Avaya Solution & Interoperability Test Lab

Application Notes for configuring NICE Engage Platform R6.4 to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 using 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 an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0 using Multi-Registration.

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

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

1. Introduction

These Application Notes describe the configuration steps for the NICE Engage Platform R6.4 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0. NICE Engage Platform uses Communication Manager's Multiple Registrations feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording on various Communication Manager endpoints, listed in **Section 4**.

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 DMCC API associated with the AES server monitors the digital and VoIP extensions. The application uses the AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device and records the call.

The NICE Engage Platform is fully integrated into a LAN (Local Area Network), and includes easy-to-use Web based applications (i.e. Nice Application) that works with the Microsoft .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. 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 AES and Communication Manager. A range of Avaya endpoints were used in the compliance testing all of which are listed in **Section 4**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Inbound/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **Forwarded calls** - Test call recording for calls that were forwarded to various endpoints.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park and Call Pickup.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into one-X® Agent.
- **Serviceability testing** - The behavior of NICE Engage Platform under different simulated failure conditions.

2.2. Test Results

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

1. **Call Pickup**. There is an issue with "Call Pickup" using SIP Phones to pick up the call. If the DMCC registration API (GetDeviceID, Monitor, RegisterTerminal) are performed **before** the call picked up, RTP packets and Media Start event are missing. If the DMCC registration API performed **after** the call picked up, RTP and Media Start event received as expected. Logs were taken and a ticket was raised with the AES team here in Avaya. Avaya Ticket AES-14000 has been opened via DevConnect to investigate this issue.
2. **Transfer/Conference**. If a transfer or conference is attempted the NICE recorder receives two RTP streams destined for the same port and this is an issue as one of the RTP streams is empty and there is not recording present. This affects all "supervised" transfer and conference calls to any unmonitored devices. A fix for this issue will be included in CM 7.0.1.0.0 which is planned for release in May 2016.
3. **Call Park**. The un-parked call is not being recorded. It appears that there are no events being sent for un-parking a call by Communication Manager. Modification Report [**CM-9860**] has been raised with the Communication Manager support team. A fix for this issue will be implemented for release 7.1 of Communication Manager.

2.3. Support

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

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Engage Platform with the Avaya solution using DMCC Multi-Registration to record calls. The NICE Application Server is setup for DMCC Multi-Registration mode and connects to the AES.

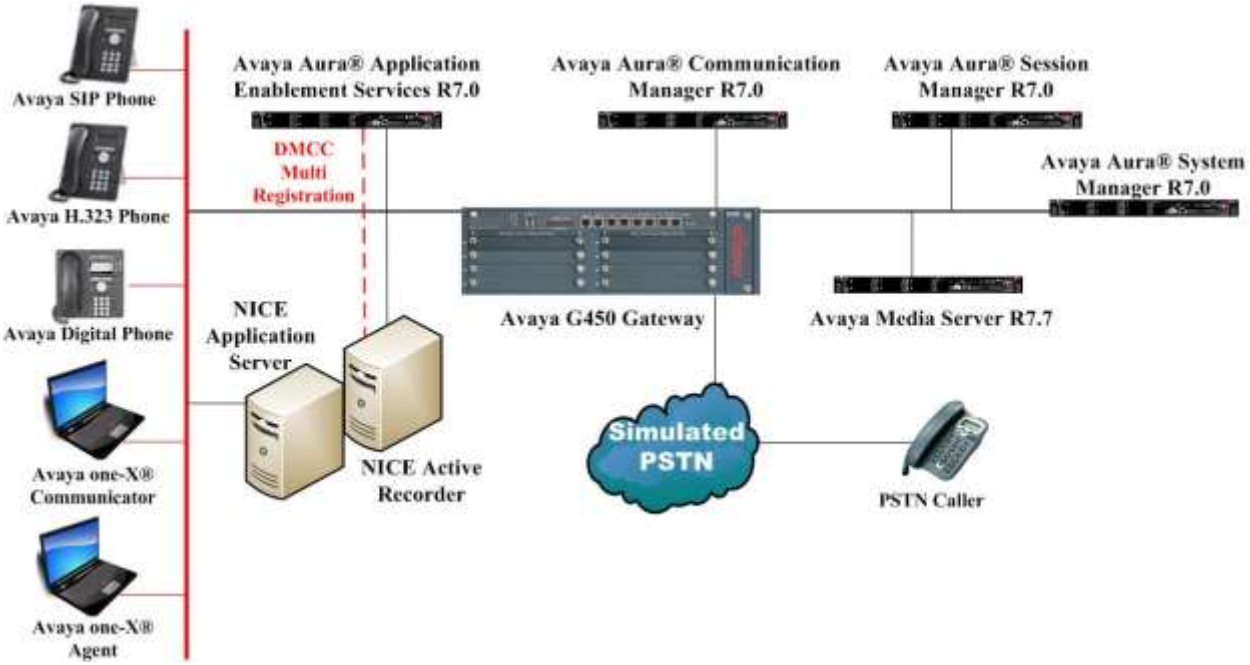


Figure 1: Connection of NICE Engage Platform R6.4 with Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager R7.0 and Avaya Aura® Application Enablement Services R7.0

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Virtual Server	R7.0.0.0.0 Build 7.0.0.0.16266-7.0.9.9.902 SW Update Revision No. 7.0.0.0.3873
Avaya Aura® Session Manager running on Virtual Server	R7.0.0.0.700007
Avaya Aura® Communication Manager running on Virtual Server	R7.0 Build 017x.00.0.441.0.22477
Avaya Aura® Application Enablement Services running on Virtual Server	R7.0 Build No – 7.0.0.0.0.13-0
Avaya G450 Gateway	37.19.0 /1
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 6.5.0.17
Avaya 9630 SIP Deskphone	R2.6.13.1
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Avaya one-X® Agent	R 2.5.50022.0
Avaya 9408 Digital Deskphone	FW Version 2
NICE Engage Platform - Application Server - Advanced Interactions Recorder	R6.4

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify System Features

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

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  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
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                            DS1 MSP? y
                                  ATMS? y             DS1 Echo Cancellation? y
                   Attendant Vectoring? y
```

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

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

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

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

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

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

```
change ip-services                                          Page   1 of   4

                                   IP SERVICES
 Service      Enabled     Local        Local       Remote      Remote
  Type                    Node         Port        Node        Port
AESVCS         y          procr        8765
```

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

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

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

```
change ip-services                                          Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:        aes70vmpg         ********          y          idle
      2:
      3:
```

5.4. Configure CTI Link for TSAPI Service

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

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

5.5. Configure H323 Stations for Multi-Registration

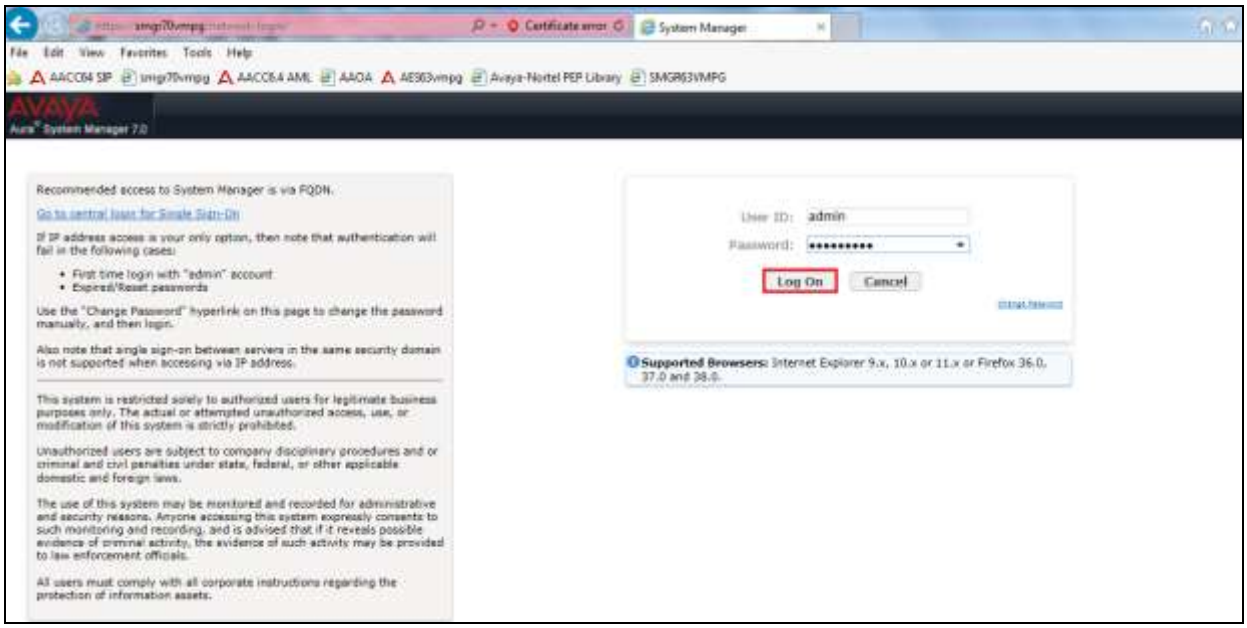
All endpoints that are to be monitored by NICE will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required 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: 9608                       Security Code: 1234            TN: 1
     Port: S00101                     Coverage Path 1:               COR: 1
     Name: Extension                  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
```

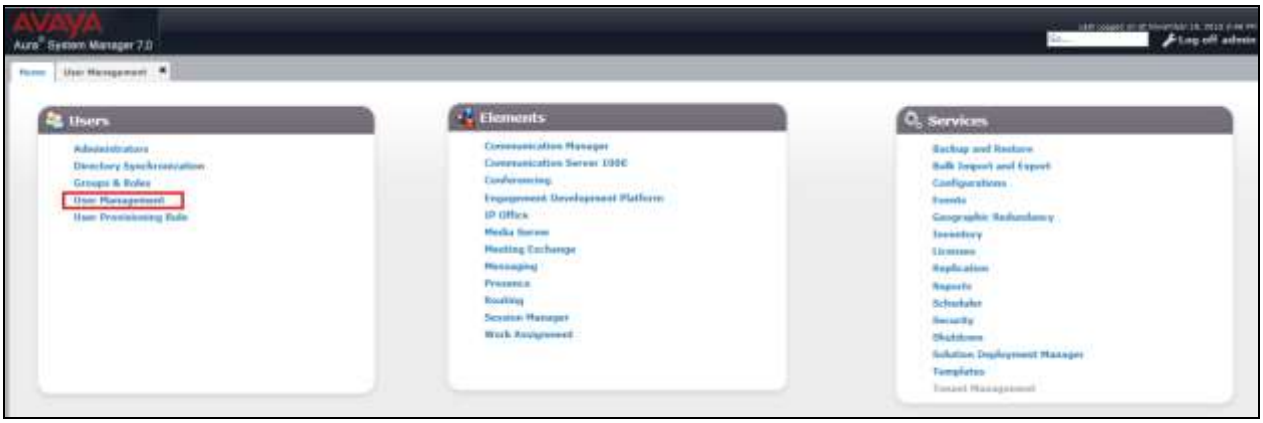
5.6. Configure SIP Stations for Multi-Registration

Any SIP extension that is to be recorded requires some configuration changes to allow call recording using multiple registration. Changes 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 Adddress >/SMGR**. Log in using appropriate credentials.

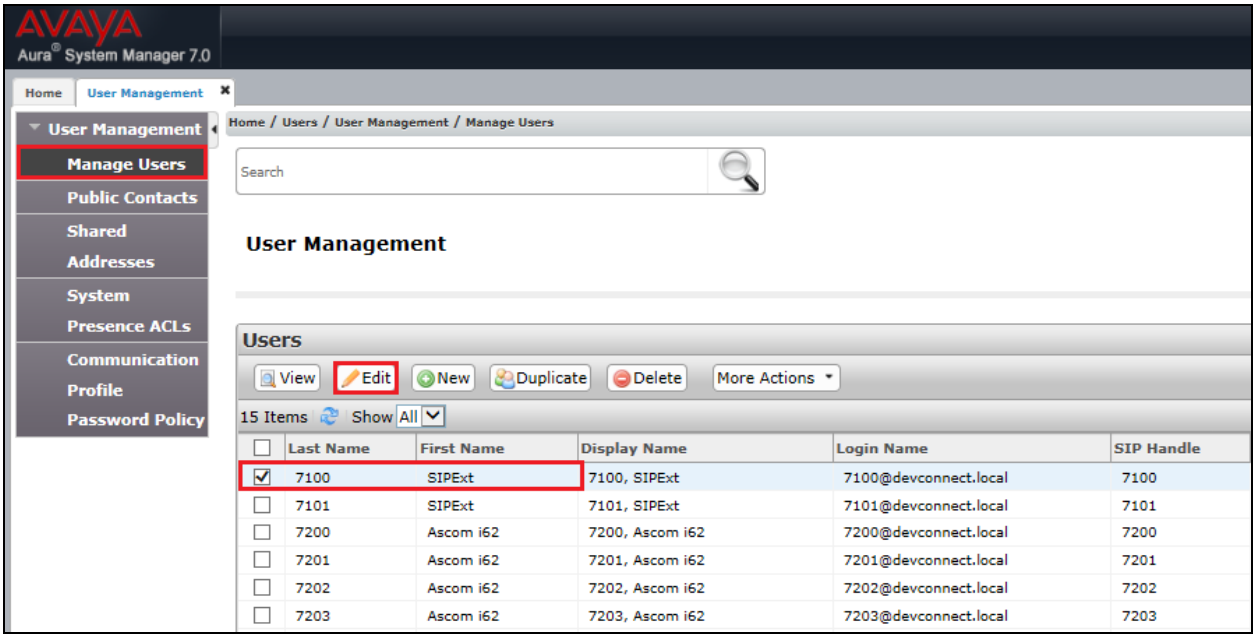
Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



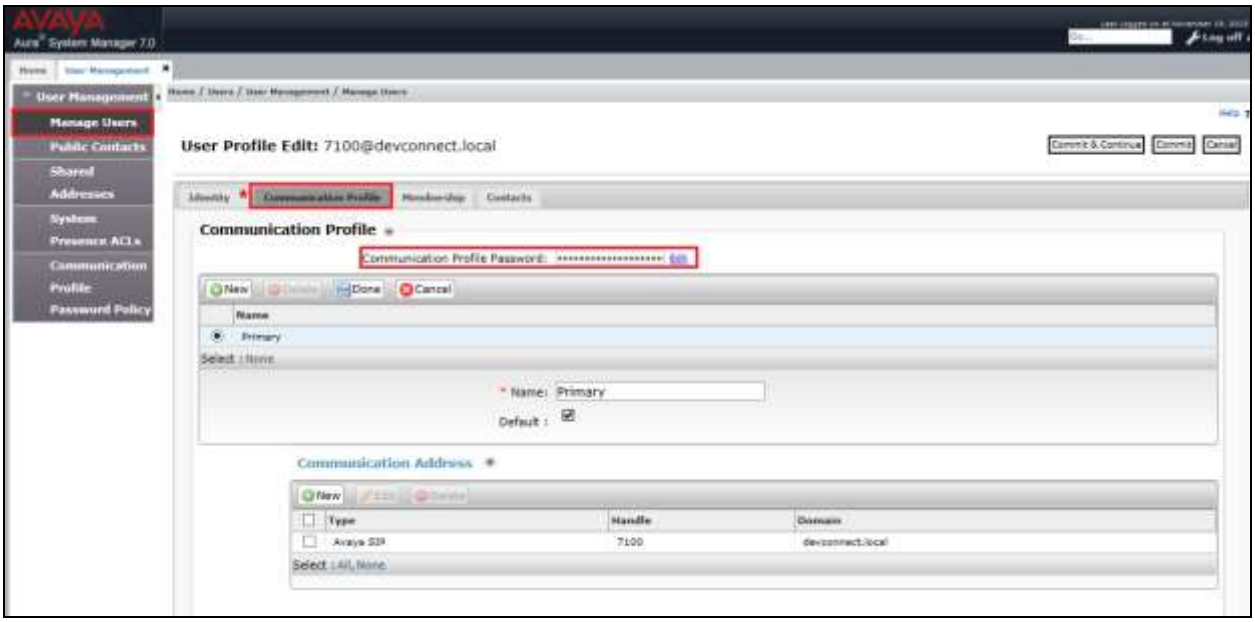
From the home page click on **User Management** highlighted below.



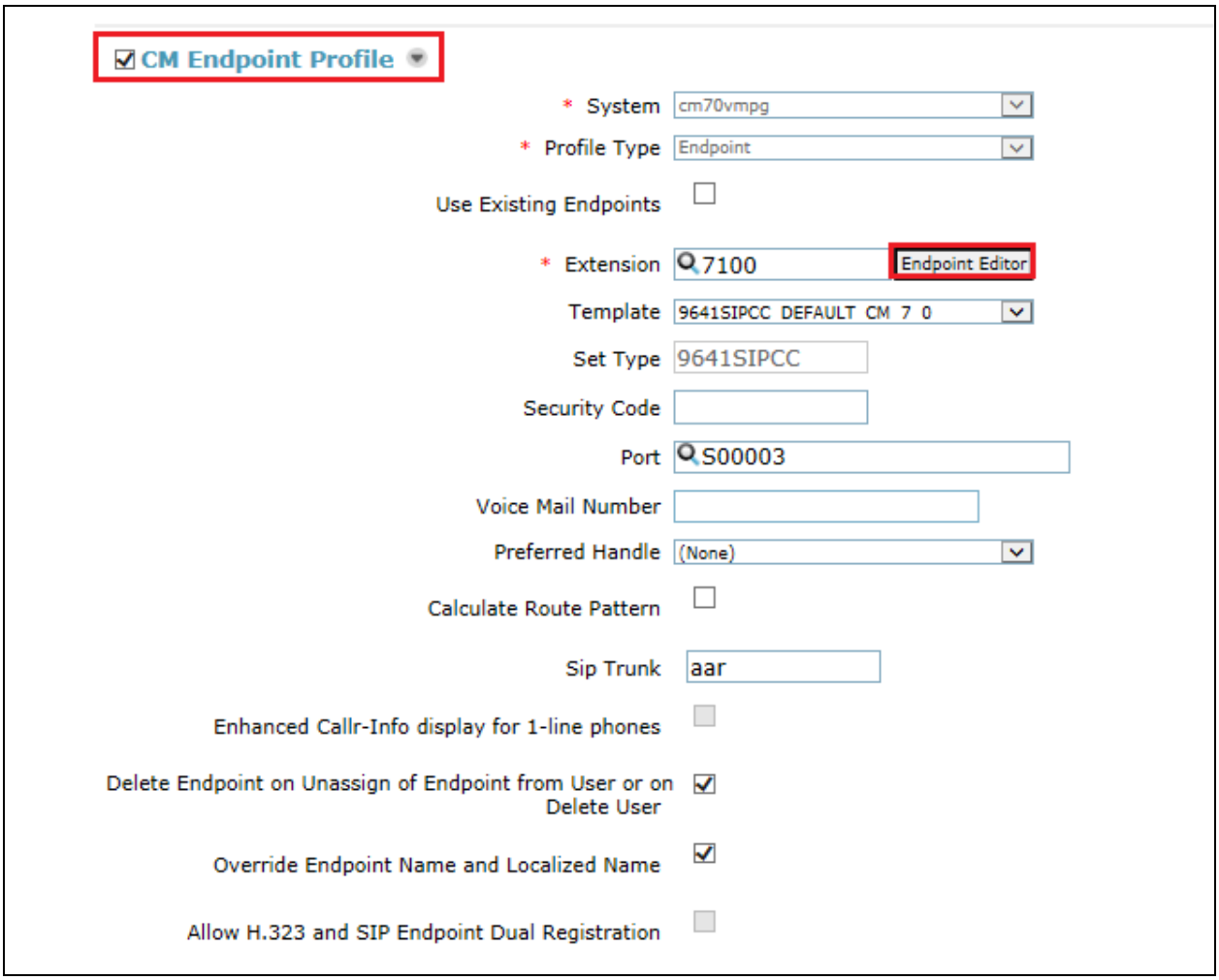
Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



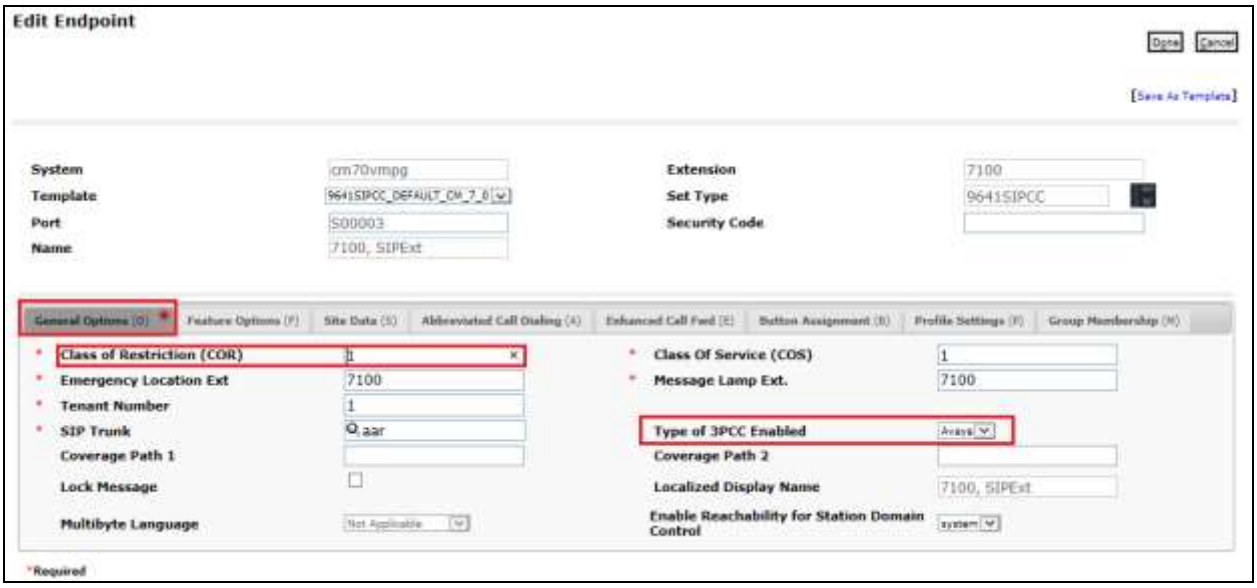
Click on the **Communication Profile** tab. Ensure that the **Communication Profile Password** is known and if not click on edit to change it.



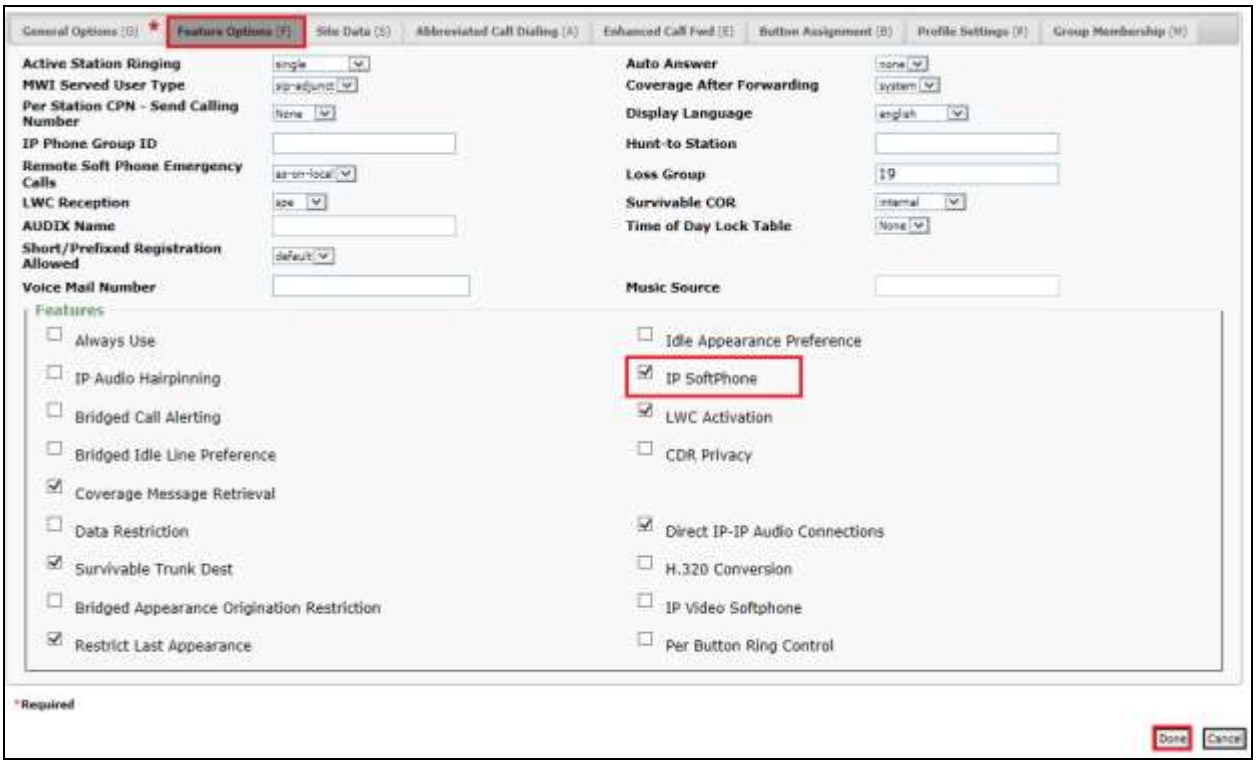
From the same page scroll down to **CM Endpoint Profile** click on **Endpoint Editor** to make further changes.



