



Application Notes for configuring NICE Engage Platform R6.3 to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 using Passive Station Side VoIP with SMS - 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 R6.3, an Avaya Aura® Session Manager R6.3, and Avaya Aura® Application Enablement Services R6.3 using Passive Station Side VoIP 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 R6.3 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R6.3, an Avaya Aura® Session Manager R6.3 and Avaya Aura® Application Enablement Services R6.3. The NICE Engage Platform was setup to use passive station-side VoIP recording with SMS to record both internal and external calls 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 phones 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 calls** – Test call recording for inbound calls to the Communication Manager from PSTN callers.
- **Outbound calls** – Test call recording for outbound calls from the Communication Manager to PSTN callers.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **EC500 Calls/Forwarded calls** - Test call recording for calls terminated on Avaya DECT handsets using EC500.
- **Call Park/Call Pickup** 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.
- **Failover testing** - The behaviour of NICE Engage Platform under different simulated failure conditions on the Avaya platform will also be observed.

2.2. Test Results

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

Observations:

1. The recording of DECT and other similar devices is not supported using passive recording. This will work for one DECT call at a time as it is the base station that is being monitored, if there is more than one DECT handset in use then only one still gets recorded. The same will be true for any device such as digital or analog sets that do not have IP addresses.

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.

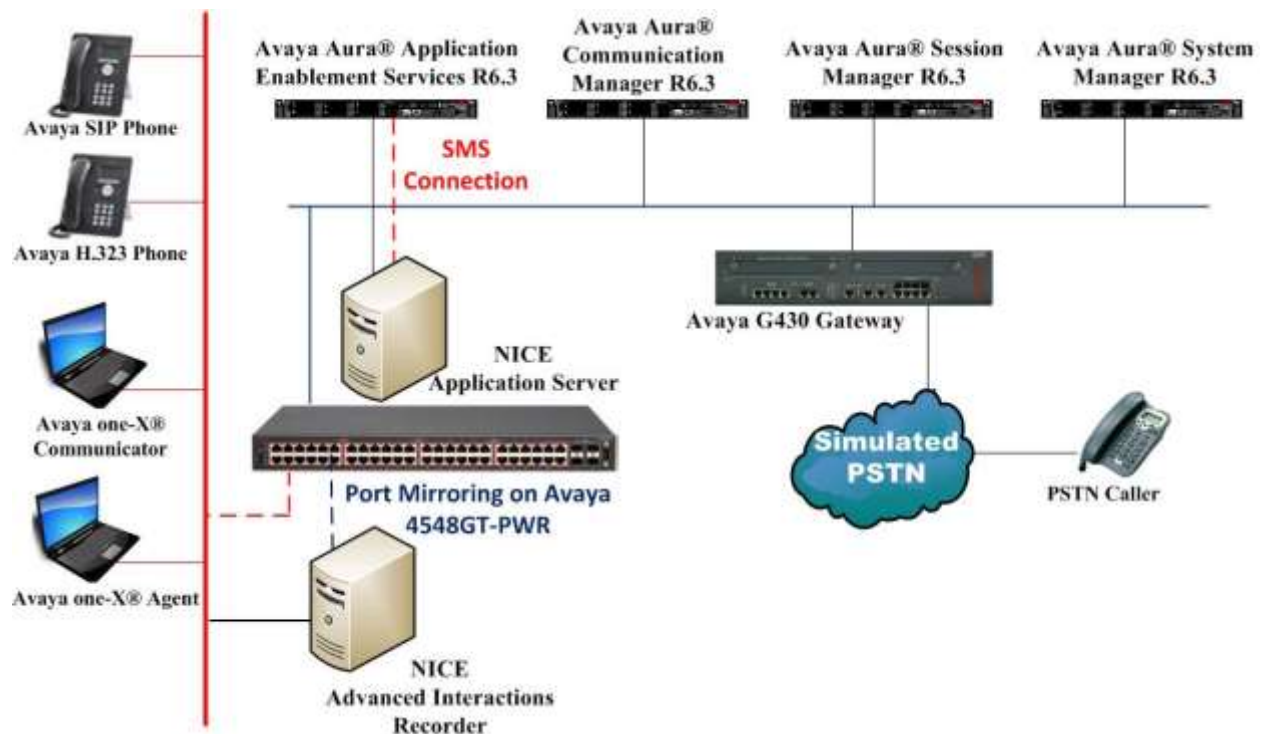


Figure 1: Connection of NICE Engage Platform R6.3 with Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3 and Avaya Aura® Application Enablement Services R6.3

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	R6.3.10 [Build 6.3.0.8.5682-6.3.8.4514] [SW Update Rev 6.3.10.7.2656]
Avaya Aura® Session Manager running on Virtual Server	R6.3 (SP9) 6.3.9.0.639011
Avaya Aura® Communication Manager running on Virtual Server	R6.3 SP8 R016x.03.0.124.0 03.0.124.0-21588
Avaya Aura® Application Enablement Services running on Virtual Server	R6.3 Build No – 6.3.3.1.10-0
Avaya G430 Gateway	33.12.0 /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	96xx H.323 Release 6.4014U
Avaya 9620 H323 Deskphone	R3.186A
Avaya 9641 SIP Deskphone	96x1-IPT-SIP-R6_4_1-081114
Avaya 9630 SIP Deskphone	R2.6.12.1
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Avaya one-X® Communicator SIP	R6.2.4.07-FP4
Avaya one-X® Agent	R 2.5.50022.0
NICE Engage Platform <ul style="list-style-type: none">- NICE Application Server- Advanced Interactions Recorder- NICE NDM Server	R6.3

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** and AES (**aes63vmpg**).

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM100	10.10.40.34		
aes63vmpg	10.10.40.30		
default	0.0.0.0		
g430	10.10.40.15		
procr	10.10.40.31		

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 **aes63vmpg**.
- **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:	aes63vmpg	*****	y	idle			
2:							
3:							

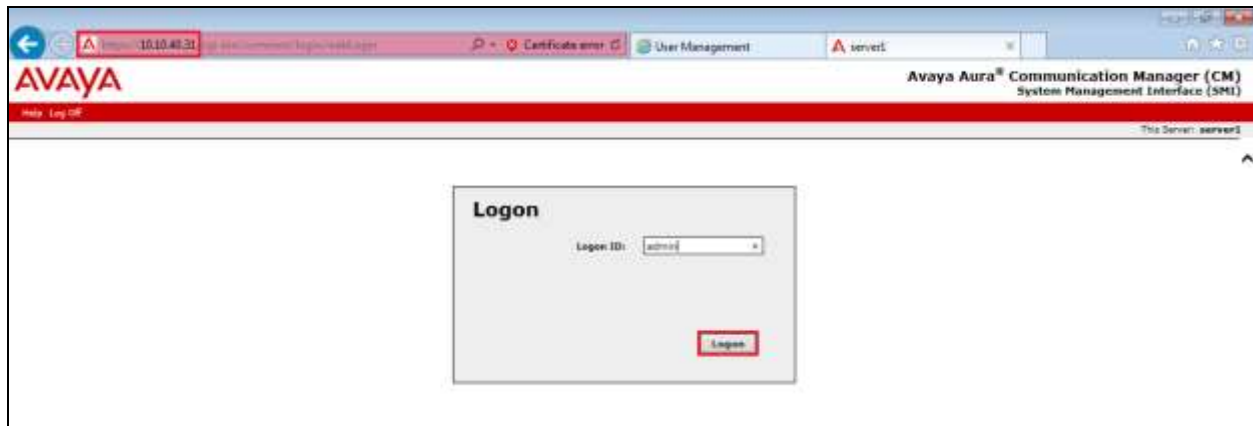
5.4. Configure CTI Link for TSAPI Service

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: aes63vmpg			

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 **Unprivileged Administrator** as shown below. Click on **Submit** when finished.

The screenshot displays the Avaya Administration web interface. The left sidebar contains a navigation menu with categories: Server Configuration, Server Upgrades, Data Backup/Restore, and Security. The 'Security' category is expanded, and 'Administrator Accounts' is highlighted with a red box. 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 within it, the 'Unprivileged Administrator' option is also selected. Other options include Privileged Administrator, SAT Access Only, Web Access Only, CDR Access Only, Business Partner Login (dadmin), Business Partner Craft Login, and Custom Login. Below these are four rows of actions: 'Change Login', 'Remove Login', 'Lock/Unlock Login', and 'Add Group', each with a 'Select Login' dropdown menu. The 'Remove Group' option has a 'Select Group' dropdown menu. At the bottom of the form, the 'Submit' button is highlighted with a red box, along with a 'Help' button.

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: Unprivileged 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

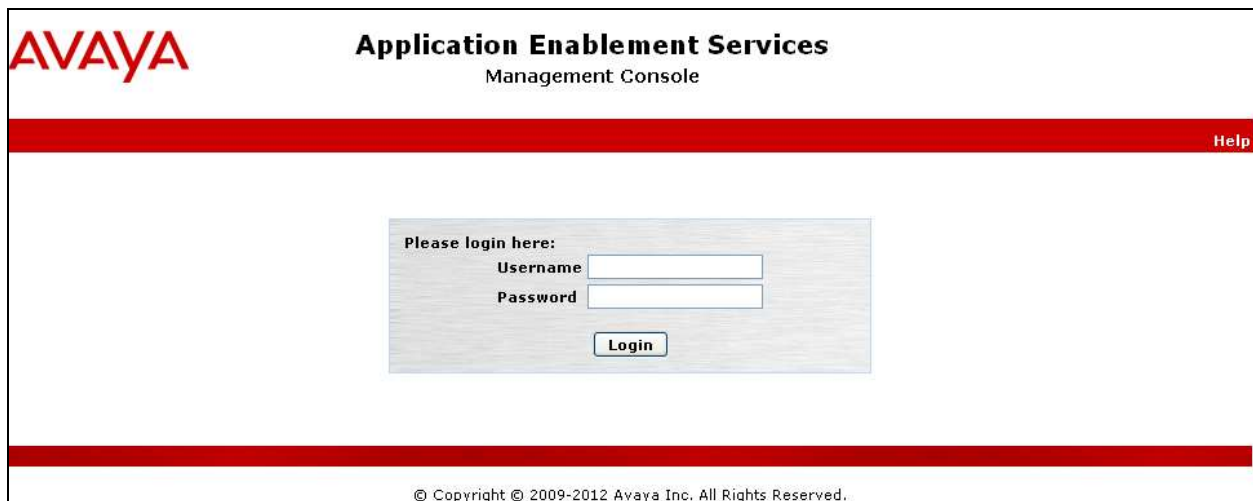
6. Configure Avaya Aura® Application Enablement Services

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
- Enable TSAPI Ports
- Create CTI User
- Set Up Security Database on AES
- Associate Devices with CTI User

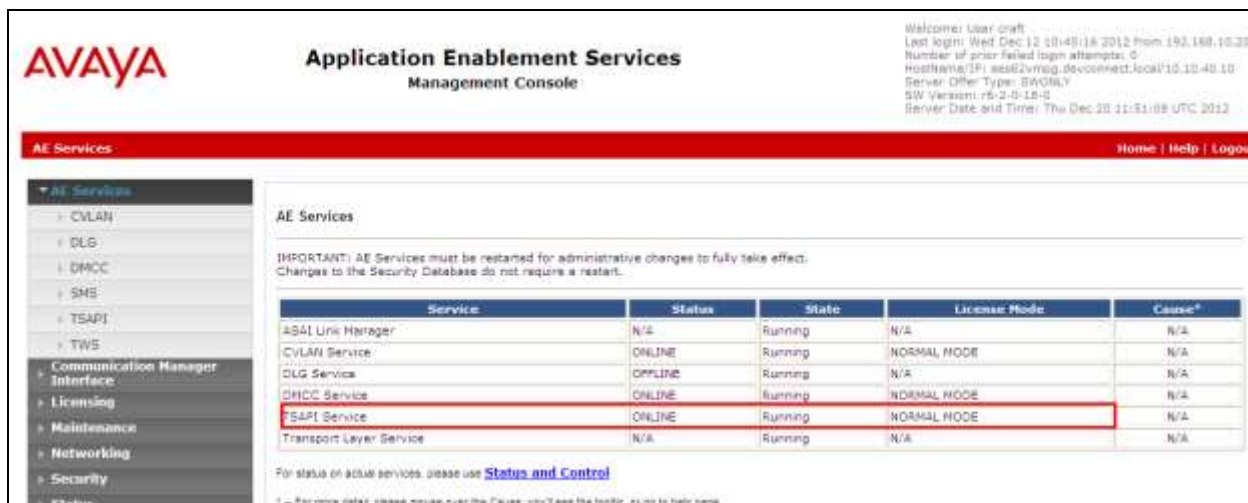
6.1. Verify Licensing

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 screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." is displayed.

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



AVAYA Application Enablement Services Management Console

Welcome! User: craft
Last login: Wed Dec 12 10:48:16 2012 from 193.168.10.208
Number of prior failed login attempts: 0
HostName/IP: aes63vmag.devconnect.local/10.10.40.10
Server Offer Type: SWONLY
SW Version: r6-2.0-18-0
Server Date and Time: Thu Dec 20 11:51:08 UTC 2012

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 ¹
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	ONLINE	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

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

¹ - For more detail, please mouse over the Cause; you'll see the tooltip, or go to help page.

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: craft
Last login: Thu Nov 14 20:22:12 2012 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMFG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.8.212-0
Server Date and Time: Tue Dec 3 15:33:26 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

CM63VMFG Add Connection

Connection Name	Processor Element	Max Period	Number of Active Connections

Edit Connection Edit PE/CN 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.

AVAYA Application Enablement Services Management Console

Welcome: User: cm63
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.113-0
Server Date and Time: Tue Dec 3 15:35:47 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Connection Details - CM63vmpg

Switch Password: [REDACTED]
Confirm Switch Password: [REDACTED]
Tag Period: 30 Minutes (1 - 72)
SSL: [X]
Processor Ethernet: [X]
Apply Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown, see screen at the bottom of page 12). 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.

