Avaya Solution & Interoperability Test Lab

Application Notes for NICE Engage Platform R7.3 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using DMCC Service Observing and Single Step Conference - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the NICE Engage Platform R7.3 to interoperate with Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1, and Avaya Aura® Application Enablement Services R10.1 using DMCC Service Observing and Single Step Conference to record telephone calls.

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.

©2023 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps for the NICE Engage Platform R7.3 to interoperate with Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1, and Avaya Aura® Application Enablement Services R10.1. NICE Engage Platform uses either Avaya Aura® Communication Manager Service Observing feature or Single Step Conference feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services Application Programming Interface (TSAPI) to capture the audio and call details for call recording on various Communication Manager endpoints, listed in **Section 4**.

The TSAPI integration allows NICE Engage Platform to receive call-related events and metadata from AES. This integration must be paired with an audio capture method, in this case DMCC Service Observing feature or Single Step Conference to provide an audio source for recordings.

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 AES DMCC to 'Observe' the target extension using Virtual Extensions on Communication Manager to do so. When the target extension joins a call, the application using Service Observing receives the call's aggregated RTP media stream via the recording device and records the call.

NICE Engage Platform provides the ability to record multi-channel interactions across the organization for regulatory compliance and to utilize these interactions for multiple business applications in order to extract insights and gain value. The platform tightly integrates with the telephony environment via CTI, APIs and SIP and stores the metadata in a single recording platform to ensure regulatory adherence and standardized workforce optimization processes across multiple channels. It provides comprehensive search tools and media retrieval, as well as a wide variety of Real-Time capabilities for PCI compliance and advanced applications.

The NICE Engage Platform uses the Communication Manager Service Observing feature to observe an extension on a call; this way the call is recorded and can be played back at a later time. NICE can also conference into the call and record the call using this method. Both methods of call recording use virtual stations on Communication Manager in order to observe or conference into existing calls to record them.

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 Service Observation and Single Step Conference 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

©2023 Avaya Inc. All Rights Reserved.

the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and NICE Engage Platform did not include use of any specific encryption features as requested by NICE.

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.
- **EC500 Calls/Forwarded calls -** Test call recording for calls terminated on Avaya DECT handsets using EC500.
- **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 Avaya Agent for Desktop.
- **Serviceability testing -** The behavior of NICE Engage Platform under different simulated failure conditions.

©2023 Avaya Inc. All Rights Reserved.

2.2. Test Results

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

- An issue was observed when a SIP phone made a supervised transfer using all monitored phones where the “Service Observer” was not dropped from the call upon completion of the transfer. The call scenario is A calls B (SIP Phone) and B then transfers A to C. A and C are now talking, when A hangs up the display on C changes to that of the “virtual station” and same if C hangs up first then the display of A shows the “virtual station”. The call is cleared when the second person (A or C) hangs up. This is not the same as if a H.323 makes the transfer. This issue appears when using Service Observation where all extensions are being observed constantly. Avaya investigated the issue and indicated it was working as designed.

2.3. Support

Technical support can be obtained for NICE Engage Platform from the website https://www.nice.com/contact-us

©2023 Avaya Inc. All Rights Reserved.

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Engage platform with the Avaya solution using DMCC Service Observing and Single Step Conference to record calls. The NICE Application server is set up for DMCC Service Observe and Single Step Conference mode and connects to AES.

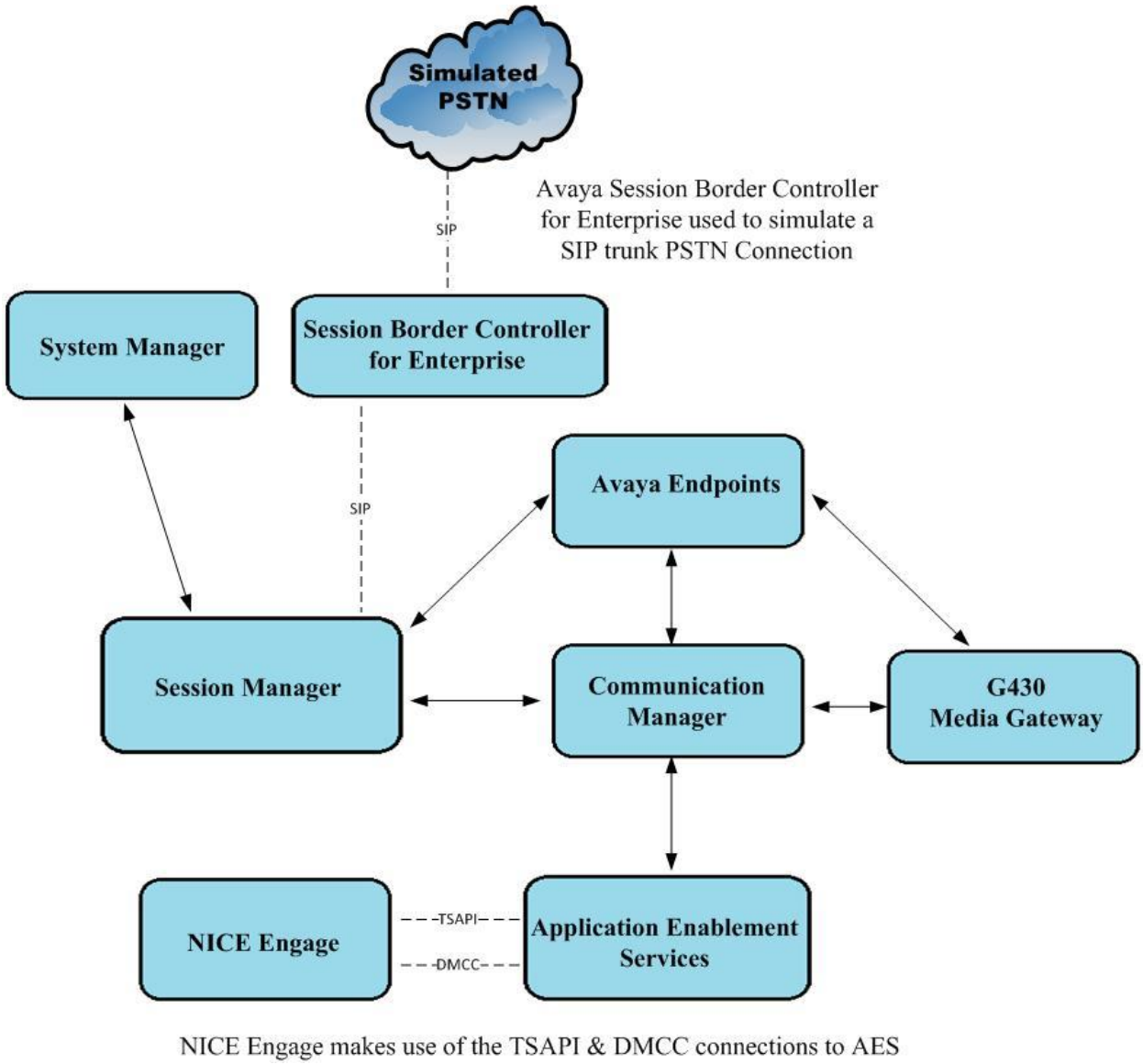


Figure 1: Connection of NICE Engage Platform R7.3 with Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1 and Avaya Aura® Application Enablement Services R10.1

©2023 Avaya Inc. All Rights Reserved.

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	System Manager 10.1.0.2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Service Pack 2
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0.2.0 – SP2 R020x.01.0.974.0 Update ID 01.0.974.0-27607
Avaya Aura® Application Enablement Services	10.1.0 Build 10.1.0.2.0.12-0
Avaya Aura® Media Server	10.1.0.101
Avaya G430 Media Gateway	42.7.0 /2
Avaya 9404 Digital Phones	17.0
Avaya J100 Series Phones (SIP)	7.1.2.0.14
Avaya J100 Series Phones (H.323)	7.0.14.0.7
Avaya Agent for Desktop (SIP)	2.0.6.23.3005
Avaya Workplace (SIP)	3.26.0.64
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	10.1.0
NICE Engage - NICE Engage Application Server - NICE Advanced Interactions Recording Server - NICE Engage NDM Server	7.3

All equipment is running on virtual servers on VMware.

©2023 Avaya Inc. All Rights Reserved.

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 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

```
display system-parameters customer-options                    Page   4 of  12
                              OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y              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? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               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




        (NOTE: You must logoff & login to effect the permission changes.)
```

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

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

```
display node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                IP Address
SM100                10.10.40.12
aespri101x           10.10.40.16
default              0.0.0.0
g450                 10.10.40.15
procr                10.10.40.13
```


©2023 Avaya Inc. All Rights Reserved.