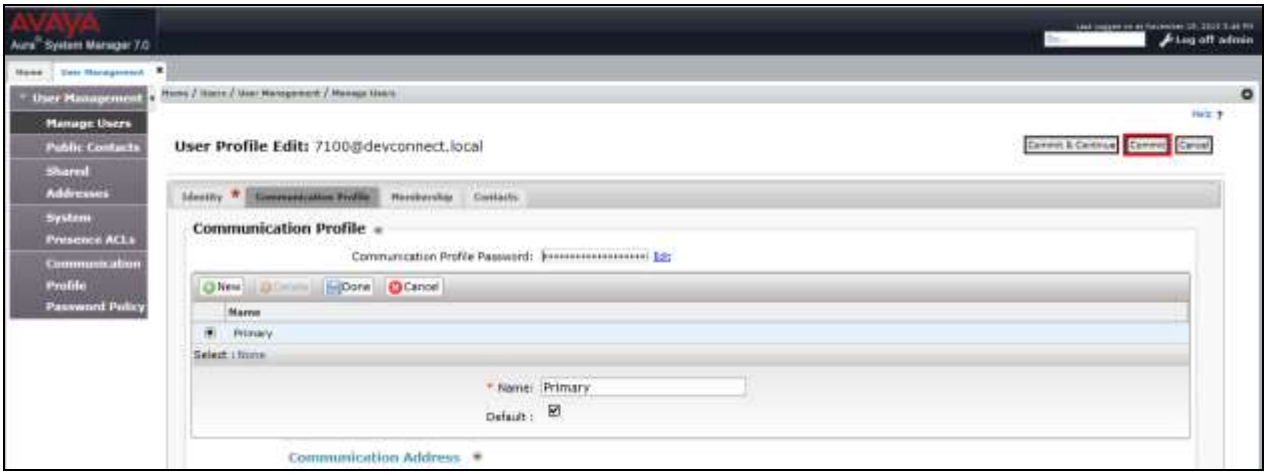
In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.



Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done**, at the bottom of the screen, once this is set.



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



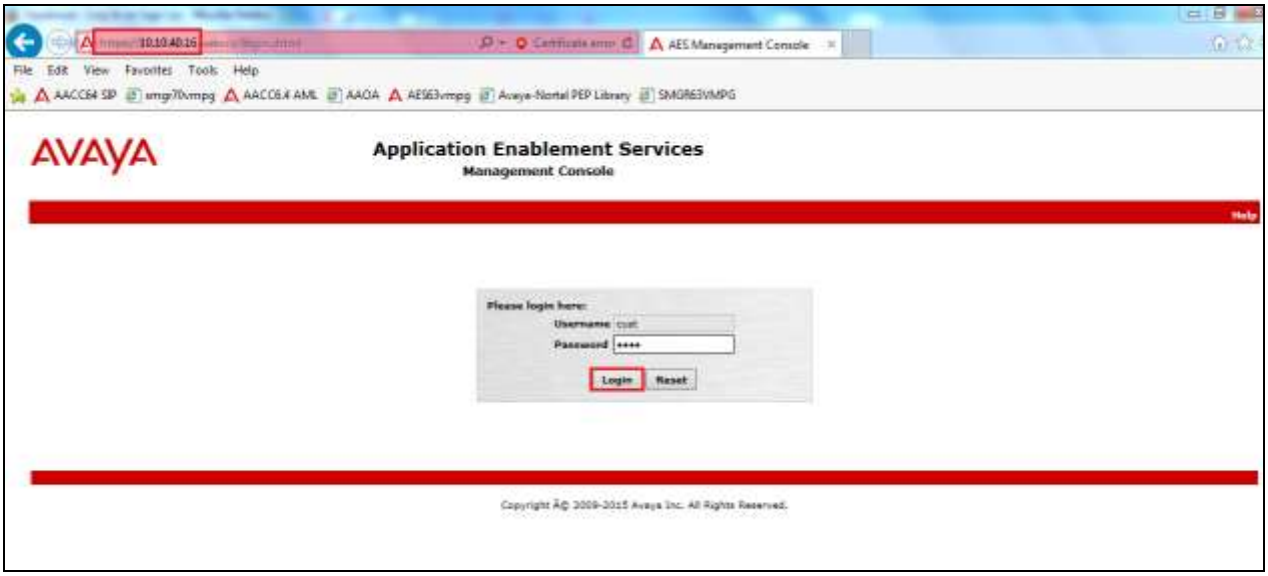
6. Configure Avaya Aura® Application Enablement Services

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

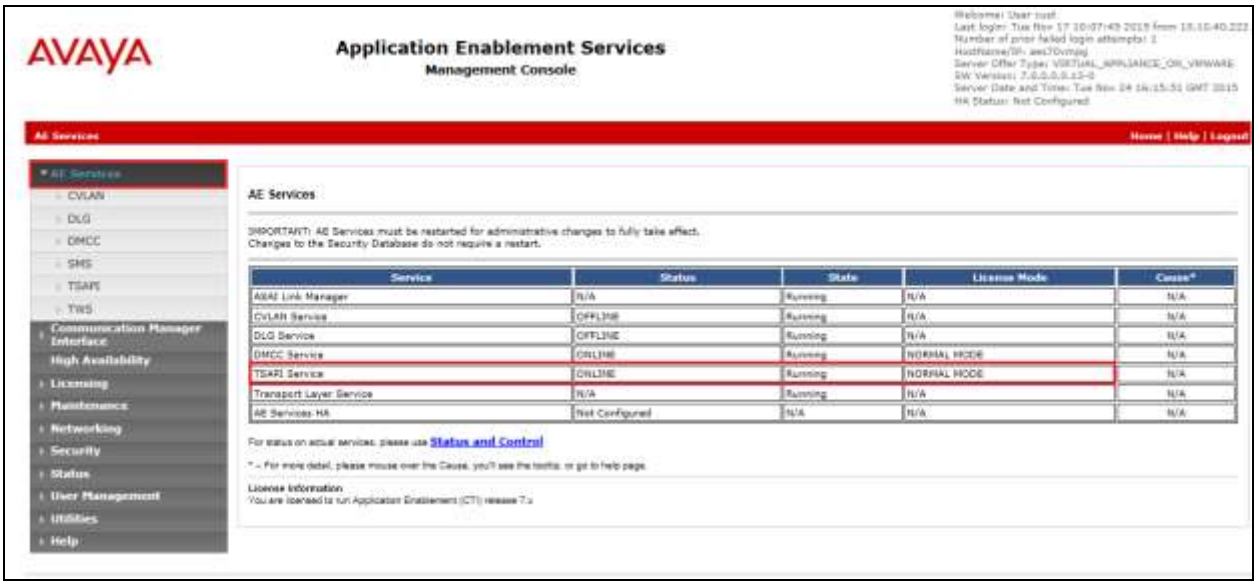
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI and DMCC Ports
- Create CTI User
- Set Up Security Database on AES
- Associate Devices with CTI User

6.1. Verify Licensing

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



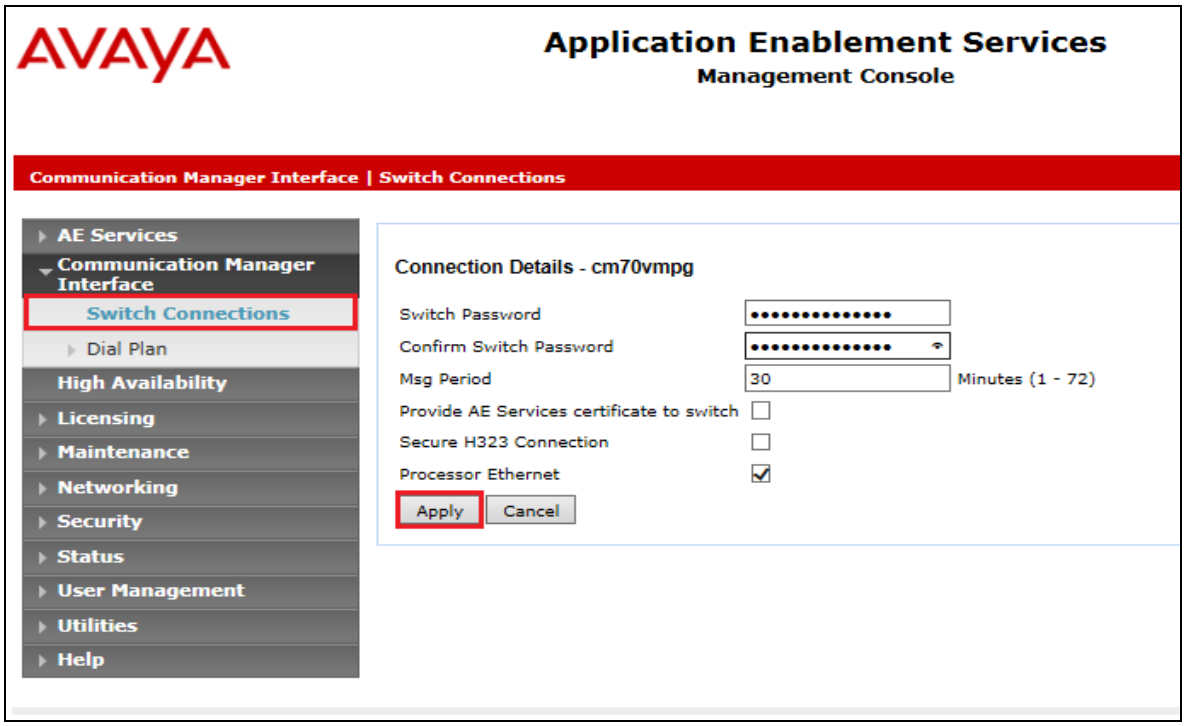
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL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



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.

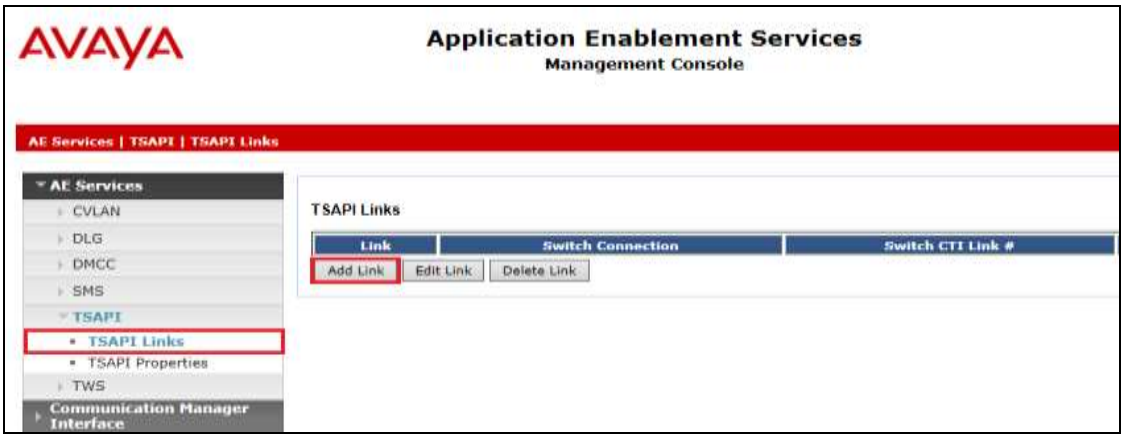
In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. Default values may be accepted for the remaining fields. Click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



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

6.3. Administer TSAPI link

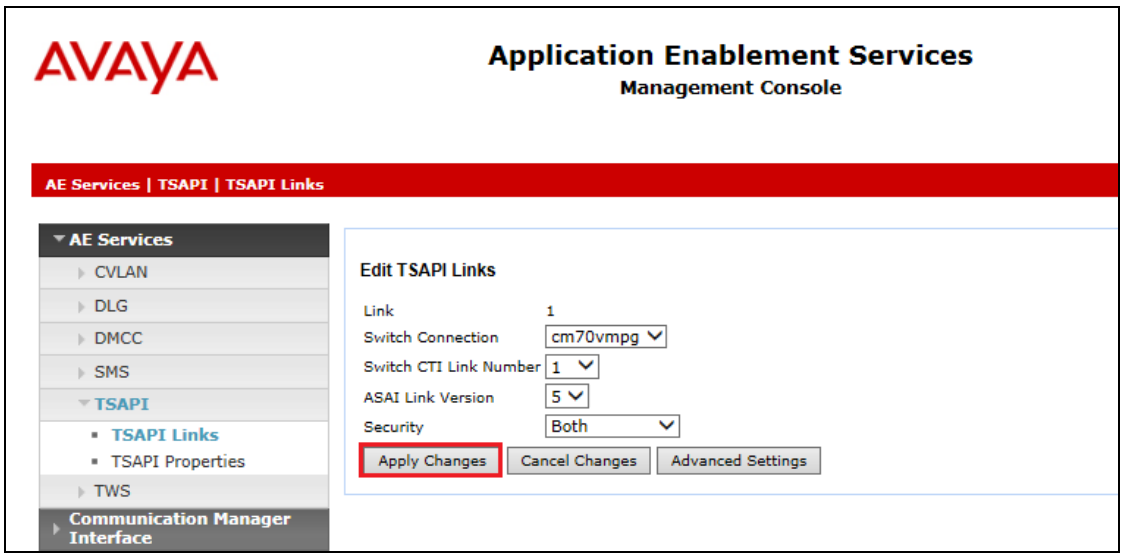
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



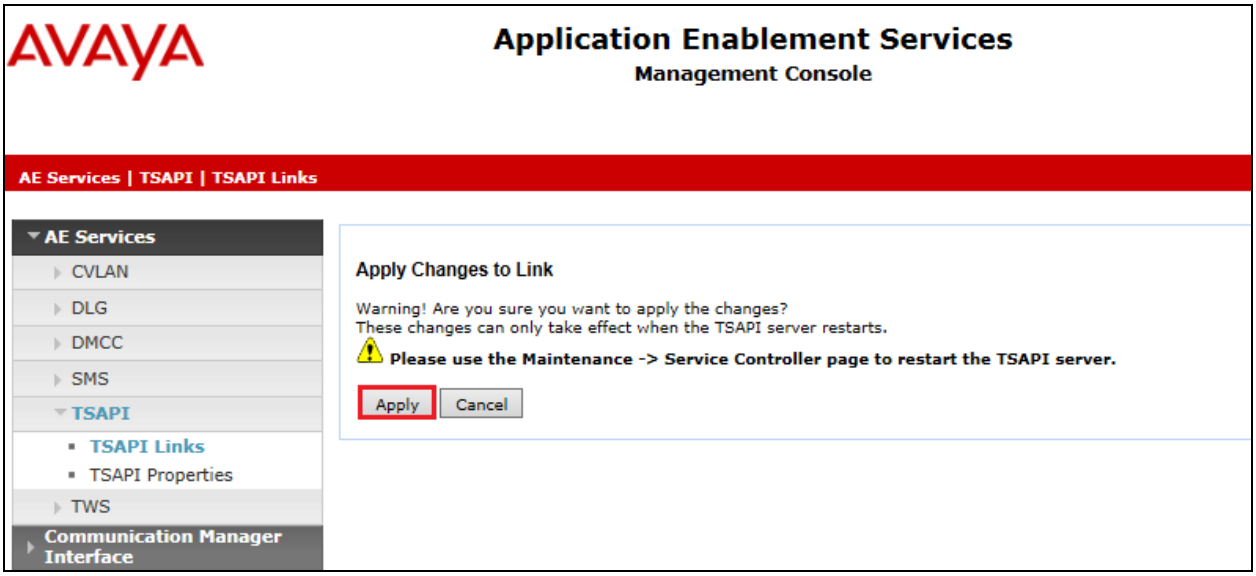
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm70vmpg**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

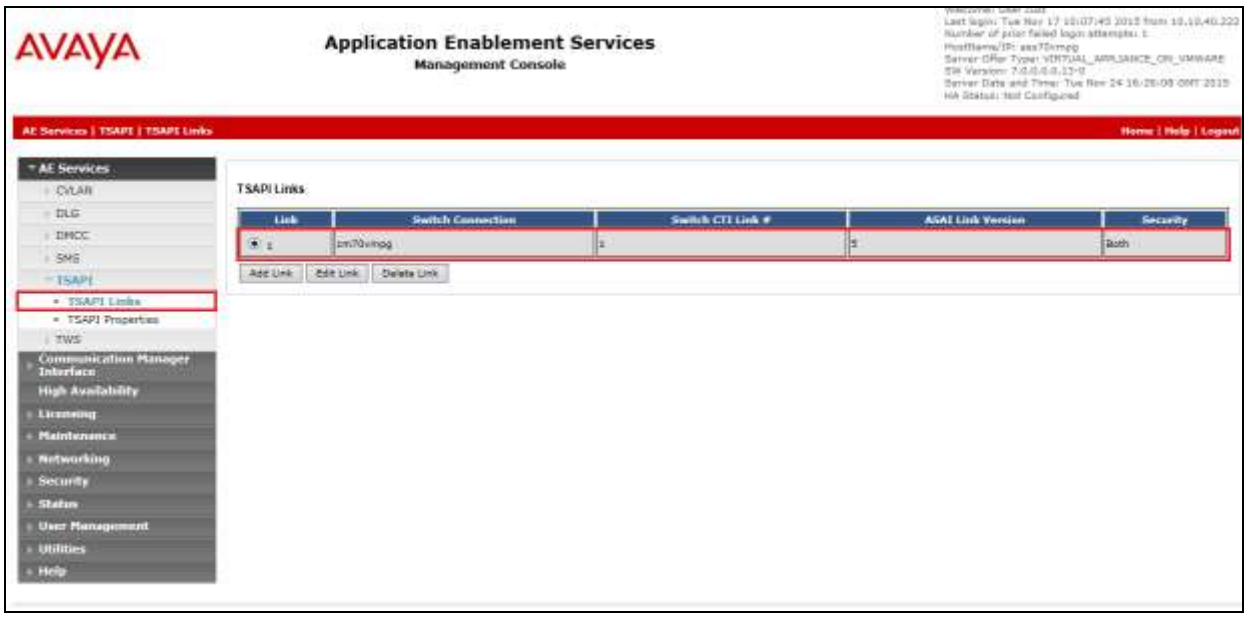
Once completed, select **Apply Changes**.



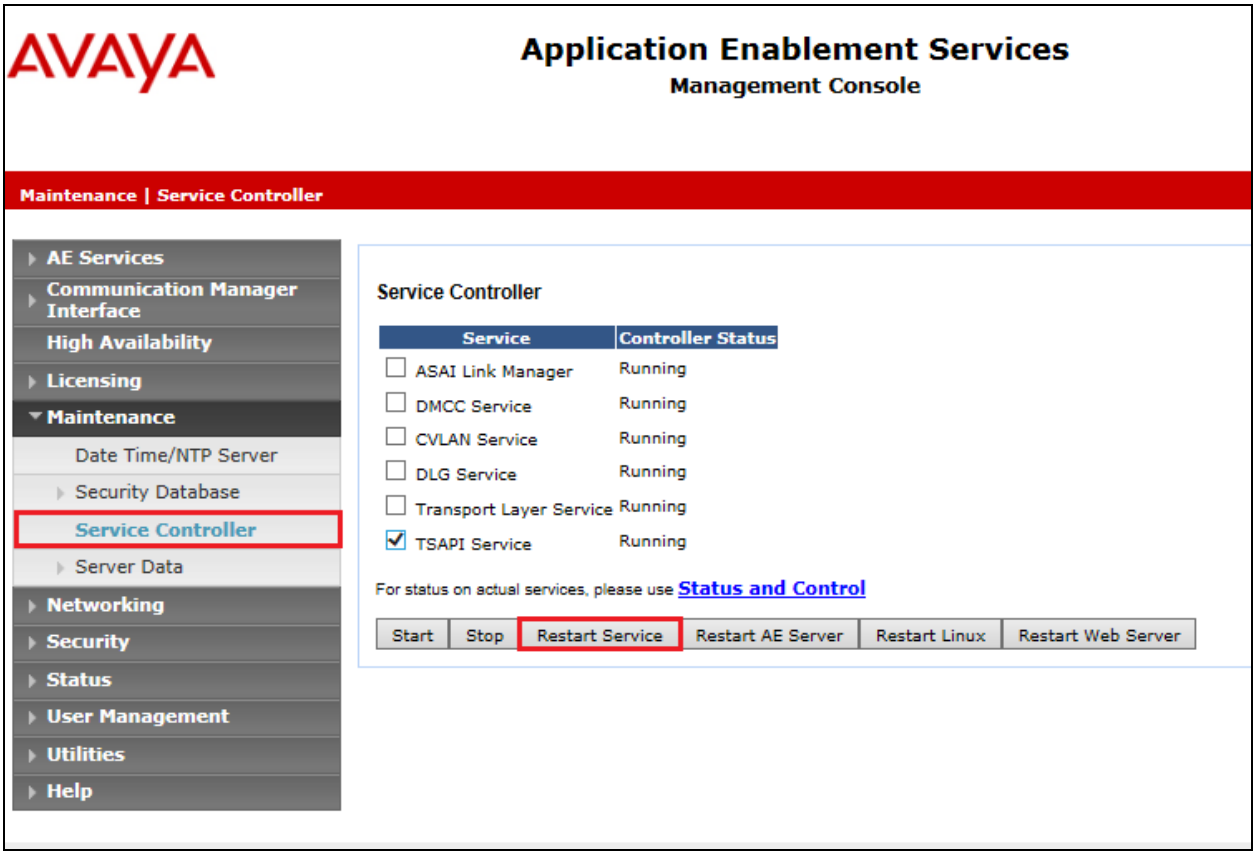
Another screen appears for confirmation of the changes made. Choose **Apply**.



