



Avaya Solution & Interoperability Test Lab

Application Notes for configuring NICE Engage Platform R6.3 to interoperate with Avaya Proactive Contact R5.1 and Avaya Aura® Application Enablement Services R6.3 using DMCC Multi-Registration to record calls - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the NICE Engage Platform to interoperate with the Avaya solution consisting of Avaya Proactive Contact R5.1, Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3, and Avaya Aura® Application Enablement Services R6.3.

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 required for NICE Engage Platform to interoperate with the Avaya solution consisting of Avaya Proactive Contact R5.1, Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3, and Avaya Aura® Application Enablement Services R6.3 using DMCC Multi-Registration to record telephone calls on Proactive Contact.

The Avaya Proactive Contact system is an enterprise outbound solution software application that consists of software, hardware, and network components. The system is comprised of a system cabinet, supervisor workstation, agent workstations with a hardware connection to Avaya Aura® Communication Manager using an ISDN trunk to engage Elite agent on Communication Manager.

The NICE Engage Platform is setup to use Device Media Call Control Multi-Registration to record the voice calls of Communication Manager agents on various Proactive Contact Jobs, inbound, outbound and blended. Device Media Call Control (DMCC) works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure.

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 .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. This application registers an extension with Communication Manager and waits for that extension to be dialed. 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 DMCC Multi-Registration with Proactive Contact and AES. The NICE Engage Platform registers with the event server on Proactive Contact in order to receive call and agent events to stop and start call recording.

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:

The testing focuses on the following types of calls:

- **Proactive Contact Outbound job** – Recording of all calls types for agents on an outbound job on Proactive Contact, including transfer, conference and forward work.
- **Proactive Contact Managed job** - Recording of all calls types for agents on a preview outbound job on Proactive Contact, including transfer, conference and forward work.
- **Proactive Contact Inbound Job-** Recording of all calls types for agents on an inbound job on Proactive Contact, including transfer, conference and forward work.
- **Proactive Contact Agent Blending (PAB)** - Recording of agents on a blended job where the agent is switching between answering VDN calls and outbound calls.
- **Proactive Contact Intelligent Call Blending (ICB)** - Recording of agents on a blended job where the agent is switching between answering inbound calls and outbound calls.
- **Failover testing** - The behaviour of the NICE Engage Platform under different simulated LAN failure conditions on the Avaya solution.

2.2. Test Results

Most functionality and serviceability test cases were completed successfully. The following issues and observations were noted.

Issue 1: “Forward Work - Supervised Transfer” [Note Forward Work is when Agent 1 transfers/conferences the call to Agent 2 using the Proactive Contact method “Forward Work”]. When a call is transferred in a supervised fashion using Forward Work, there are two recordings present - Recording 1 has the whole conversation from Agent 1 out to the PSTN and the transferred call to agent 2 talking to the PSTN. Recording 2 should contain the “consultation” between agents but there is nothing present to playback. This issue was reproduced in the NICE labs and a hot fix is available from NICE to resolve this issue, note this fix was produced after the completion of compliance testing and was therefore not compliance tested.

Issue 2: “Forward Work - Conference” - PSTN hangs up the call. There are two recordings present Recording 1 has the whole conversation from Agent 1 out to the PSTN and the transferred call to agent 2 talking to the PSTN. Recording 2 should contain the “consultation” between agents but there is nothing present to playback. This issue has been documented as a limitation on NICE Engage Platform Integration Description Document.

Issue 3: “Forward Work - Conference” - Agent 1 hangs up the call. The “conference” part of the call is not fully recorded; the recorded portion only starts when agent 1 hangs up the call as the NICE omits the conversation when all three are in conference. The initial conference is viewed as if the call was on hold. This issue has been documented as limitation on NICE Engage Platform Integration Description Document.

Issue 4: “Forward Work - Conference” - Agent 2 hangs up the call. There are two recordings present, the initial call between agent 1 and the PSTN, the recording on the second call is only as long as when Agent 2 hangs up the call. The Conversation between Agent 1 and the PSTN is not recorded after Agent 2 hangs up. This issue has been documented as limitation on NICE Engage Platform Integration Description Document.

Observation 1: “Ordinary Conference” with PSTN hanging up - There is a call up between Proactive Contact Agent and a PSTN customer and there is a conference (either blind or supervised) with a supervisor (ordinary office phone that is also monitored). When the PSTN hangs up the call – all calls are then automatically dropped (this is what happens on the Proactive Contact/Communication Manager when the PSTN drops the call). The first leg of the call i.e., the initial call between Agent 1 and the PSTN only appears when Agent 1 releases the line.

Observation 2: For an inbound job only, the playback does not contain the consult bit in the main screen; this consultation needs to be played by the segments. This only happens for inbound jobs and supervised transfer to the PSTN or a Monitored phone.

Observation 3: There is a 7 second delay before the recording stops after CTRL + F7 is pressed. This is the same if F8 is pressed, basically any “release line” event.

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 during the compliance test of the NICE Engage Platform with Avaya Proactive Contact using DMCC Multi-Registration to record calls. The NICE Application Server is setup for DMCC Multi-Registration mode and connects to both the AES and Proactive Contact Event Manager.

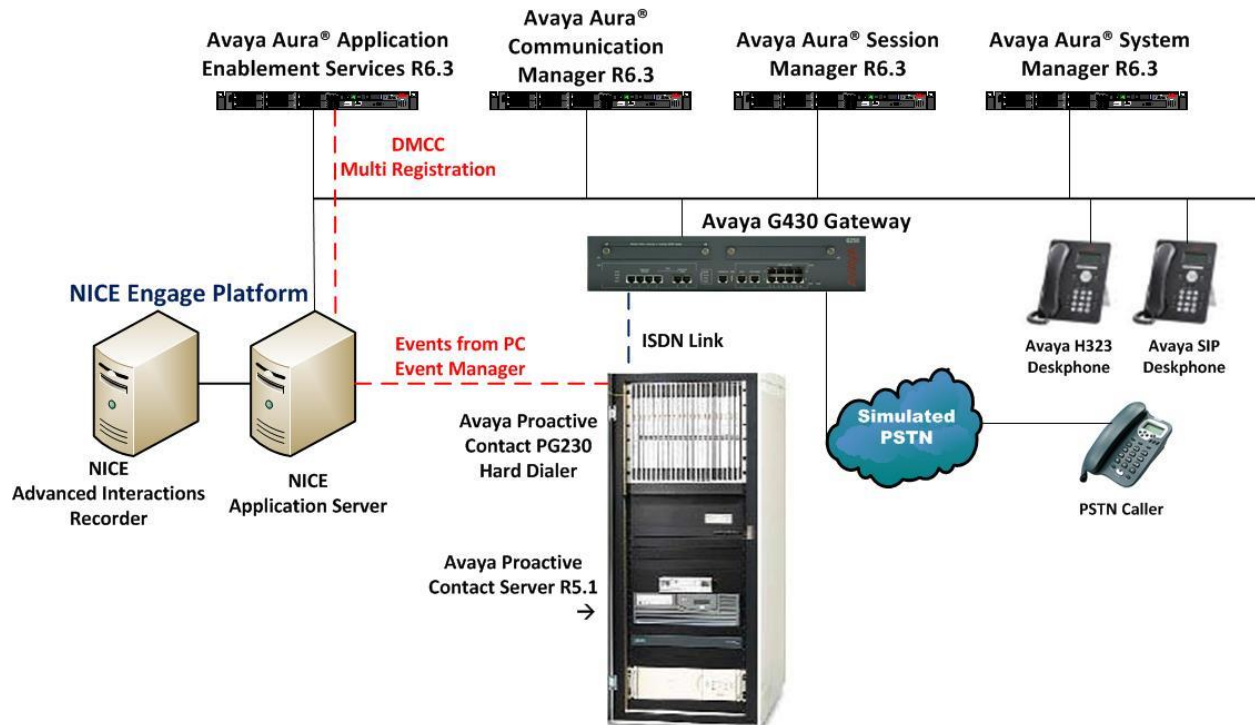


Figure 1: Connection of NICE Engage Platform R6.3 with Avaya Proactive Contact R5.1, Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3

4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| Avaya Proactive Contact | R5.1 |
| Avaya Proactive Contact PG230 Hard Dialer | R5.1 |
| 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 9630 H323 Deskphone | R3.186A |
| Avaya 9640 SIP Deskphone | R2.6.12.1 |
| NICE Engage Platform <ul style="list-style-type: none">- Application Server- Advanced Interactions Recorder- 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 11**.

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 | | | |

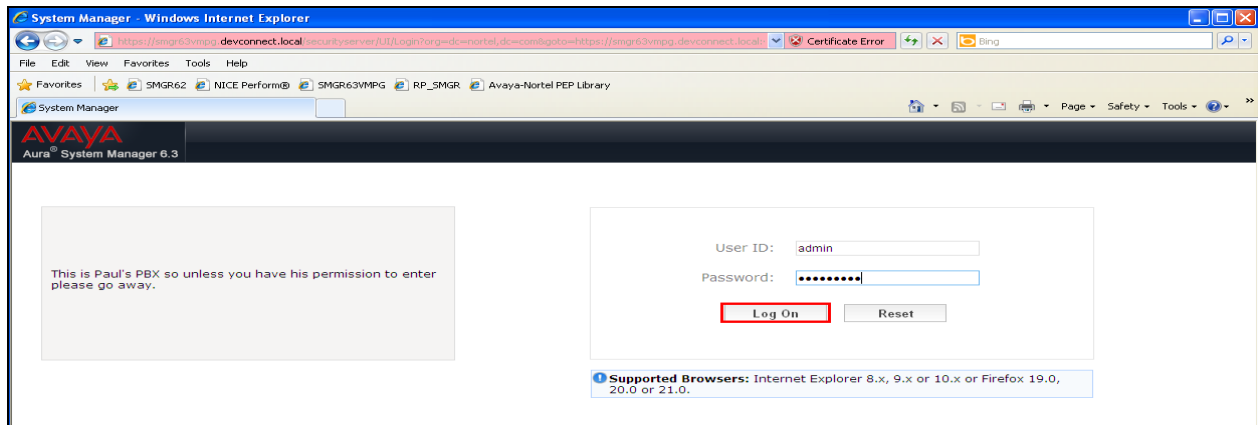
5.5. Configure H323 Stations for Multi-Registration

All endpoints that are to be monitored by NICE will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required in **Section 8.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

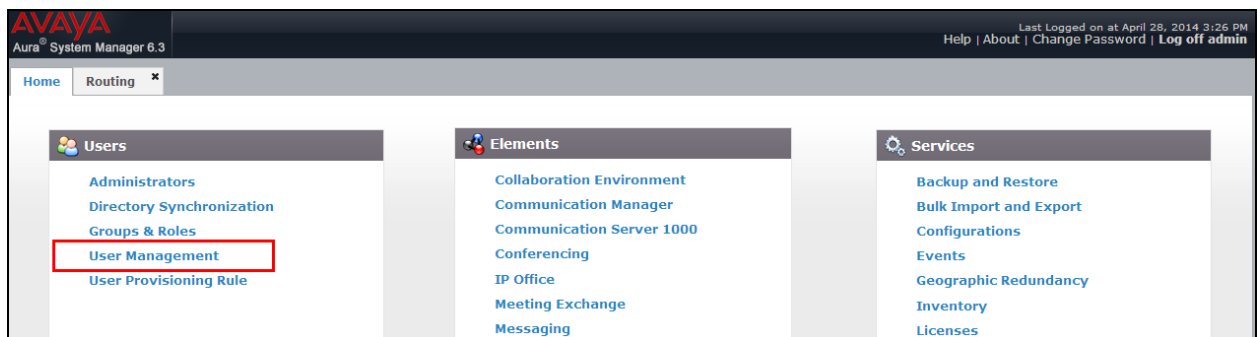
| | | |
|---------------------------|--|--------|
| change station x | Page 1 of 6 | |
| STATION | | |
| Extension: x | Lock Messages? n | BCC: 0 |
| Type: 9630 | Security Code: 1234 | TN: 1 |
| Port: S00101 | Coverage Path 1: | COR: 1 |
| Name: Recorder | Coverage Path 2: | COS: 1 |
| | Hunt-to Station: | |
| STATION OPTIONS | | |
| | Time of Day Lock Table: | |
| Loss Group: 19 | Personalized Ringing Pattern: 1 | |
| | Message Lamp Ext: 1591 | |
| Speakerphone: 2-way | Mute Button Enabled? y | |
| Display Language: english | | |
| Survivable GK Node Name: | | |
| Survivable COR: internal | Media Complex Ext: | |
| Survivable Trunk Dest? y | IP SoftPhone? y | |
| | IP Video Softphone? n | |
| | Short/Prefixed Registration Allowed: default | |

5.6. Configure SIP Stations for Multi-Registration

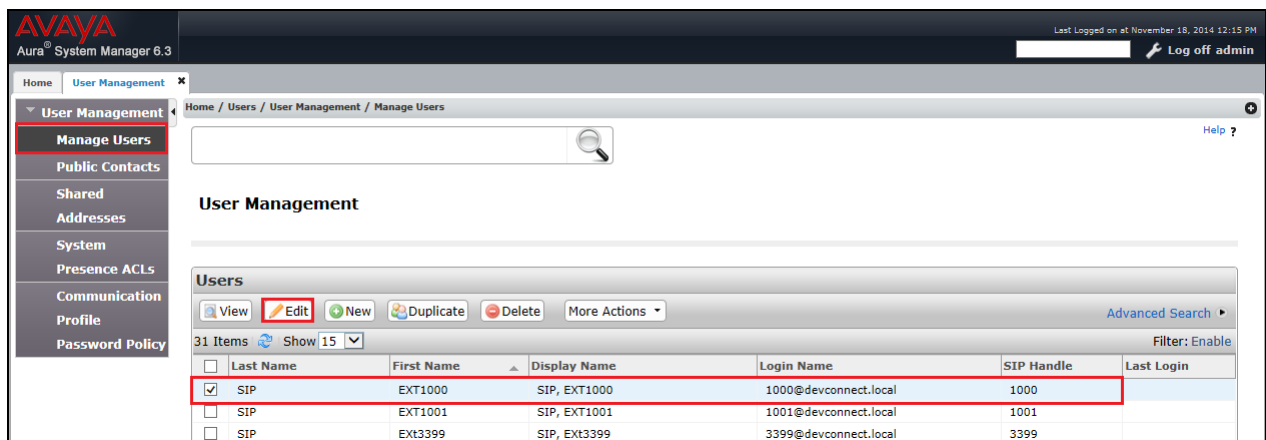
The configuration of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where <FQDN> is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.



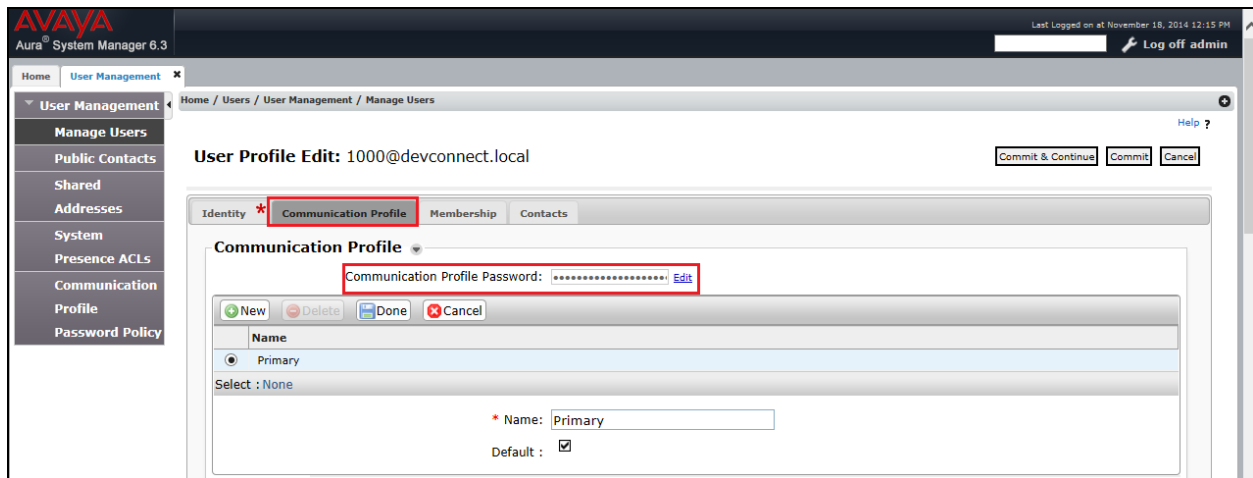
From the home page click on **User Management** highlighted below.



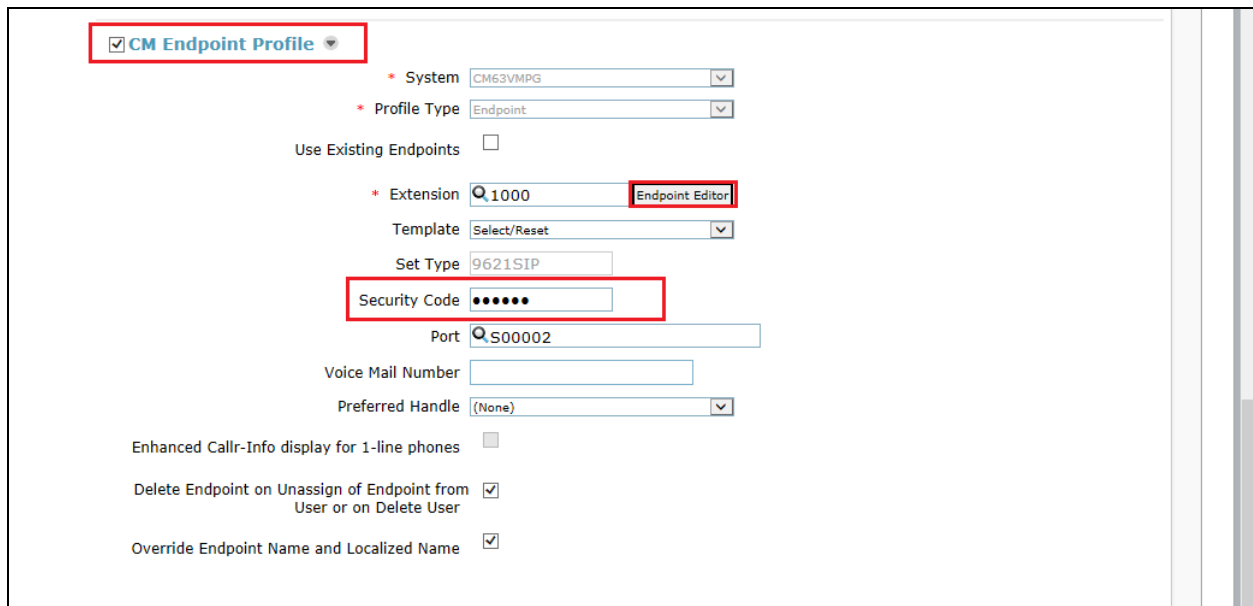
Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



Click on the **Communication Profile** tab. Ensure that the **Communication Profile Password** is known and if not click on edit to change it.



From the same page scroll down to **CM Endpoint Profile** and enter the **Security Code**, note this should be the same as the password above and will be required again in **Section 8.1** during the configuration of the NICE Engage Platform. Click on **Endpoint Editor** to make further changes.



In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

AVAYA
Aura System Manager 6.3

Home / Users / User Management / Manage Users

Edit Endpoint

System: CM63VMPG
Extension: 1000
Set Type: 9621SIP
Port: S00002
Name: SIP, EXT1000

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P)

Group Membership (M)

* Class of Restriction (COR): 1
* Emergency Location Ext: 1000
* Tenant Number: 1
* SIP Trunk: Q1
Coverage Path 1:
Lock Message: ☐
Multibyte Language: Not Applicable

* Class Of Service (COS): 1
* Message Lamp Ext.: 1000
Type of 3PCC Enabled: Avaya
Coverage Path 2:
Localized Display Name: SIP, EXT1000

* Required

Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done** once this is set (not shown).

General Options (G) * **Feature Options (F)** Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P)

Group Membership (M)

Active Station Ringing: single
MWI Served User Type: qsig-mwi
Per Station CPN - Send Calling Number: None
IP Phone Group ID:
Remote Soft Phone Emergency Calls: as-on-local
LWC Reception: spe
AUDIX Name:
EC500 State: enabled
Short/Prefixed Registration Allowed: default
Music Source:

Auto Answer: none
Coverage After Forwarding: system
Display Language: english
Hunt-to Station:
Loss Group: 19
Survivable COR: internal
Time of Day Lock Table: None
Location:
Voice Mail Number:

Features

☐ Always Use
☐ IP Audio Hairpinning
☐ Bridged Call Alerting
☐ Bridged Idle Line Preference
☒ Coverage Message Retrieval
☐ Data Restriction
☒ Survivable Trunk Dest
☐ Bridged Appearance Origination Restriction
☒ Restrict Last Appearance

☐ Idle Appearance Preference
☒ **IP SoftPhone**
☒ LWC Activation
☐ CDR Privacy
☒ Direct IP-IP Audio Connections
☐ H.320 Conversion
☐ IP Video Softphone
☐ Per Button Ring Control

Click on **Commit** once this is done to save the changes.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 6.3', and a 'Log off admin' button. The left sidebar contains a 'User Management' menu with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System', 'Presence ACLs', 'Communication Profile', and 'Password Policy'. The main content area is titled 'User Profile Edit: 1000@devconnect.local'. It features a 'Communication Profile' tab with a 'Communication Profile Password' field and an 'Edit' link. Below this, there is a 'Name' field with a 'Primary' radio button selected. A 'Select : None' dropdown is also present. At the bottom, there is a 'Name' field with the value 'Primary' and a 'Default' checkbox checked. The 'Commit' button is highlighted with a red box.

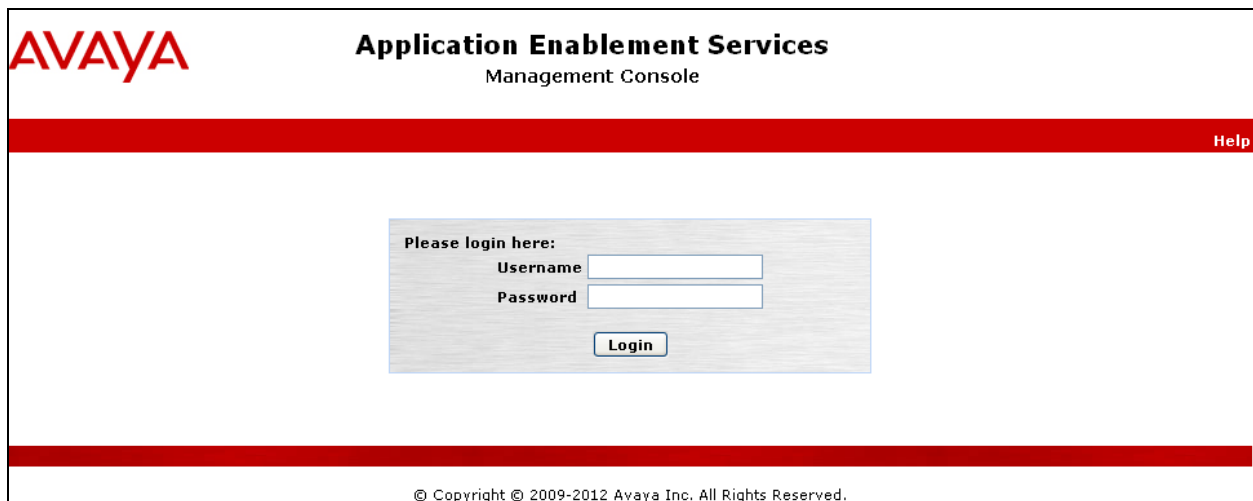
6. Configure Avaya Aura® Application Enablement Services

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

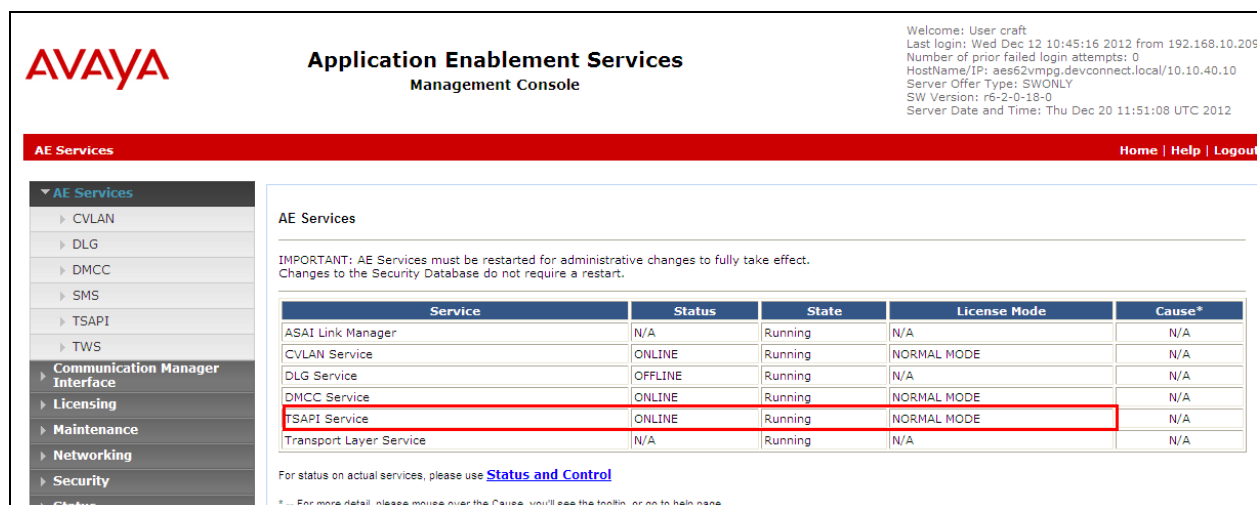
6.1. Verify Licensing

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 contains the copyright notice: "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

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 10:45:16 2012 from 192.168.10.209
Number of prior failed login attempts: 0
HostName/IP: aes62vmppg.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

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ TWS
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status

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.

