Avaya Solution & Interoperability Test Lab

Application Notes for configuring NICE Engage Platform R6.3 to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 using Passive Station Side VoIP with SMS - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the NICE Engage Platform to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R6.3, an Avaya Aura® Session Manager R6.3, and Avaya Aura® Application Enablement Services R6.3 using Passive Station Side VoIP with SMS.

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

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

1. Introduction

These Application Notes describe the configuration steps for the NICE Engage Platform R6.3 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R6.3, an Avaya Aura® Session Manager R6.3 and Avaya Aura® Application Enablement Services R6.3. The NICE Engage Platform was setup to use passive station-side VoIP recording with SMS to record both internal and external calls on various Communication Manager endpoints, listed in **Section 4**.

Passive Station-Side VoIP Recording (passive recording) uses port mirroring to record the RTP from each phones set. All phone sets that are to be recorded are plugged into the Avaya 4548GT-PWR layer 3 switch where all of these particular ports are mirrored to one port where the NICE Advanced Interactions server is plugged into. All of the RTP information from all of these phone sets will be delivered to the sniffer port on the NICE Advanced Interactions server. An additional Network Interface Card (NIC) is therefore required on the NICE Advanced Interactions Server. This NIC is not configured to access the IP stack. It will have no IP configuration. This NIC connects into the mirrored port network that allows access to the phone network connection. This is effectively a hub environment. The promiscuous port needs to be on the same physical media path as any telephone endpoint that it is going to record.

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

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

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the NICE Engage Platform to carry out call recording in a variety of scenarios using passive recording with AES and Communication Manager. A range of Avaya endpoints were used in the compliance testing all of which are listed in **Section 4**.

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

2.1. Interoperability Compliance Testing

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

- **Inbound calls** – Test call recording for inbound calls to the Communication Manager from PSTN callers.
- **Outbound calls** – Test call recording for outbound calls from the Communication Manager to PSTN callers.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **EC500 Calls/Forwarded calls -** Test call recording for calls terminated on Avaya DECT handsets using EC500.
- **Call Park/Call Pickup** Test call recording for calls that are parked or picked up using Call Park and Call Pickup.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into one-X® Agent.
- **Failover testing -** The behaviour of NICE Engage Platform under different simulated failure conditions on the Avaya platform will also be observed.

2.2. Test Results

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

Observations:

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

2.3. Support

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

3. Reference Configuration

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

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

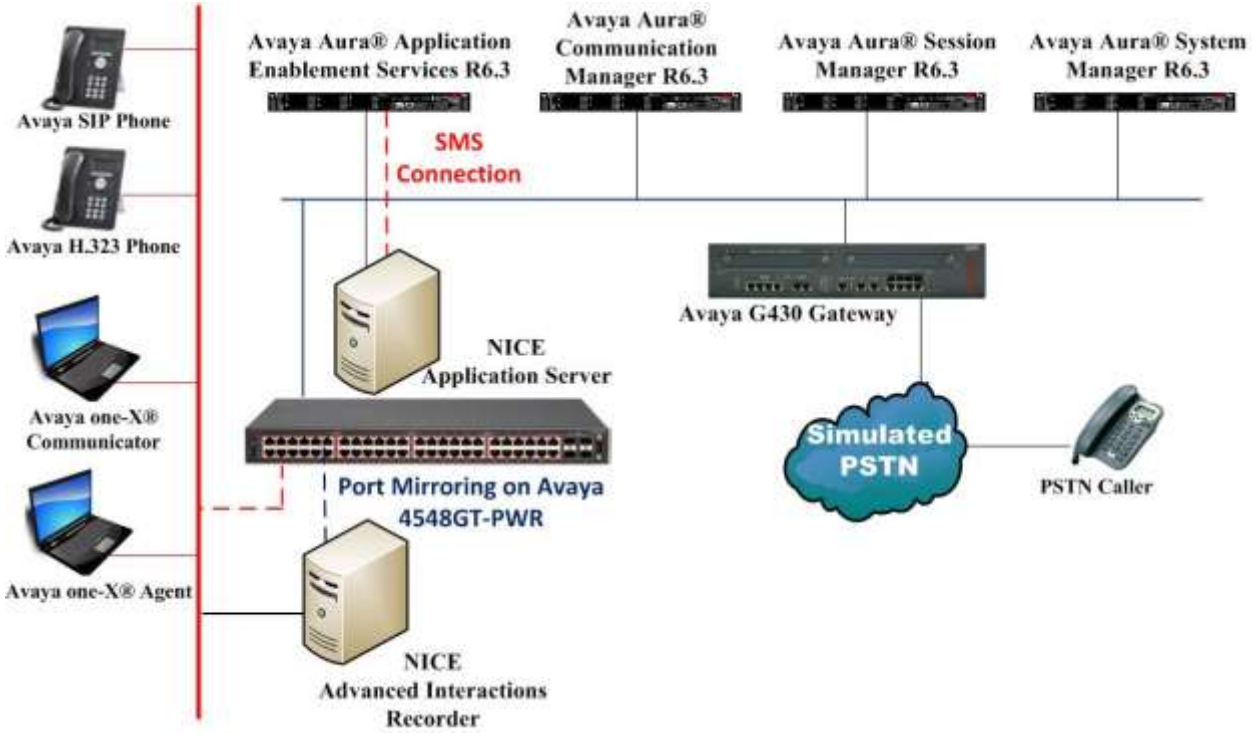


Figure 1: Connection of NICE Engage Platform R6.3 with Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3 and Avaya Aura® Application Enablement Services R6.3

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Virtual Server	R6.3.10 [Build 6.3.0.8.5682-6.3.8.4514] [SW Update Rev 6.3.10.7.2656]
Avaya Aura® Session Manager running on Virtual Server	R6.3 (SP9) 6.3.9.0.639011
Avaya Aura® Communication Manager running on Virtual Server	R6.3 SP8 R016x.03.0.124.0 03.0.124.0-21588
Avaya Aura® Application Enablement Services running on Virtual Server	R6.3 Build No – 6.3.3.1.10-0
Avaya G430 Gateway	33.12.0 /1
Avaya 4548GT-PWR Ethernet Switch	Boot Image: ver. 5.0.0.9 Diag Image: ver. 5.1.0.8 Agent Image: ver. 5.7.0.009
Avaya 9608 H323 Deskphone	96xx H.323 Release 6.4014U
Avaya 9620 H323 Deskphone	R3.186A
Avaya 9641 SIP Deskphone	96x1-IPT-SIP-R6_4_1-081114
Avaya 9630 SIP Deskphone	R2.6.12.1
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Avaya one-X® Communicator SIP	R6.2.4.07-FP4
Avaya one-X® Agent	R 2.5.50022.0
NICE Engage Platform - NICE Application Server - Advanced Interactions Recorder - NICE NDM Server	R6.3

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify System Features

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

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

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                  ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  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 (**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       Password          Enabled    Status
                   Server
      1:        aes63vmpg         ********          y          idle
      2:
      3:
```

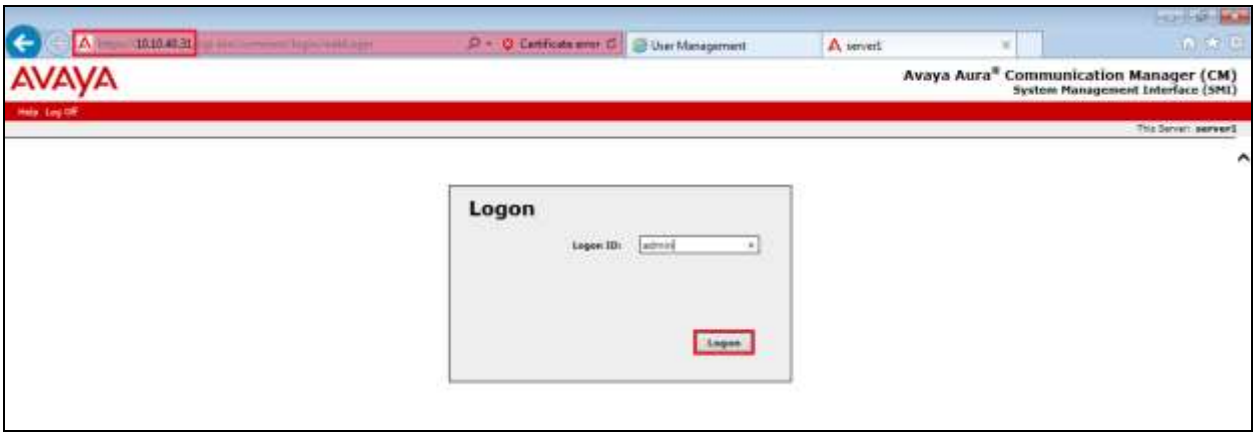
5.4. Configure CTI Link for TSAPI Service

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