AVAYA Application Enablement Services Management Console

Welcome: User: cm63
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.113-0
Server Date and Time: Tue Dec 03 15:36:31 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit Processor Ethernet IP - CM63vmpg

10.10.40.31 Add/Edit Name or IP

Name or IP Address	Status
10.10.40.31	In Use

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.



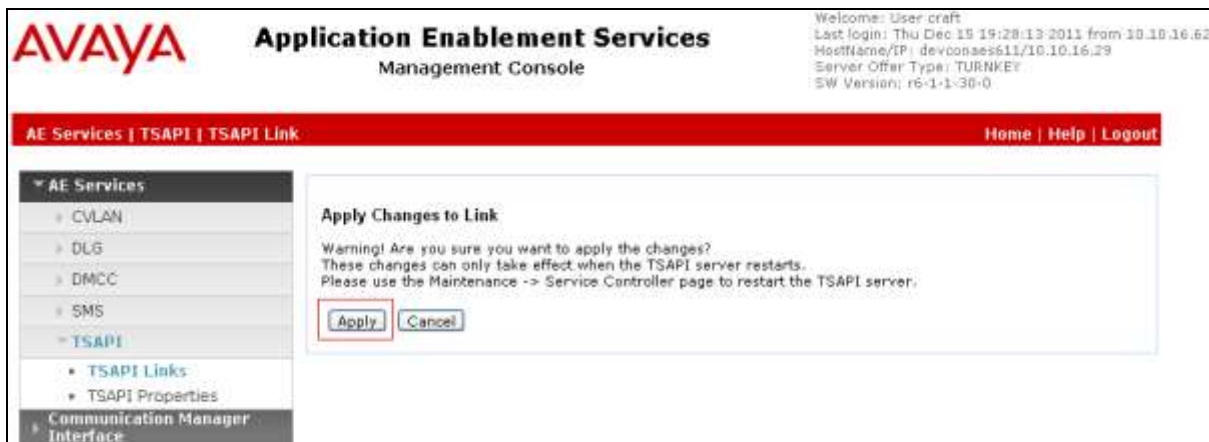
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM63VMPG**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



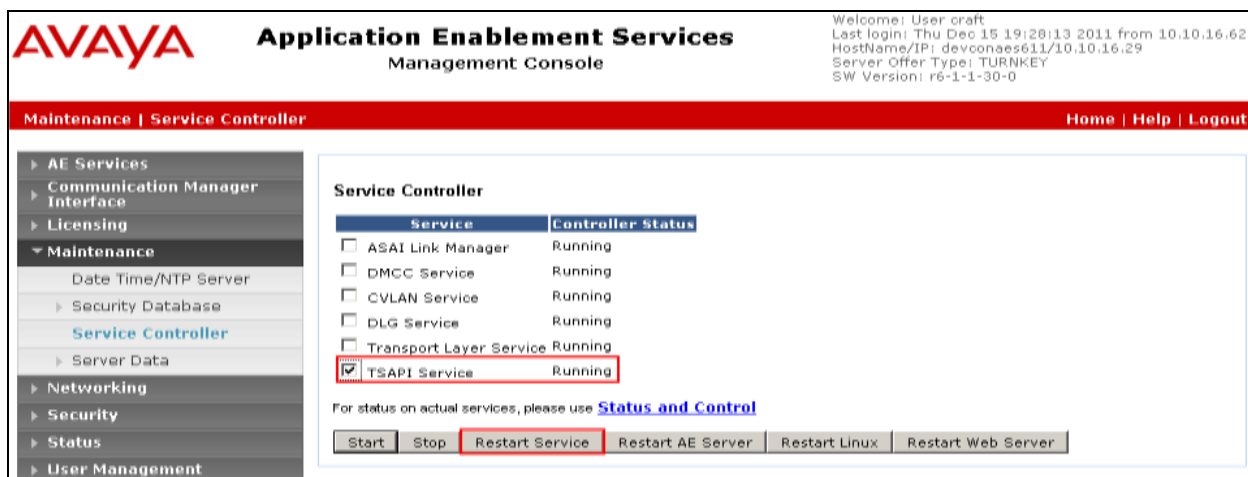
Another screen appears for confirmation of the changes made. Choose **Apply**.



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



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



6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the Tlink Group in **Section 6.7.2**.

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 is a sidebar menu with various categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. The Security section is expanded, showing sub-items like Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, and Security Database. The Security Database is further expanded to show Control, CTI Users, Devices, Device Groups, and Tlinks, which is highlighted with a red box. The main content area is titled "Tlinks" and contains a "Tlink Name" section with two radio buttons. The first option, "AVAYA#CM63VMPG#CSTA#AES63VMPG", is selected and highlighted with a red box. The second option is "AVAYA#CM63VMPG#CSTA-S#AES63VMPG". Below the radio buttons is a "Delete Tlink" button.

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. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.1**.

AVAYA Application Enablement Services Management Console

Last login: Thu Nov 27 12:26:42 2014 from 10.10.10.10
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.10.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Dec 01 16:06:19 GMT 2014
HA Status: Not Configured

Networking | Ports Home | Help | Logout

Ports

CVLAN Ports

Unencrypted TCP Port	9999	Enabled Disabled
Encrypted TCP Port	9998	Enabled Disabled

DLG Port

TCP Port	5678
----------	------

TSAPI Ports

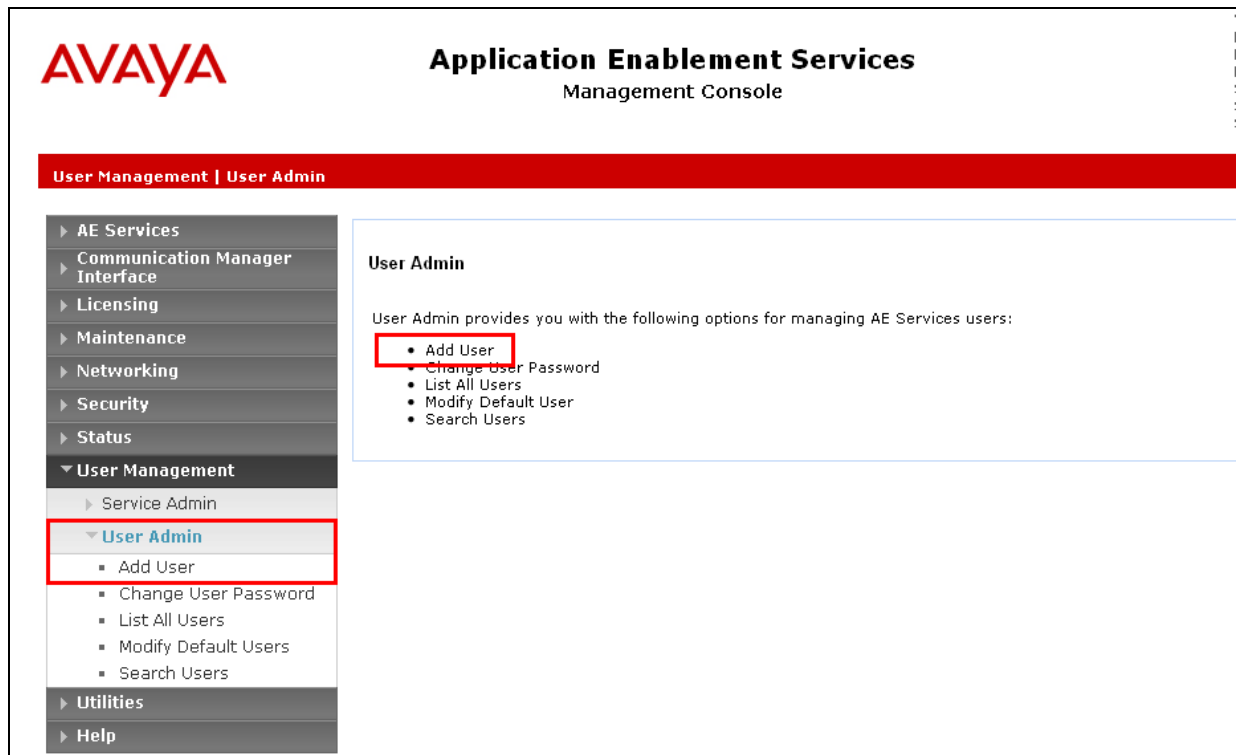
TSAPI Service Port	450	Enabled Disabled
Local TLINK Ports		
TCP Port Min	1024	
TCP Port Max	1039	
Unencrypted TLINK Ports		
TCP Port Min	1050	
TCP Port Max	1065	
Encrypted TLINK Ports		
TCP Port Min	1066	
TCP Port Max	1081	

DMCC Server Ports

Unencrypted Port	4721	Enabled Disabled
Encrypted Port	4722	Enabled Disabled
TR/S7 Port	4723	Enabled Disabled

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

Welcome: user root
 Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.30
 Number of error failed login attempts: 0
 HostName/IP: AES63VMFG/10.10.60.30
 Server Offer Type: VIRTUAL_APPLANCE_ON_VMWARE
 SW Version: 6.3.1.1.10-0
 Server Date and Time: Mon Dec 01 16:03:36 GMT 2014
 HA Status: Not Configured

User Management | User Admin | List All Users

Home | Help | Logout

Left Sidebar: All Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (selected), Service Admin, User Admin (selected), Add User (selected), Change User Password, List All Users, Modify Default Users, Search Users, Utilities, Help.

Edit User Form:

- * User Id: nice
- * Common Name: nice
- * Surname: nice
- User Password:
- Confirm Password:
- Admin Note:
- Avaya Role: None
- Business Category:
- Car Licenses:
- CM Home:
- Cx Home:
- CT User: Yes
- Department Number:
- Display Name:
- Employee Number:
- Employee Type:

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

Left Sidebar: User Admin (selected), Add User, Change User Password, List All Users, Modify Default Users, Search Users, Utilities, Help.

Form Fields:

- CM Home:
- Cx Home:
- CT User: Yes
- Department Number:
- Display Name:
- Employee Number:
- Employee Type:
- Enterprise Handle:
- Given Name:
- Home Phone:
- Home Postal Address:
- Initials:
- Labeled URI:
- Mail:
- MIM Home:
- Mobile:
- Organization:
- Pager:
- Preferred Language: English
- Room Number:
- Telephone Number:

Buttons: Apply Changes, Cancel Changes

6.7. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created 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
asc	asc	NONE	NONE
cube	cube	NONE	NONE
emc	emc	NONE	NONE
jacada	jacada	NONE	NONE
nice	nice	NONE	NONE
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.

User Profile:	User ID	Common Name	Worktop Name	Unrestricted Access
	nice	nice	NONE	<input checked="" type="checkbox"/>

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

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.
- **Proxy Log Destination** — Use the default destination **/var/log/avaya/aes/ossicm.log** for the CM Proxy Trace logs on the AE Server.
- **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**.

AE Services

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

SMS Properties

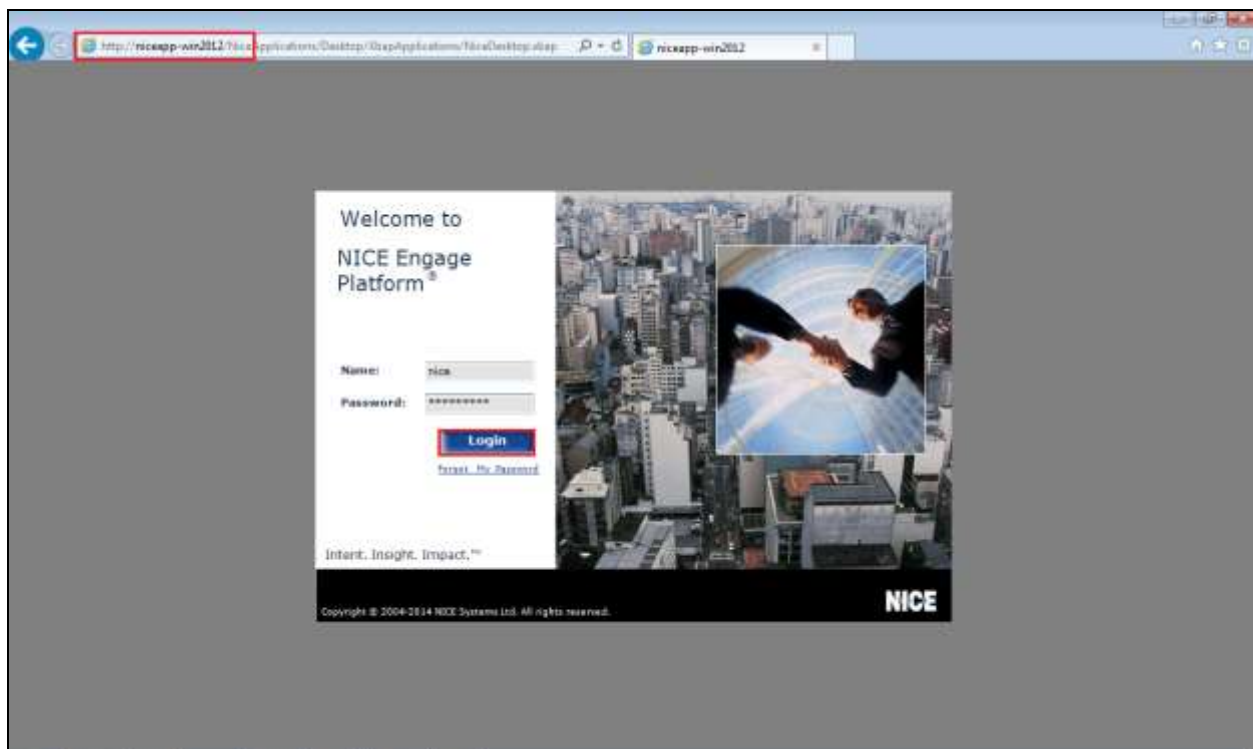
Default CM Host Address	10.10.40.31	
Default CM Admin Port	5022	
CM Connection Protocol	SSH	
SMS Logging	NORMAL	
SMS Log Destination	apache	
CM Proxy Trace Logging	NONE	
Max Sessions per CM	5	
Proxy Shutdown Timer	1800	seconds
SAT Login Keepalive	180	seconds
CM Terminal Type	OSSIZ	
Proxy Log Destination	/var/log/avaya/aes/ossicm.log	