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 **aespri101x**.
- **Password:** Enter a password to be administered on AES.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on AES 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:        aespri101x        ********          y          in use
      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: 1990
     Type: ADJ-IP
                                                                      COR: 1
     Name: aespri101x
```


©2023 Avaya Inc. All Rights Reserved.

5.5. Configure Communication Manager for Service Observing

Type display cor x, where x is the COR number in the screen above, to check the existing Class of Restriction. Ensure that **Can be Service Observed** and **Can Be A Service Observer** are set to **y**, if not type **change cor x** to make a change to the Class or Restriction. These values need to be enabled in order for Service Observe to work for call recording.

```
display cor 1                                                  Page 1 of 23
                            CLASS OF RESTRICTION
               COR Number: 1
          COR Description:

                       FRL: 0                                 APLT? y
  Can Be Service Observed? y           Calling Party Restriction: all-toll
Can Be A Service Observer? y            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? y
     Restriction Override: all        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n
   Unrestricted Call List: 1
           Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7           Hear VDN of Origin Annc.? n
         Send ANI for MFE? n            Add/Remove Agent Skills? n
            MF ANI Prefix:             Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                         Can Be Picked Up By Directed Call Pickup? y
                                    Can Use Directed Call Pickup? y
                                    Group Controlled Restriction: inactive
```

Type **change system-parameters features**, on **Page 11** ensure that **Allow Two Observes in Same Call** is set to **y**.

```
change system-parameters features                              Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                    Delay:
    Message Waiting Lamp Indicates Status For: station
  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
               Converse Signaling Tone (msec): 100         Pause (msec): 70
                     Prompting Timeout (secs): 10
                  Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                              BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? y     or Conference Tone? n
 Service Observing/SSC Allowed with Exclusion? n
             Allow Two Observers in Same Call? y
```


©2023 Avaya Inc. All Rights Reserved.

Type **change feature-access-codes** to access the feature codes on Communication Manager. Scroll to **Page 5** in order to view or change the **Service Observing** access codes. Note the **Service Observing Listen Only Access Code** is ***56**; this will be required in **Section 7.1** during the setup of NICE Engage Platform.

```
change feature-access-codes                                    Page   5 of  10
                               FEATURE ACCESS CODE (FAC)
                                 Call Center Features
  AGENT WORK MODES
                           After Call Work Access Code: #36
                                  Auto-In Access Code: #38
                                 Aux Work Access Code: #39
                                    Login Access Code: #40
                                   Logout Access Code: #41
                                Manual-in Access Code: #42
  SERVICE OBSERVING
            Service Observing Listen Only Access Code: *56
            Service Observing Listen/Talk Access Code: *57
                Service Observing No Talk Access Code:
   Service Observing Next Call Listen Only Access Code:
 Service Observing by Location Listen Only Access Code:
 Service Observing by Location Listen/Talk Access Code:

  AACC CONFERENCE MODES
                     Restrict First Consult Activation:      Deactivation:
                    Restrict Second Consult Activation:      Deactivation:
```

5.6. Configure H.323 Stations for Service Observing

All endpoints that are to be monitored by NICE will need to have the appropriate Class of Restriction which would be that created in **Section** Error! Reference source not found.. Ensure that COR is set to the correct number. Note the **Security Code** that may be required in **Section** Error! Reference source not found..

```
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
```


©2023 Avaya Inc. All Rights Reserved.

5.7. Configure Virtual Stations for Service Observing and Single Step Conference

Add virtual stations to allow NICE Inform Recorder record calls using Service Observing and Single Step Conference. Type **add station x** where x is the extension number of the station to be configured, also note this extension number for configuration required in **Section** Error! Reference source not found.. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**. Note also the **COR** for the stations, this will be set to that configured in **Section** Error! Reference source not found..

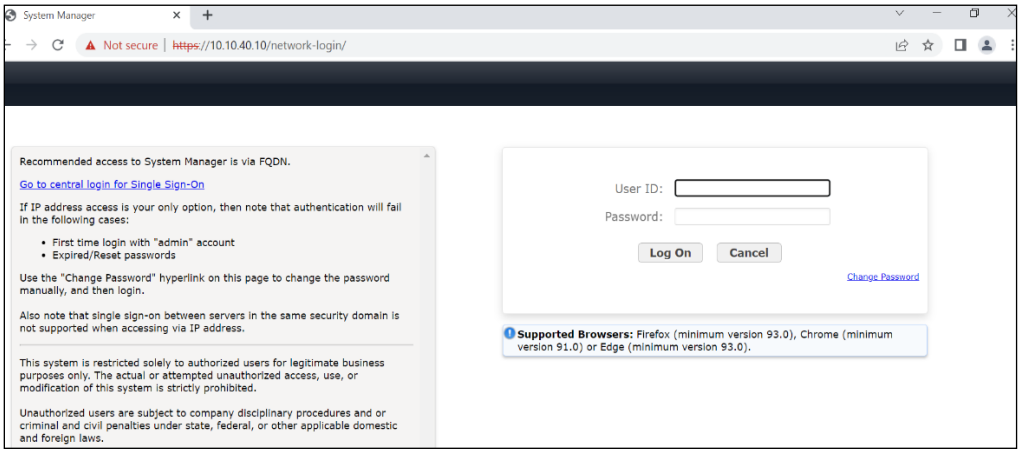
```
add station 33001                                          Page   1 of   6
                                    STATION

