



Avaya Solution & Interoperability Test Lab

Application Notes for configuring NICE Engage Platform R6.10 to interoperate with Avaya Aura® Communication Manager R8.0 and Avaya Aura® Application Enablement Services R8.0 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 R8.0, an Avaya Aura® Session Manager R8.0, and Avaya Aura® Application Enablement Services R8.0 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 R6.10 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R8.0, an Avaya Aura® Session Manager R8.0 and Avaya Aura® Application Enablement Services R8.0. 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 Recording 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 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. 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.

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 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.

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 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 phonesets.

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**.

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

All functionality and serviceability test cases were completed successfully. There were no issues to report.

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.

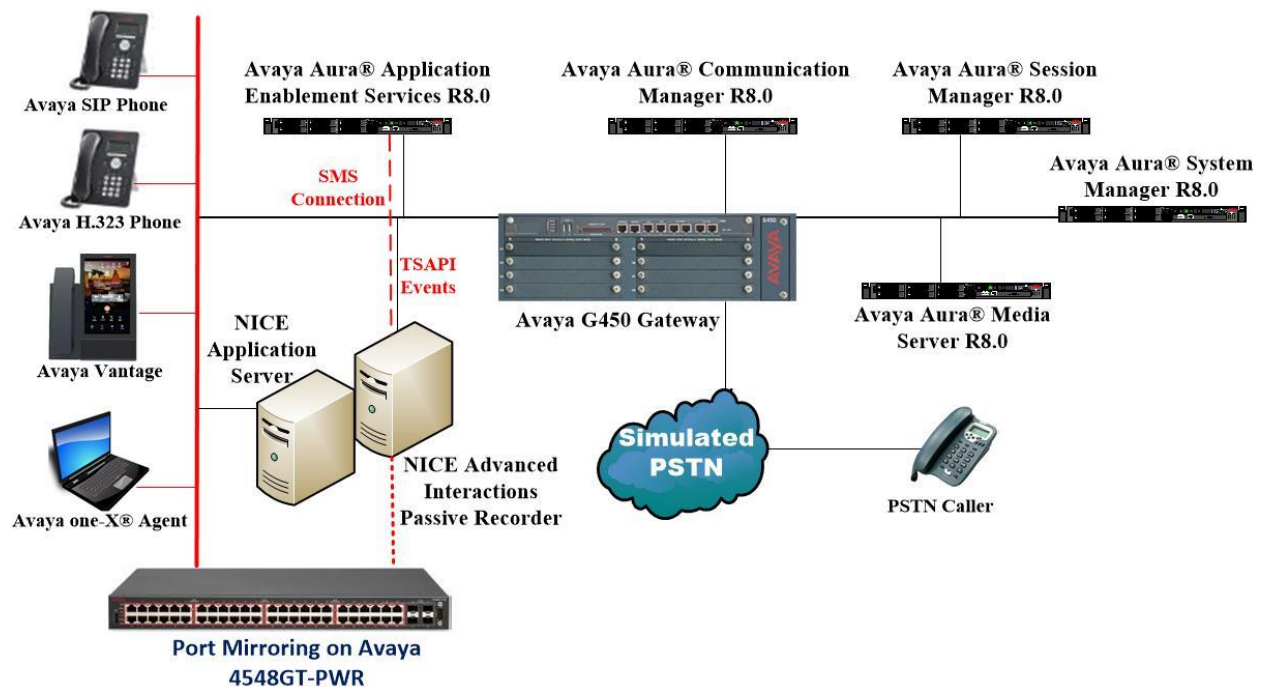


Figure 1: Connection of NICE Engage Platform R6.10 with Avaya Aura® Communication Manager R8.0, Avaya Aura® Session Manager R8.0 and Avaya Aura® Application Enablement Services R8.0

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	R8.0.0.0.0 Build 8.0.0.0.931077 SW Update Revision No. 8.0.0.0.098174
Avaya Aura® Session Manager running on Virtual Server	R8.0.0.0.8000035
Avaya Aura® Communication Manager running on Virtual Server	R8.0 Build 00.0.822.0-24826
Avaya Aura® Application Enablement Services running on Virtual Server	R8.0 Build No – 8.0.0.0.0.6-0
Avaya G450 Gateway	41.10.1 /1
Avaya Media Server running on a Virtual Server	8.0.0.150
Avaya 4548GT-PWR Ethernet Switch	5.7.3.030
Avaya 96x1 H323 Deskphone	6.6.115
Avaya 1616 -I H323 Deskphone	Ha1616ua1_3110A
Avaya J179 H323 Deskphone	7.002U
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J129 SIP Deskphone	1.0.0.0.0.43
Avaya Vantage Equinox	1.0.0.2
Avaya one-X® Agent	2.5.8
NICE Engage Platform <ul style="list-style-type: none">- NICE Application Server- Advanced Interactions Recorder	6.10

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify System Features

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

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

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

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

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM100	10.10.40.34		
Aes80vmpg	10.10.40.56		
default	0.0.0.0		
g450	10.10.40.15		
procr	10.10.40.59		

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 **aes80vmpg**.
- **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:	aes80vmpg	*****	y	idle			
2:							
3:							

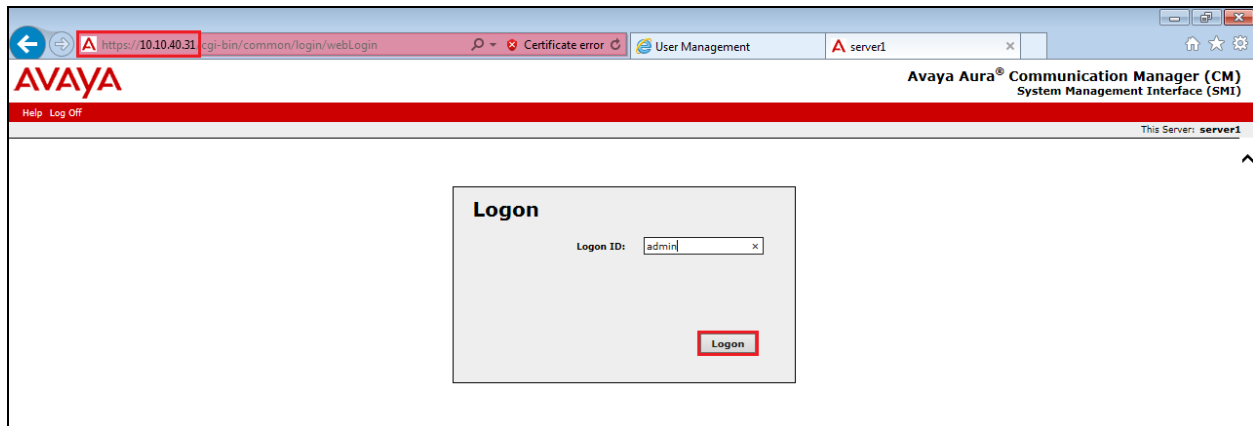
5.4. Configure CTI Link for TSAPI Service

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: aes80vmpg			

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.

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: nicecm

Primary group: users

Additional groups (profile): prof19

Linux shell: /bin/bash

Home directory: /var/home/nicecm

Lock this account: ☐

SAT Limit: none

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

Submit Cancel Help

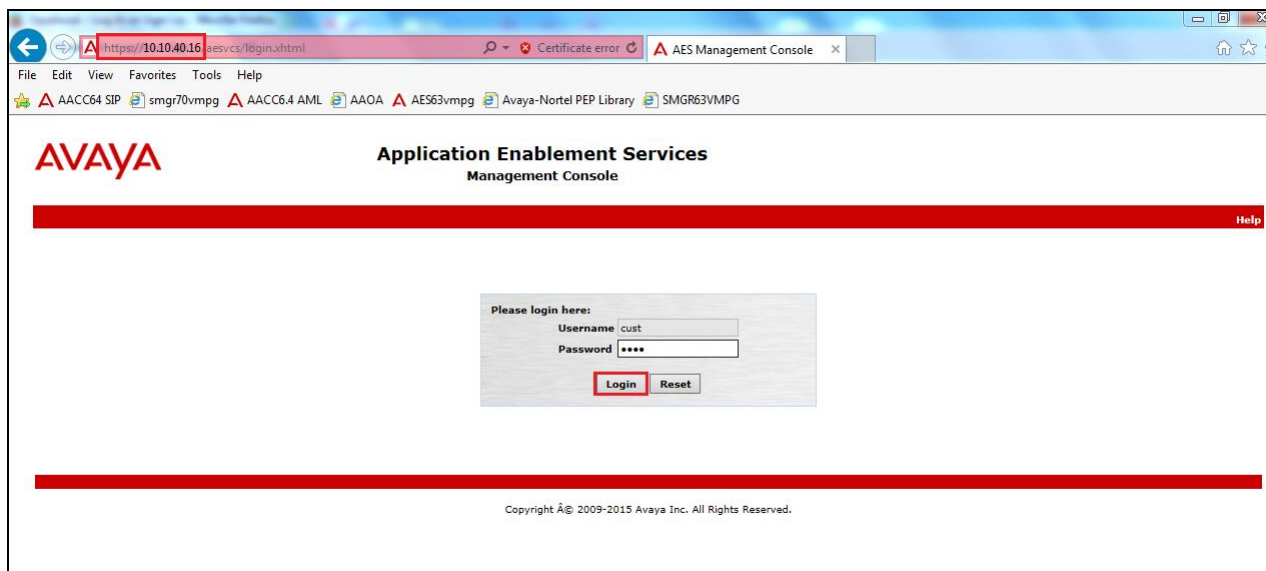
6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Configure Networking Ports
- Create CTI User
- Configure Security Database
- 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 Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

AVAYA Application Enablement Services Management Console

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

AE Services Home | Help | Logout

AE Services

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
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

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

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

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

6.2. Create Switch Connection

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

AVAYA Application Enablement Services Management Console

Communication Manager Interface | Switch Connections

Switch Connections

cm80vmppg **Add Connection**

Connection Name	Processor Ethernet	Msg Period
Edit Connection	Edit PE/CLAN IPs	Edit H.323 Gatekeeper
Delete Connection	Survivability Hierarchy	

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

Connection Details - cm80vmpg

Switch Password: [password field]

Confirm Switch Password: [password field]

Msg Period: 30 Minutes (1 - 72)

Provide AE Services certificate to switch: ☐

Secure H323 Connection: ☐

Processor Ethernet: ☒

Apply Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button.

Switch Connections

cm80vmpg Add Connection

Connection Name	Processor Ethernet	Msg Period
Edit Connection	Edit PE/CLAN IPs	Edit H.323 Gatekeeper
Delete Connection		Survivability Hierarchy

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.

Edit Processor Ethernet IP - cm80vmpg

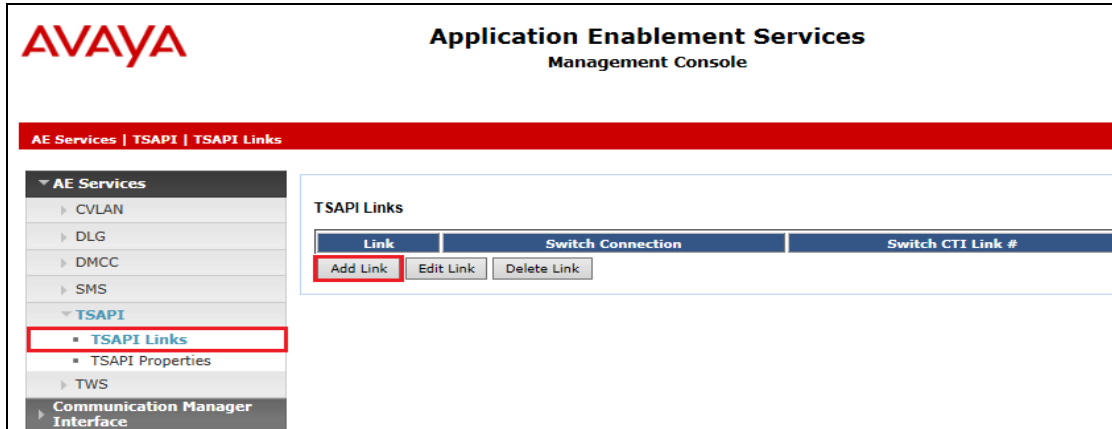
10.10.40.59 **Add/Edit Name or IP**

Name or IP Address
10.10.40.59

Back

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 **cm80vmpg**, 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 should correspond with the Communication Manager version.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.

The screenshot shows the 'Edit TSAPI Links' form. It contains the following fields and values:


Field	Value
Link	1
Switch Connection	cm80vmpg
Switch CTI Link Number	1
ASAI Link Version	8
Security	Both

At the bottom of the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

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

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.


 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

Apply **Cancel**

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	cm80vmpg	1	8	Both
Add Link Edit Link Delete Link				

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**.



Application Enablement Services
Management Console

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 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**.

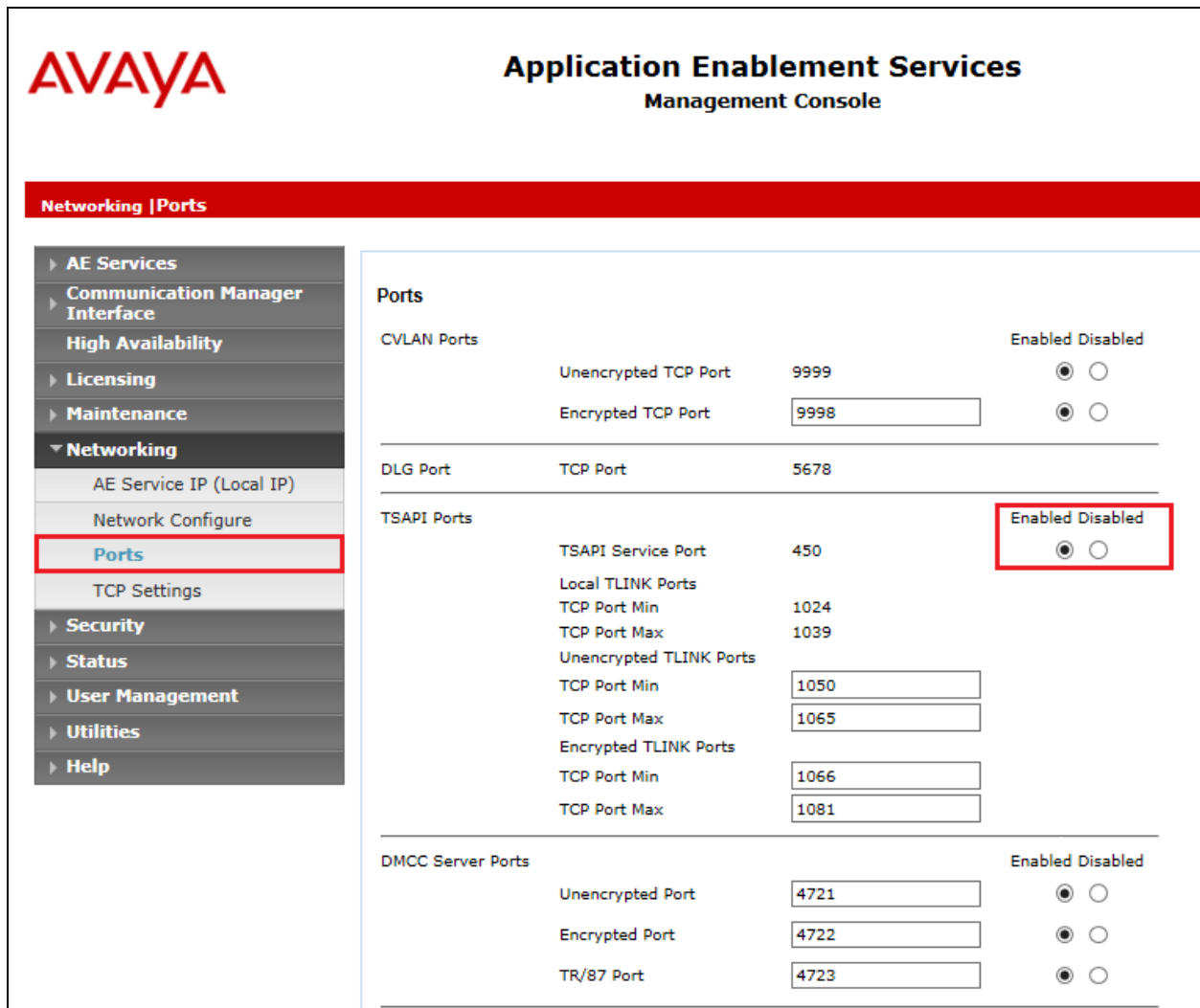
The screenshot displays the NICE Engage Platform configuration interface. On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, Tlinks (highlighted with a red box), Tlink Groups, and Worktops. The main content area is titled 'Tlinks' and contains a 'Tlink Name' section with two radio button options: 'AVAYA#CM80VMPG#CSTA#AES80VMPG' (selected and highlighted with a red box) and 'AVAYA#CM80VMPG#CSTA-S#AES80VMPG'. Below these options is a 'Delete Tlink' button.