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

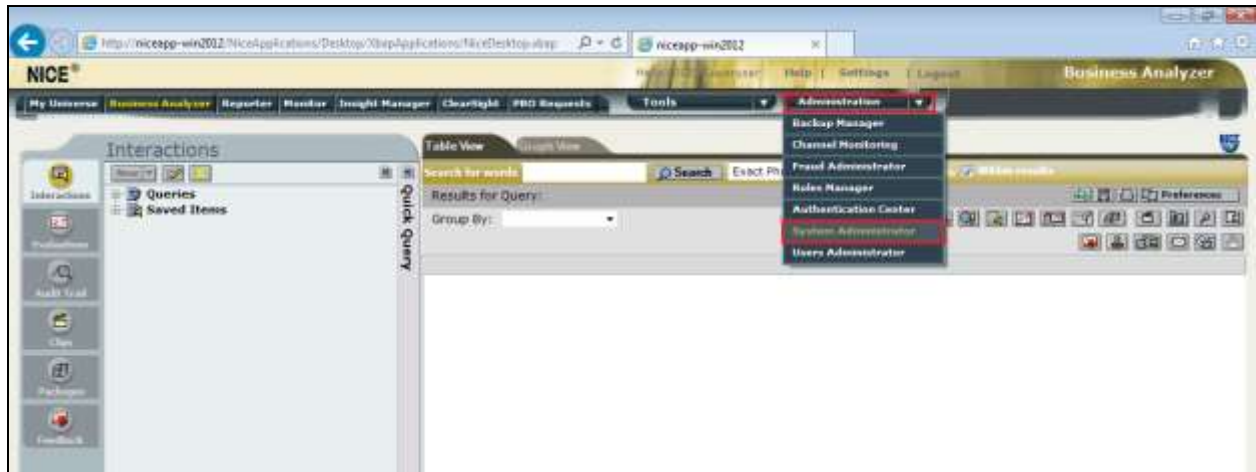
7. Configure NICE Engage Platform

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**.

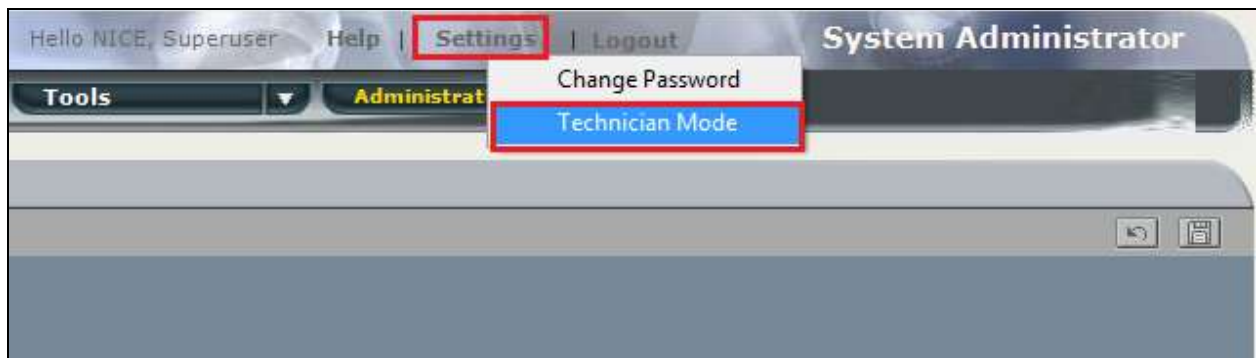
The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya Solution. All configuration of the NICE Engage Platform for connection with the AES is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser as shown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

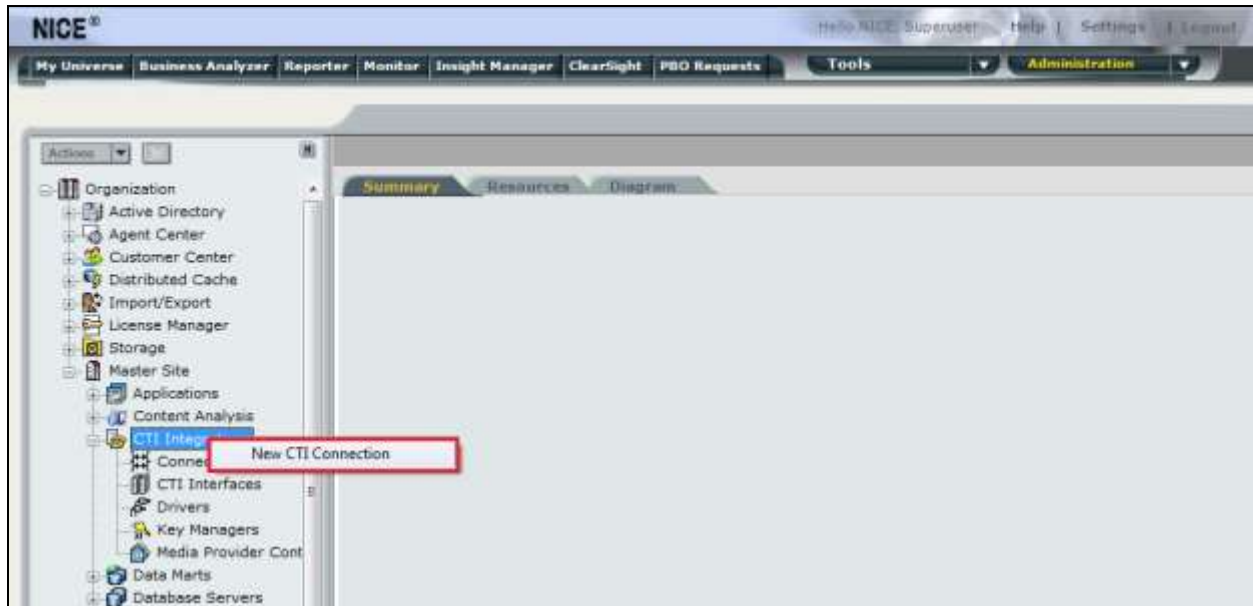


Before any changes can be made, switch to Technician Mode by clicking into Settings at the top of the screen as shown below.

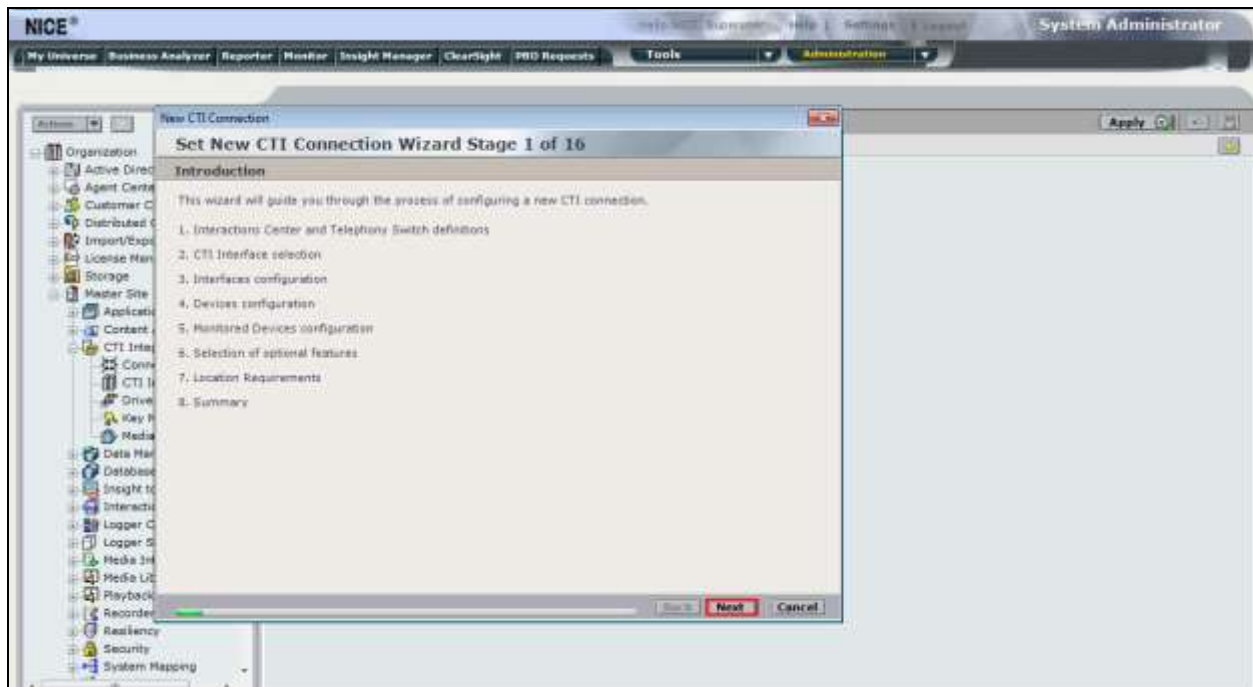


7.1. New CTI Connection

Navigate to **Master Site** → **CTI Integration** in the left window then right-click on CTI Integration and select **New CTI Connection** as shown below.

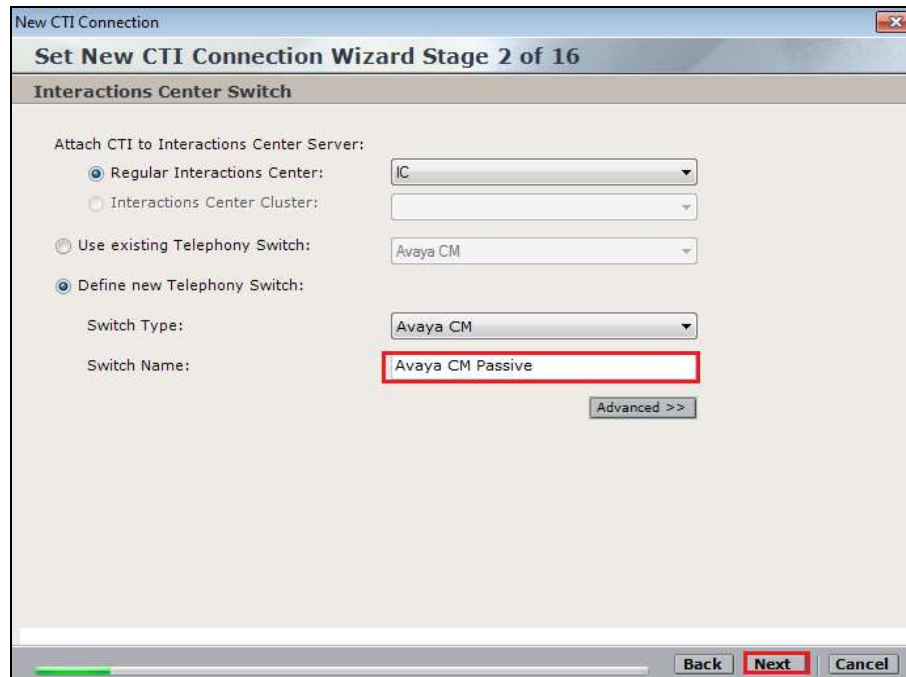


The **New CTI Connection Wizard** is opened and this will go through the 16 steps required to setup the connection to the AES for DMCC Service Observe and Single Step Conference type of call recording. Click on **Next** to continue.



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.



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.



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

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 16

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	
LoginID	
Password	
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

Back Next Cancel

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

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 16

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	
LoginID	
Password	
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