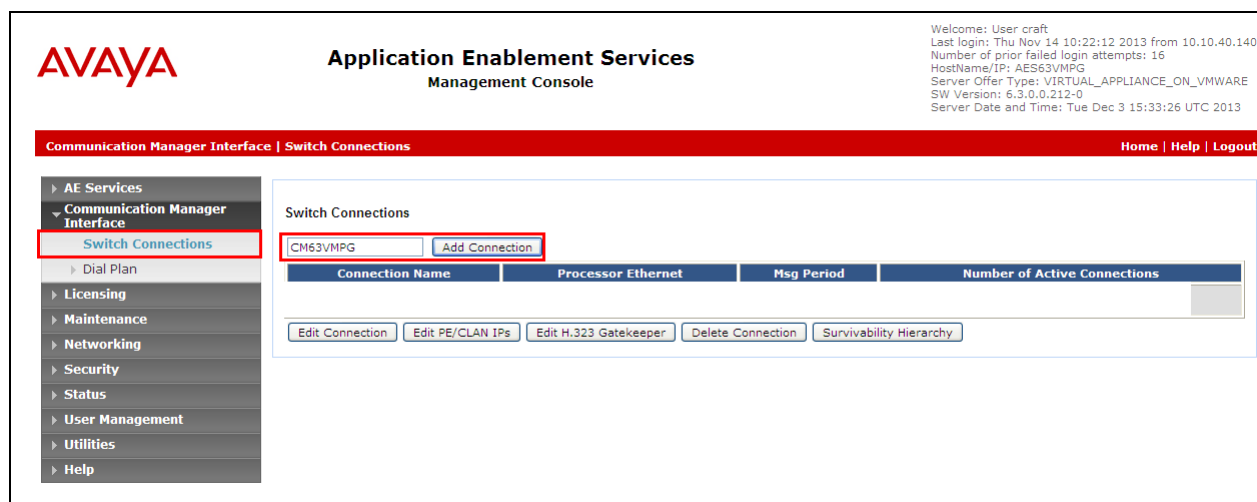
| Service | Status | State | License Mode | Cause* |
|-------------------------|---------------|----------------|--------------------|------------|
| ASAI Link Manager | N/A | Running | N/A | N/A |
| CVLAN Service | ONLINE | Running | NORMAL MODE | N/A |
| DLG Service | OFFLINE | Running | N/A | N/A |
| 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 |

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.

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 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 3 15:33:26 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

Switch Connections

CM63VMPPG Add Connection

| Connection Name | Processor Ethernet | Msg Period | Number of Active Connections |
|-----------------|--------------------|------------|------------------------------|
| | | | |

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.

AVAYA Application Enablement Services Management Console

Welcome: User craft
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: 6.3.0.0.212-0
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 - CM63vmppg

Switch Password: [Redacted]
Confirm Switch Password: [Redacted]
Msg Period: 30 Minutes (1 - 72)
SSL: ☒
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 (not shown, see screen at the bottom of page 10). 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 craft
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: 6.3.0.0.212-0
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 - CM63vmppg

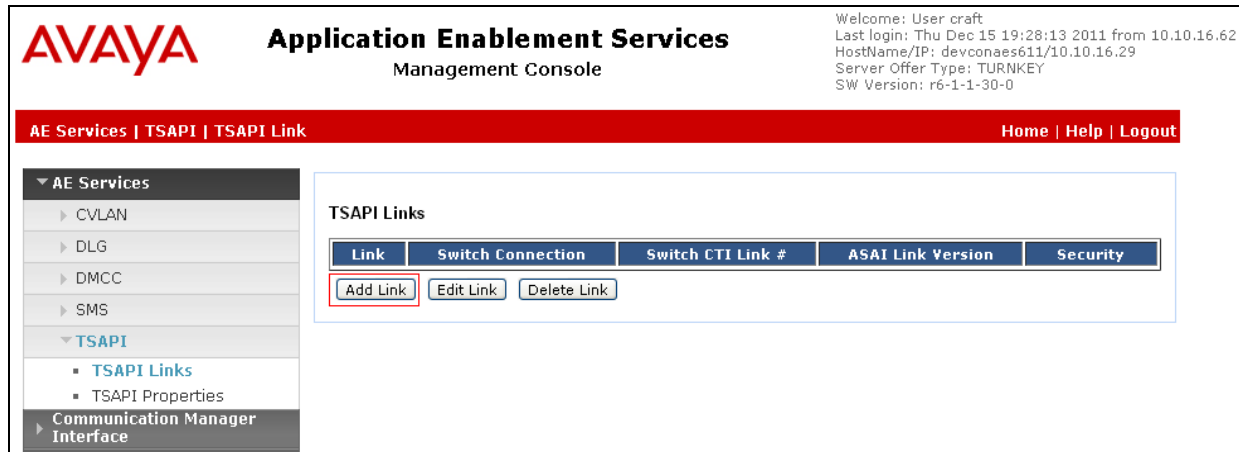
10.10.40.31 Add/Edit Name or IP

| Name or IP Address | Status |
|--------------------|--------|
| 10.10.40.31 | In Use |

Back

6.3. Administer TSAPI link

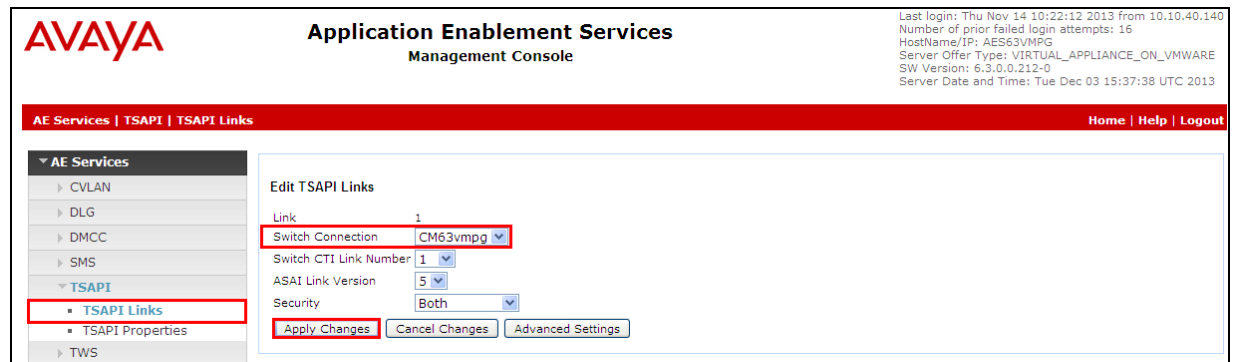
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

AE Services | TSAPI | TSAPI Link Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ **TSAPI**
 - **TSAPI Links**
 - TSAPI Properties
- ▶ Communication Manager Interface

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.

AVAYA Application Enablement Services Management Console

Last login: Tue Dec 3 15:32:14 2013 from 10.10.40.225
Number of prior failed login attempts: 17
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 16:34:53 UTC 2013

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ **TSAPI**
 - **TSAPI Links**
 - TSAPI Properties

TSAPI Links

| Link | Switch Connection | Switch CTI Link # | ASAI Link Version | Security |
|------|-------------------|-------------------|-------------------|----------|
| 1 | CM63Vmpg | 1 | 5 | Both |

Add Link **Edit Link** **Delete Link**

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

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

Maintenance | Service Controller Home | Help | Logout

▶ AE Services

- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ **Maintenance**
 - Date Time/NTP Server
 - ▶ Security Database
 - ▶ **Service Controller**
 - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management

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**. Take note of value of the **Tlink Name**, it will be needed later to configure the NICE CTI Connection in **Section 8.1**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar contains the links "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services, with "Security" expanded to show "Security Database", which in turn has "Tlinks" highlighted with a red box. The main content area, titled "Tlinks", shows a "Tlink Name" field with two radio button options: "AVAYA#CM63VMPG#CSTA#AES63VMPG" (selected) and "AVAYA#CM63VMPG#CSTA-S#AES63VMPG". A "Delete Tlink" button is located below the options.

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 8.1**.

AVAYA

**Application Enablement Services
Management Console**

Last login: Thu Nov 27 13:38:43 2014 from 10.10.80.30
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.40.30
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

AE Services

Communication Manager
Interface

High Availability

Licensing

Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

Security

Status

User Management

Utilities

Help

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

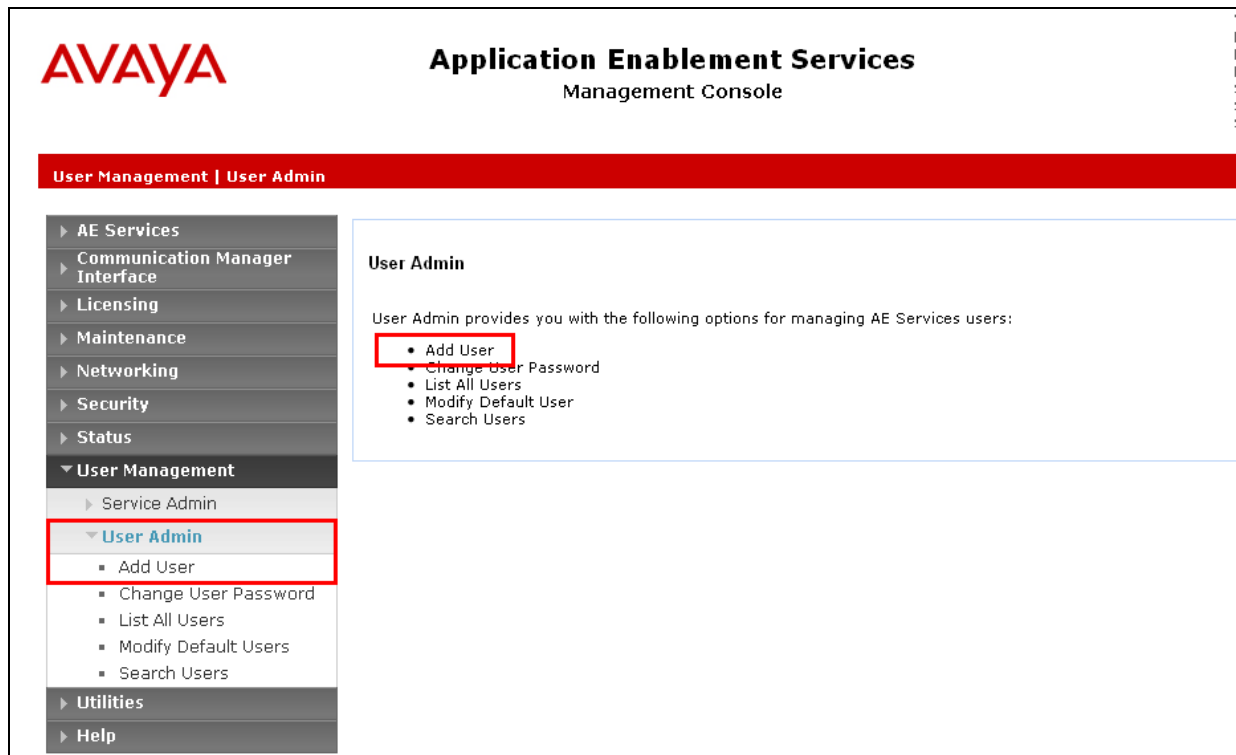
Enabled Disabled

TR/87 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 8.1**.
- **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 8.1**.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** Changes at the bottom of the screen (not shown).

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: AES63VMGP/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
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

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Service Admin
User Admin
Add User
Change User Password
List All Users
Modify Default Users
Search Users
Utilities
Help

Edit User

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

6.7. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**, select **nice** under **User ID**, and click on **Edit**.

AVAYA Application Enablement Services Management Console

Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Dec 01 16:05:02 GMT 2014
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users
Search Users

CTI Users

| 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 |

Edit List All

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

AVAYA Application Enablement Services Management Console

Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Dec 01 16:05:37 GMT 2014
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users

Edit CTI User

User Profile:

| | |
|---------------------|-------------------------------------|
| User ID | nice |
| Common Name | nice |
| Worktop Name | NONE |
| Unrestricted Access | <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 | <input type="checkbox"/> |

Routing Control:

| | |
|---------------------------------|------|
| Allow Routing on Listed Devices | None |
|---------------------------------|------|

Apply Changes Cancel Changes

7. Configure Avaya Proactive Contact

It is assumed that a fully operational Proactive Contact is in place and the connection is made to Communication Manager in order to acquire agents. Documentation on the Installation and Configuration of Proactive Contact may be found in **Section 11** of these Application Notes.

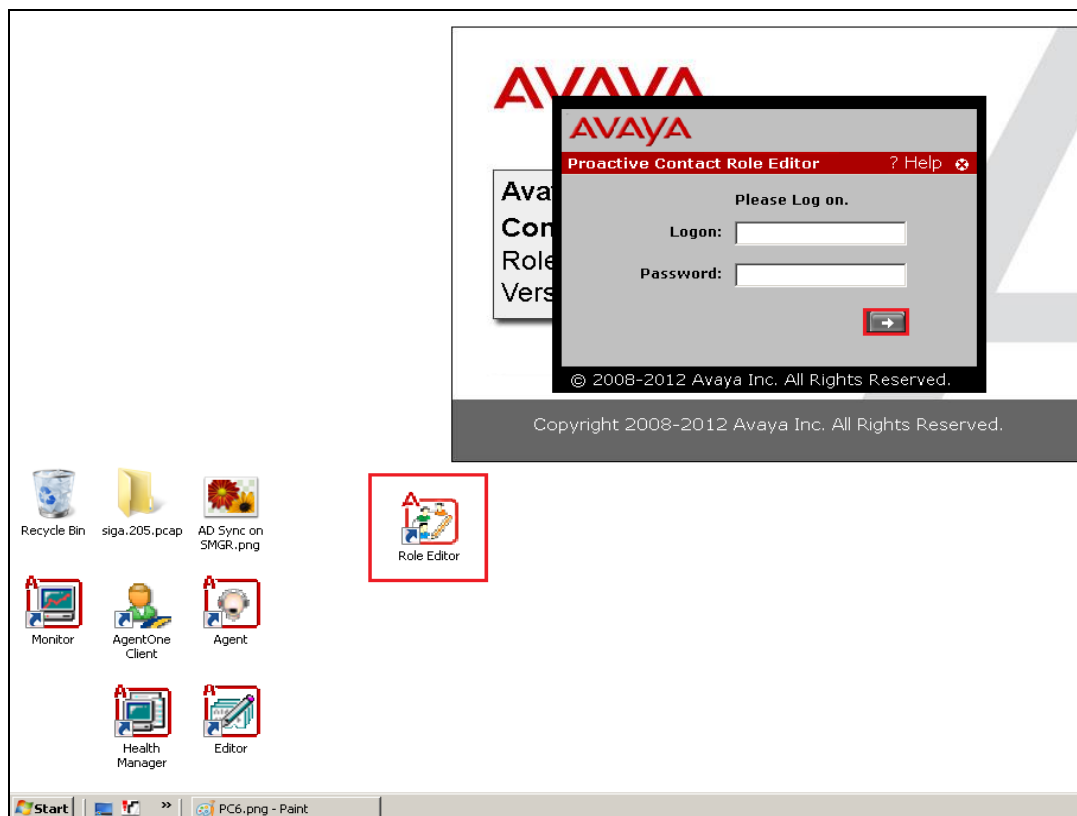
7.1. Obtain Proactive Contact Certificates

NICE Engage Platform is required to register certificates from Avaya Proactive Contact and these certificates can be obtained as follows:

1. On the Proactive Contact server, go to **/opt/avaya/pds/openssl**
2. Copy the following files
 /private/**corbaServer_key.pem**
 /certificate/**corbaServer_cert.pem**
 /cacertificate/**ProactiveContactCA.pem**
3. Paste the above three files into the **C:\Certificates** folder on the NICE Engage Platform.

7.2. Check Proactive Contact Event User Details

Proactive Contact is installed with 10 pre-configured agents Agent 01-10 with corresponding passwords. The default client1 was used to register for events from Proactive Contact. To check on these users open Proactive Contact **Role Editor**, enter the correct credentials and click on the login icon highlighted.



Click on **User Management** at the top left of the screen and select the correct **Tenant** from the main window. A list of **Tenant Users** is then displayed in the right window with **Client1** highlighted as shown. If this user is not present a different user may be used to monitor events. Note this Client1 user will be used later in **Section 8.3**.

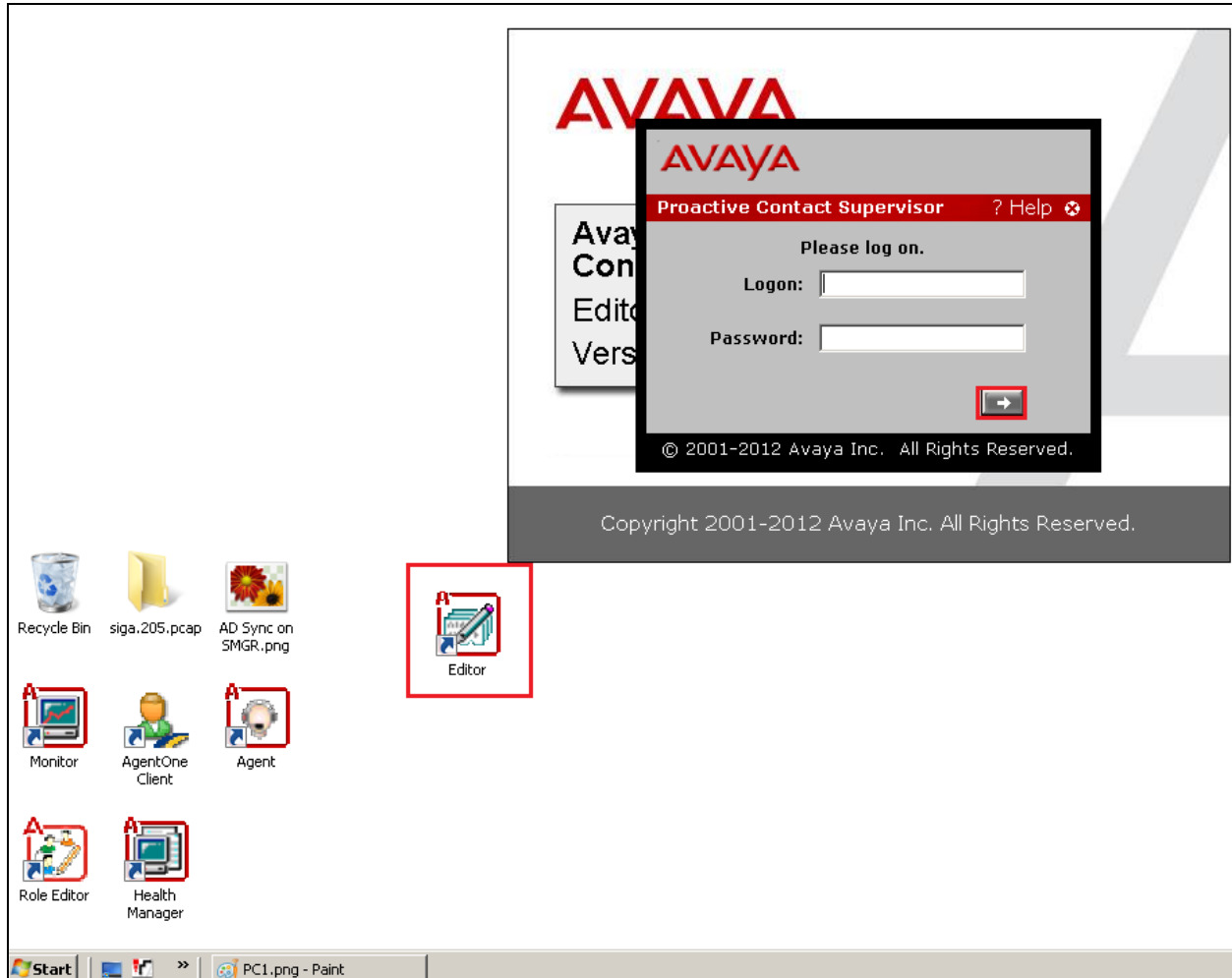
The screenshot shows the 'Proactive Contact Administration Tool' window. The left sidebar has 'User Management' selected. The main area is titled 'Tenant Management: Default - Active' and contains a table with tenant information. Below this, a 'Tenant Users' table is displayed, with 'client1' highlighted in red.

| Tenant Name | Tenant Description | Dialer | Version | Attribute | Attribute Value |
|-------------|--------------------------|-------------|---------|--------------------|-----------------|
| Ten01 | First Alternative Tenant | DEVCONHD501 | Active | Blend Domain Group | NORTH_USA |
| Default | Default Tenant | DEVCONHD501 | Active | Calling Lists | 978 |
| | | | | Completion Codes | 210-999 |
| | | | | Description | Default Tenant |

| User Name | User Type | Tenant Administrator |
|-----------|-----------|----------------------|
| admin | system | |
| agent1 | agent | |
| agent10 | agent | |
| agent2 | agent | |
| agent3 | agent | |
| agent4 | agent | |
| agent5 | agent | |
| agent6 | agent | |
| agent7 | agent | |
| agent8 | agent | |
| agent9 | agent | |
| analysis | pcanal | |
| auditor | auditor | |
| client1 | agent | |
| cust1 | system | |
| dadmin | system | |
| leadadm | leadadm | |
| roleadm | rbac | |
| rsync | system | |
| sysadm | sysadm | |
| system | system | |
| ten01adm | sysadm | |

7.3. Start Proactive Contact Jobs running

To start a job on Proactive Contact open Proactive Contact **Editor**, enter the correct credentials and click on the login icon highlighted.



Once logged in click on any job that requires starting for example **outbnd2** as is highlighted below and right-click on that job and select **Run**. That will start that particular job and allow the Proactive Contact agents to join that job.