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

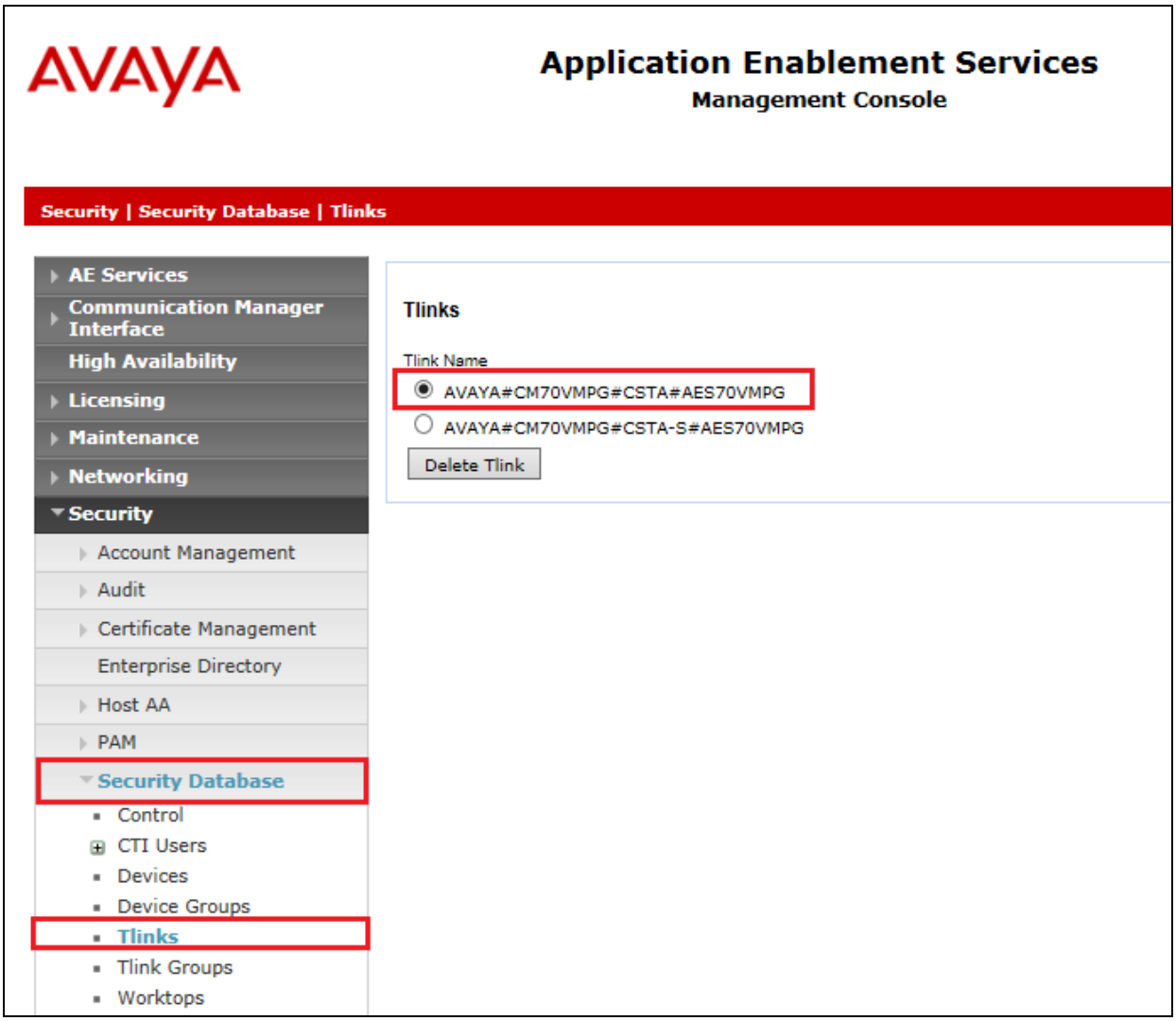


The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



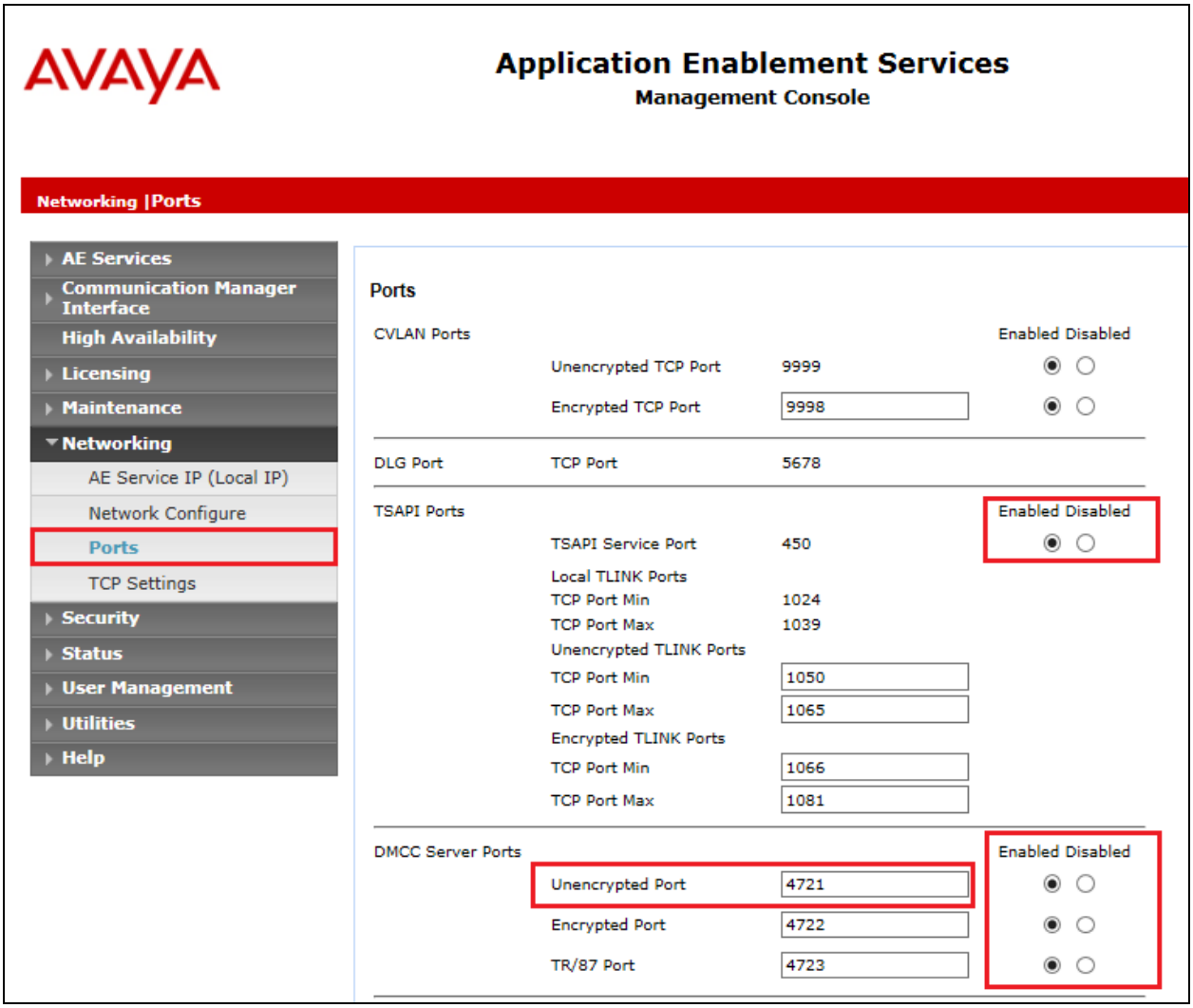
6.4. Identify Tlinks

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



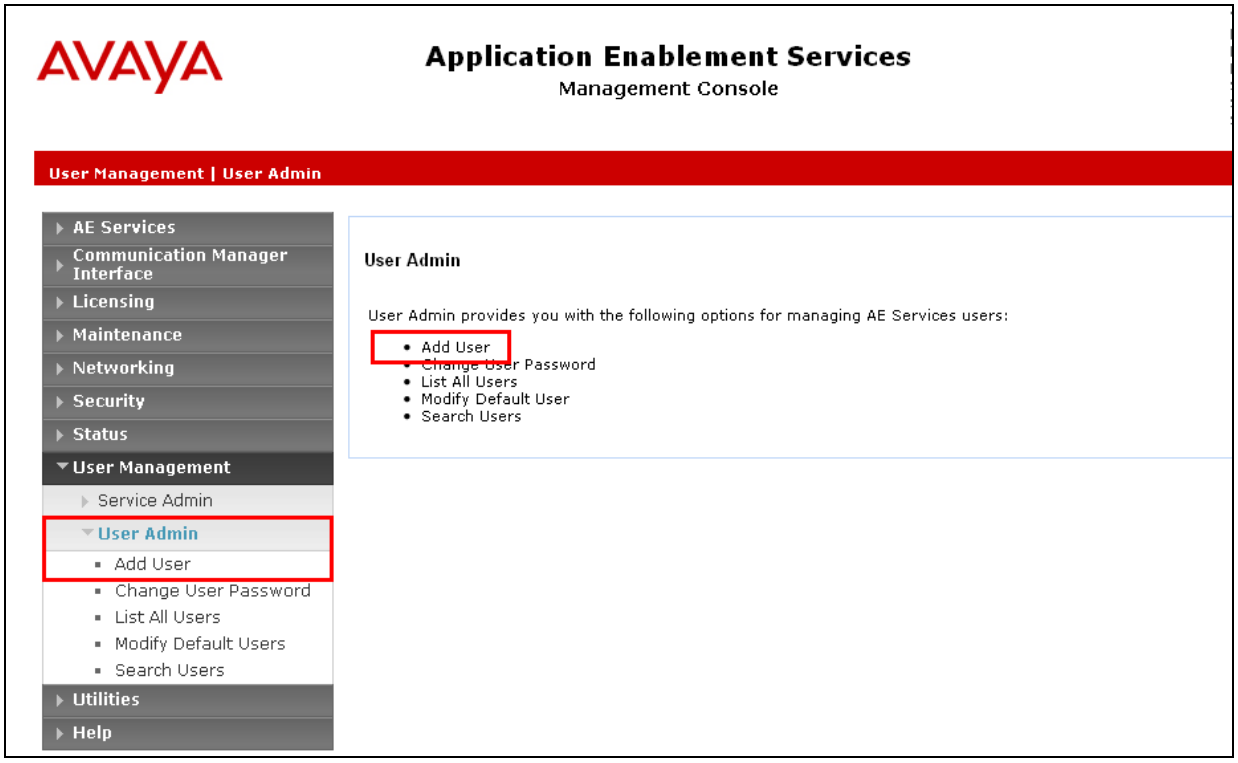
6.5. Enable TSAPI and DMCC Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.1**.



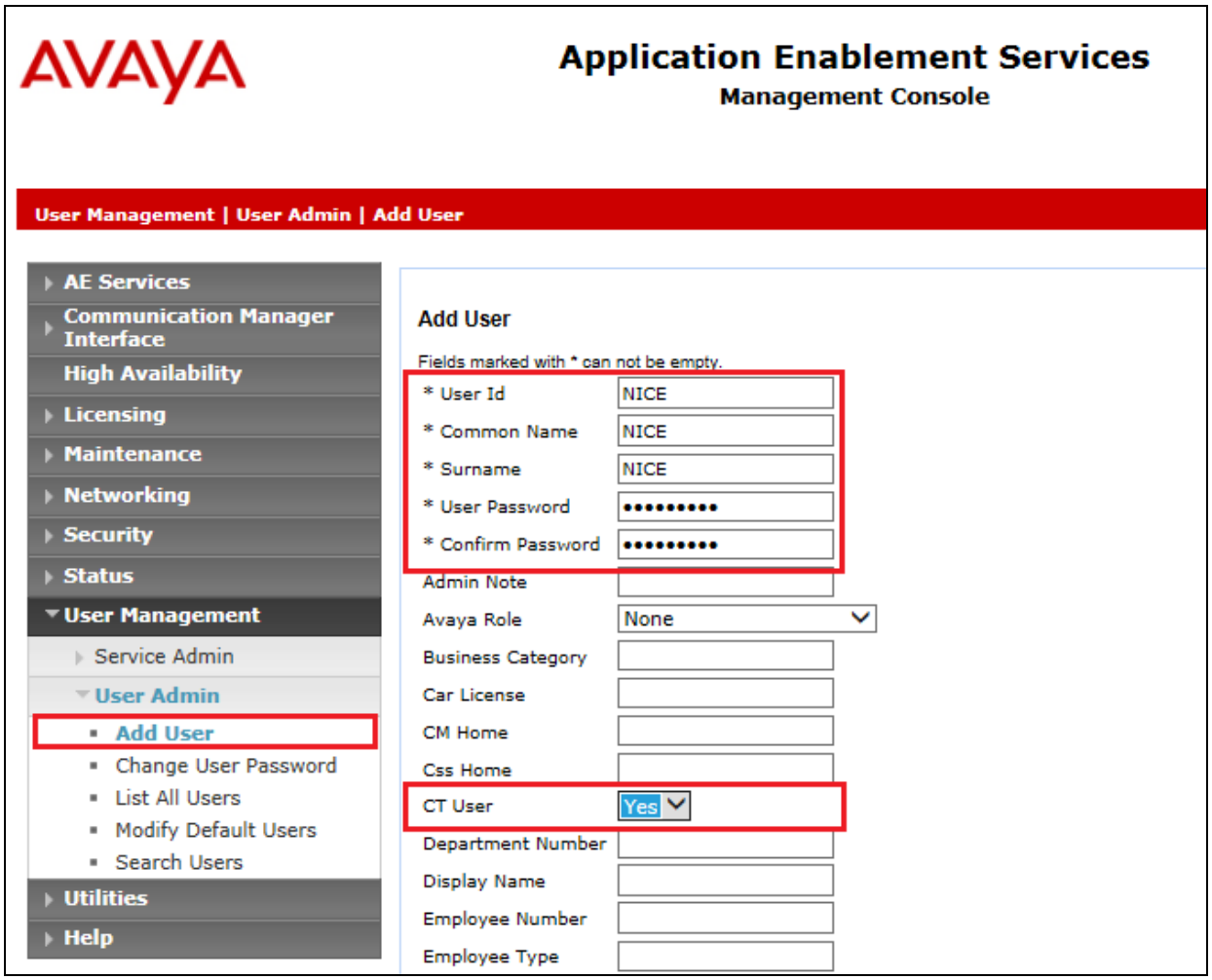
6.6. Create CTI User

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

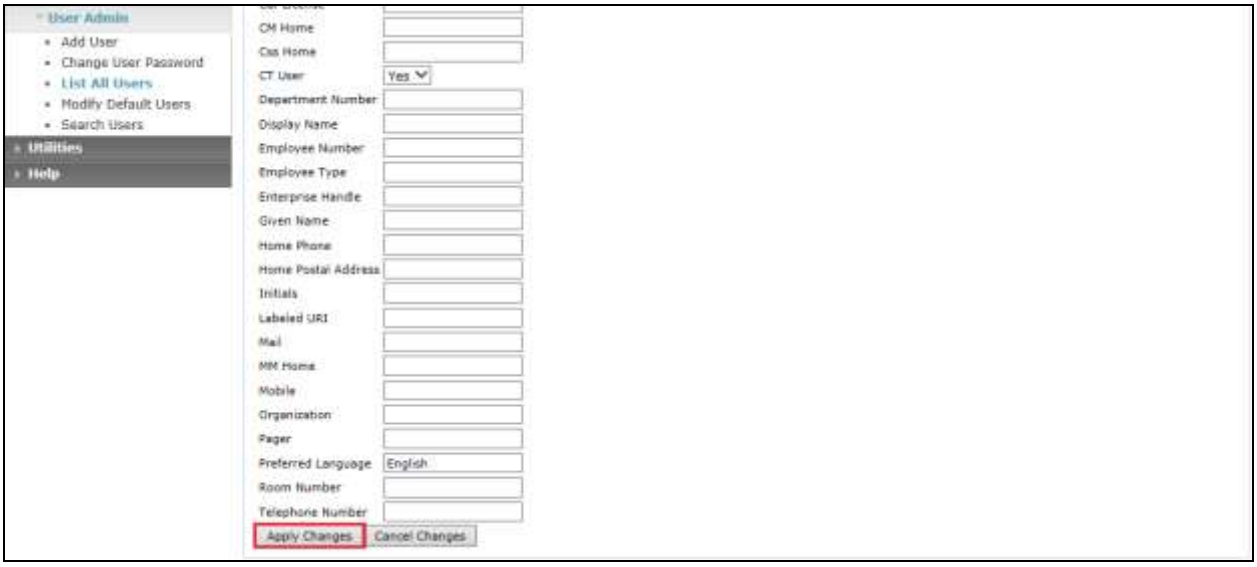


In the **Add User** screen shown below, enter the following values:

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

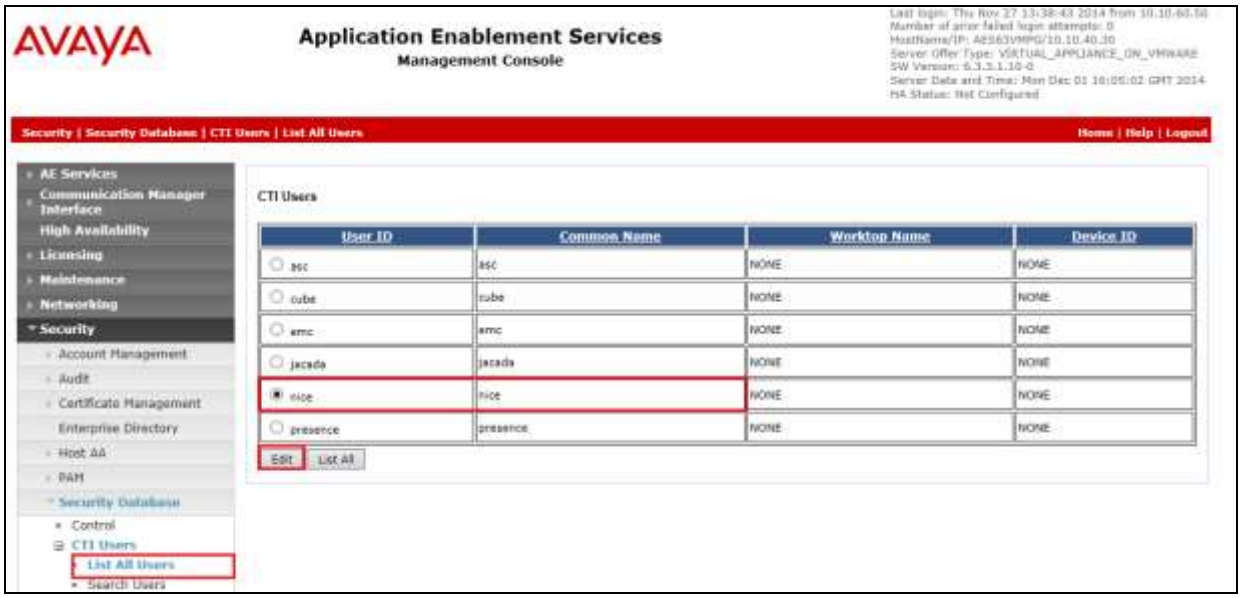


Scroll down and click on **Apply Changes**.

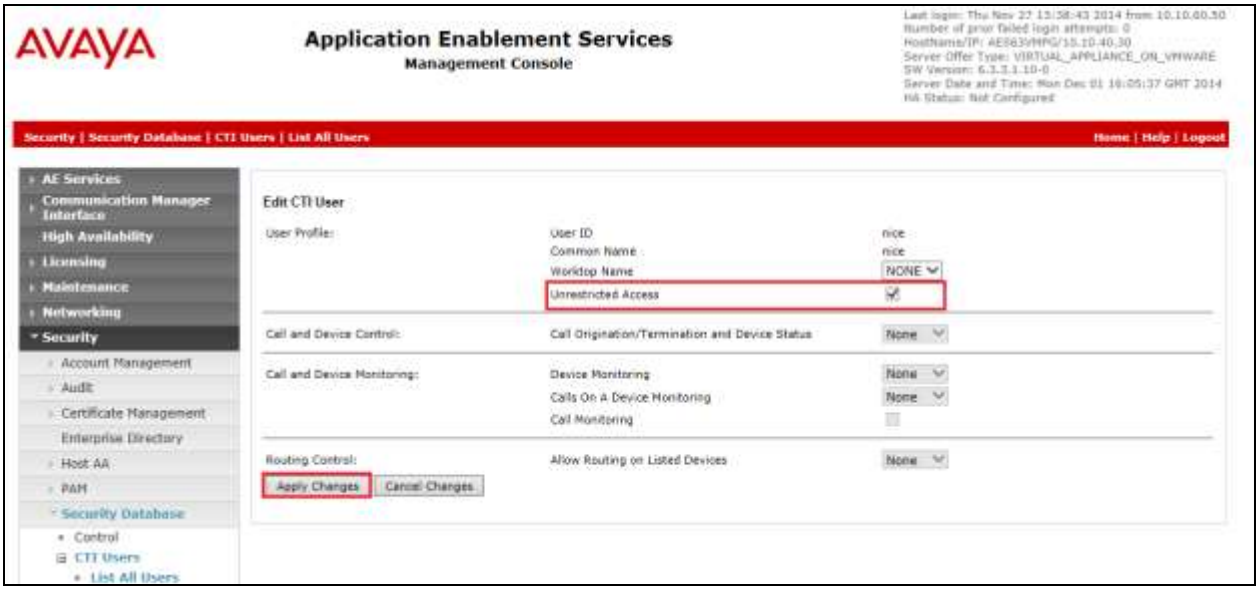


6.7. Associate Devices with CTI User

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



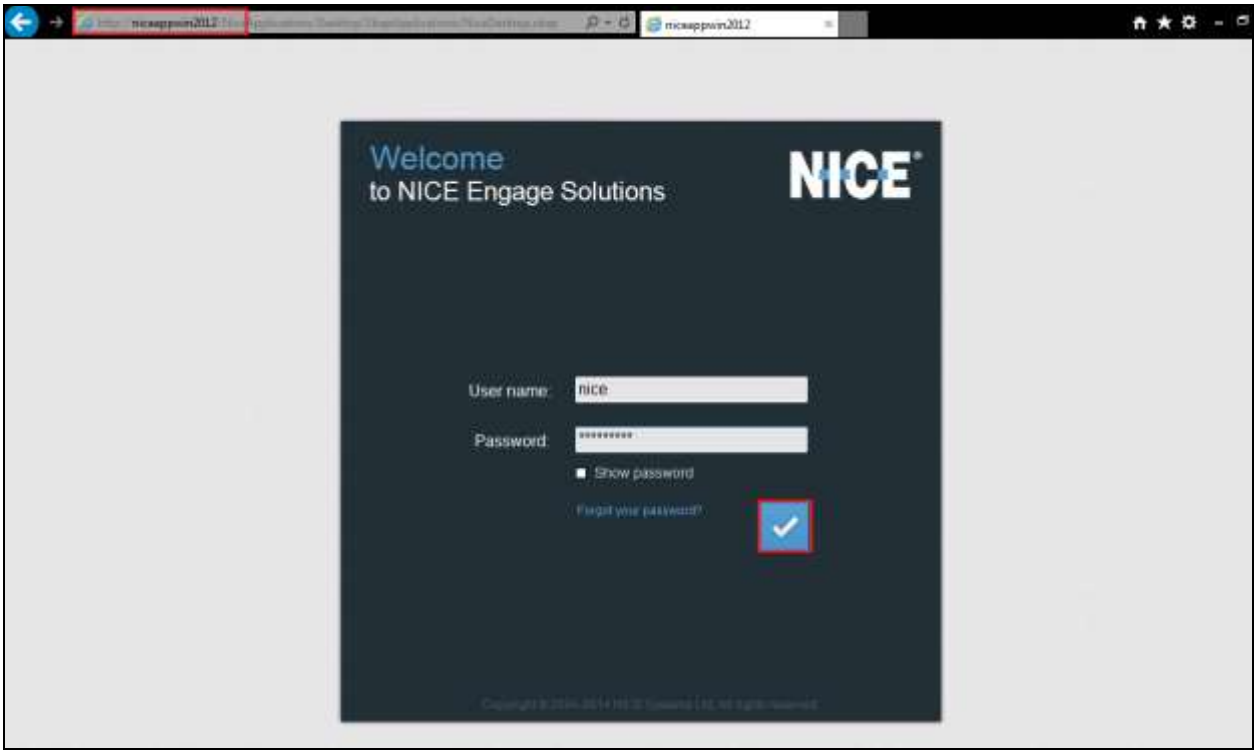
In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.



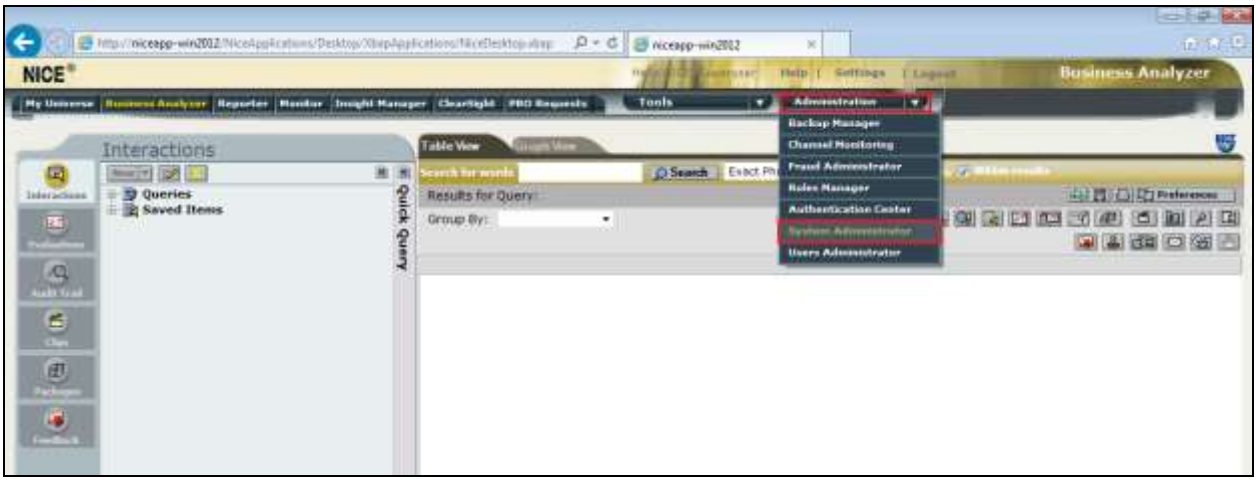
7. Configure NICE Engage Platform

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

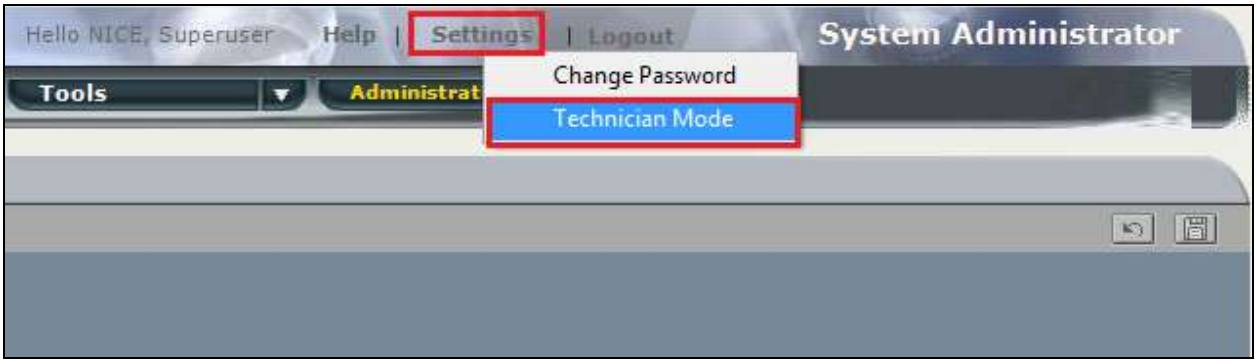
The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya Solution. All configuration of the NICE Engage Platform for connection with the AES is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser as shown navigate to **http://<NICEEngageApplicationServerIP>/Nice** as shown below and enter the proper credentials and click on **Login**.