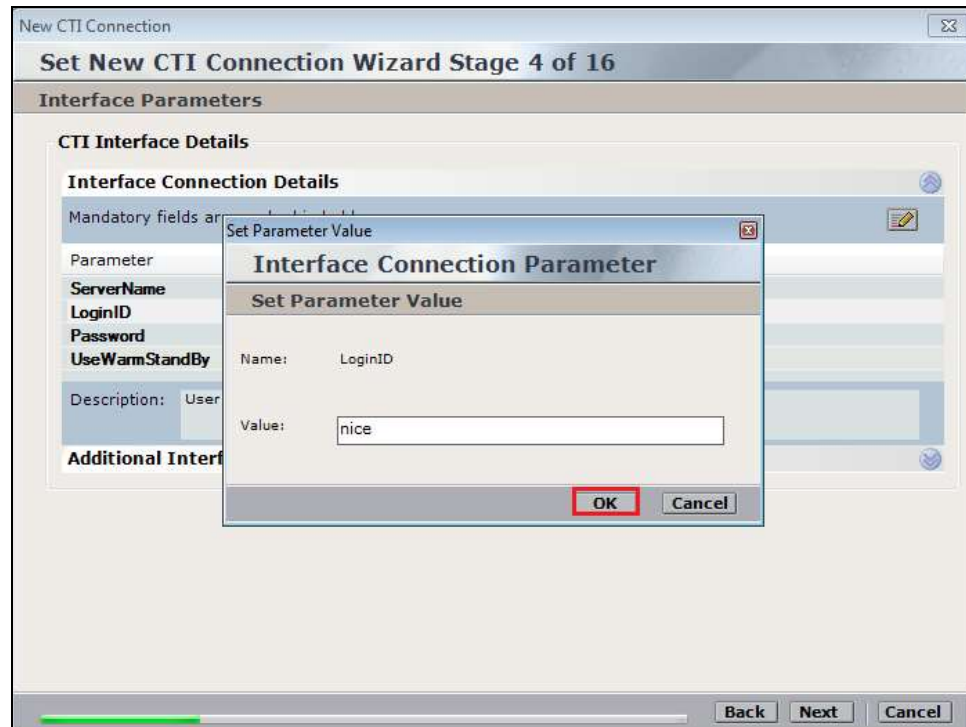
Name: ServerName

Value: AVAYA#CM63VMPG#CSTA#AES63VMPG

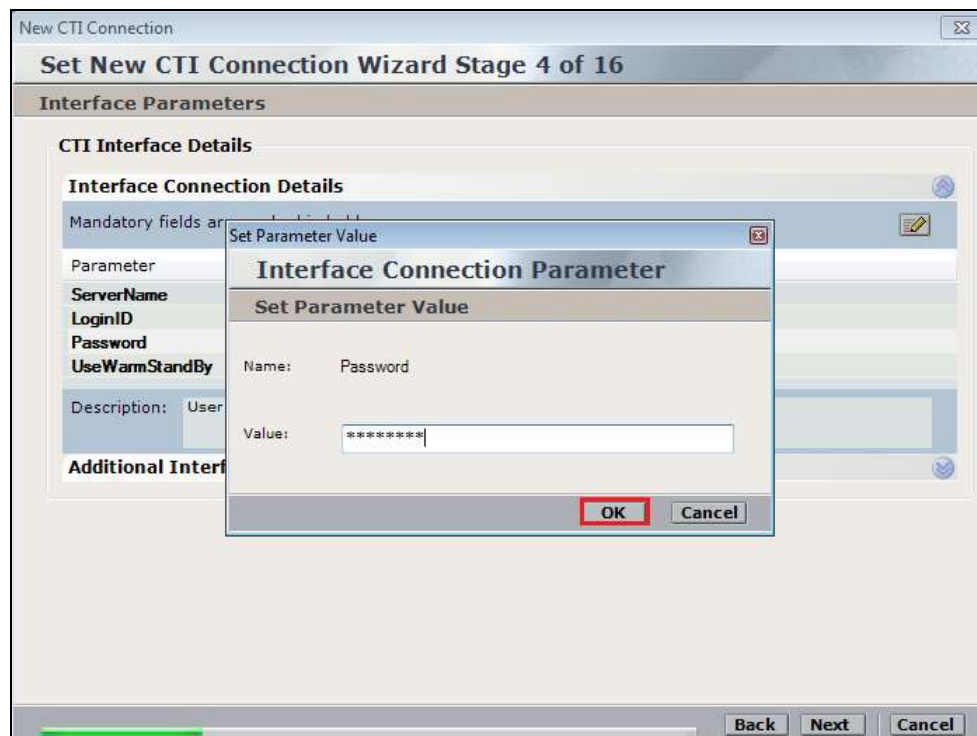
OK Cancel

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.

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. Below the table is a description field and an 'Additional Interface Parameters' section. At the bottom, the 'Next' button is highlighted with a red box.

Parameter	Value
ServerName	AVAYA#CM63VMPPG#CSTA#AES63VMPPG
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**.

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. Below the table is a description field and an 'Additional Interface Parameters' section. At the bottom, the 'Next' button is highlighted with a red box.

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**.

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

Set Parameter Value

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

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

Name: SmsHostIpAddress

Value: 10.10.40.30

OK Cancel

Back Next Cancel

As before enter the username that was created in **Section 5.5** and click on **OK**.

New CTI Connection

Set New CTI Connection Wizard

VoIP Mapping

VoIP Mapping Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter

SmsRequestTimeoutInSec

UserName

Password

UseWarmStandbyFeature no

Description: Username for the CM (mylogin@cmserveraddr).

Additional Interface Parameters

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

Name: UserName

Value: nicecm

OK Cancel

Back Next Cancel

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

New CTI Connection

Set New CTI Connection Wizard

VoIP Mapping

VoIP Mapping Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter

SmsRequestTimeoutInSec

UserName

Password

UseWarmStandbyFeature

Description: Password for the CM.

Additional Interface Parameters

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

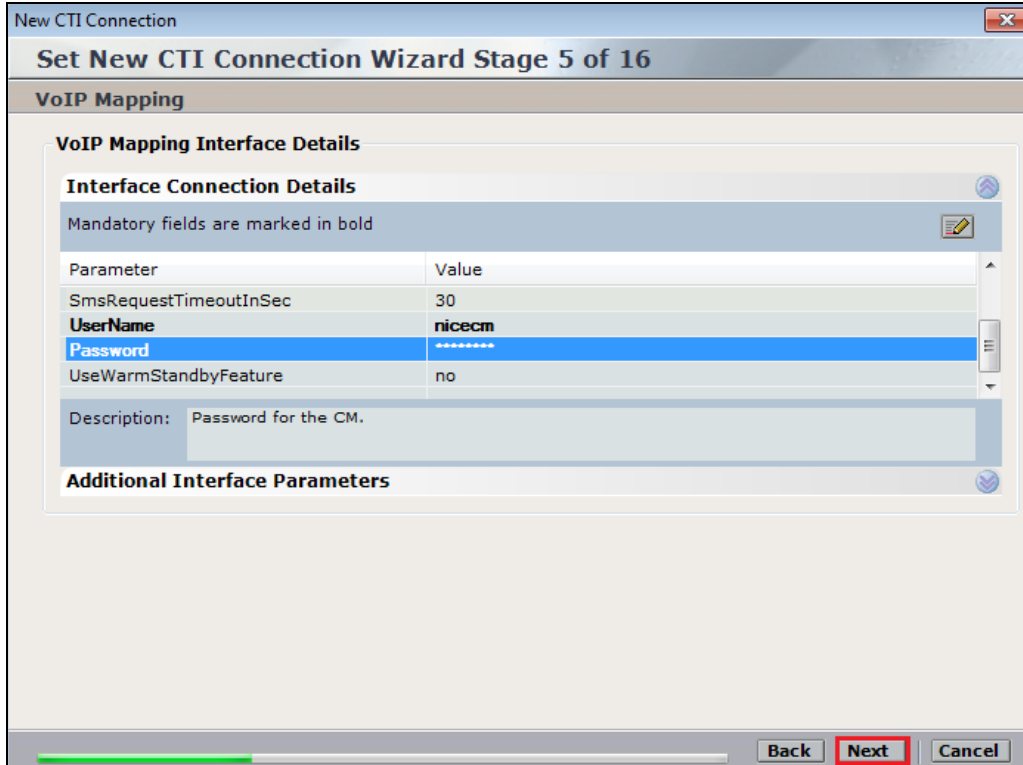
Name: Password

Value: *****

OK Cancel

Back Next Cancel

Click on **Next** to continue.




The screenshot shows the 'Set New CTI Connection Wizard Stage 5 of 16' window. The title bar is 'New CTI Connection'. The main title is 'Set New CTI Connection Wizard Stage 5 of 16'. The section is 'VoIP Mapping'. Below it is 'VoIP Mapping Interface Details'. Under 'Interface Connection Details', there is a table with parameters and values. The 'Password' field is highlighted in blue. Below the table is a 'Description' field with the text 'Password for the CM.'. At the bottom, there is a 'Next' button highlighted with a red box, along with 'Back' and 'Cancel' buttons.

Parameter	Value
SmsRequestTimeoutInSec	30
UserName	nicecm
Password	*****
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 is 'New CTI Connection'. The main title is 'Set New CTI Connection Wizard Stage 10 of 16'. The section is 'Devices'. Below it is 'Available Devices'. There is a text area for 'Provide telephony switch available devices' and a status '0 devices'. To the right of the text area are buttons: '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'. At the bottom, there is a 'Next' button highlighted with a red box, along with 'Back' 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 'Device Type' is set to 'Extension'. The 'Device Number' is '2000' and the 'IP' is '10.10.40.158'. The 'OK' button is highlighted with a red box. The 'Advanced Device Parameters' section is also visible, showing a table for 'Name' and 'Value' and a 'Description' field.

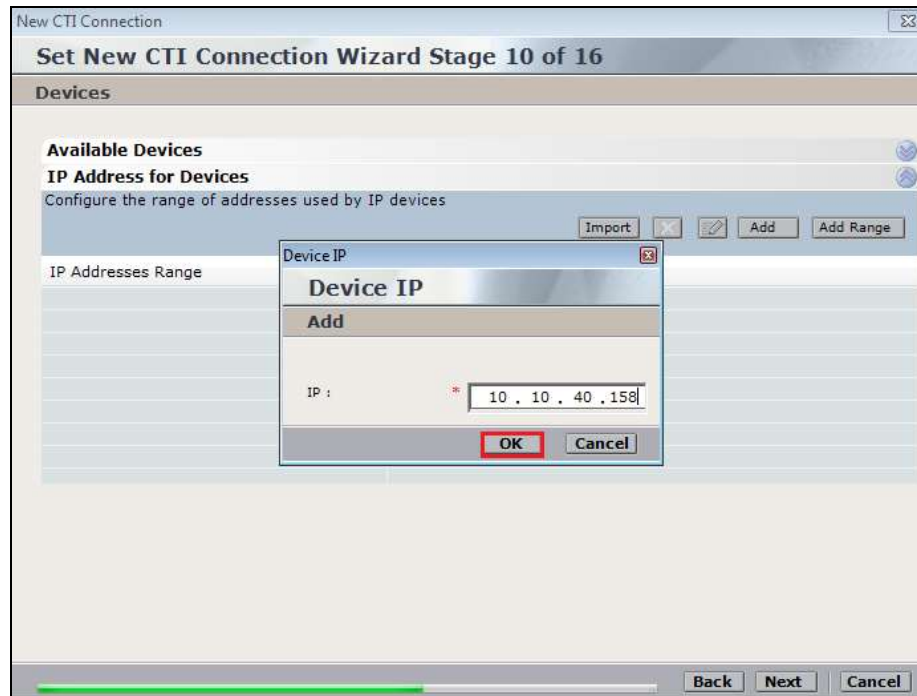
Name	Value

Click on **Add** to add the **IP Address** of the device.

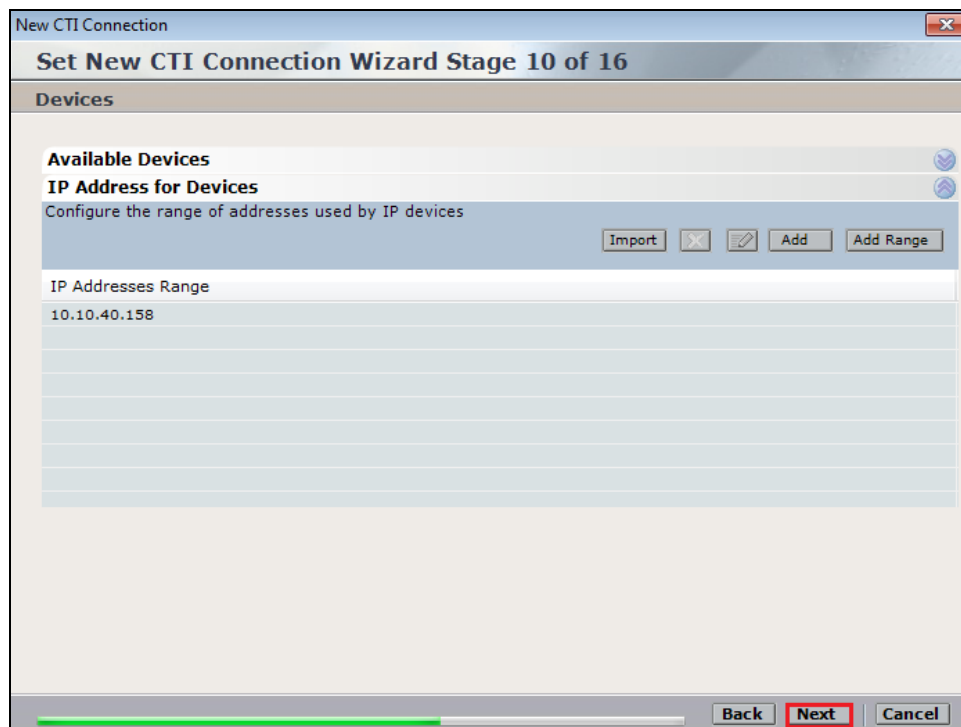
The screenshot shows the 'Set New CTI Connection Wizard Stage 10 of 16' dialog box. The 'Available Devices' section is highlighted with a red box. The 'IP Address for Devices' section is also visible, showing a table for 'IP Addresses Range' and buttons for 'Import', 'Add', and 'Add Range'. The 'Add' button is highlighted with a red box.

IP Addresses Range

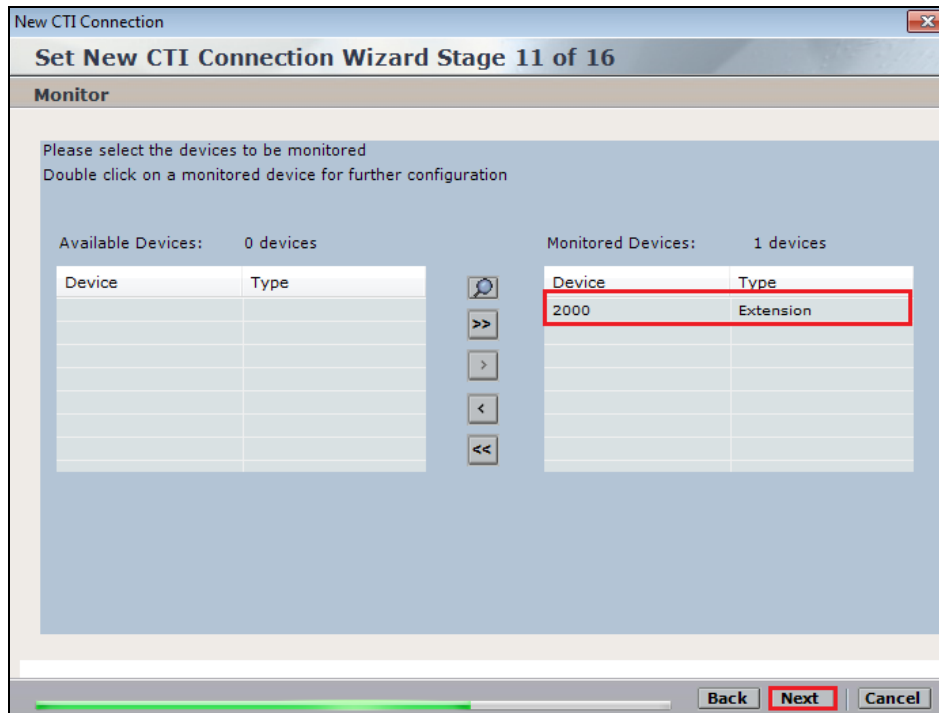
Enter the correct **IP** for the phone set extension.