The screenshot shows the 'Editor - [Jobs: Active outbnd2]' window. On the left is a sidebar with 'Contact Management' and icons for Strategies, Selections, Selection Reports, Jobs (highlighted with a red box), and Job Templates. The main area displays a table of jobs. The job 'outbnd2' is highlighted in blue, and a right-click context menu is open over it, with the 'Run' option highlighted in red. The table columns are Job, Job type, File Version, Outbound list, Inbound list, and Status. The job details on the right show settings for Basic, Call, Files, and Interact.

| Job | Job type | File Version | Outbound list | Inbound list | Status |
|------------|----------|--------------|--------------------|--------------------|---------|
| outbnd3 | Outbound | Active | devconhd501-list10 | | Running |
| outbnd4 | Outbound | Active | devconhd501-list6 | | Running |
| outbnd6 | Outbound | Active | devconhd501-list8 | | Running |
| NiceBlend | Blend | Active | devconhd501-list11 | devconhd501-inbnd6 | Stopped |
| blend | Blend | Active | devconhd501-list1 | devconhd501-inbnd1 | Stopped |
| blendPG | Blend | Active | devconhd501-list4 | devconhd501-inbnd5 | Stopped |
| inbnd1 | Inbound | Active | | devconhd501-inbnd4 | Stopped |
| inbnd2 | Inbound | Active | | devconhd501-inbnd2 | Stopped |
| inbnd4 | Inbound | Active | | devconhd501-inbnd6 | Stopped |
| inbnd5pg | Inbound | Active | | devconhd501-inbnd5 | Stopped |
| inbnd6 | Inbound | Active | | devconhd501-inbnd6 | Stopped |
| infinity10 | Outbound | Active | devconhd501-list10 | | Stopped |
| managed | Managed | Active | devconhd501-list10 | | Stopped |
| outbnd | Outbound | Active | devconhd501-list1 | | Stopped |
| outbnd2 | Outbound | Active | devconhd501-list10 | | Stopped |
| outbnd5 | Outbound | Active | devconhd501-list7 | | Stopped |
| verify | Outbound | Active | devconhd501-list1 | | Stopped |
| virtual | Virtual | Active | devconhd501-list1 | | Stopped |
| ManagedPG1 | Managed | Active | devconhd501-list10 | | Stopped |
| InboundPG1 | Inbound | Active | | devconhd501-inbnd6 | Stopped |

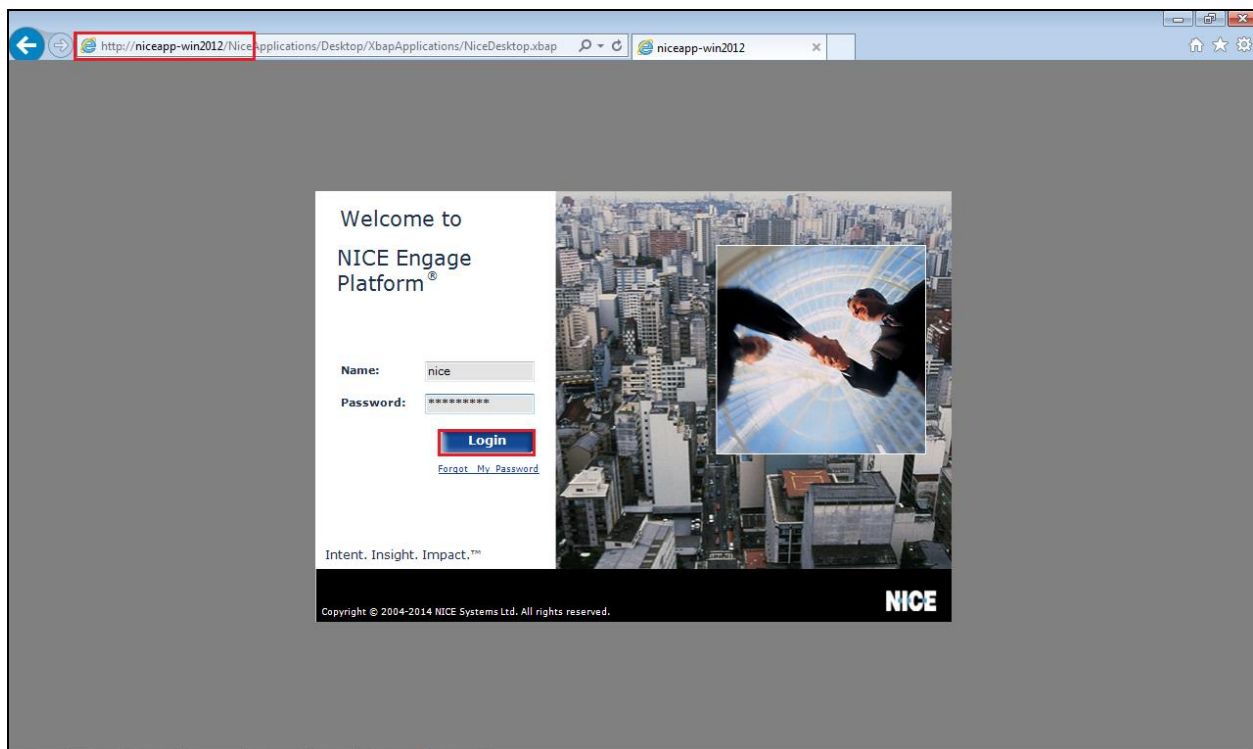
Job Detail:

- Basic**
 - Job: generic
 - Tagged: 0
 - Line: REG
 - Earliest: 08:00
 - Latest: 23:57
 - Calling: 0
 - Require: ☐
 - Transacti: 93
- Call**
 - Call: Expert Calling Ratio
 - Expert: w/0
 - Initial hit: 50
 - Minimum: 20
 - Cell: 0
- Files**
 - Outboun: devconhd501-list10
 - Record: all
 - Outboun: list1
 - Agent: ag_cmd1
 - Do Not: DNC
 - Name of: inbnd1
- Interact**
 - Allow: ☐
 - IVR:
 - Initial:
 - Script to:
- Job**

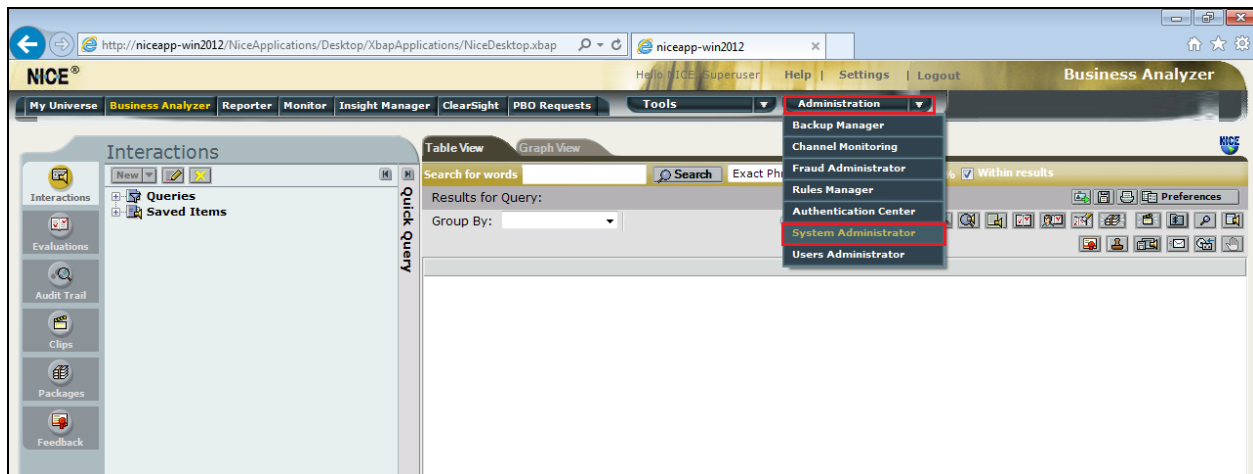
8. Configure NICE Engage Platform

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**.

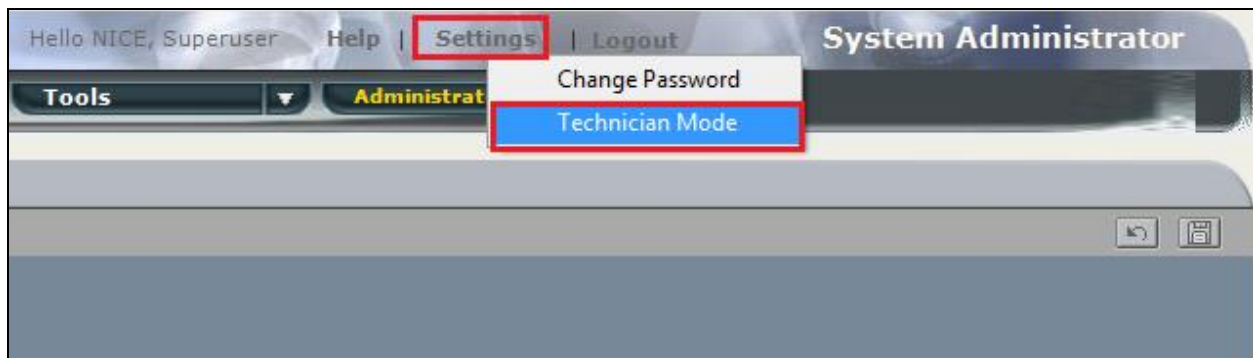
The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya Solution. All configuration of the NICE Engage Platform for connection with the AES is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser as shown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

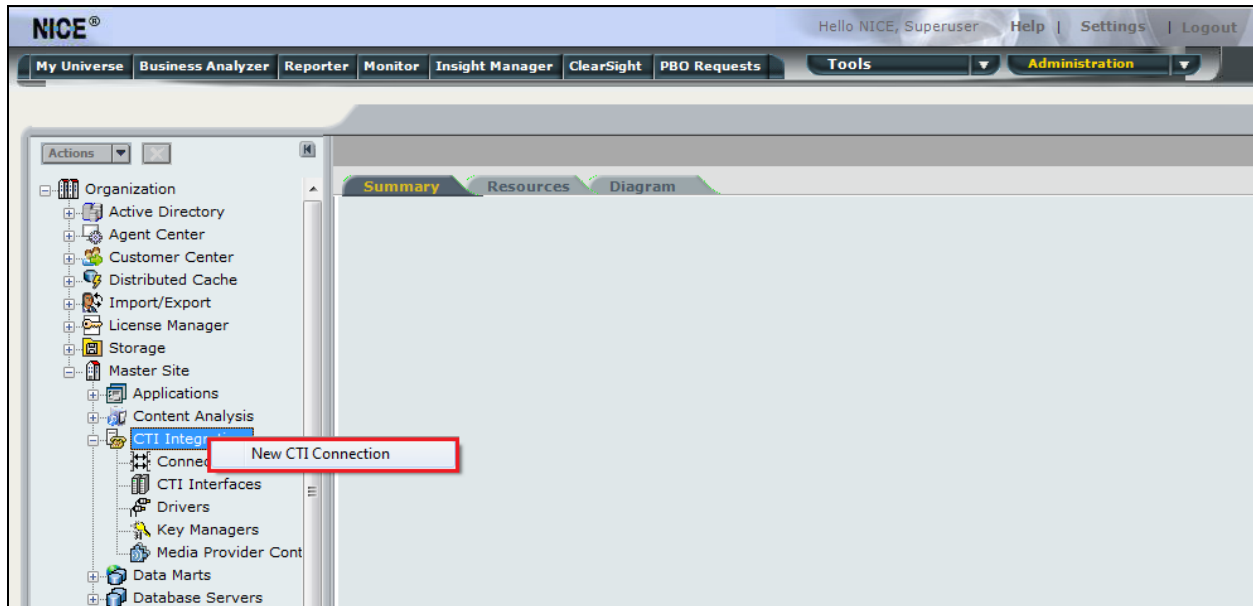


Before any changes can be made, switch to **Technician Mode** by clicking into **Settings** at the top of the screen as shown below.

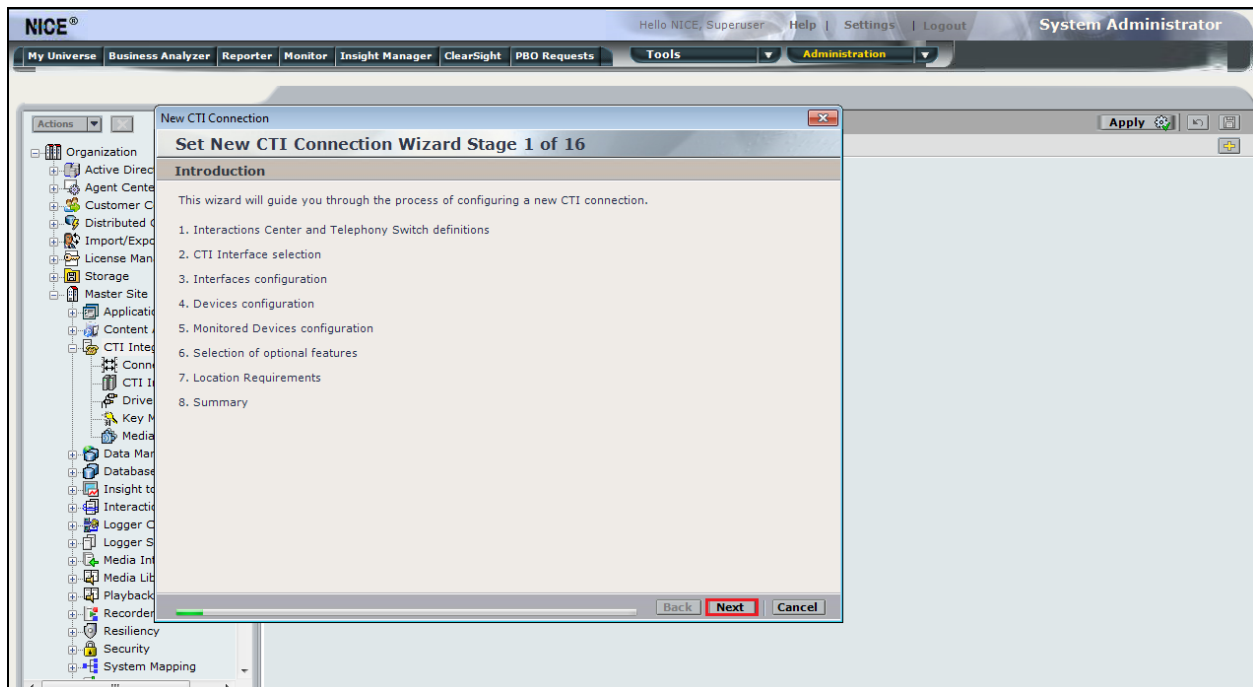


8.1. New CTI Connection

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 Multi-Registration type of call recording. Click on **Next** to continue.

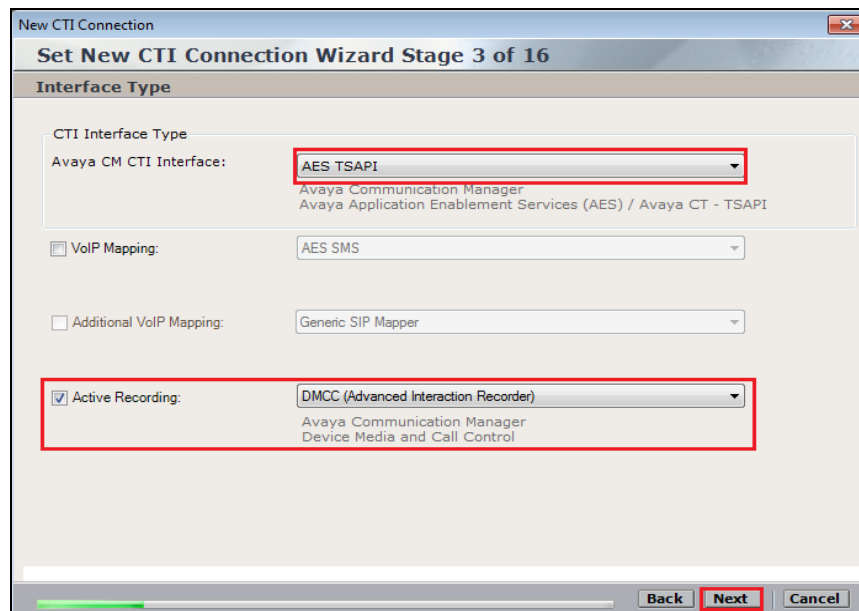


The value for Regular Interactions Center is a value that was already created during the installation of the NICE Engage platform. This value is therefore pre-chosen for the CTI connection being created below.

The **Telephony Switch** must be selected, under **Switch Type** select **Avaya CM** from the dropdown menu. Enter a suitable name for this **Switch Name**. Click on **Next** to continue.



Select **AES TSAPI** for the **Avaya CM CTI Interface**, ensure that **Active Recording** is ticked and select the **DMCC (Advanced interaction Recorder)** from the dropdown menu. Click on **Next** to continue.



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

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**. Click **OK**.

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

Set Parameter Value

Interface Connection Parameter

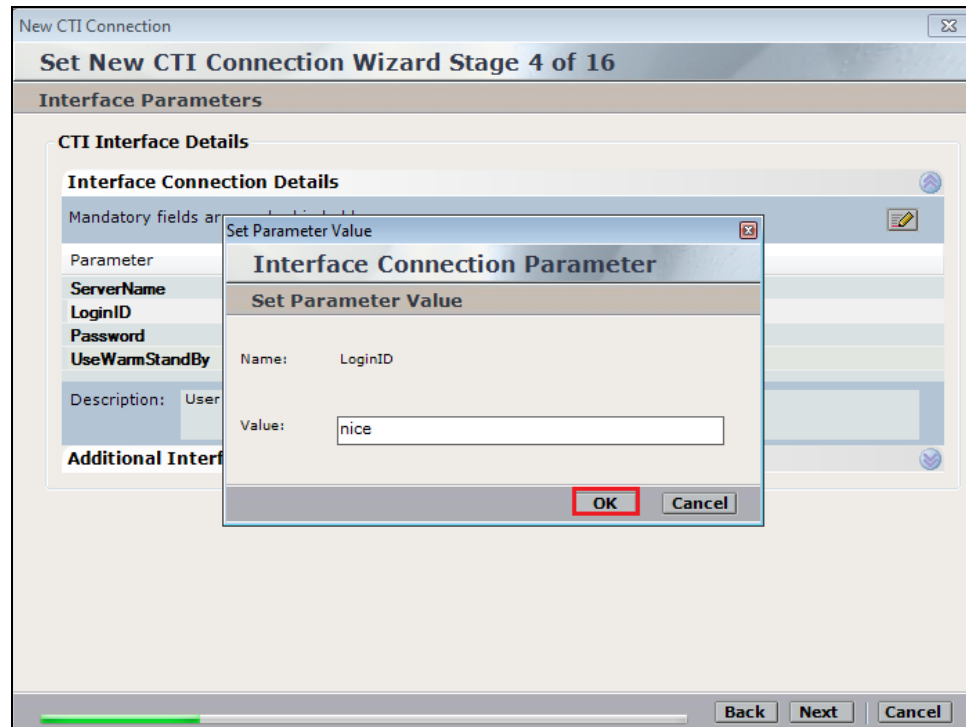
Set Parameter Value

Name: ServerName

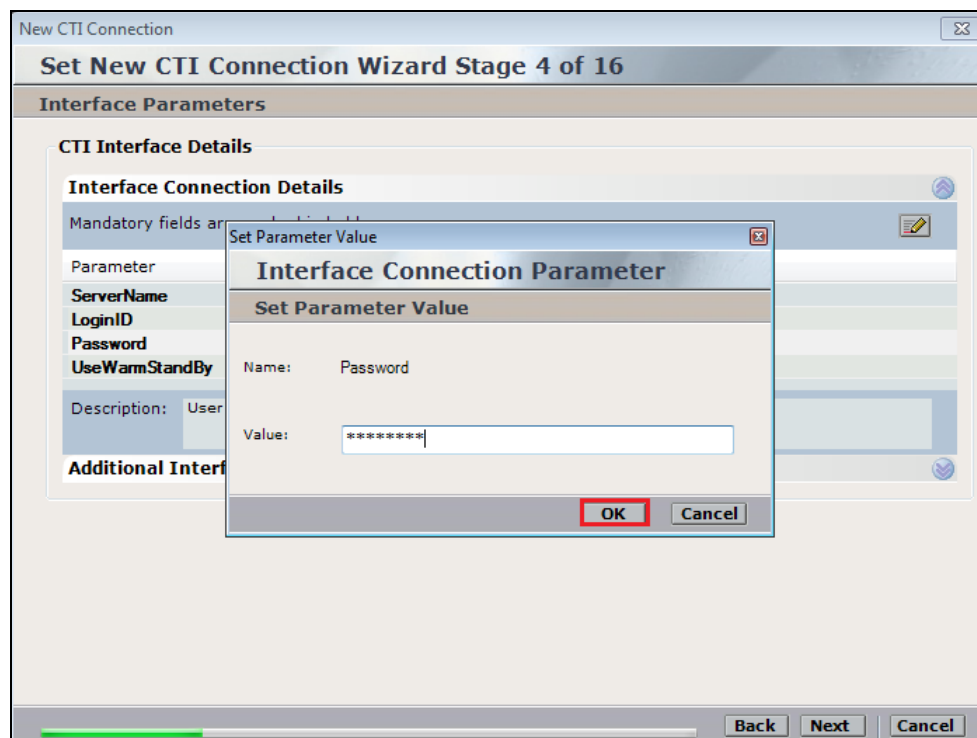
Value: AVAYA#CM63VMGP#CSTA#AES63VMGP

OK Cancel

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



Double-click on **Password** and enter the value for the password that was created in **Section 6.6**. Click on **OK** to continue.



Click on **Next** once all values have been all filled in.

The screenshot shows the 'Set New CTI Connection Wizard Stage 4 of 16' window. The 'Interface Parameters' section is active. Under 'CTI Interface Details', the 'Interface Connection Details' table is highlighted with a red box. The table has two columns: 'Parameter' and 'Value'. The rows are: 'ServerName' with value 'AVAYA#CM63VMPG#CSTA#AES63VMPG', 'LoginID' with value 'nice', 'Password' with value '*****', and 'UseWarmStandBy' with value 'No'. Below the table is a 'Description' field with the text 'Is warm standby supported?'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red box.

| Parameter | Value |
|----------------|-------------------------------|
| ServerName | AVAYA#CM63VMPG#CSTA#AES63VMPG |
| LoginID | nice |
| Password | ***** |
| UseWarmStandBy | No |

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

The screenshot shows the 'Set New CTI Connection Wizard Stage 8 of 16' window. The 'Active Recording' section is active. Under 'Active Recording Interface Details', the 'Interface Connection Details' table is highlighted with a red box. The table has two columns: 'Parameter' and 'Value'. The rows are: 'PrimaryAESServerAddress', 'PrimaryAESDMCCPort' with value '4722', 'PrimaryAESUserName', 'PrimaryAESPassword', and 'PrimaryAESStandByConnection' with value 'TRUE'. Below the table is a 'Description' field. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a red box.

| Parameter | Value |
|-----------------------------|-------|
| PrimaryAESServerAddress | |
| PrimaryAESDMCCPort | 4722 |
| PrimaryAESUserName | |
| PrimaryAESPassword | |
| PrimaryAESStandByConnection | TRUE |

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

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter

PrimaryAESServerAddress

PrimaryAESDMCCPort

PrimaryAESUserName

PrimaryAESPassword

Description: AES Server IP Address

Additional Interface Parameters

Media Provider Controllers

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

Name: PrimaryAESServerAddress

Value: 10.10.40.30

OK Cancel

Back Next Cancel

Enter the **Value** for the **AESDMCCPort**, note this will be the same port that was configured in **Section 6.5**. In this example the unencrypted port **4721** is entered. Click on **OK**.