6.5. Configure Networking Ports

Ensure that all ports are enabled for connections to the AES from NICE.

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.



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

			Enabled	Disabled
TCP Port	5678		<input checked="" type="radio"/>	<input type="radio"/>

TSAPI Ports

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

DMCC Server Ports

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

6.5.2. 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**.

Networking | TCP / TLS Settings

AE Services
Communication Manager
Interface
High Availability
Licensing
Maintenance
Networking
AE Service IP (Local IP)
Network Configure
Ports
TCP/TLS Settings
Security
Status
User Management
Utilities
Help

TCP / TLS Settings

TLSv1 Protocol Configuration

- ☒ Support TLSv1.0 Protocol
- ☒ Support TLSv1.1 Protocol
- ☒ Support TLSv1.2 Protocol

TCP Retransmission Count

- ☒ Standard Configuration (15)
- ☐ TSAPI Routing Application Configuration (6)

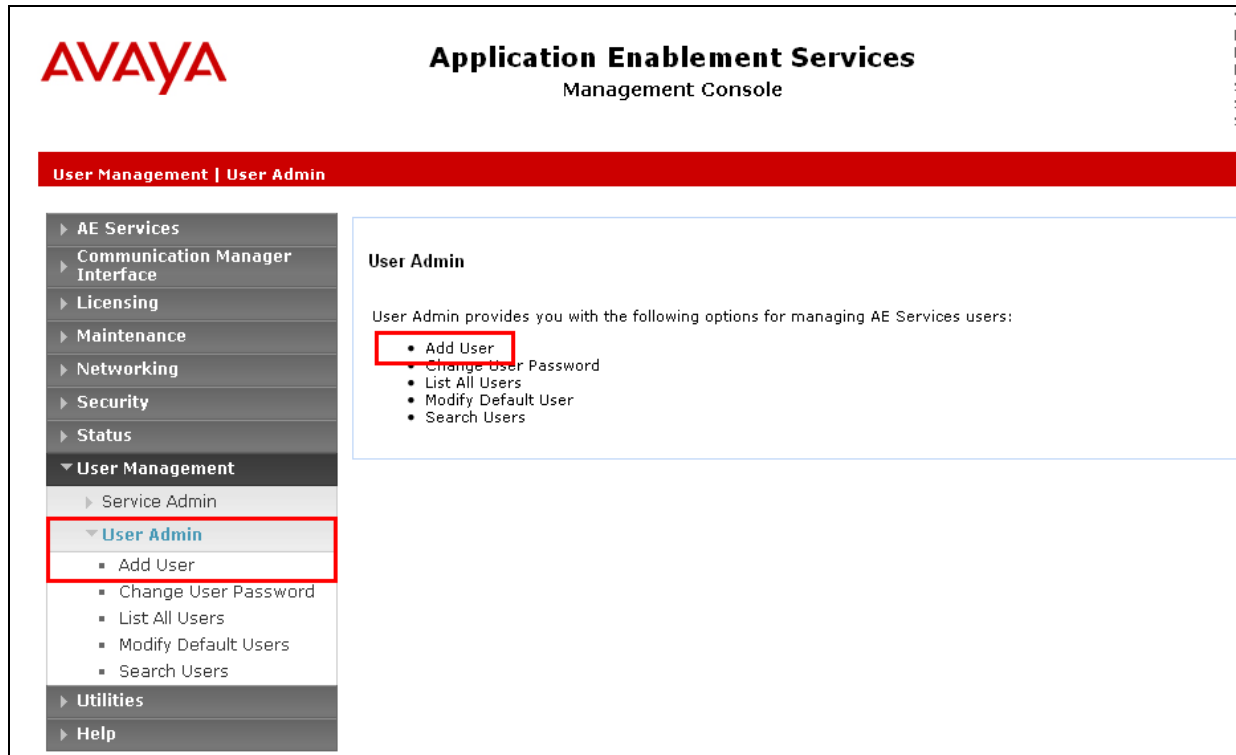
Apply Changes Restore Defaults Cancel Changes

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.

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.



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**.

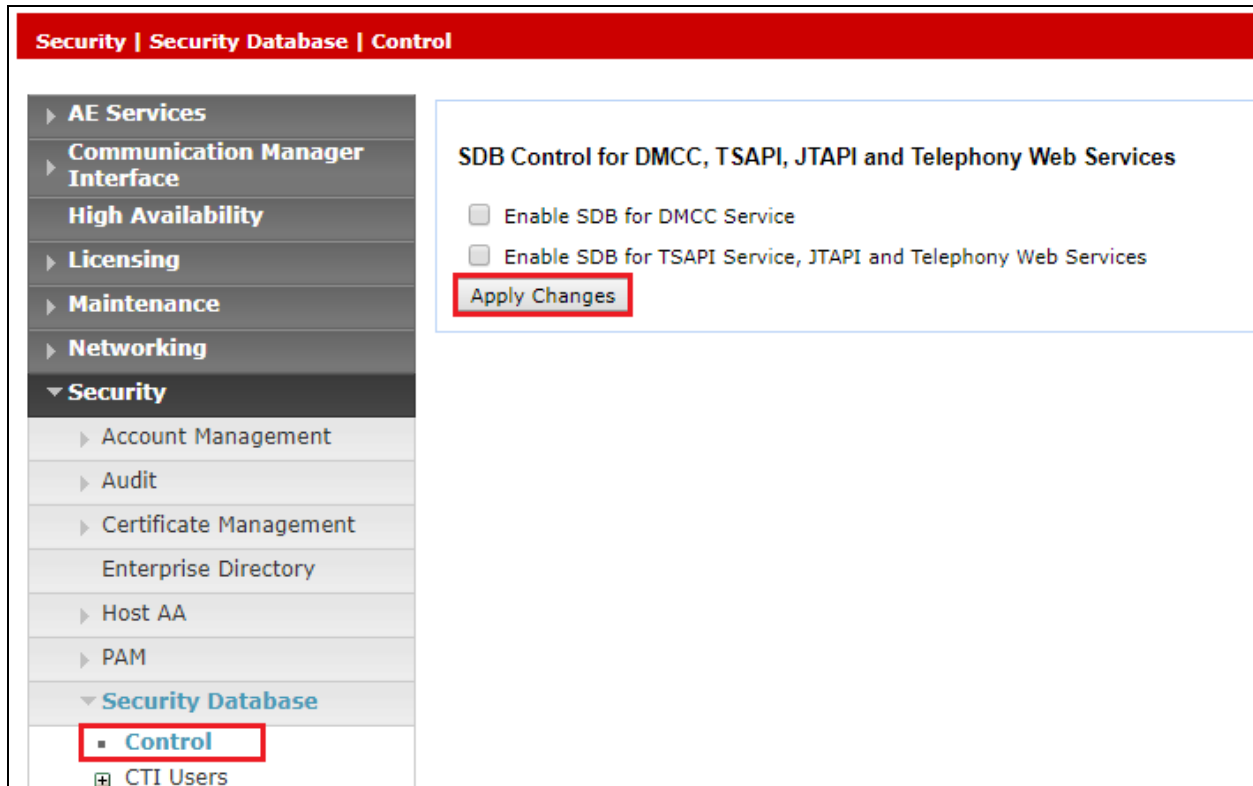
User Admin	CM Home	<input type="text"/>
▪ Add User	Css Home	<input type="text"/>
▪ Change User Password	CT User	<input type="text" value="Yes"/>
▪ List All Users	Department Number	<input type="text"/>
▪ Modify Default Users	Display Name	<input type="text"/>
▪ Search Users	Employee Number	<input type="text"/>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

6.7. Configure Security Database

For compliance testing associated with these Application Notes the Security Database was not enabled and the user associated with NICE was given unrestricted access.

6.7.1. Disable the Security Database Control

Navigate to **Security** → **Security Database** → **Control** as shown below. Ensure that no boxes are ticked and click on **Apply Changes** if necessary.



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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. Under Security, the 'Security Database' is expanded, and 'CTI Users' is selected, with 'List All Users' highlighted. The main content area displays a table of CTI Users. The table has four columns: User ID, Common Name, Worktop Name, and Device ID. The 'nice' user is selected with a radio button. Below the table are 'Edit' and 'List All' buttons. The top right corner shows system information including last login, failed login attempts, host name, server offer type, SW version, server date and time, and HA status.

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

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

The screenshot shows the 'Edit CTI User' page for the 'nice' user. The left sidebar is the same as the previous screenshot. The main content area shows the user profile with fields for User ID, Common Name, and Worktop Name. The 'Unrestricted Access' checkbox is checked. Below this are sections for Call and Device Control, Call and Device Monitoring, and Routing Control, each with a dropdown menu. At the bottom, there are 'Apply Changes' and 'Cancel Changes' buttons. The top right corner shows the same system information as the previous screenshot.

User ID	Common Name	Worktop Name
nice	nice	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

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

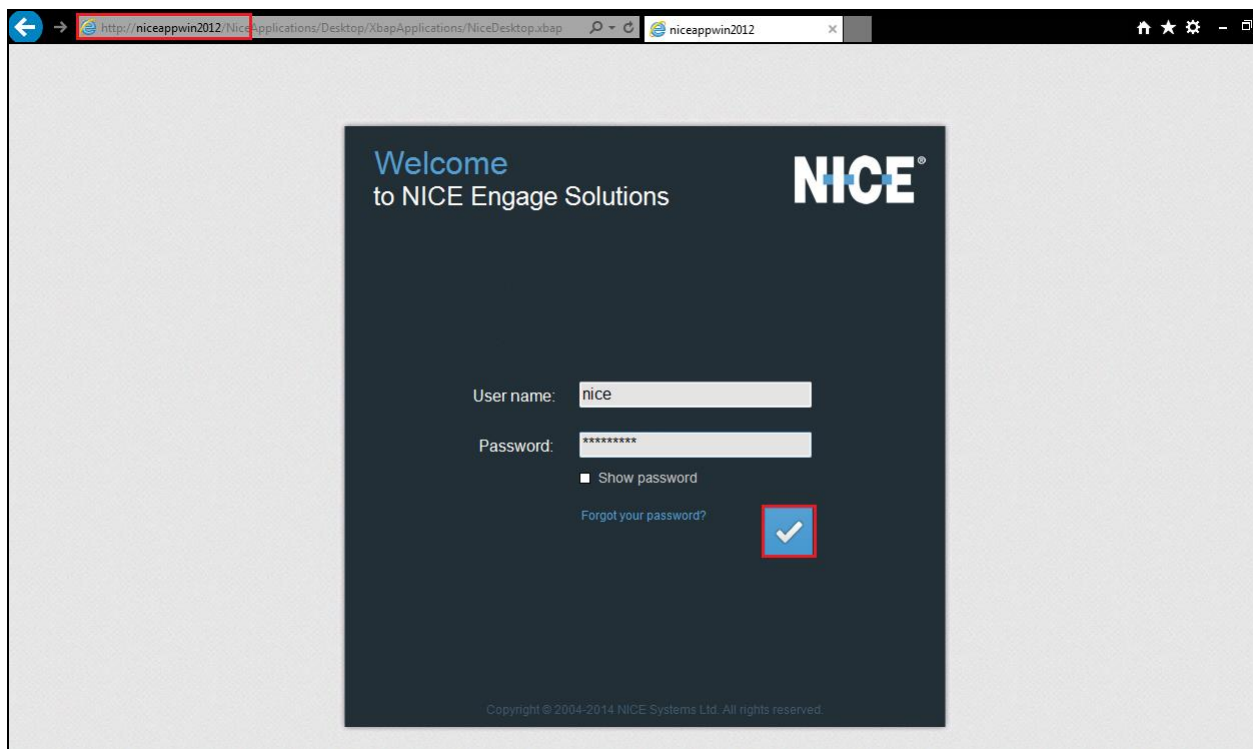
Default CM Host Address	10.10.40.59	
Default CM Admin Port	5022	
CM Connection Protocol	SSH	
SMS Logging	NORMAL	
SMS Log Destination	apache	
CM Proxy Trace Logging	NONE	
Max Sessions per CM	5	
Proxy Shutdown Timer	1800	seconds
SAT Login Keepalive	180	seconds
CM Terminal Type	OSSIZ	
Proxy Log Destination	/var/log/avaya/aes/ossicm.log	

Apply Changes **Restore Defaults** **Cancel**

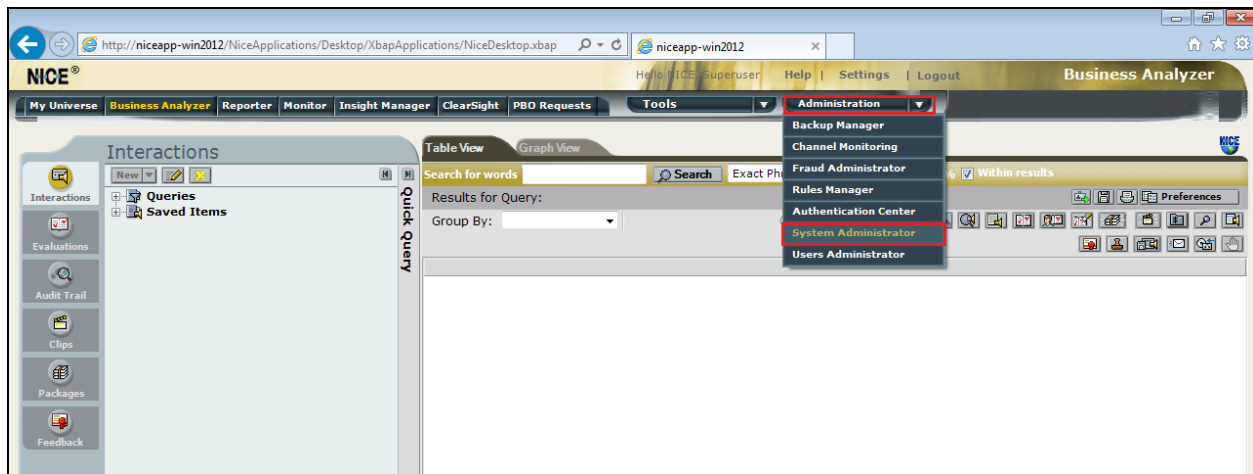
7. Configure NICE Engage Platform

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**.