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

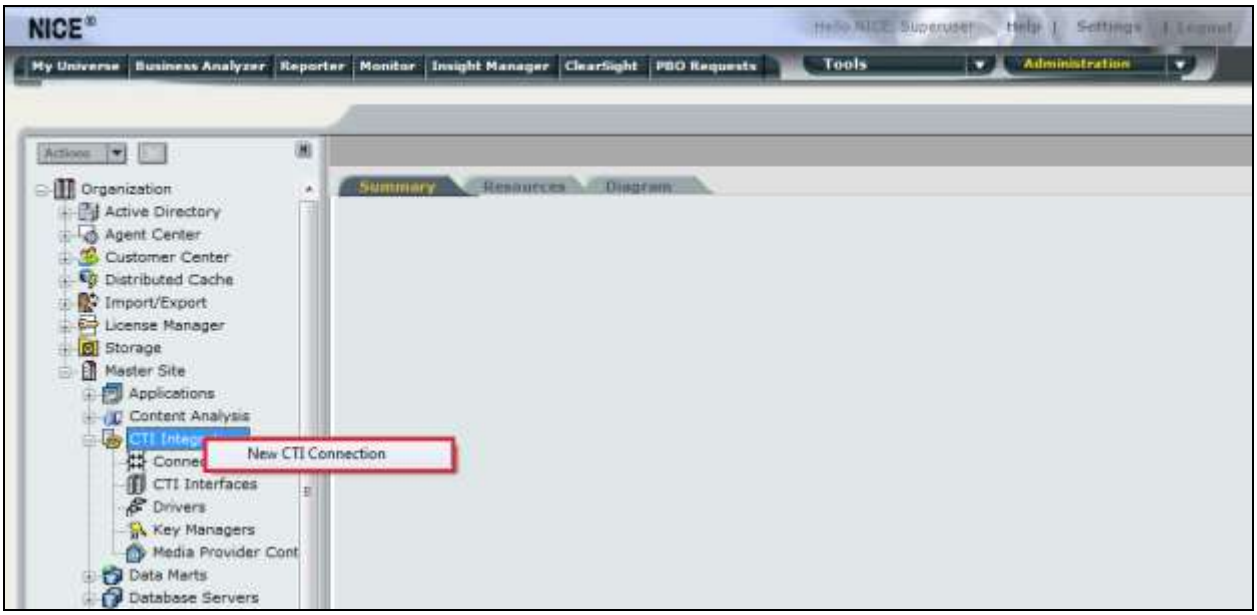


Before any changes can be made, switch to Technician Mode by clicking into Settings at the top of the screen as shown below.

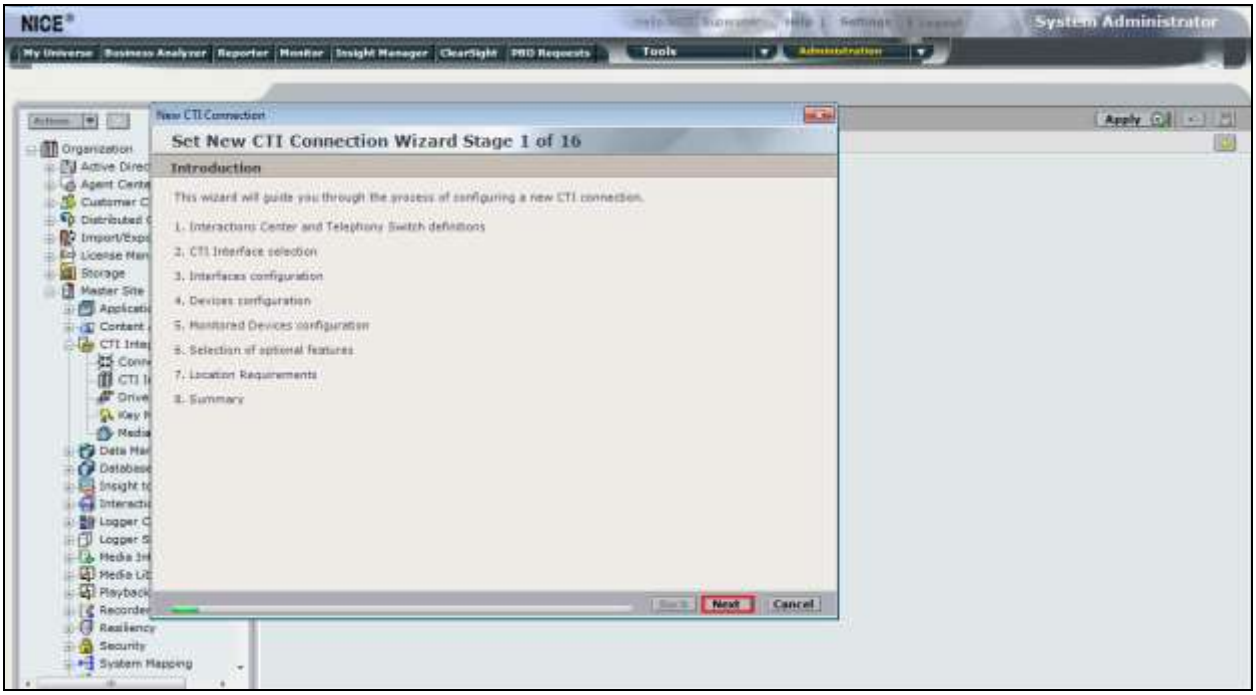


7.1. New CTI Connection

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



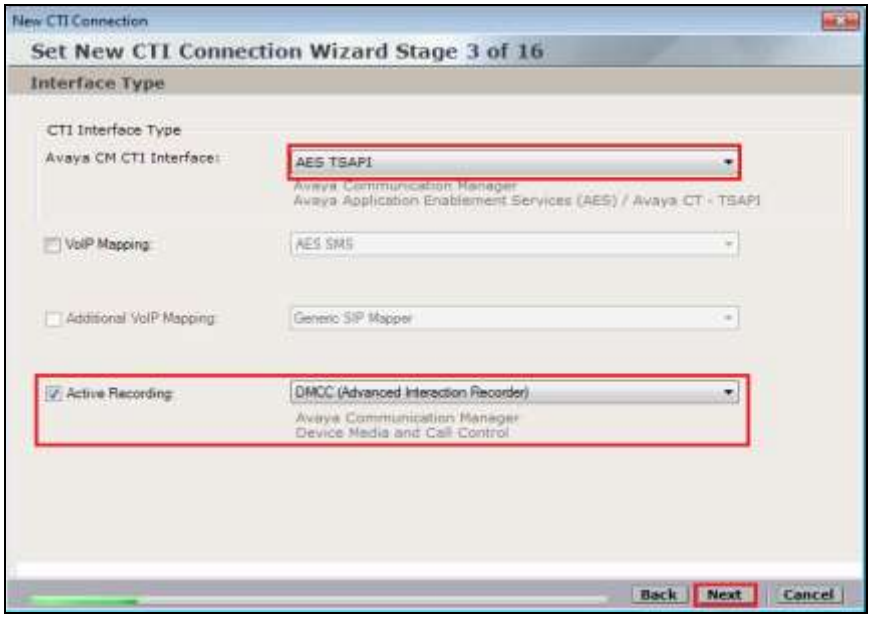
The **New CTI Connection Wizard** is opened and this will go through the 16 steps required to setup the connection to the AES for DMCC Multi-Registration type of call recording. Click on **Next** to continue.



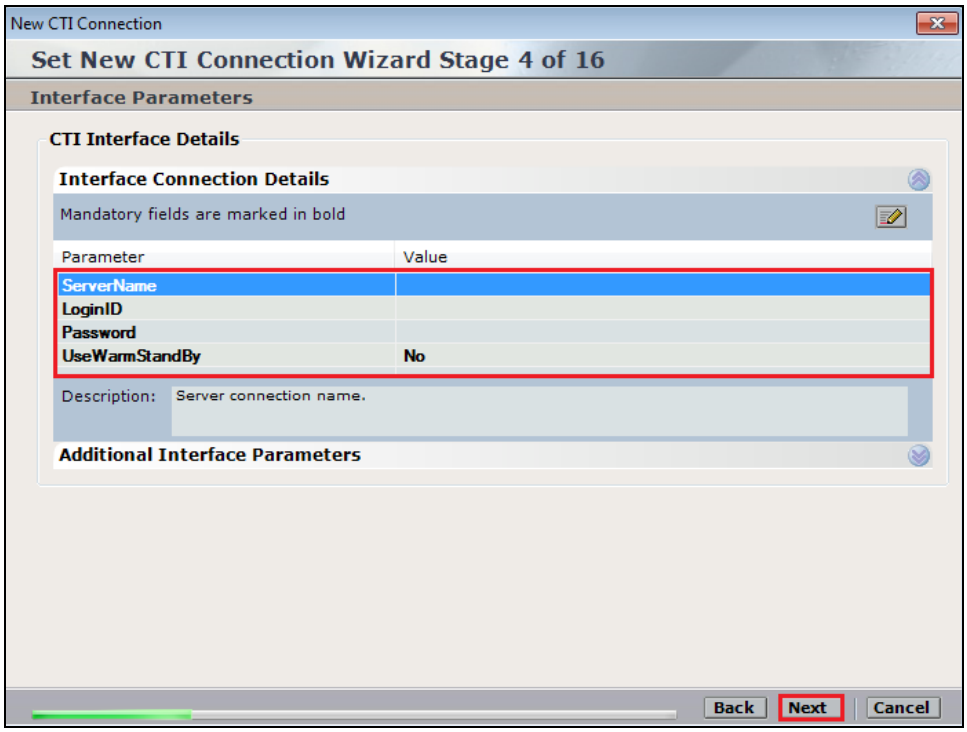
The value for **Regular Interactions Center** (**IC**) is a value that was already created during the installation of the NICE Engage platform. This value is therefore pre-chosen for the CTI connection being created below.

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

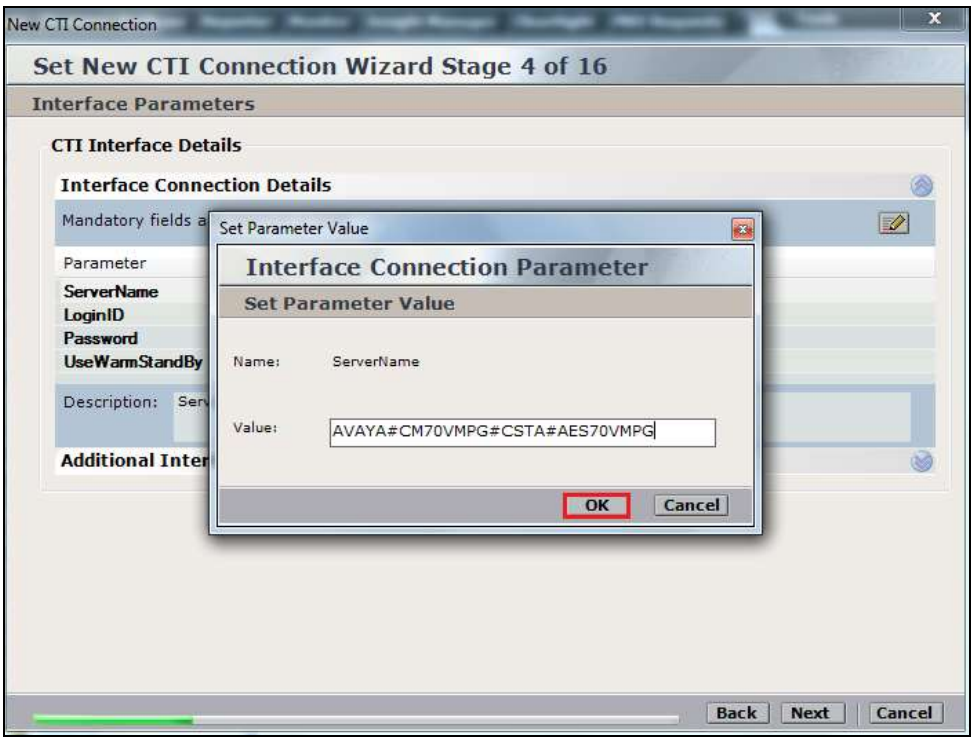
Select **AES TSAPI** for the **Avaya CM CTI Interface**, ensure that **Active Recording** is ticked and select the **DMCC (Advanced integration Recorder)** from the dropdown menu. Click on **Next** to continue.



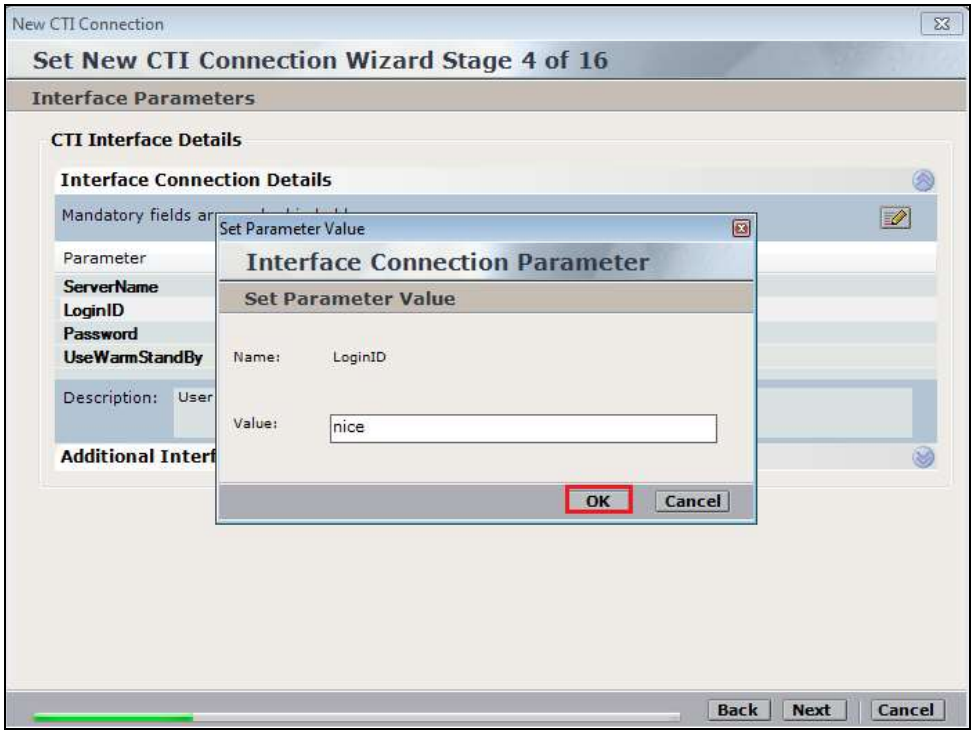
Each of the values below must be filled in. Double-click on each **Parameter** to enter a value for that parameter.



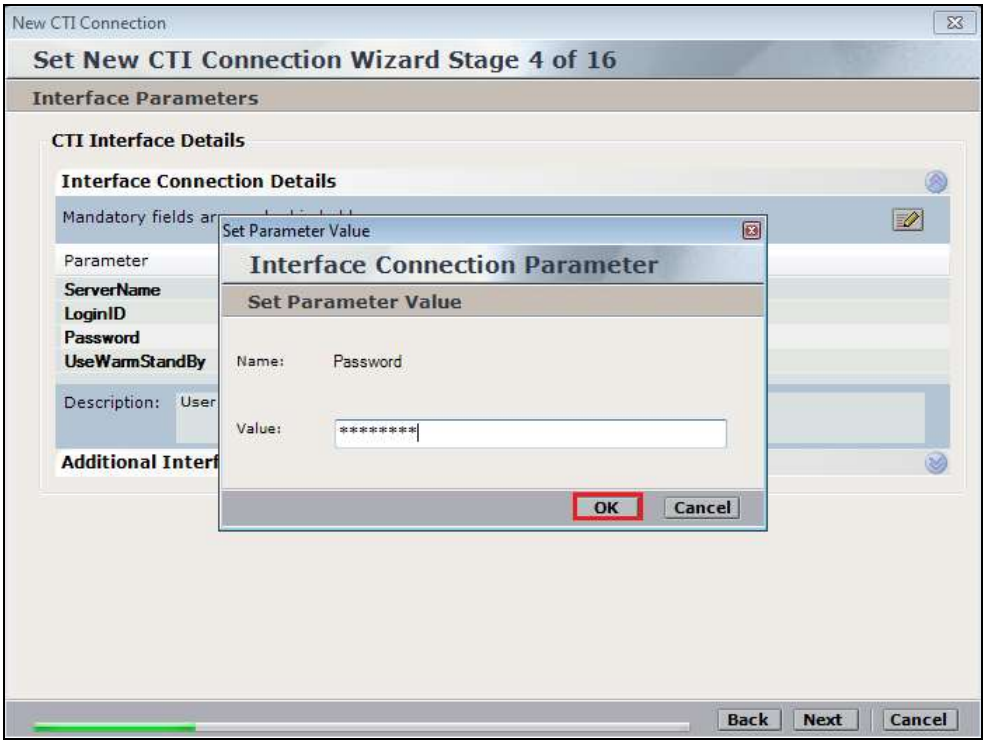
Double-click on **ServerName** and enter the TSAPI link **Value** from **Section 6.4**.



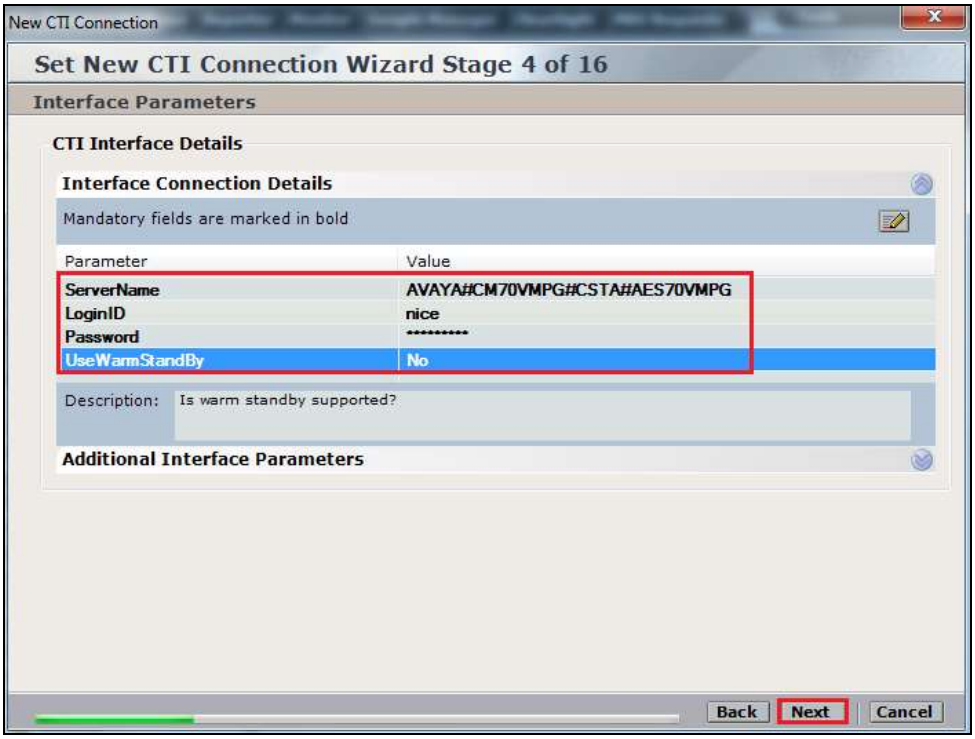
Double-click on **LoginID** and enter the username that was created in **Section 6.6**. Click on **OK**.



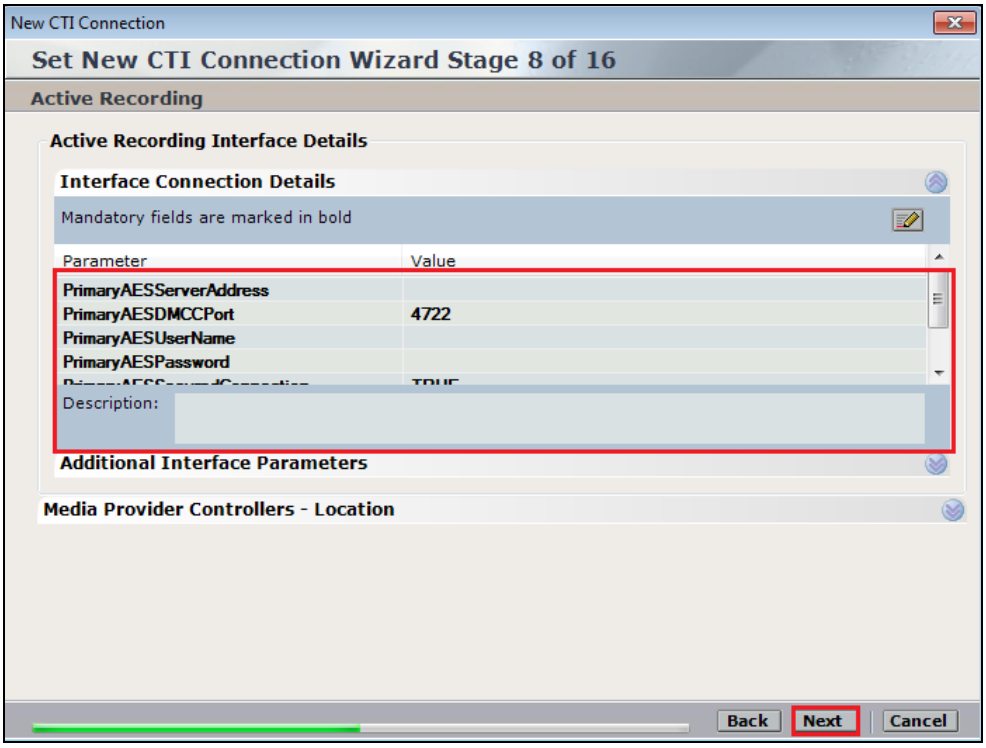
Double-click on **Password** and enter the value for the password that was created in **Section 6.6**.



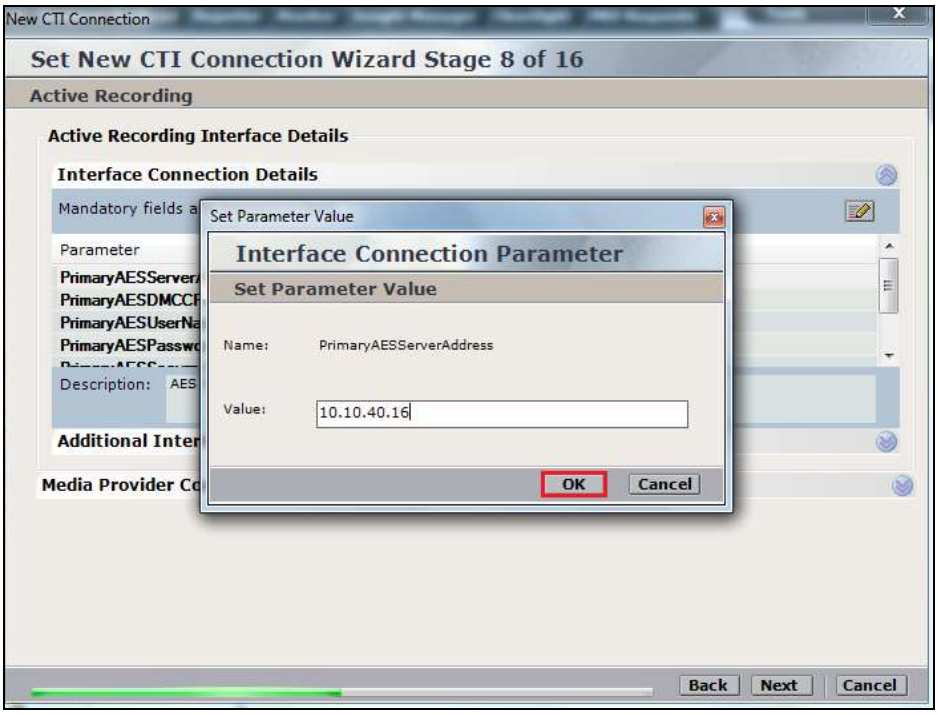
Click on **Next** once these values are all filled in.



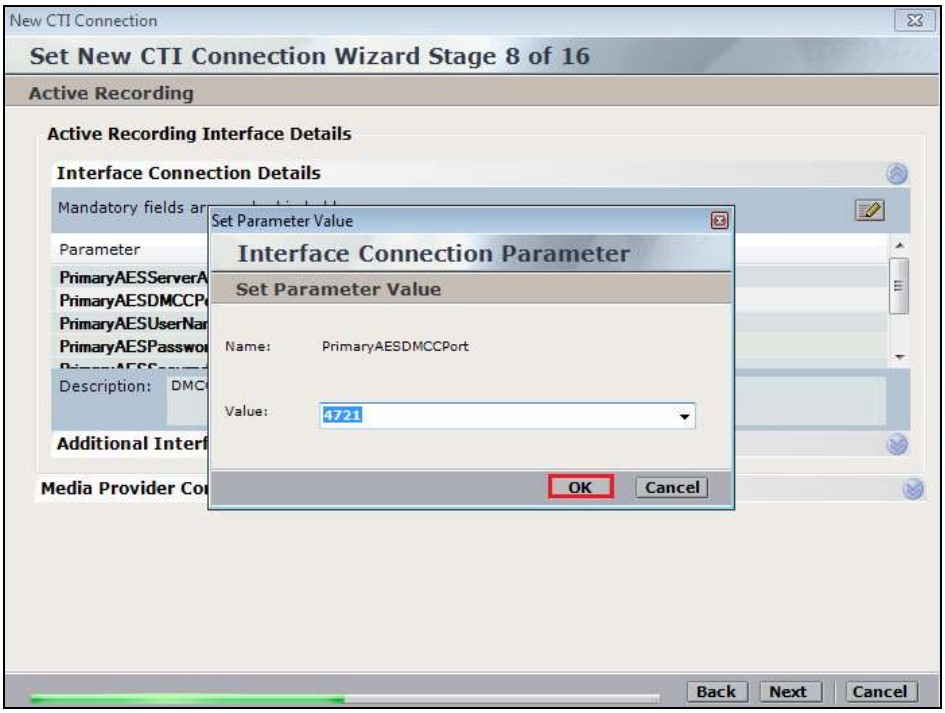
The values below must be filled in by double-clicking on each **Parameter**.