```
add    cti-link 1                                           Page   1 of   3
                                     CTI LINK
 CTI Link: 1
Extension: 2002
     Type: ADJ-IP
                                                                  COR: 1
     Name: aes63vmpg
```

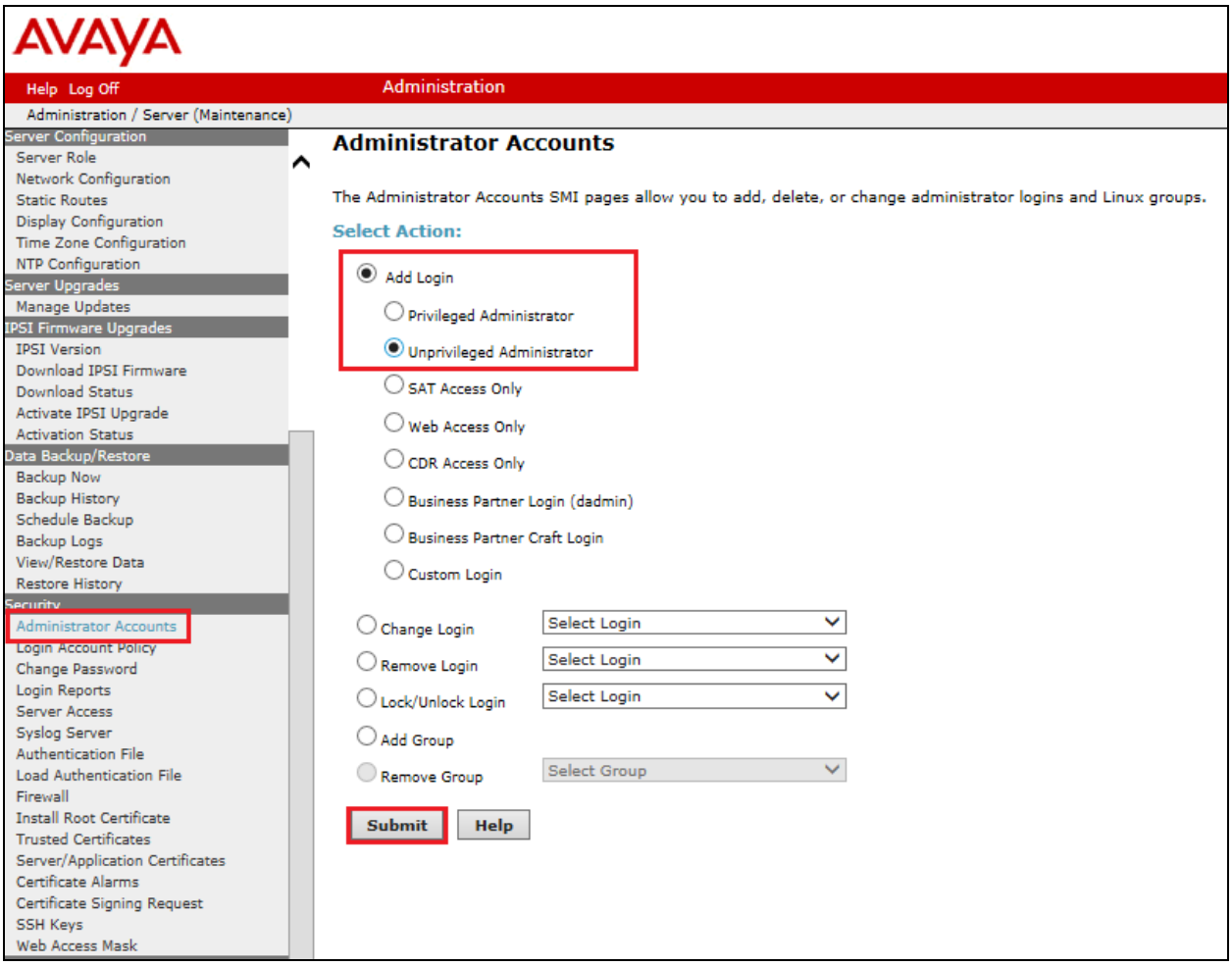
5.5. Configure System Management Service user on Avaya Aura® Communication Manager

This user is created specifically for the SMS connection that NICE utilise for this specific type of call recording. Using a web browser navigate to the Communication Manager IP Address. Enter the proper credentials and click on Logon.

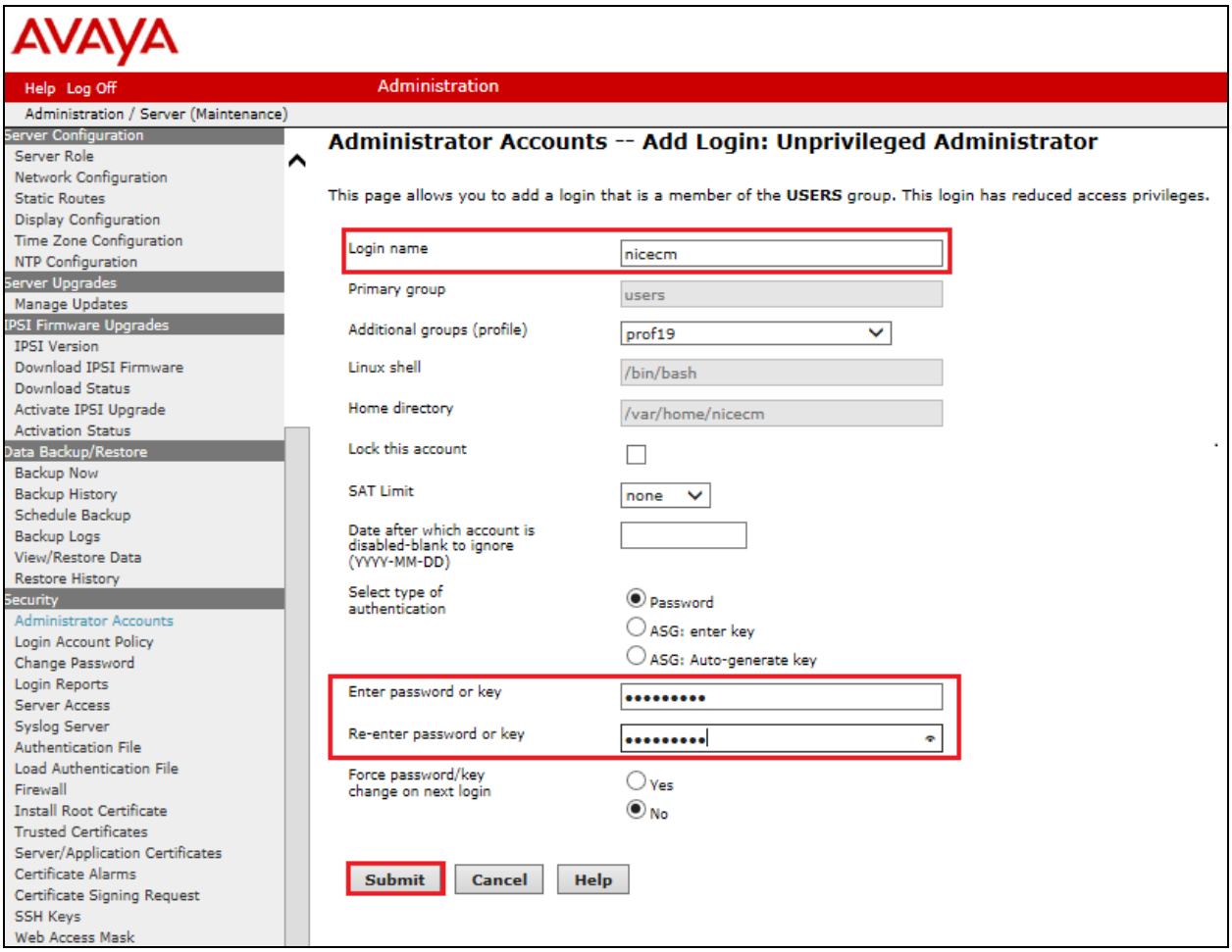


Once logged in click on **Administration** at the top of the page and select **Server (Maintenance)** from the drop-down menu.

In the left window navigate to **Security → Administrator Accounts**. In the main window select **Add Login** and **Unprivileged Administrator** as shown below. Click on **Submit** when finished.



Enter a suitable **Login name** and enter a suitable **password**, then click on **Submit** as all other settings can be left as default. Note this name and password will be needed in **Section 7.1**.



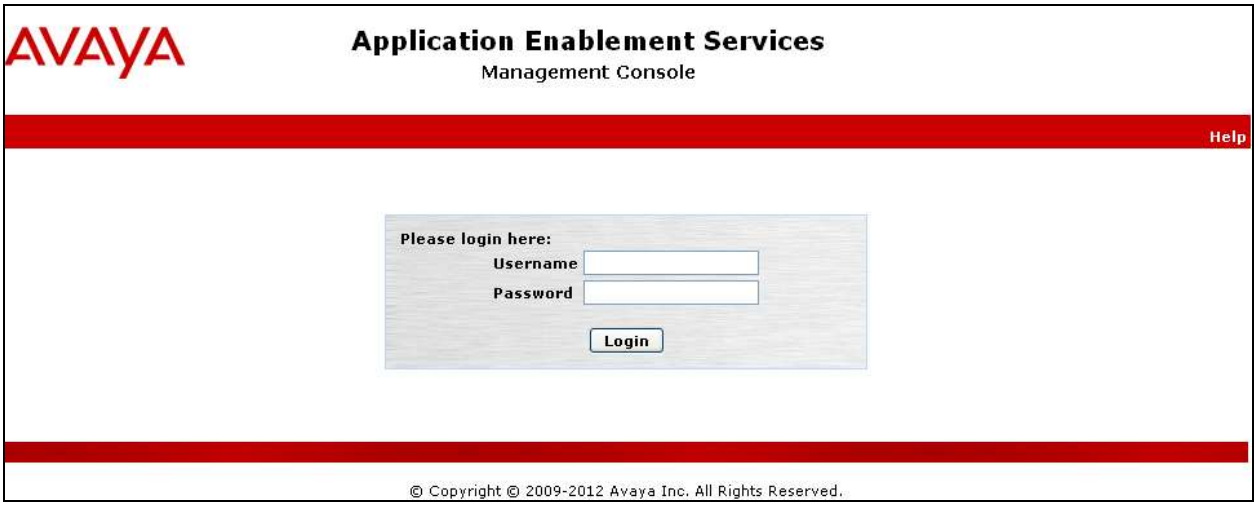
6. Configure Avaya Aura® Application Enablement Services

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

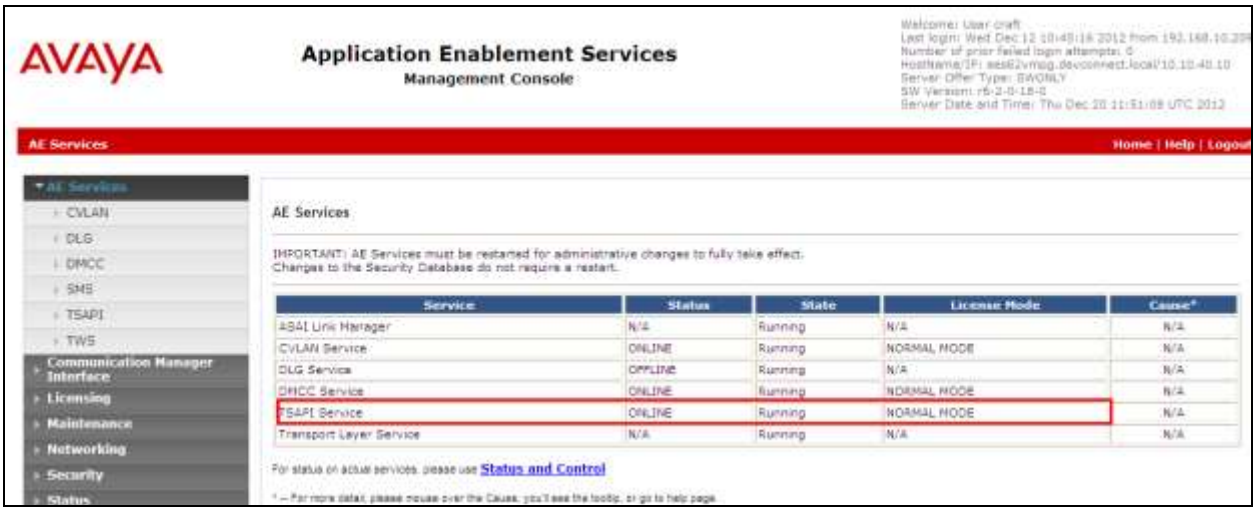
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Set Up Security Database on AES
- Associate Devices with CTI User

6.1. Verify Licensing

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

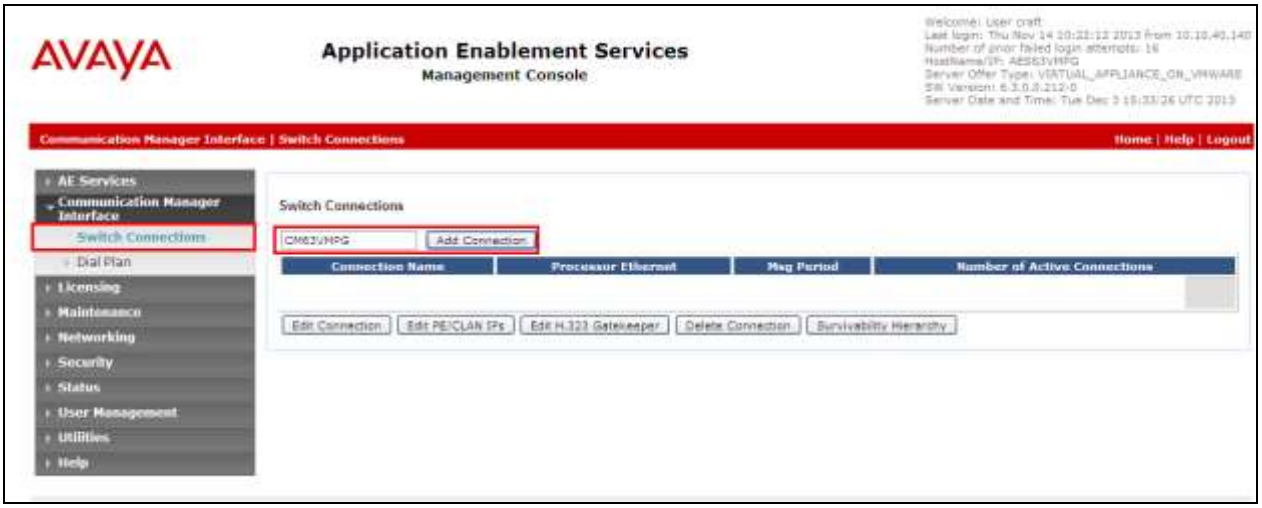


The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL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

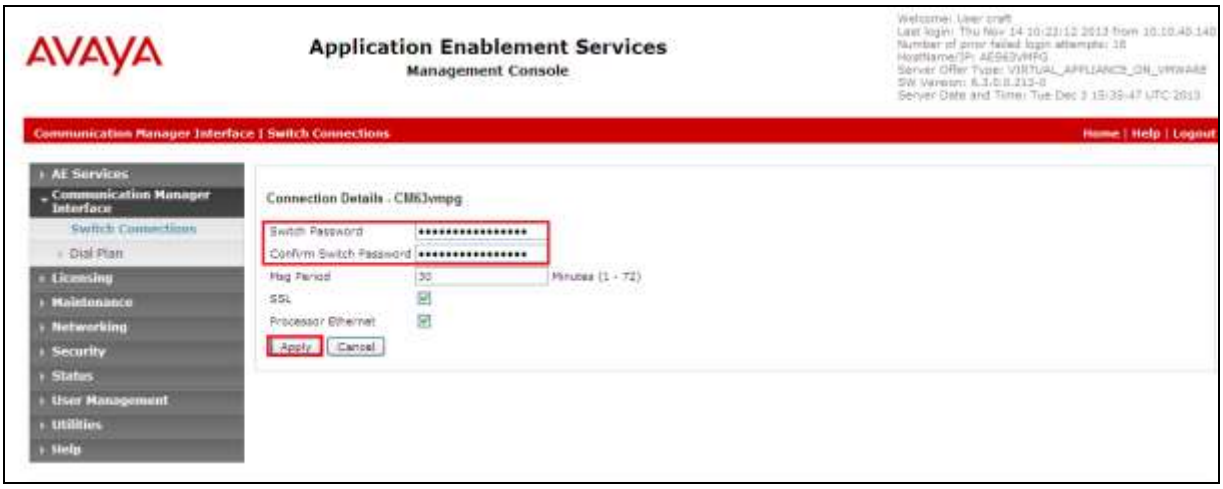


6.2. Create Switch Connection

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.



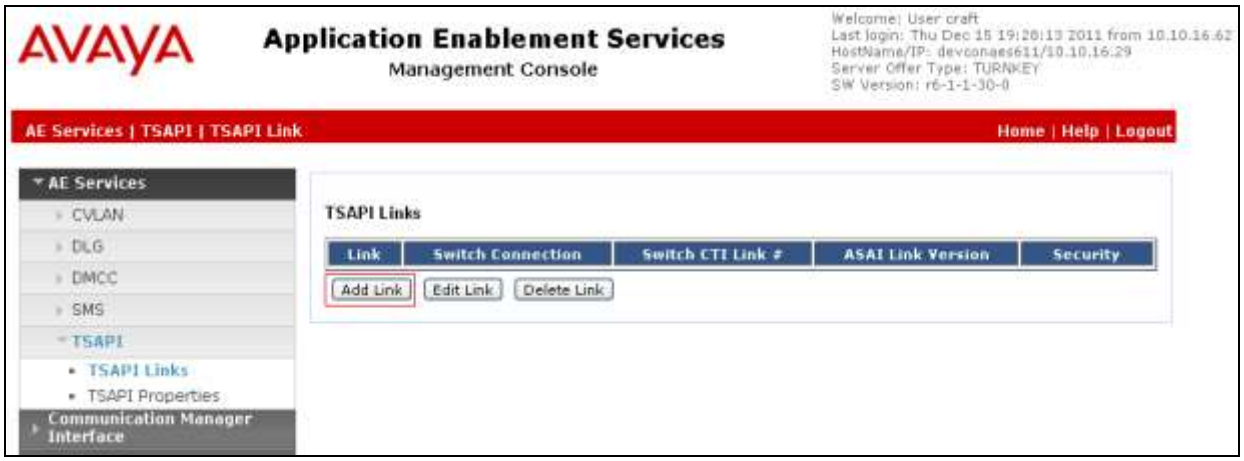