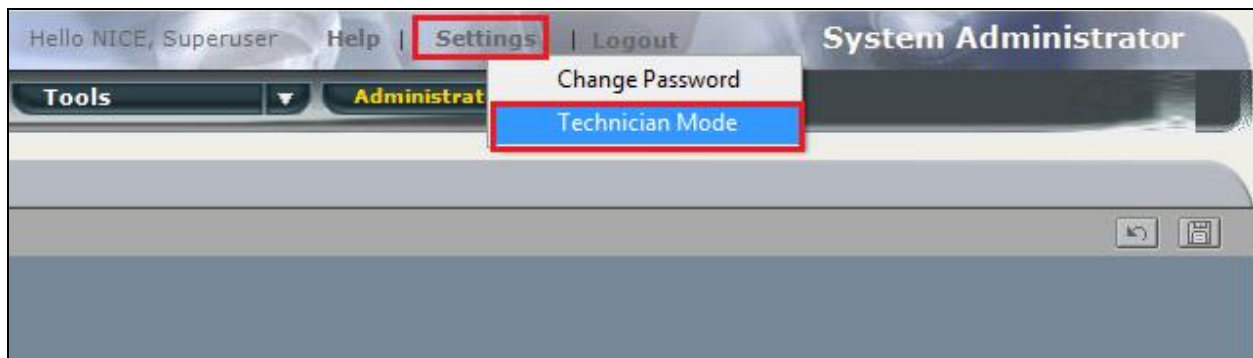
The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya solution. All configuration of the NICE Engage Platform for connection with the AES is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser as shown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

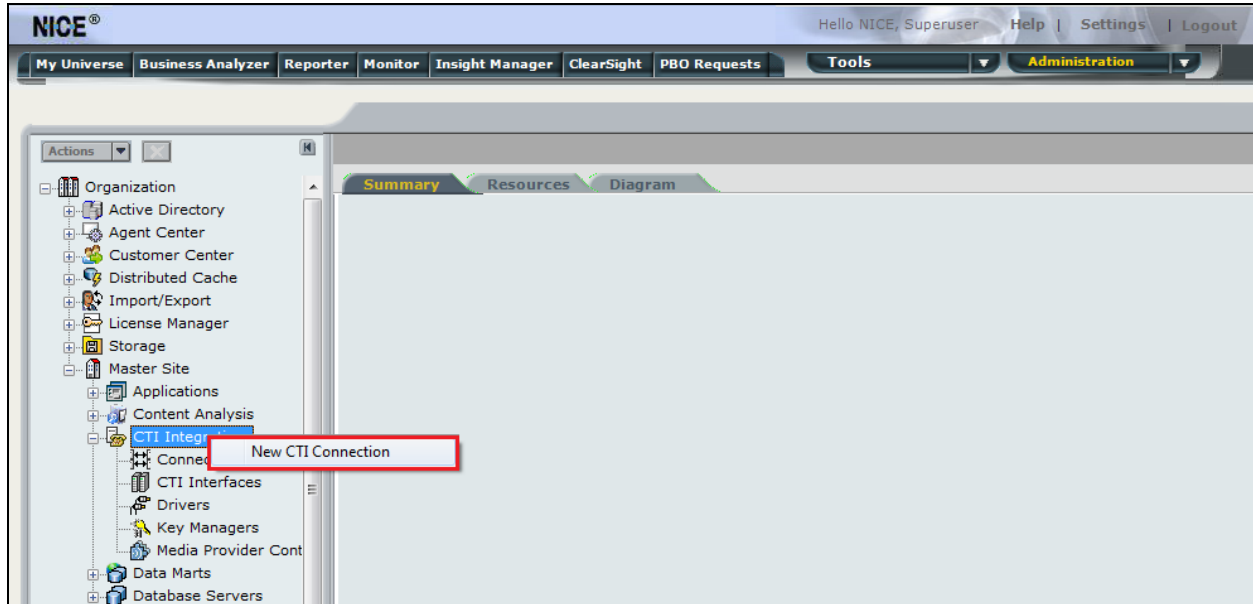


Before any changes can be made, switch to Technician Mode by clicking into Settings at the top of the screen as shown below.

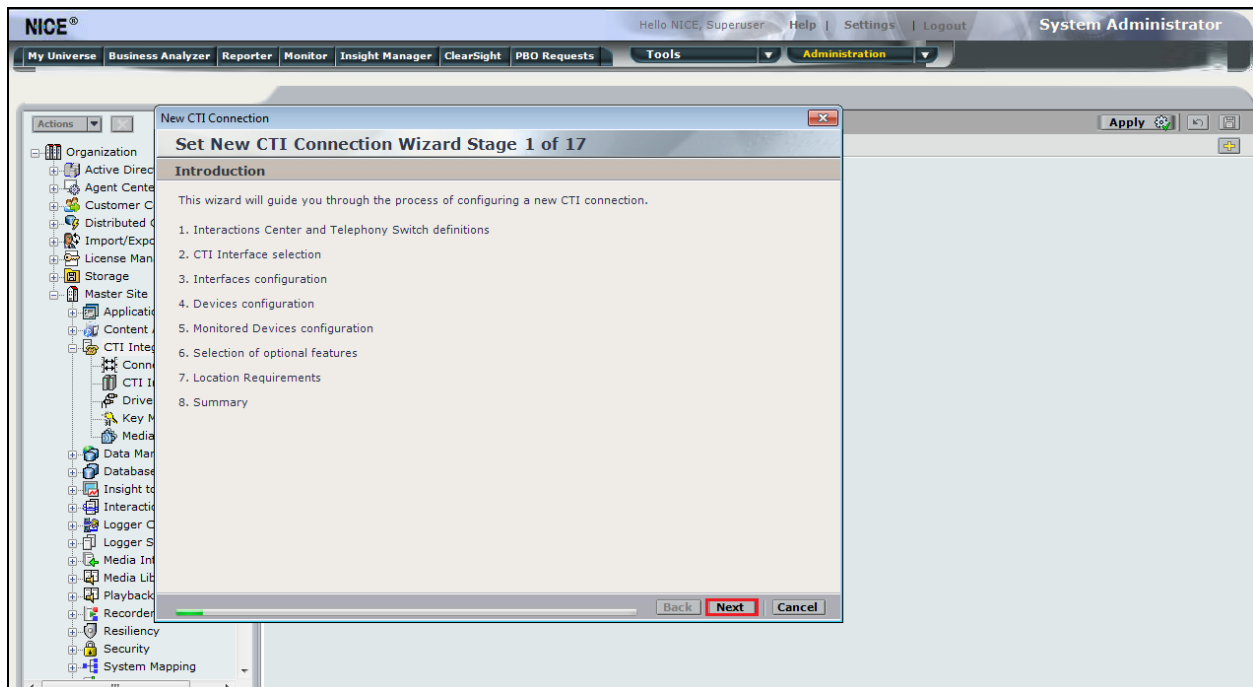


7.1. New CTI Connection

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 17 steps required to setup 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.

New CTI Connection

Set New CTI Connection Wizard Stage 2 of 17

Interactions Center Switch

Attach CTI to Interactions Center Server:

☒ Regular Interactions Center: IC (nice-app)

☐ Interactions Center Cluster:

☐ Use existing Telephony Switch: Avaya CM

☒ Define new Telephony Switch:

Switch Type: Avaya CM

Switch Name: Avaya CM Passive

Agent Logon Mode

Interactions Centers should accept agent logins on this switch if agent logins:

☒ To the same station again

☒ To more than one station

☒ To a station another agent is logged into

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. Ensure that **Additional VoIP Mapping** is ticked, and that **Generic SIP Mapper** is chosen from the dropdown. Click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 3 of 17

Interface Type

CTI Interface Type

Avaya CM CTI Interface: 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

Avaya Communication Manager
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 17

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	
LoginID	
Password	
UseWarmStandBy	No

Description:

Additional Interface Parameters

Back Next Cancel

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

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 17

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	
LoginID	
Password	
UseWarmStandBy	No

Description:

Additional Interface Parameters

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

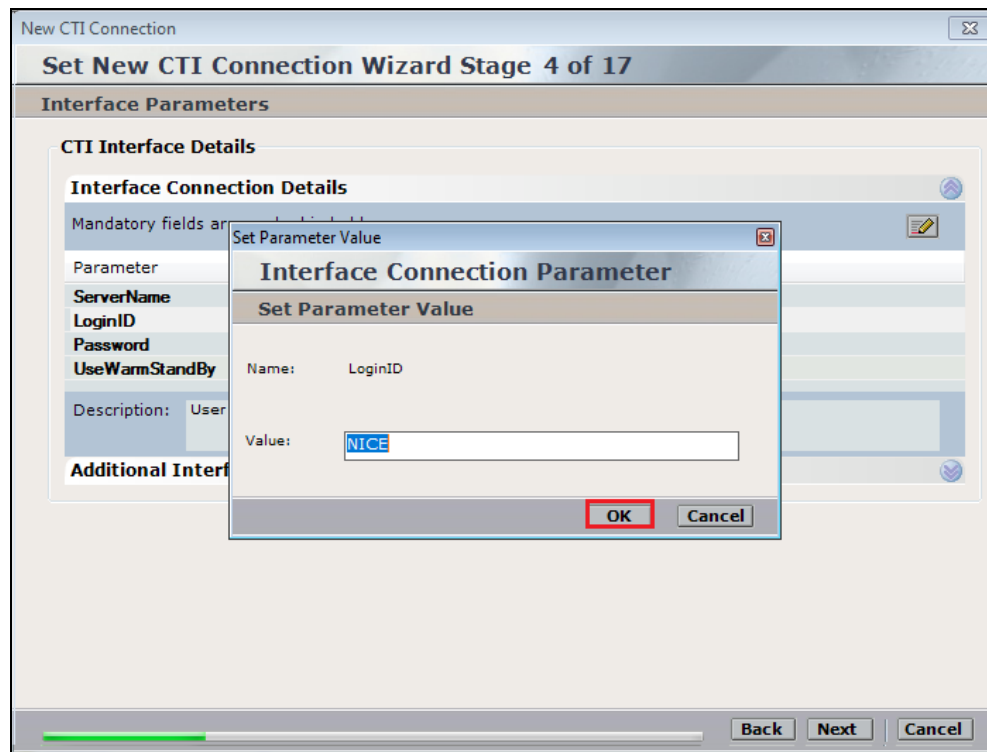
Name: ServerName

Value: AVAYA#CM80VMPPG#CSTA#AES80VMPPG

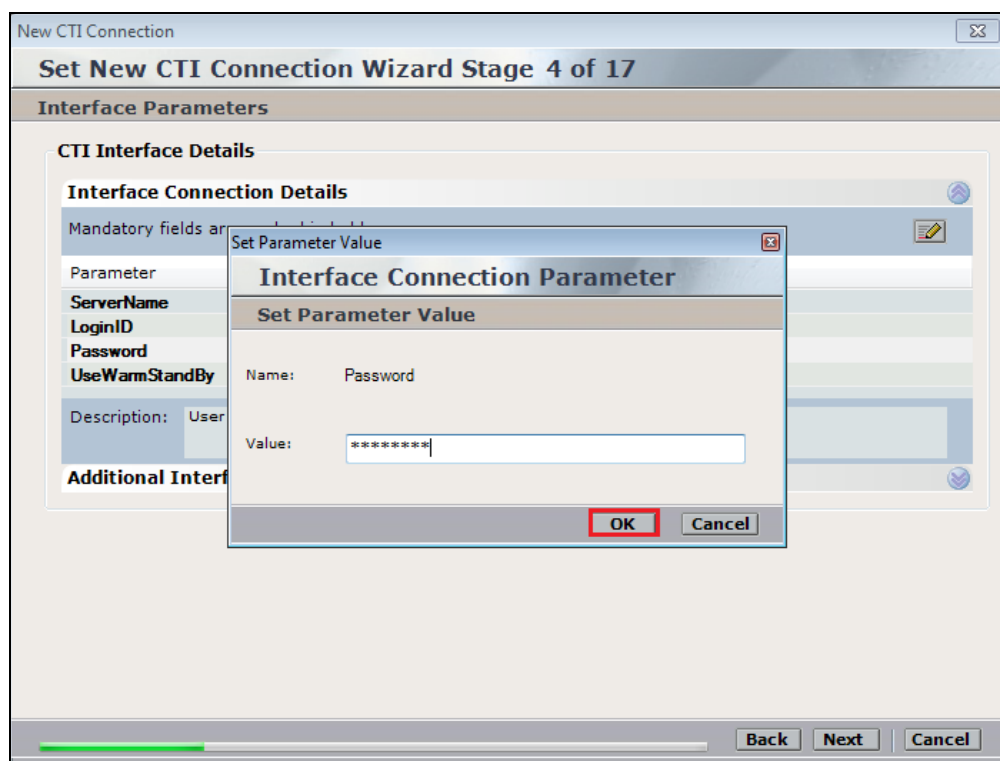
OK Cancel

Back Next Cancel

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



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



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

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 17

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	AVAYA#CM80VMPG#CSTA#AES80VMPG
LoginID	NICE
Password	*****
UseWarmStandBy	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**.

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
AESVersion	Below 4.1
SmsHostIpAddress	
SmsSessionMode	BASIC_AUTHORIZATION
SmsRequestTimeoutInSec	30

Description: AES Version.

Additional Interface Parameters

Back Next Cancel

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

The screenshot shows the 'Set New CTI Connection Wizard' with the 'Interface Connection Parameter' dialog open. The dialog is titled 'Set Parameter Value' and shows the parameter 'AESVersion' with a value of '4.1 and Above'. The 'OK' button is highlighted with a red box. The background window shows a list of parameters including 'SmsHostIpAddress', 'SmsSessionMode', 'SmsRequestTimeoutInSec', 'UserName', and 'Password'.