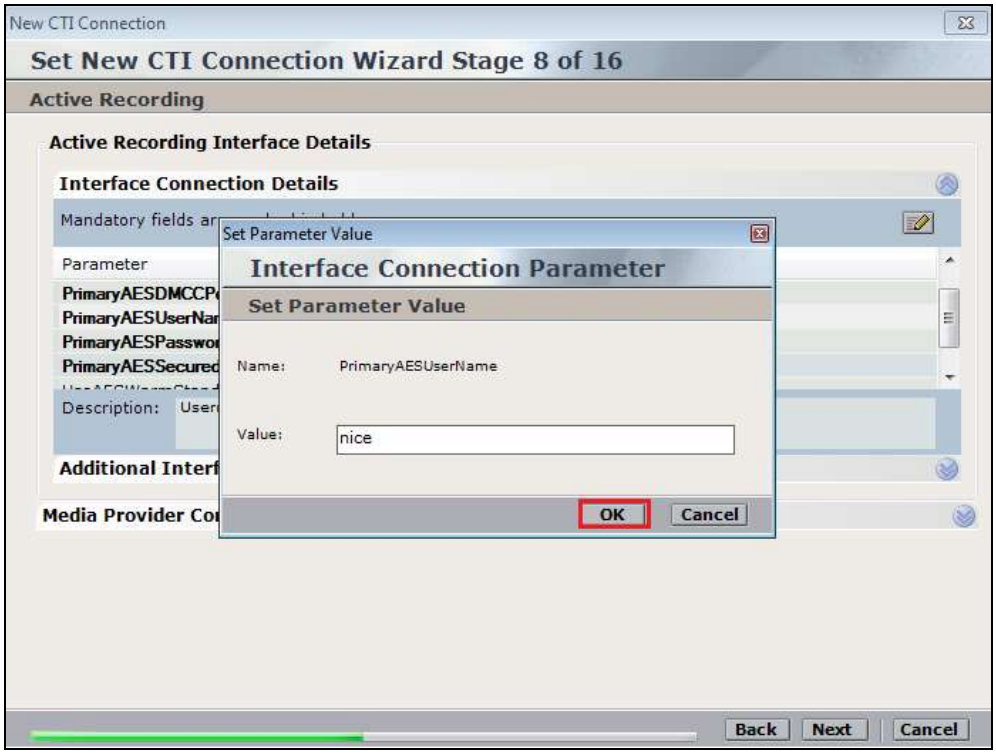
Enter the **Value** for the **AESServerAddress**, note this is the IP address of the AES server. Click on **OK**.



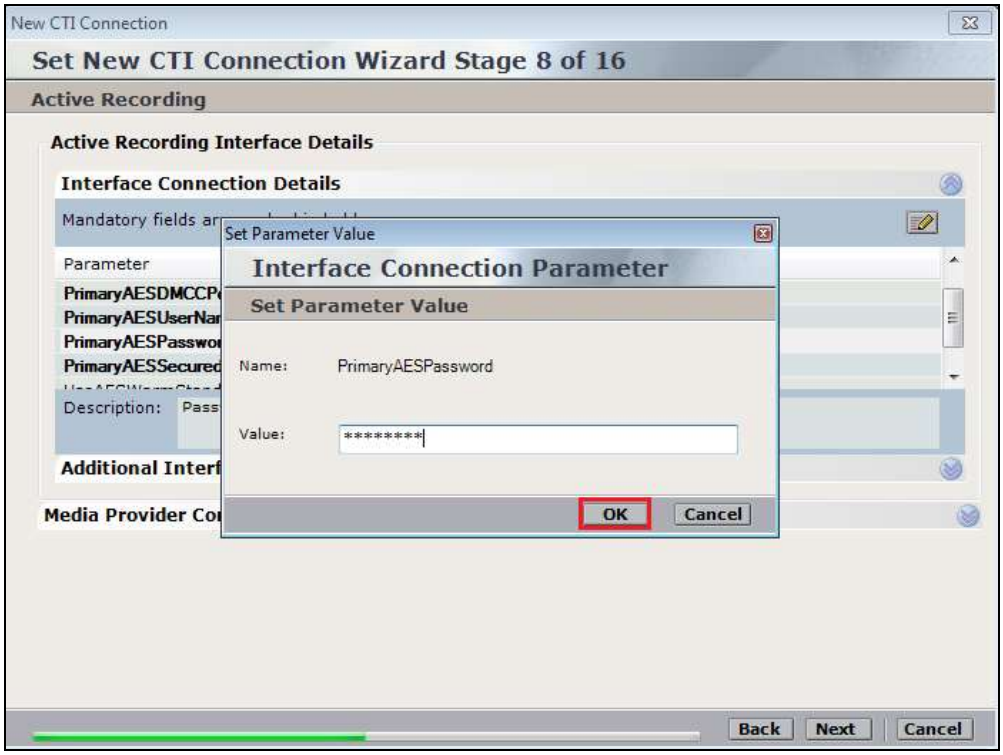
Enter the **Value** for the **AESDMCCPort**, note this will be the same port that was configured in **Section 6.5**. In this example the unencrypted port **4721** is entered.



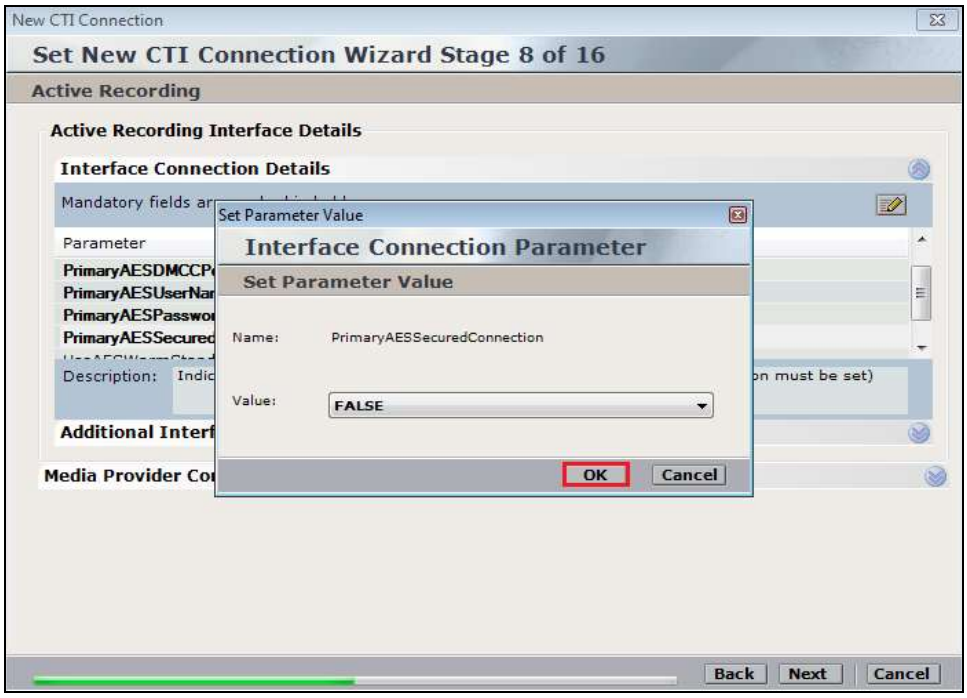
As before enter the username that was created in **Section6.6** and click on **OK**.



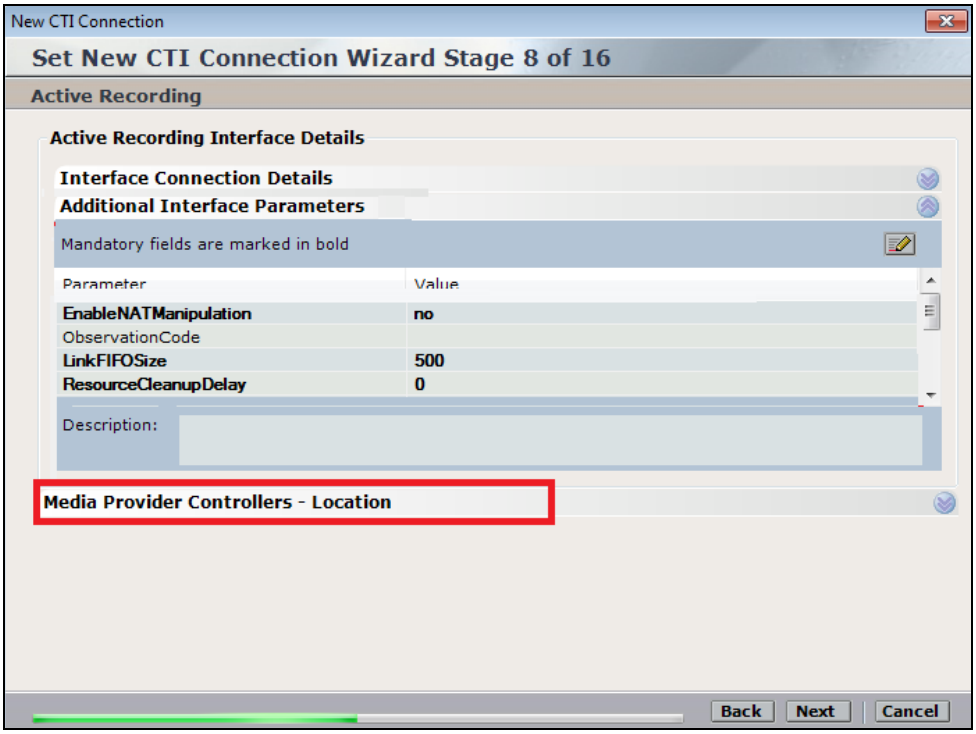
Enter the password that was created in **Section 6.6** and click on **OK**.



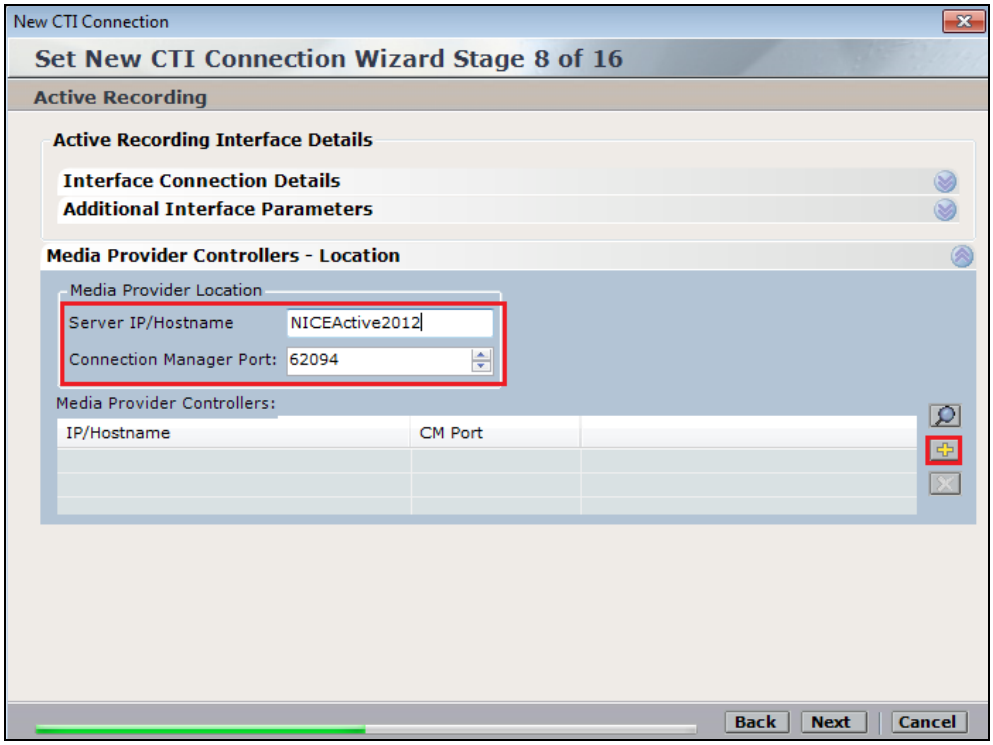
Because the unencrypted port was chosen select **False** for the **AESSecuredConnection**. Click on **OK** and then **Next** to continue.



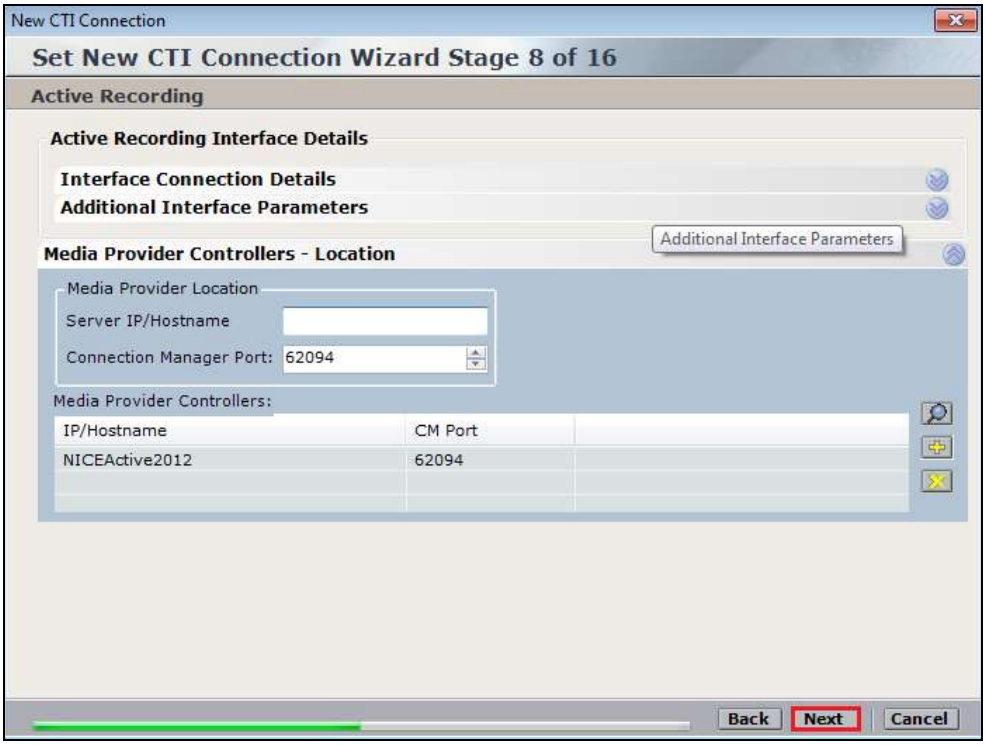
Click on **Media Provider Controllers – Location** to expand this.



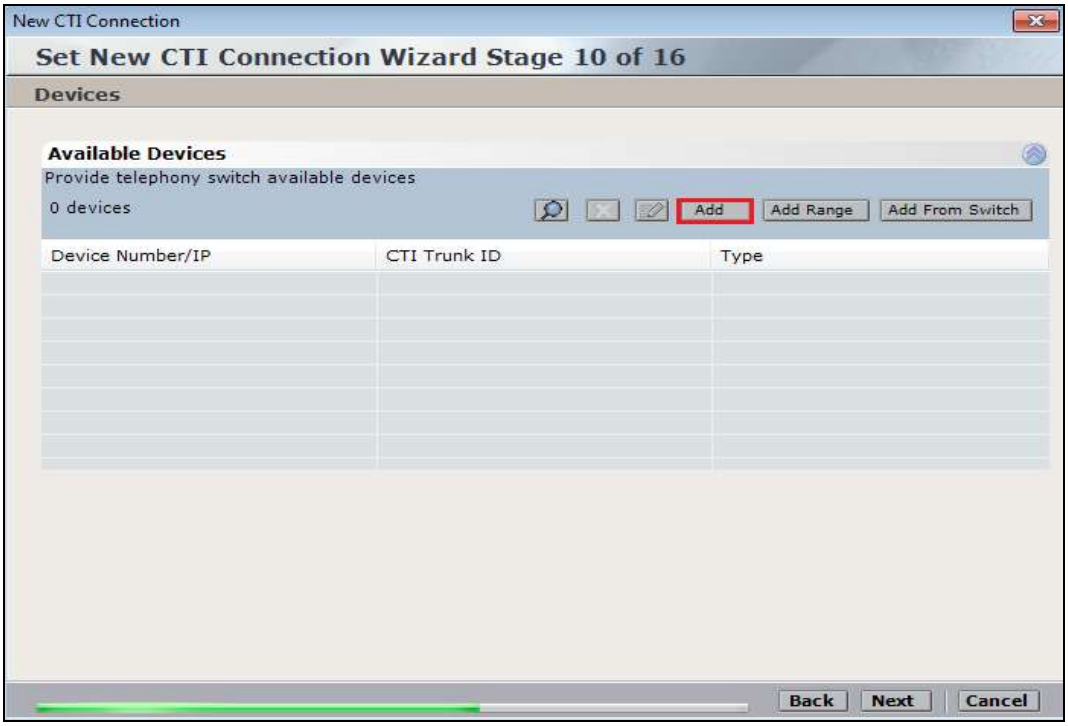
Enter the **IP/Hostname** of the Nice Advanced Interactions Server. Click on in + icon to add this.



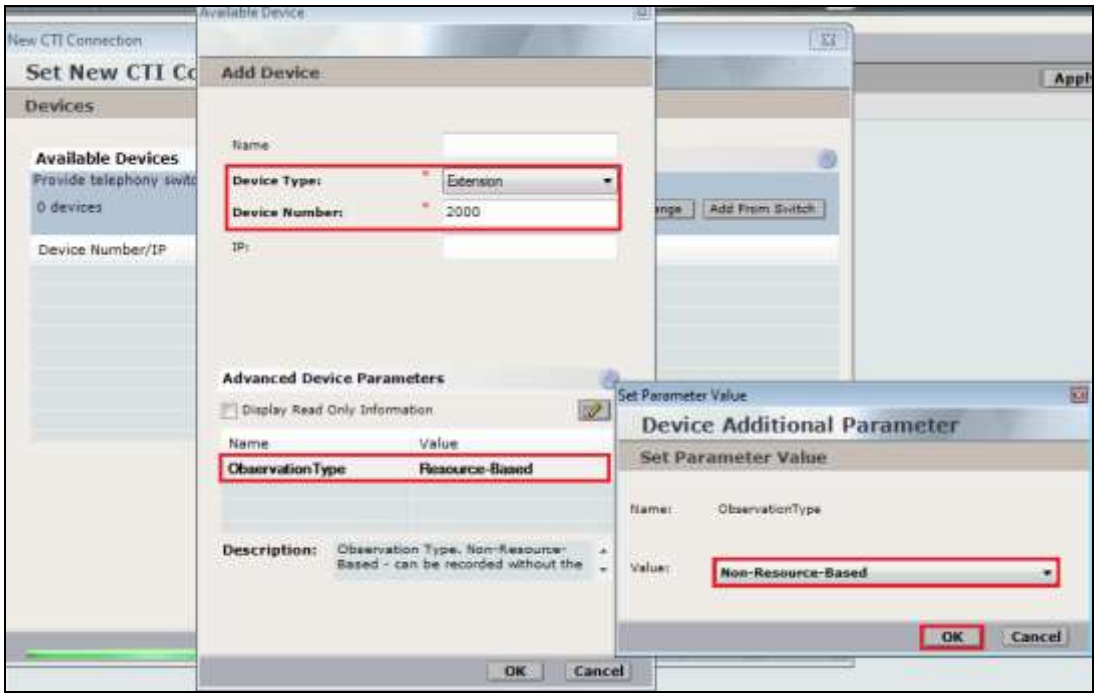
Click on **Next** to continue.



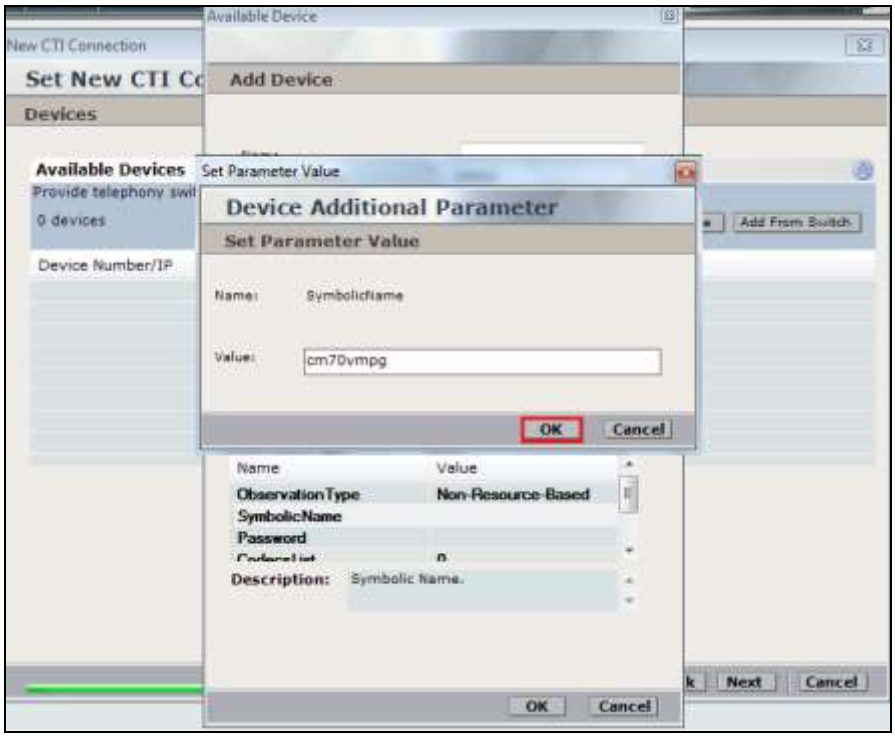
On the following screen, click on **Add,** to add the Communication Manager devices.



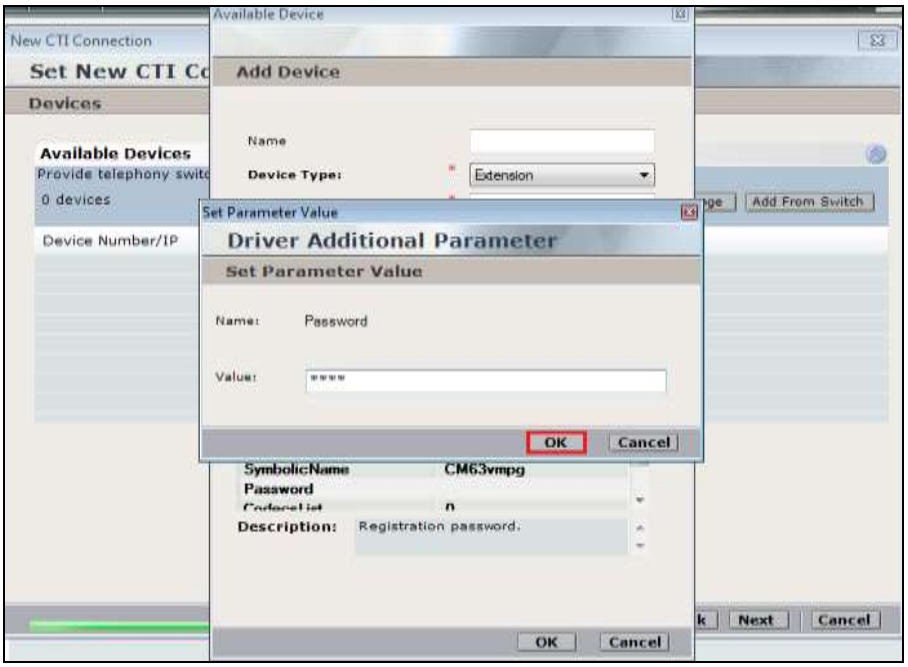
The **Device Type** should be **Extension** and insert the correct extension number. Expand **Advanced Device Parameters** and ensure that the **Value** for **Observation Type** is set to **Non-Resourced-Based**. Click on **OK** to continue.



