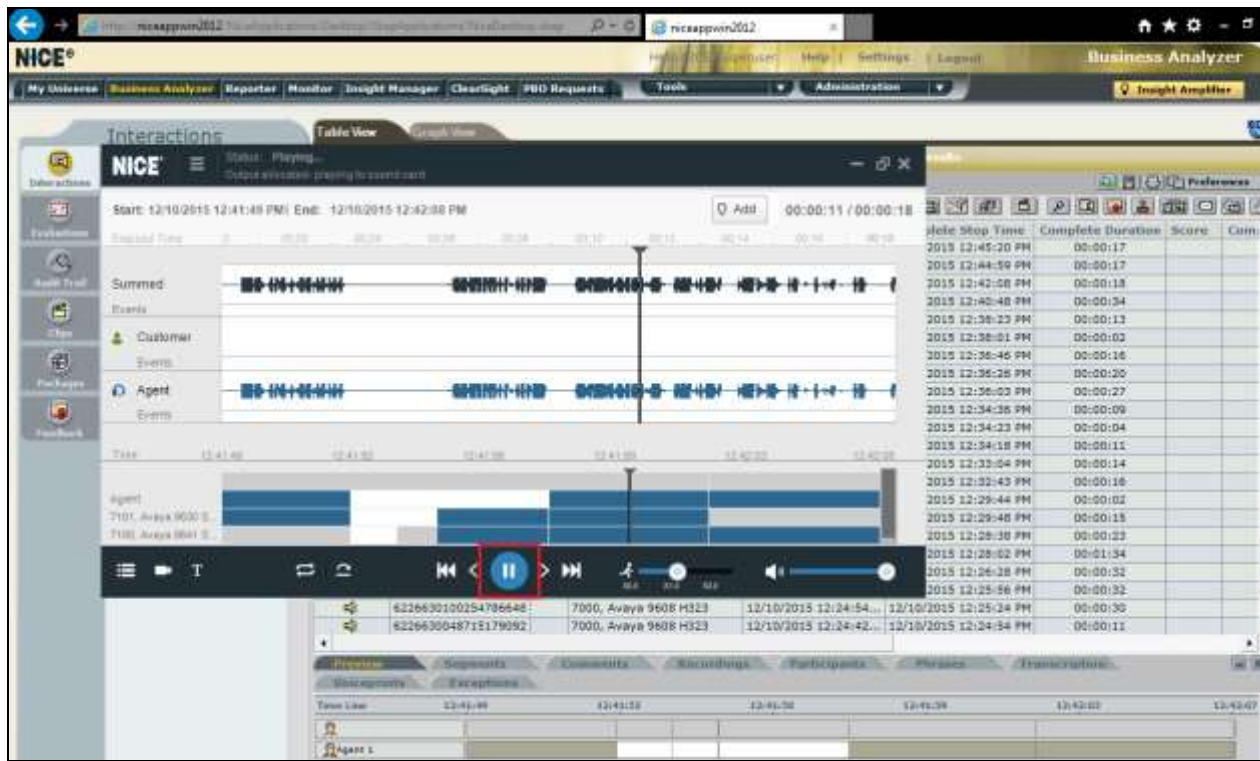
Open a browser session to the NICE Application Server as is shown below. Enter the proper credentials and click on **Login**.



The screenshot shows the NICE Business Analyzer web application. The top navigation bar includes links for 'My Universe', 'Business Analyzer' (highlighted), 'Reporter', 'Monitor', 'Insight Manager', 'Clearlight', 'PBO Requests', 'Tools', and 'Administration'. The left sidebar contains a 'Interactions' section with a 'Public' query selected. The main content area displays 'Results for Query:' with a search bar and a list of results. The top right corner shows the user's name 'Business Analyzer'.