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

The screenshot shows the 'Set New CTI Connection Wizard' with the 'Interface Connection Parameter' dialog open. The dialog is titled 'Set Parameter Value' and shows the parameter 'SmsHostIpAddress' with a value of '10.10.40.56'. The 'OK' button is highlighted with a red box. The background window shows a list of parameters including 'AESVersion', 'SmsSessionMode', 'SmsRequestTimeoutInSec', 'UserName', and 'Password'.

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 'Set New CTI Connection Wizard'. It has a 'VoIP Mapping' tab selected. Under 'VoIP Mapping Interface Details', there is a section for 'Interface Connection Details' with a note 'Mandatory fields are marked in bold'. A list of parameters is shown, with 'UserName' highlighted by a red box. Below this, there is a 'Description' field containing 'Username for the CM (mylogin@cmserveraddr)'. The foreground window is titled 'Set Parameter Value' and 'Interface Connection Parameter'. It has a 'Set Parameter Value' section with 'Name' set to 'UserName' and 'Value' set to 'nicecm'. There are 'OK' and 'Cancel' buttons at the bottom of this dialog.

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 in the list is now highlighted by a red box. The foreground 'Set Parameter Value' dialog now has 'Name' set to 'Password' and 'Value' set to a masked string of seven asterisks. The 'OK' and 'Cancel' buttons are still visible at the bottom.

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

New CTI Connection

Set New CTI Connection Wizard Stage 7 of 17

VoIP Mapping

VoIP Mapping Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
SmsRequestTimeoutInSec	30
UserName	nicecm
Password	*****
UseWarmStandbyFeature	no

Description:

Additional Interface Parameters

Back Next Cancel

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

Set New CTI Connection Wizard Stage 7 of 17

Additional VoIP Mapping

Additional VoIP Mapping Interface Details

Interface Connection Details

Additional Interface Parameters

Mandatory fields are marked in bold

Parameter	Value
MaxNumOfLines	150
MaxDigitsInAgentPhone	5
SystemTablesRefreshingInterval	180
MaxCallDuration	180

Description: This parameter represents the maximum number of digits in the agent phone number. It decides the call type [Internal|Outgoing].

Set Parameter Value

Interface Additional Parameter

Set Parameter Value

Name: MaxDigitsInAgentPhone

Value: 4

OK Cancel

Back Next Cancel

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

[illegible]

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.

Set New CTI Connection

New CTI Connection

Set New CTI Connection

Devices

Available Devices

Provide telephony switch

0 devices

Device Number/IP

Device Type: *

Device Number: *

IP:

Advanced Device Parameters

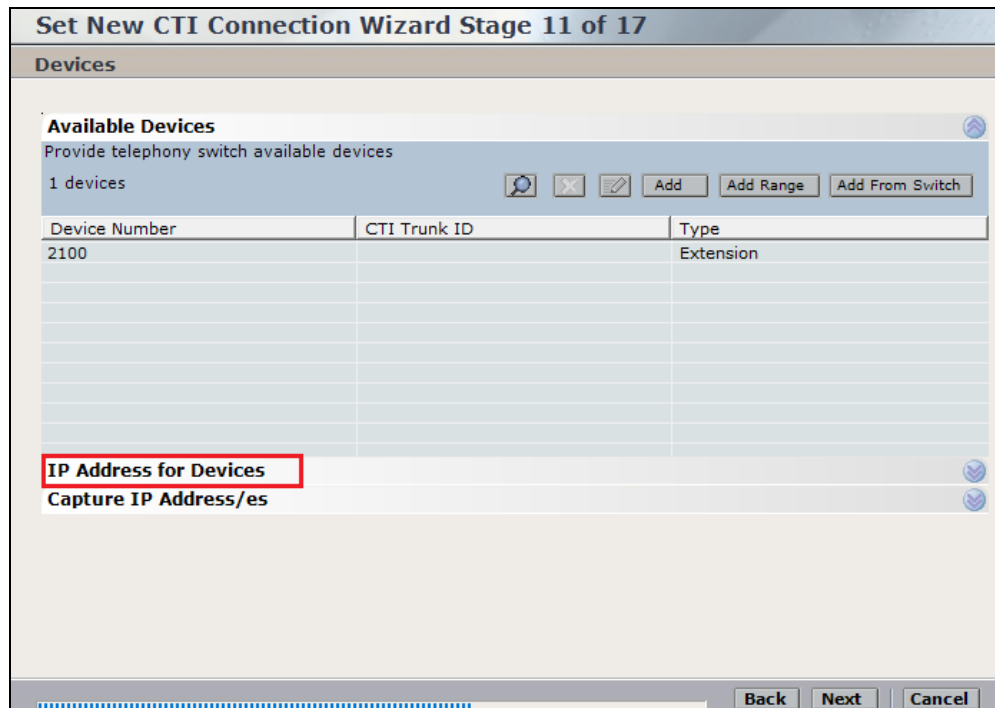
☐ Display Read Only Information

Name	Value

Description:

OK **Cancel**

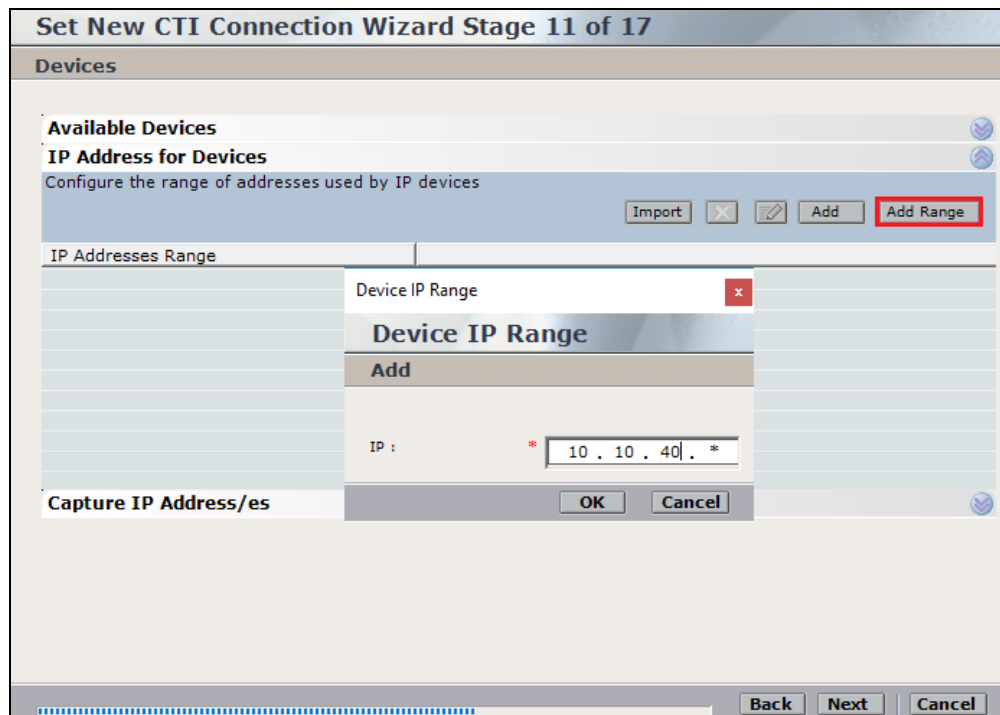
Click on **IP Address for Devices**. This will add the address range for the IP addresses picked up from the SMS connection to the AES.



The screenshot shows the 'Set New CTI Connection Wizard Stage 11 of 17' window. The 'Devices' section is active, showing 'Available Devices' with a table containing one device: Device Number 2100, CTI Trunk ID, and Type Extension. Below the table, the 'IP Address for Devices' option is highlighted with a red box. The 'Capture IP Address/es' option is also visible. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Device Number	CTI Trunk ID	Type
2100		Extension

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**.



The screenshot shows the 'Set New CTI Connection Wizard Stage 11 of 17' window. The 'Devices' section is active, showing 'Available Devices' with a table containing one device: Device Number 2100, CTI Trunk ID, and Type Extension. Below the table, the 'IP Address for Devices' option is highlighted with a red box. The 'Capture IP Address/es' option is also visible. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons. A 'Device IP Range' dialog box is open, showing the 'Add' button and the IP range '10 . 10 . 40 . *'.

Device Number	CTI Trunk ID	Type
2100		Extension

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.

Set New CTI Connection Wizard Stage 11 of 17

Devices

Available Devices

IP Address for Devices

Configure the range of addresses used by IP devices

Import Add Add Range

IP Addresses Range

10.10.40.*

Capture IP Address/es

Back Next Cancel

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

New CTI Connection

Set New CTI Connection Wizard Stage 11 of 17

Devices

Available Devices

IP Address for Devices

Capture IP Address/es

Configure the Call Managers and Gatekeepers

Import Add

IP

Gatekeepers

Add

IP : 10.10.40.58

Port: 5060

OK Cancel

Back Next Cancel

Click on **Next** to continue.

[illegible]

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

New CTI Connection

Set New CTI Connection Wizard Stage 12 of 17

Monitor






Please select the devices to be monitored
Double click on a monitored device for further configuration