Extension: 33001                      Lock Messages? n                BCC: 0
     Type: 9620                       Security Code: 1234             TN: 1
     Port: S00101                     Coverage Path 1:                COR: 1
     Name: Recorder                   Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19         Personalized Ringing Pattern: 1
                                           Message Lamp Ext: 33001
           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
```


©2023 Avaya Inc. All Rights Reserved.

5.8. Configure SIP Stations for Service Observing

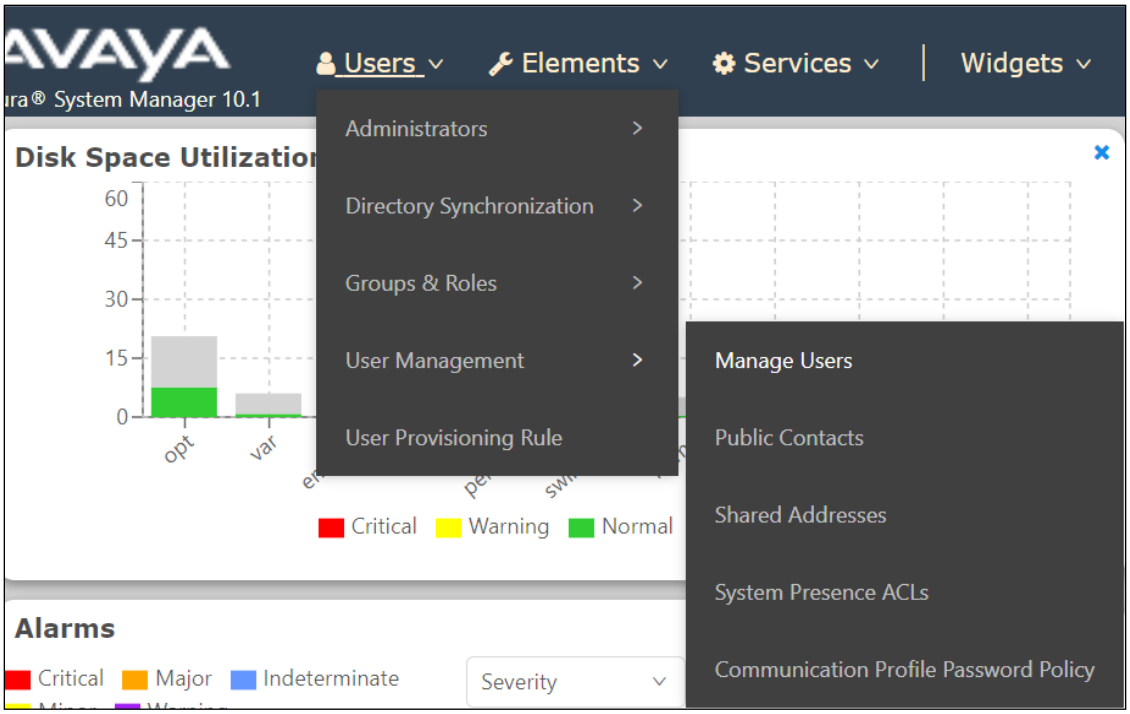
Any SIP extension that is to be recorded requires some configuration changes to allow call recording using service observing. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a web browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **Error! Hyperlink reference not valid. Address >/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.

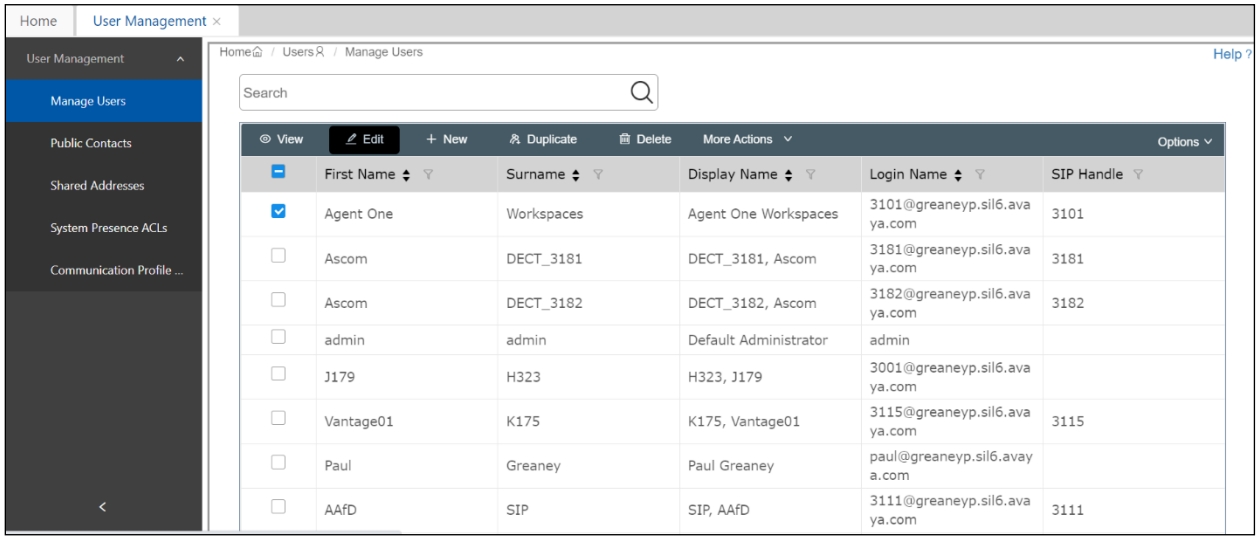


From the home page click on **Users → User Management → Manage Users** as highlighted below.

©2023 Avaya Inc. All Rights Reserved.

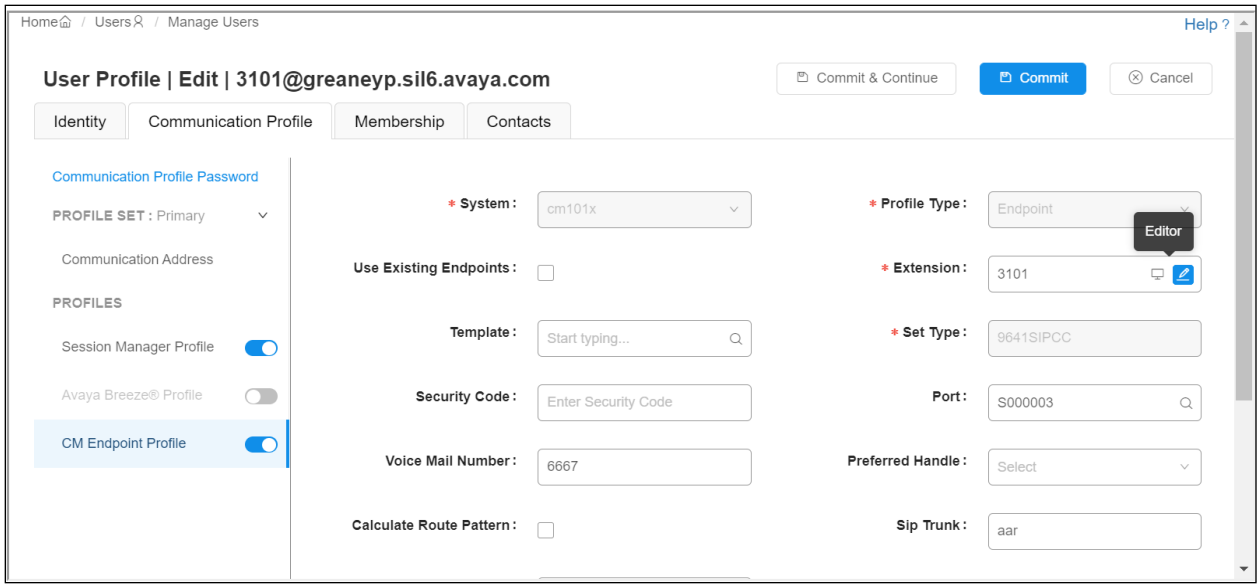


Select the station to be edited and click on **Edit**. The example below shows that SIP extension **3101** is selected.



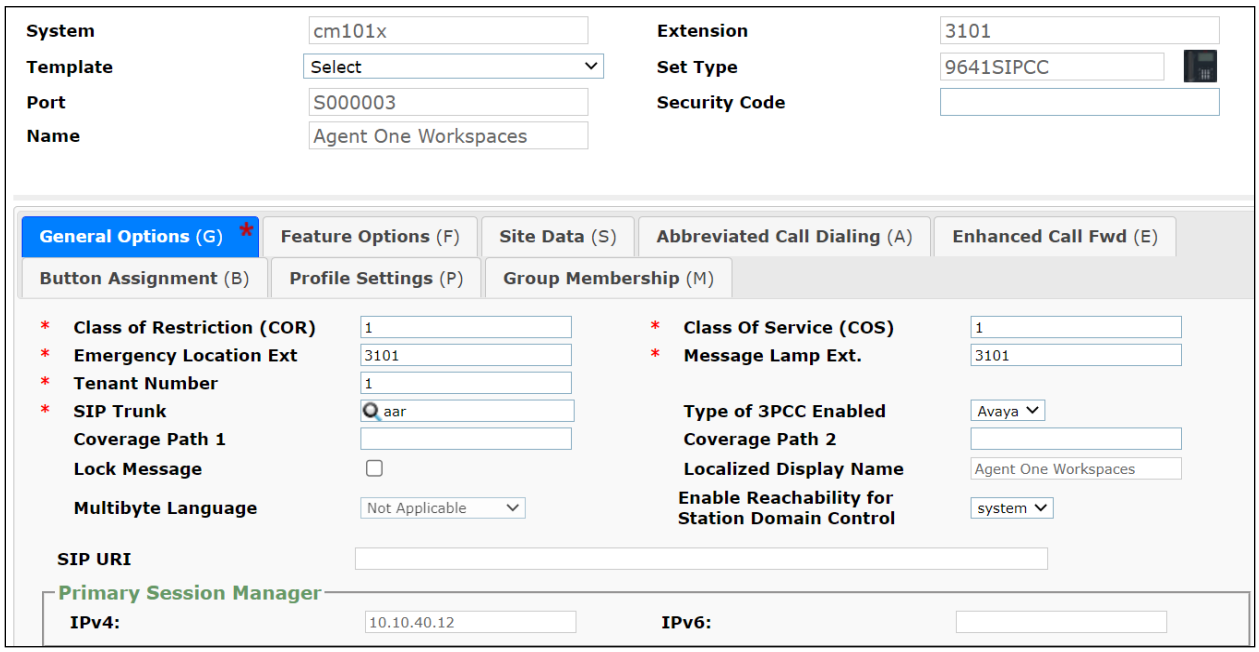
Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.

©2023 Avaya Inc. All Rights Reserved.

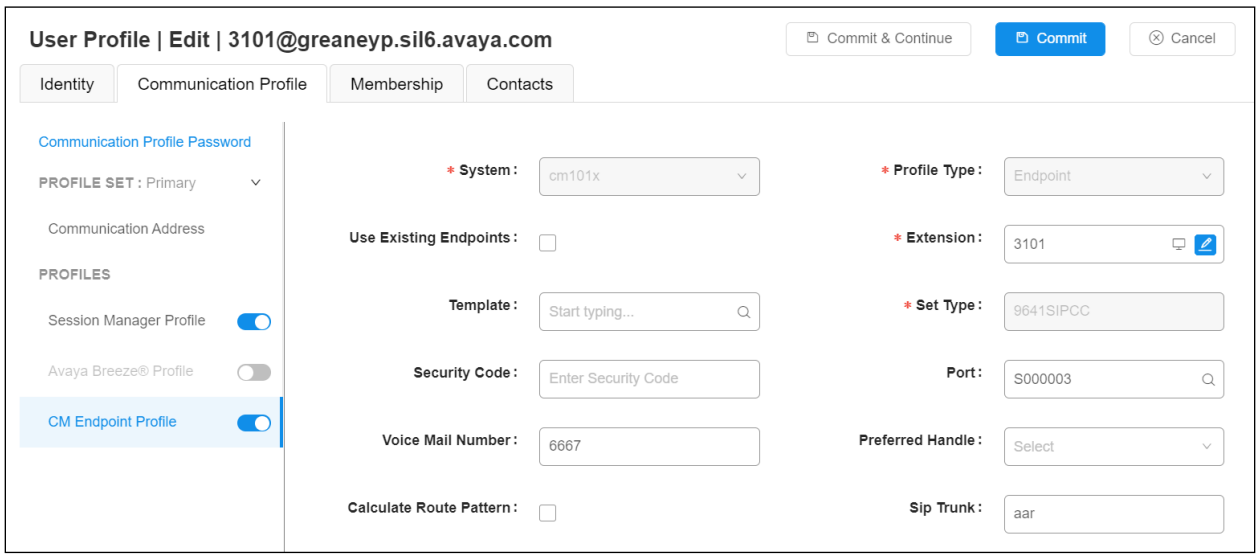


©2023 Avaya Inc. All Rights Reserved.

In the **General Options** tab ensure that **Class of Restriction** is set correctly. Set **Type of 3PCC Enabled** to **Avaya**. Click on **Done**, at the bottom of the screen once this is set, (not shown).