In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. Default values may be accepted for the remaining fields. Click **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 page 12. In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

6.3. Administer TSAPI link

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



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

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

Once completed, select **Apply Changes**.

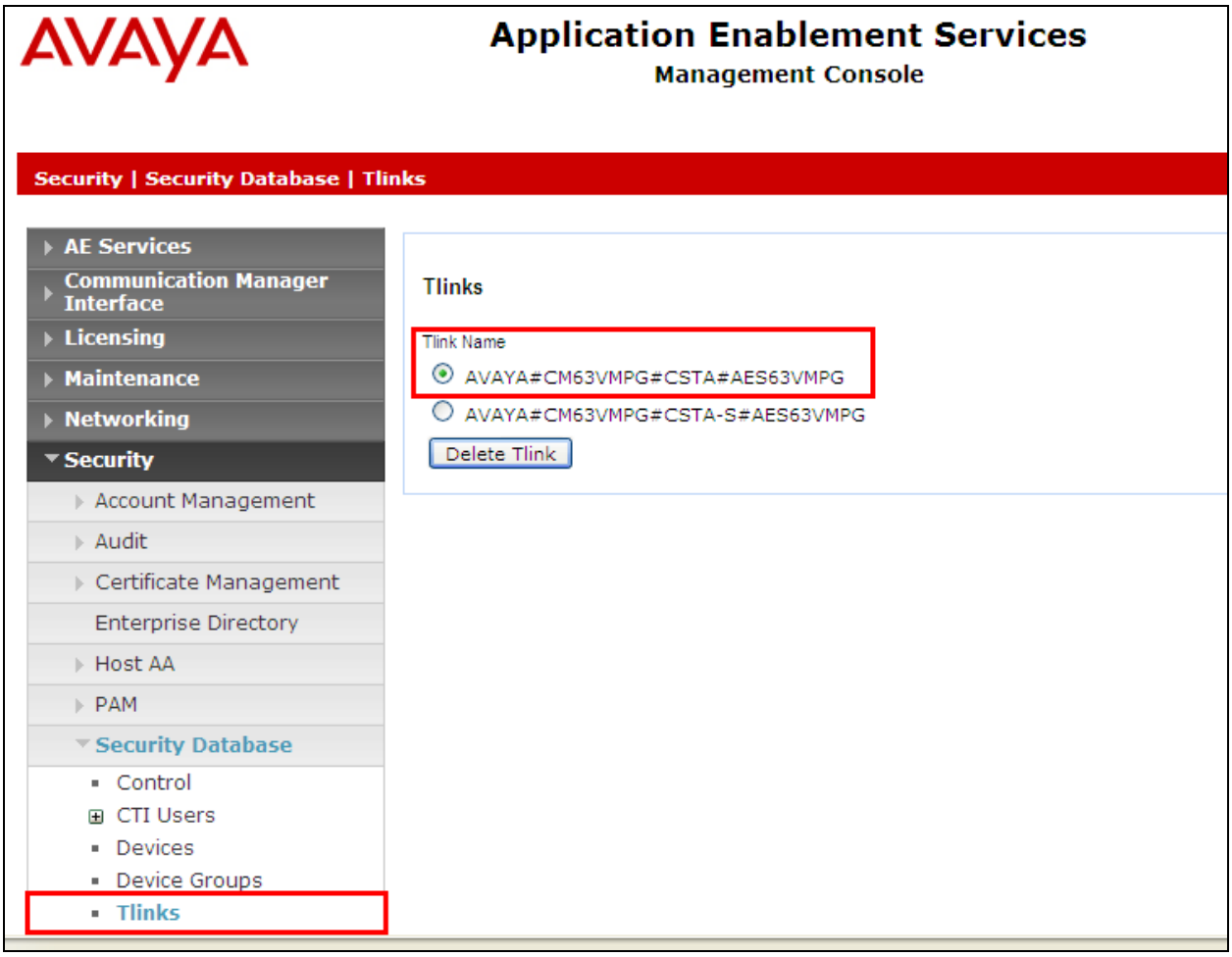
Another screen appears for confirmation of the changes made. Choose **Apply**.

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

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

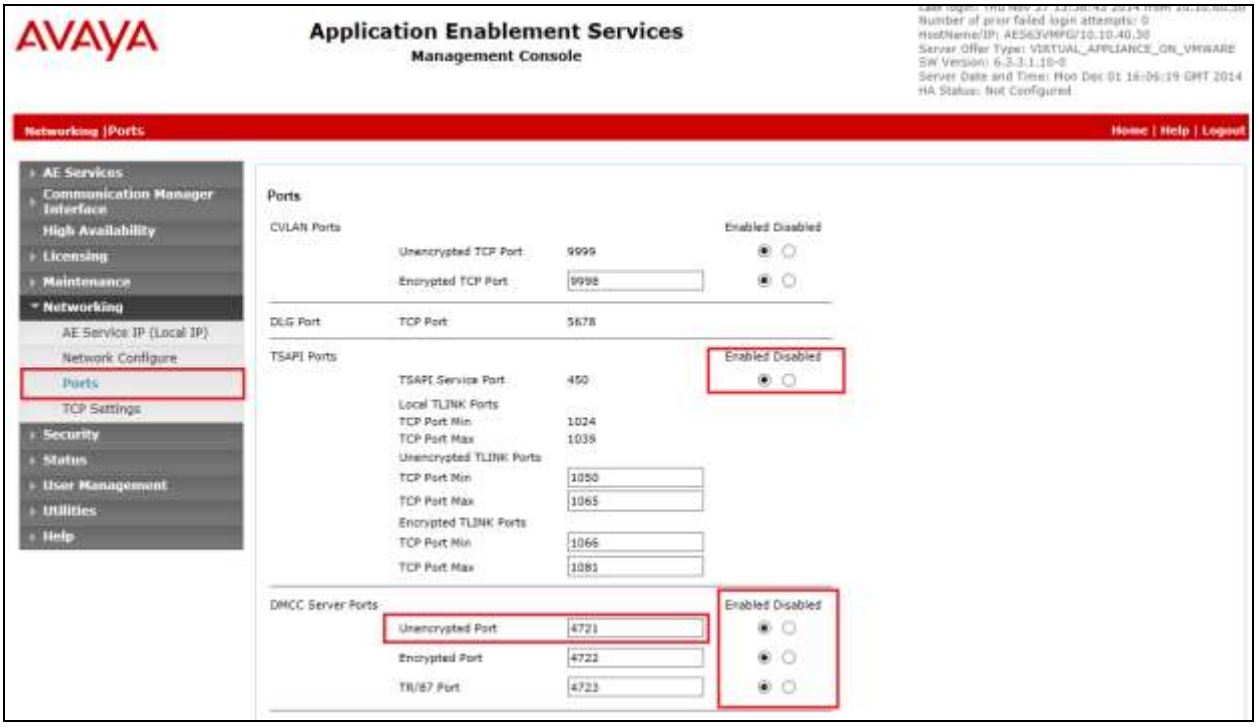
6.4. Identify Tlinks

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



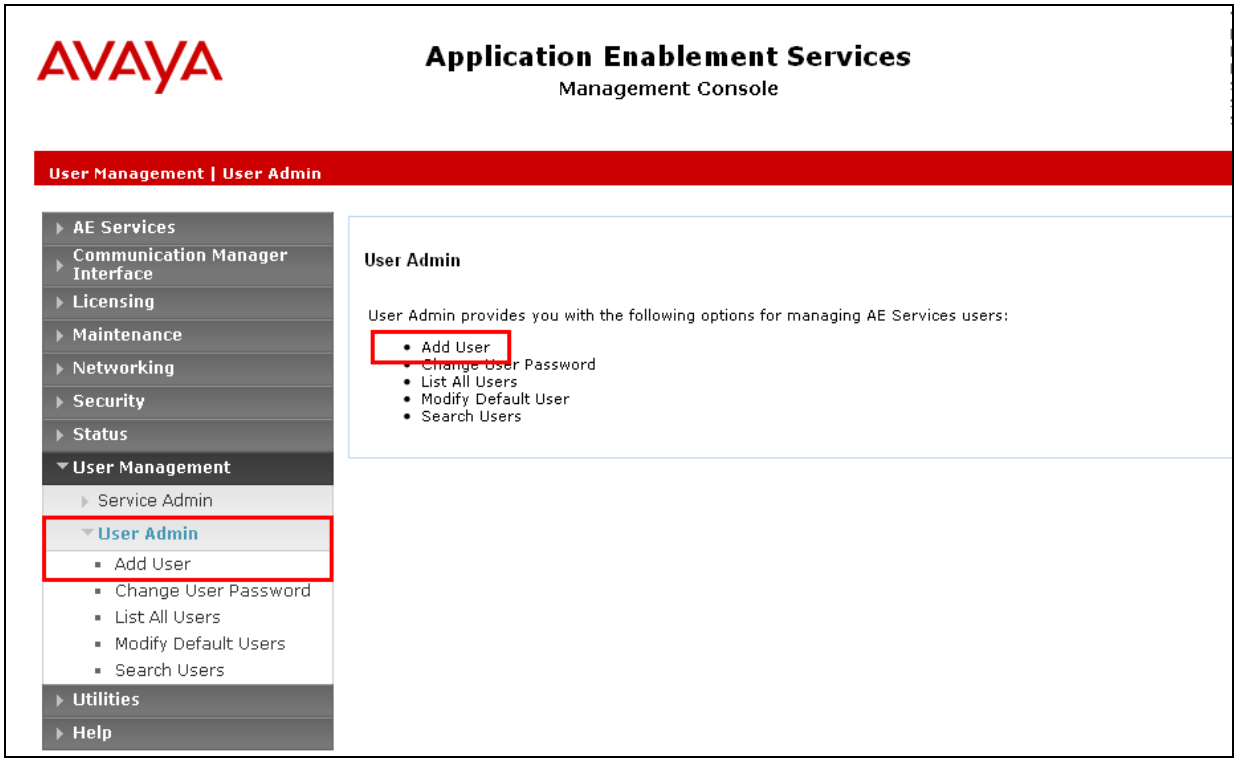
6.5. Enable TSAPI Ports

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



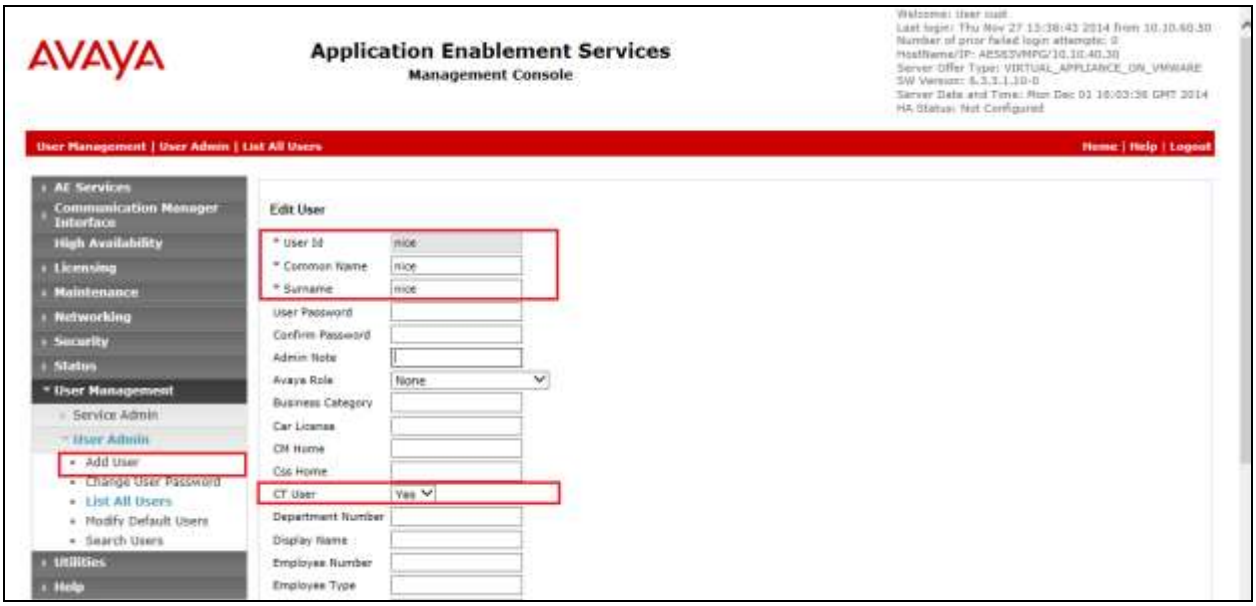
6.6. Create CTI User

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.

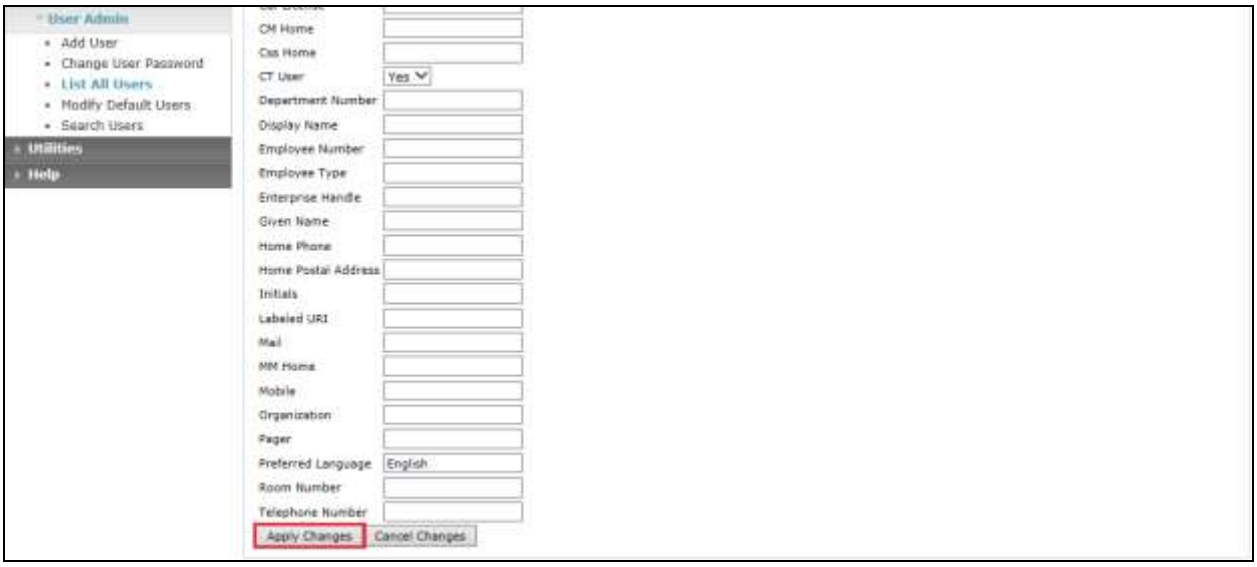


In the **Add User** screen shown below, enter the following values:

- **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.

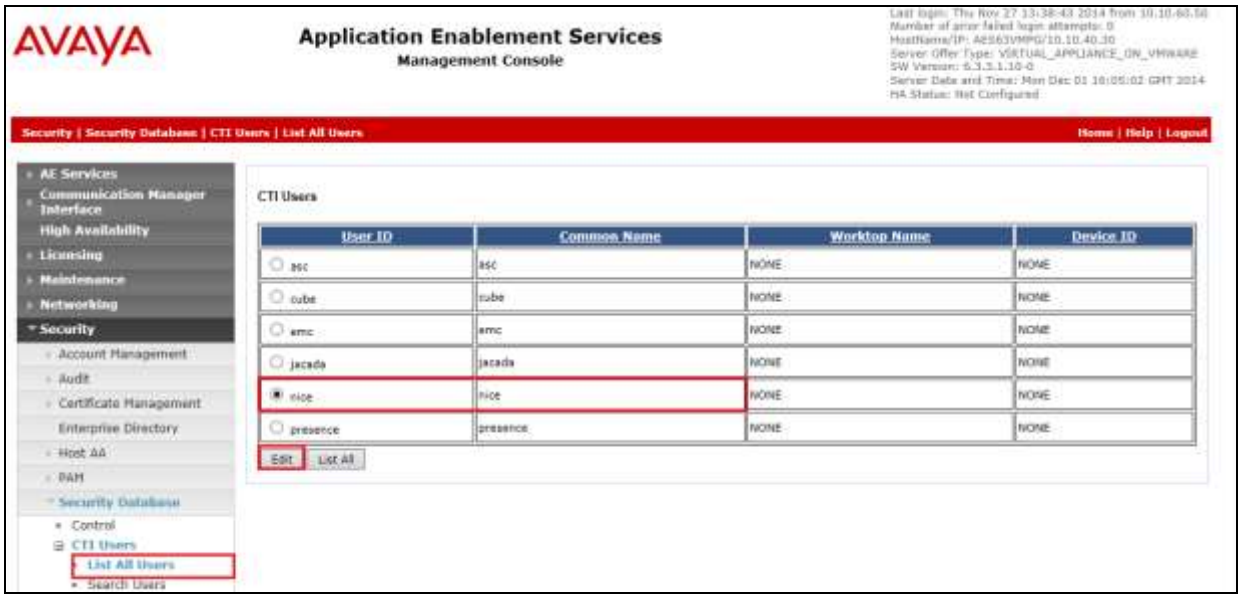


Scroll down and click on **Apply Changes**.

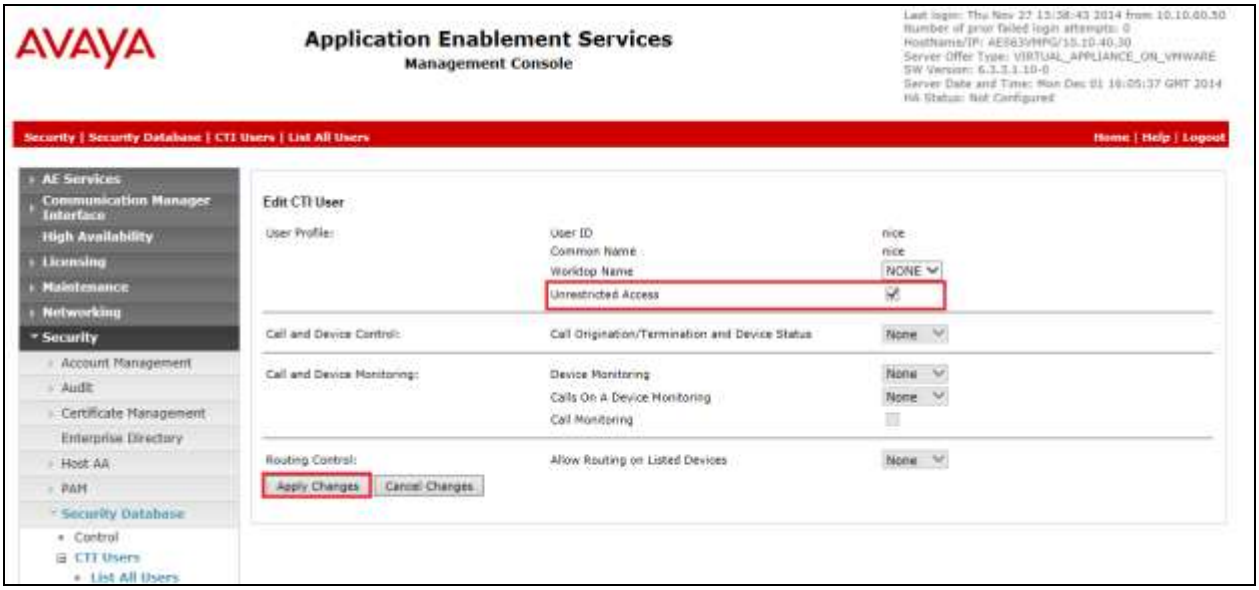


6.7. Associate Devices with CTI User

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



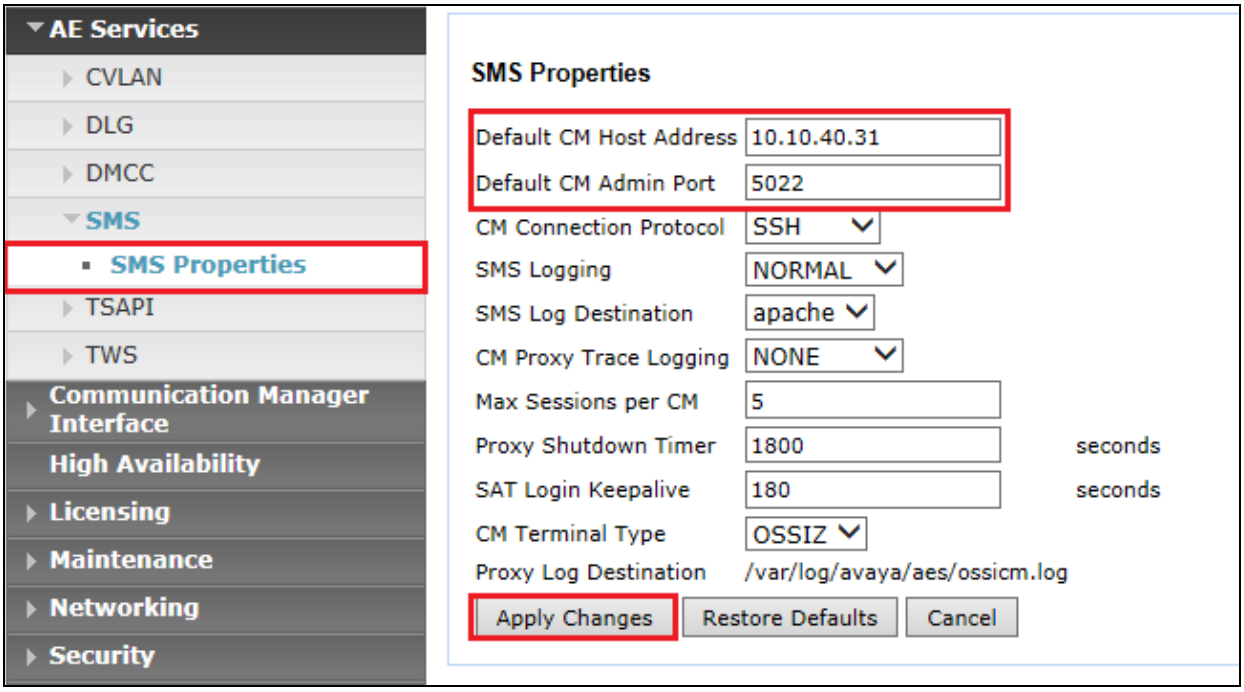
In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.



6.8. Configure the System Management Service on Avaya Aura® Application Enablement Services

From the AE Services Management Console main menu, select **AE Services → SMS → SMS Properties**. The following list describes the SMS configuration settings and provides guidelines for configuring SMS.

- **Default CM Host Address** — SMS will attempt to connect to this Communication Manager host address, as long as no host address is explicitly specified in the authorization header of a client request. If this field is blank, all SMS requests must explicitly include the target Communication Manager host address.