Available Devices: 0 devices

Device	Type

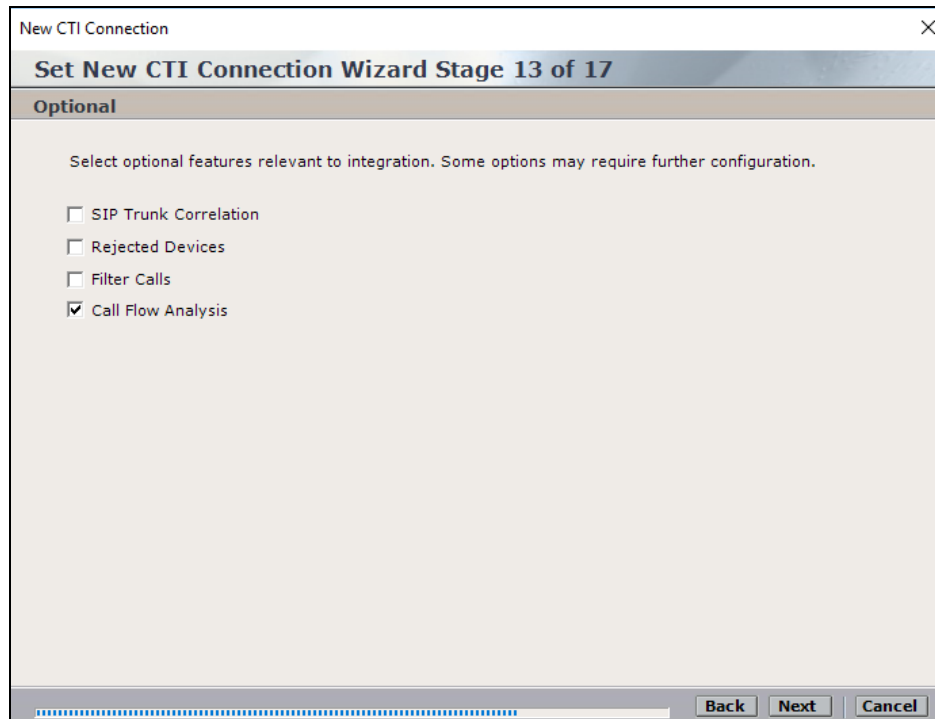
Monitored Devices: 1 devices

Device	Type
2100	Extension

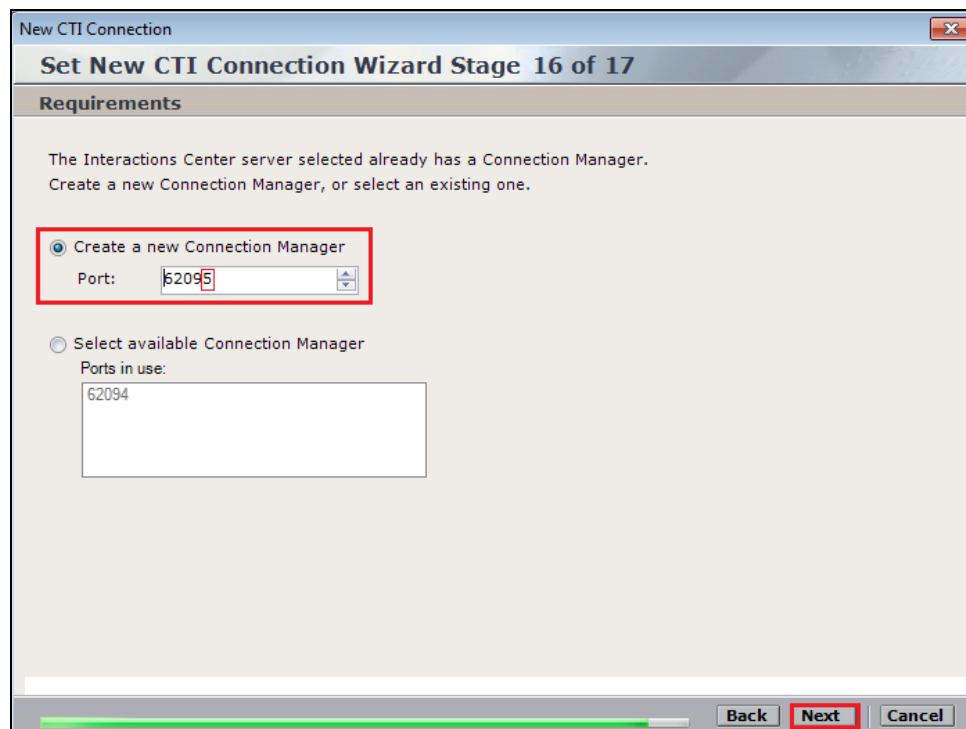
Back Next Cancel

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



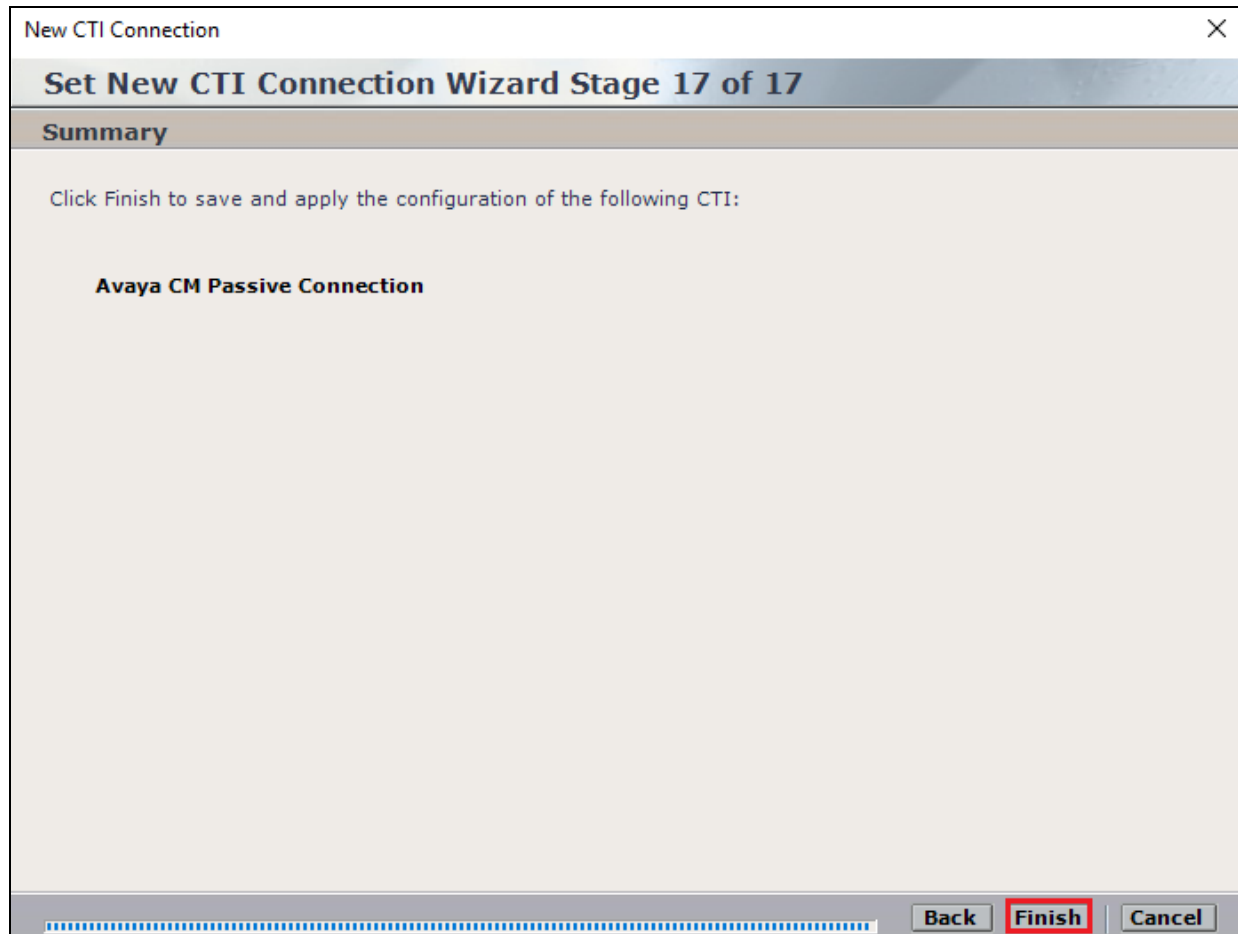
The screenshot shows a window titled "New CTI Connection" with a subtitle "Set New CTI Connection Wizard Stage 13 of 17". The main section is labeled "Optional" and contains the instruction: "Select optional features relevant to integration. Some options may require further configuration." Below this, there are four checkboxes: "SIP Trunk Correlation", "Rejected Devices", "Filter Calls", and "Call Flow Analysis". The "Call Flow Analysis" checkbox is checked. At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

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

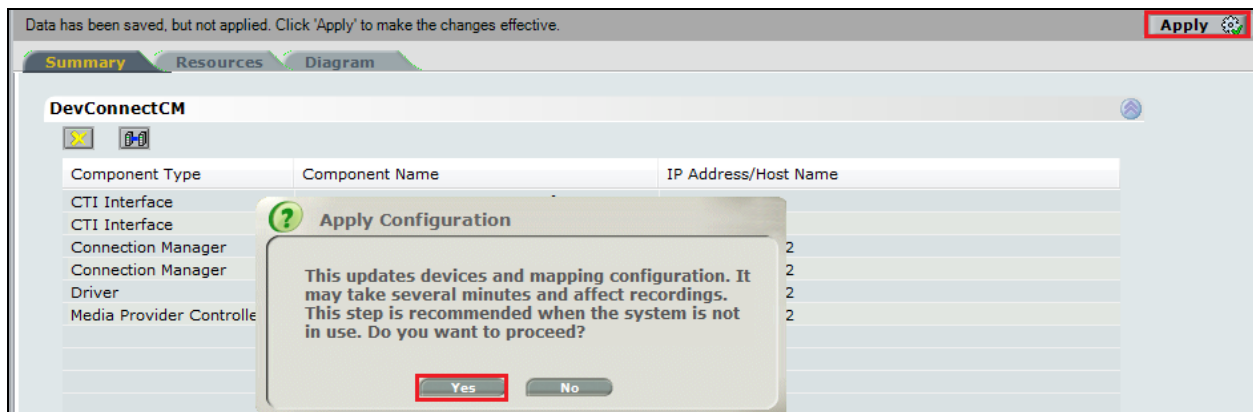


The screenshot shows a window titled "New CTI Connection" with a subtitle "Set New CTI Connection Wizard Stage 16 of 17". The main section is labeled "Requirements" and contains the instruction: "The Interactions Center server selected already has a Connection Manager. Create a new Connection Manager, or select an existing one." Below this, there are two radio buttons: "Create a new Connection Manager" (which is selected) and "Select available Connection Manager". Under "Create a new Connection Manager", there is a "Port:" label and a text box containing "62095". Under "Select available Connection Manager", there is a "Ports in use:" label and a list box containing "62094". At the bottom right, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a red border.

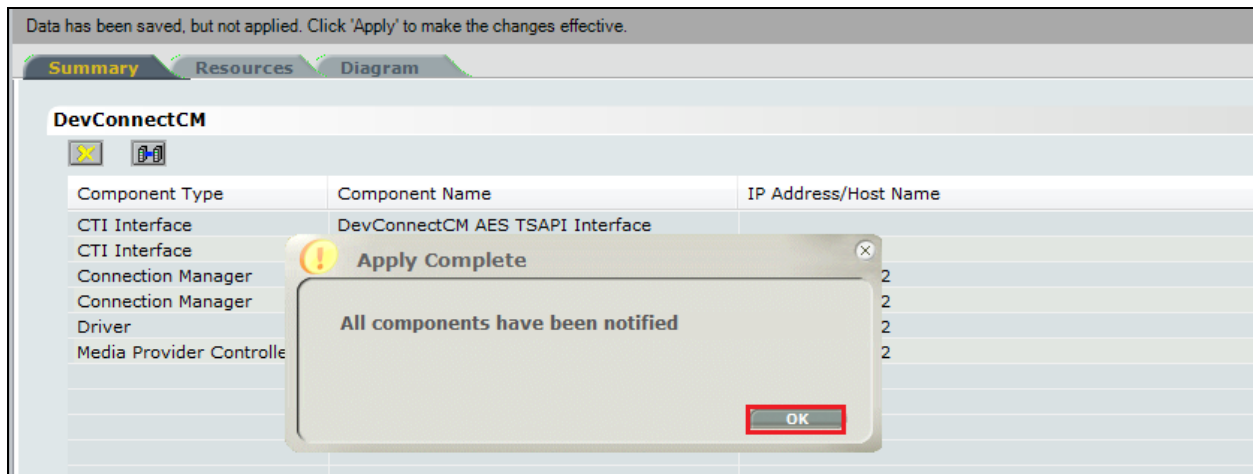
Click on **Finish** to complete the **New CTI Wizard**.



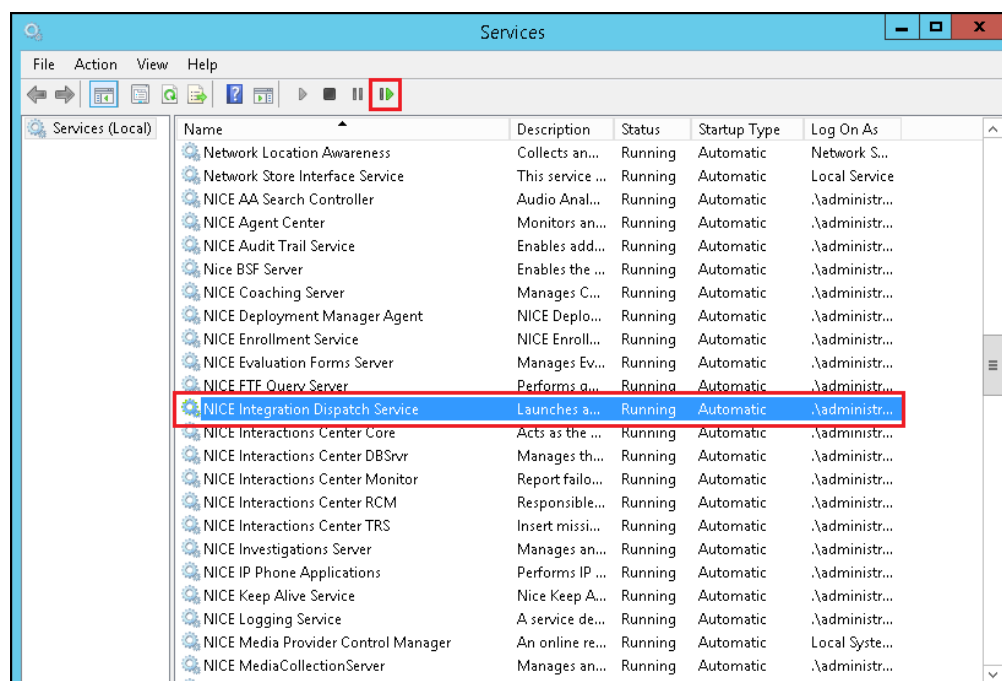
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed.



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

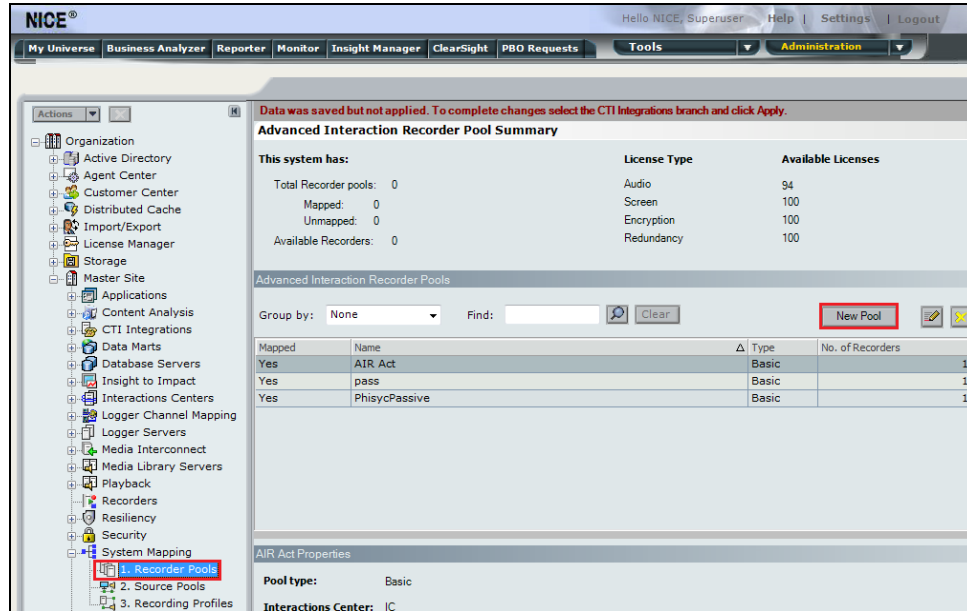


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

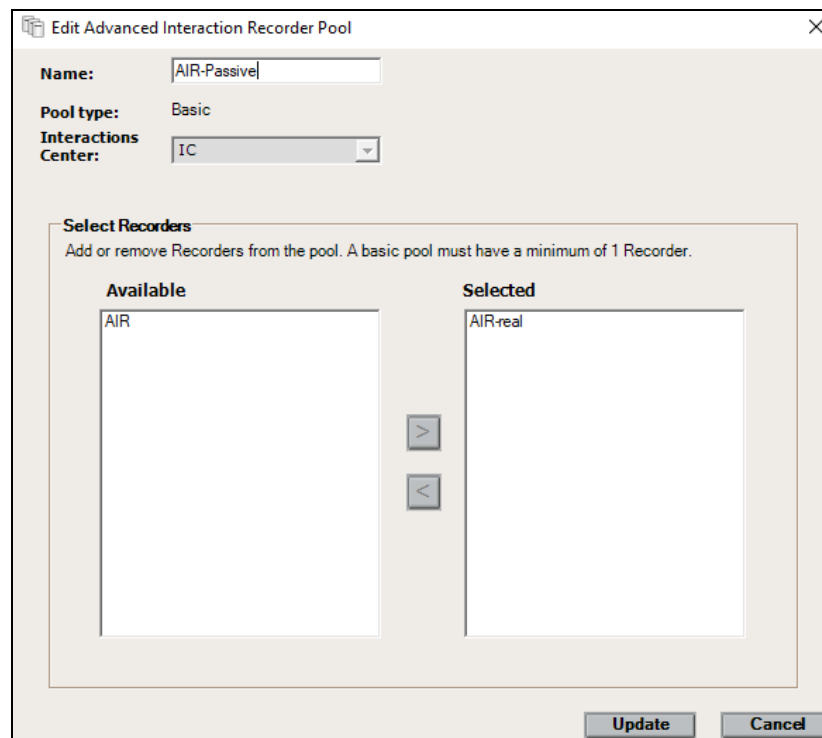


7.2. System Mapping

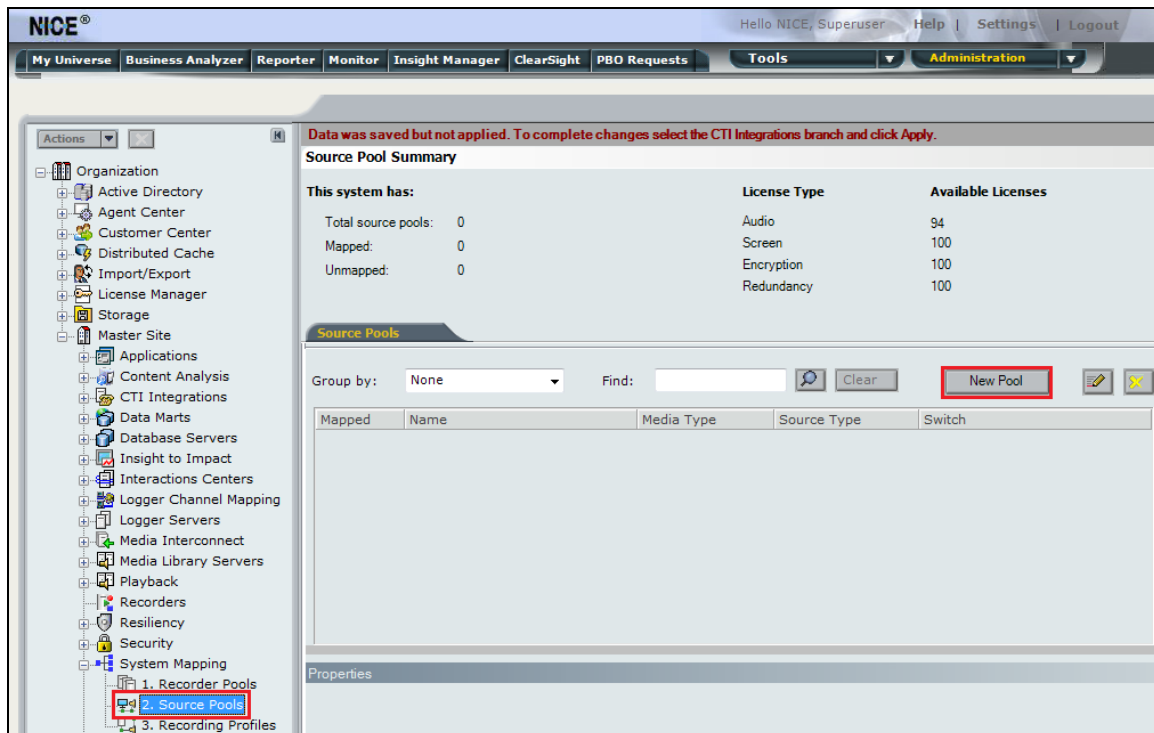
From the web browser navigate to **Master Site → System Mapping → Recorder Pools**. In the main window click on **New Pool**.