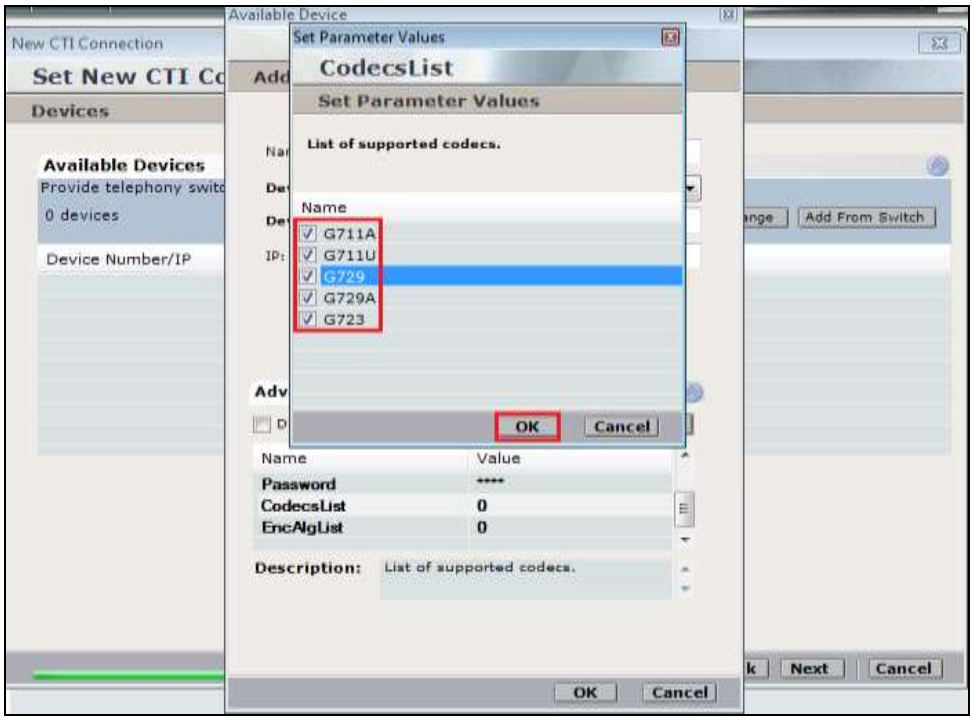
Next enter the correct **Value** for **SymbolicName**. Double-click on **SymbolicName** to set the value. This should be the same as the switch name entered in **Section 6.2**.



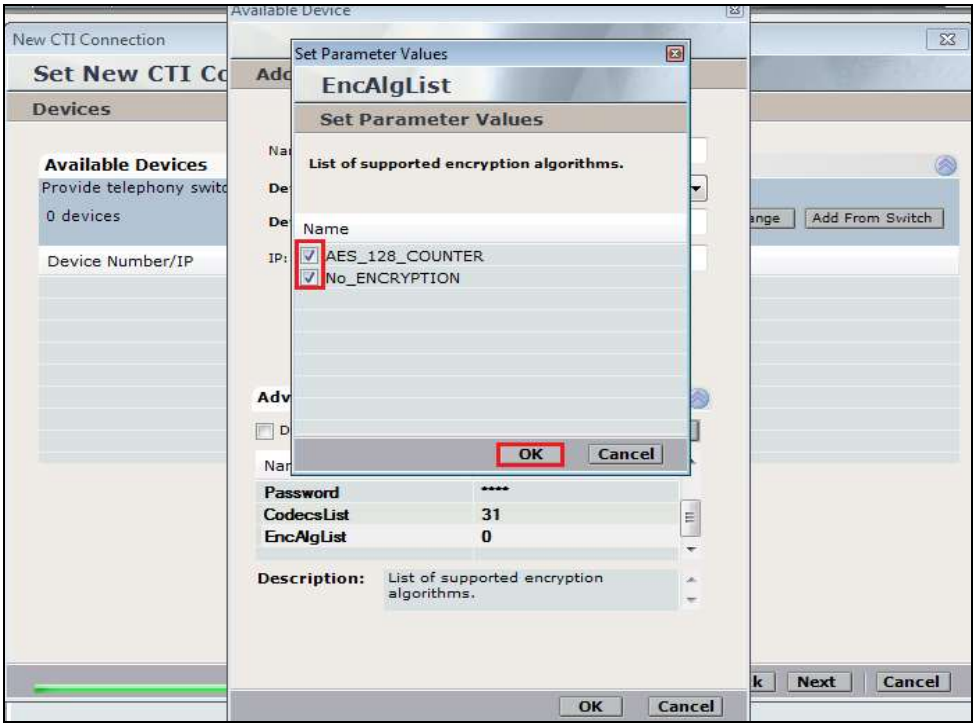
Enter the correct **Password** and note this is the password for the extension that is being added here. This is the station password which was entered during the creation of the station. A printout of an extension can be found in **Section 5.5** of these Application Notes.



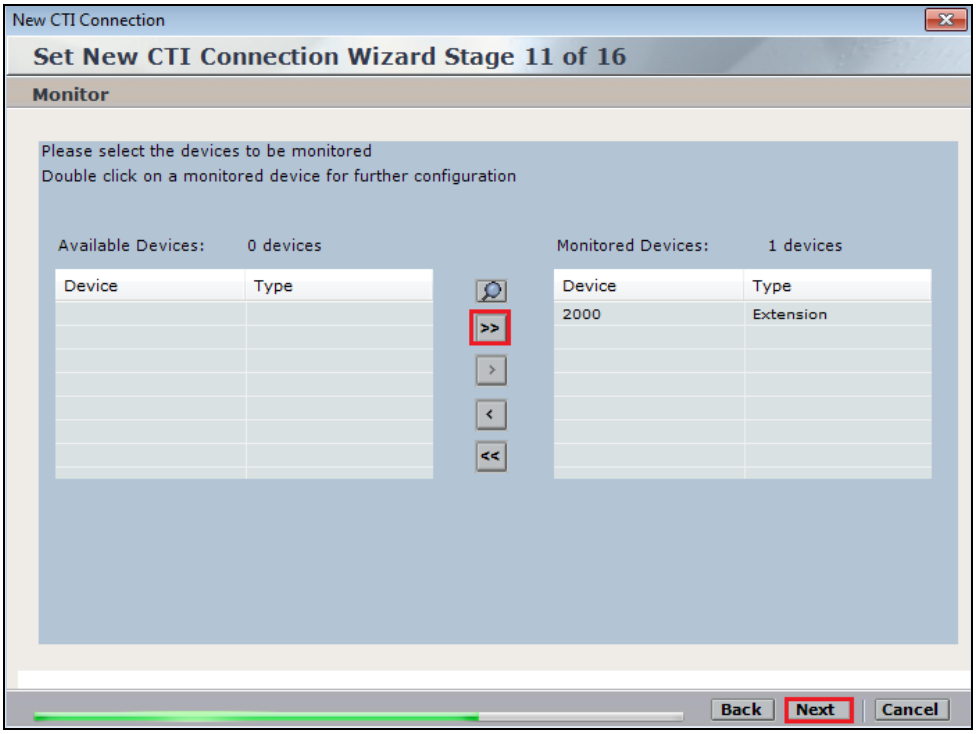
Double-click on **CodecsList** and ensure that all the values are ticked as shown below. Click on **OK** to continue.



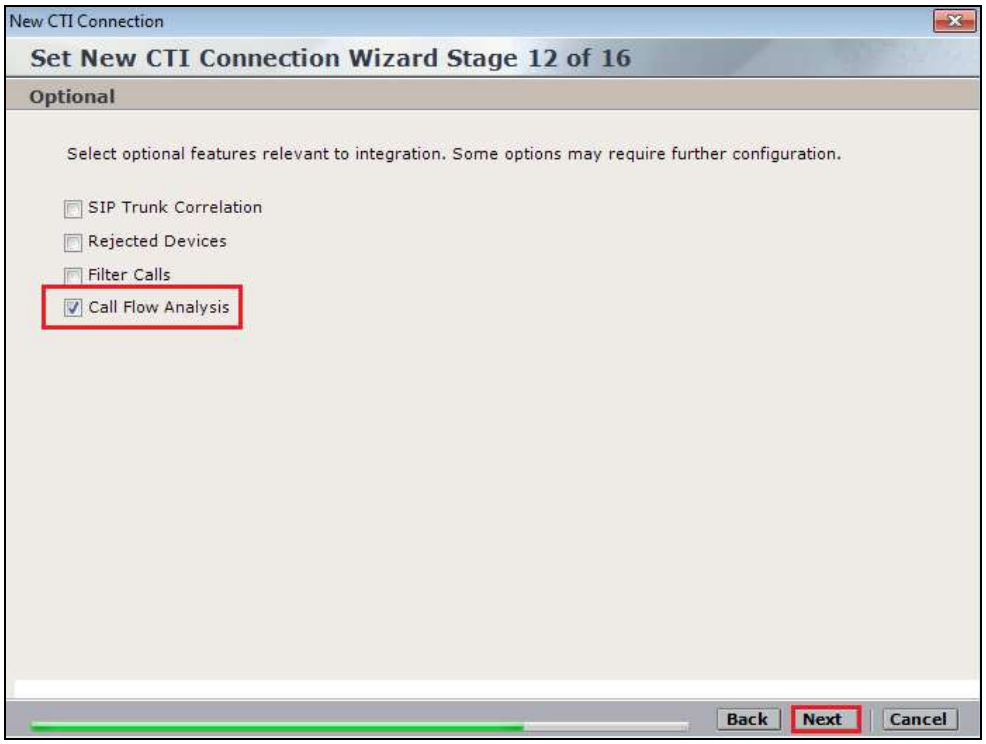
Double-click on **EncAlgList** and ensure both options are ticked as shown below. Click on **OK** to continue.



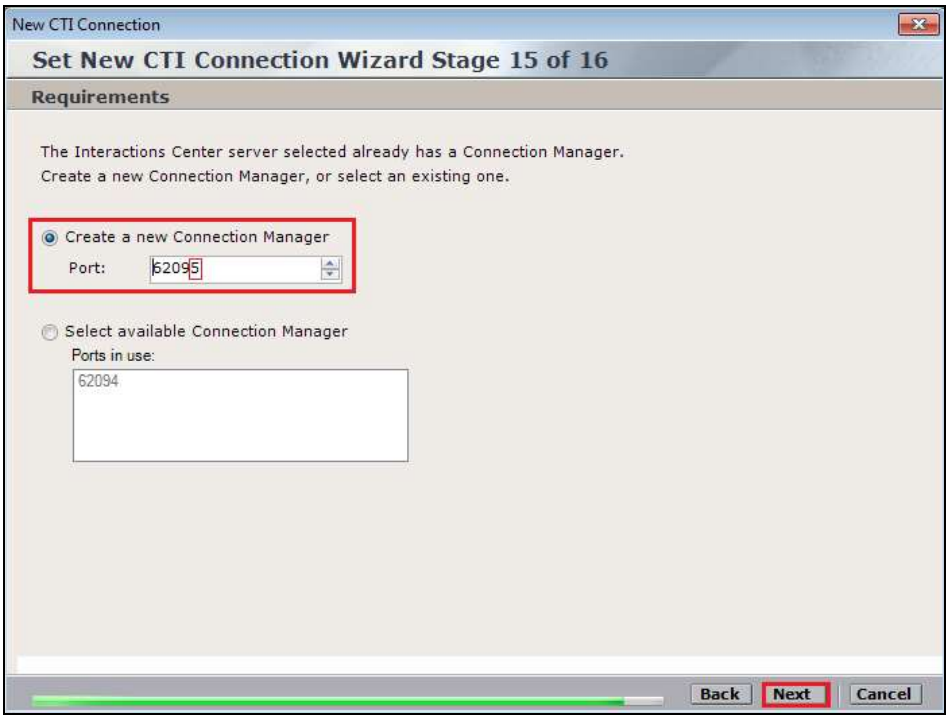
Select the new extension and click on the >> icon as shown. Click on **Next** to continue.



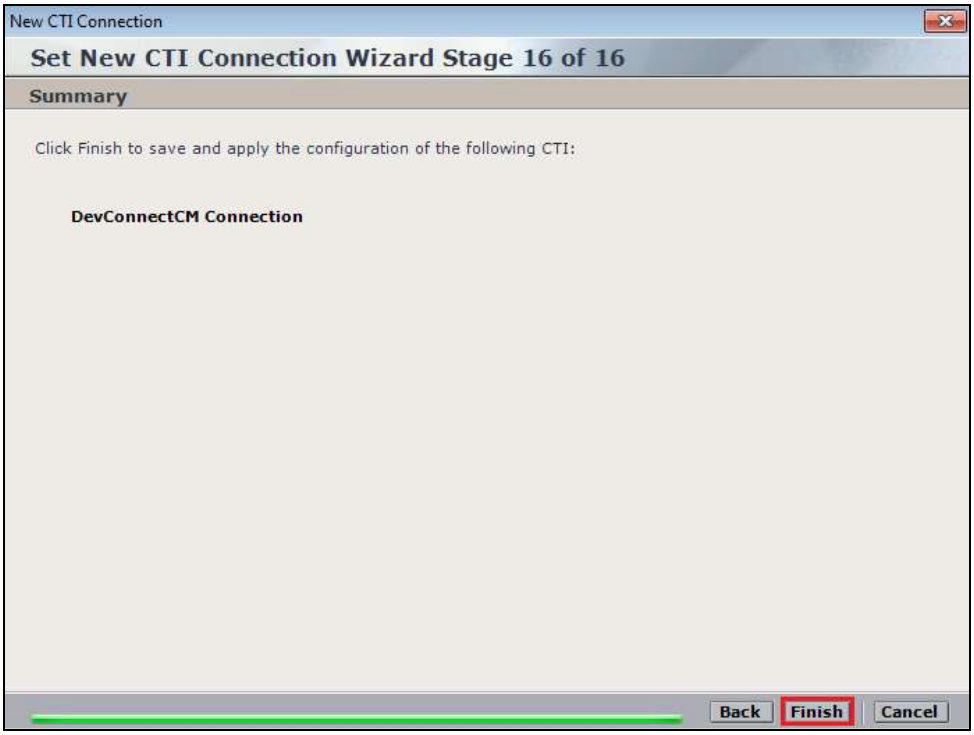
This is optional, but for better analysis tick on **Call Flow Analysis** and click on **Next** to continue.



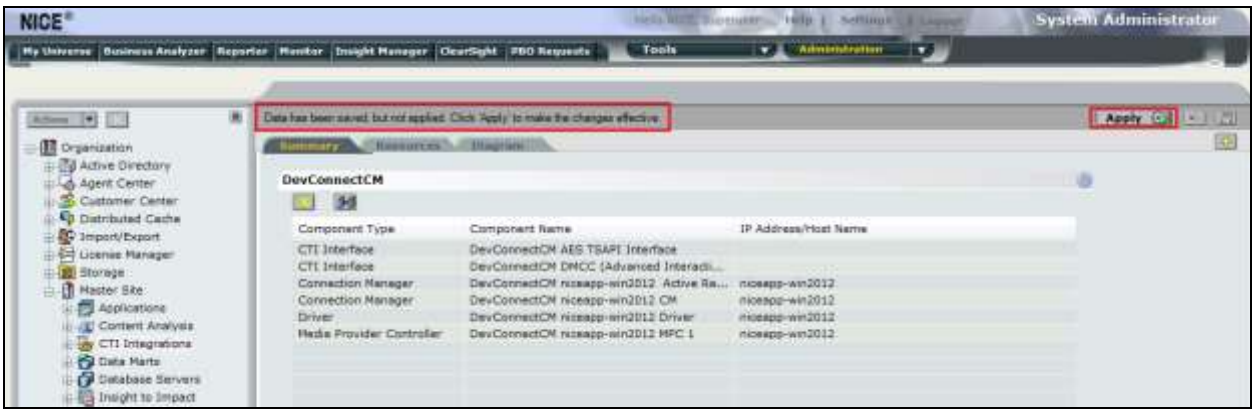
Select a different **Port** number as shown below **62095** is chosen simply because **62094** was already in use.



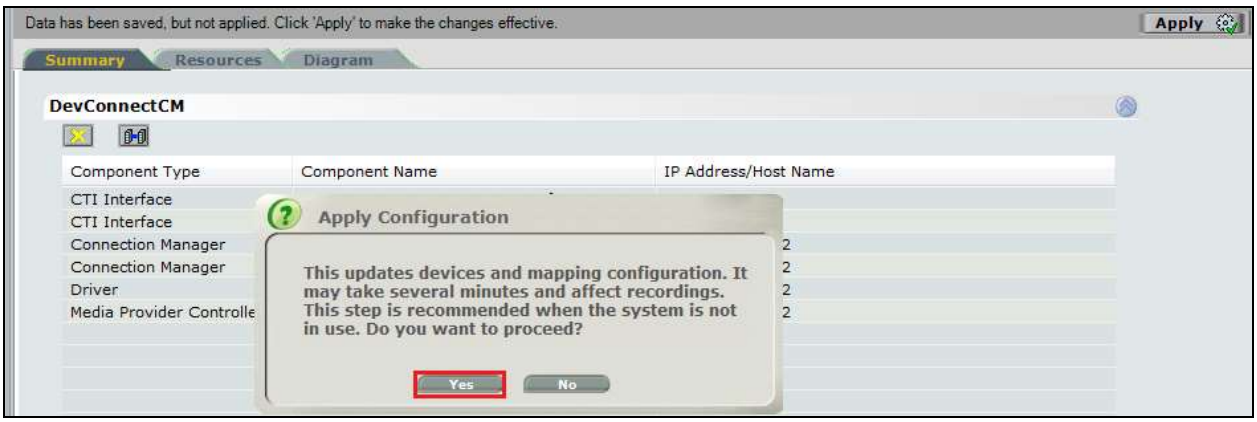
Click on **Finish** to complete the **New CTI Wizard**.



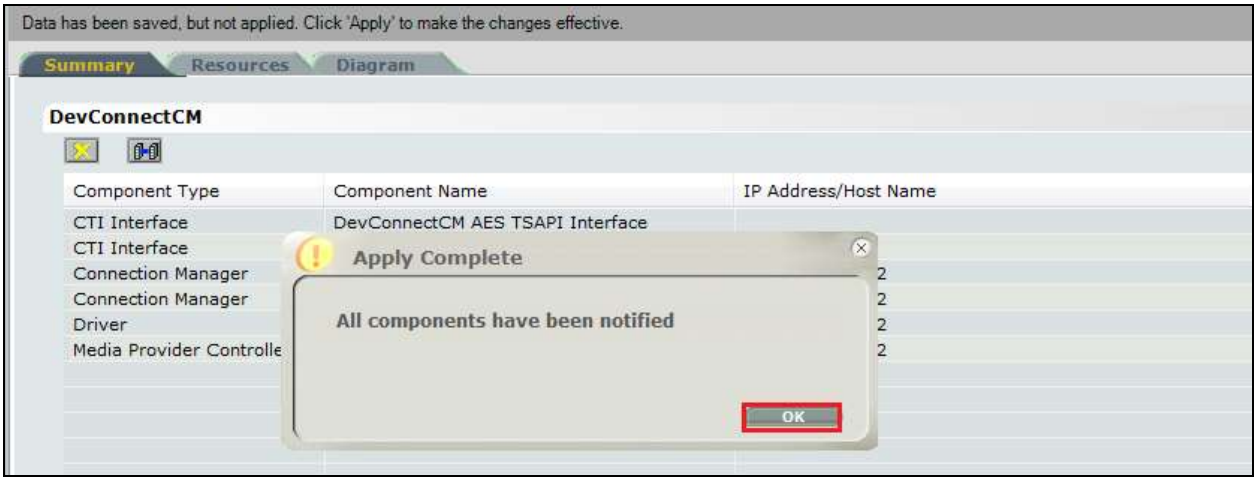
Click on **Apply** at the top right of the screen to save the new connection.



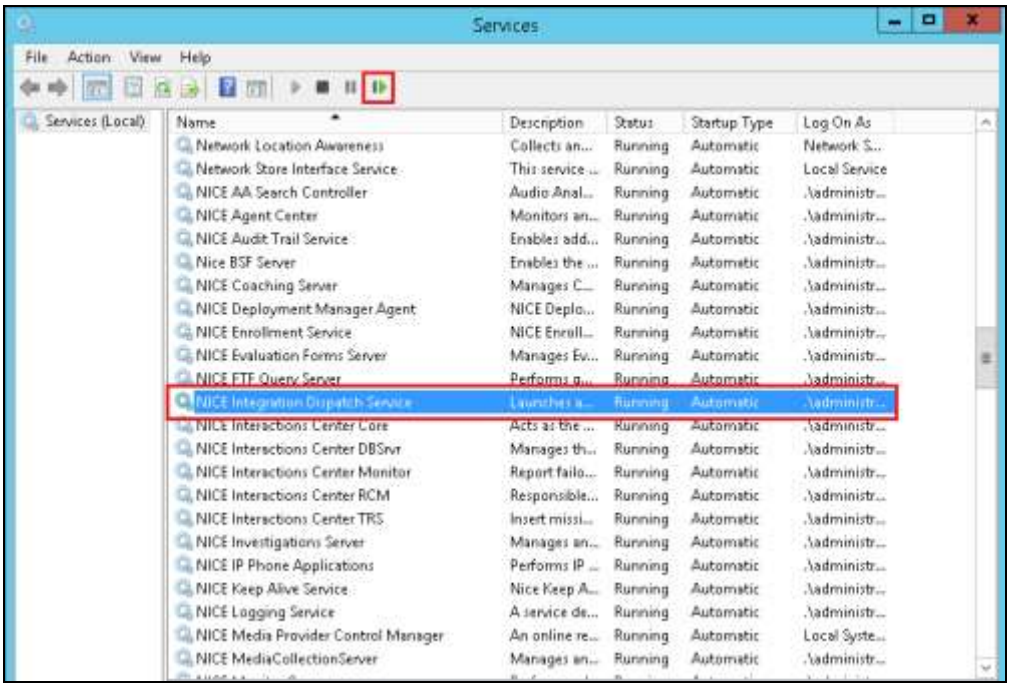
Click on **Yes** to proceed.



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

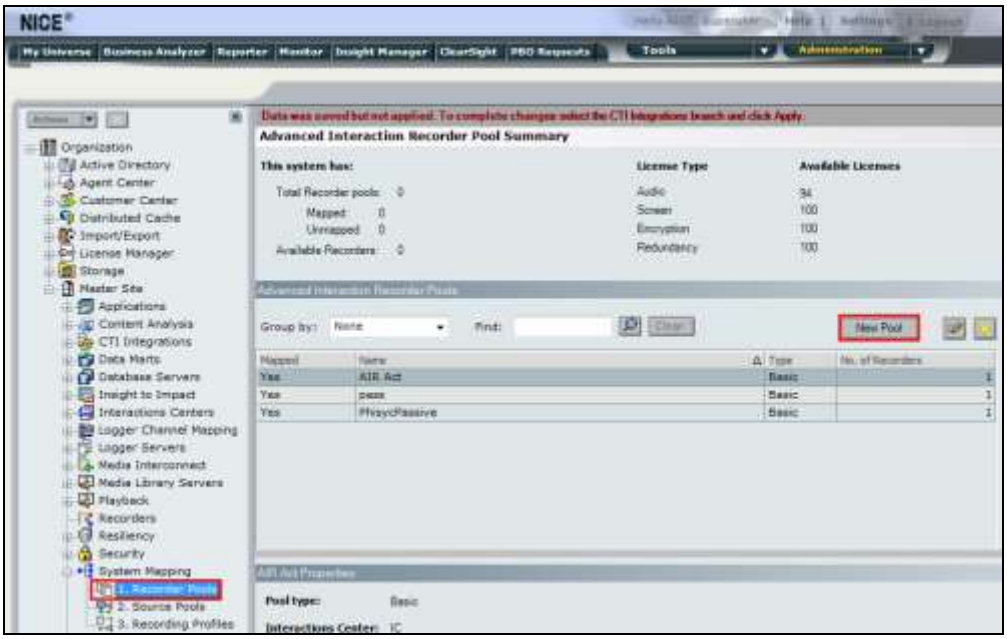


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

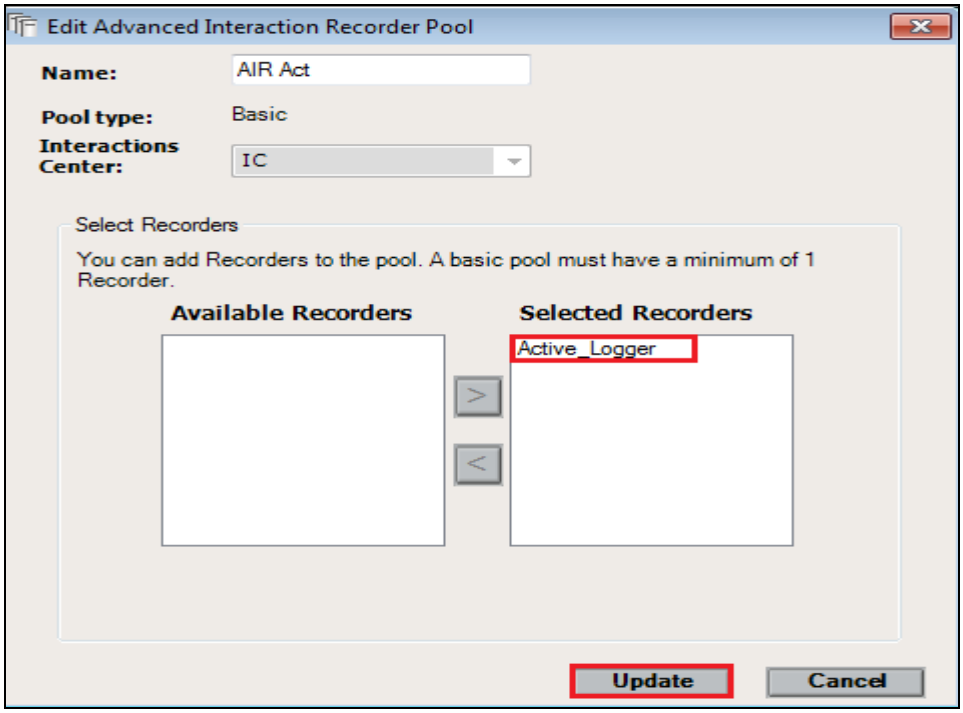


7.2. System Mapping

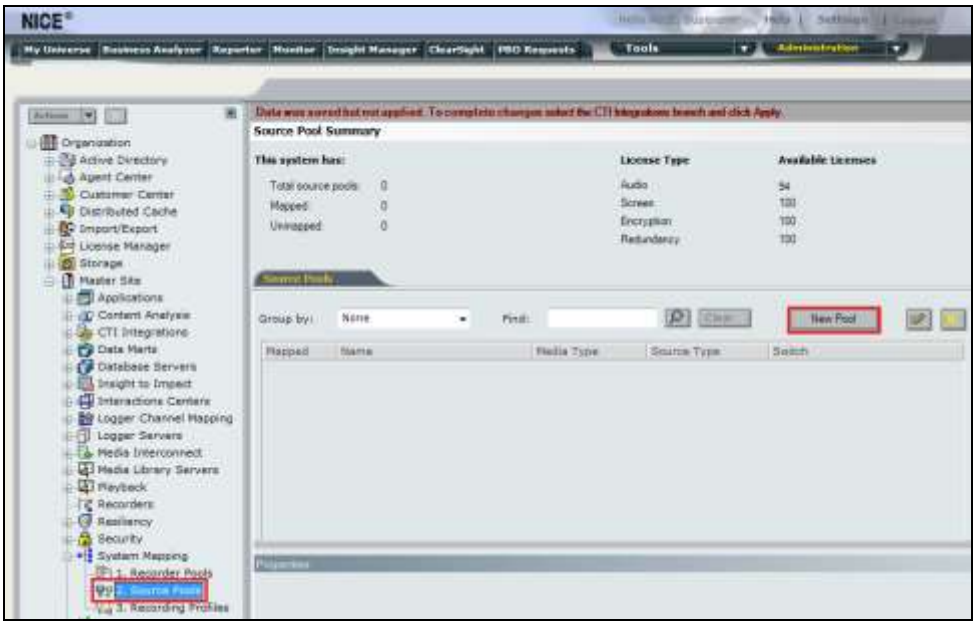
From the web browser navigate to **Master Site → System Mapping → Recorder Pools**. In the main window click on **New Pool**.