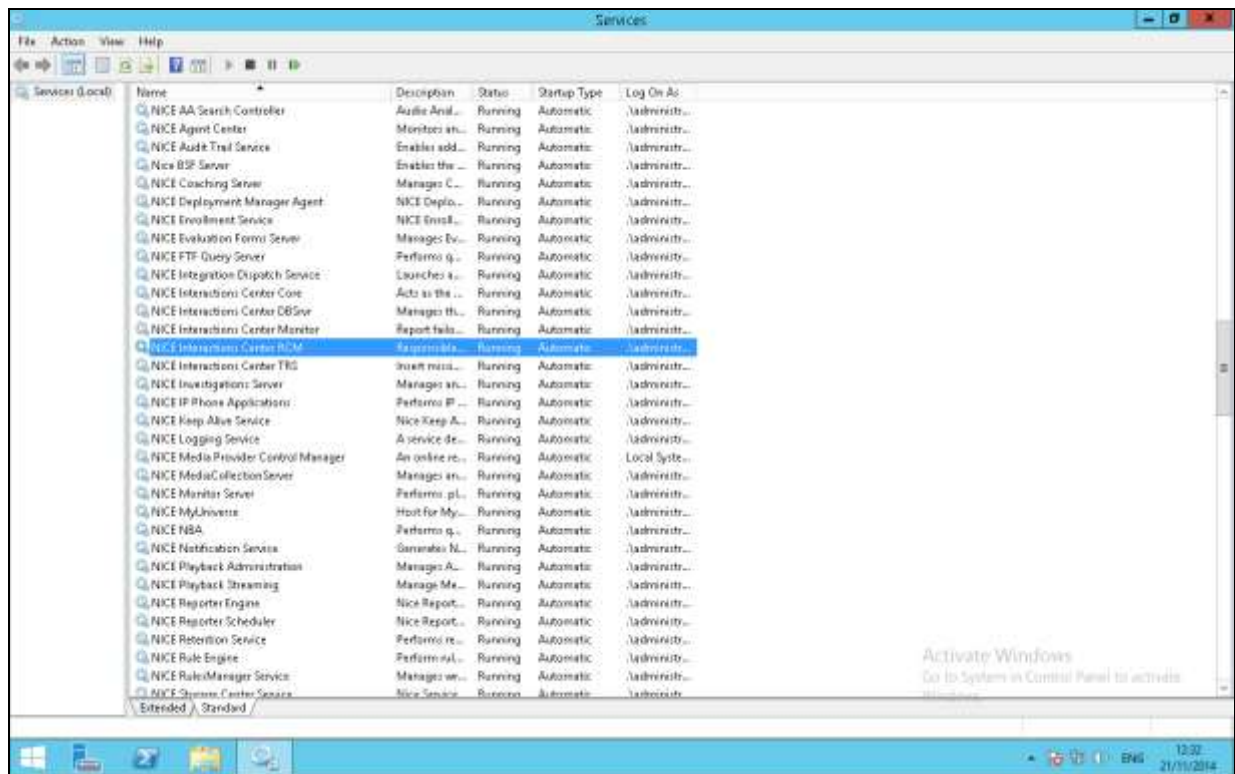
[illegible]

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



## 8.4. 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 to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0 to connect to using Passive Station Side VoIP with SMS to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

## 10. Additional References

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

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

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 7.0
- [4] *Avaya Aura® Session Manager Overview*, Doc # 03603323 *Avaya Aura® Contact Centre SIP Commissioning*, Doc # NN44400-511, Release 7.0

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

## Appendix

### Avaya one-X® Agent Softphone

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

display station 2100	Page 1 of 5	
STATION		
Extension: 2100	Lock Messages? n	BCC: 0
Type: 9630	Security Code: *	TN: 1
Port: S00031	Coverage Path 1:	COR: 1
Name: one-X Agent1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 2100	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? Y	

display station 2100	Page 2 of 5	
	STATION	
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 2100	Always Use? n IP Audio Hairpinning? n	

55 of 58  
NICE64AES70VoIP



## Avaya 9608 H.323 Deskphone

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

display station 2000	Page 1 of 5	
STATION		
Extension: 2000	Lock Messages? n	BCC: 0
Type: 9608	Security Code: *	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: Ext2000	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 2000	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: yes	
	Customizable Labels? y	

display station 2000	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	
	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	EC500 State: enabled
Multimedia Mode: enhanced	Audible Message Waiting? n
MWI Served User Type: sip-adjunct	Display Client Redirection? n
	Select Last Used Appearance? n
	Coverage After Forwarding? s
	Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y
Emergency Location Ext: 2000	Always Use? n IP Audio Hairpinning? n



display station 2000 Page 3 of 5

STATION

```

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

```

```

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

```

ENHANCED CALL FORWARDING

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

SAC/CF Override: n

display station 2000 Page 4 of 5

STATION

SITE DATA

```

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

```

## ABBREVIATED DIALING

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

## BUTTON ASSIGNMENTS

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

voice-mail

---

**©2016 Avaya Inc. All Rights Reserved.**

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

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