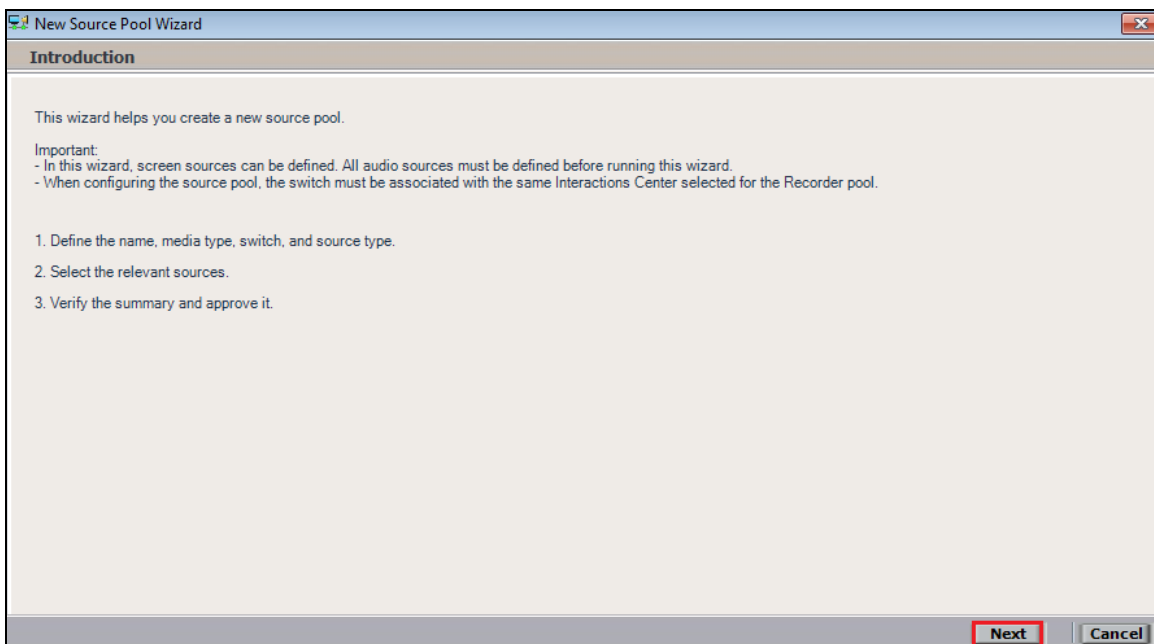
Enter a suitable **Name** for the **Recorder Pool** and select the **AIR-real** from the list of **Available Recorders** and click on **Update** to continue.



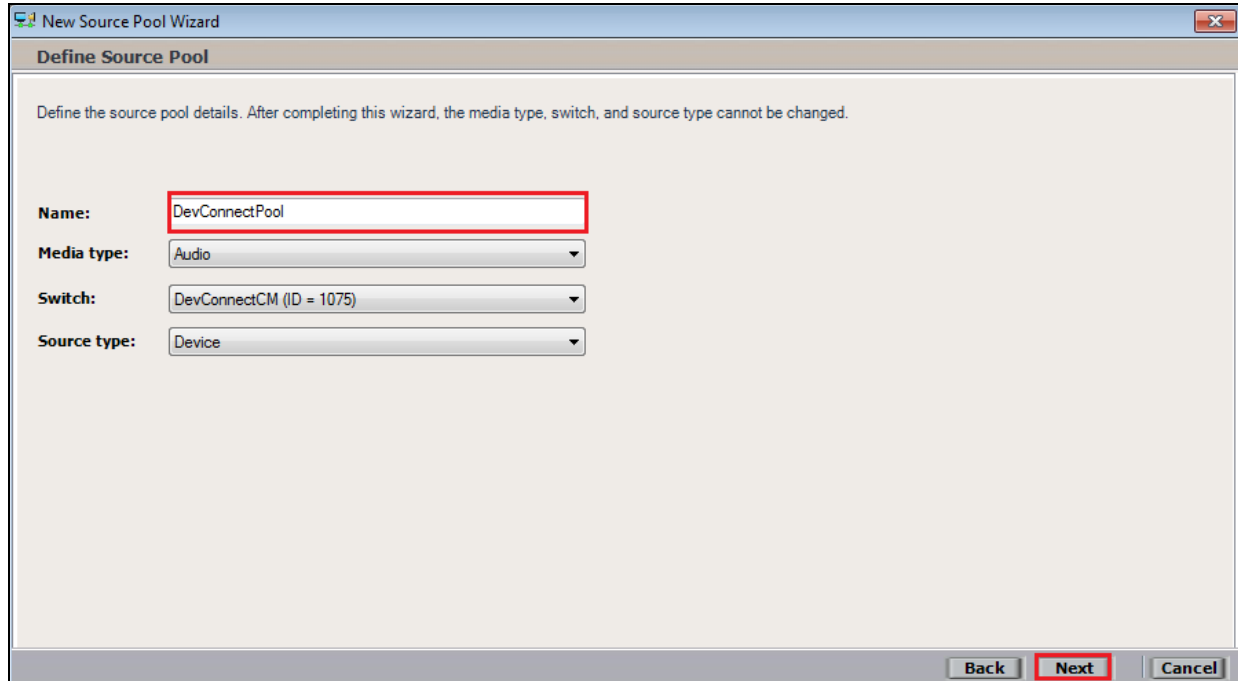
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



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' 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

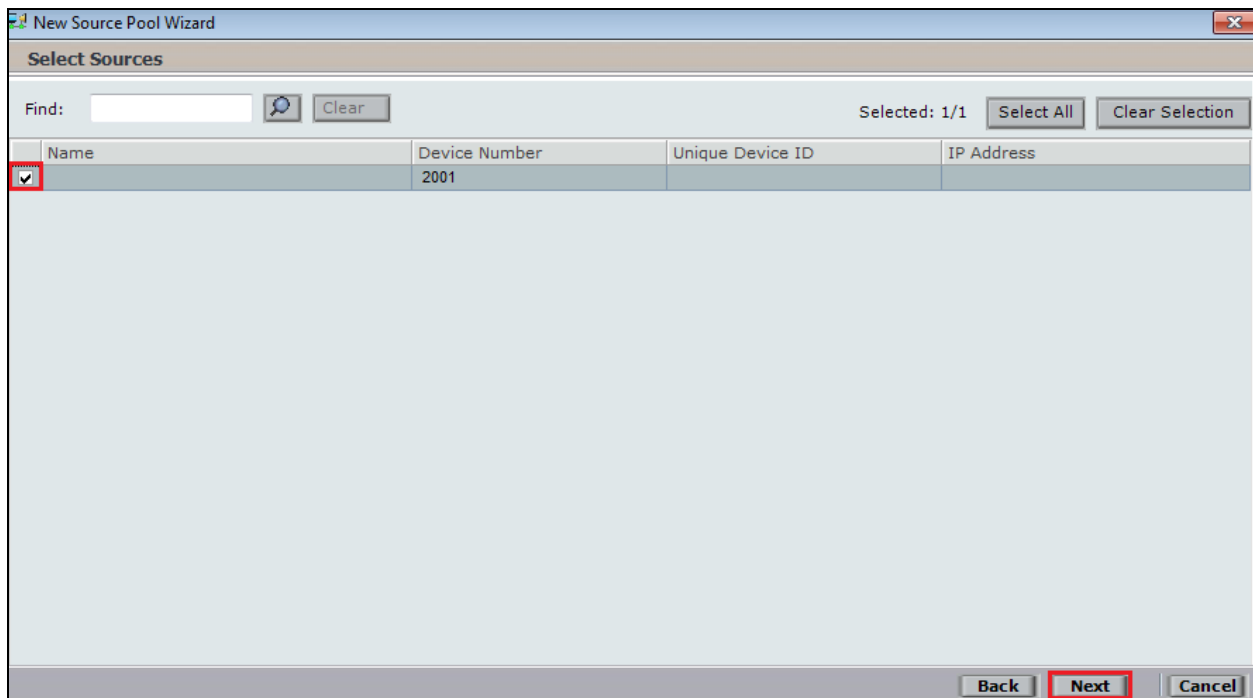
Media type: Audio

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.

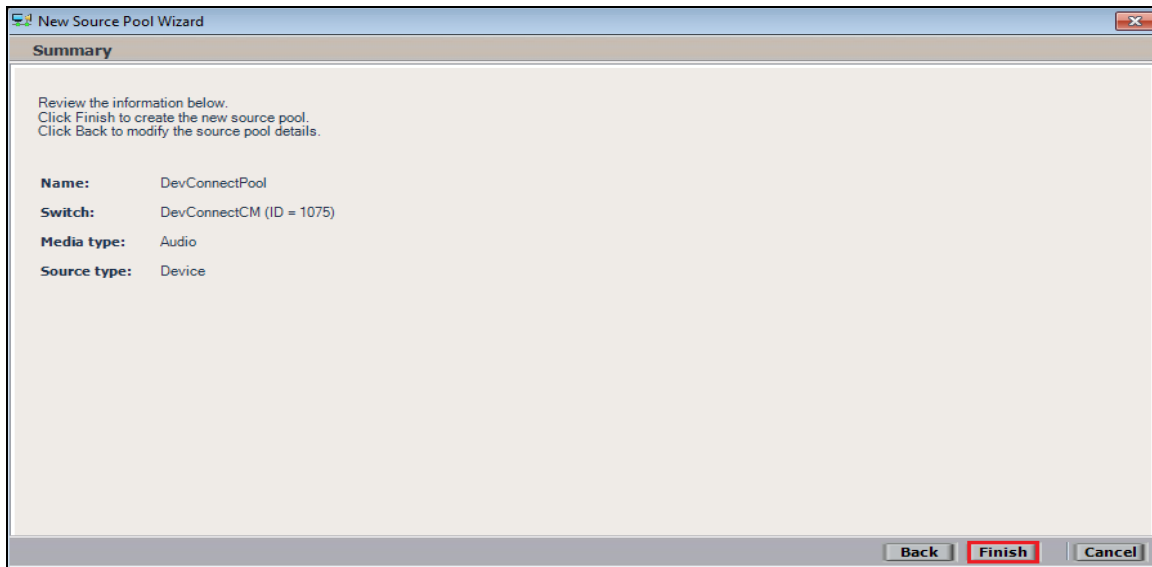
Find: Clear

Selected: 1/1 Select All Clear Selection

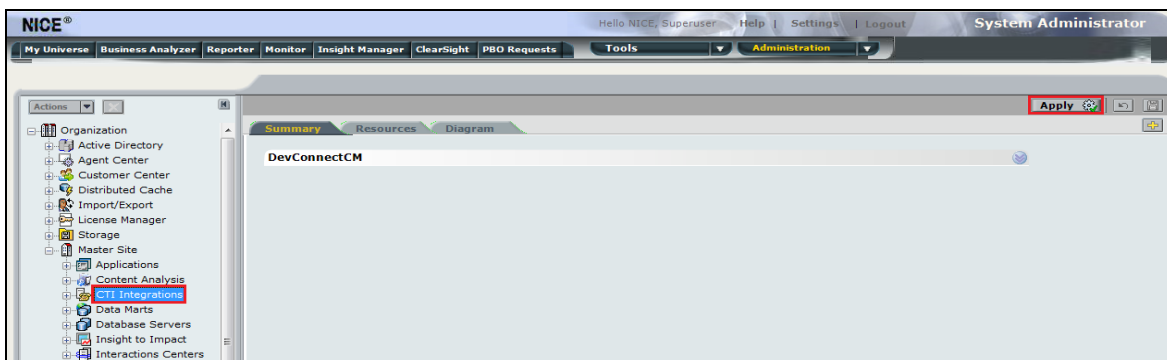
Name	Device Number	Unique Device ID	IP Address
<input checked="" type="checkbox"/>	2001		

Back Next Cancel

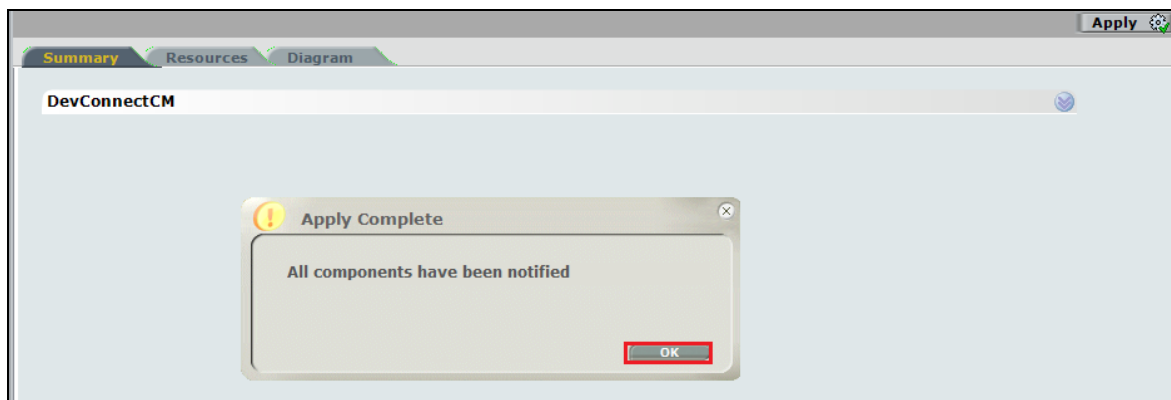
Click on **Finish** to complete the New Source Pool Wizard.