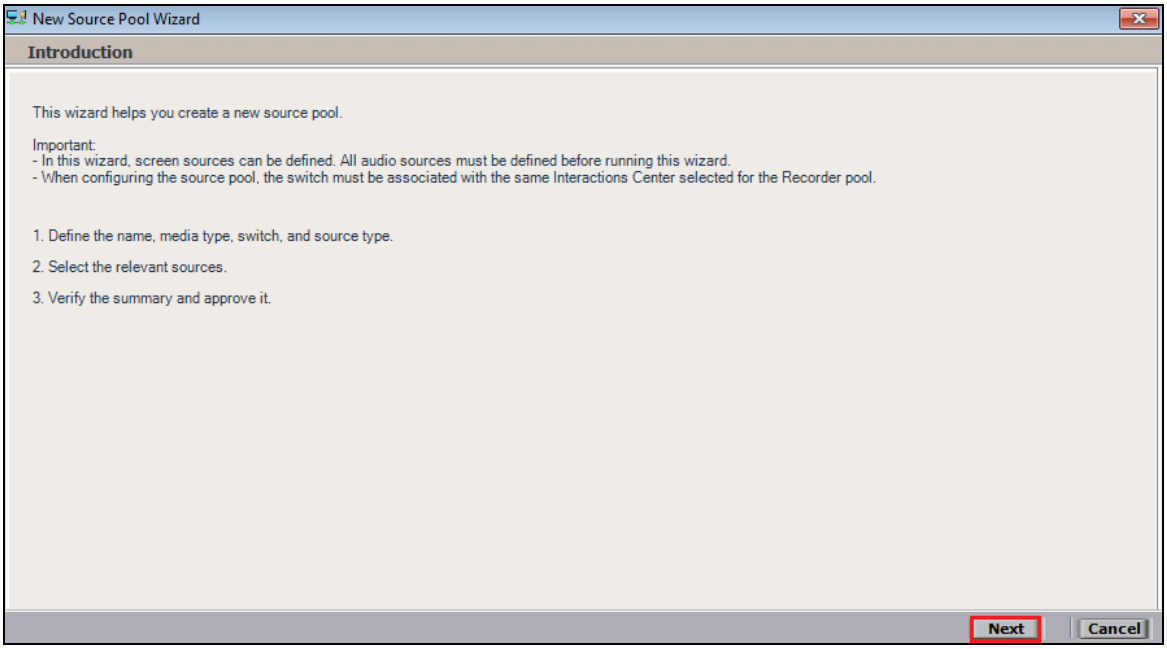
Enter a suitable **Name** for the **Recorder Pool** and select the **Active_Logger** from the list of **Available Recorders** and click on **Update** to continue.



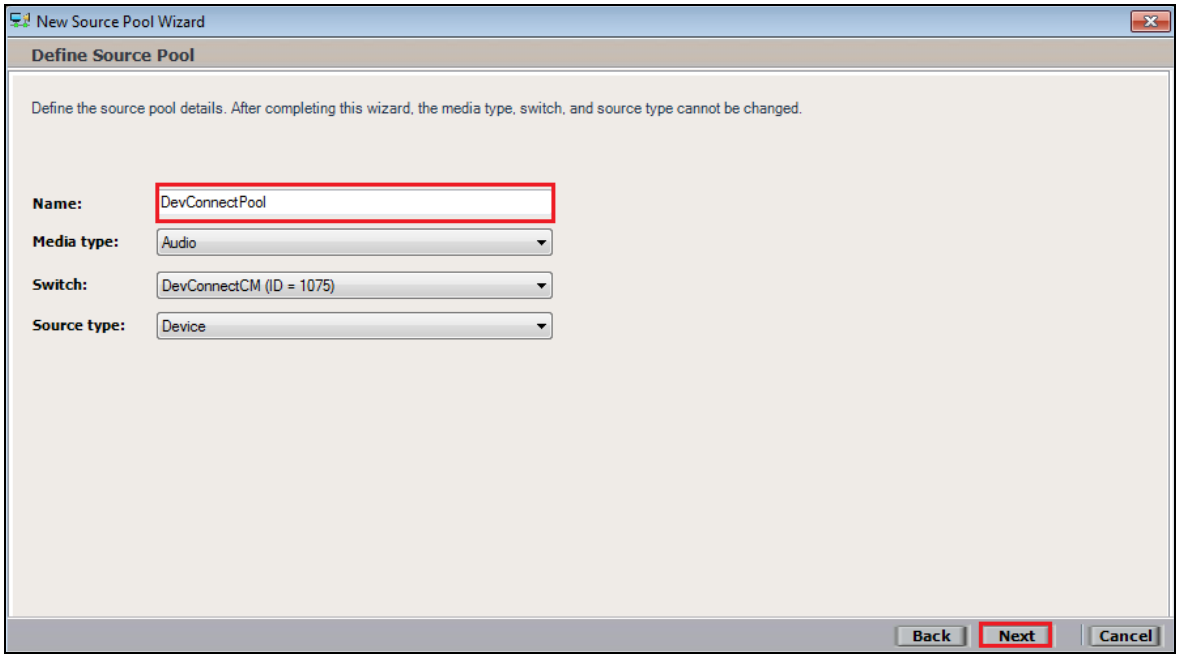
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



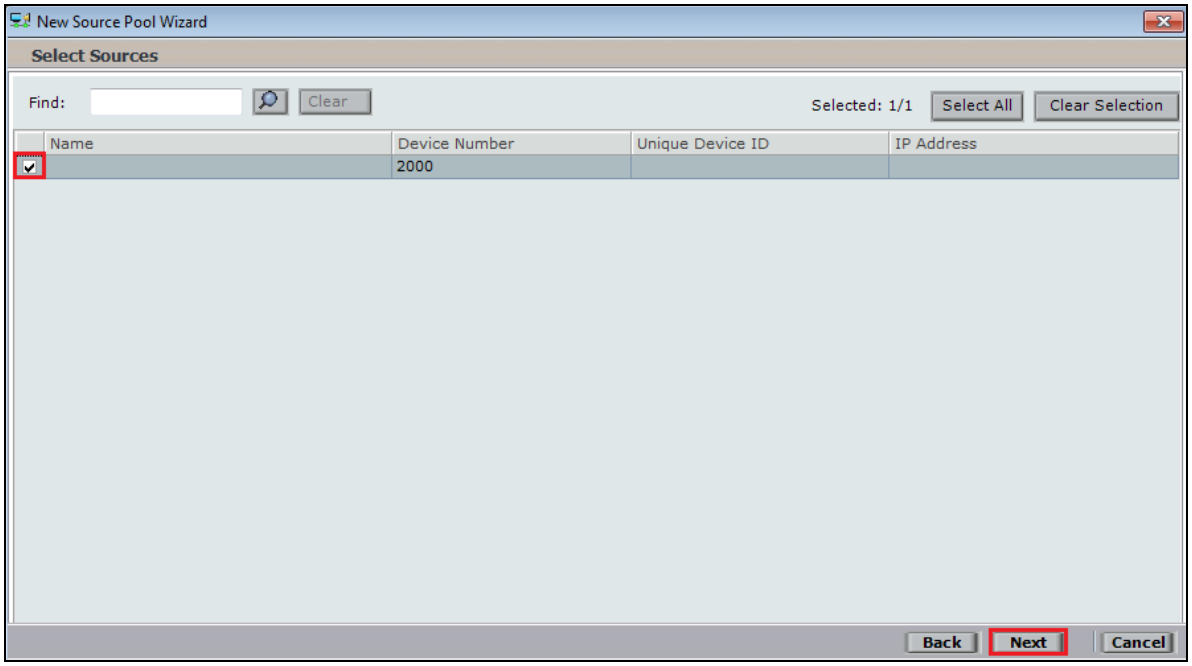
Click on **Next** to continue to add a new **Source Pool.**



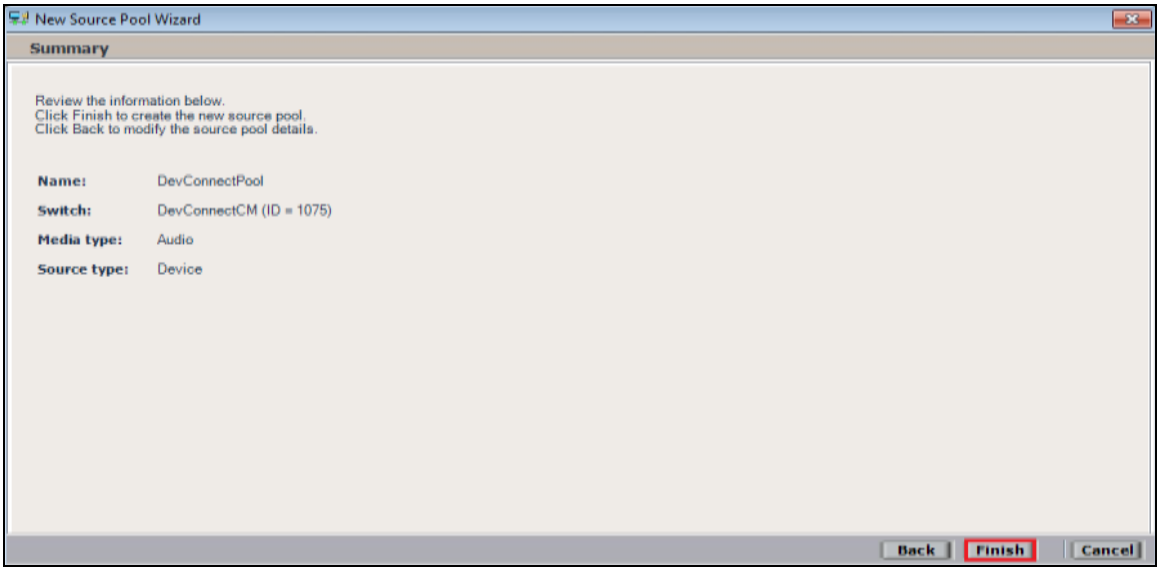
Enter a suitable **Name** and the other values were left as default. Click on **Next** to continue.



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

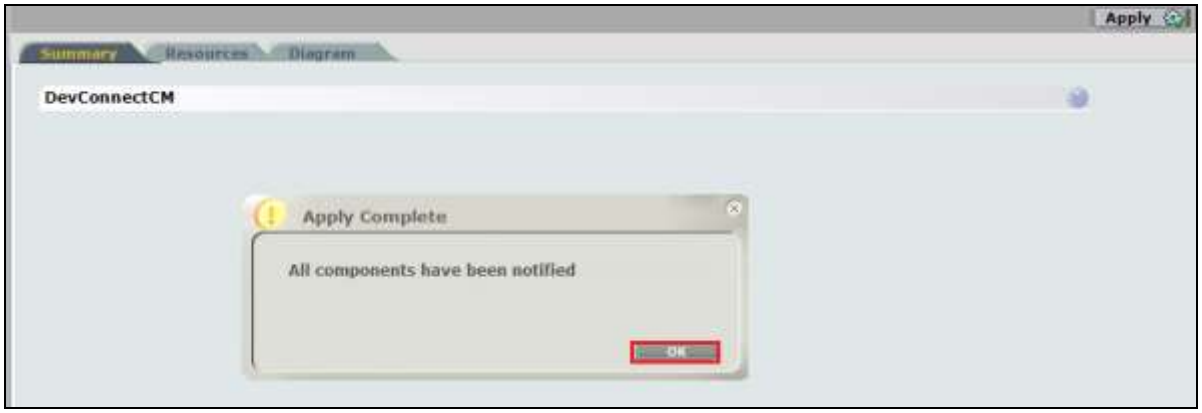


Click on **Finish** to complete the **New Source Pool Wizard**.

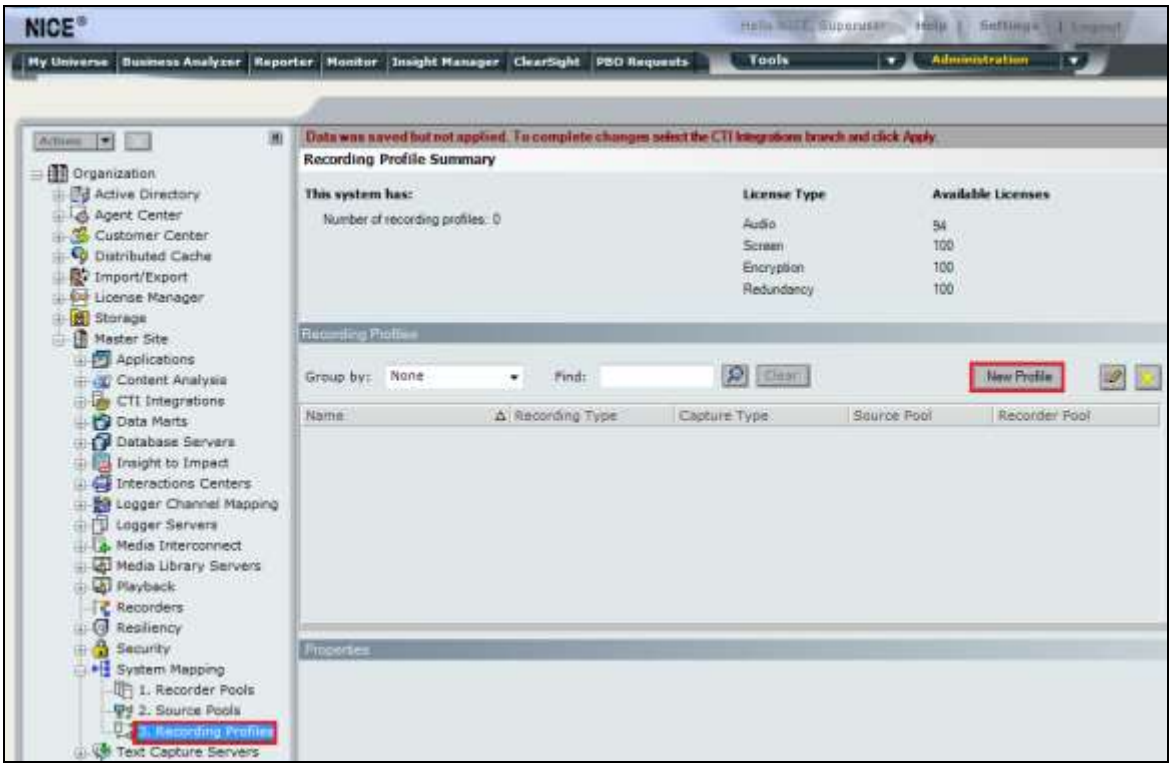


To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.

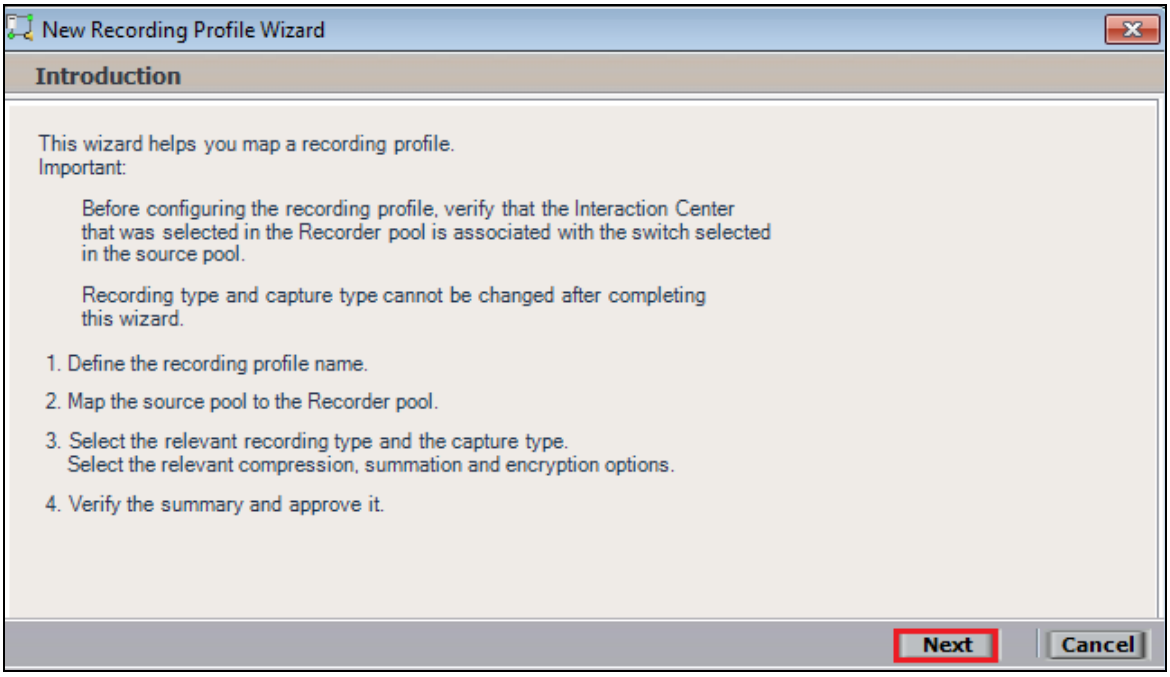
The following screen shows the changes were saved correctly. Click on **OK** to continue.



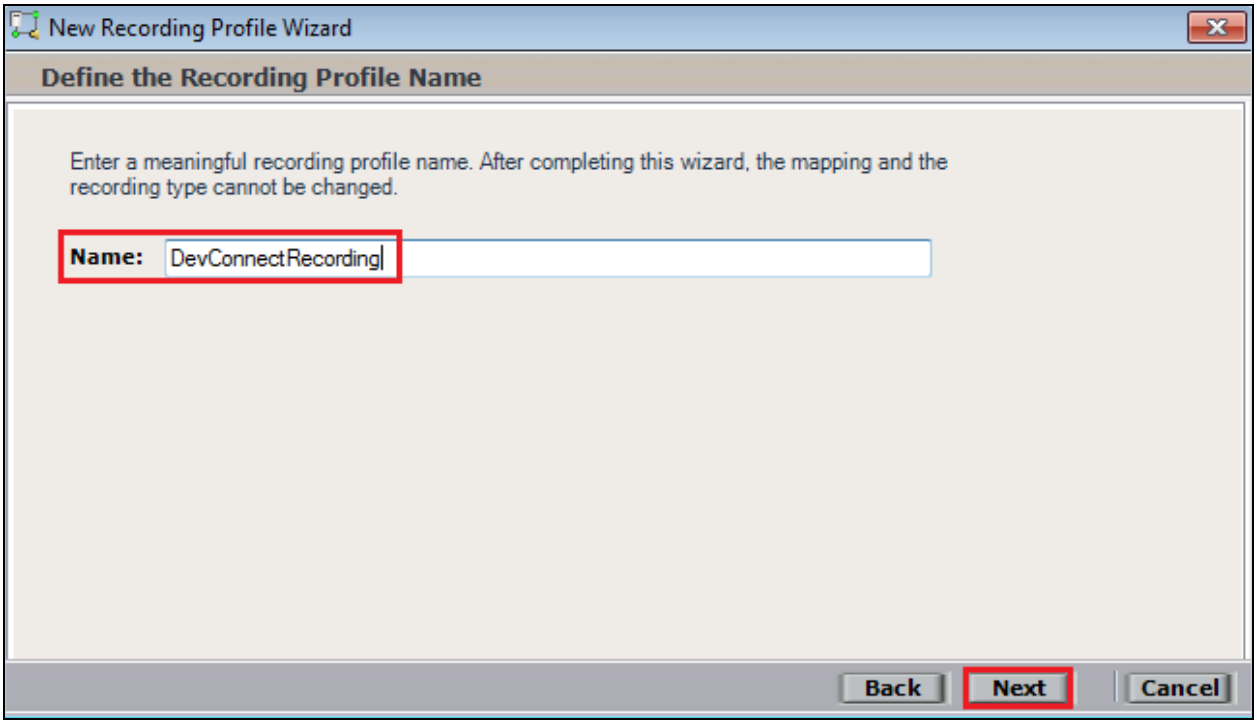
From the left window navigate to **Master Site → System Mapping → Recording Profiles** and in the main window click on **New Profile**.



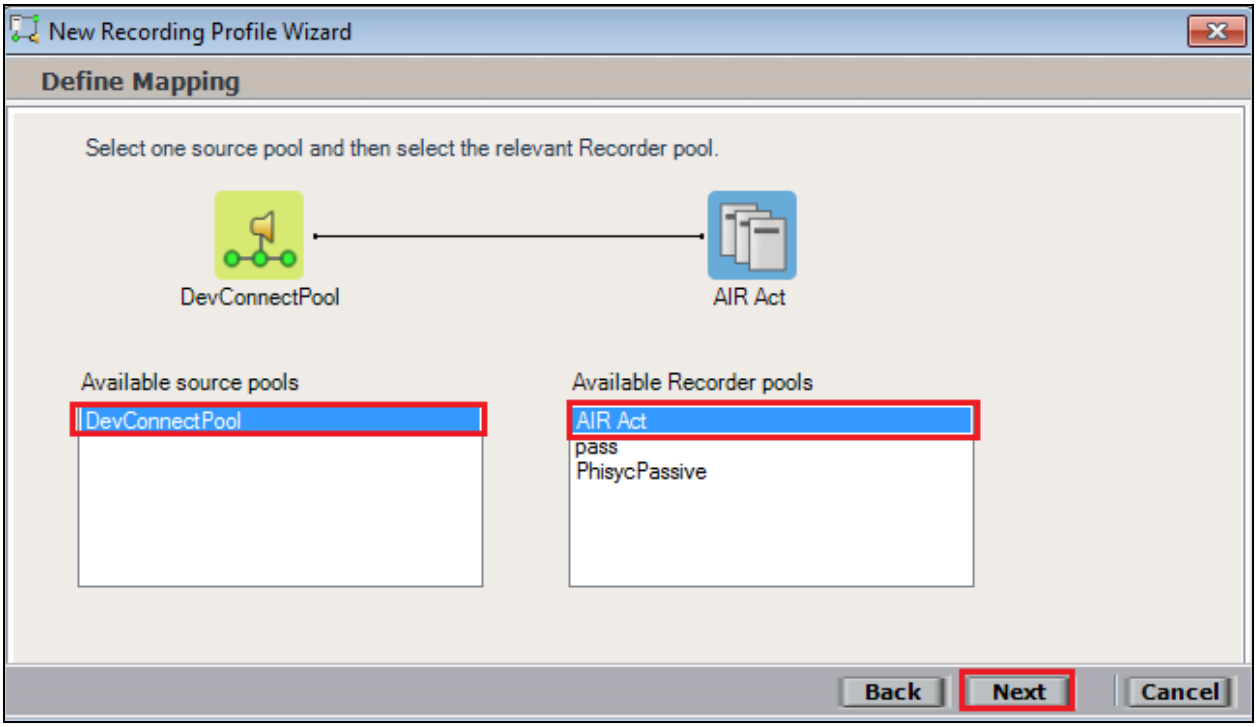
Click on **Next** to continue with the **New Recording Profile Wizard**.