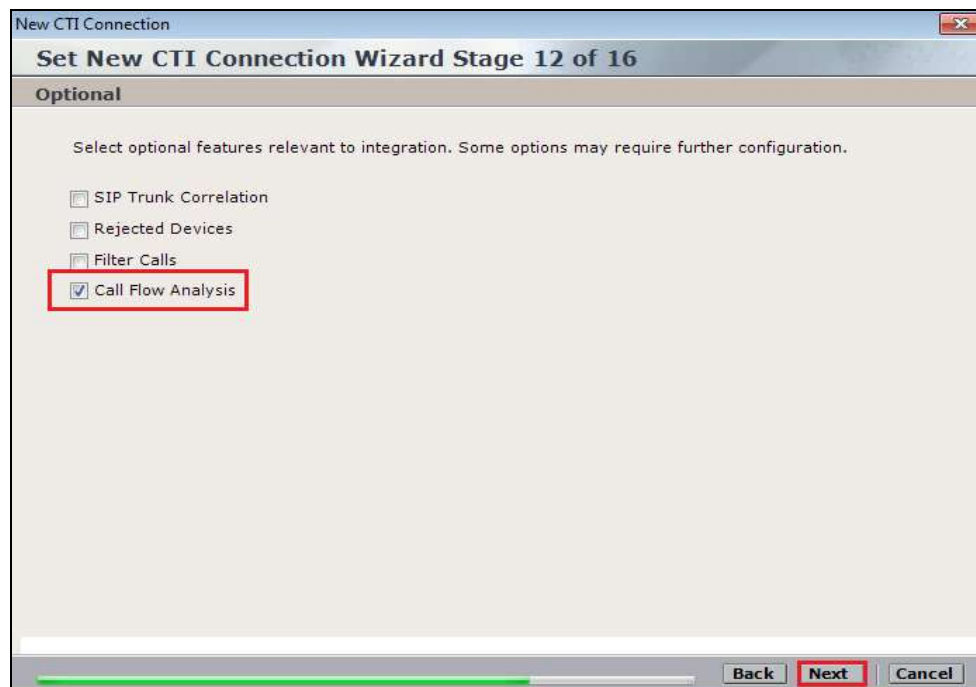
Enter the IP addresses for all devices that are to be recorded and click on **Next** to continue.



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

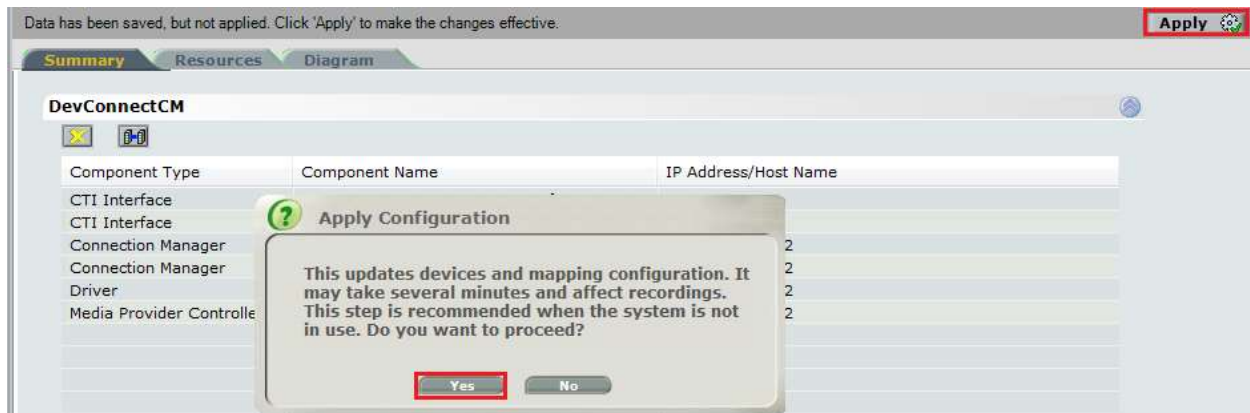
Summary

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

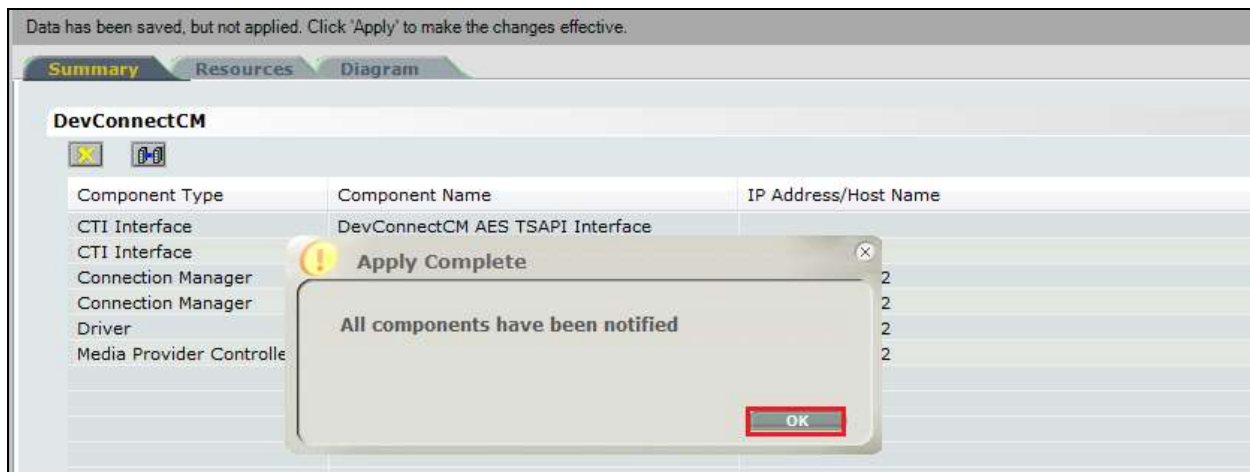
DevConnectCM Connection

Back Finish Cancel

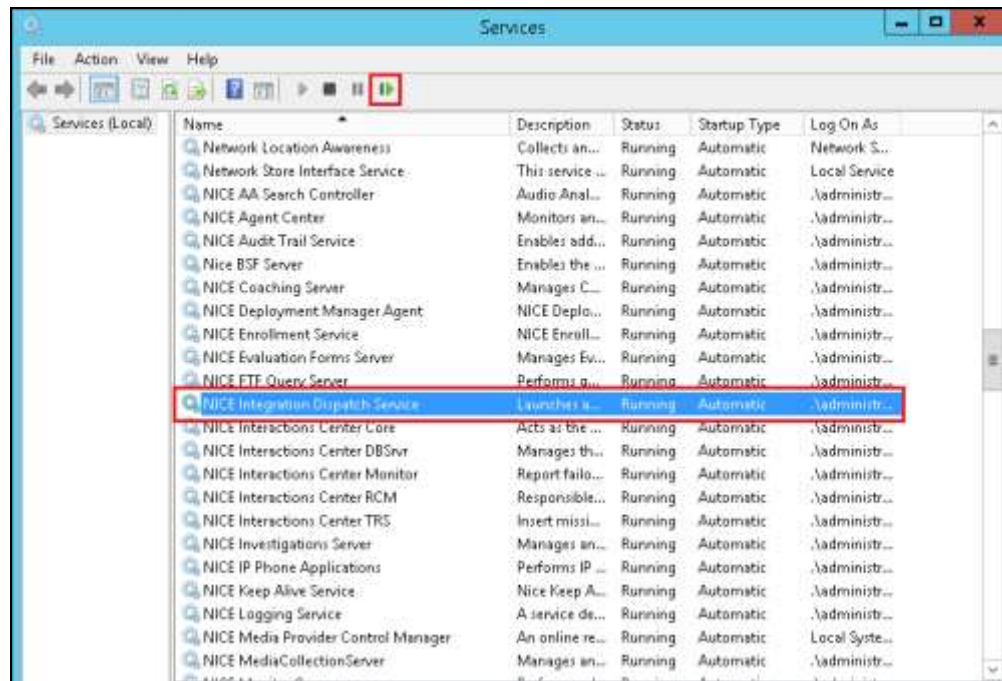
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed.



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

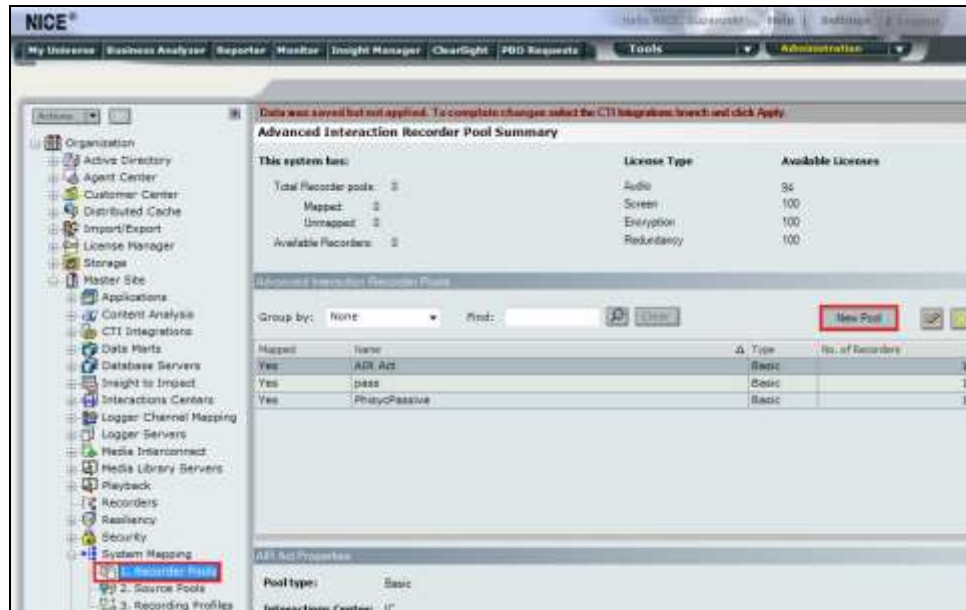


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

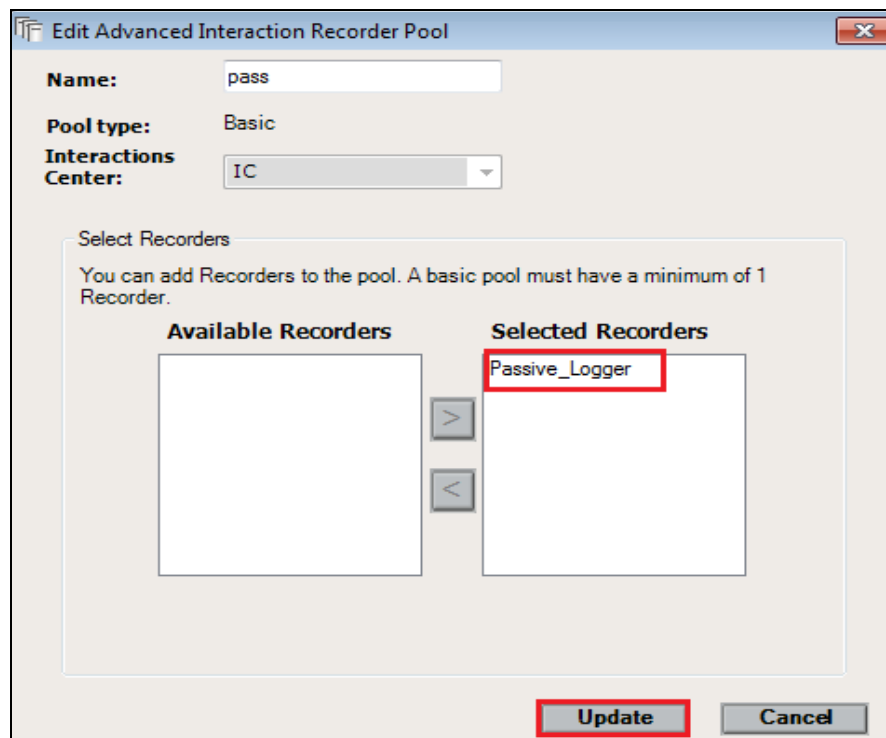


7.2. System Mapping

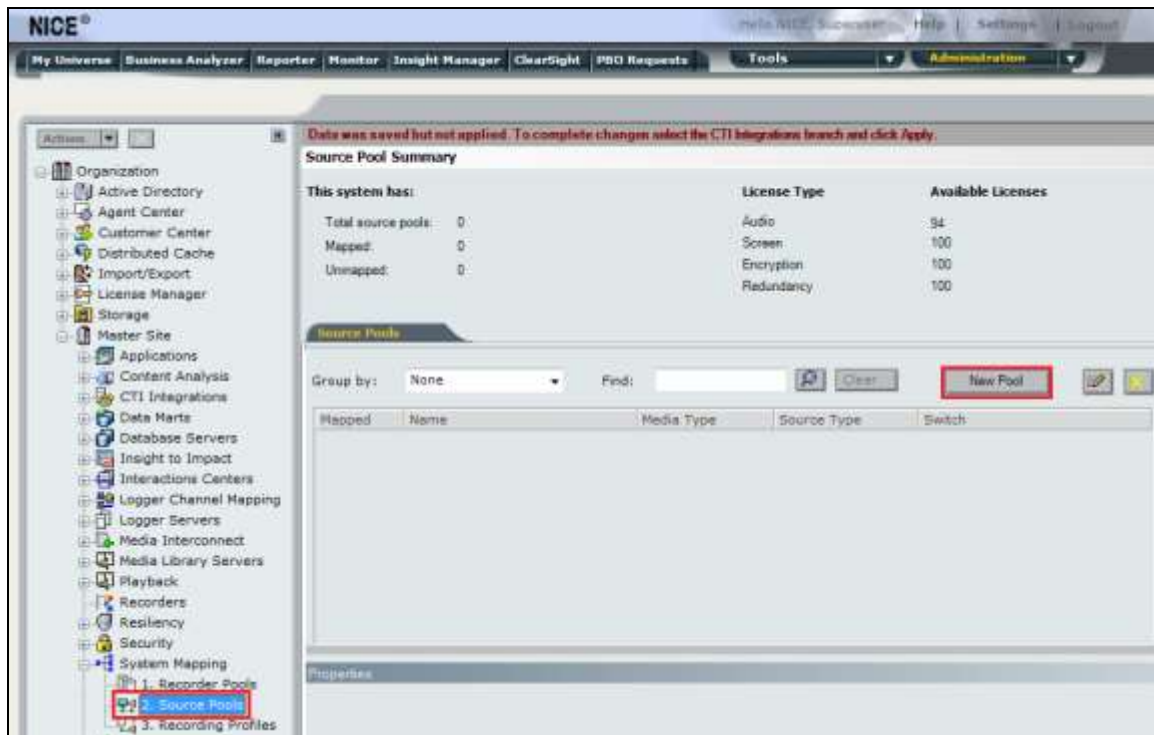
From the web browser navigate to **Master Site → System Mapping → Recorder Pools**. In the main window click on **New Pool**.