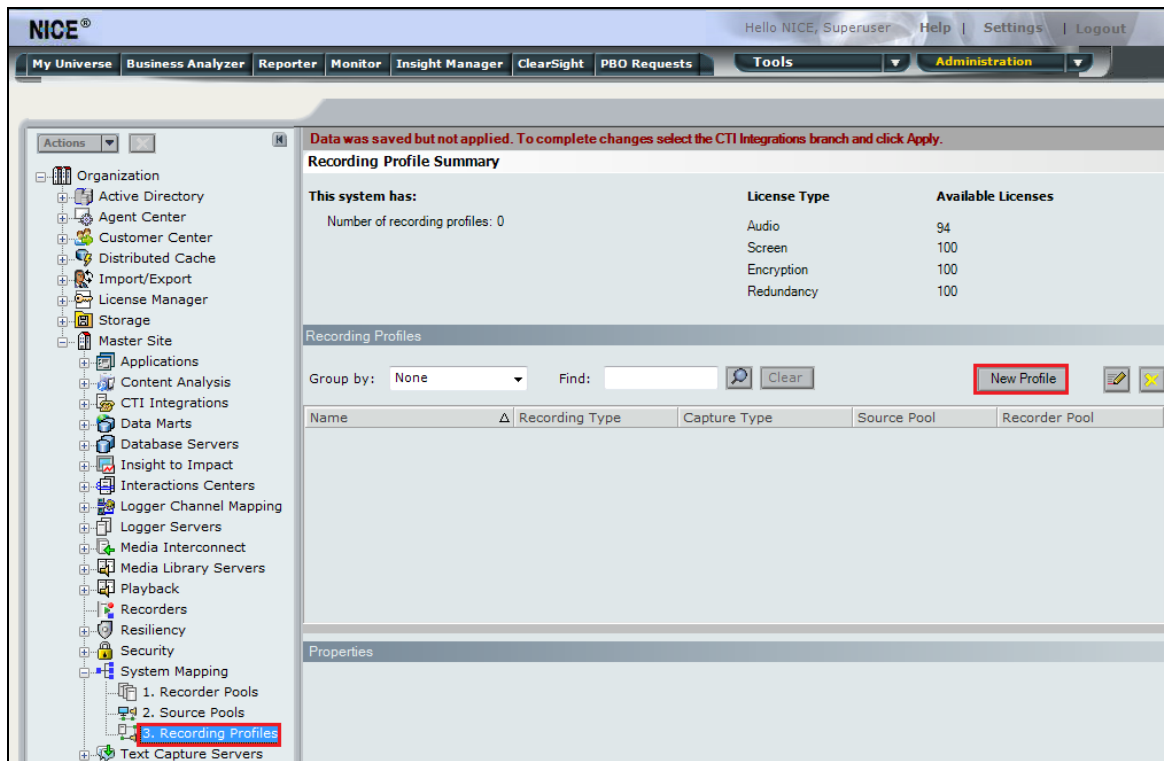
To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.



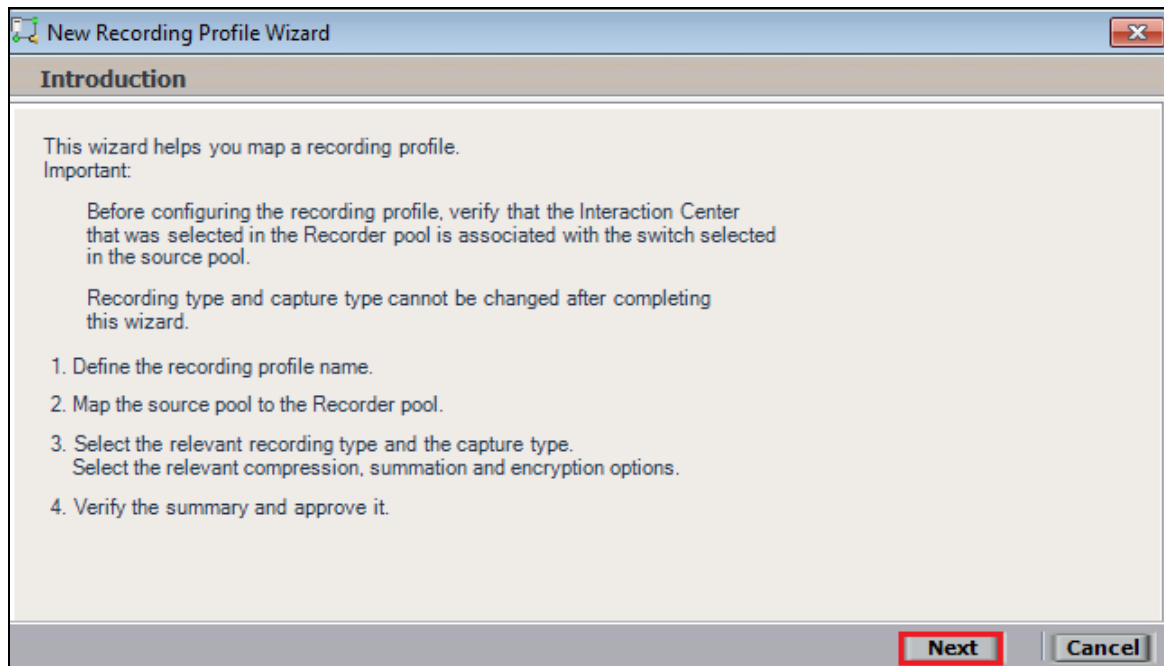
The following screen shows the changes were saved correctly. Click on **OK** to continue.



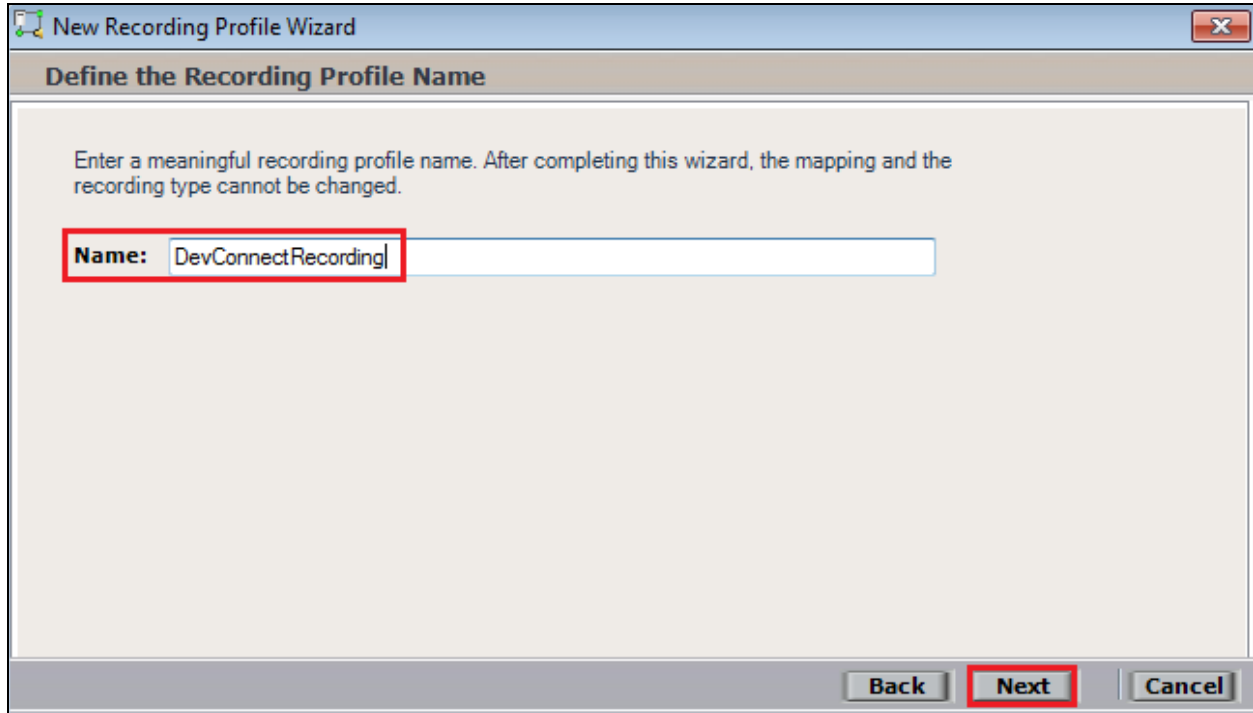
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



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

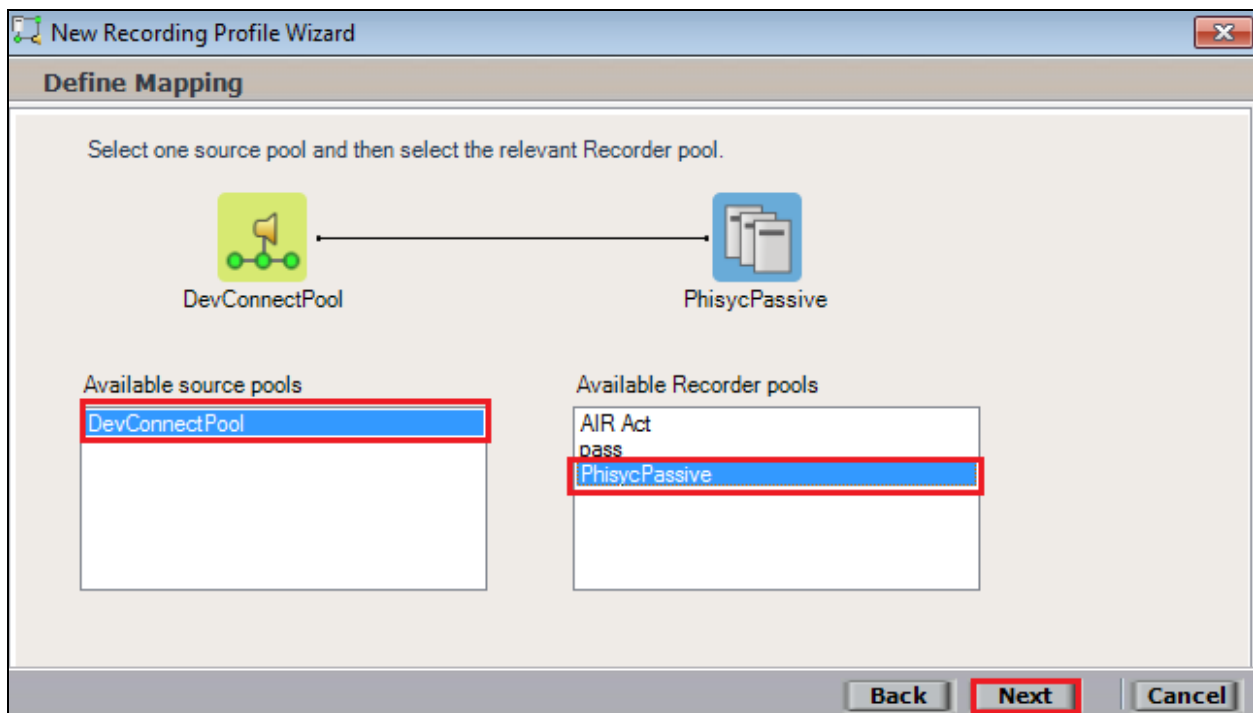


Enter a suitable **Name** for the Recording profile.



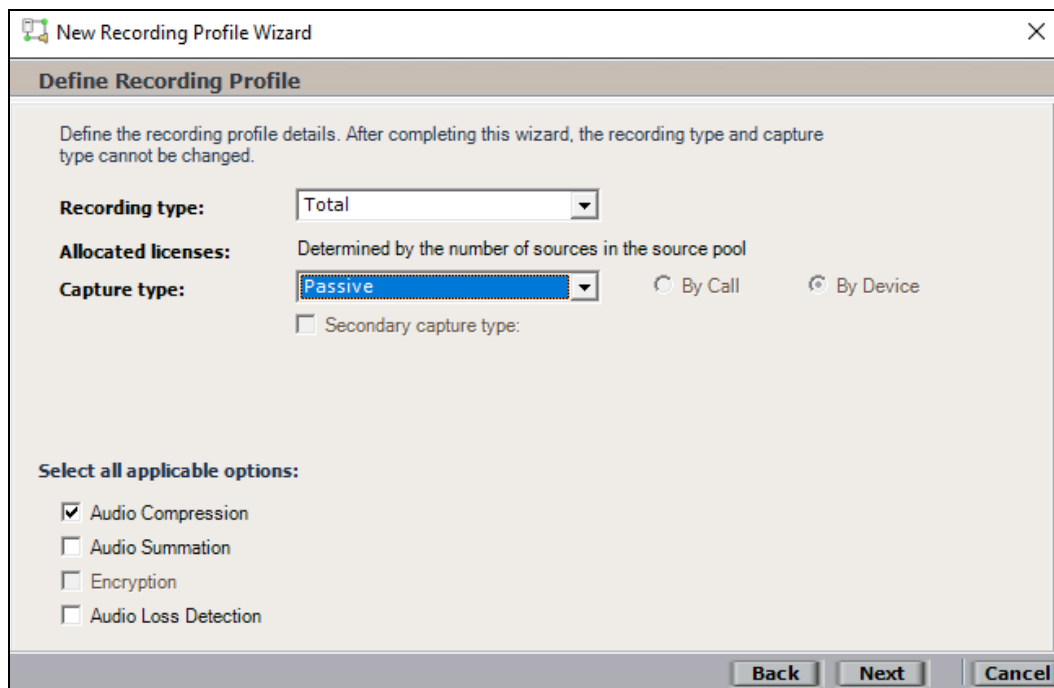
The screenshot shows the 'New Recording Profile Wizard' window with the title 'Define the Recording Profile Name'. The instruction text reads: 'Enter a meaningful recording profile name. After completing this wizard, the mapping and the recording type cannot be changed.' Below this, there is a text input 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 'DevConnectPool' (represented by a green icon) connected to 'PhisycPassive' (represented by a blue icon). Below the diagram, there are two lists: 'Available source pools' and 'Available Recorder pools'. In the 'Available source pools' list, 'DevConnectPool' is selected and highlighted with a red box. In the 'Available Recorder pools' list, 'PhisycPassive' is 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. **Audio Compression** is selected as default and can be left like this. Click on **Next** to continue.