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



©2023 Avaya Inc. All Rights Reserved.

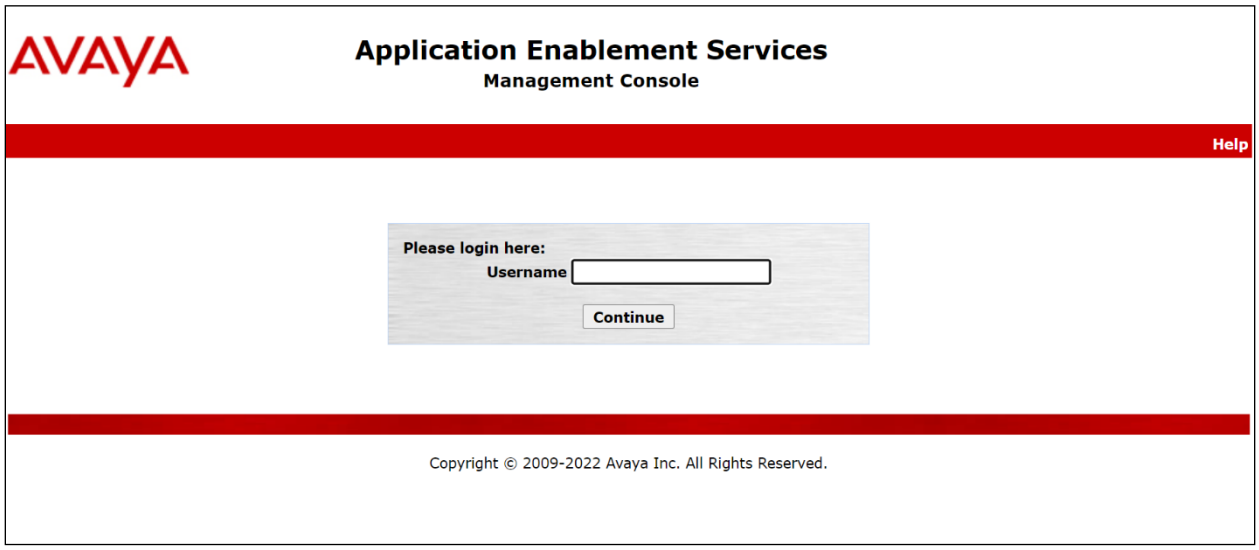
6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI Link
- Identify Tlinks
- Configure Networking Ports
- Create CTI User
- Configure Security
- Restart AE Server

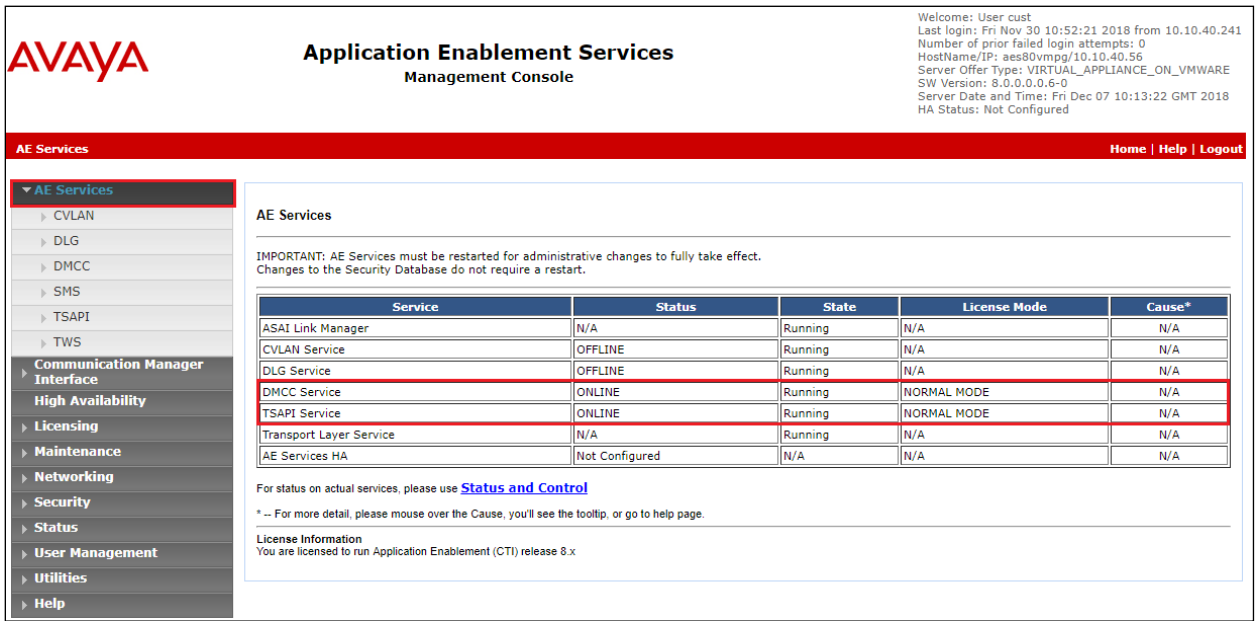
6.1. Verify Licensing

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.

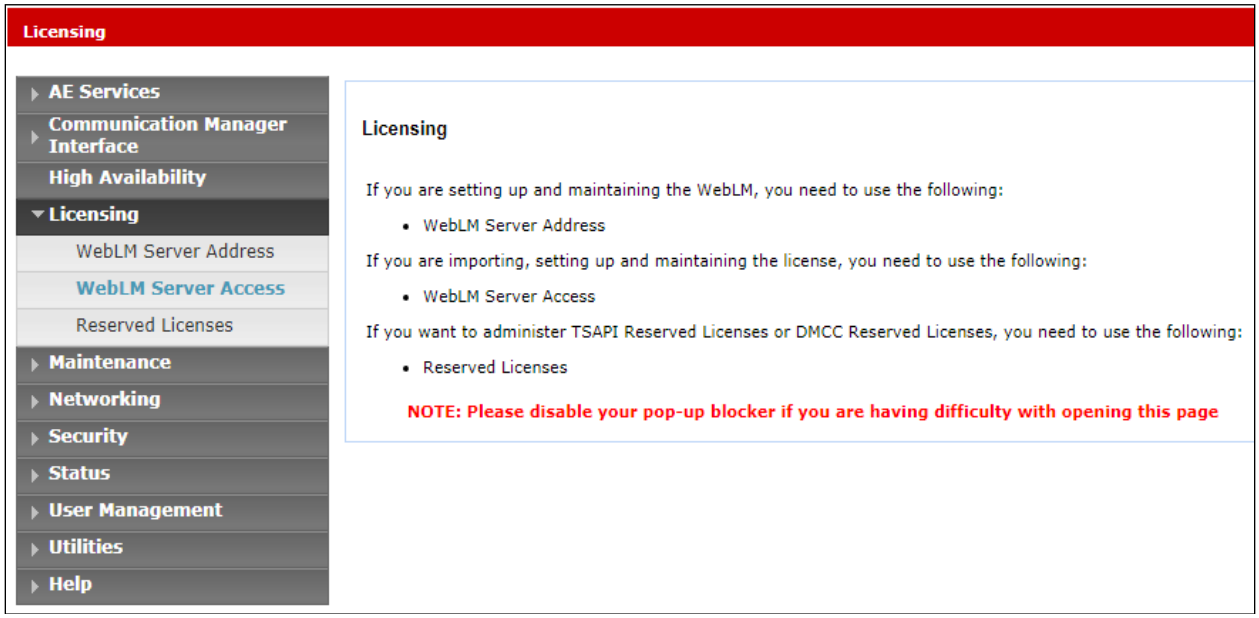


©2023 Avaya Inc. All Rights Reserved.

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

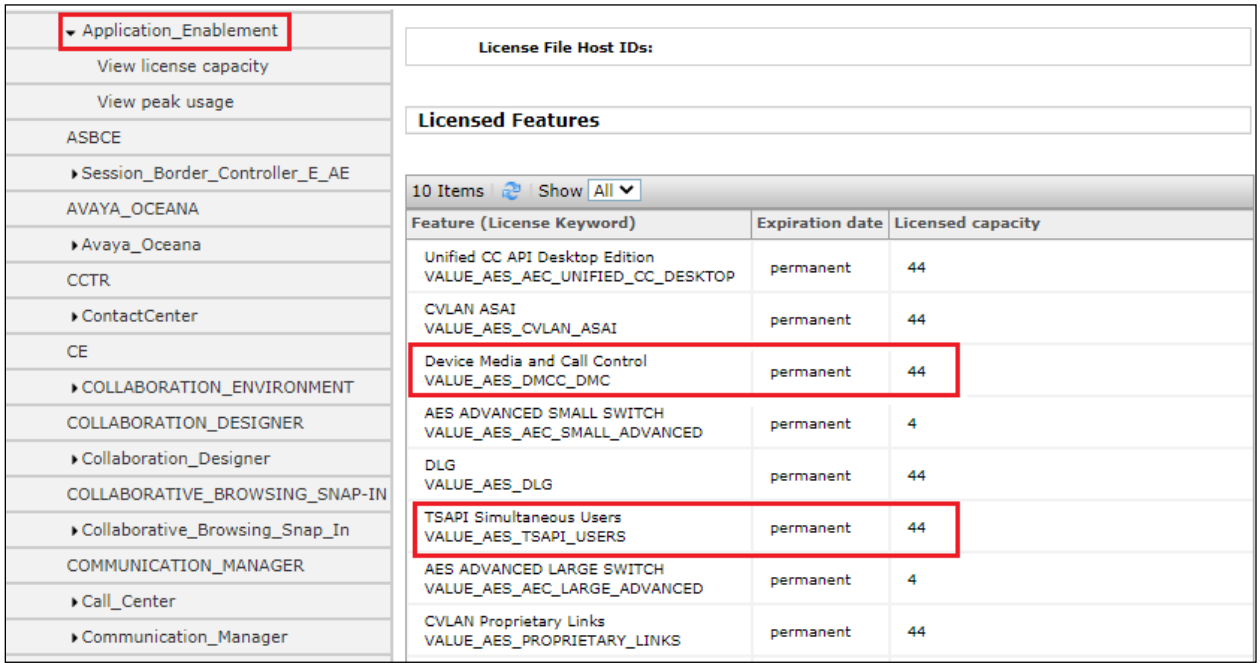


The TSAPI and DMCC licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.



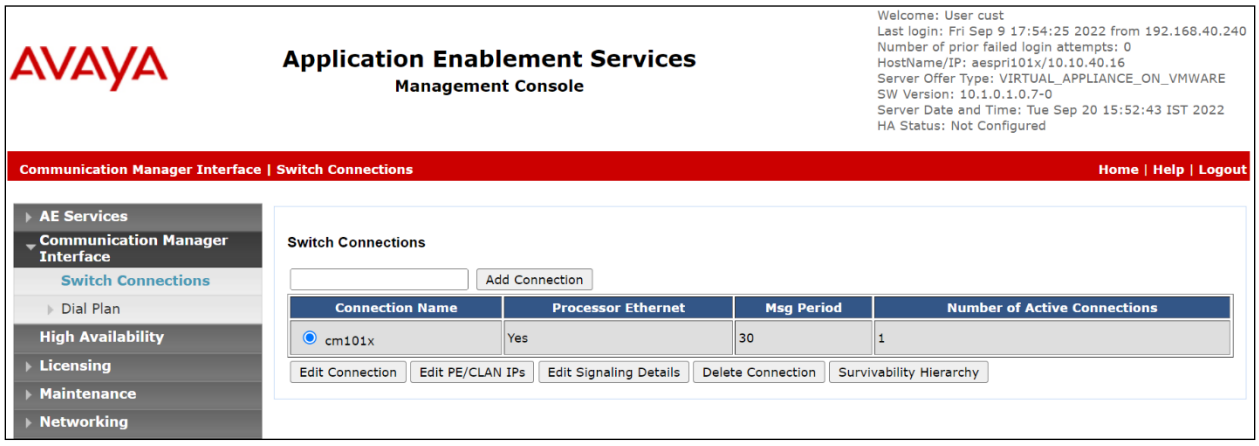