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter

PrimaryAESServerAddress

PrimaryAESDMCCPort

PrimaryAESUserName

PrimaryAESPassword

Description: DMCC

Additional Interface Parameters

Media Provider Controllers

Set Parameter Value

Interface Connection Parameter

Set Parameter Value

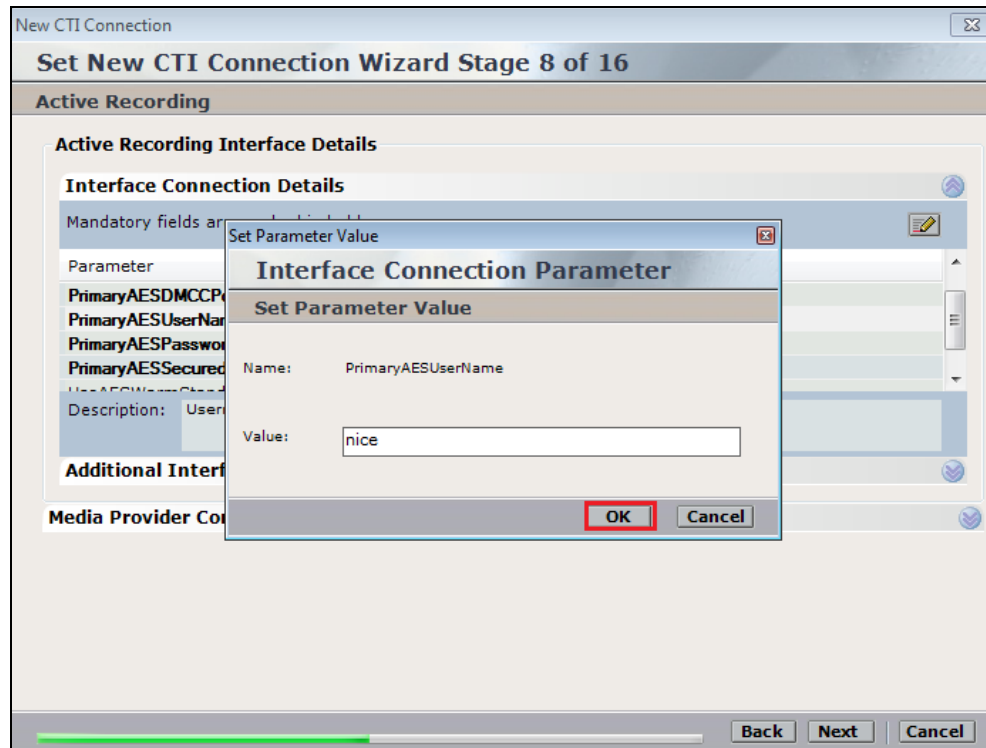
Name: PrimaryAESDMCCPort

Value: 4721

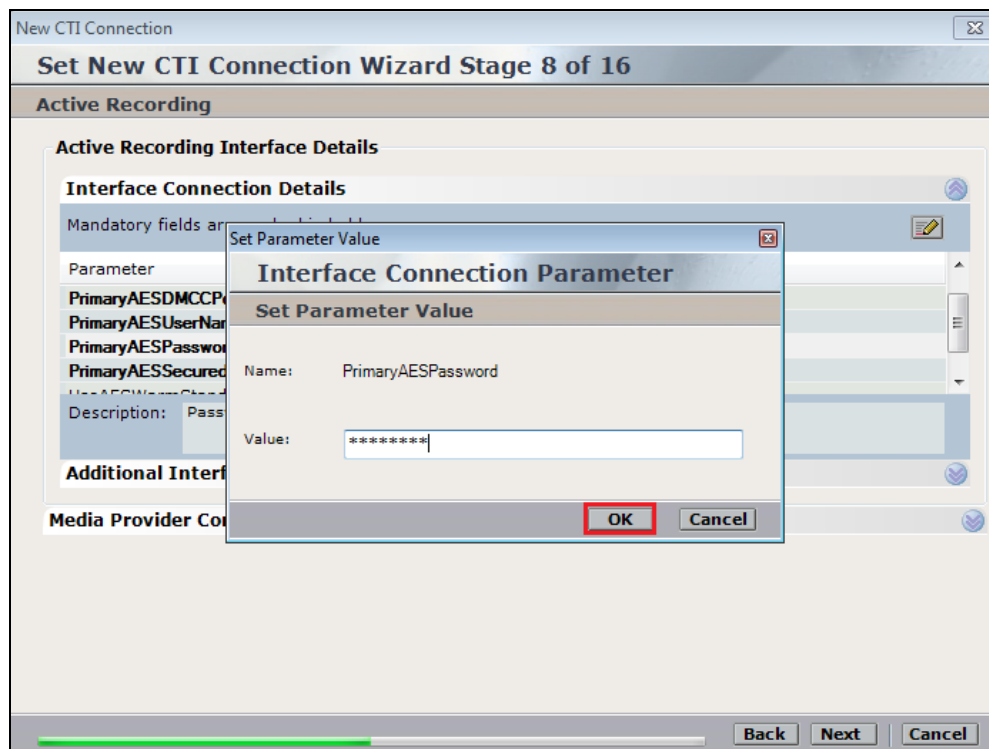
OK Cancel

Back Next Cancel

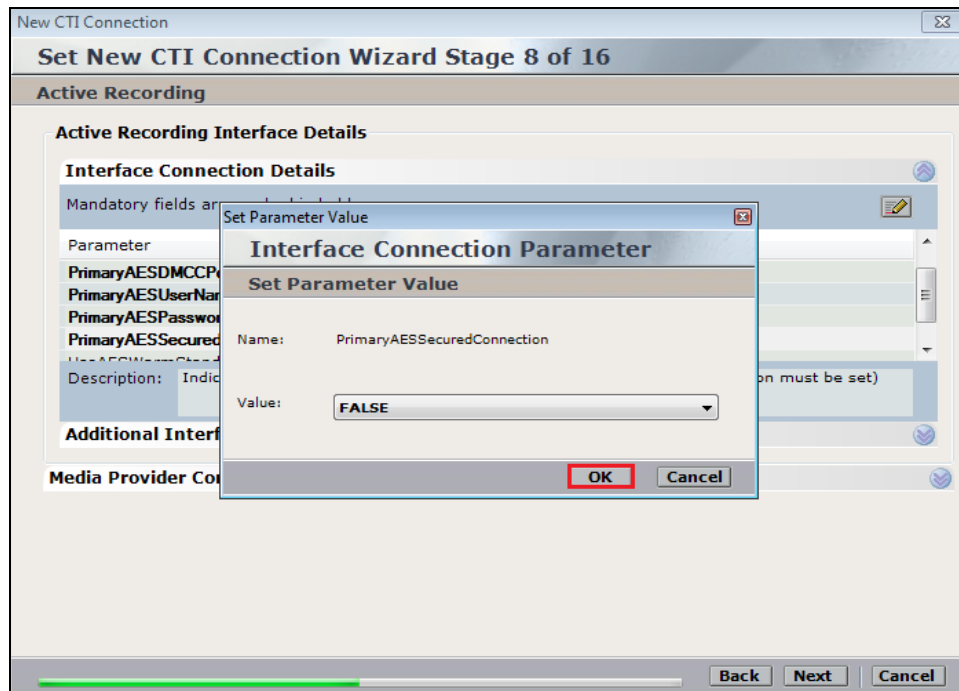
As before enter the username that was created in **Section 6.6** and click on **OK**.



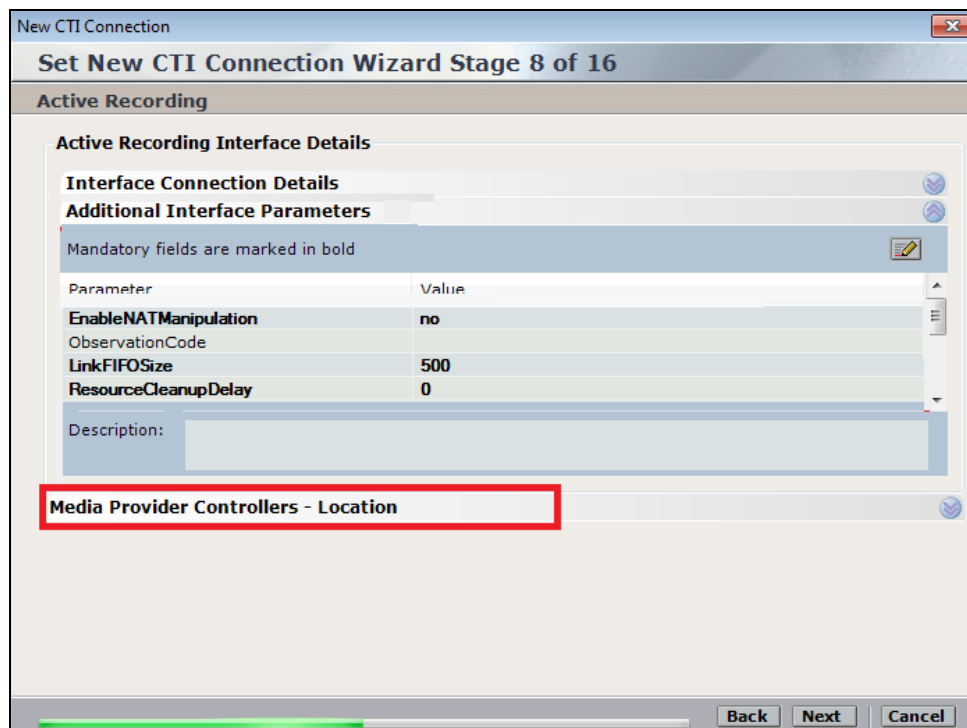
Enter the password that was created in **Section 6.6** and click on **OK**.



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



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



Enter the **IP/Hostname** of the Nice Advanced Interactions Server. Click on in + icon to add this entry.

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Additional Interface Parameters

Media Provider Controllers - Location

Media Provider Location

Server IP/Hostname: NICEActive2012

Connection Manager Port: 62094

Media Provider Controllers:

| IP/Hostname | CM Port |
|-------------|---------|
| | |
| | |
| | |

Back Next Cancel

Click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Additional Interface Parameters

Media Provider Controllers - Location

Media Provider Location

Server IP/Hostname:

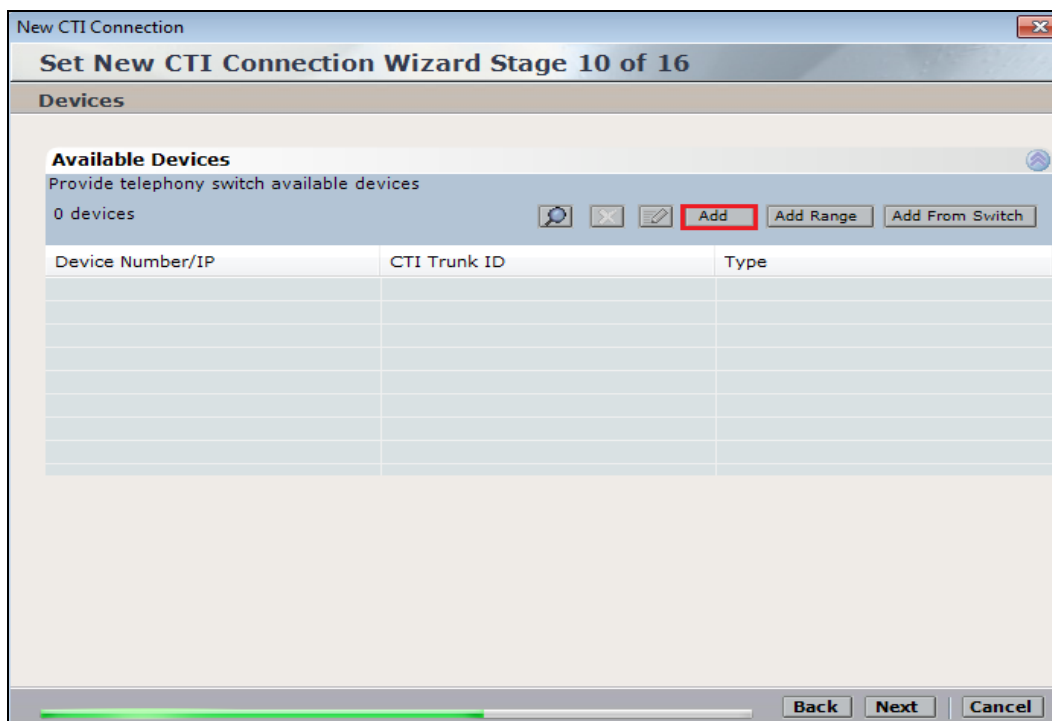
Connection Manager Port: 62094

Media Provider Controllers:

| IP/Hostname | CM Port |
|----------------|---------|
| NICEActive2012 | 62094 |
| | |
| | |

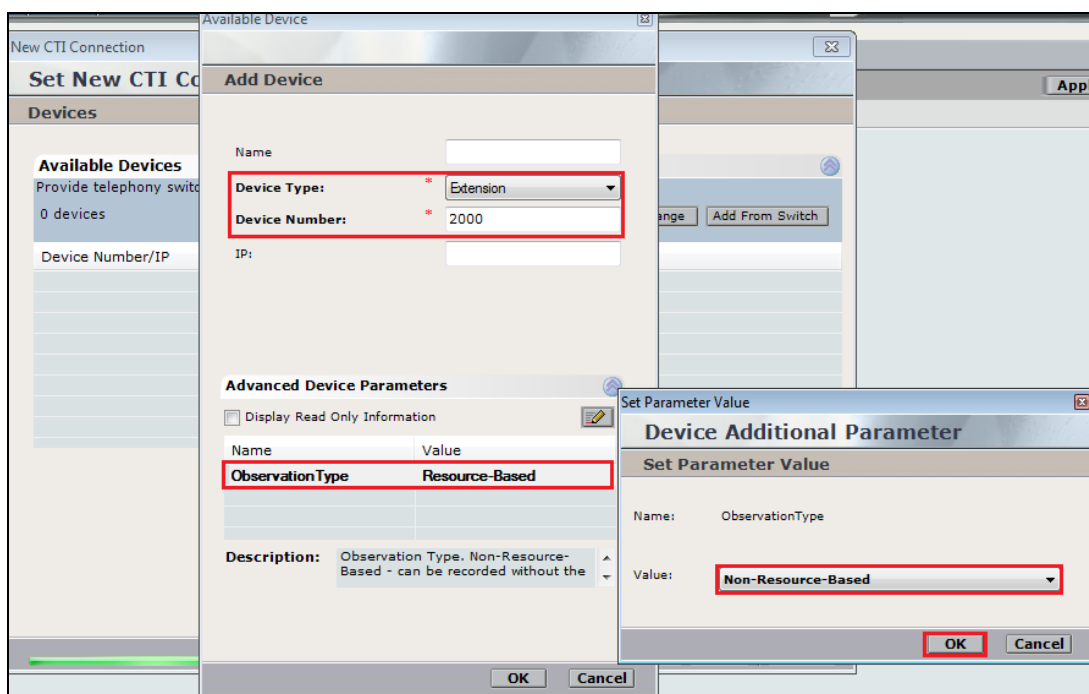
Back Next Cancel

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



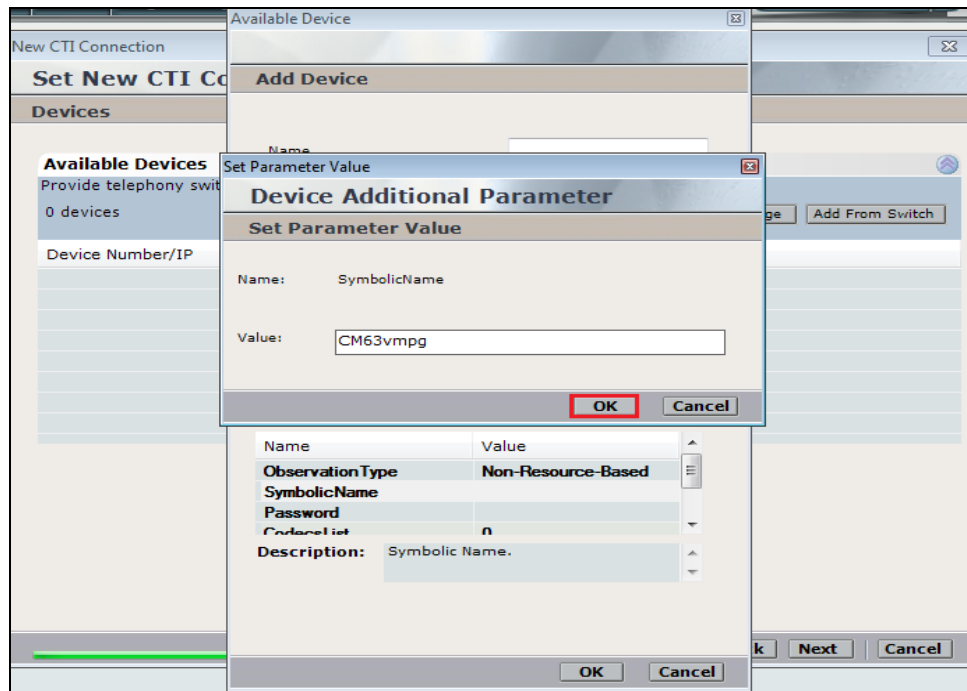
The screenshot shows the 'Set New CTI Connection Wizard Stage 10 of 16' window. The 'Devices' section is active, displaying 'Available Devices' with a list of 0 devices. The 'Add' button is highlighted with a red box. Below the list is a table with columns: Device Number/IP, CTI Trunk ID, and Type. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

The **Device Type** should be **Extension** and insert the correct extension number. Expand **Advanced Device Parameters** and ensure that the **Value** for **Observation Type** is set to **Non-Resourced-Based**. Click on **OK** to continue.

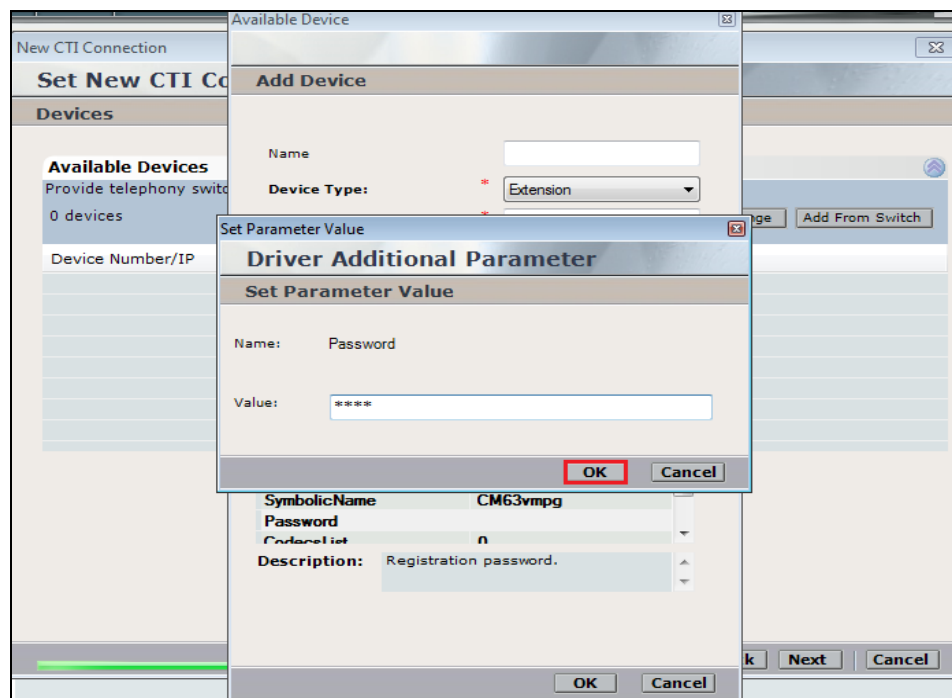


The screenshot shows the 'Add Device' dialog box and the 'Set Parameter Value' dialog box. In the 'Add Device' dialog, the 'Device Type' is set to 'Extension' and the 'Device Number' is '2000'. The 'Advanced Device Parameters' section is expanded, showing 'ObservationType' set to 'Resource-Based'. The 'Set Parameter Value' dialog box is open, showing the 'ObservationType' parameter set to 'Non-Resource-Based'. The 'OK' button is highlighted with a red box.

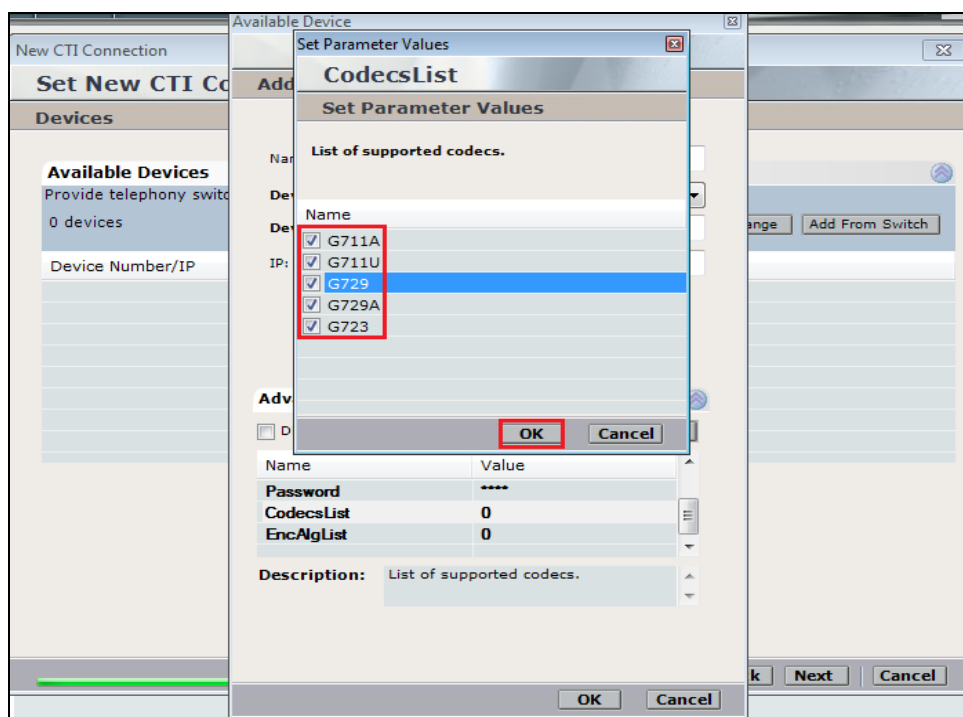
Next enter the correct **Value** for **SymbolicName**. Double-click on **SymbolicName** to set the value. This should be the same as the switch name entered in **Section 6.2**. Click **OK**.



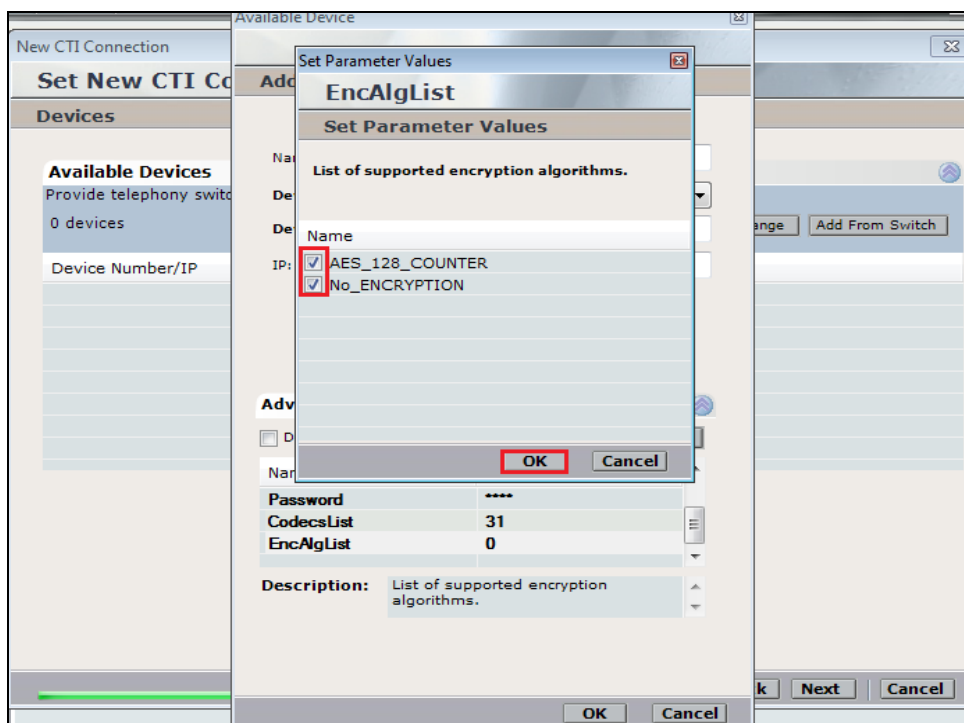
Enter the correct **Password** and note this is the password for the extension that is being added here. This is the station password which was entered during the creation of the station. A printout of an extension can be found in **Section 5.5** of these Application Notes. Click **OK**.