- **Default CM Admin Port** — By default the System Management Service will use **5022** to connect to a Communication Manager server.
- **CM Connection Protocol** — Use the default **SSH** port. The default TUI (or SAT) ports on Communication Manager are **SSH** Port=5022 Telnet Port=5023.
- **SMS Logging** — Use the default setting **NORMAL** unless debugging.
- **SMS Log Destination** — Use the default **apache**, unless debugging.
- **CM Proxy Trace Logging** — Use the default **NONE**, unless debugging.
- **Proxy Log Destination** — Use the default destination **/var/log/avaya/aes/ossicm.log** for the CM Proxy Trace logs on the AE Server.
- **Max Sessions per CM** — This is a safety setting that prevents SMS from consuming all of the TUI processes on Communication Manager. By default the setting is **5**.
- **Proxy Shutdown Timer** — Use the default **1800** seconds.
- **SAT Login Keepalive** — Use the default **180** seconds.
- **CM Terminal Type** — Use the default **OSSIZ**.

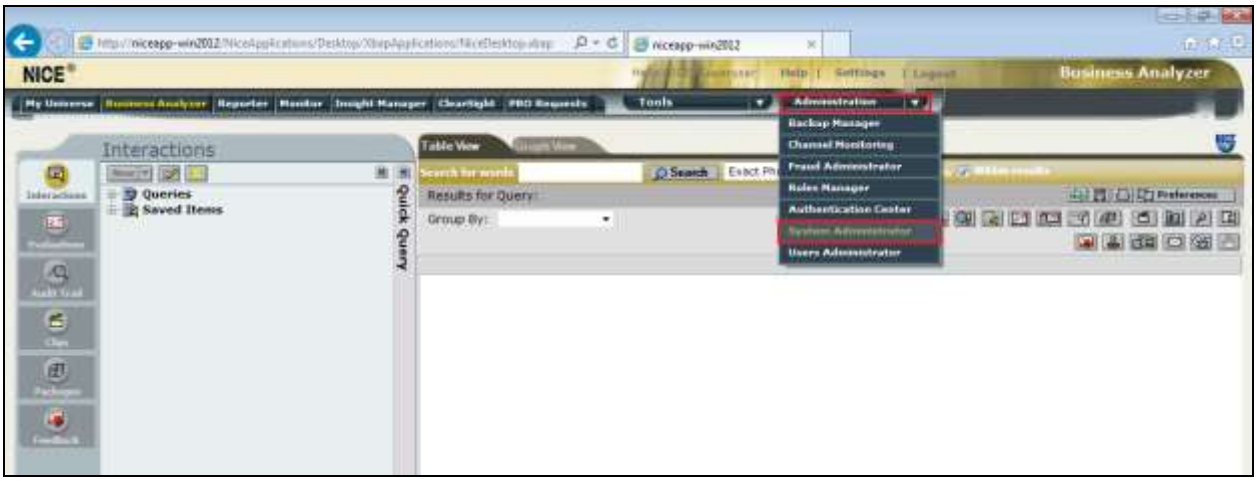


7. Configure NICE Engage Platform

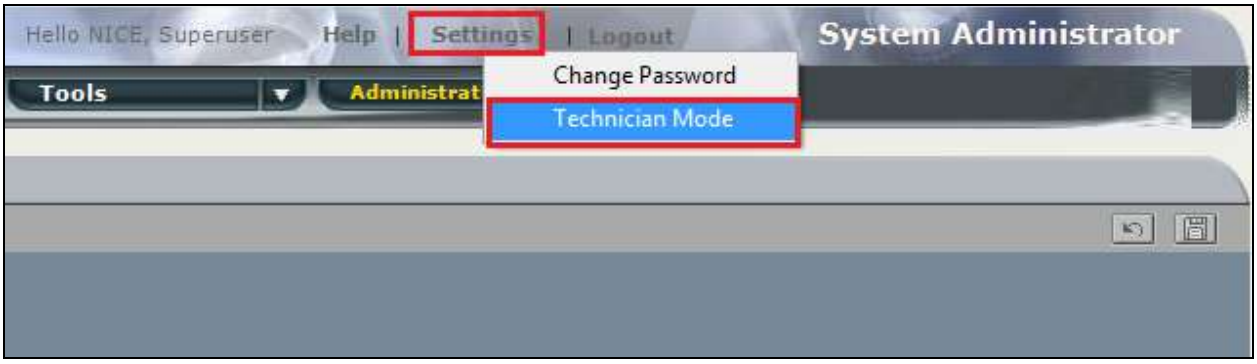
The installation of NICE Engage Platform is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of the NICE Engage Platform contact NICE as per the information provided in **Section 2.3**.

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

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

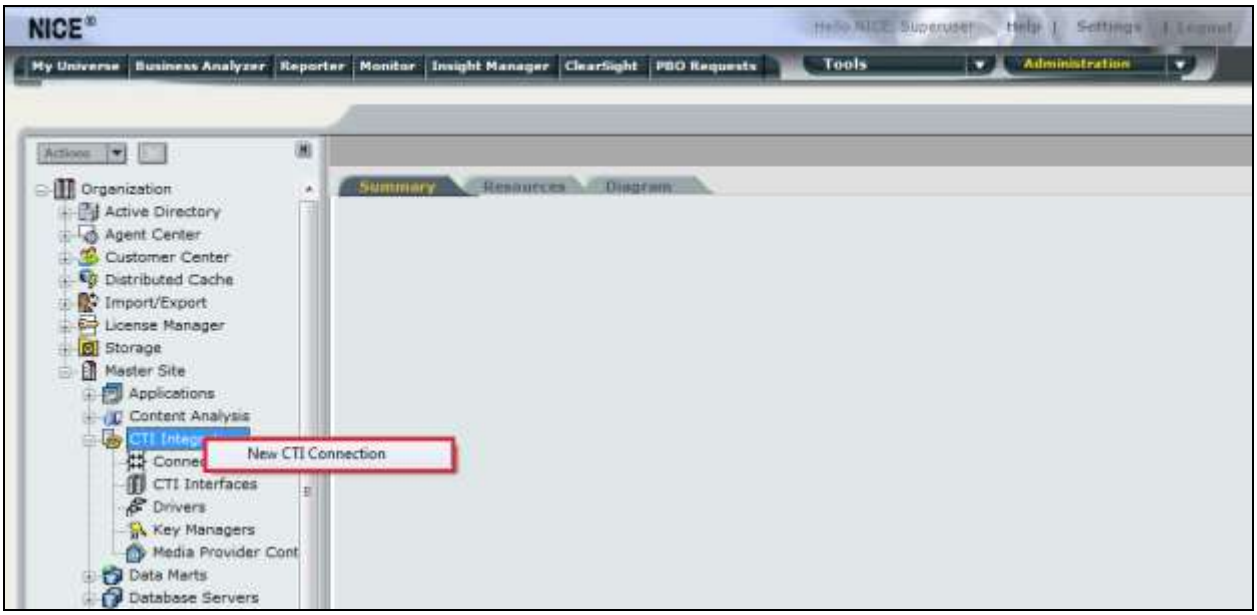


Before any changes can be made, switch to Technician Mode by clicking into Settings at the top of the screen as shown below.

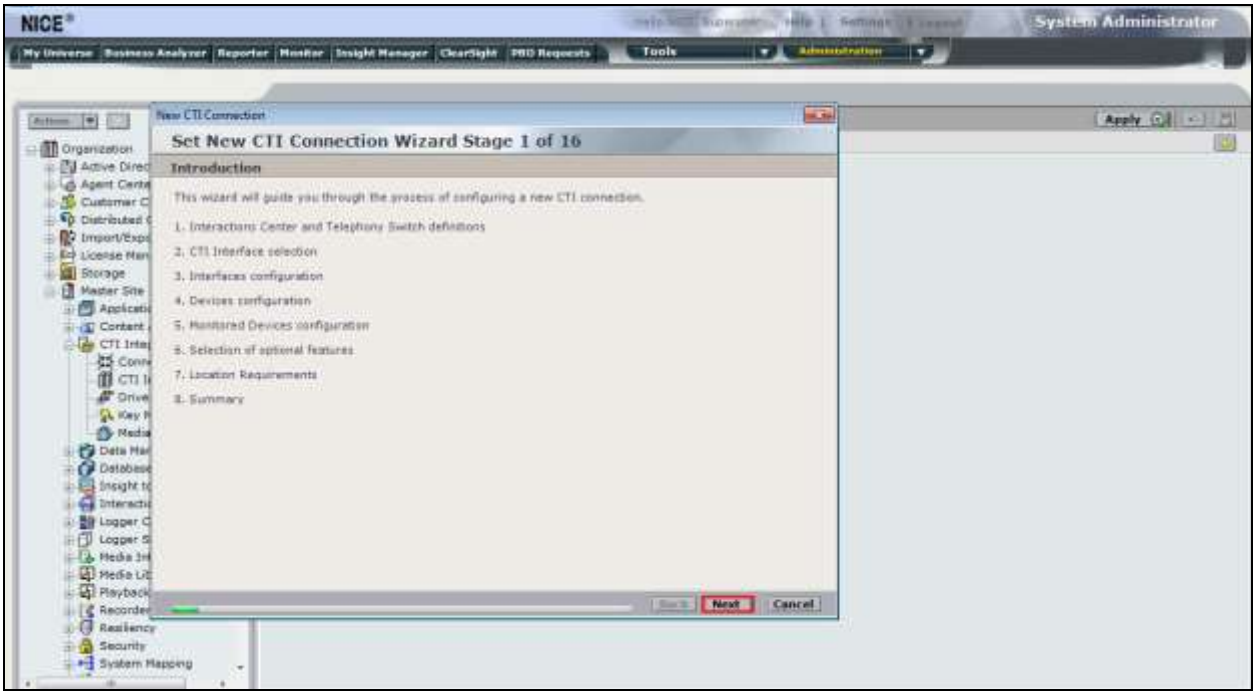


7.1. New CTI Connection

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

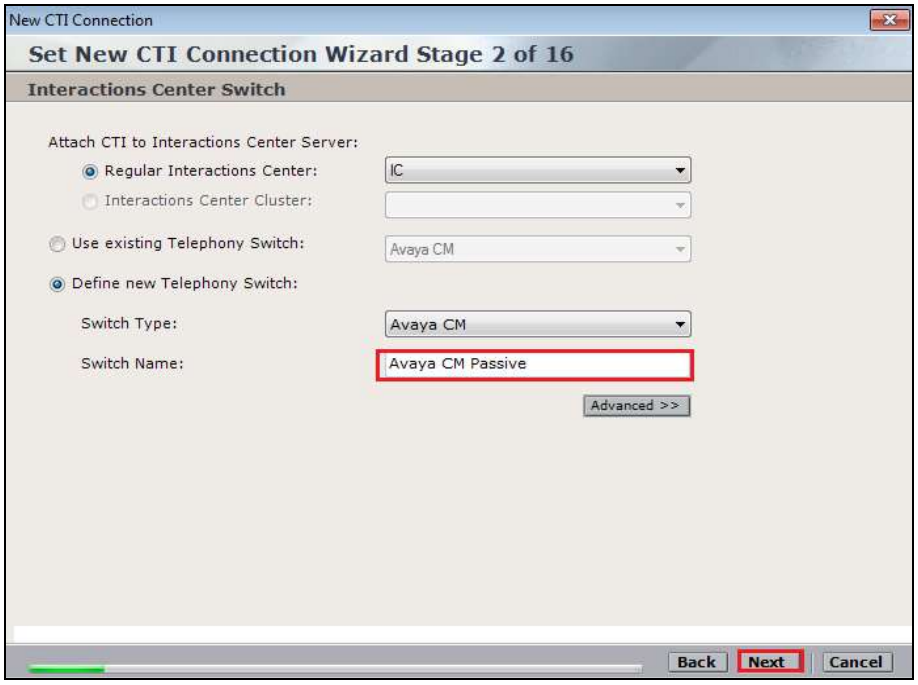


The **New CTI Connection Wizard** is opened and this will go through the 16 steps required to setup the connection to the AES for DMCC Service Observe and Single Step Conference type of call recording. Click on **Next** to contimue.