©2023 Avaya Inc. All Rights Reserved.

The following screen shows the available licenses for **TSAPI** and **DMCC** users.



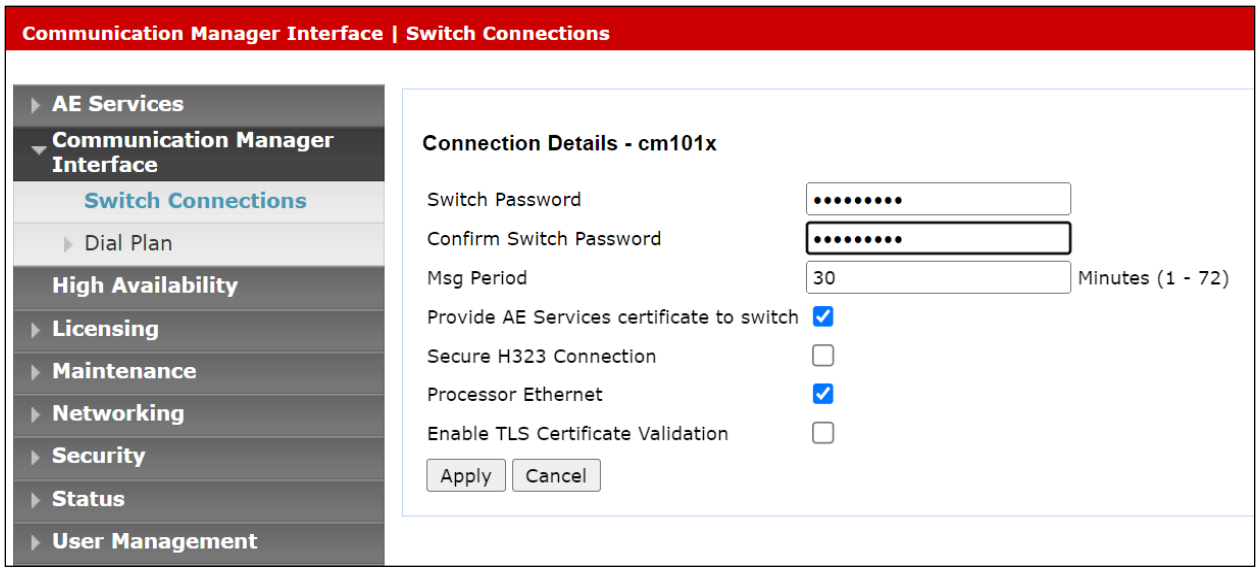
6.2. Create Switch Connection

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.

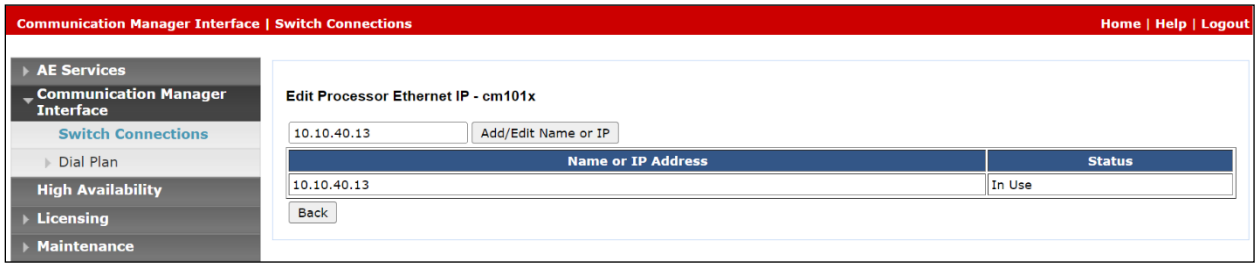


©2023 Avaya Inc. All Rights Reserved.

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.

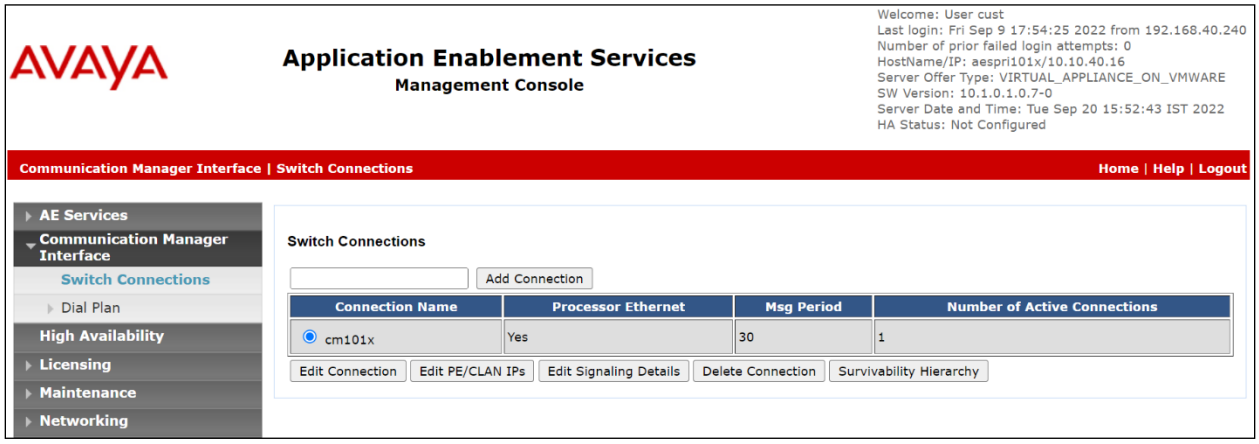


From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button. In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

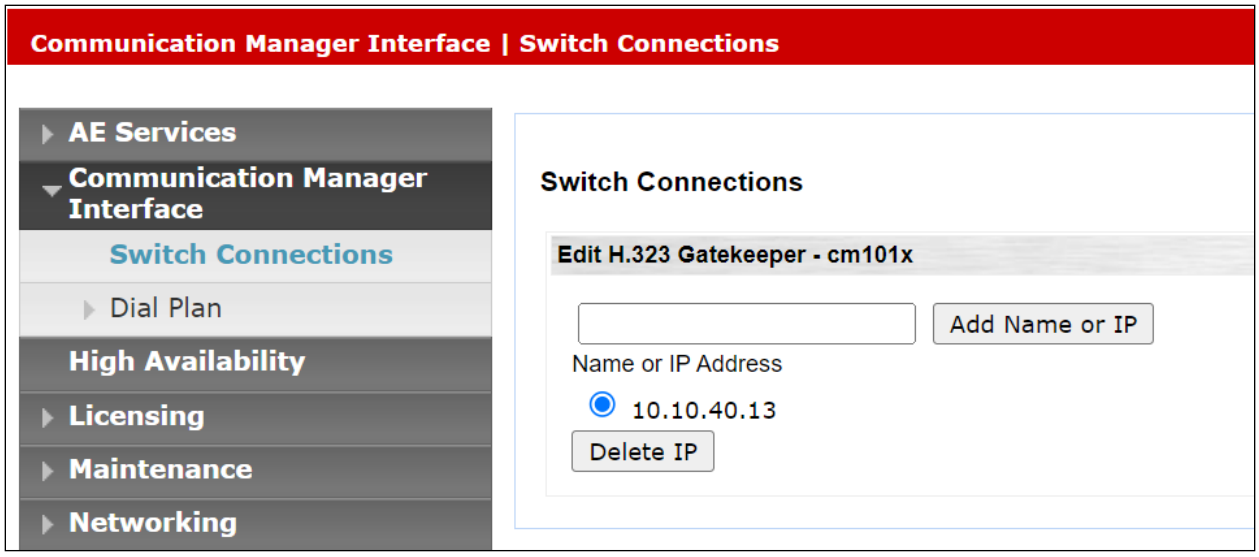


©2023 Avaya Inc. All Rights Reserved.

Clicking on **Edit Signaling Details** below brings up the H.323 Gatekeeper page.



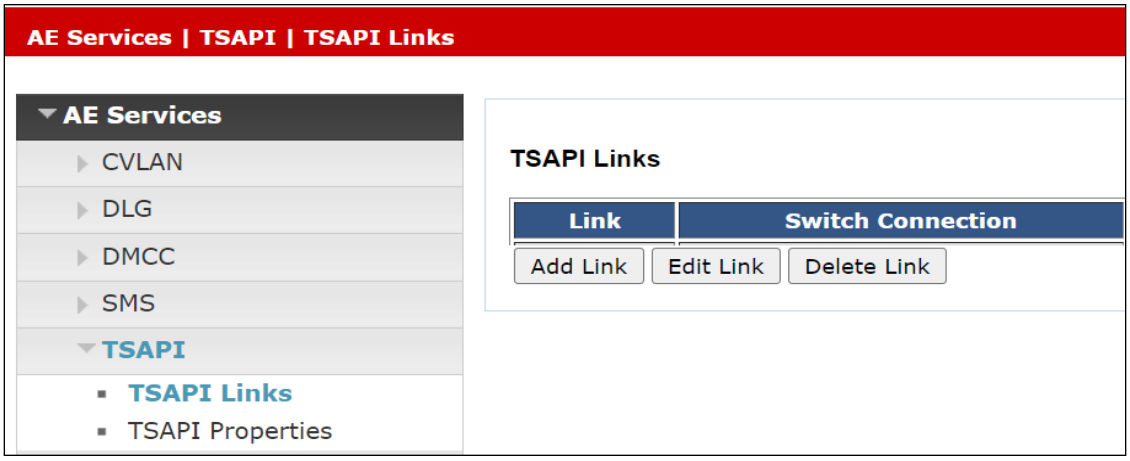
The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.