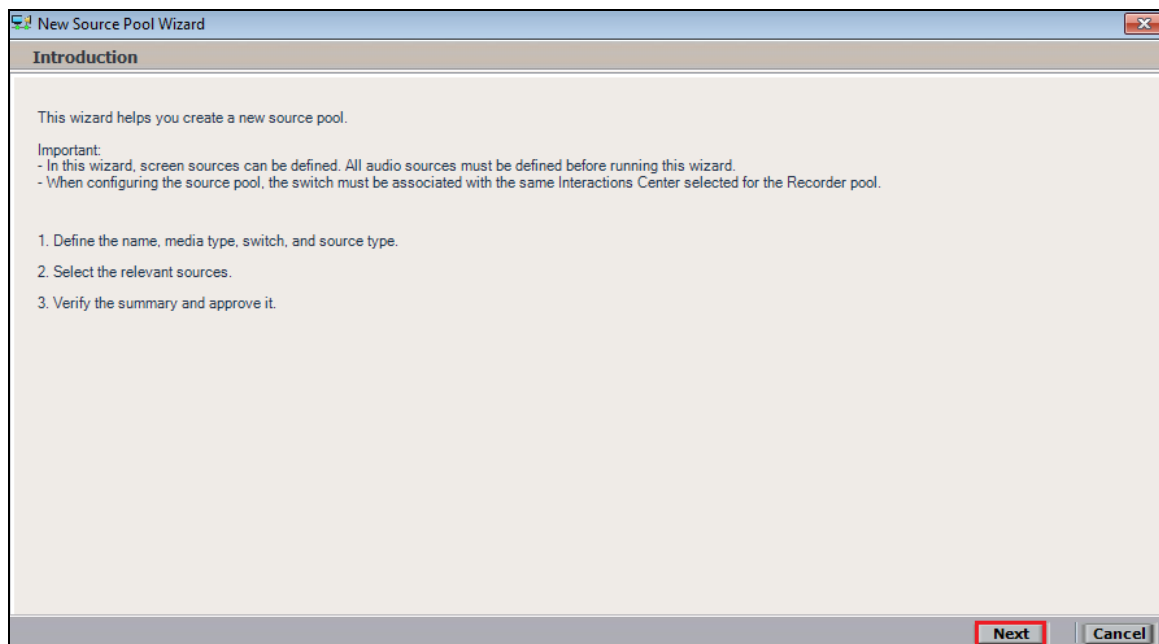
Enter a suitable **Name** for the **Recorder Pool** and select the **Passive_Logger** from the list of **Available Recorders** and click on **Update** to continue.



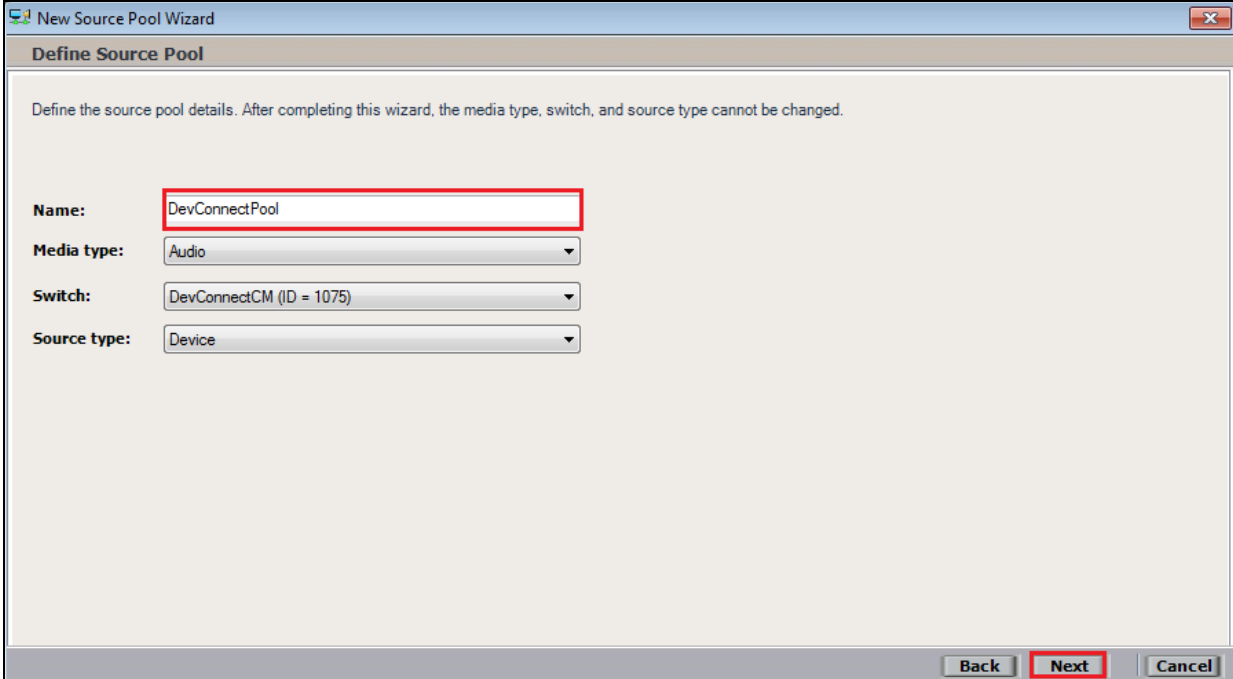
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



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 subtitle is 'Define Source Pool'. Below the subtitle 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

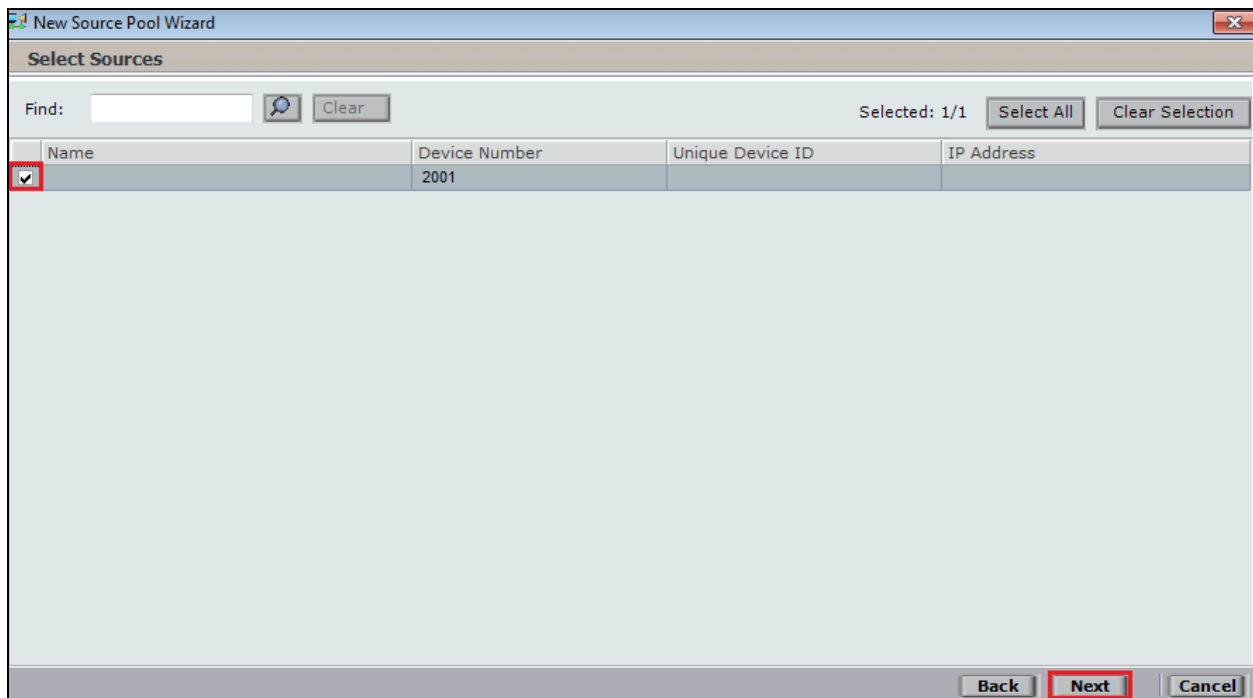
Media type: Audio

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 subtitle 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 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.

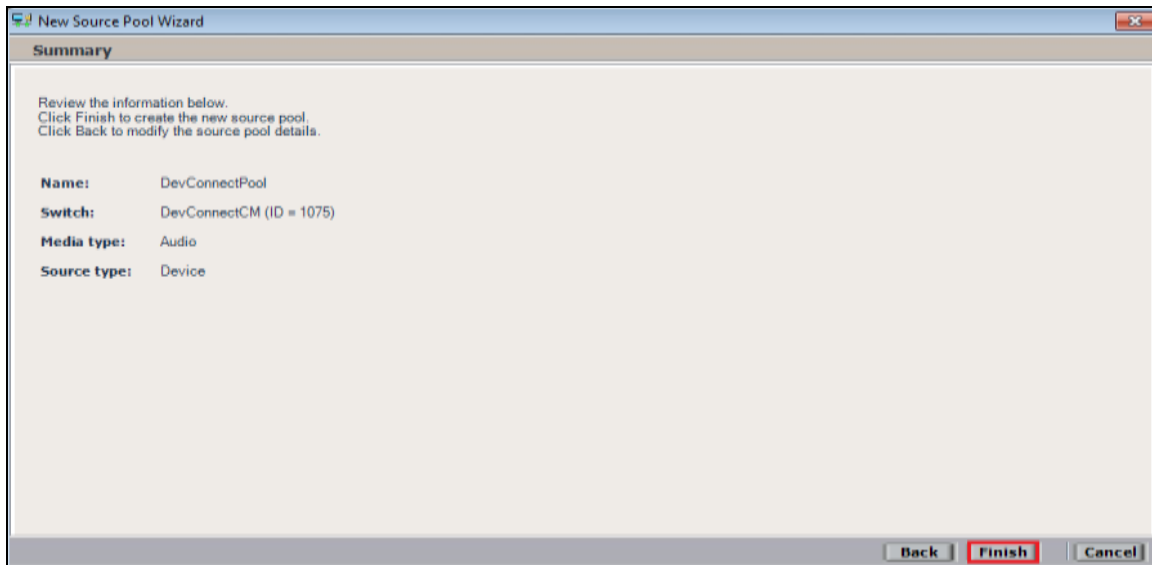
Find: [Search] Clear

Selected: 1/1 Select All Clear Selection

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

Back Next Cancel

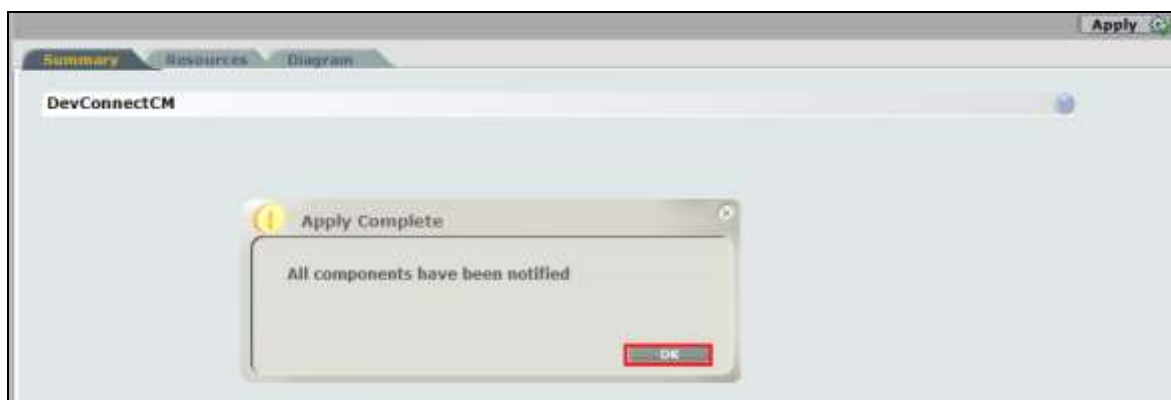
Click on **Finish** to complete the New Source Pool Wizard.