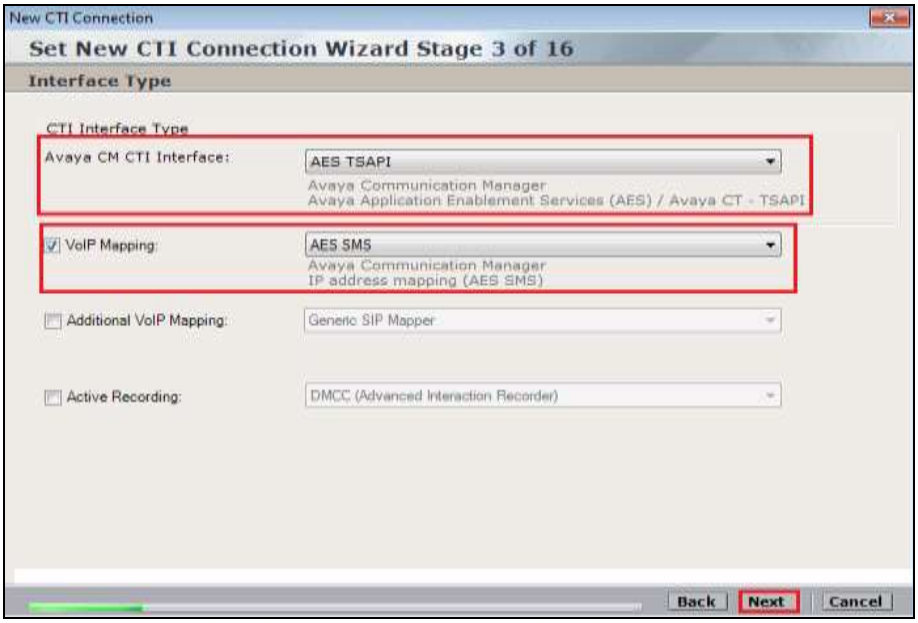


The value for Regular Interactions Center is a value that was already created during the installation of the NICE Engage platform. This value is therefore pre-chosen for the CTI connection being created below.

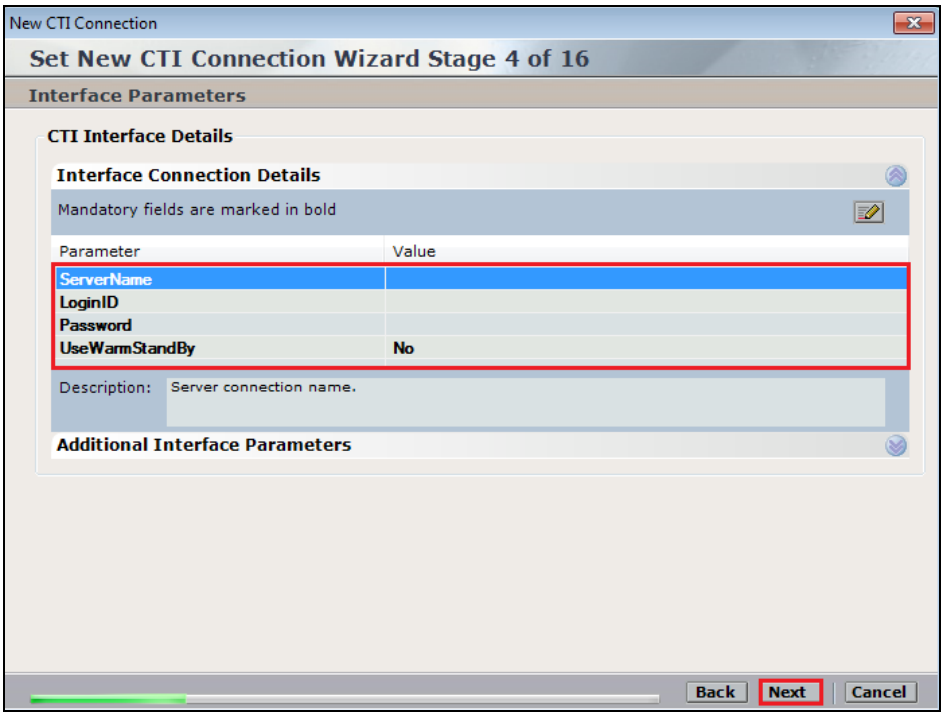
The **Telephony Switch** must be selected and this will be **Avaya CM**. Enter a suitable name for this **Switch Name**. Click on **Next** to continue.



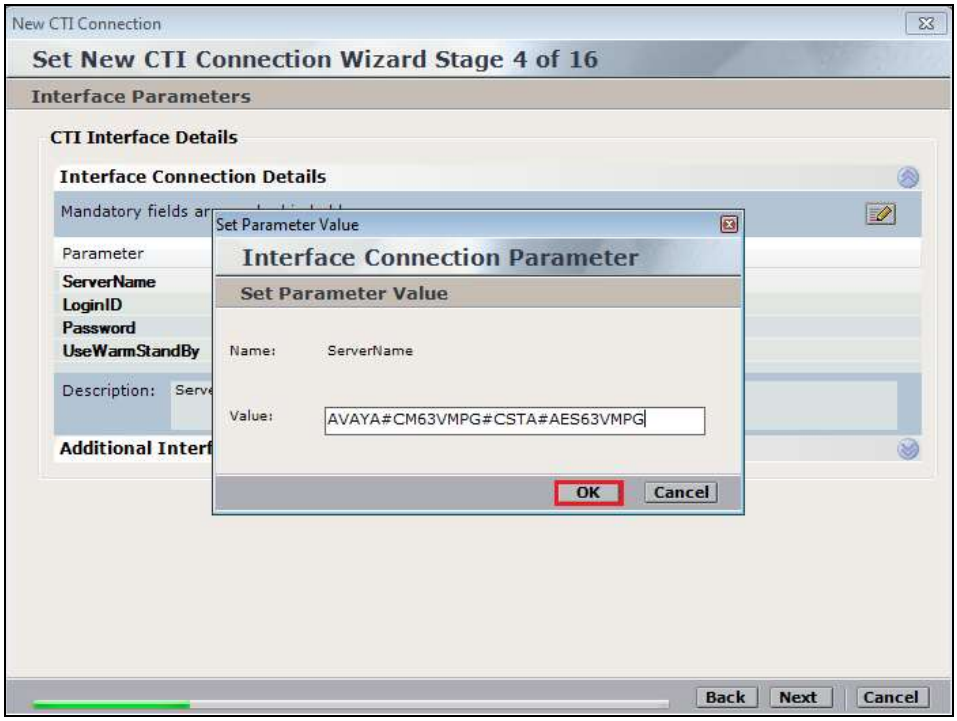
Select **AES TSAPI** for the **Avaya CM CTI Interface**, ensure that **VoIP Mapping** is ticked and select the **AES SMS** from the dropdown menu. Click on **Next** to continue.



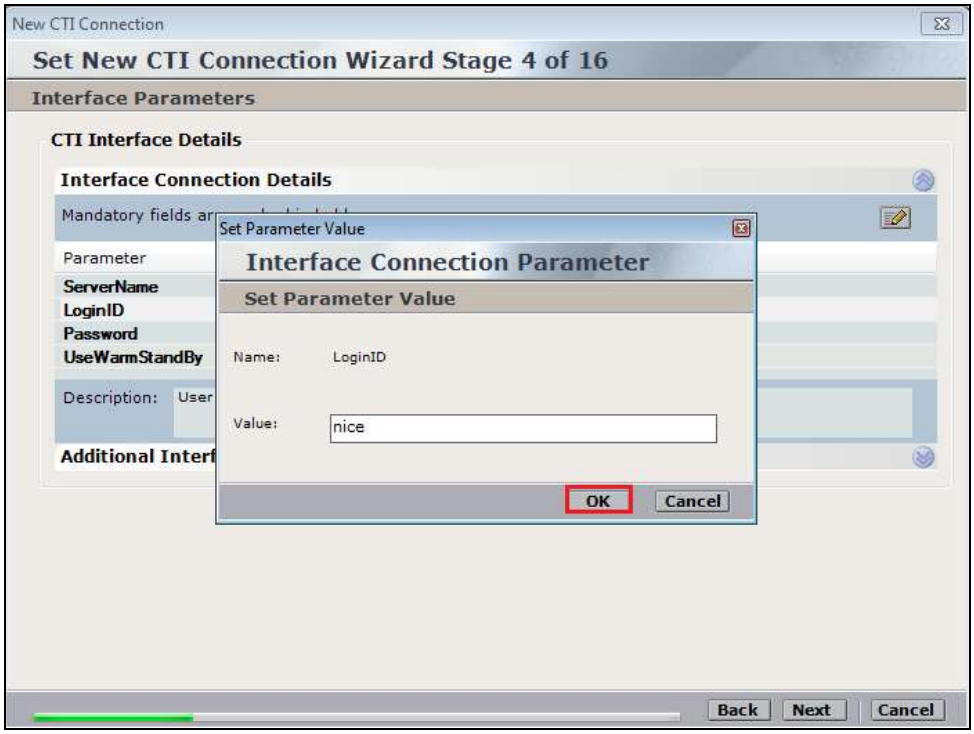
Each of the values below must be filled in. Double-click on each **Parameter** to enter a value for that parameter.



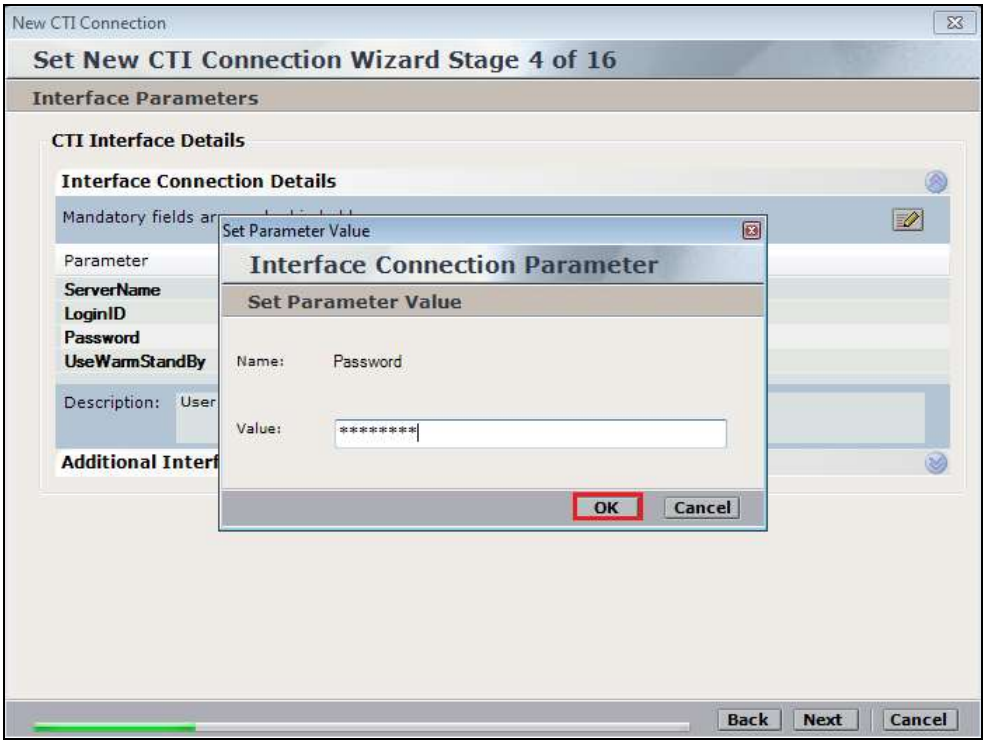
Double-click on **ServerName** and enter the TSAPI link **Value** from **Section 6.4**.



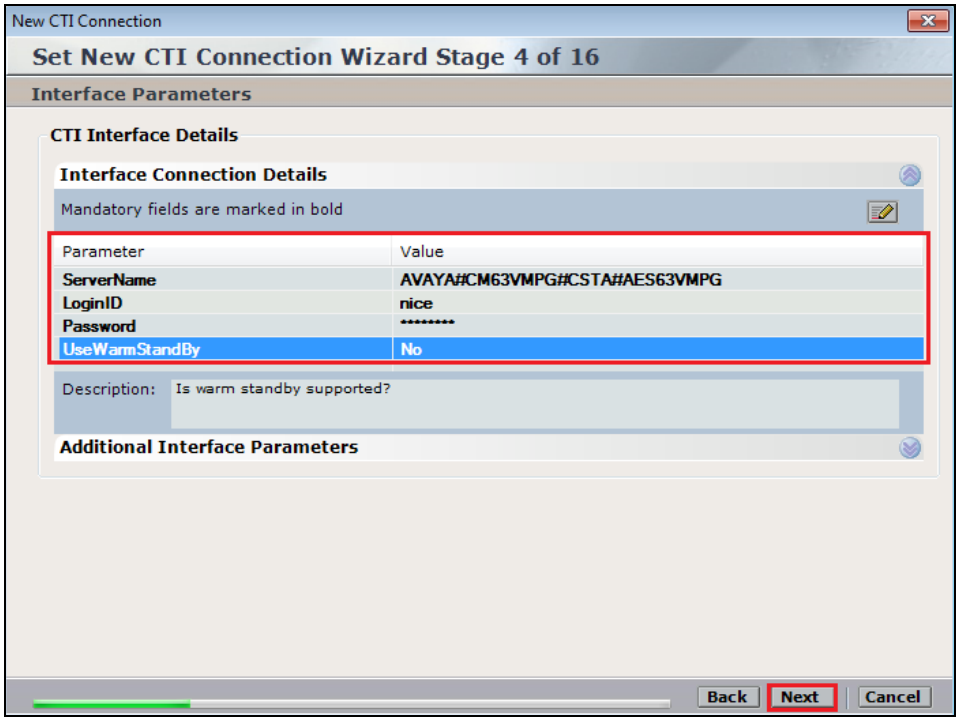
Double-click on LoginID and enter the username that was created in **Section 6.6**. Click on **OK**.



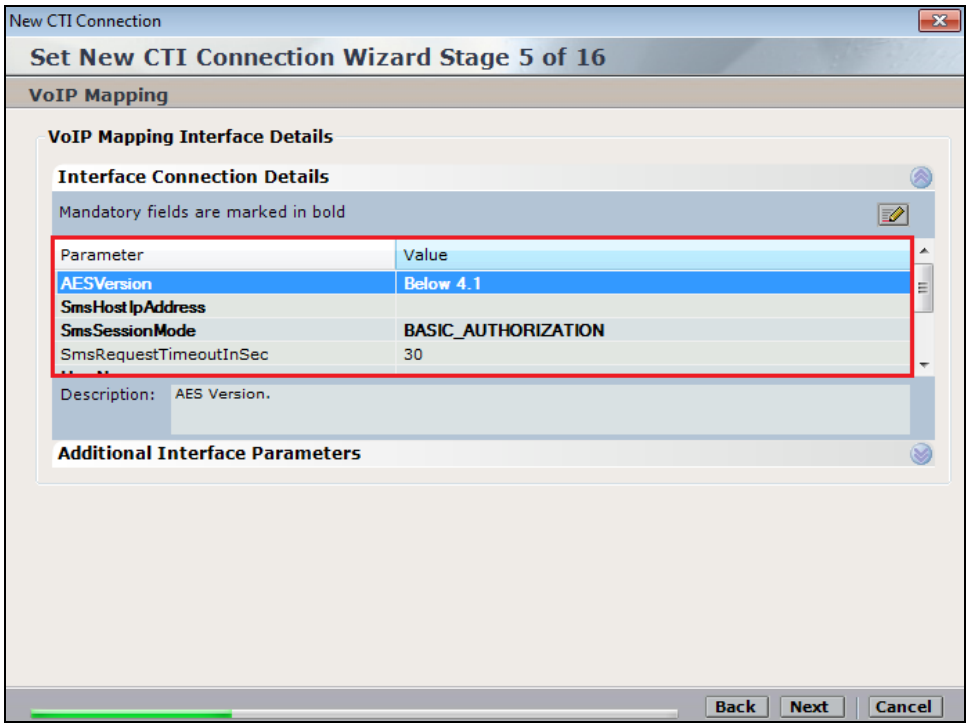
Double-click on password and enter the value for the password that was created in **Section 6.6**.



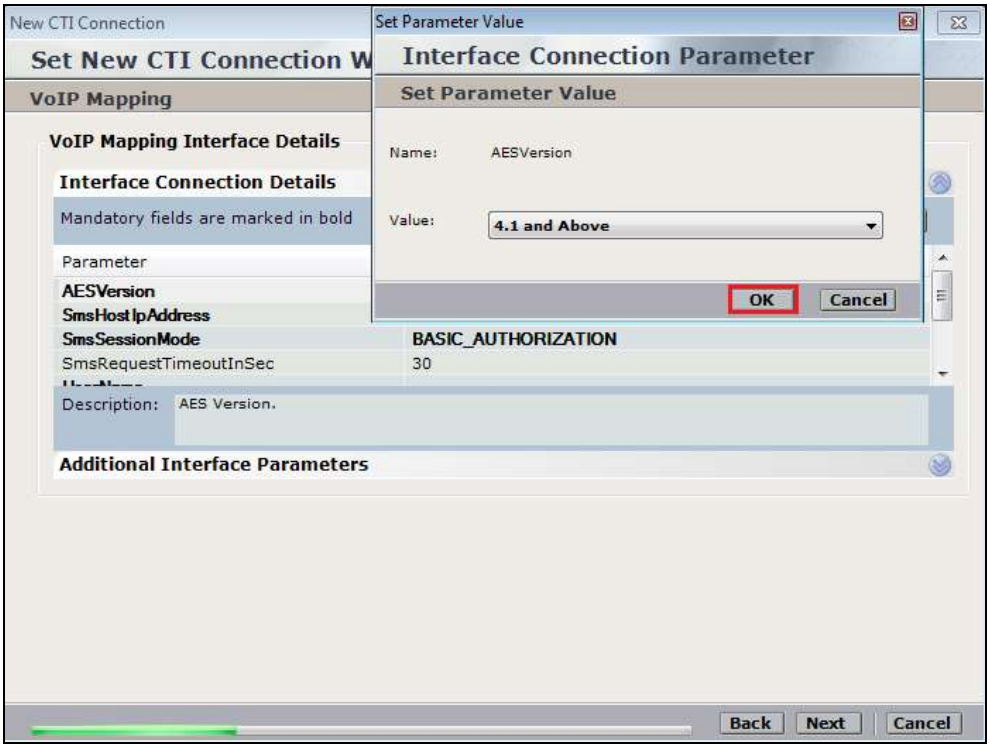
Click on **Next** once these values are all filled in.



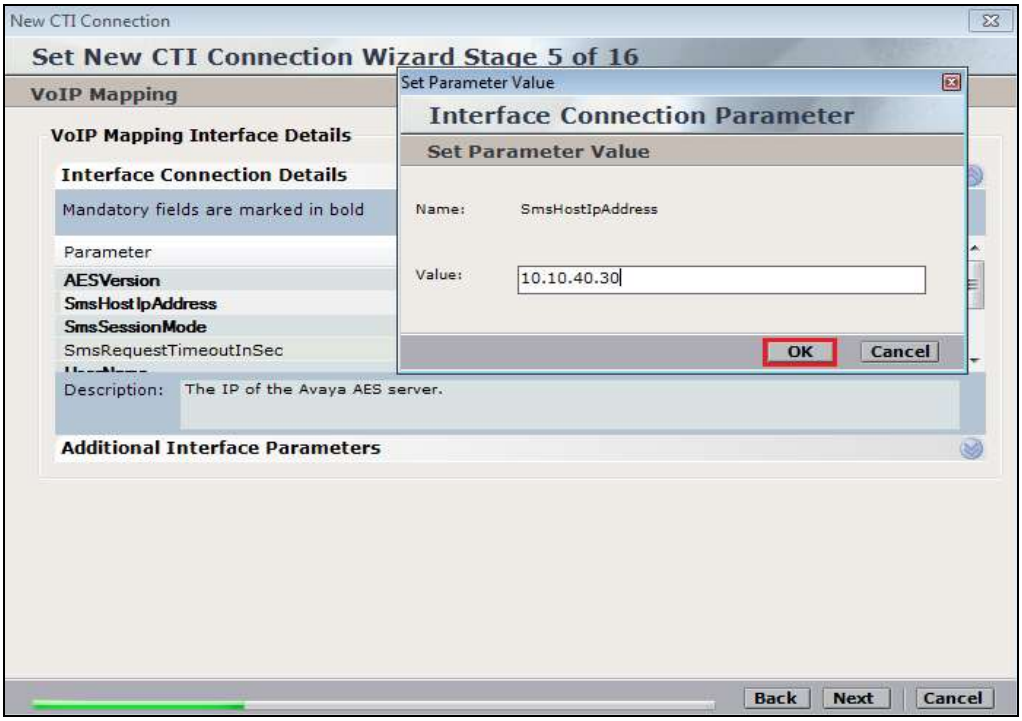
The values below must be filled in by double-clicking on each **Parameter**.



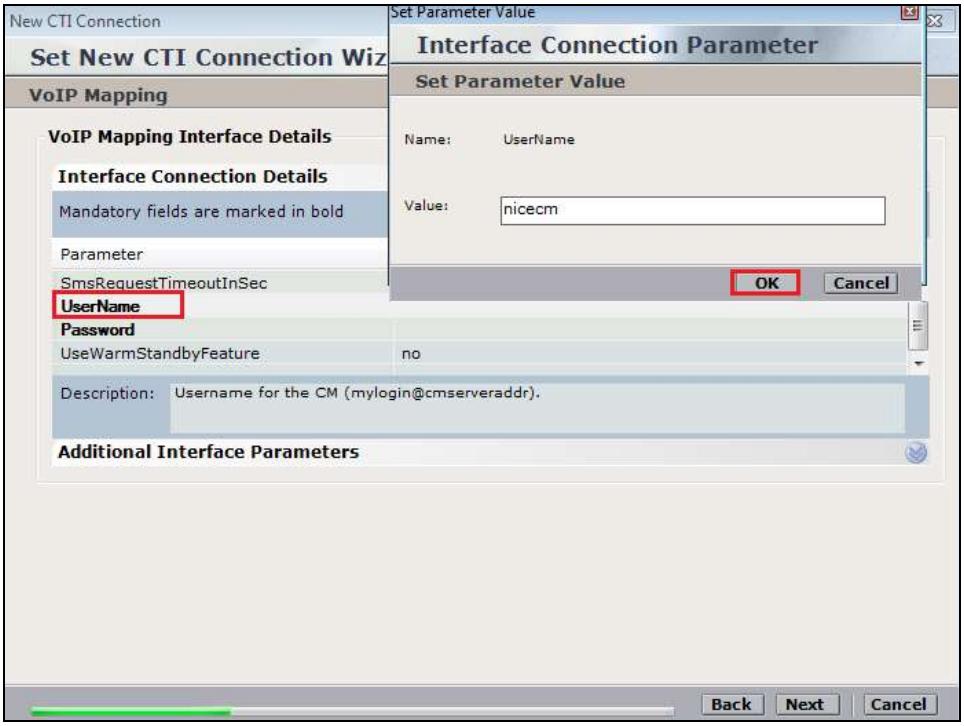
Enter the **Value** for the **AESVersion**. Click on **OK**.



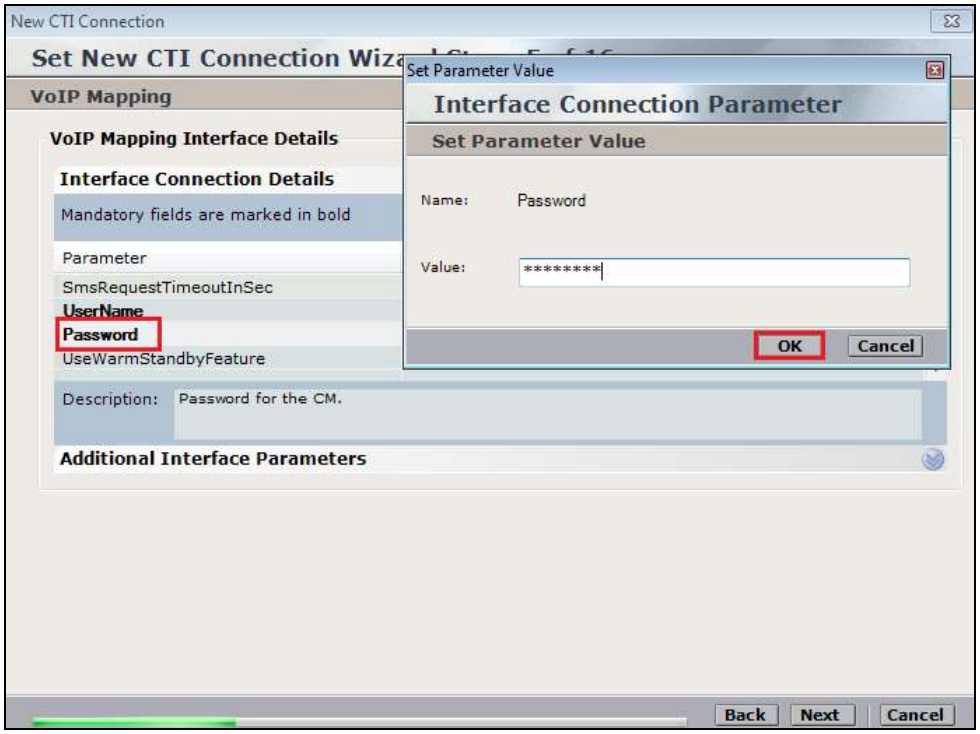
Enter the **Value** for the **SmsHostIpAddress**, note this will be the IP address of the AES in the solution. Click on **OK** to continue.



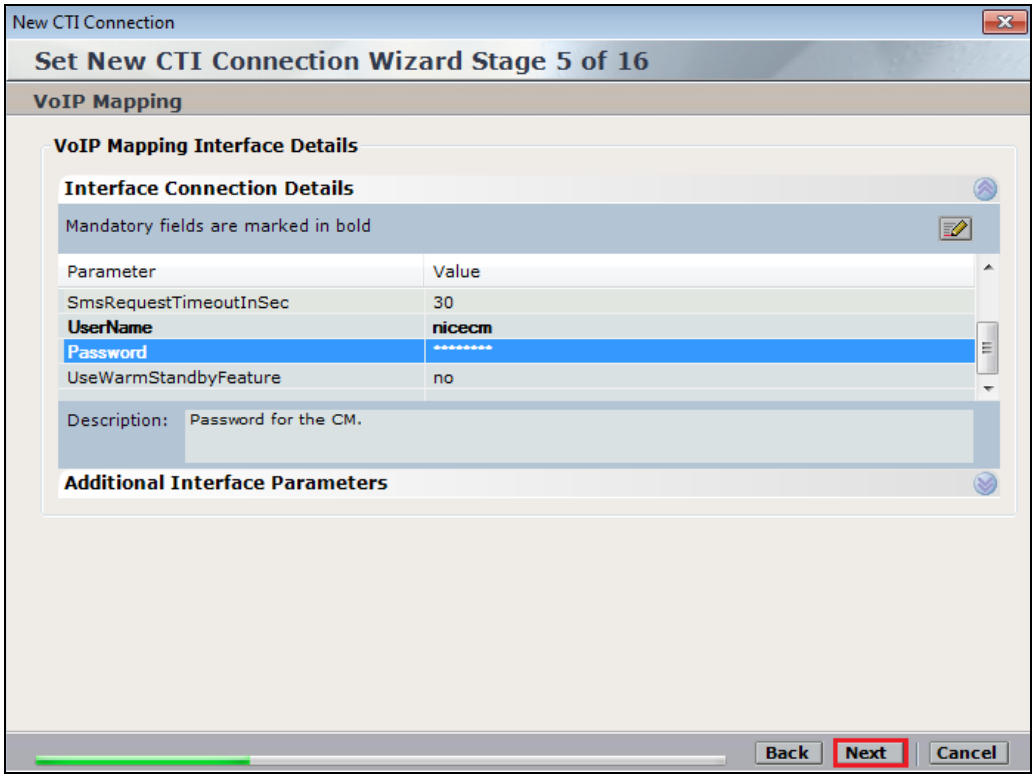
As before enter the username that was created in **Section5.5** and click on **OK**.



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

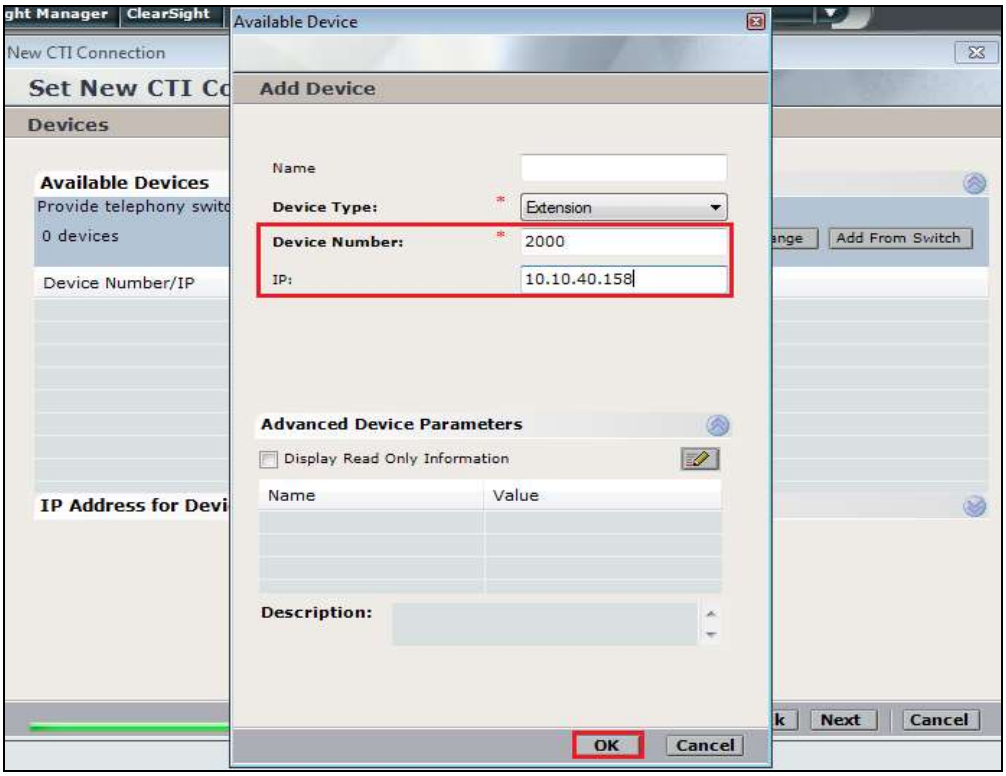


Click on **Next** to continue.