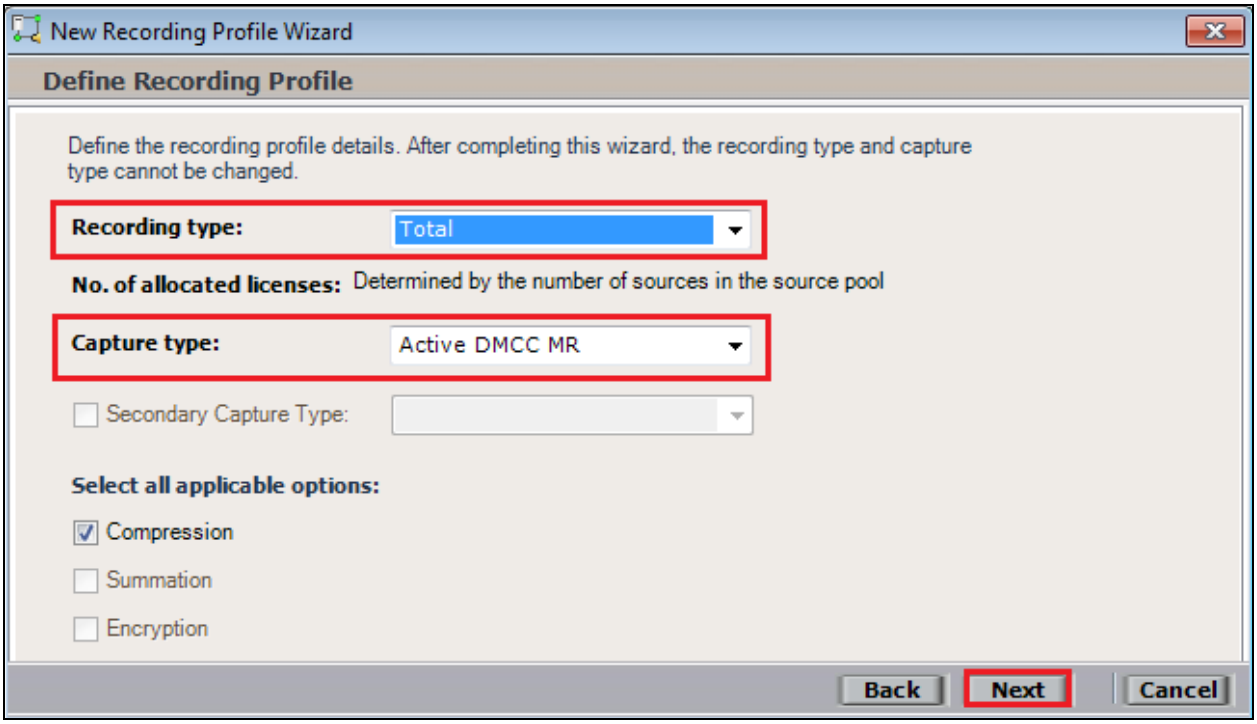
Enter a suitable **Name** for the Recording profile.



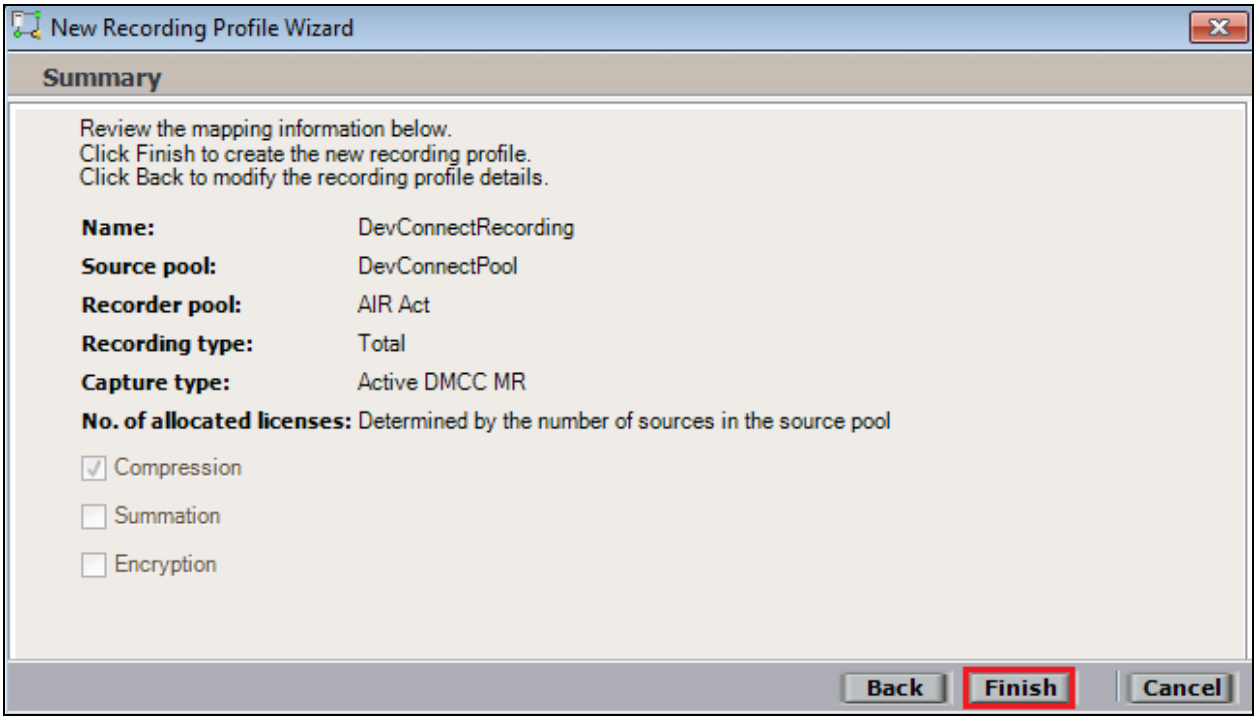
Select the correct **source pool** and **Recorder pool**, then click **Next** to continue.



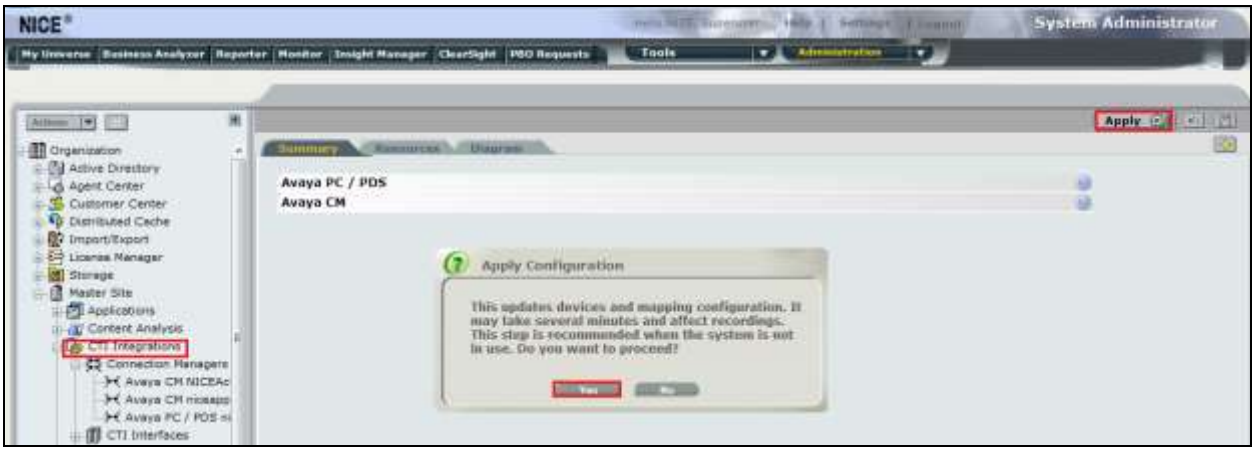
For total recording i.e., the recording of all calls, select **Total** as the **Recording type**. For **Capture type** ensure that **Active DMCC MR** is selected from the drop-down box. Compression is selected as default and can be left like this. Click on **Next** to continue.



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



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.

8. Verification Steps

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

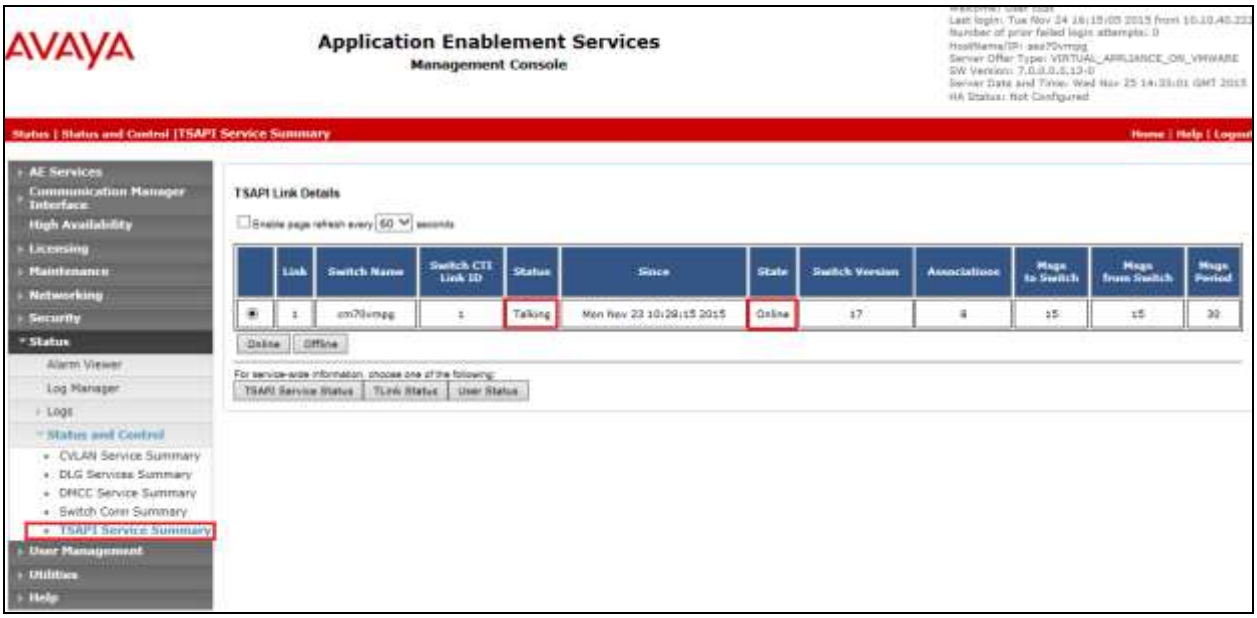
8.1. Verify Avaya Aura® Communication Manager CTI Service State

Before checking the connection between the NICE Engage Platform and AES, check the connection between Communication Manager and AES to ensure it is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI    Version      Mnt    AE Services      Service       Msgs      Msgs
Link                Busy     Server          State        Sent      Rcvd

1          5        no      aes70vmpg      established    18        18
```

8.2. Verify TSAPI Link

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



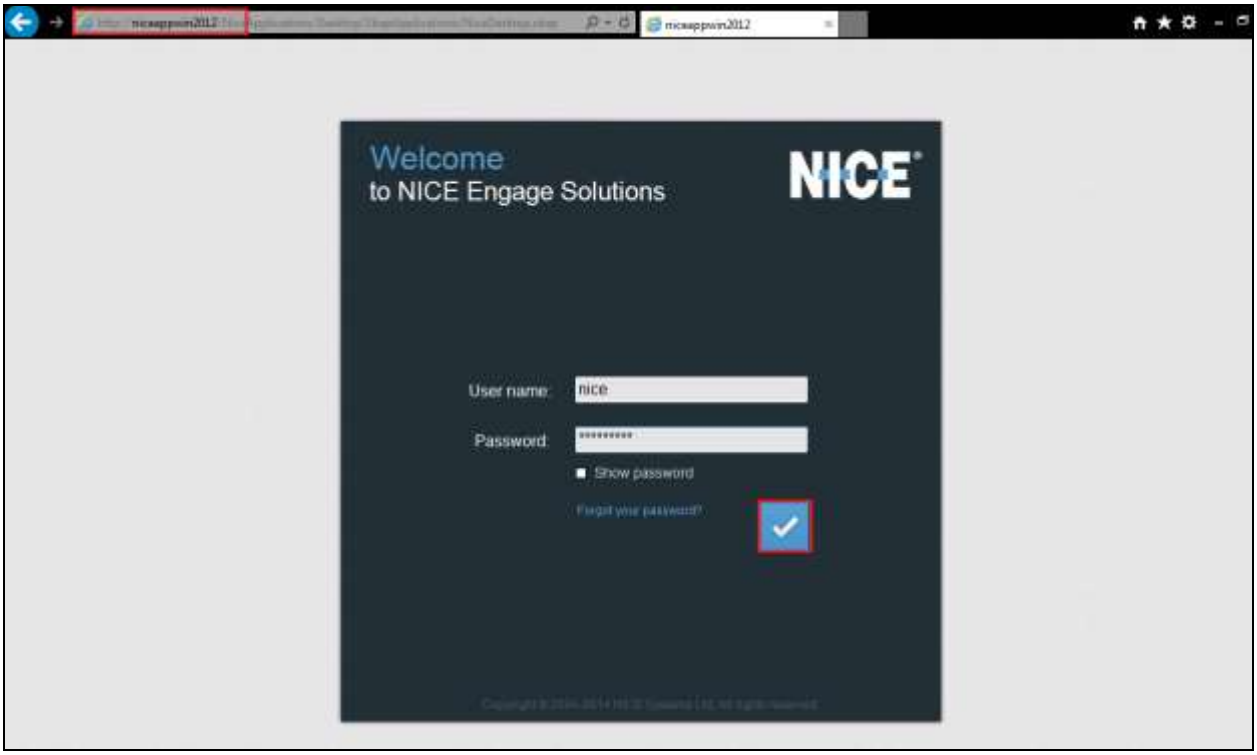
8.3. Verify DMCC link on AES

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** to display the **DMCC Service Summary – Session Summary** screen. The screen below shows that the user **NICE** is connected from the IP address **10.10.40.126**, which is the NICE Application server.

8.4. Verify calls are being recorded

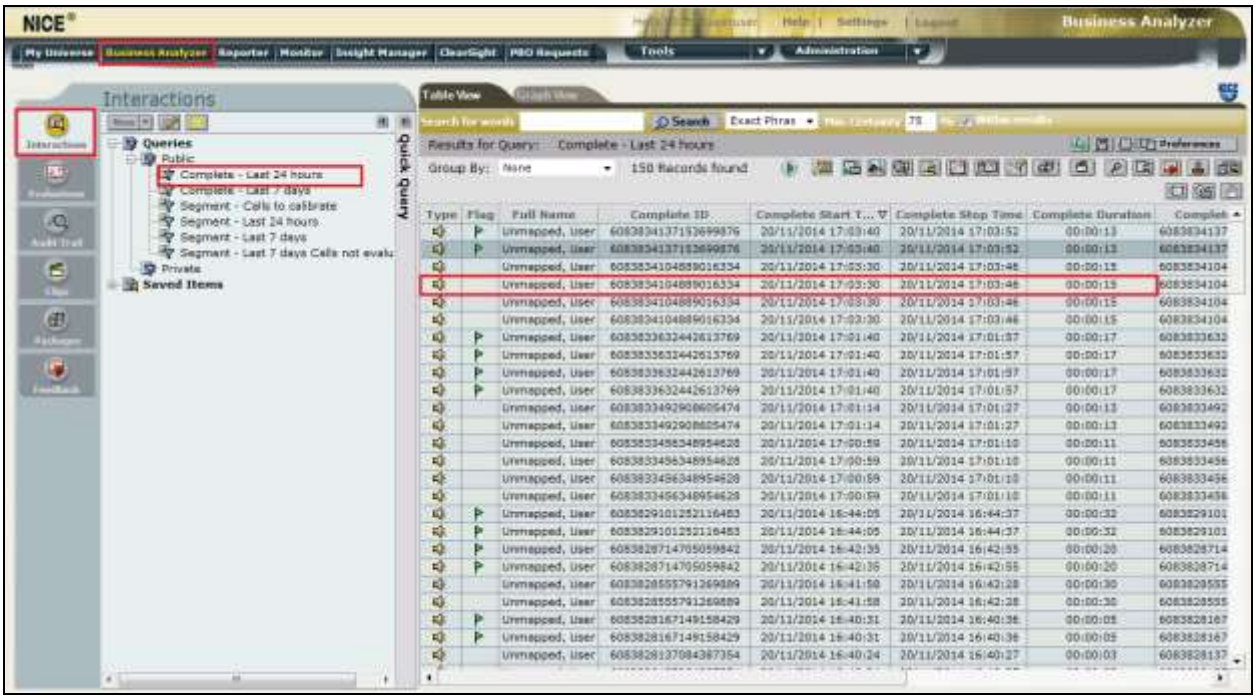
From any of the monitored Avaya endpoints make a series of inbound and outbound calls. Once these calls are completed they should be available for playback through a web browser to the NICE Application Server.

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

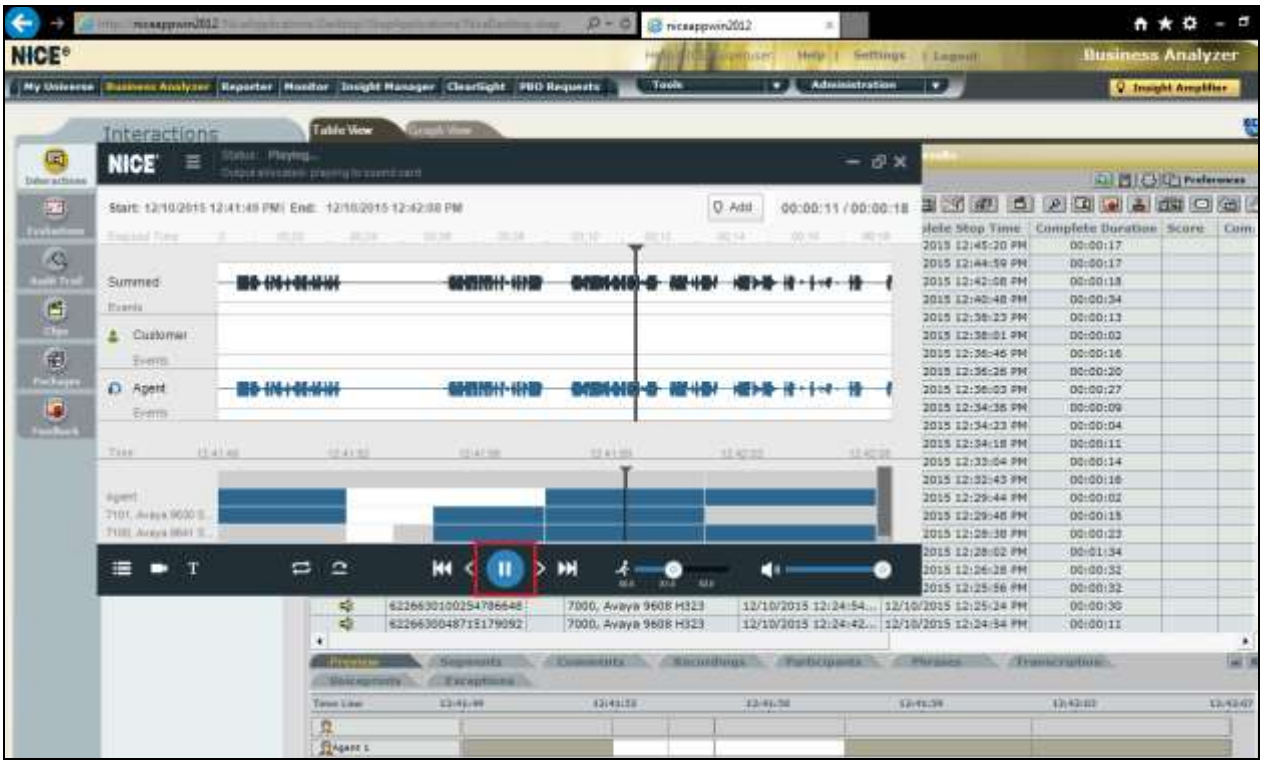


Click on **Business Analyser** at the top of the screen. Select **Interactions** from the left window and then navigate to **Queries → Public**.

Click on **Complete – Last 24 hours**. This should reveal all the recordings that took place over the previous 24 hours. Select the required recording from the list and double-click on this to play the recording.

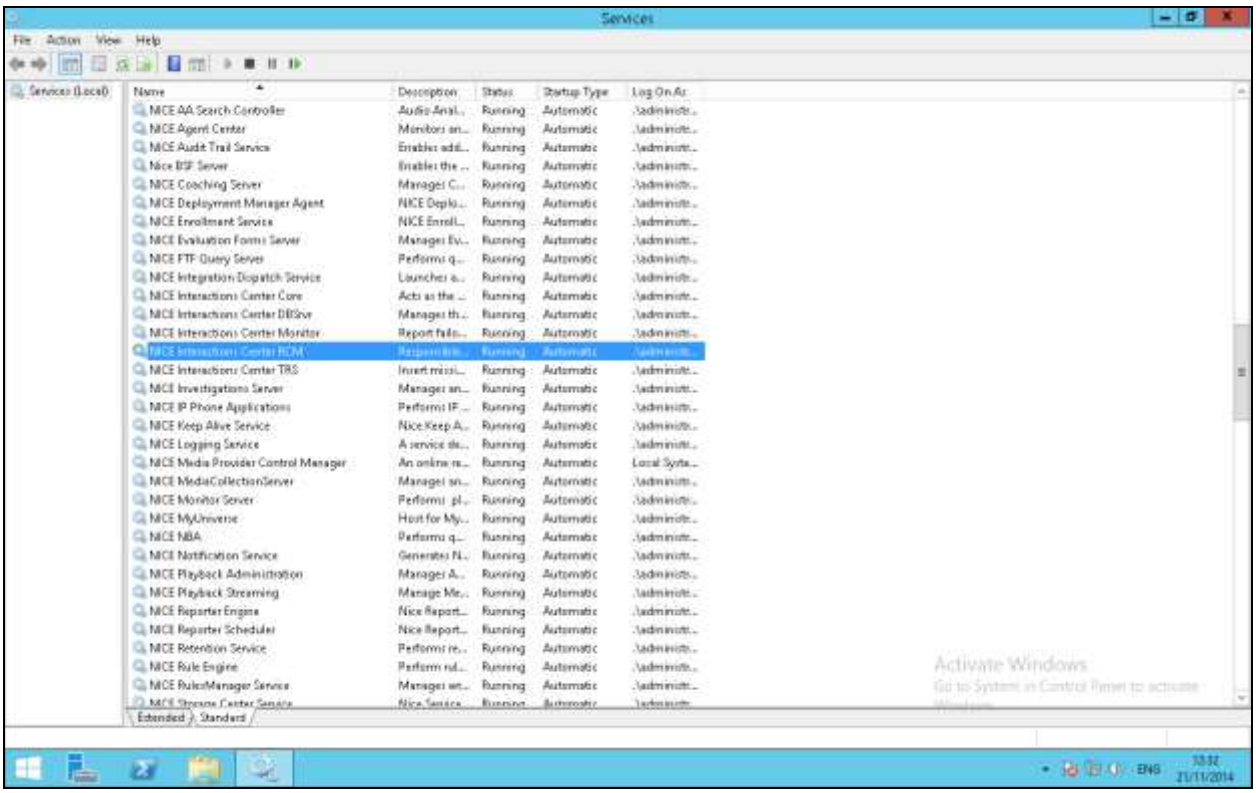


The NICE player is opened and the recording is presented for playback. Click on the **Play/Pause** icon highlighted below to play back the recording.



8.5. 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.



9. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0 to connect to using 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**.

10. Additional References

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

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

[1] *Administering Avaya Aura® Communication Manager,* Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 7.0

[4] *Avaya Aura® Session Manager Overview*, Doc *# 03603323Avaya Aura ® Contact Centre SIP Commissioning*, Doc # NN44400-511, Release 7.0

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

Appendix

Avaya one-X® Agent Softphone

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

```
display station 2100                                            Page   1 of   5
                                     STATION

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

                                              IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                             Customizable Labels? Y
```

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

```
display station 2100                                          Page   3 of   5
                                     STATION

             Conf/Trans on Primary Appearance? n
   Bridged Appearance Origination Restriction? n


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

                              ENHANCED CALL FORWARDING
                                     Forwarded Destination         Active
 Unconditional For Internal Calls To: 1000                            n
                   External Calls To: 1000                            n
          Busy For Internal Calls To:                                 n
                   External Calls To:                                 n
      No Reply For Internal Calls To:                                 n
                   External Calls To:                                 n

            SAC/CF Override: n
```

```
display station 2100                                          Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                       Cord Length: 0
   Building:                                         Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5: manual-in          Grp:
 2: call-appr                            6: after-call         Grp:
 3: call-appr                            7: aux-work    RC:    Grp:
 4: auto-in            Grp:              8:

    voice-mail
```

Avaya 9608 H.323 Deskphone

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

```
display station 2000                                            Page   1 of   5
                                     STATION

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

                                              IP Video Softphone? n
                              Short/Prefixed Registration Allowed: yes

                                             Customizable Labels? y
```

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

```
display station 2000                                          Page   3 of   5
                                     STATION

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

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

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

            SAC/CF Override: n
```

```
display station 2000                                          Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                        Cord Length: 0
   Building:                                          Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




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

    voice-mail
```

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.