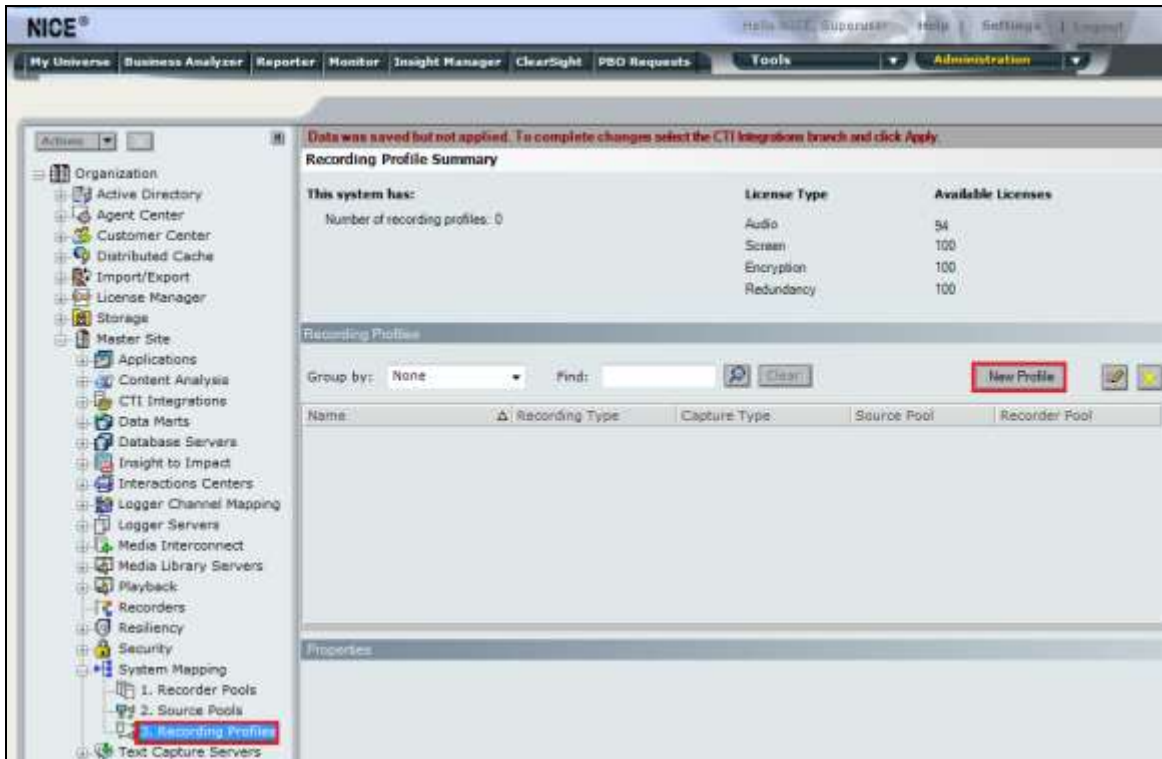
To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.



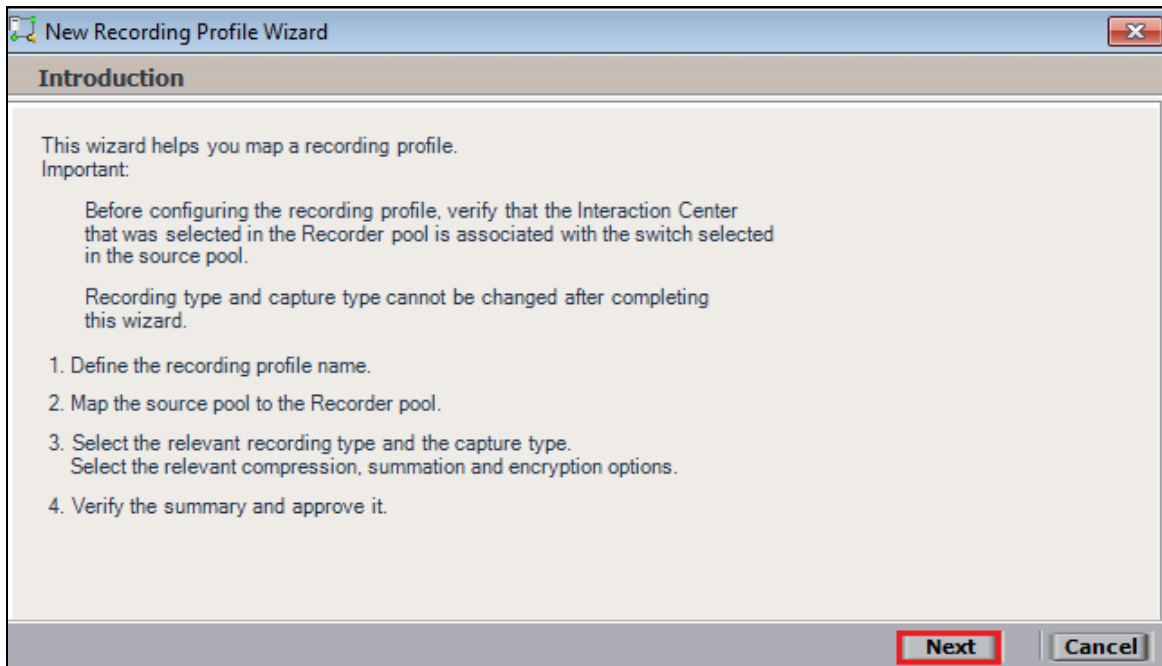
The following screen shows the changes were saved correctly. Click on **OK** to continue.



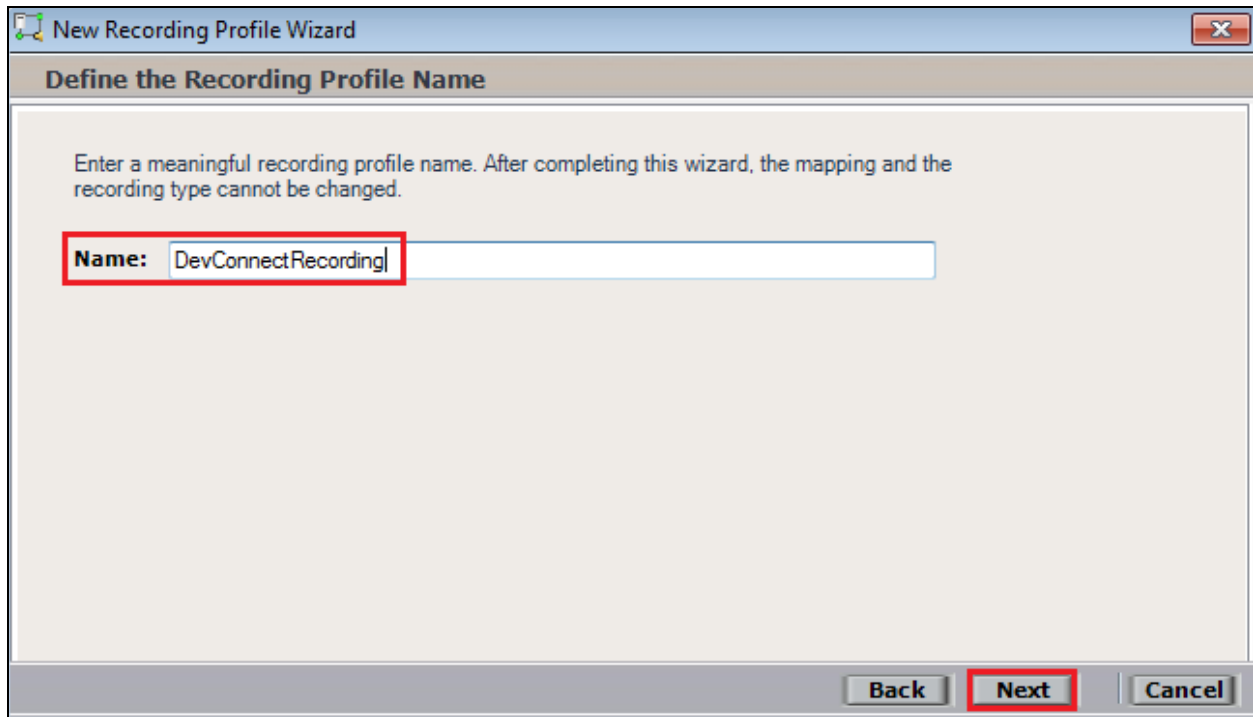
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



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

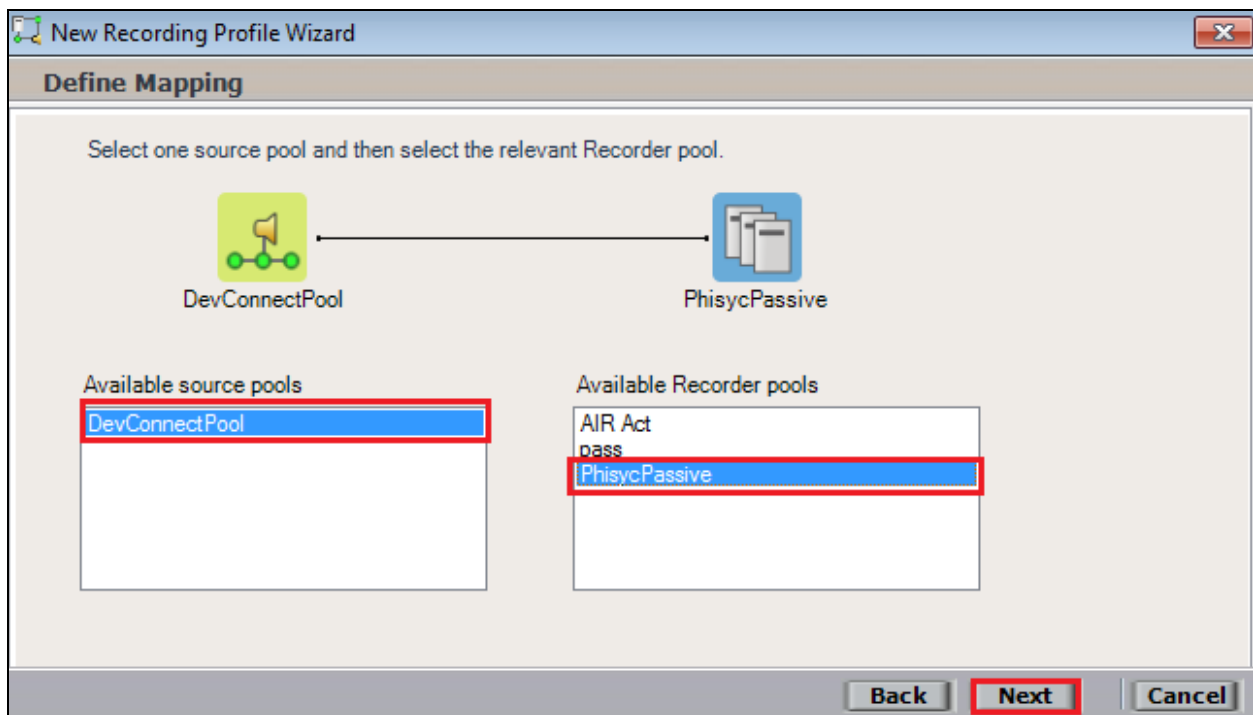


Enter a suitable **Name** for the Recording profile.



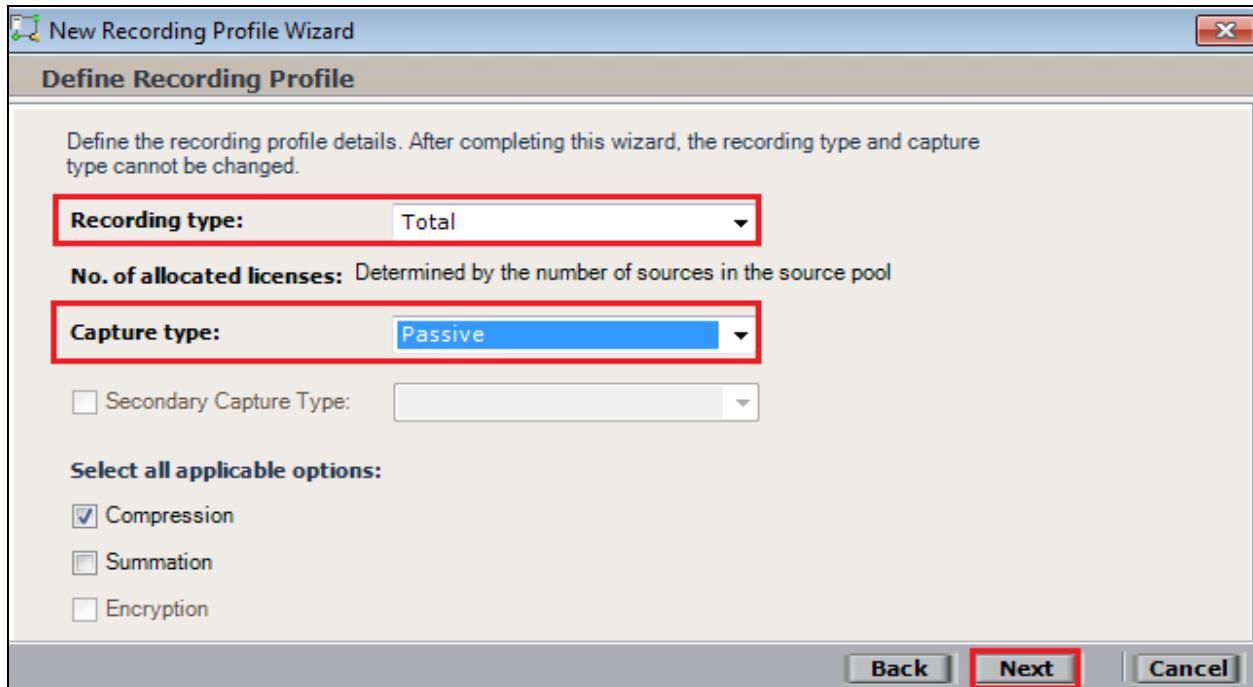
The screenshot shows the 'New Recording Profile Wizard' window with the title 'Define the Recording Profile Name'. The instruction text reads: 'Enter a meaningful recording profile name. After completing this wizard, the mapping and the recording type cannot be changed.' Below this, there is a text input 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 'DevConnectPool' (represented by a green icon) connected by a double-headed arrow to 'PhisycPassive' (represented by a blue icon). Below the diagram, there are two list boxes. The 'Available source pools' list box contains 'DevConnectPool' and is highlighted with a red box. The 'Available Recorder pools' list box contains 'AIR Act', 'pass', and 'PhisycPassive', with 'PhisycPassive' 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 image shows a screenshot of the 'New Recording Profile Wizard' window, specifically the 'Define Recording Profile' step. The window has a title bar with a close button. Below the title bar, the text 'Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.' is displayed. 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 shown. 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 of the window, 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.