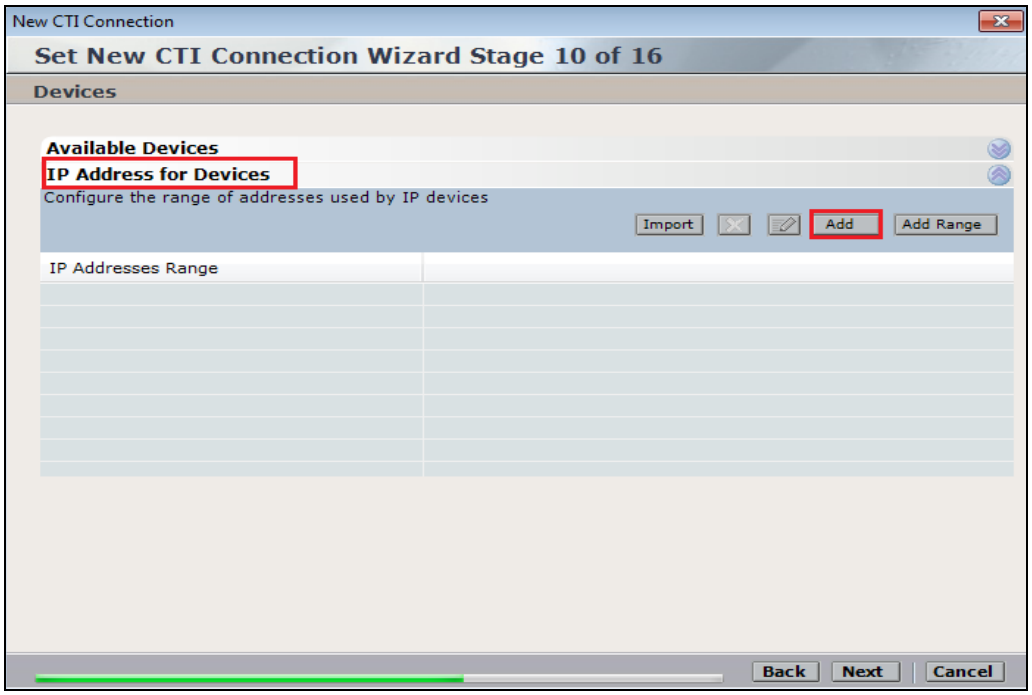


On the following screen, click on **Add,** to add the Communication Manager devices.

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

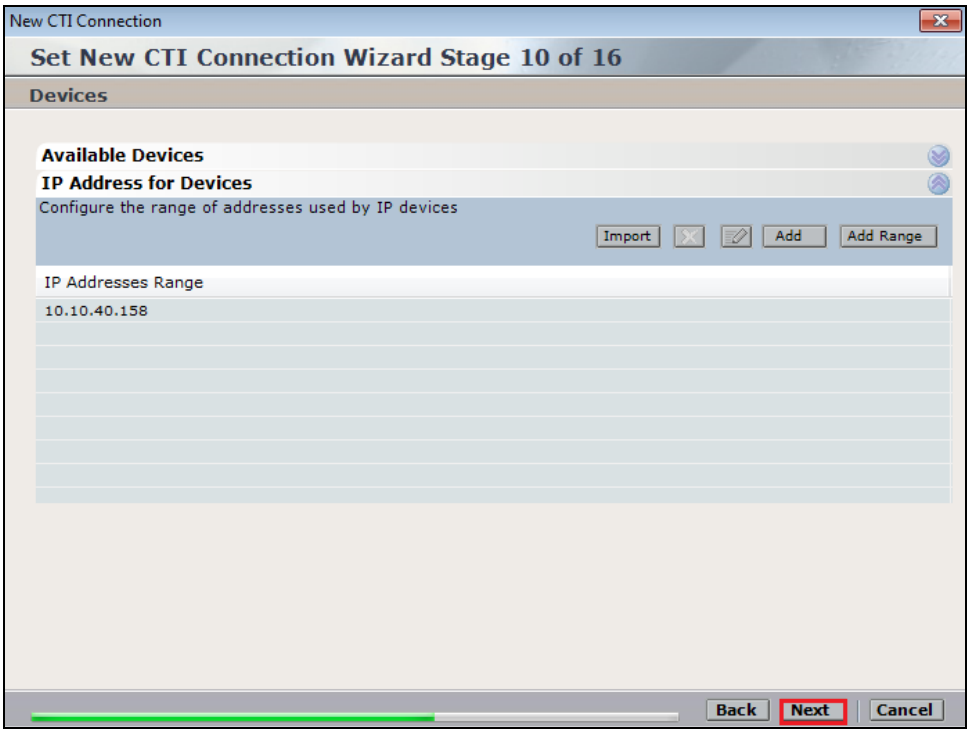


Click on **Add** to add the **IP Address** of the device.

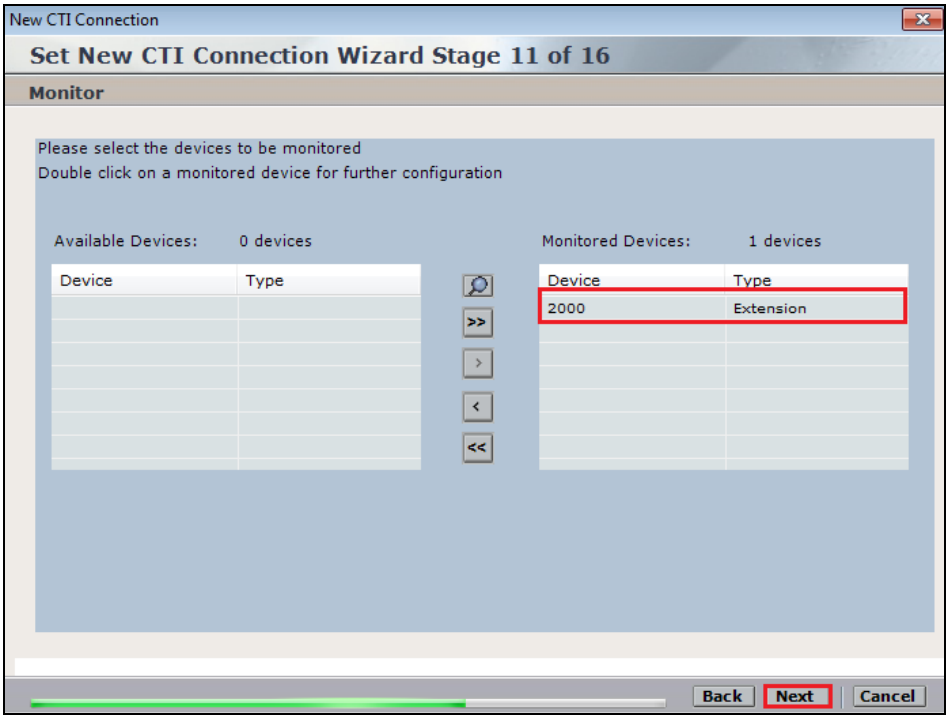


Enter the correct **IP** for the phone set extension.

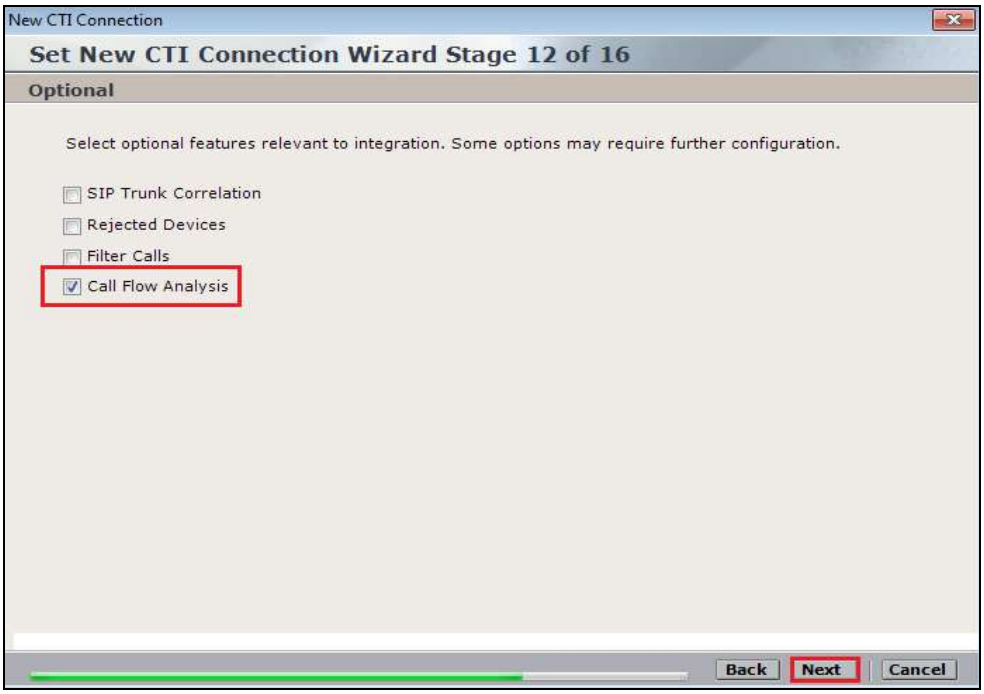
Enter the IP addresses for all devices that are to be recorded and click on **Next** to continue.



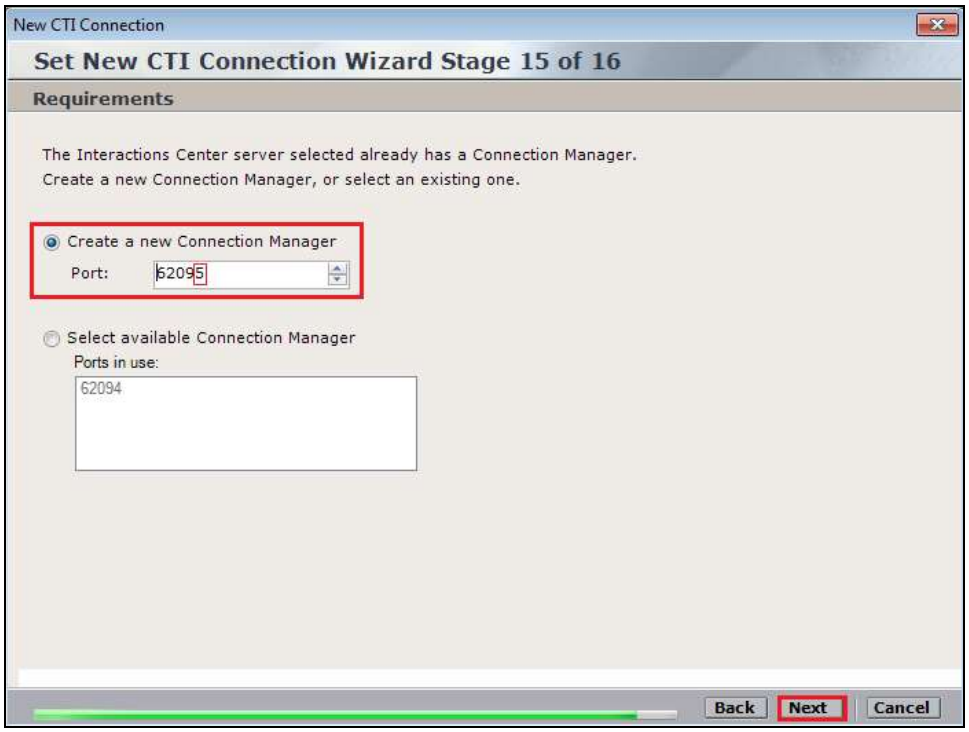
Select the new extension and click on the >> icon as shown. Click on **Next** to continue.



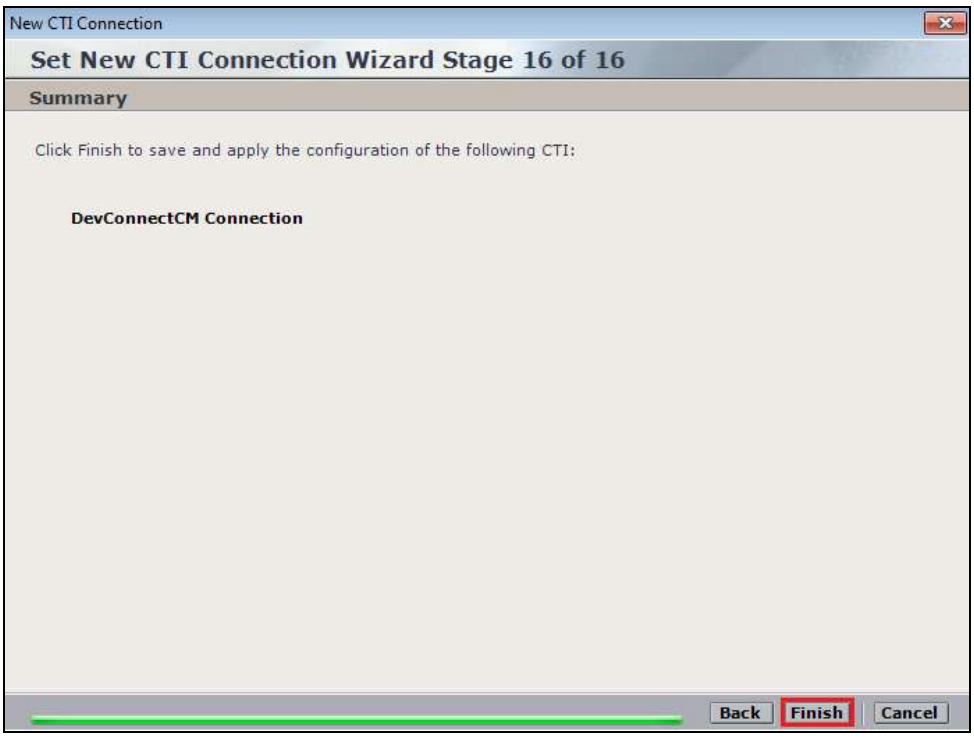
It is optional, but for better analysis tick on **Call Flow Analysis** and click on **Next** to continue.



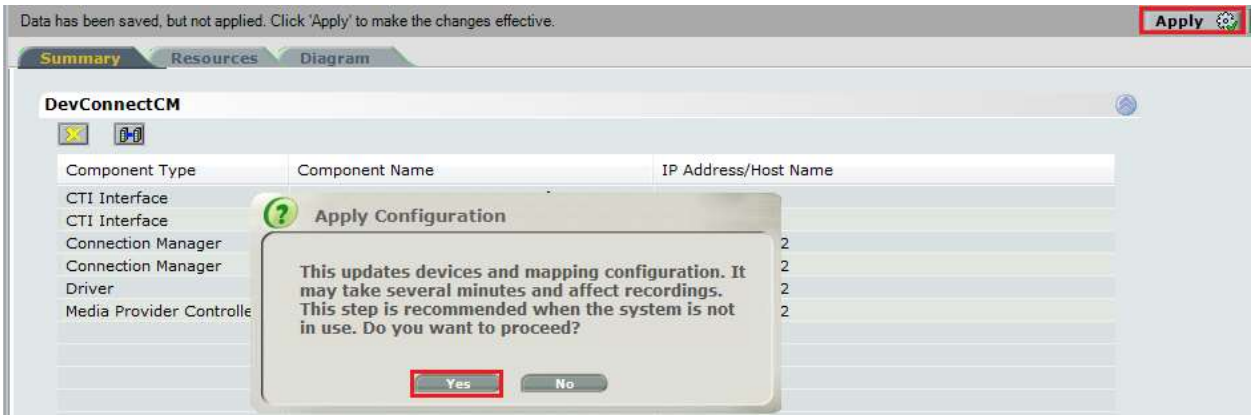
Select a different **Port** number as shown below **62095** is chosen simply because **62094** is already in use.



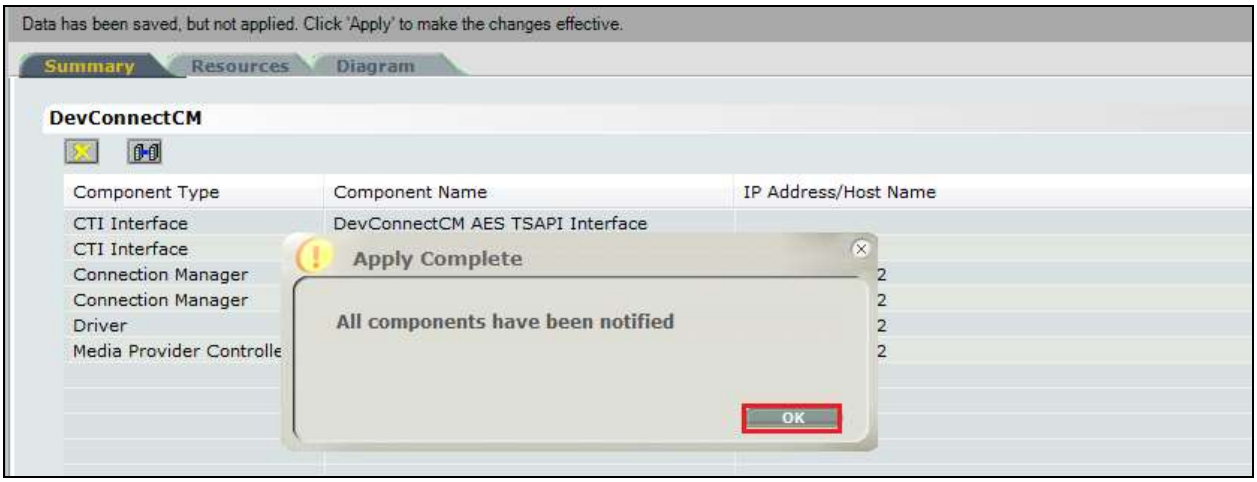
Click on **Finish** to complete the **New CTI Wizard**.



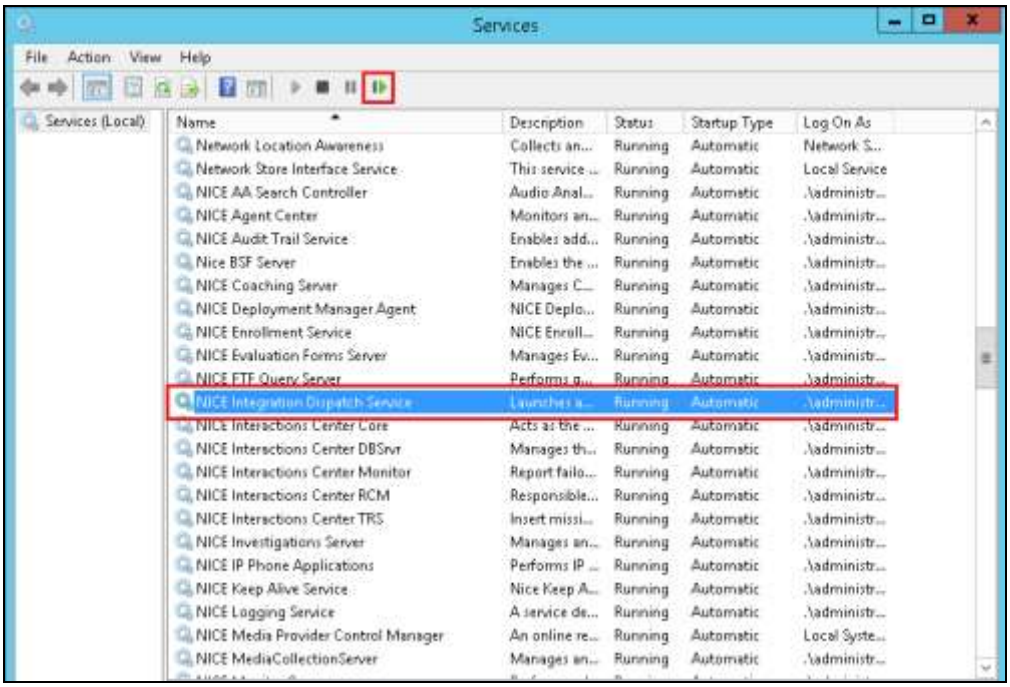
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed.



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

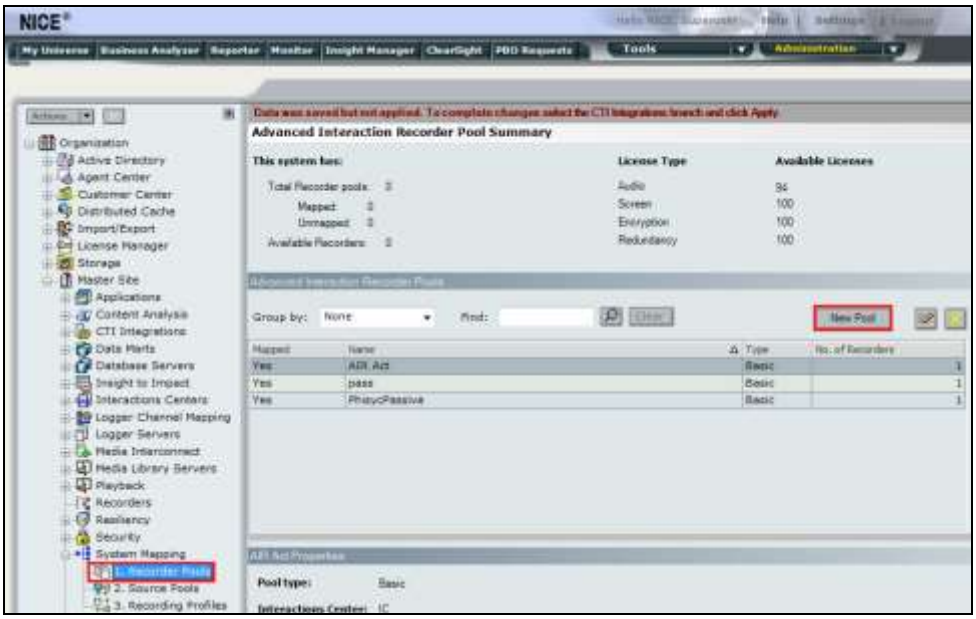


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

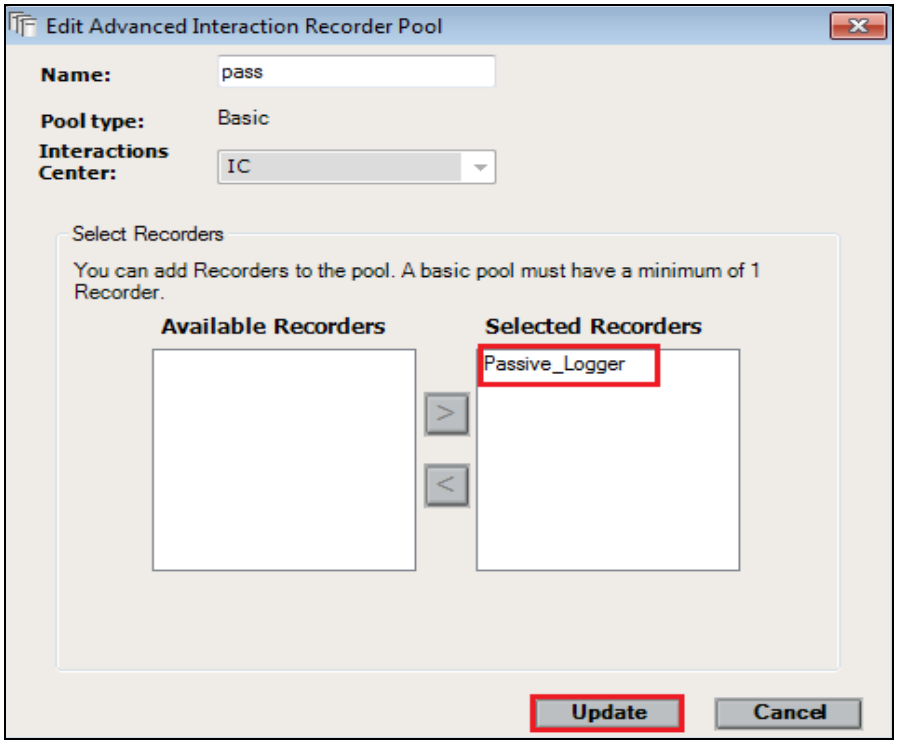


7.2. System Mapping

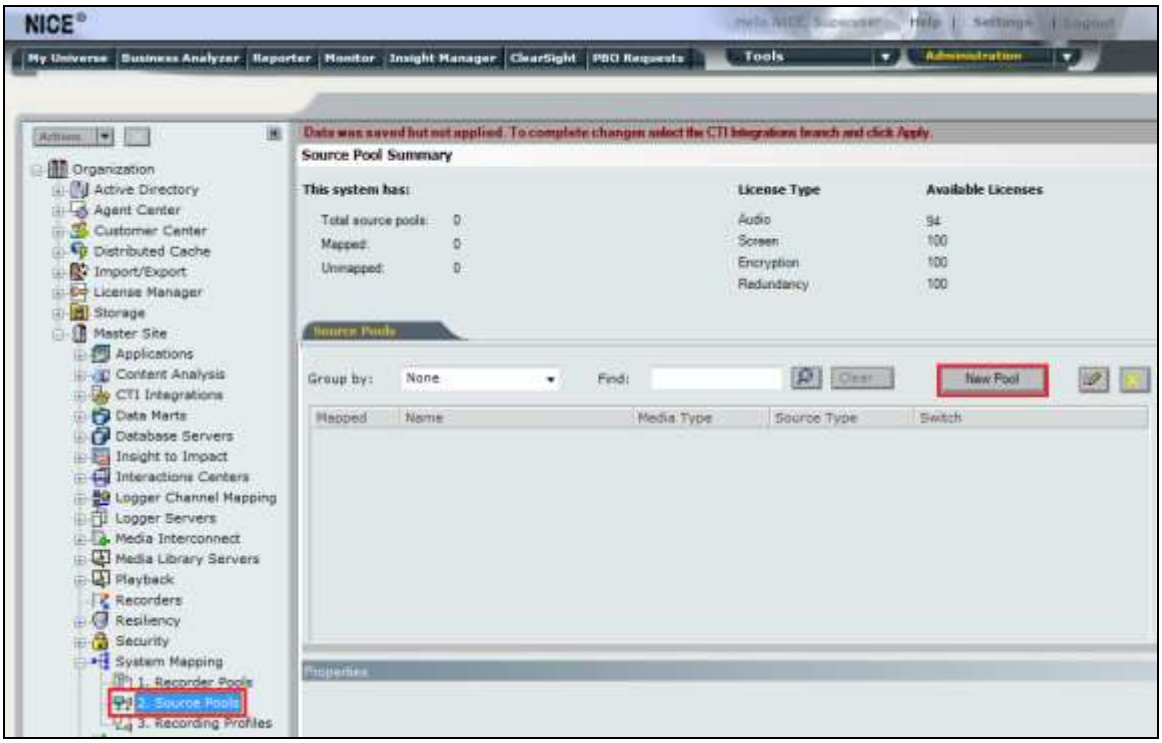
From the web browser navigate to **Master Site → System Mapping → Recorder Pools**. In the main window click on **New Pool**.



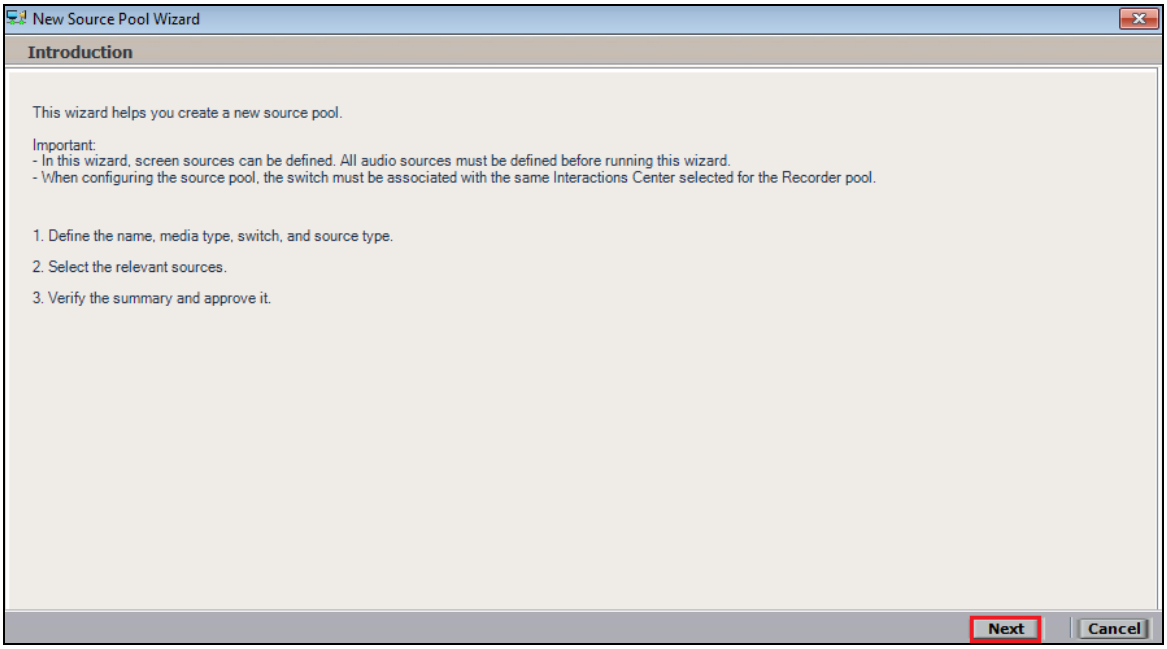
Enter a suitable **Name** for the **Recorder Pool** and select the **Passive_Logger** from the list of **Available Recorders** and click on **Update** to continue.



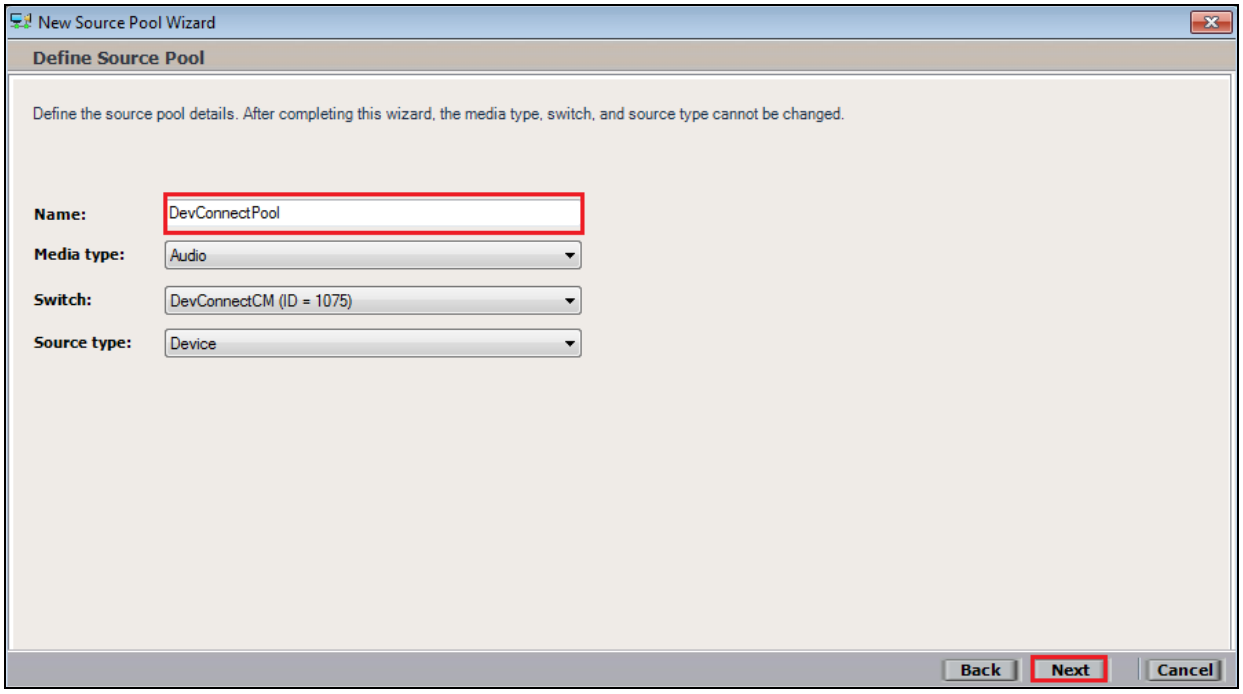
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



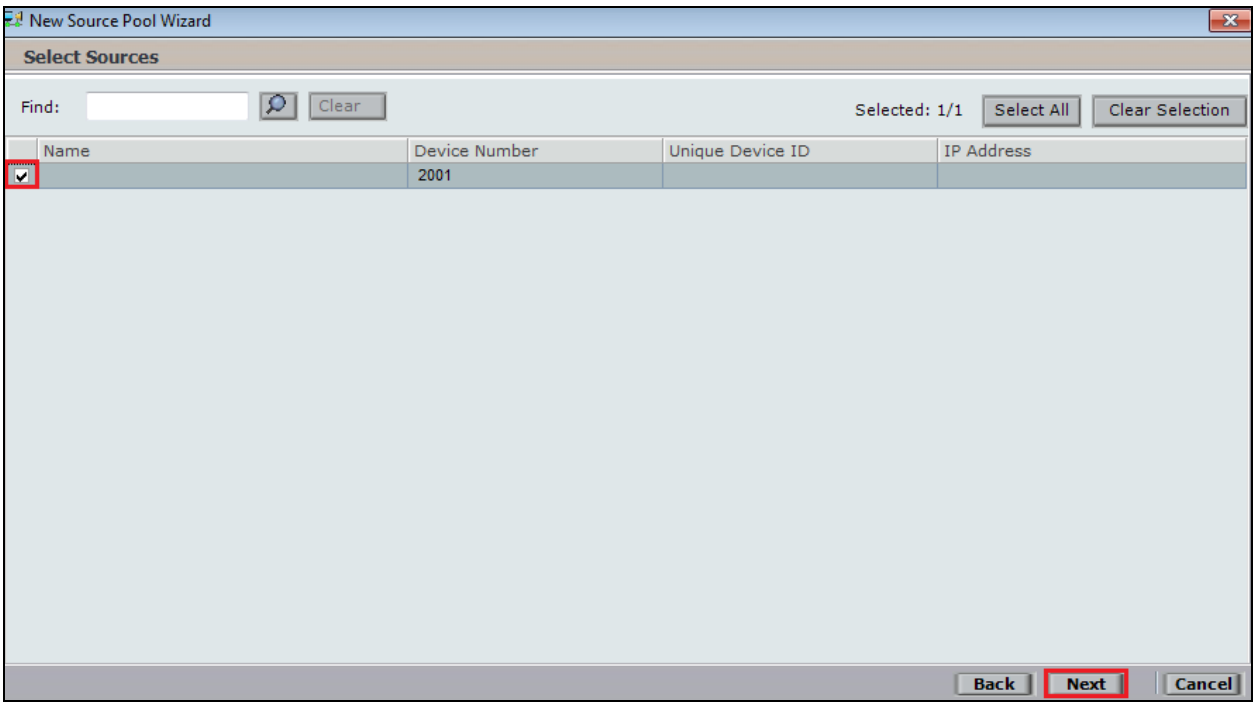
Click on **Next** to continue to add a new **Source Pool.**



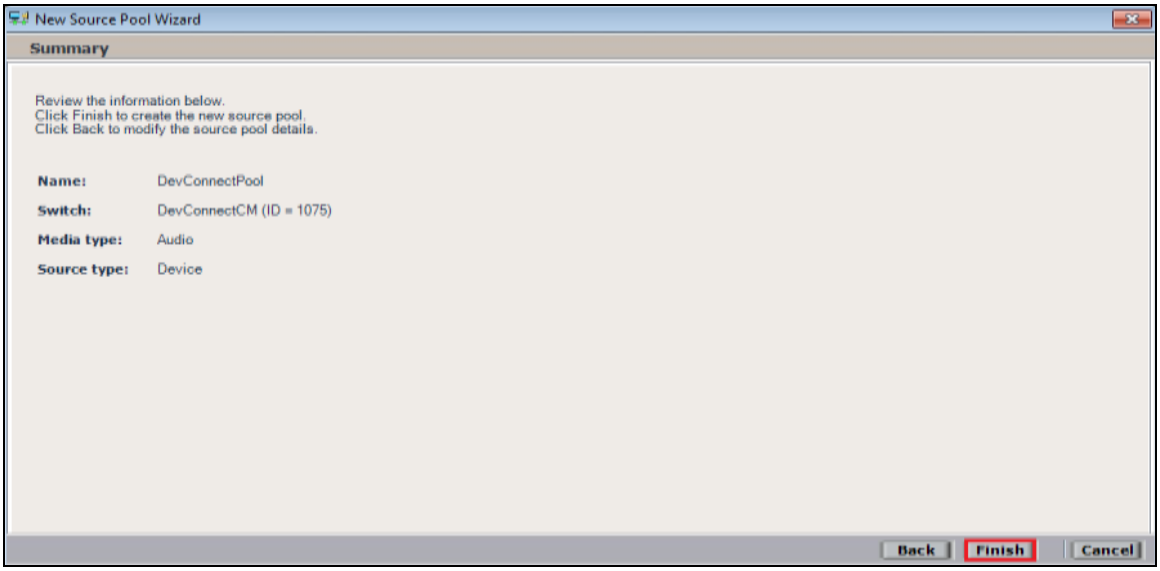