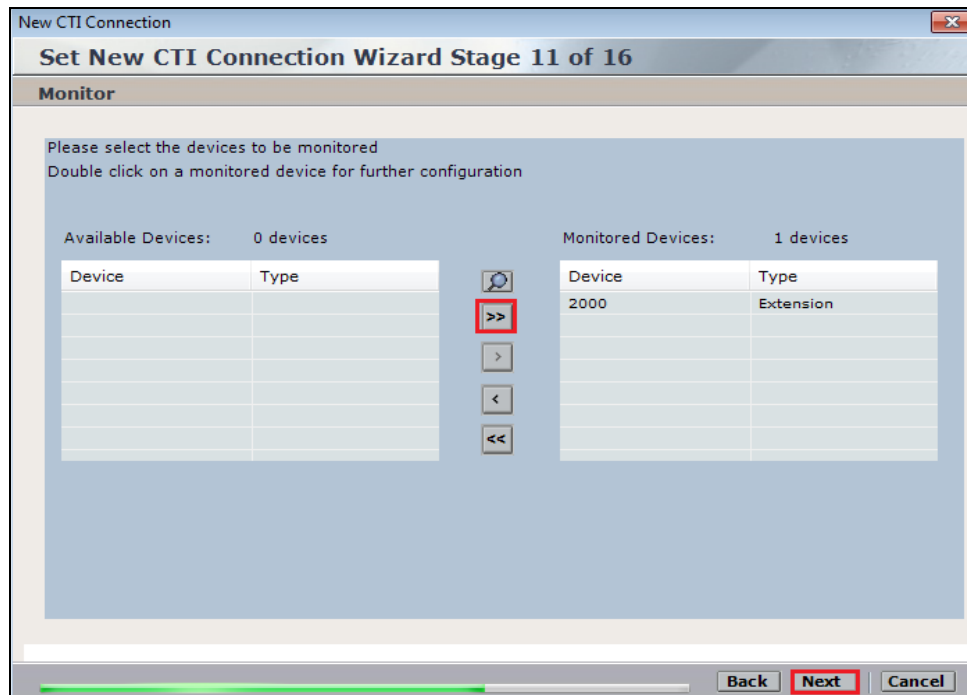
Double-click on **CodecsList** and ensure that all the values are ticked as shown below. Click on **OK** to continue.



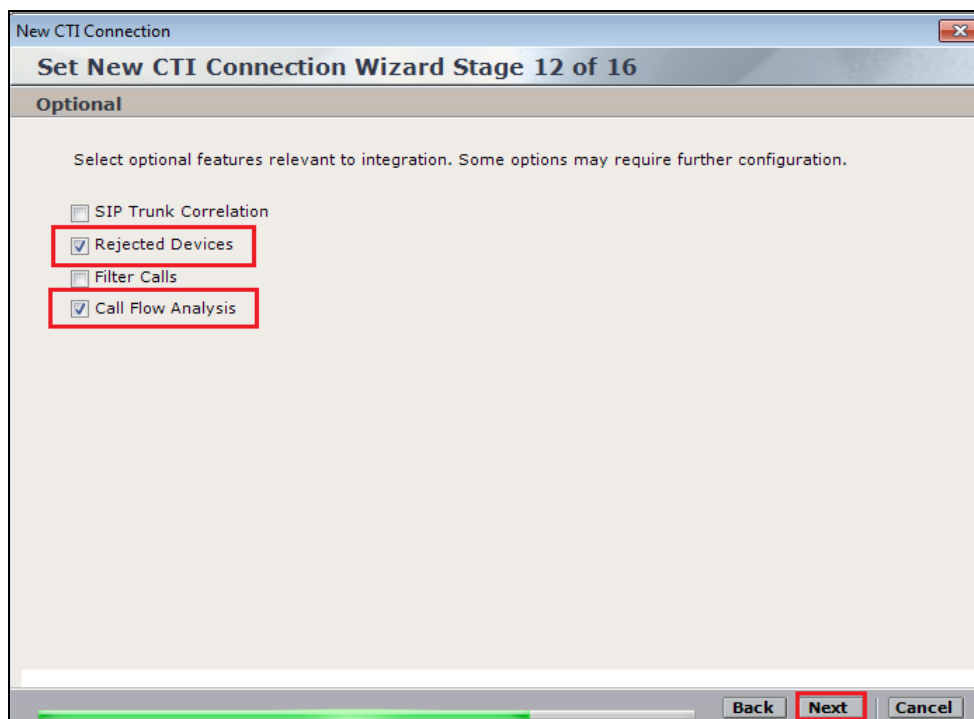
Double-click on **EncAlgList** and ensure both options are ticked as shown below. Click on **OK** to continue.



Under **Available Devices** select the new extension and click on the >> icon to move it to the **Monitored Devices**, as shown. Click on **Next** to continue.



This is optional, but for better analysis tick on **Call Flow Analysis**. For the connection to Proactive Contact **Rejected Devices** must also be ticked, then click on **Next** to continue.



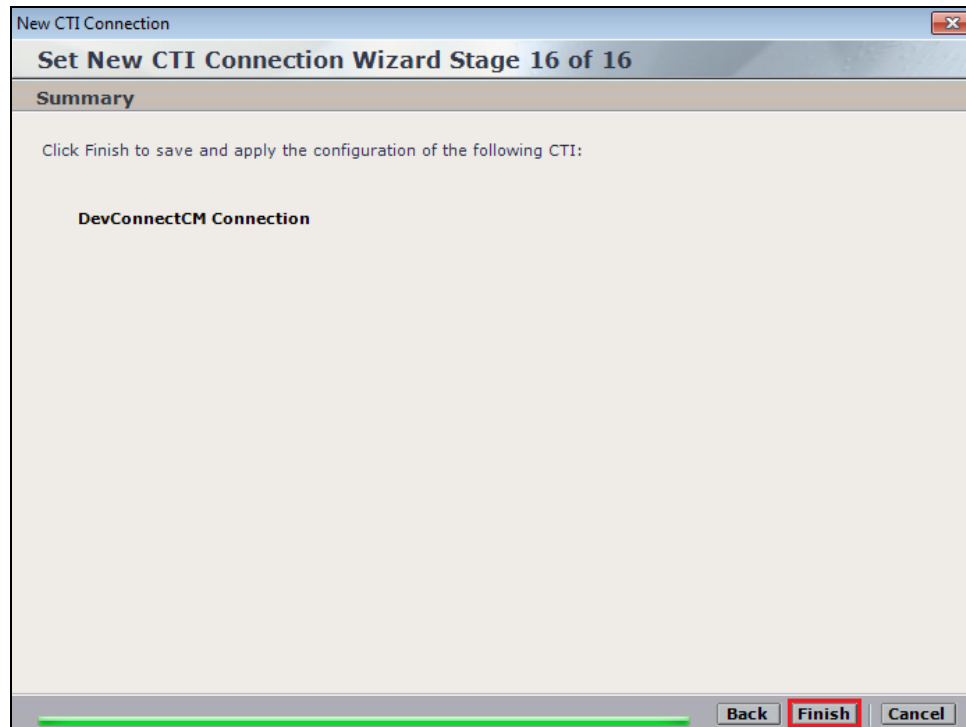
Enter the trunk number of the trunk that connects the Proactive Contact to Communication Manager. In the example below this is 3 so **T3#*** (Trunk 3 all channels) is added and selected. Click on **Next** to continue.

The screenshot shows a window titled "New CTI Connection" with the subtitle "Set New CTI Connection Wizard Stage 14 of 17". The main section is titled "Rejected Devices" and contains the instruction "Please select the devices to be rejected". On the left, under "Available Devices:", it says "0 devices" and shows an empty table with columns "Device" and "Type". On the right, under "Rejected Devices:", it says "1 devices" and shows a table with columns "Device" and "Type". The first row in the "Rejected Devices" table is highlighted with a red box and contains the text "T3#*" in the "Device" column and "RejectedDevice" in the "Type" column. Between the two tables are navigation buttons: a magnifying glass, ">>", ">", "<", and "<<". At the bottom right are "Back", "Next", and "Cancel" buttons. The "Next" button is highlighted with a red box.

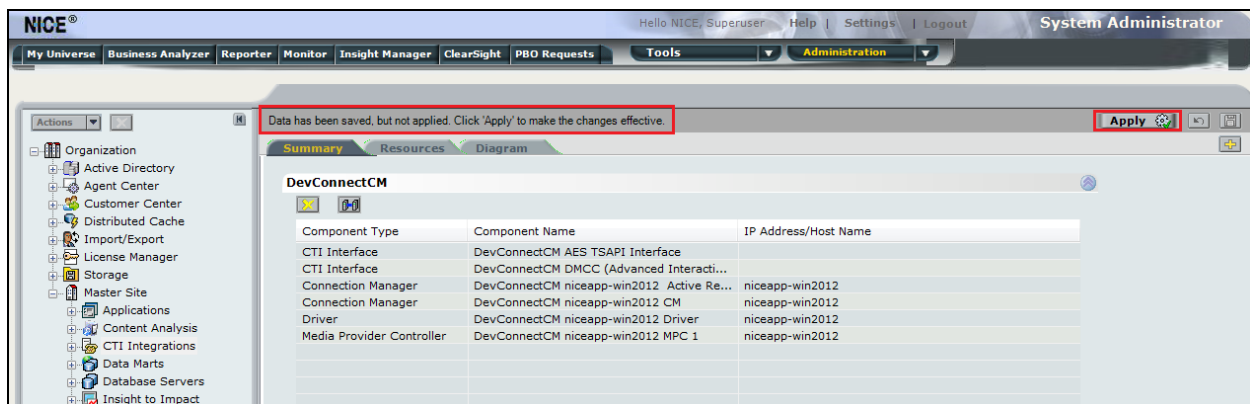
Select a different **Port** number as shown below, **62095** is chosen simply because **62094** was already in use.

The screenshot shows a window titled "New CTI Connection" with the subtitle "Set New CTI Connection Wizard Stage 15 of 16". The main section is titled "Requirements" and contains the text: "The Interactions Center server selected already has a Connection Manager. Create a new Connection Manager, or select an existing one." There are two radio button options. The first option, "Create a new Connection Manager", is selected and highlighted with a red box. Below it is a "Port:" label followed by a text box containing "62095", which is also highlighted with a red box. The second option, "Select available Connection Manager", is unselected. Below it is a "Ports in use:" label followed by a text box containing "62094". At the bottom right are "Back", "Next", and "Cancel" buttons. The "Next" button is highlighted with a red box.

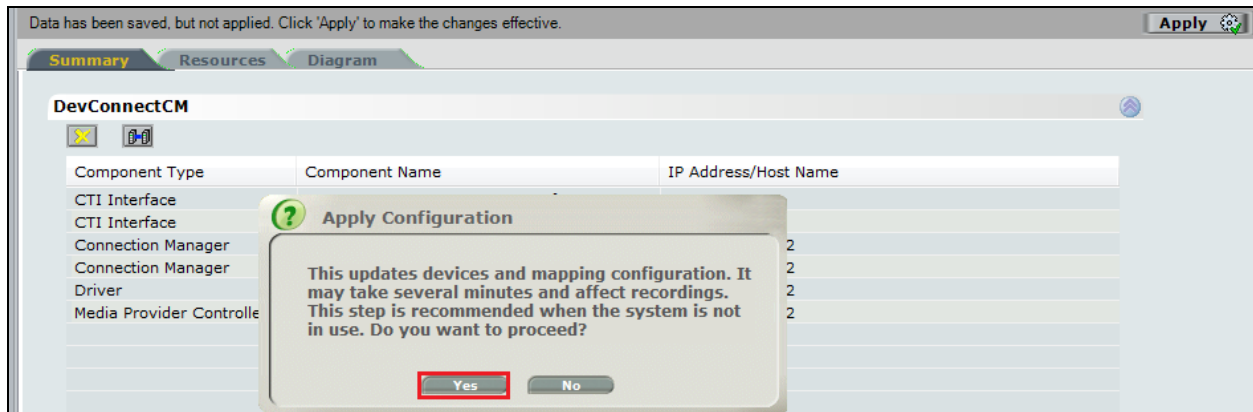
Click on **Finish** to complete the New CTI Wizard.



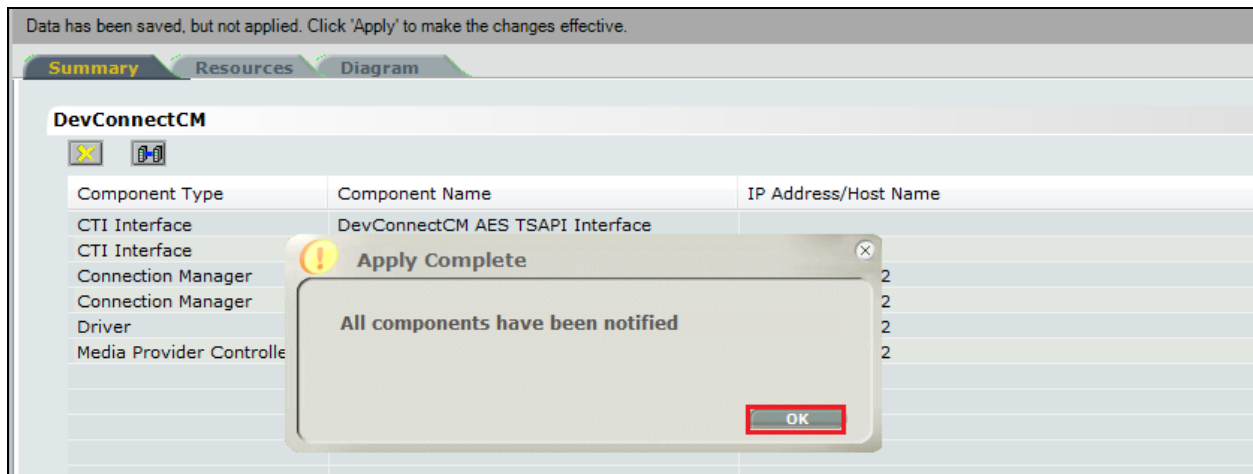
Click on **Apply** at the top right of the screen to save the new connection.



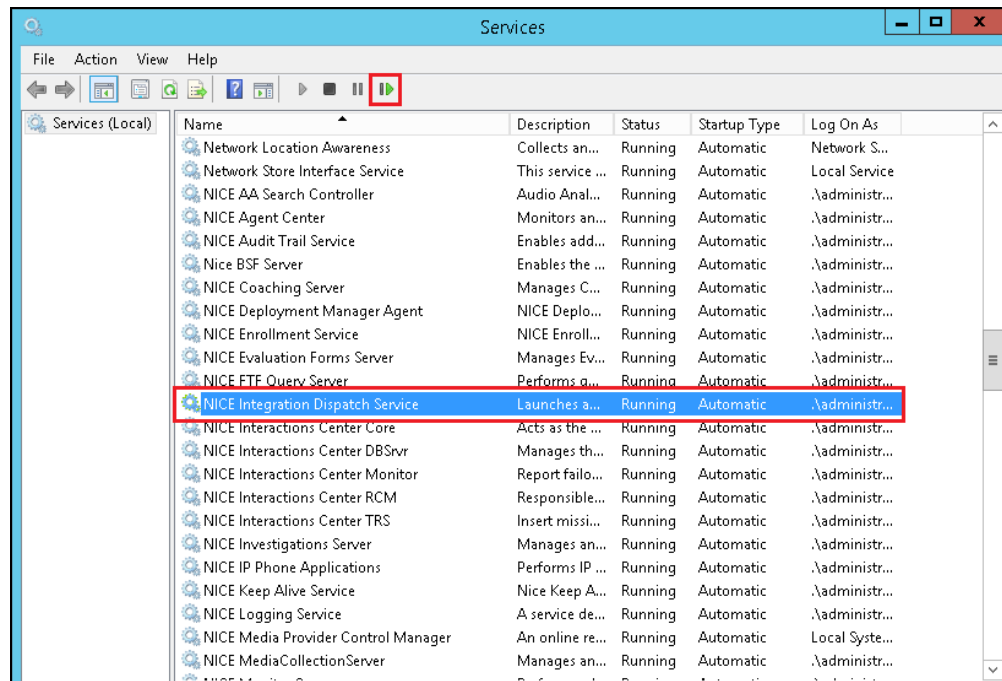
Click on **Yes** to proceed.



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

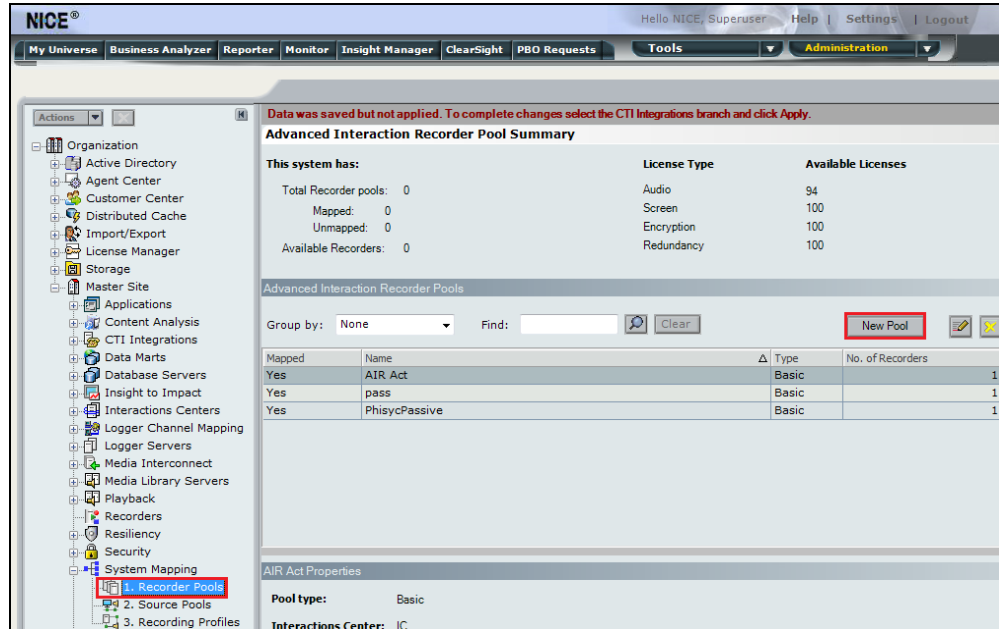


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

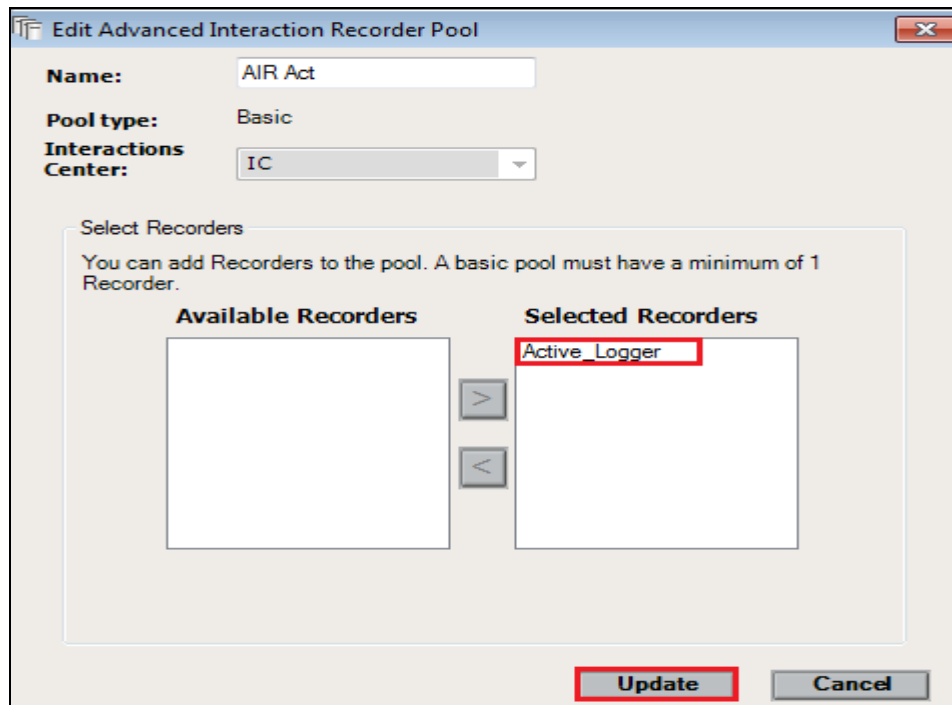


8.2. System Mapping

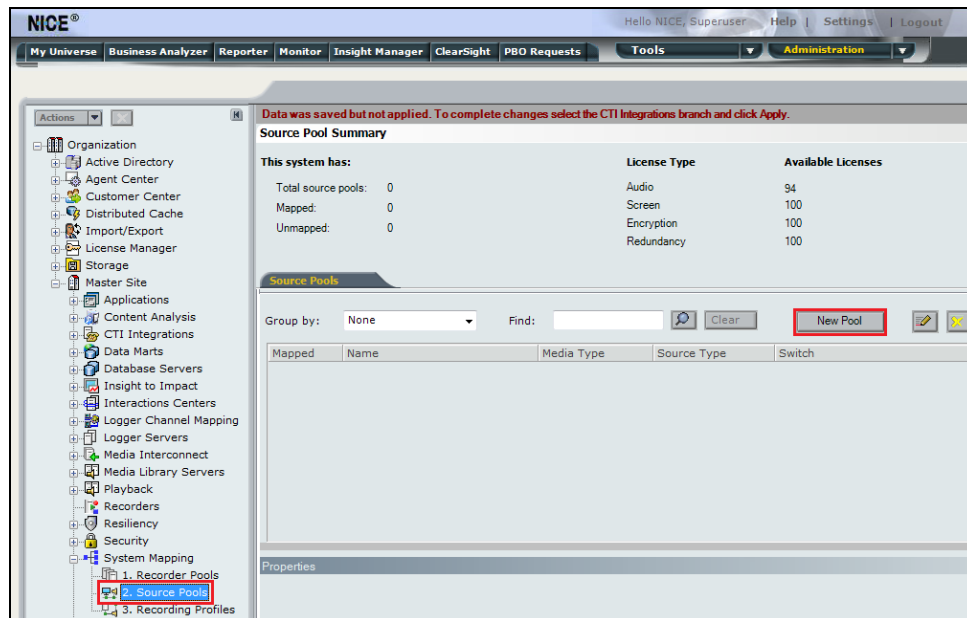
From the web browser navigate to **Master Site → System Mapping → Recorder Pools**. In the main window click on **New Pool**.