New Recording Profile Wizard

Summary

Review the mapping information below.
Click Finish to create the new recording profile.
Click Back to modify the recording profile details.

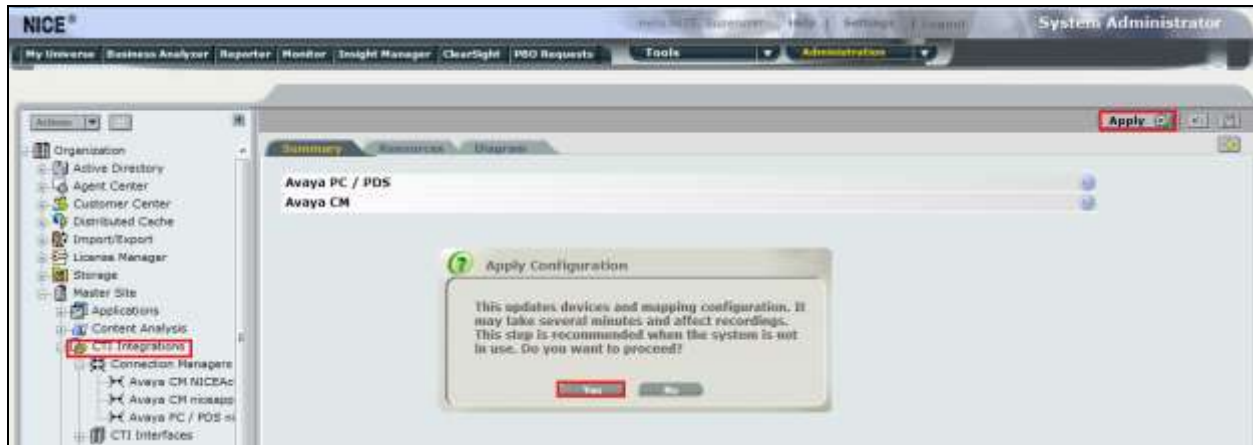
Name:	DevConnectRecording
Source pool:	DevConnectPool
Recorder pool:	PhisycPassive
Recording type:	Total
Capture type:	Passive

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

☒ Compression
☐ Summation
☐ Encryption

Back **Finish** **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	aes63vmpg	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**.

Welcome! User: craft
Last login: Thu Feb 20 11:01:32 2014 from 192.168.10.223
Number of prior failed login attempts: 33
HostName: SP1-AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.213-0
Server Date and Time: Thu Feb 20 11:14:02 UTC 2014

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

AE Services
Communication Manager
Interface
Licensing
Maintenance
Networking
Security
* Status
Alarm Viewer
Log Manager
Logs
* Status and Control
 • CxLAN Service Summary
 • DLG Services Summary
 • DMCC Service Summary
 • Switch Conn Summary
 • TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	CH63vmpg	1	Talking	Tue Feb 18 11:21:49 2014	Online	16	5	15	15	30

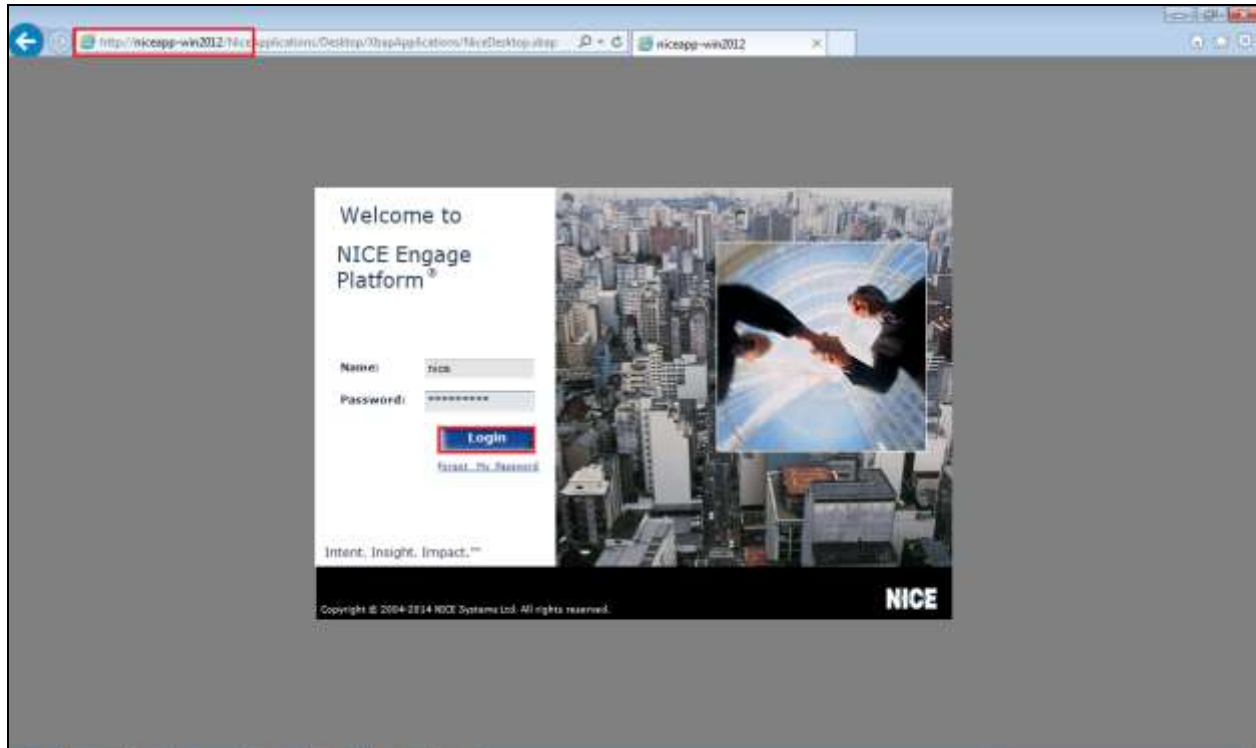
Online Offline

For service-wide information, choose one of the following:
TSAPI Service Status Link Status 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 interface. The left sidebar has a menu with 'Interactions' highlighted. Under 'Interactions', 'Queries' is selected. The main panel shows a list of queries under the 'Queries' tab. The queries listed are: 'Complete - Last 24 hours', 'Complete - Last 7 days', 'Segment - Calls to calibrate', 'Segment - Last 24 hours', 'Segment - Last 7 days', and 'Segment - Last 7 days Calls not eval'. Below the queries, there is a 'Saved Items' section.

The screenshot displays the NICE Business Analyzer interface. The top navigation bar includes 'My Workspace', 'Business Analyzer', 'Reporter', 'Monitor', 'Insight Manager', 'ClearSight', 'PBO Requests', 'Tools', 'Administration', and 'Logout'. The 'Business Analyzer' tab is active.

On the left, the 'Interactions' sidebar shows a tree view with 'Queries' and 'Public'. The 'Queries' section is expanded, showing a list of queries including 'Complete - Last 24 hours', 'Complete - Last 7 days', 'Segment - Calls to callback', 'Segment - Last 24 hours', 'Segment - Last 7 days', and 'Segment - Last 7 days Calls not eval'. The 'Complete - Last 24 hours' query is selected and highlighted with a red box.

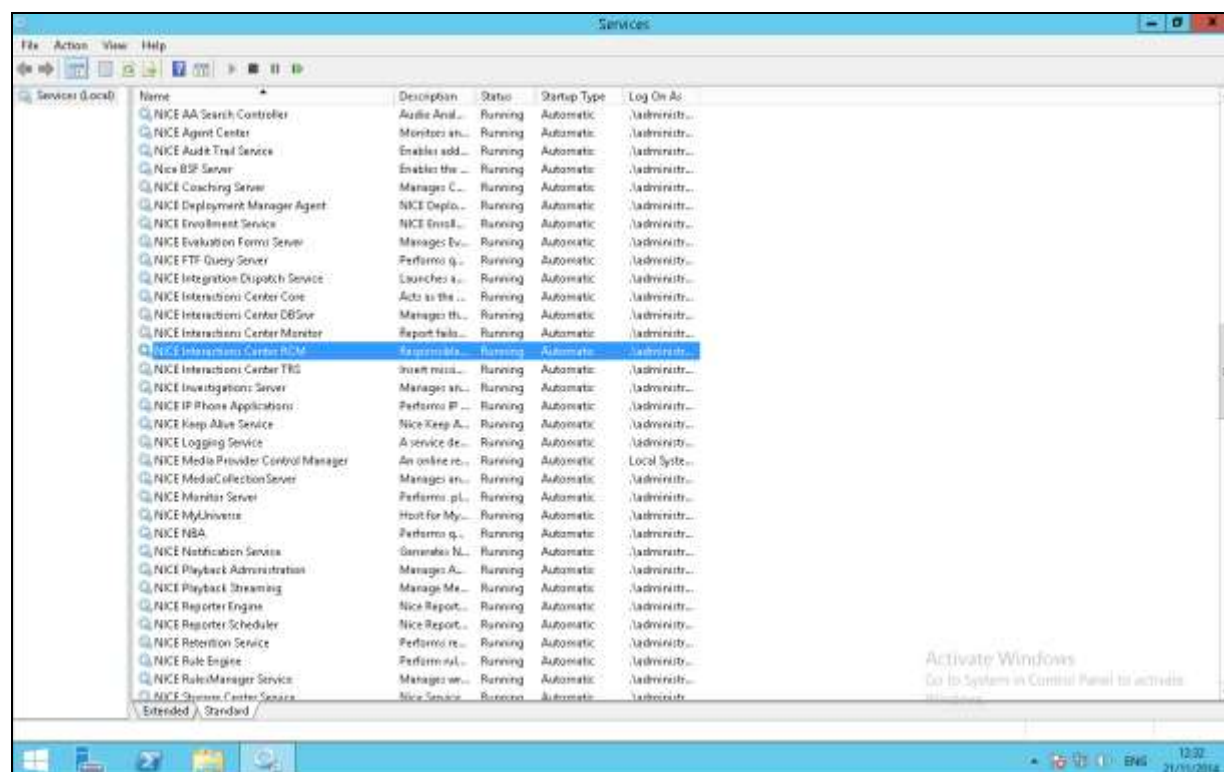
The main area displays a table view of the results for the selected query. The table has columns: Type, Flag, Full Name, Complete ID, Complete Start Time, Complete Stop Time, Complete Duration, and Complete. The table shows a list of interactions, with the first few rows highlighted in red. The first row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The second row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The third row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The fourth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The fifth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The sixth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The seventh row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The eighth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The ninth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The tenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The eleventh row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twelfth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirteenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The fourteenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The fifteenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The sixteenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The seventeenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The eighteenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The nineteenth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twentieth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-first row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-second row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-third row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-fourth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-fifth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-sixth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-seventh row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-eighth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The twenty-ninth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirtieth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-first row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-second row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-third row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-fourth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-fifth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-sixth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-seventh row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-eighth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The thirty-ninth row is: Unmapped, User, 60832834137153699876, 20/11/2014 17:03:40, 20/11/2014 17:03:52, 00:00:13, 60832834137. The fortieth row is:

The NICE player is opened and the recording is presented for playback. Click on the **Play** 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 Active 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 R6.3 using Avaya Aura® Application Enablement Services R6.3 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 6.3*
- [4] *Avaya Aura® Session Manager Overview*, Doc # 03603323 *Avaya Aura® Contact Centre SIP Commissioning*, Doc # NN44400-511, Release 6.3

Product documentation for NICE products may be found at: <http://www.nice.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 9620 H.323 Deskphone

This is a printout of the Avaya 9620 H.323 Deskphone used during compliance testing.

display station 2000	Page 1 of 5	
STATION		
Extension: 2000	Lock Messages? n	BCC: 0
Type: 9620	Security Code: *	TN: 1
Port: S00000	Coverage Path 1: 2	COR: 1
Name: Paul 2000	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: 2000	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Short/Prefixed Registration Allowed: default	
	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? y
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
	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

```

```

Call Appearance Display Format: inter-location
IP Phone Group ID:
Enhanced Callr-Info Display for 1-Line Phones? n

```

ENHANCED CALL FORWARDING

			Forwarded Destination	Active
Unconditional For	Internal Calls To:	4000		n
	External Calls To:	4000		n
Busy For	Internal Calls To:	4202		n
	External Calls To:	4202		n
No Reply For	Internal Calls To:	2101		n
	External Calls To:	2101		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                4: manual-in              Grp:
2: call-appr                5: after-call             Grp:
3: auto-in                  Grp:    6: aux-work               RC:   Grp:

```

voice-mail

Avaya Agent LoginID

This is a printout of one of the agents used during compliance testing.

```
display agent-loginID 4400                                Page 1 of 3

                                AGENT LOGINID

      Login ID: 4400                                AAS? n
      Name: Paul                                AUDIX? n
      TN: 1                                LWC Reception: spe
      COR: 1                                LWC Log External Calls? n
      Coverage Path:                                AUDIX Name for Messaging:
      Security Code:

                                LoginID for ISDN/SIP Display? n
                                Password:
                                Password (enter again):
                                Auto Answer: station
                                MIA Across Skills: system
                                ACW Agent Considered Idle: system
                                Aux Work Reason Code Type: system
                                Logout Reason Code Type: system
                                Maximum time agent in ACW before logout (sec): system
                                Forced Agent Logout Time: :
```

```
display agent-loginID 4400                                Page 2 of 3

                                AGENT LOGINID

      Direct Agent Skill:                                Service Objective? n
      Call Handling Preference: skill-level                                Local Call Preference? n

      SN  RL  SL      SN  RL  SL      SN  RL  SL      SN  RL  SL
1: 33    1           16:           31:           46:
2: 34    1           17:           32:           47:
3:           18:           33:           48:
4:           19:           34:           49:
5:           20:           35:           50:
6:           21:           36:           51:
7:           22:           37:           52:
8:           23:           38:           53:
9:           24:           39:           54:
10:          25:           40:           55:
11:          26:           41:           56:
12:          27:           42:           57:
13:          28:           43:           58:
14:          29:           44:           59:
15:          30:           45:           60:
```

©2015 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.