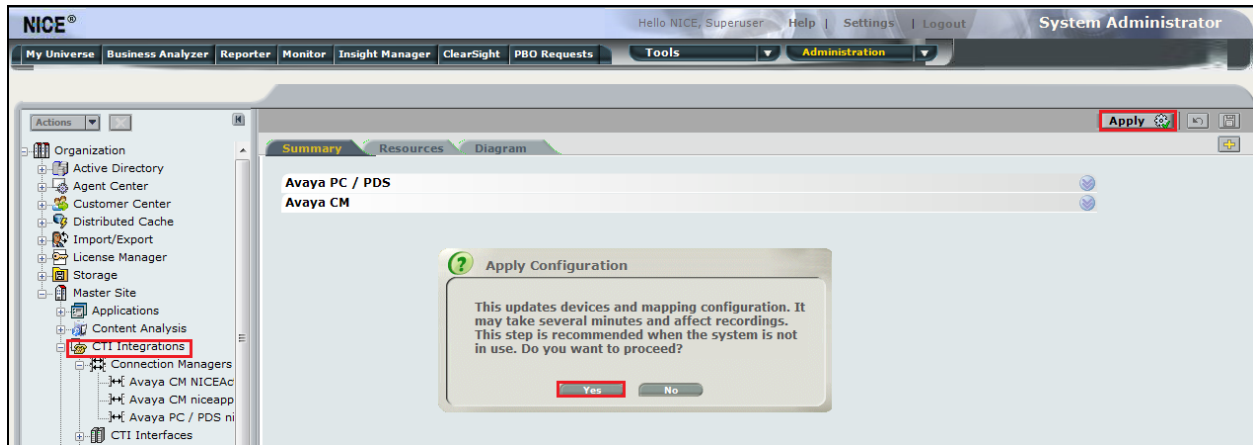
The screenshot shows the 'Define Recording Profile' step of the 'New Recording Profile Wizard'. The window title is 'New Recording Profile Wizard'. The main heading is 'Define Recording Profile'. Below the heading, a note states: 'Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.' The 'Recording type' is set to 'Total' in a dropdown menu. The 'Allocated licenses' are 'Determined by the number of sources in the source pool'. The 'Capture type' is set to 'Passive' in a dropdown menu. There are two radio buttons for 'By Call' and 'By Device', with 'By Device' being selected. A checkbox for 'Secondary capture type' is present and unchecked. Under the 'Select all applicable options:' section, there are four checkboxes: 'Audio Compression' (checked), 'Audio Summation' (unchecked), 'Encryption' (unchecked), and 'Audio Loss Detection' (unchecked). At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

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, a note states: 'Review the mapping information below. Click Finish to create the new recording profile. Click Back to modify the recording profile details.' The summary information is as follows: 'Name: DevConnectPool', 'Source pool: DEV-POOL', 'Recorder pool: AIR-Passive', 'Recording type: Total', 'Capture type: Passive', and 'Allocated licenses: Determined by the number of sources in the source pool'. Under the 'Select all applicable options:' section, there are four checkboxes: 'Audio Compression' (checked), 'Audio Summation' (unchecked), 'Encryption' (unchecked), and 'Audio Loss Detection' (unchecked). At the bottom, there are 'Back', 'Finish', and 'Cancel' buttons. The 'Finish' button is highlighted with a red box.

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	aes80vmpg	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**.

TSAPI Link Details

☐ Enable page refresh every 60 seconds

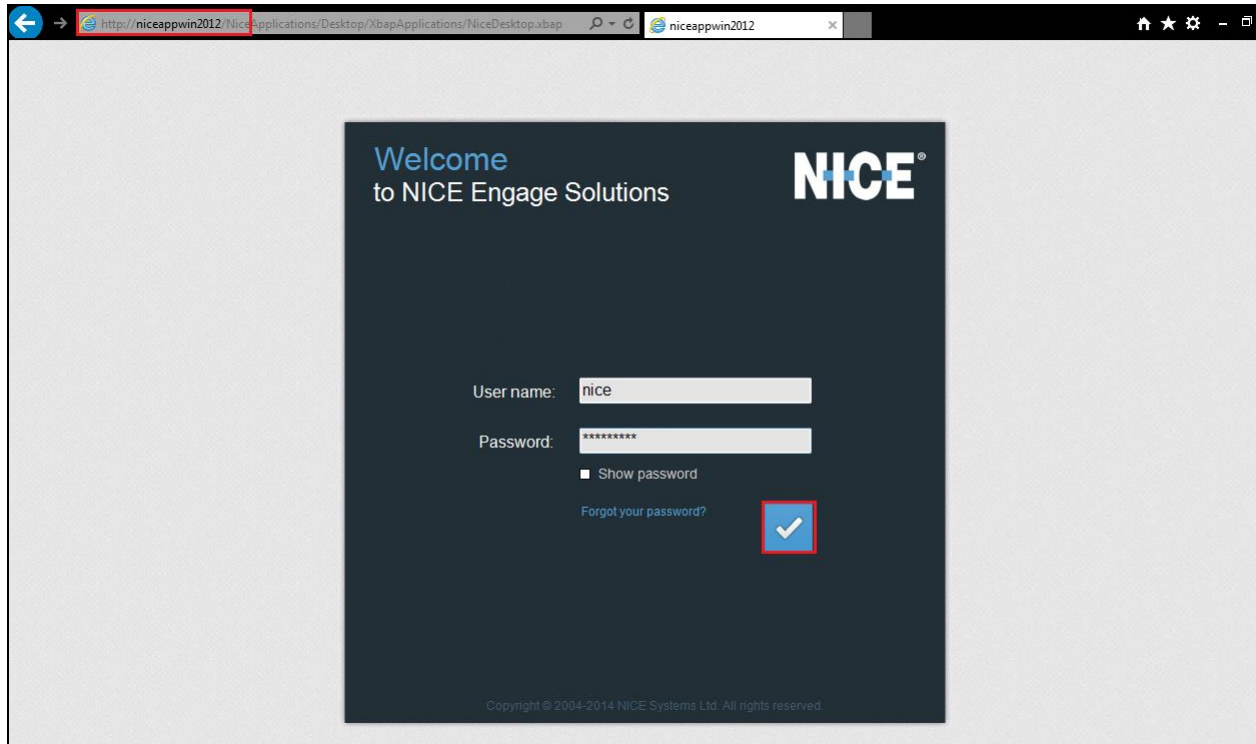
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm80vmpg	1	Talking	Wed Dec 5 10:53:21 2018	Online	18	8	15	15	30

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

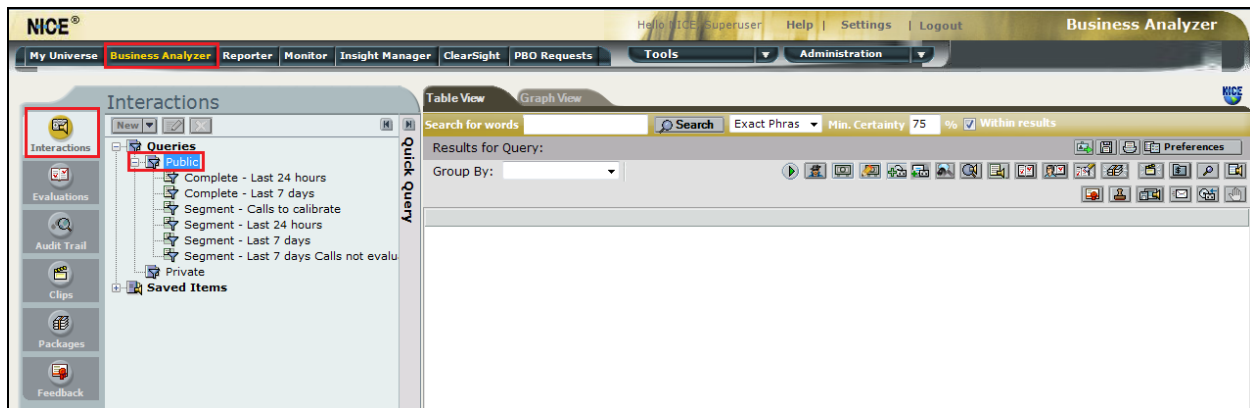
8.3. Verify calls are being recorded

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.

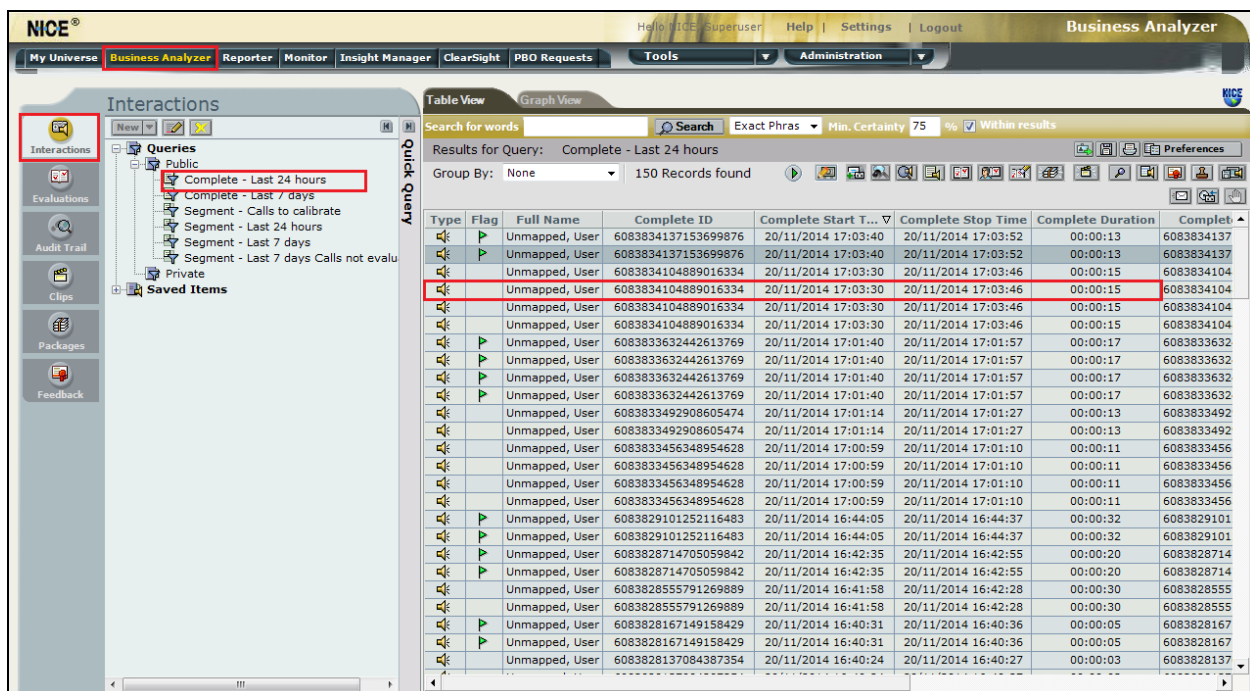
Open a browser session to the NICE Application Server as is shown below. Enter the proper credentials and click on **Login**.



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.



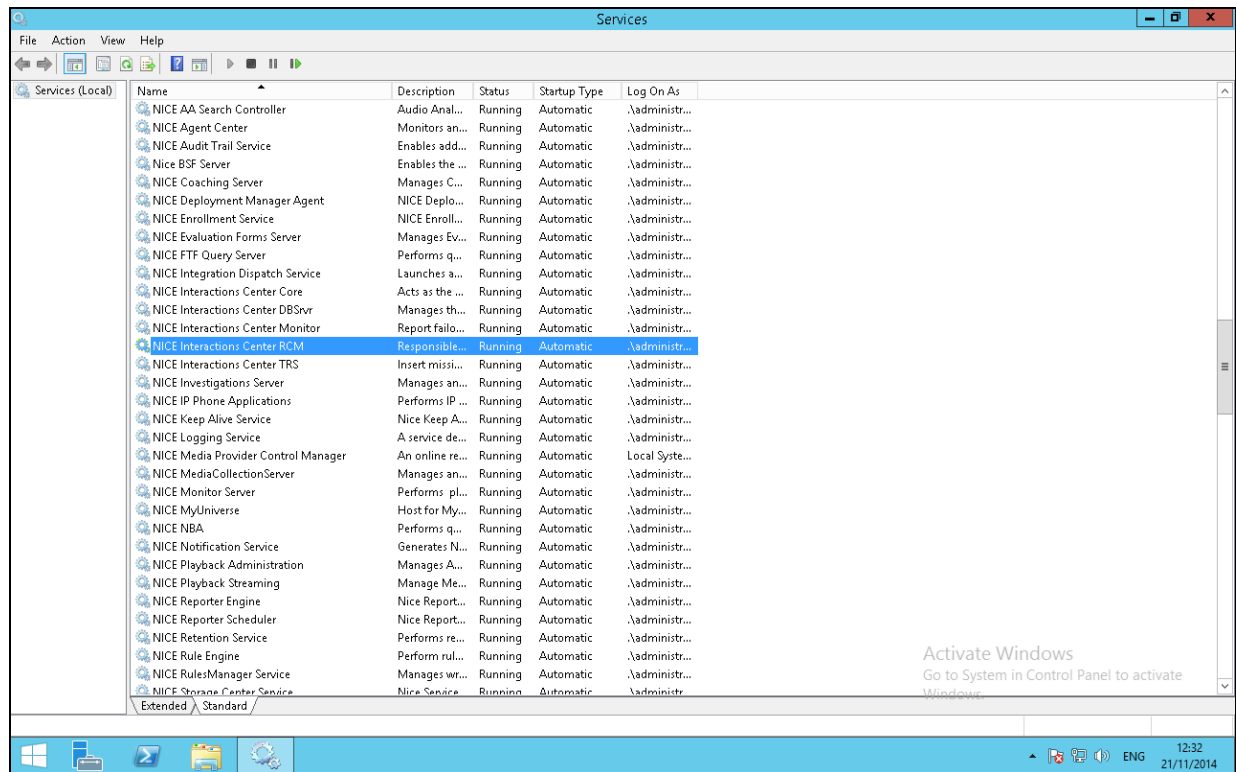
The NICE player is opened and the recording is presented for playback. Click on the **Play/Pause** icon highlighted below to play back the recording.

The screenshot shows the NICE Business Analyzer interface. The top navigation bar includes 'My Universe', 'Business Analyzer', 'Reporter', 'Monitor', 'Insight Manager', 'ClearSight', 'PBO Requests', 'Tools', and 'Administration'. The main area displays a timeline with various tracks for 'Summed', 'Customer', and 'Agent' events. A red box highlights the 'Play/Pause' button in the playback controls at the bottom. The bottom section shows a table of recordings with columns for 'Time Line', 'Segments', 'Comments', 'Recordings', 'Participants', 'Phrases', and 'Transcription'.

Time Line	Segments	Comments	Recordings	Participants	Phrases	Transcription
12:41:49	12:41:52	12:41:56	12:41:59	12:42:03	12:42:07	
Agent 1						

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 R6.10 to successfully interoperate with Avaya Aura® Communication Manager R8.0 using Avaya Aura® Application Enablement Services R8.0 to connect to using Passive Station Side VoIP with SMS to record calls. All feature functionality and serviceability test cases were completed successfully with 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® 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

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

Appendix

Avaya one-X® Agent Softphone

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

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

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

display station 2100	STATION	Page 3 of 5
<p>Conf/Trans on Primary Appearance? n</p> <p>Bridged Appearance Origination Restriction? n</p>		
<p>Call Appearance Display Format: disp-param-default</p> <p>IP Phone Group ID:</p> <p>Enhanced Callr-Info Display for 1-Line Phones? n</p>		
ENHANCED CALL FORWARDING		
	Forwarded Destination	Active
Unconditional For Internal Calls To: 1000		n
External Calls To: 1000		n
Busy For Internal Calls To:		n
External Calls To:		n
No Reply For Internal Calls To:		n
External Calls To:		n
SAC/CF Override: n		

display station 2100	STATION	Page 4 of 5
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5: manual-in	Grp:
2: call-appr	6: after-call	Grp:
3: call-appr	7: aux-work	RC: Grp:
4: auto-in	8:	
	Grp:	
voice-mail		

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		
Loss Group: 19	Time of Day Lock Table:	
	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

©2019 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.