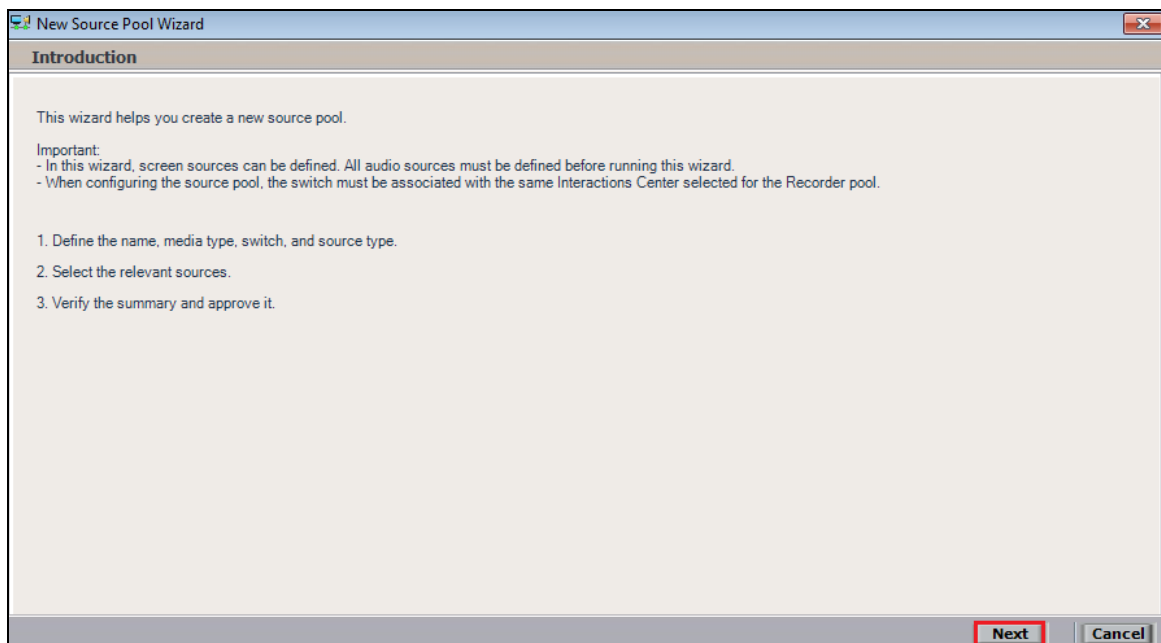
Enter a suitable **Name** for the **Recorder Pool** and select the **Active_Logger** from the list of **Available Recorders** and click on **Update** to continue.



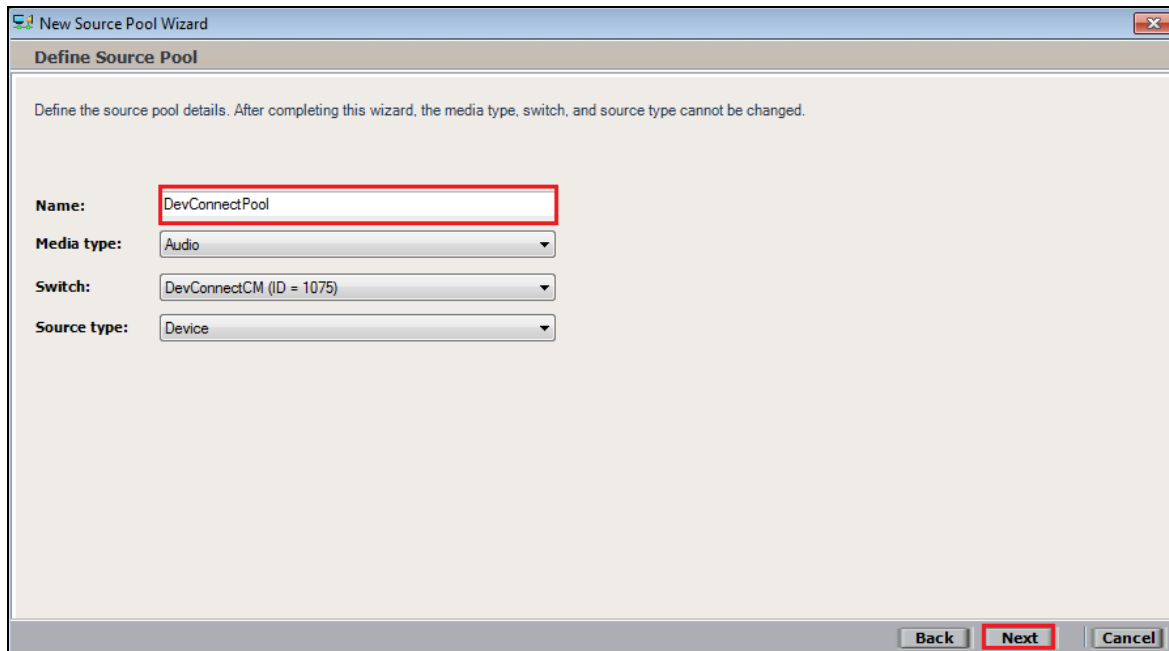
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



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 are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red box.

Name: DevConnectPool

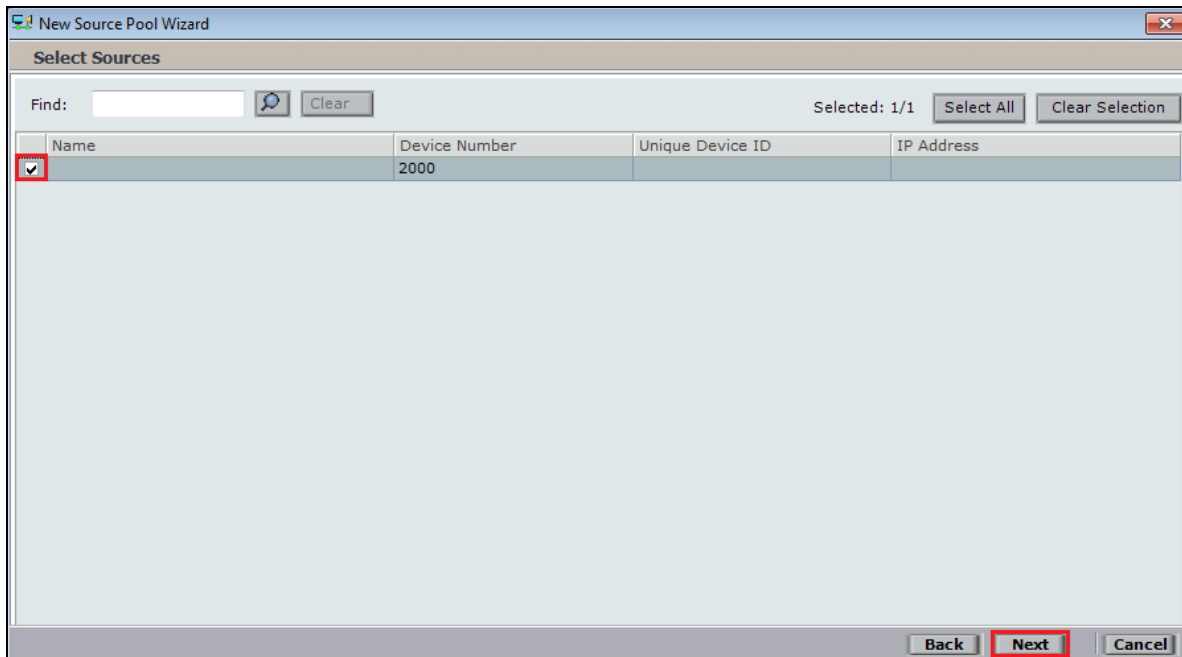
Media type: Audio

Switch: DevConnectCM (ID = 1075)

Source type: Device

Back Next Cancel

Select the extensions that were created in **Section 8.1**, 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 'Find:' text box with a search icon and a 'Clear' button. To the right, it says 'Selected: 1/1' with 'Select All' and 'Clear Selection' buttons. Below this is a table with four columns: 'Name', 'Device Number', 'Unique Device ID', and 'IP Address'. The first row has a checked checkbox in the 'Name' column, and the 'Device Number' is '2000'. At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red box.

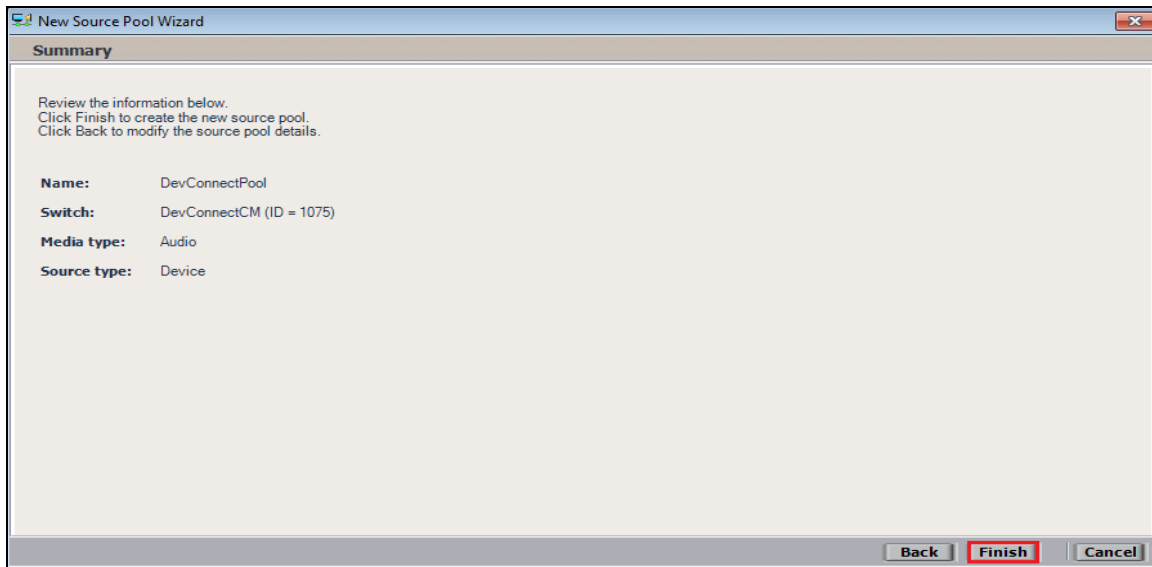
Find: [] Clear

Selected: 1/1 Select All Clear Selection

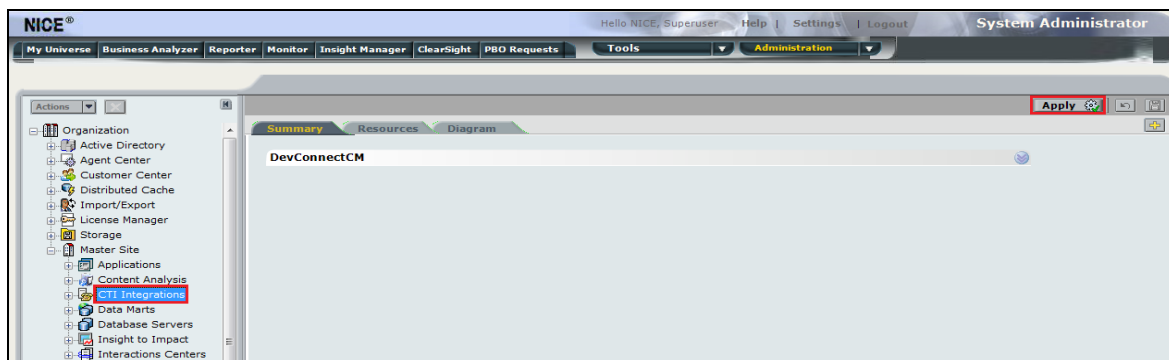
| Name | Device Number | Unique Device ID | IP Address |
|-------------------------------------|---------------|------------------|------------|
| <input checked="" type="checkbox"/> | 2000 | | |

Back Next Cancel

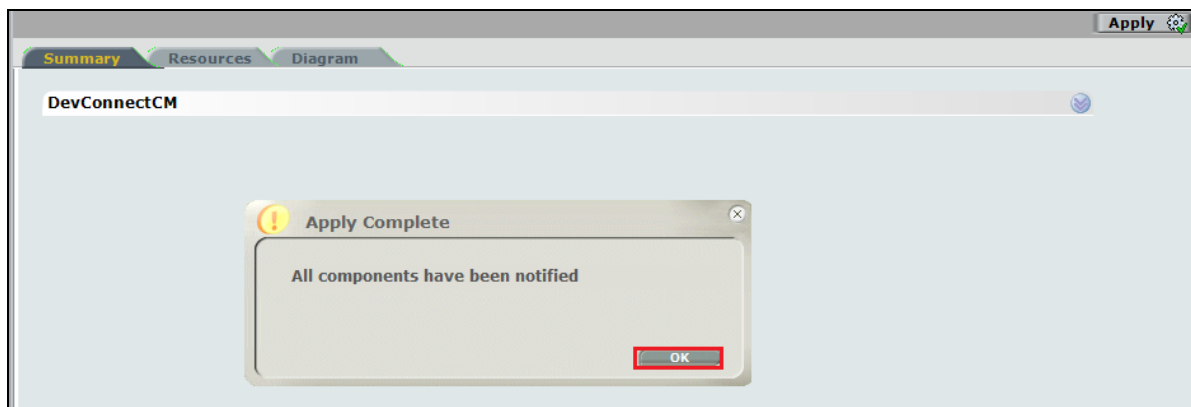
Click on **Finish** to complete the New Source Pool Wizard.



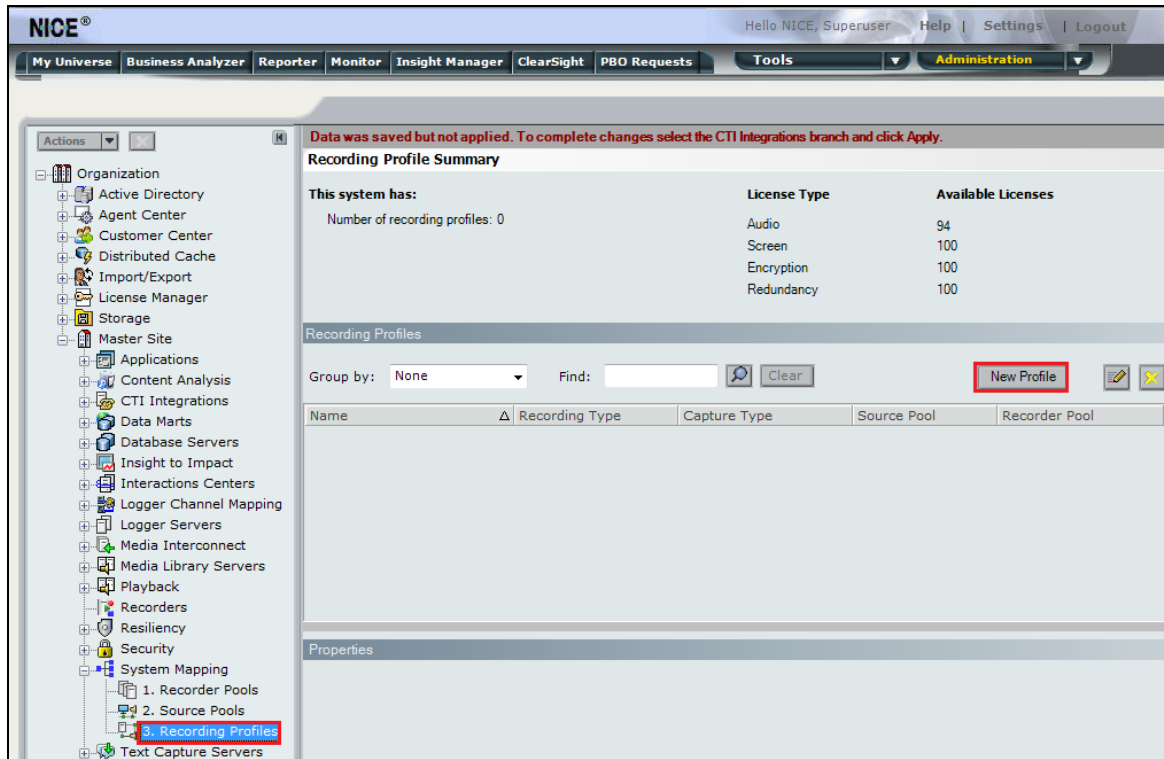
To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.



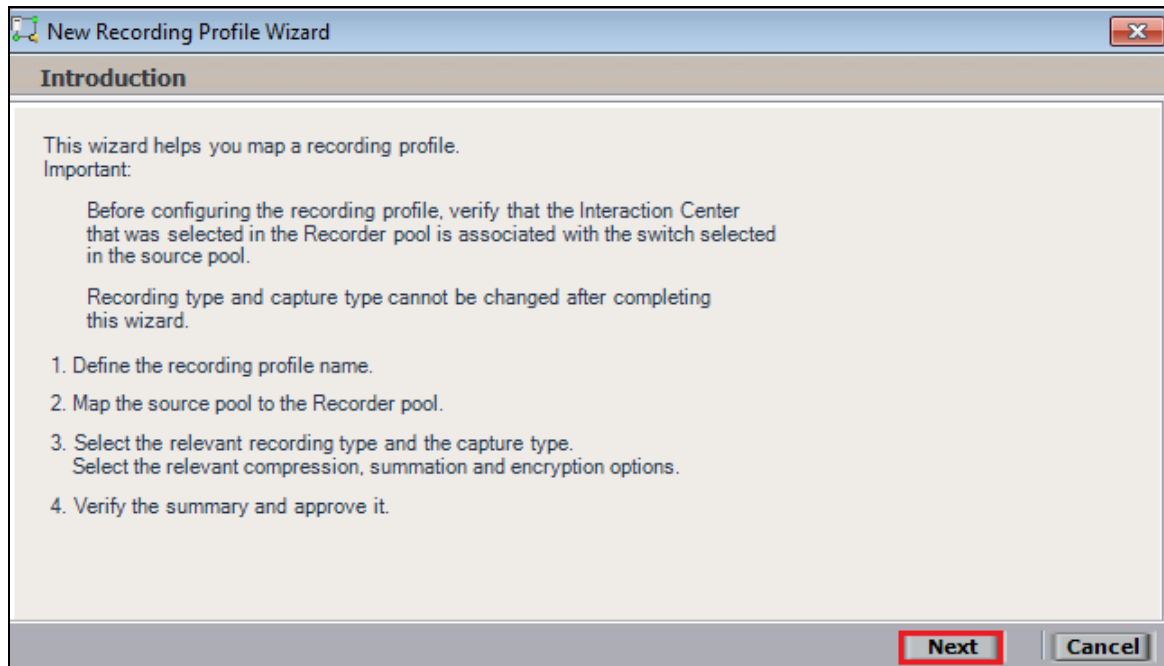
The following screen shows the changes were saved correctly. Click on **OK** to continue.



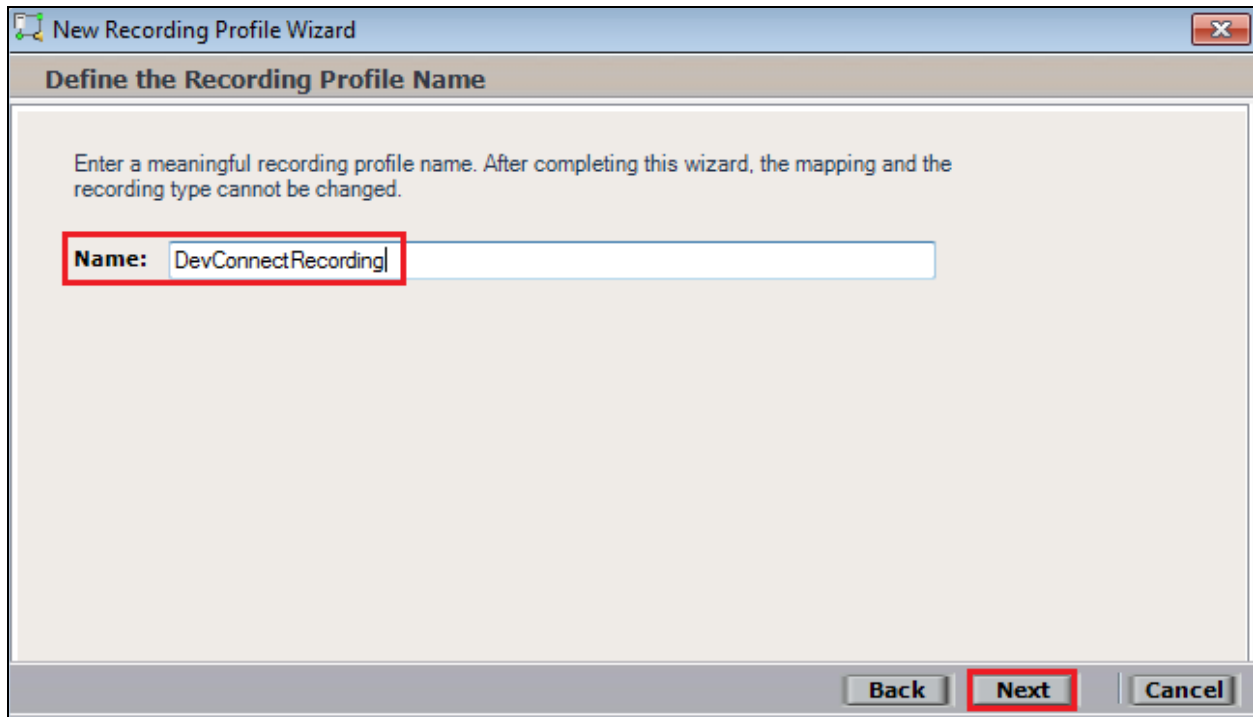
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



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 'Define the Recording Profile Name' step. The window has a title bar with a close button. The main area contains a text box labeled 'Name:' with the text 'DevConnectRecording' entered. Below the text box are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red border.

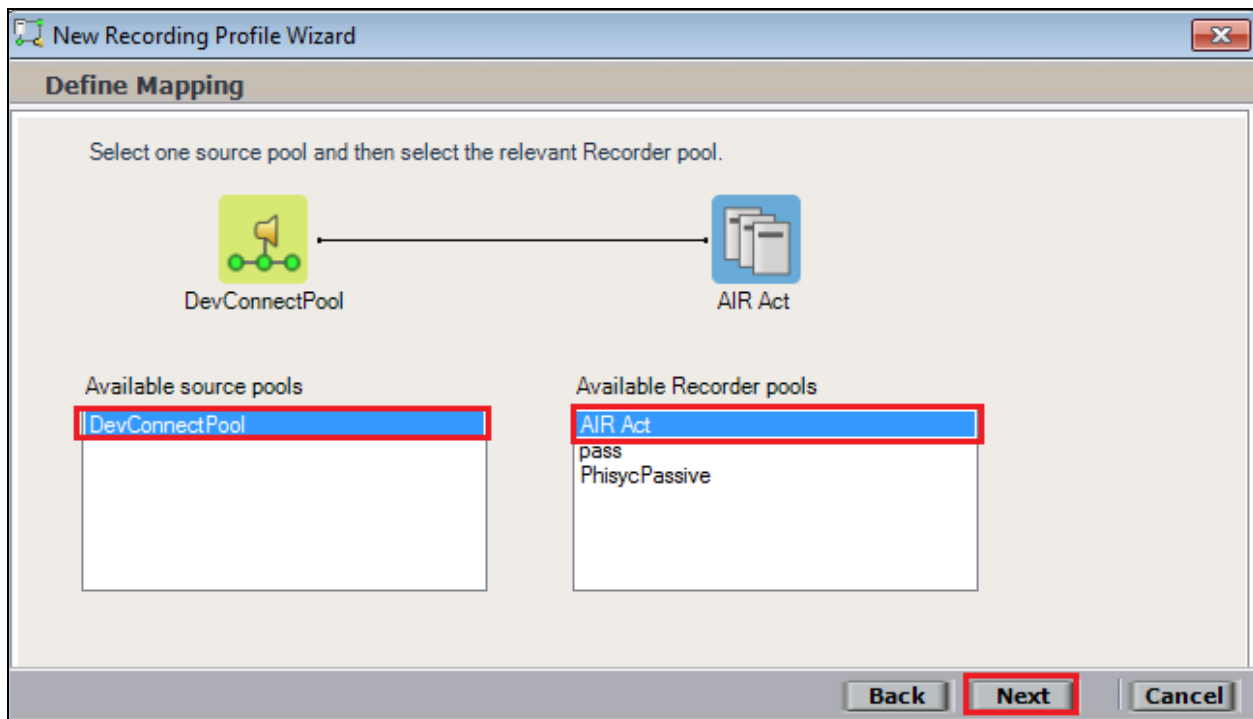
Define the Recording Profile Name

Enter a meaningful recording profile name. After completing this wizard, the mapping and the recording type cannot be changed.