Enter a suitable **Name** and the other values were left as default. Click on **Next** to continue.



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.

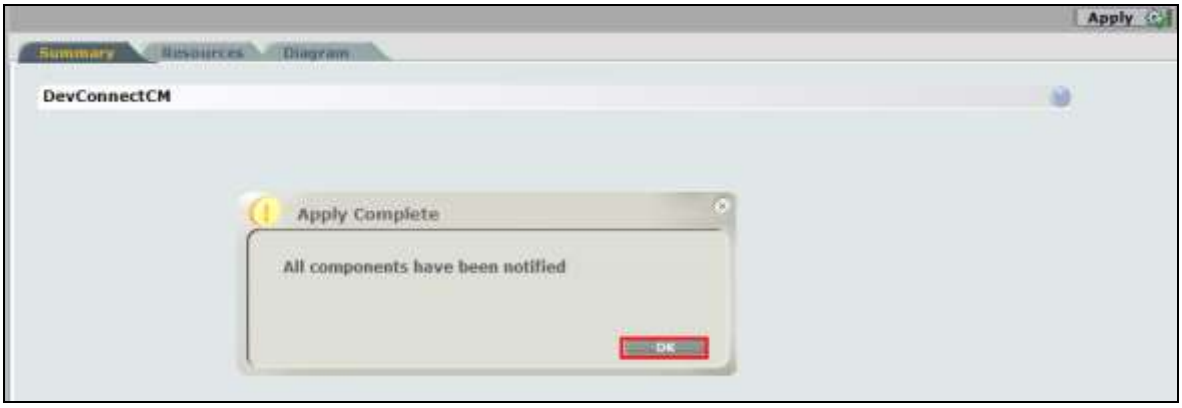


Click on **Finish** to complete the **New Source Pool Wizard**.

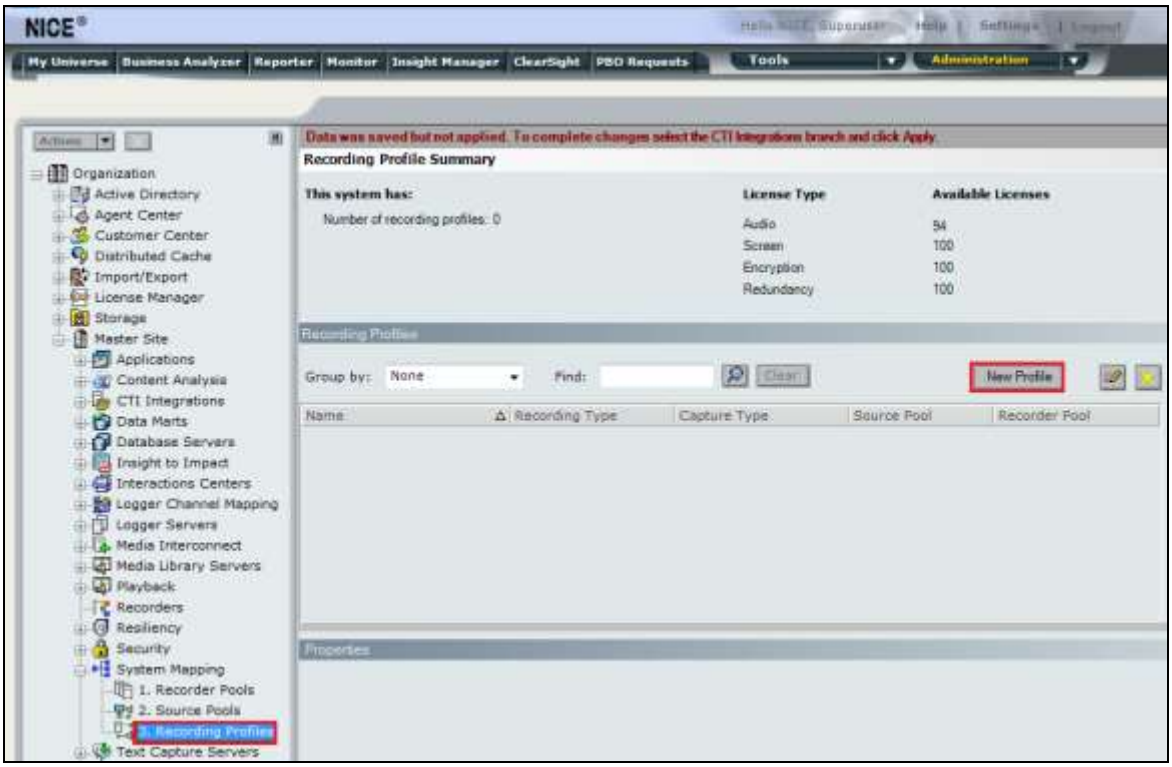


To implement these new changes, navigate to **Master Site → CTI Integrations** in the left window and in the main window click on **Apply** at the top right of the window.

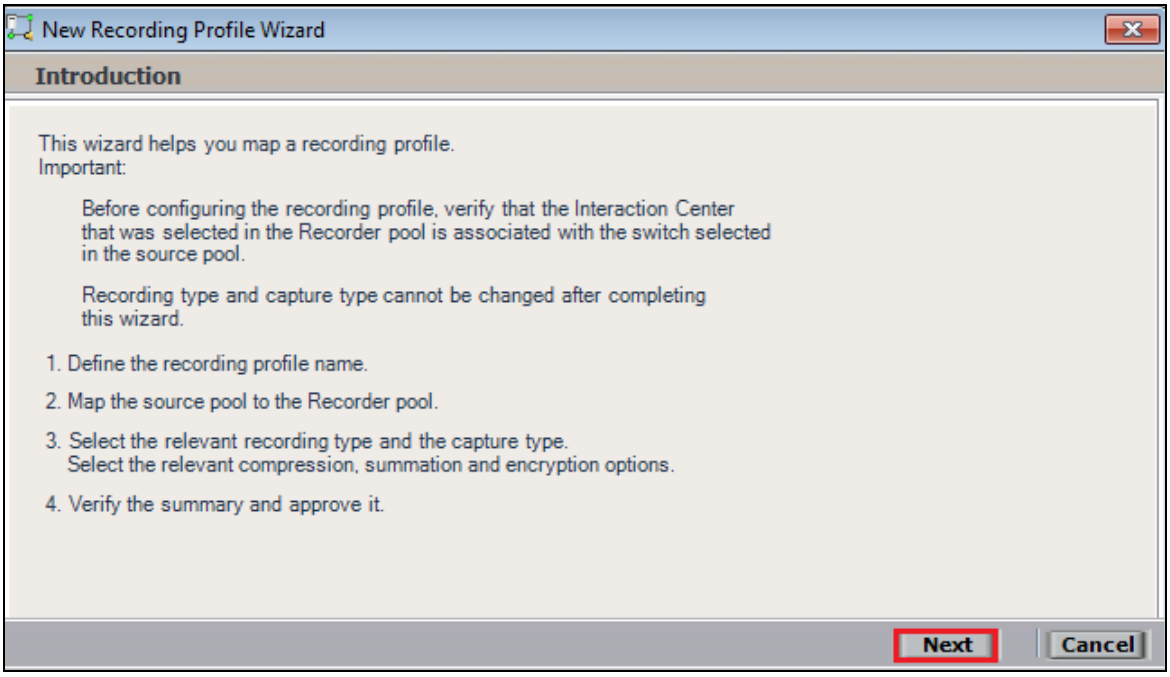
The following screen shows the changes were saved correctly. Click on **OK** to continue.



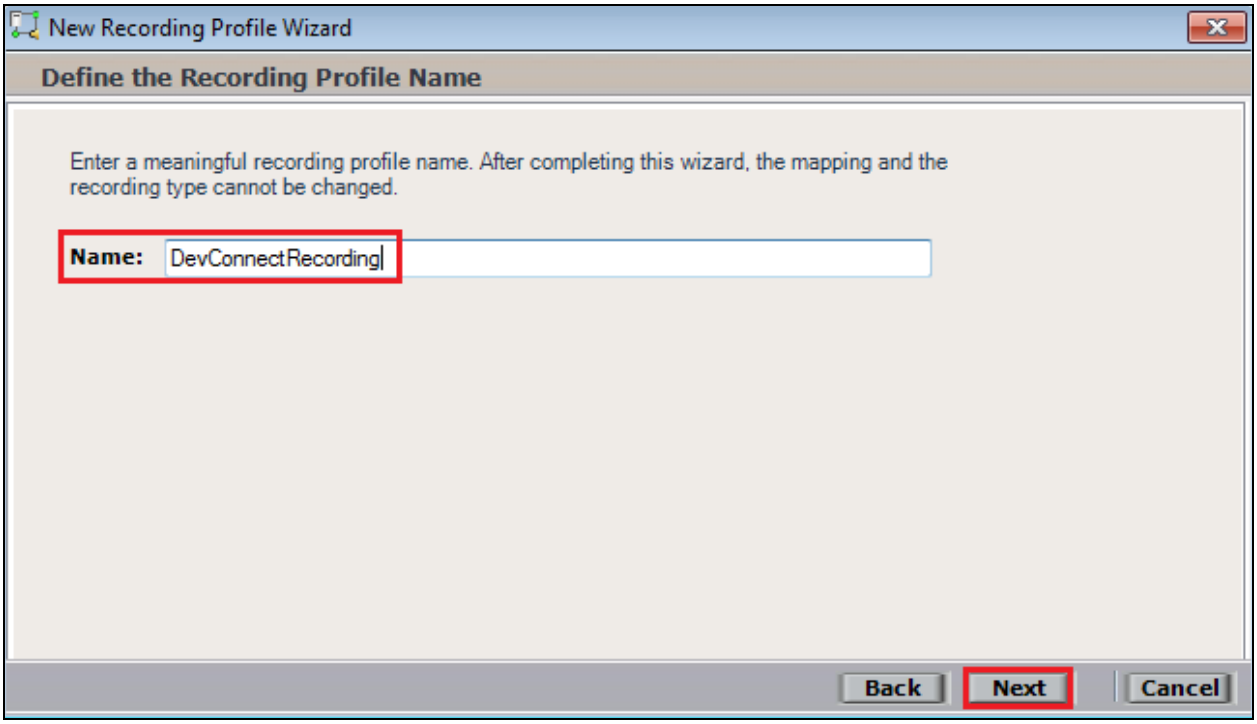
From the left window navigate to **Master Site → System Mapping → Recording Profiles** and in the main window click on **New Profile**.



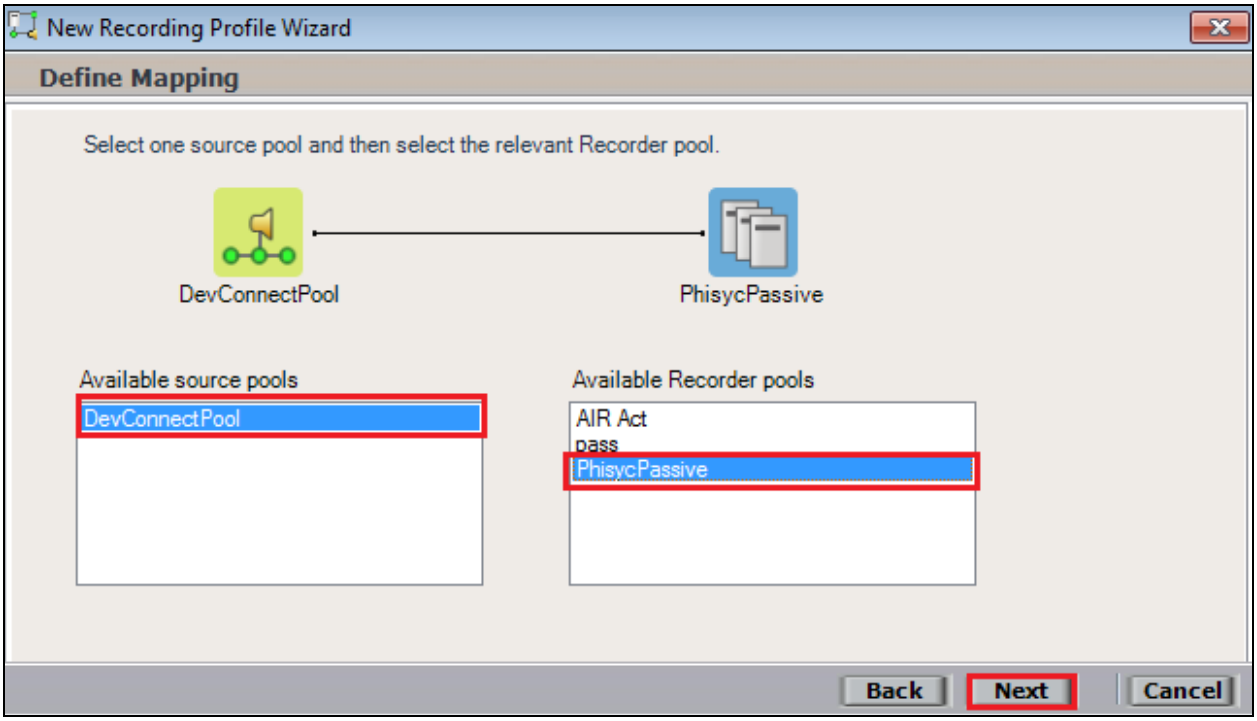
Click on **Next** to continue with the **New Recording Profile Wizard**.



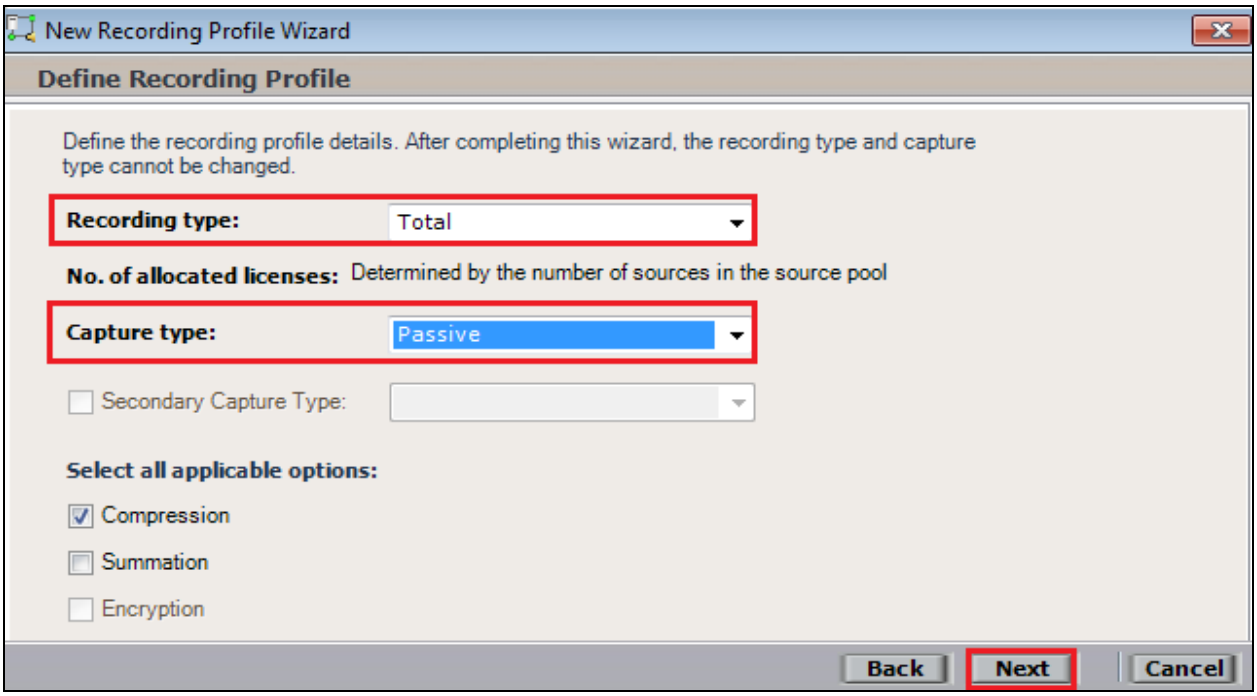
Enter a suitable **Name** for the Recording profile.



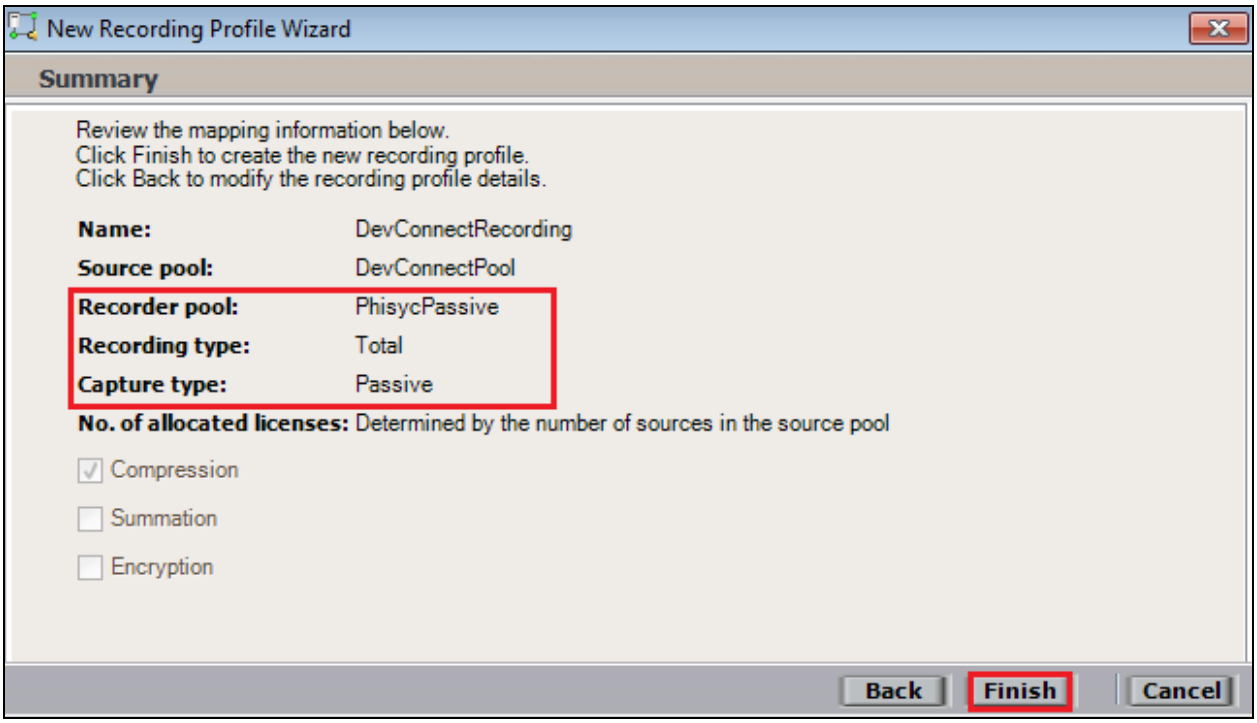
Select the correct **source pool** and **Recorder pool**, click **Next** to continue. The recorder pool below shows **Phisyc Passive** but this should be the Recorder pool that was created above and in this case will be **pass**.



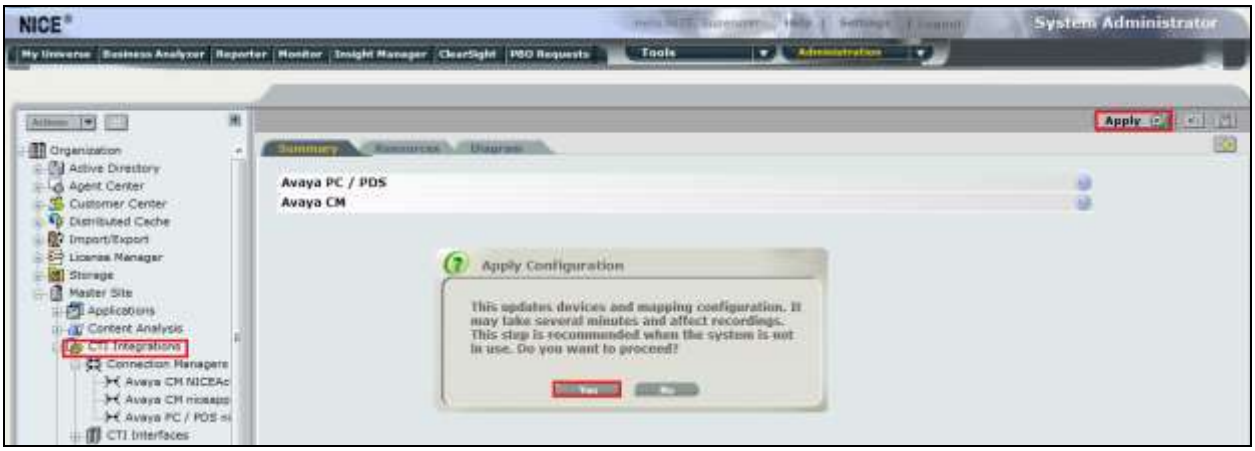
For total recording i.e., the recording of all calls, select **Total** as the **Recording type**. For **Capture type**, ensure that **Passive** is selected from the drop-down box. Compression is selected as default and can be left like this. Click on **Next** to continue.



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



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



This concludes the setup of the NICE Application Server for Passive Station Side VoIP SMS recording.

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager CTI Service State

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

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1          4        no      aes63vmpg      established    18        18
```