©2023 Avaya Inc. All Rights Reserved.

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.

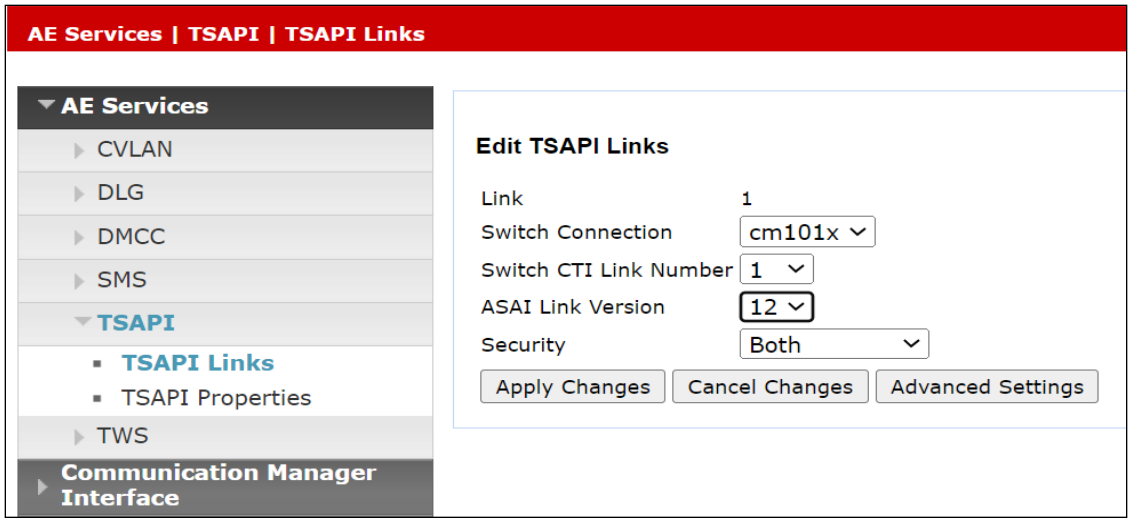


On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm101x**, 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:** Version **12** was used for compliance testing but the latest version available can be chosen.
- **Security:** This can be left at the default value of **both**. An unencrypted TSAPI link was used.

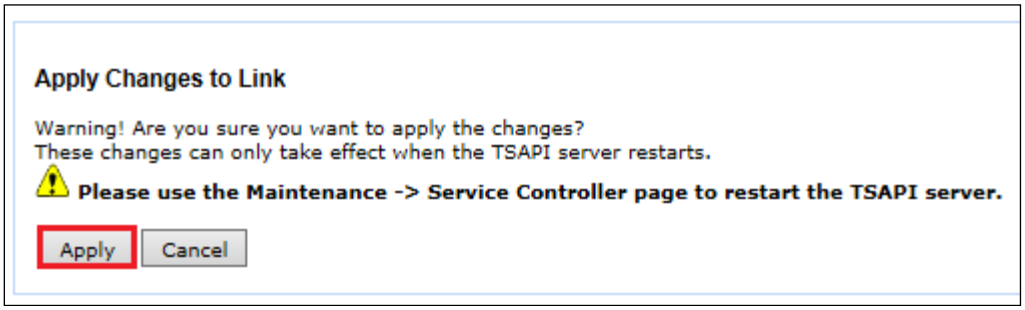
Once completed, select **Apply Changes**.

©2023 Avaya Inc. All Rights Reserved.

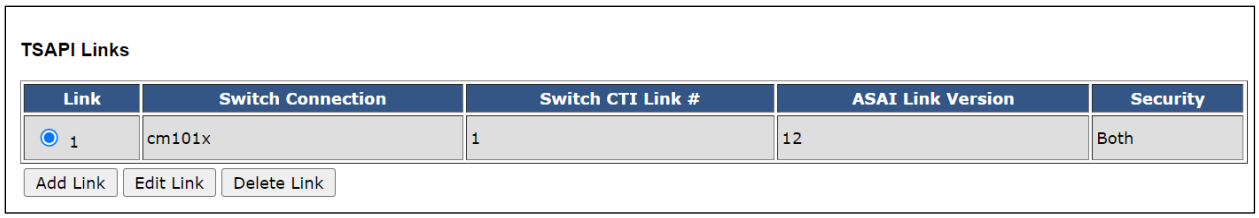


©2023 Avaya Inc. All Rights Reserved.

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



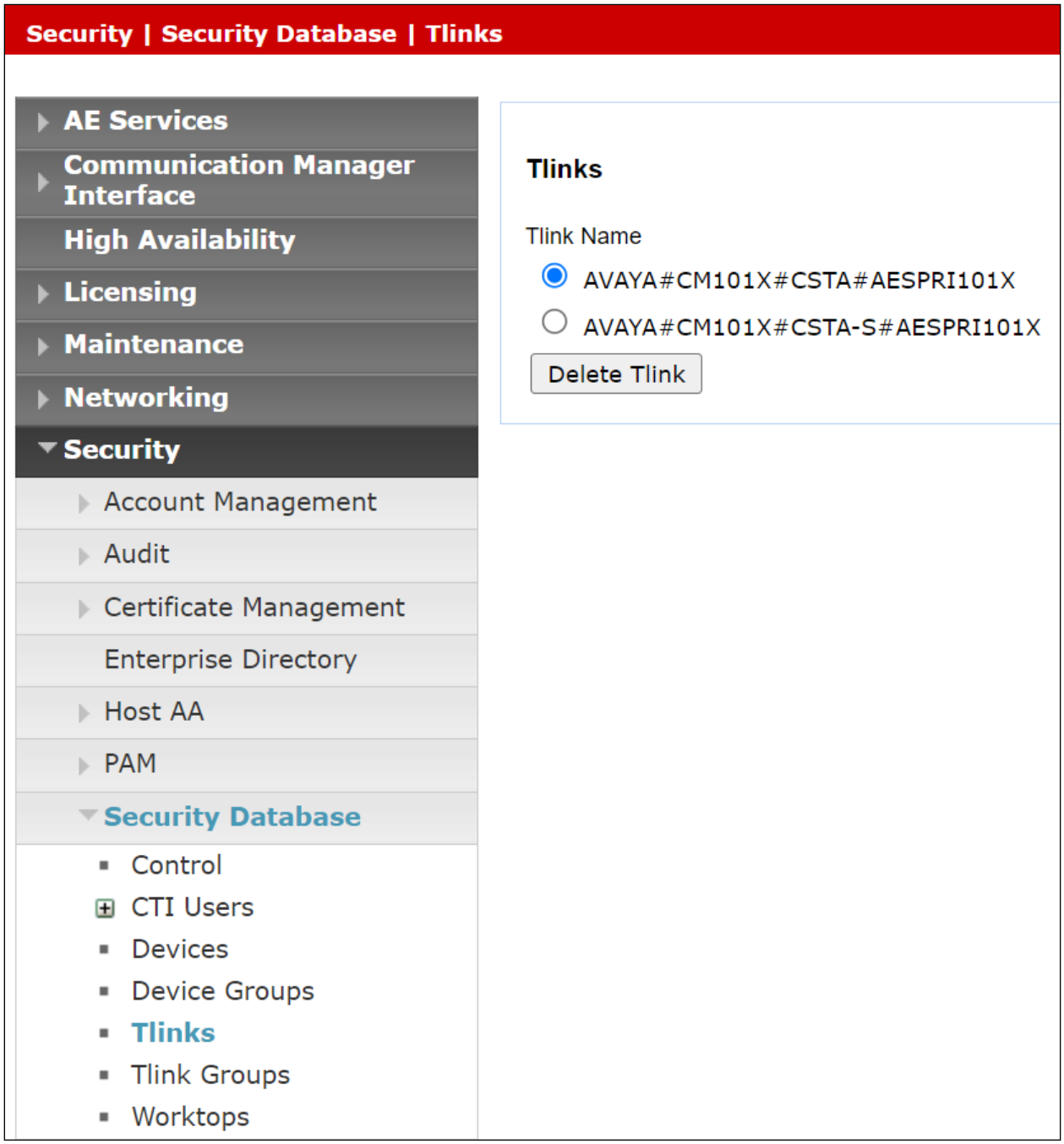
When the TSAPI Link is completed, it should resemble the screen below.