Name: DevConnectRecording

Back Next Cancel

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



The screenshot shows the 'New Recording Profile Wizard' window with the 'Define Mapping' step. The window has a title bar with a close button. The main area contains a diagram showing a mapping from 'DevConnectPool' to 'AIR Act'. Below the diagram are two lists: 'Available source pools' and 'Available Recorder pools'. The 'Available source pools' list contains 'DevConnectPool'. The 'Available Recorder pools' list contains 'AIR Act', 'pass', and 'PhisycPassive'. The 'Next' button is highlighted with a red border.

Define Mapping

Select one source pool and then select the relevant Recorder pool.

DevConnectPool AIR Act

Available source pools

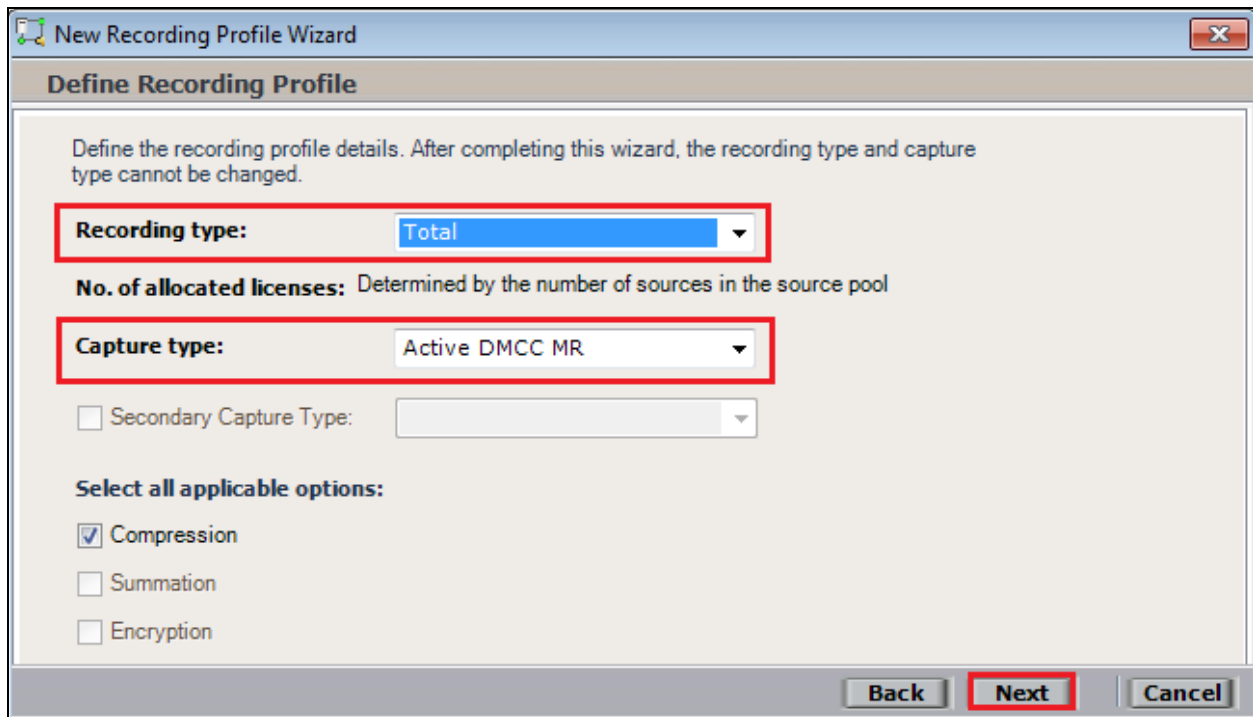
DevConnectPool

Available Recorder pools

AIR Act
pass
PhisycPassive

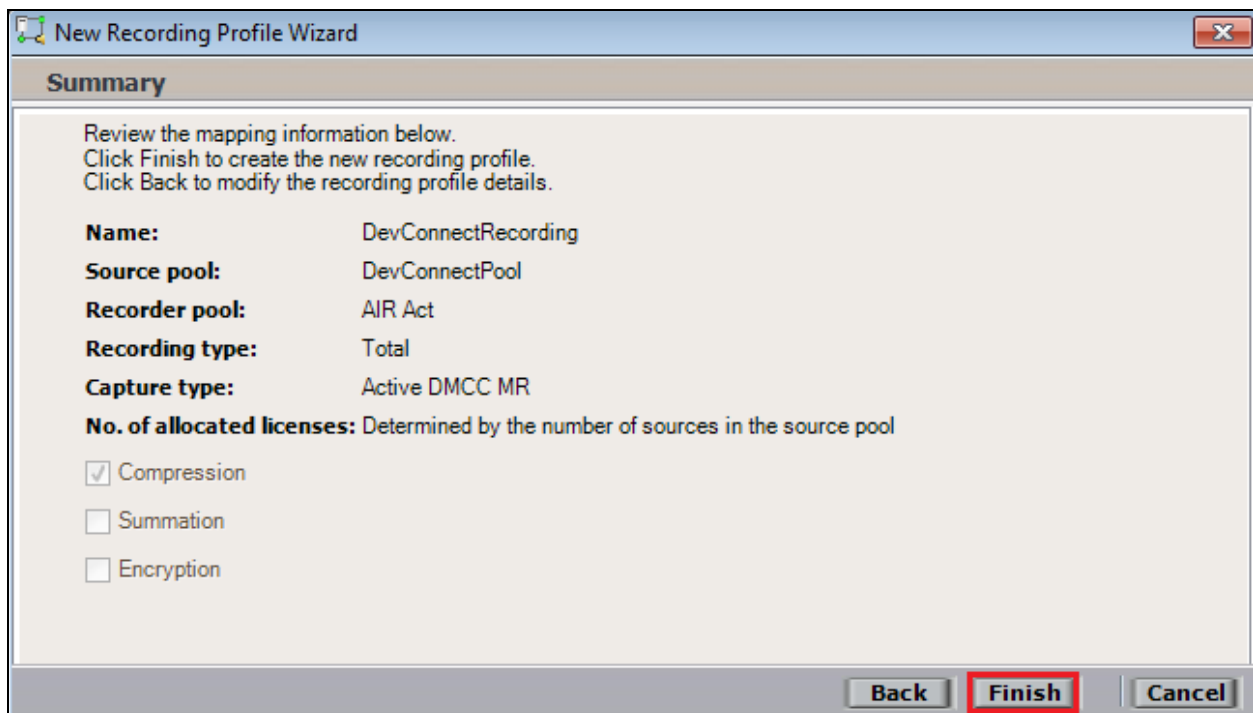
Back Next Cancel

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



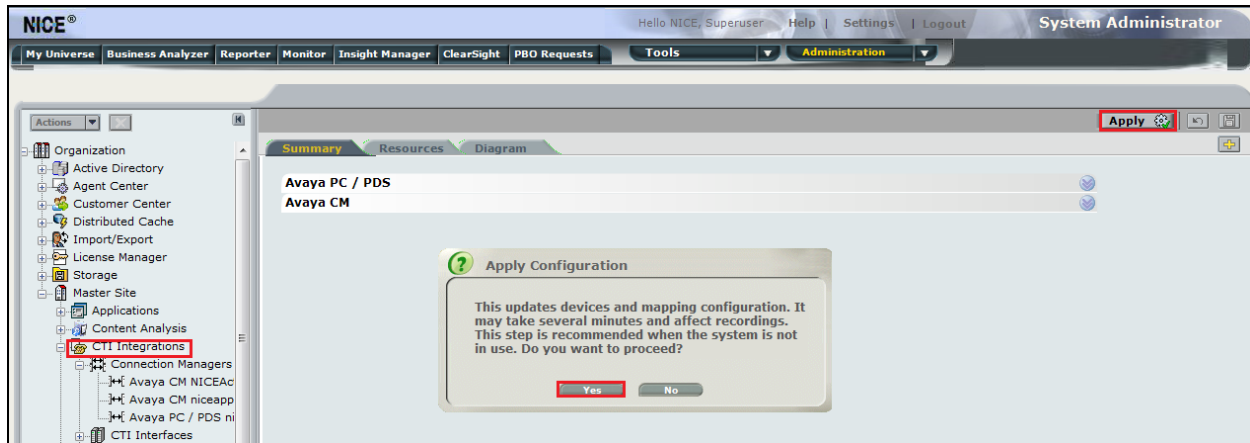
The image shows the 'Define Recording Profile' step of the 'New Recording Profile Wizard'. The window title is 'New Recording Profile Wizard'. The main heading is 'Define Recording Profile'. Below the heading, there is a text box that says 'Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.' There are two red rectangular boxes highlighting the 'Recording type' dropdown menu, which is set to 'Total', and the 'Capture type' dropdown menu, which is set to 'Active DMCC MR'. Below these, there is a checkbox for 'Secondary Capture Type' which is unchecked. There is a section titled 'Select all applicable options:' with three checkboxes: 'Compression' (checked), 'Summation' (unchecked), and 'Encryption' (unchecked). At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red box), and 'Cancel'.

Click on **Finish** to complete the **New Recording Profile Wizard**.



The image shows the 'Summary' step of the 'New Recording Profile Wizard'. The window title is 'New Recording Profile Wizard'. The main heading is 'Summary'. Below the heading, there is a text box that says 'Review the mapping information below. Click Finish to create the new recording profile. Click Back to modify the recording profile details.' There is a list of settings: 'Name: DevConnectRecording', 'Source pool: DevConnectPool', 'Recorder pool: AIR Act', 'Recording type: Total', 'Capture type: Active DMCC MR', and 'No. of allocated licenses: Determined by the number of sources in the source pool'. There are three checkboxes: 'Compression' (checked), 'Summation' (unchecked), and 'Encryption' (unchecked). At the bottom right, there are three buttons: 'Back', 'Finish' (highlighted with a red box), and 'Cancel'.

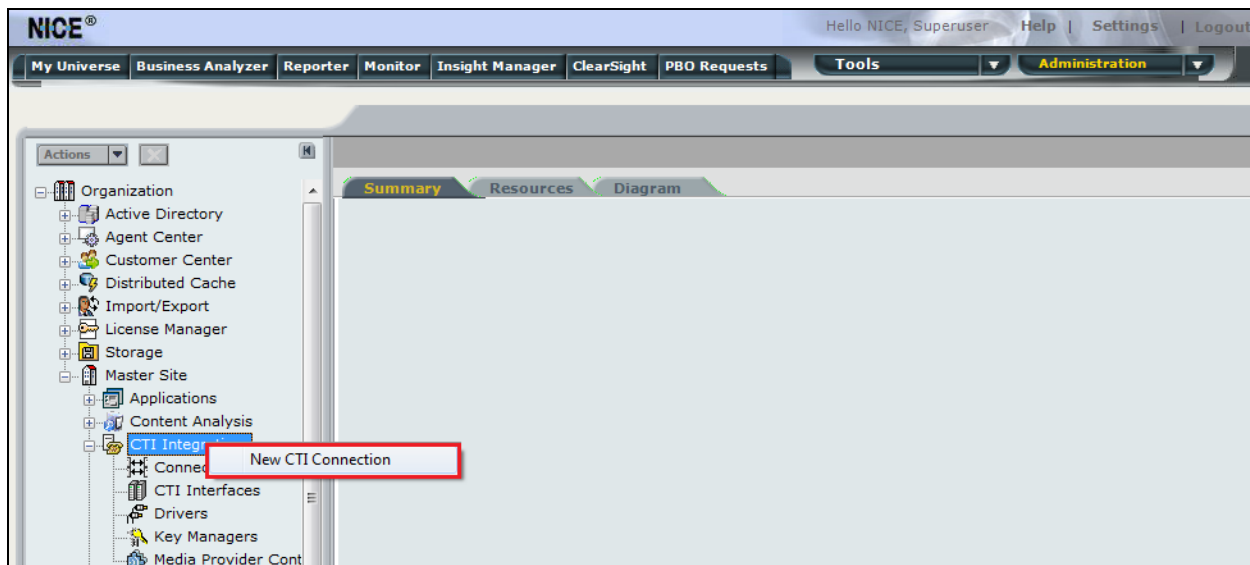
Navigate to **Master Site** → **CTI Integrations** and from the main window click on **Apply**. Then click on **Yes** to proceed.



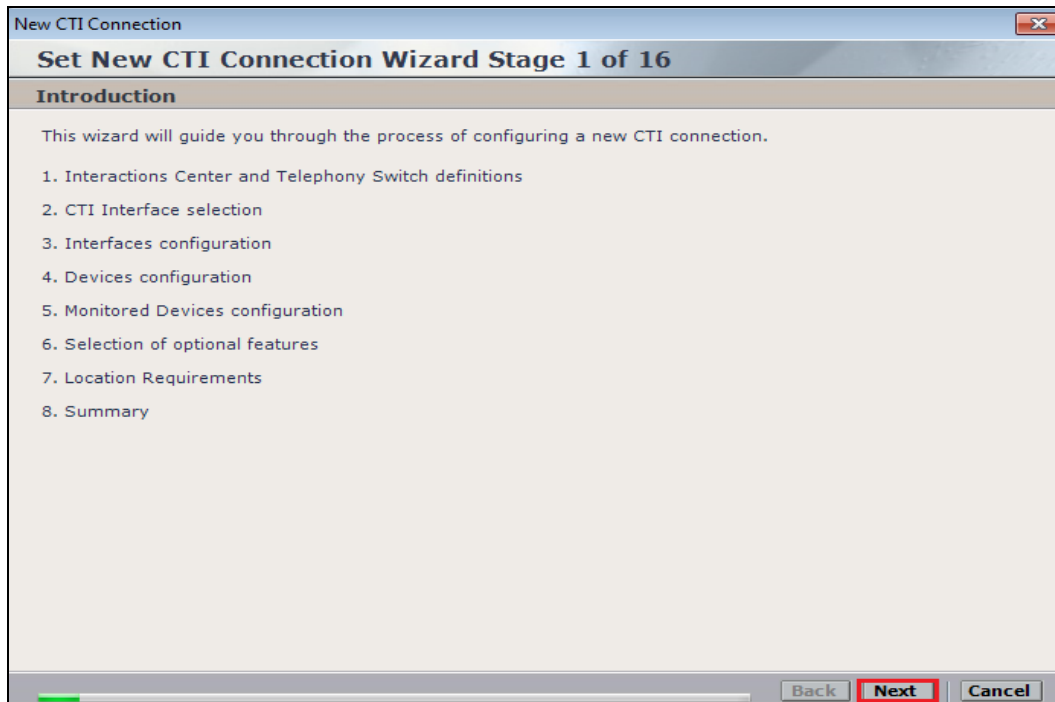
This concludes the setup of the NICE Application Server for DMCC Multi-Registration recording. However there are extra steps now required to setup the Proactive Contact connection in order to obtain events from Proactive Contact in order to start and stop call recordings for Proactive Contact calls.

8.3. Add CTI Connection for Proactive Contact

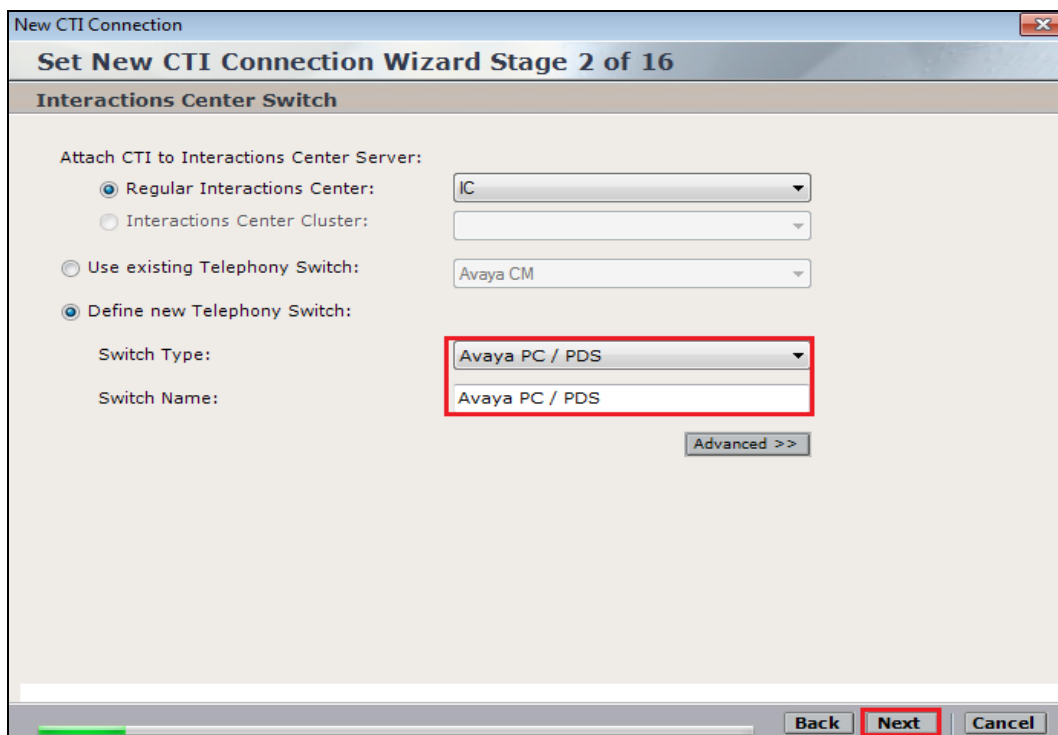
Another New CTI Connection is required for Proactive Contact. From the left window navigate to **Master Site** → **CTI Integrations** and right-click on CTI Integrations and select **New CTI Connection**.



Click on **Next** to continue.



As with the previous CTI Connection there is only one **Interactions Center** available for selection and this was created during the initial installation. Select **Avaya PC/PDS** as the **Switch Type** and enter a suitable **Switch Name**. Click on **Next** to continue.



Event Service should already be chosen by default but if not ensure this is picked and click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 3 of 16

Interface Type

CTI Interface Type

Avaya PC / PDS CTI Interface: **Event Service**

Avaya Proactive Contact / Predictive Dialer System (formerly MOSAIX)
Event Service

☐ VoIP Mapping: [Dropdown]

☐ Active Recording: [Dropdown]

Back **Next** Cancel

The following parameters need to be set for the connection to Proactive Contact and each of these values are set by double-clicking on each individual 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 |
|---------------------------------|-------|
| AvayaPD Version | |
| Event Service Host Name | |
| Naming Service Host Name | |
| AvayaPD Client Username | |

Description: [Text Area]

Additional Interface Parameters

Back **Next** Cancel

Enter the version of the Proactive Contact from the drop-down box and click on **OK** to continue.

New CTI Connection

Set New CTI Connection Wizard

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter

AvayaPD Version

Event Service Host Name

Naming Service Host Name

AvayaPD Client Username

AvayaPD Client Password

Description: AvayaPD Version: PC3 , PC4.

Additional Interface Parameters

Set Parameter Value

Name: AvayaPD Version

Value: PC5

OK Cancel

Back Next Cancel

Enter the IP address or hostname of the Proactive Contact for the **Event Service Host Name**. Click on **OK** to continue.

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

AvayaPD Version

Event Service Host Name

Naming Service Host Name

AvayaPD Client Username

AvayaPD Client Password

Description: Event Service Host Name.

Additional Interface Parameters

Set Parameter Value

Name: Event Service Host Name

Value: 10.10.16.95

OK Cancel

Back Next Cancel

Enter the IP address or hostname of the Proactive Contact for the **Naming Service Host Name**. Click on **OK** to continue.

The screenshot shows the 'Set New CTI Connection Wizard' dialog box. The 'Interface Connection Details' tab is active, displaying a list of parameters. The 'Naming Service Host Name' parameter is selected, and its value is entered as '10.10.16.95'. The 'OK' button is highlighted with a red box. The 'Set Parameter Value' dialog box is also visible, showing the same parameter and value.

Enter the **AvayaPD Client Username**. This user that will be used to monitor events from Proactive Contact and this will be the same username that was displayed in **Section 7.2**. Click on **OK** to continue.

The screenshot shows the 'Set New CTI Connection Wizard' dialog box. The 'Interface Connection Details' tab is active, displaying a list of parameters. The 'AvayaPD Client Username' parameter is selected, and its value is entered as 'client1'. The 'OK' button is highlighted with a red box. The 'Set Parameter Value' dialog box is also visible, showing the same parameter and value.

Enter the **AvayaPD Client Password**. This will be the same password that was displayed in **Section 7.2**. Click on **OK** to continue.

Set New CTI Connection

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

| Parameter | Value |
|---------------------------------|----------|
| Naming Service Host Name | client 1 |
| AvayaPD Client Username | client 1 |
| AvayaPD Client Password | ***** |
| Client Port ID | 6666 |

Description: AvayaPD Client Password - The CTILink will use this parameter in order to login to the AvayaPD server.

Additional Interface Parameters

Set Parameter Value

Name: AvayaPD Client Password

Value: *****

OK **Cancel**

Back **Next** **Cancel**

With this information correctly filled in click on **Next** to continue.

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 |
|---------------------------------|-------------|
| Naming Service Host Name | 10.10.16.95 |
| AvayaPD Client Username | client 1 |
| AvayaPD Client Password | ***** |
| Client Port ID | 6666 |

Description: AvayaPD Client Password - The CTILink will use this parameter in order to login to the AvayaPD server.

Additional Interface Parameters

Back **Next** **Cancel**

The actual devices to be monitored are already added in **Section 8.1**. Click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 10 of 16

Devices

Available Devices
Provide telephony switch available devices
0 devices

Buttons: Add, Add Range, Add From Switch

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

Buttons: Back, **Next**, Cancel

Call Flow Analysis can be added as an option, click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 12 of 16

Optional

Select optional features relevant to integration. Some options may require further configuration.

- ☐ SIP Trunk Correlation
- ☐ Rejected Devices
- ☐ Filter Calls
- ☒ Call Flow Analysis

Buttons: Back, **Next**, Cancel

Ensure that a unique **Port** is set for the **new Connection Manager**, then click on **Next** to continue.

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:

☐ Select available Connection Manager

Ports in use:

- 62094
- 62100
- 62095

Back Next Cancel

Click on **Finish** to complete the Proactive Contact CTI connection.

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:

Avaya PC / PDS1 Connection

Back Finish Cancel

9. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the NICE Engage Platform and both Avaya Proactive Contact and Avaya Aura® Application Enablement Services.