8.2. Verify TSAPI Link

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

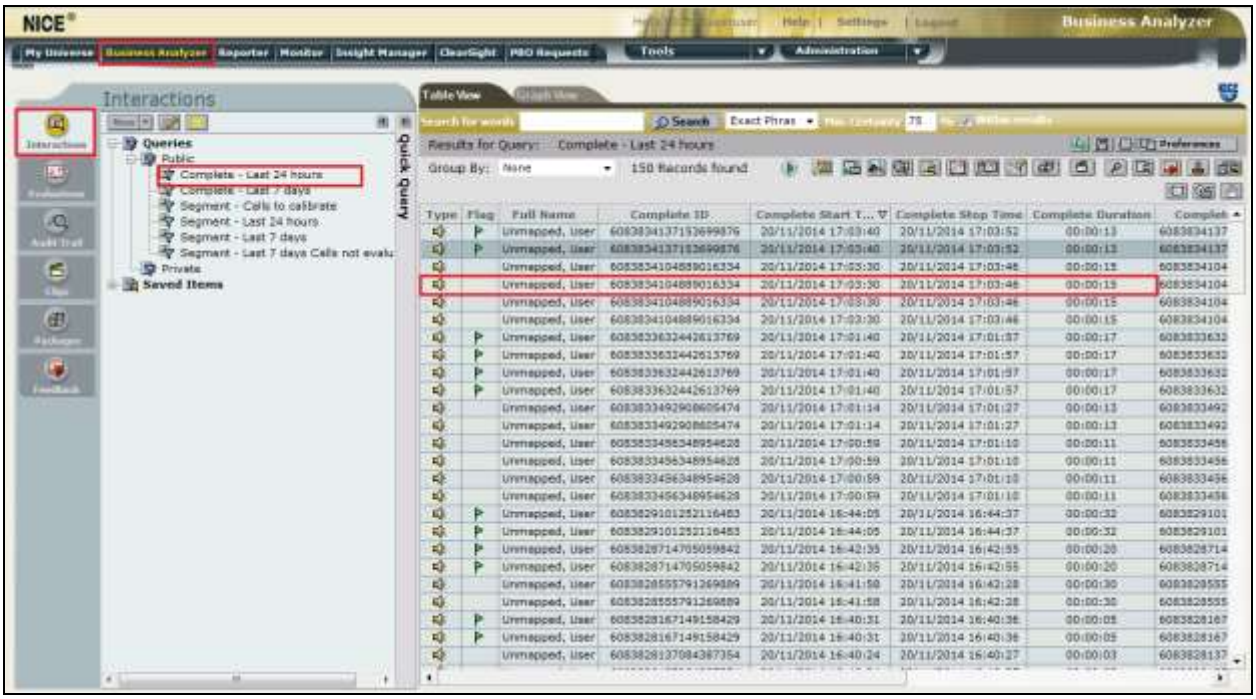
8.3. Verify calls are being recorded

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

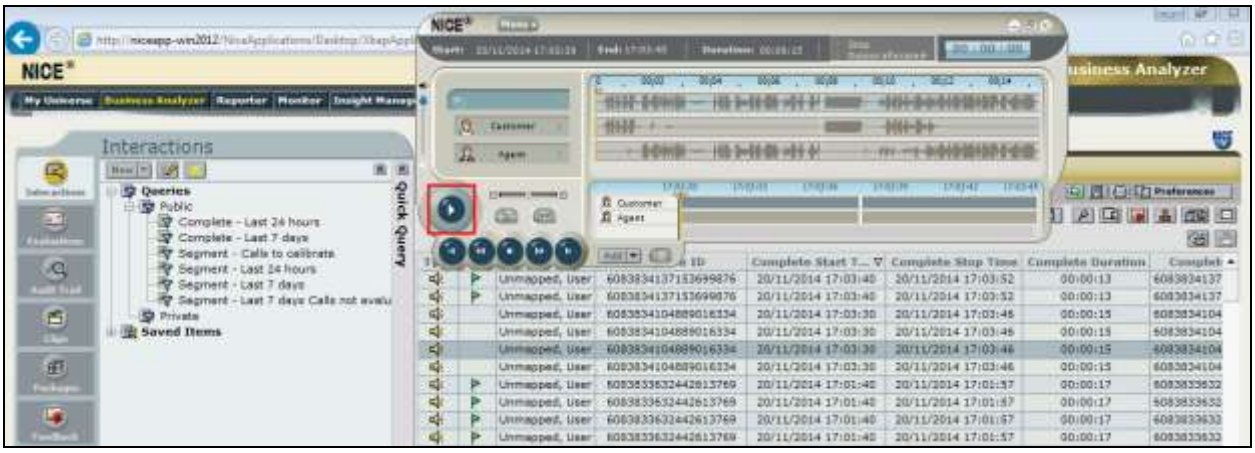
Open a browser session to the NICE Application Server as is shown below. Enter the proper credentials and click on **Login**.

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

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

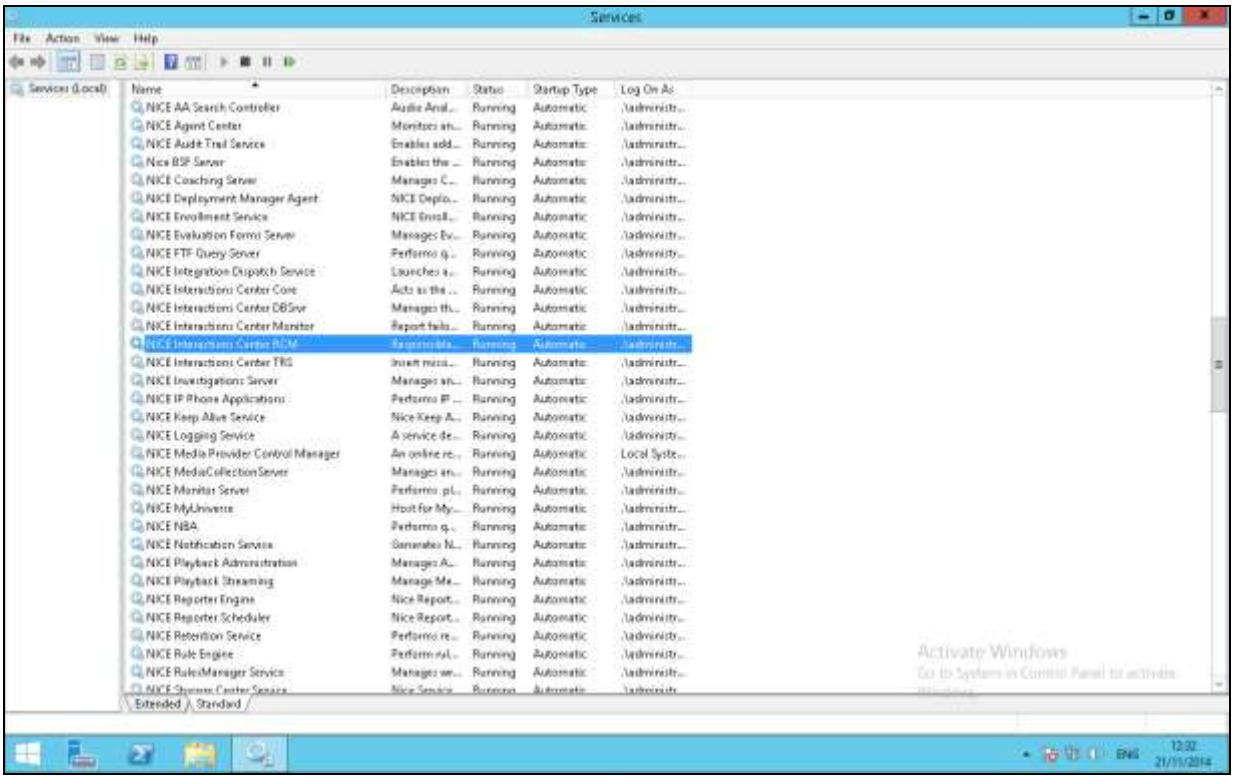


The NICE player is opened and the recording is presented for playback. Click on the **Play** icon highlighted below to play back the recording.



8.4. Verify NICE Services

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



9. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform to successfully interoperate with Avaya Aura® Communication Manager R6.3 using Avaya Aura® Application Enablement Services R6.3 to connect to using Passive Station Side VoIP with SMS to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

10. Additional References

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

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

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

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

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 6.3*

[4] *Avaya Aura® Session Manager Overview*, Doc *# 03603323Avaya Aura ® Contact Centre SIP Commissioning, Doc # NN44400-511, Release 6.3*

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

Appendix

Avaya one-X® Agent Softphone

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

```
display station 2100                                            Page   1 of   5
                                     STATION

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

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

                                             Customizable Labels? Y
```

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

```
display station 2100                                          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 9620 H.323 Deskphone

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

```
display station 2000                                          Page   1 of   5
                                     STATION

Extension: 2000                          Lock Messages? n               BCC: 0
     Type: 9620                          Security Code: *                TN: 1
     Port: S00000                      Coverage Path 1: 2               COR: 1
     Name: Paul 2000                   Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                Location:                  Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 2000
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                        IP Video? n
                               Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

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

```
display station 2000                                          Page   3 of   5
                                     STATION

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


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

                              ENHANCED CALL FORWARDING
                                   Forwarded Destination         Active
 Unconditional For Internal Calls To: 4000                          n
                   External Calls To: 4000                          n
          Busy For Internal Calls To: 4202                          n
                   External Calls To: 4202                          n
      No Reply For Internal Calls To: 2101                          n
                   External Calls To: 2101                          n

            SAC/CF Override: n
```

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

ABBREVIATED DIALING
     List1:                    List2:                    List3:




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


    voice-mail
```

Avaya Agent LoginID

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

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

                Login ID: 4400                                       AAS? n
                    Name: Paul                                      AUDIX? n
                      TN: 1                                LWC Reception: spe
                     COR: 1                      LWC Log External Calls? n
           Coverage Path:                       AUDIX Name for Messaging:
           Security Code:
                                         LoginID for ISDN/SIP Display? n
                                                             Password:
                                               Password (enter again):
                                                          Auto Answer: station
                                                    MIA Across Skills: system
                                             ACW Agent Considered Idle: system
                                             Aux Work Reason Code Type: system
                                               Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                               Forced Agent Logout Time:   :
```

```
display agent-loginID 4400                                          Page   2 of   3
                                  AGENT LOGINID
      Direct Agent Skill:                                  Service Objective? n
Call Handling Preference: skill-level                   Local Call Preference? n

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

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.