9.1. Verify Avaya Aura® Communication Manager CTI Service State


Before the connection between the NICE Engage Platform and the AES is checked, the connection between Communication Manager and AES can be checked 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 |

9.2. 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**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Thu Feb 20 11:01:32 2014 from 192.168.10.222
Number of prior failed login attempts: 33
HostName/IP: AES63V/MPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
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**

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ **TSAPI Service Summary**

TSAPI Link Details

☐ Enable page refresh every 60 seconds

| Link | Switch Name | Switch CTI Link ID | Status | Since | State | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| 1 | CM63vmpg | 1 | Talking | Tue Feb 18 11:21:49 2014 | Online | 16 | 5 | 15 | 15 | 30 |

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

9.3. Verify Proactive Contact services are running

Using putty open an SSH connection to Proactive Contact and **login** using the appropriate credentials as shown below.

```
login as: admin
~~~~~

*** WARNING NOTICE ***

This system is restricted solely to Avaya authorized users for legitimate
business purposes only. The actual or attempted unauthorized access, use,
or modification of this system is strictly prohibited by Avaya. Unauthorized
users are subject to Company disciplinary proceedings and/or criminal and
civil penalties under state, federal, or other applicable domestic and
foreign laws. The use of this system may be monitored and recorded for
administrative and security reasons. Anyone accessing this system expressly
consents to such monitoring and is advised that if monitoring reveals possible
evidence of criminal activity, Avaya may provide the evidence of such activity
to law enforcement officials. All users must comply with Avaya Security
Instructions regarding the protection of Avaya's information assets.

~~~~~
Using keyboard-interactive authentication.
Password:
```

Once logged in correctly type **check_pds** as shown below.

```
=====
=====
# ID Sev Short Text Enabled First
Instance Last Instance Count State
-----
-----
3 QPC000D0001 Info Services started - PDS Yes 2012-03-01
16:06:48 2012-03-01 16:06:48 1 ACTIVE
4 QPC000D0002 Info Services started - MTS Yes 2012-02-29
16:31:39 2012-02-29 16:31:39 1 ACTIVE
5 QPC000D0003 Info Services started - DB Yes 2012-02-29
16:30:30 2012-02-29 16:30:30 1 ACTIVE
25 QPC000D0023 Warning Illegal agent logoff Yes 2011-05-24
18:48:20 2012-03-01 16:25:58 431 ACTIVE
=====
=====
Found '4' ACTIVE or RETIRED alarms.

DEVCONHD(admin)@/opt/avaya/pds [992]
$ check_pds
```

The following screen should show **All processes running!**.

```
root      28532      1  0 Mar01 ?          00:00:00 agent -d
admin     28543      1  0 Mar01 ?          00:00:00 ao_recall
admin     28539      1  0 Mar01 ?          00:00:00 recall_rmp
admin     28529      1  0 Mar01 ?          00:00:00 listserver
admin     28216      1  0 Mar01 ?          00:00:00 opmon
root      28238      1  0 Mar01 ?          00:00:00 evmon
root      28125 28116  0 Mar01 ?          00:00:00 /opt/avaya/pds/bin/enforcer -ORB
root      28106      1  0 Mar01 ?          00:00:00 bridgeSmEnf -ORBSvcConf /opt/ava
admin     28101      1  0 Mar01 ?          00:00:00 switcher
admin     28069      1  0 Mar01 ?          00:00:00 job_strter
root      28054      1  0 Mar01 ?          00:00:00 agentcount
root      28037      1  0 Mar01 ?          00:04:00 enserver -ORBSvcConf /opt/avaya/
root      28565      1  0 Mar01 ?          00:01:20 dccserver -ORBSvcConf /opt/avaya
admin     28044      1  0 Mar01 ?          00:00:08 datamgr
admin     28025      1  0 Mar01 ?          00:00:00 soe_routed
admin     28027 28025  0 Mar01 ?          00:00:00 soe_routed
root      28062      1  0 Mar01 ?          00:00:00 signalit
admin     28030      1  0 Mar01 ?          00:00:00 conn_mgr
root      28571      1  0 Mar01 ?          00:01:08 hdsc -ORBSvcConf /opt/avaya/pds/
```

>>> **All processes running!**

```
DEVCONHD(admin)/opt/avaya/pds [993]
$
```

Check the database is running correctly by typing **check_db** as shown. **All processes are running and the database is opened to the users!** should be returned.

```
DEVCONHD(admin)/opt/avaya/pds [993]
$ check_db

Checking for required database processes...
Found:
oracle    29897      1  0 Feb29 ?          00:00:21 ora_smon_orastd
oracle    29893      1  0 Feb29 ?          00:00:54 ora_lgwr_orastd
oracle    29885      1  0 Feb29 ?          00:00:12 ora_pmon_orastd
oracle    29895      1  0 Feb29 ?          00:00:56 ora_ckpt_orastd
oracle    29891      1  0 Feb29 ?          00:00:11 ora_dbw0_orastd
oracle    29899      1  0 Feb29 ?          00:00:00 ora_reco_orastd
oracle    29913      1  0 Feb29 ?          00:00:00 ora_qmnc_orastd
oracle    29901      1  0 Feb29 ?          00:01:34 ora_cjq0_orastd
oracle    29907      1  0 Feb29 ?          00:00:00 ora_d000_orastd
oracle    29889      1  0 Feb29 ?          00:00:00 ora_mman_orastd
oracle    29909      1  0 Feb29 ?          00:00:00 ora_s000_orastd
oracle    29903      1  0 Feb29 ?          00:00:20 ora_mmon_orastd
oracle    29905      1  0 Feb29 ?          00:00:10 ora_mmln_orastd
admin     29881      1  0 Feb29 ?          00:00:00 /opt/dbase/OraHome1/bin/tnslsnr
```

Verifying Database availability...

>>> **All processes are running and the database is opened to the users!**

```
DEVCONHD(admin)/opt/avaya/pds [994]
$
```


Type **check_mts**, this should return **All processes are running** as shown.

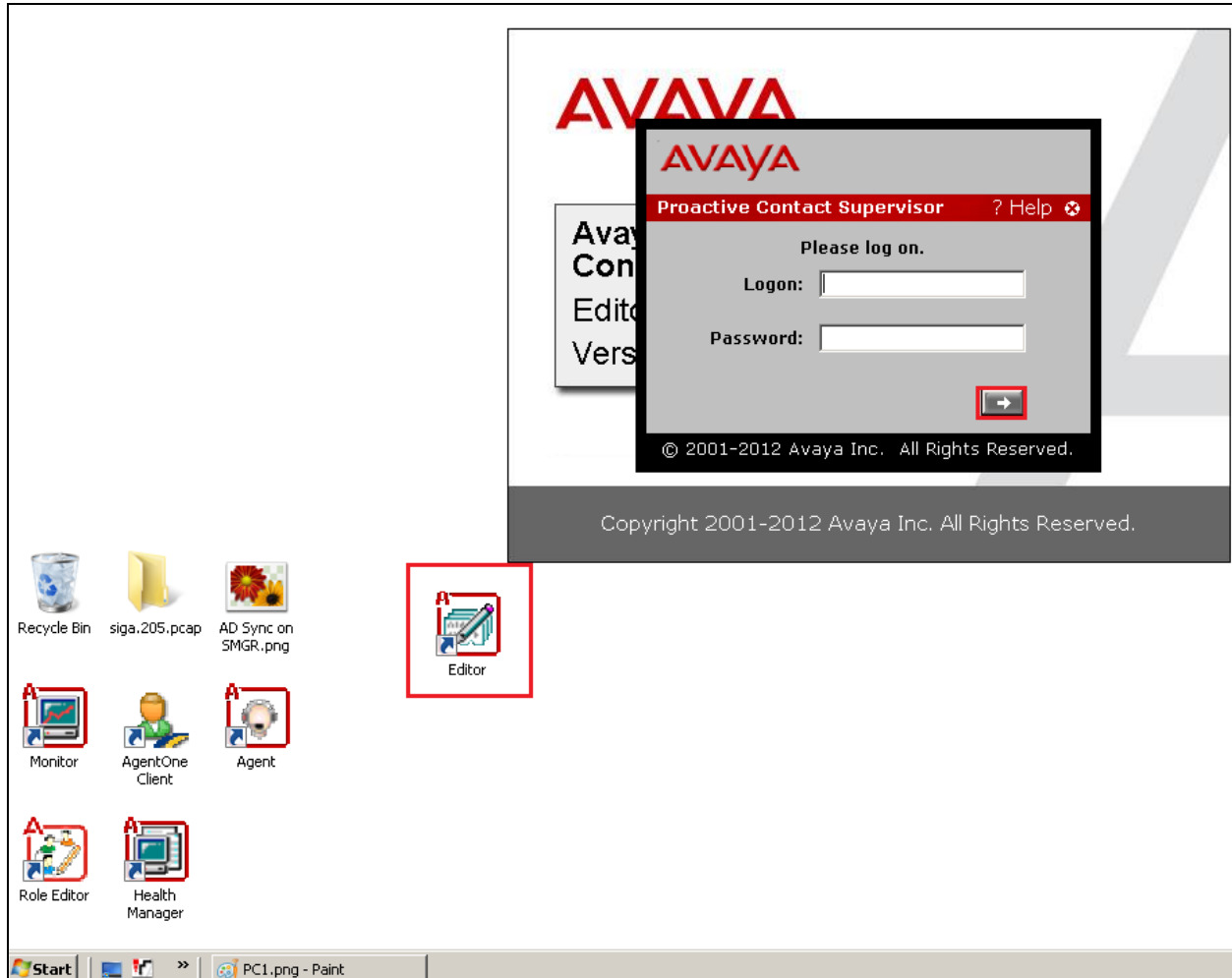
```
=====
=====
# ID Sev Short Text Enabled First
Instance Last Instance Count State
-----
3 QPC000D0001 Info Services started - PDS Yes 2012-03-01
16:06:48 2012-03-01 16:06:48 1 ACTIVE
4 QPC000D0002 Info Services started - MTS Yes 2012-02-29
16:31:39 2012-02-29 16:31:39 1 ACTIVE
5 QPC000D0003 Info Services started - DB Yes 2012-02-29
16:30:30 2012-02-29 16:30:30 1 ACTIVE
25 QPC000D0023 Warning Illegal agent logoff Yes 2011-05-24
18:48:20 2012-03-01 16:25:58 431 ACTIVE
=====
=====
Found '4' ACTIVE or RETIRED alarms.

DEVCONHD(admin)@/opt/avaya/pds [992]
$ check_mts

>>> All processes are running!
$
```

9.4. Verify Avaya Proactive Contact jobs are running

Before an agent is logged into a job verify that the correct jobs are running. Open Proactive Contact **Editor**.



Once logged in click on jobs as shown below and ensure that the correct jobs are up and running. **Jobs** can be started and stopped using the icons highlighted in the screen shot below.

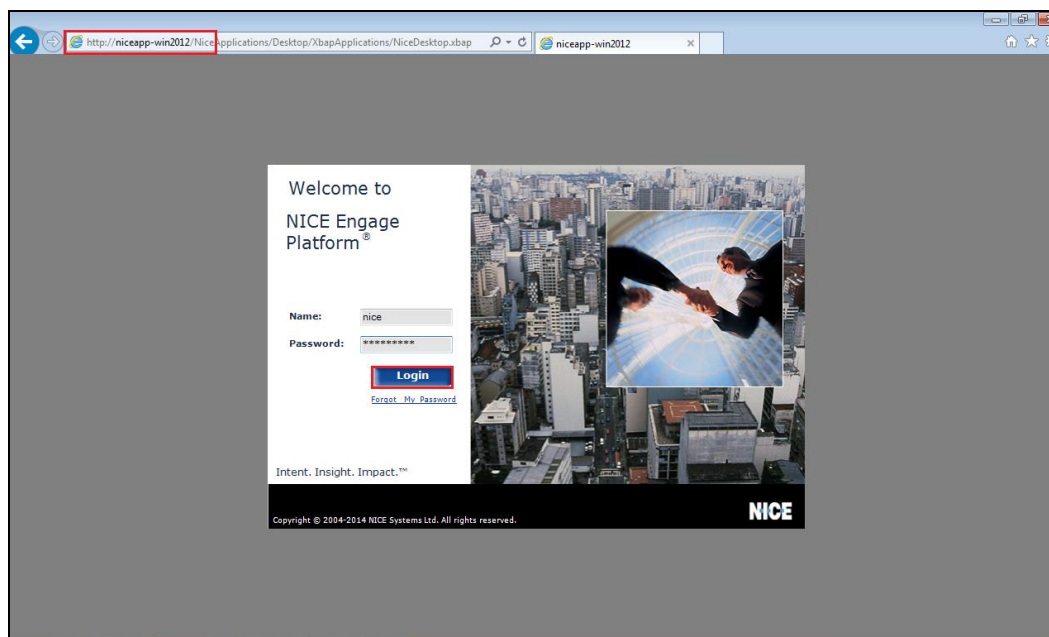
The screenshot shows the 'Editor - [Jobs: Active outbound]' window. The left sidebar has a 'Jobs' icon highlighted with a red box. The main area displays a table of jobs with columns: Job, Job type, File Version, Outbound list, Inbound list, Status, and Job Detail. The 'inbnd3PG' and 'outbnd2' jobs are highlighted with red boxes. The 'Status' column shows 'Running' for 'inbnd3PG' and 'Stopped' for 'outbnd2'. The 'Job Detail' section on the right shows settings for 'Basic' and 'Call'.

| Job | Job type | File Version | Outbound list | Inbound list | Status | Job Detail |
|----------|----------|--------------|----------------|-----------------|---------|---|
| blend | Blend | Active | devconhd-list1 | devconhd-inbnd3 | Stopped | Basic Job: generic Tagged: 0 Line: REG Earliest: 00:01 Latest: 23:59 Calling: <input type="checkbox"/> Require: <input type="checkbox"/> Transacti: 93 |
| blendPG | Blend | Active | devconhd-list1 | devconhd-inbnd3 | Stopped | |
| inbnd1 | Inbound | Active | | devconhd-inbnd4 | Stopped | |
| inbnd2 | Inbound | Active | | devconhd-inbnd2 | Stopped | |
| inbnd3PG | Inbound | Active | | devconhd-inbnd3 | Running | Call Call: Expert Calling Ratio Expert: w0 Initial hit: 50 Minimum: 20 Cell: 0 |
| managed | Managed | Active | devconhd-list1 | | Stopped | |
| outbnd | Outbound | Active | devconhd-list1 | | Stopped | |
| outbnd2 | Outbound | Active | devconhd-list4 | | Running | |
| outbnd3 | Managed | Active | devconhd-list4 | | Stopped | |
| outbnd4 | Outbound | Active | devconhd-list5 | | Stopped | |
| outbnd5 | Outbound | Active | devconhd-list7 | | Stopped | |
| outbnd6 | Outbound | Active | devconhd-list8 | | Stopped | |
| verify | Outbound | Active | devconhd-list1 | | Stopped | |
| virtual | Virtual | Active | devconhd-list1 | | Stopped | |

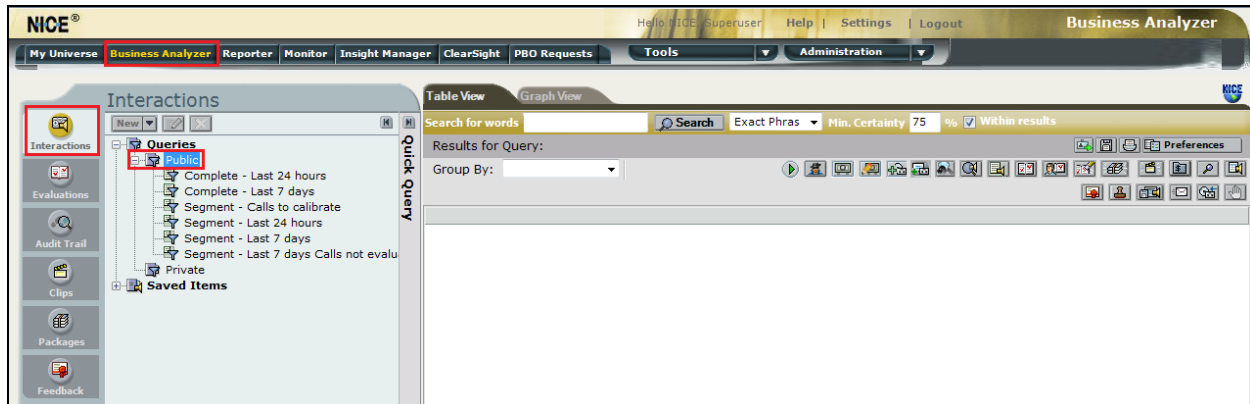
9.5. Verify calls are being recorded

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.

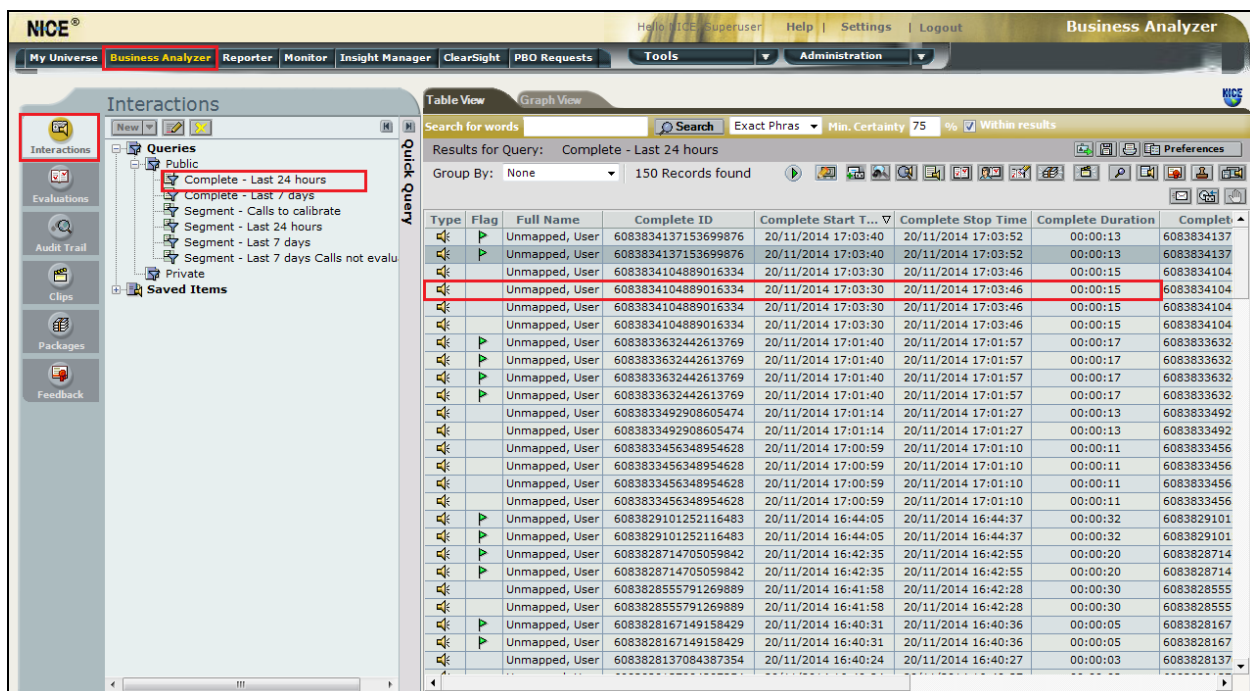
Open a browser session to the NICE Application Server as is shown below. Enter the proper credentials and click on **Login**.



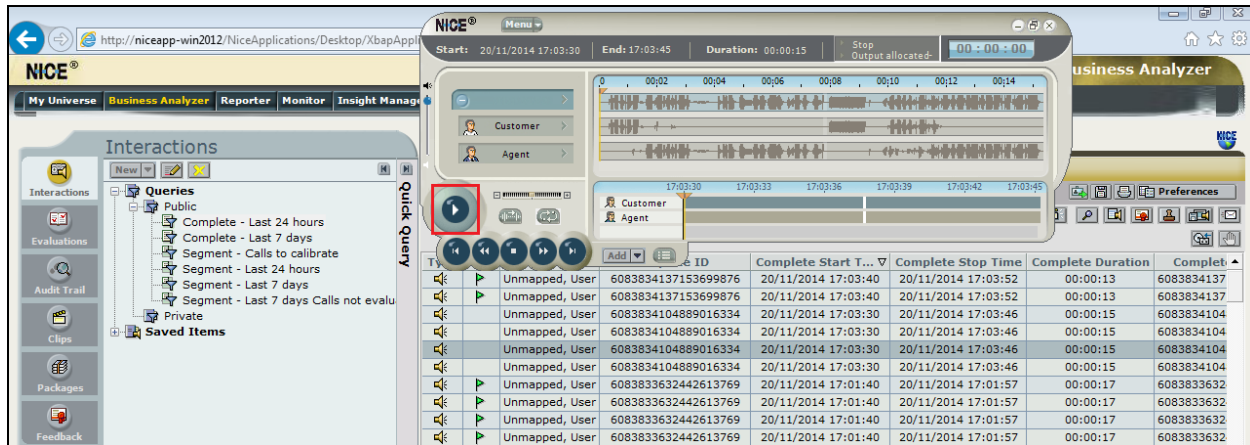
Click on **Business Analyser** at the top of the screen. Select **Interactions** from the left window and then navigate to **Queries** → **Public**.



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.

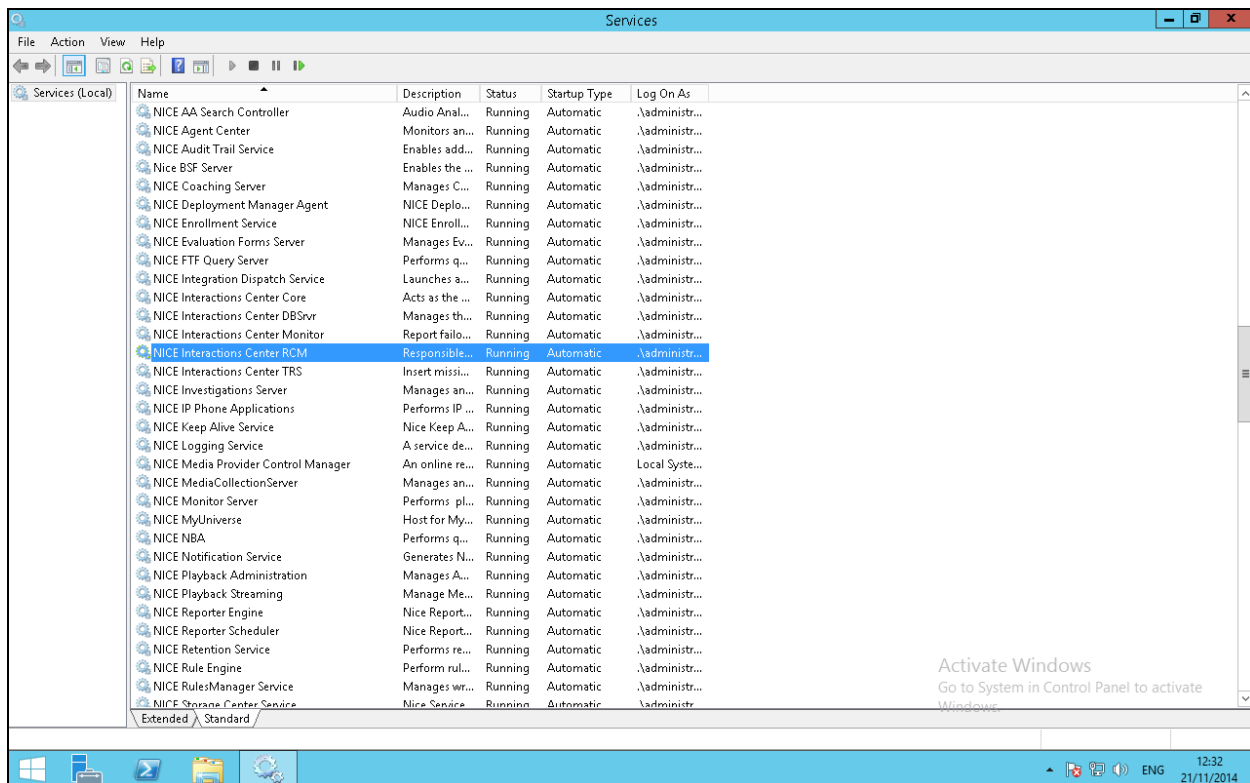


The NICE player is opened and the recording is presented for playback. Click on the **Play** icon highlighted below to play back the recording.



9.6. Verify NICE Services

If these recordings are not present or cannot be played back the NICE services may not be running or may need to be restarted. There are two separate servers as a part of this NICE Engage Platform. The NICE Application Server and the NICE Advanced Interactions Server can be logged into and checked to ensure all services beginning with NICE are running correctly. As a last resort both servers may need a reboot after the initial configuration.



10. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform to successfully interoperate with Avaya Proactive Contact R5.1 using Avaya Aura® Application Enablement Services R6.3 to connect to using DMCC Multi-Registration to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

11. 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
- [5] *Implementing Avaya Proactive Contact R5.1*

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

Appendix

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? y | |
| | 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 | |

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

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.