©2023 Avaya Inc. All Rights Reserved.

6.4. Identify Tlinks

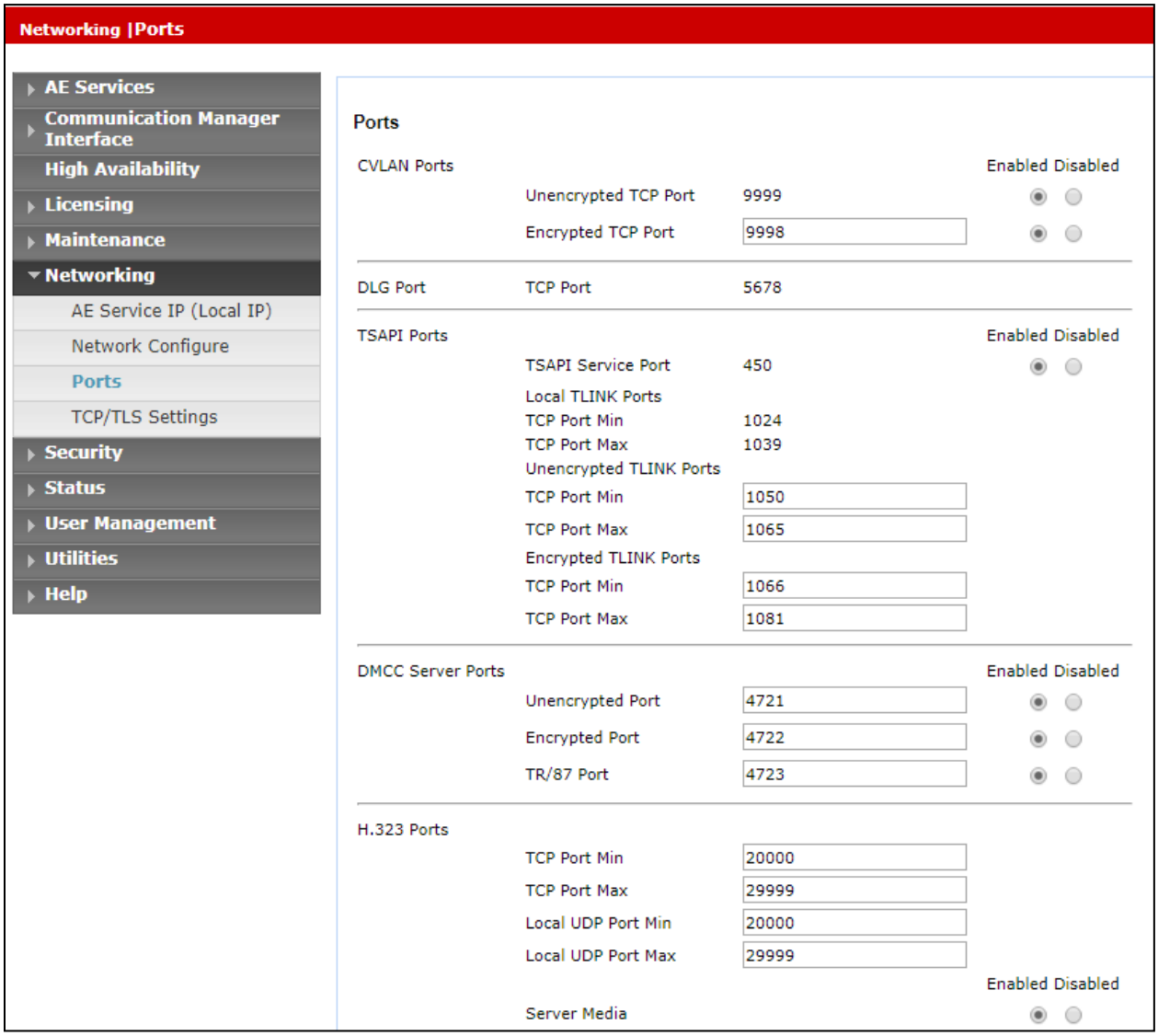
Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the NICE Engage Platform in **Section 7.1**. The Tlink for the unencrypted TSAPI link was used.



©2023 Avaya Inc. All Rights Reserved.

6.5. Configure Networking Ports

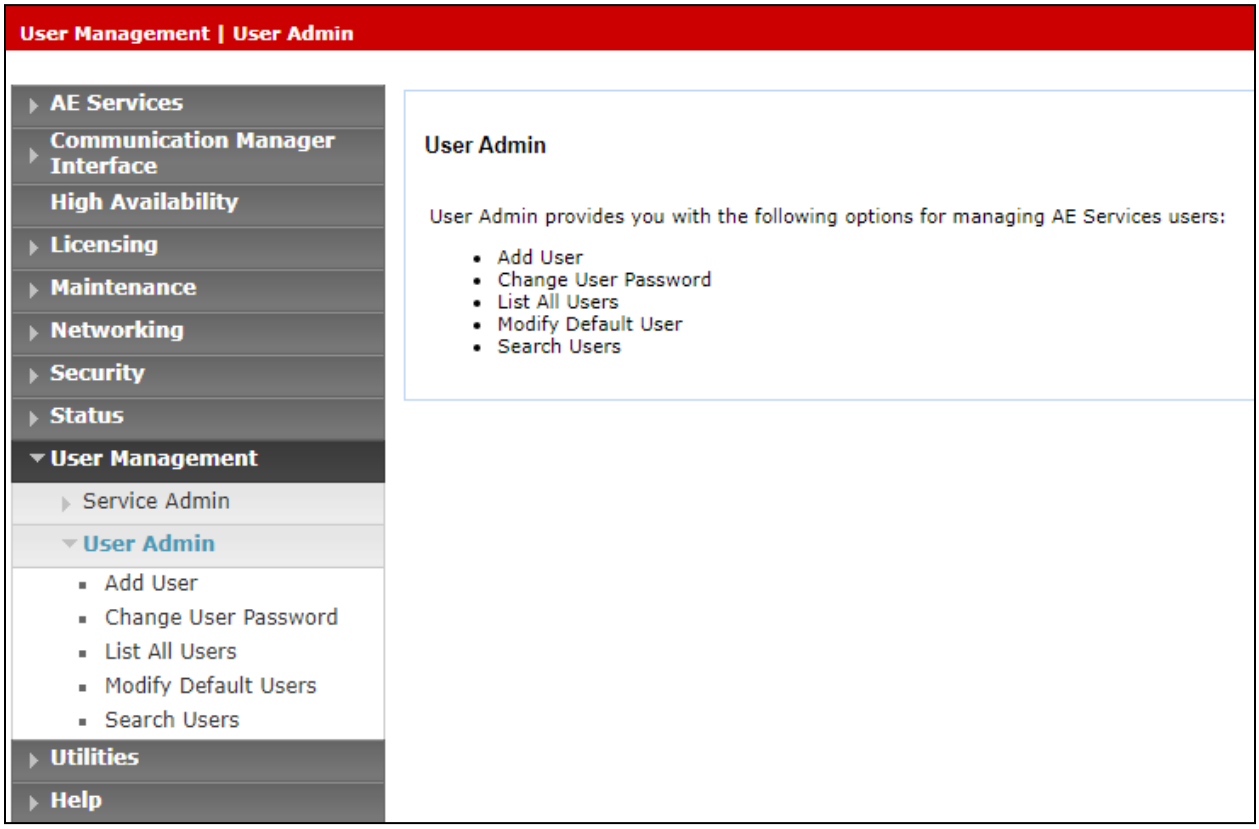
To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.1**.



©2023 Avaya Inc. All Rights Reserved.

6.6. Create CTI User

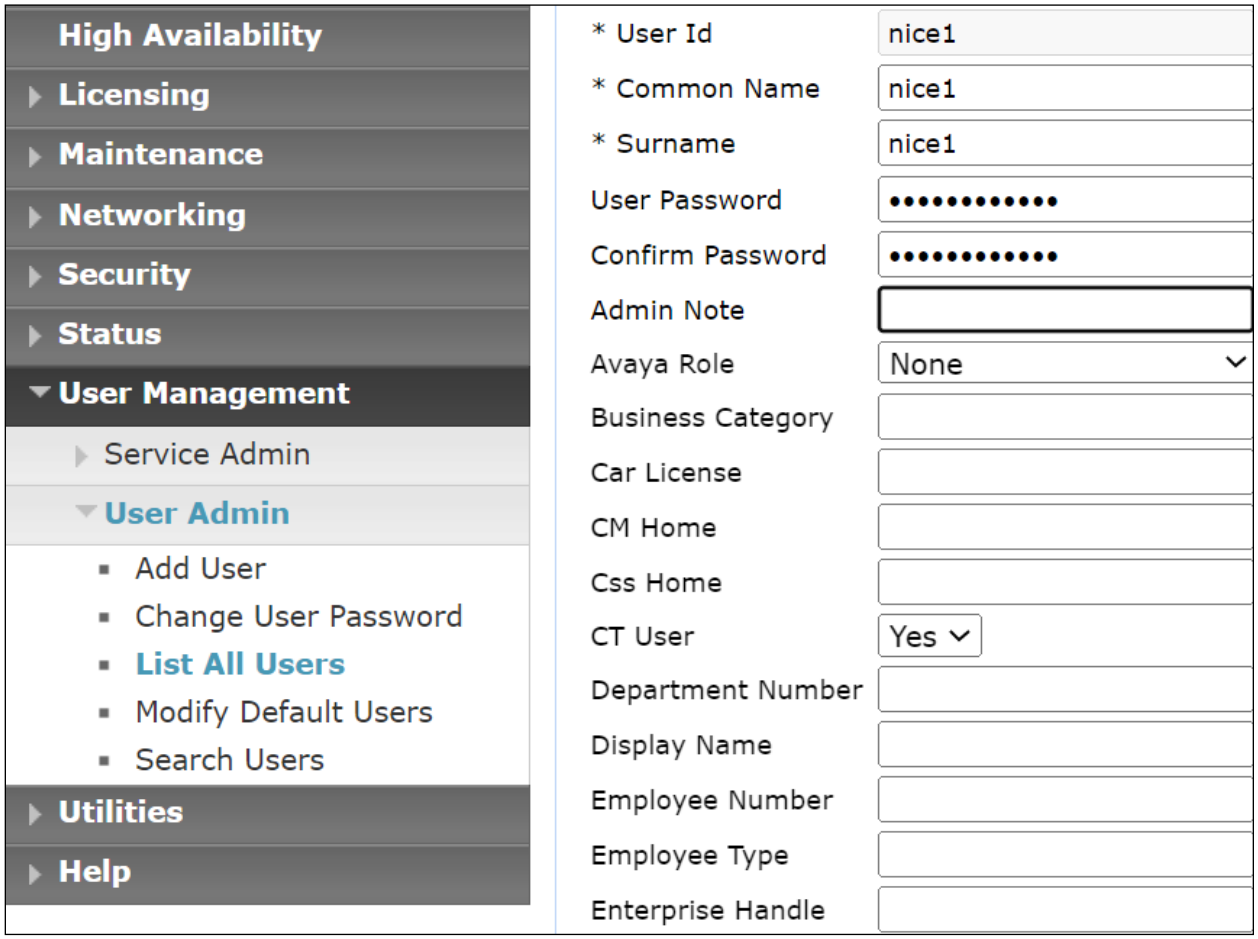
A User ID and password needs to be configured for the NICE Engage Platform to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



©2023 Avaya Inc. All Rights Reserved.

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** (not shown).

©2023 Avaya Inc. All Rights Reserved.

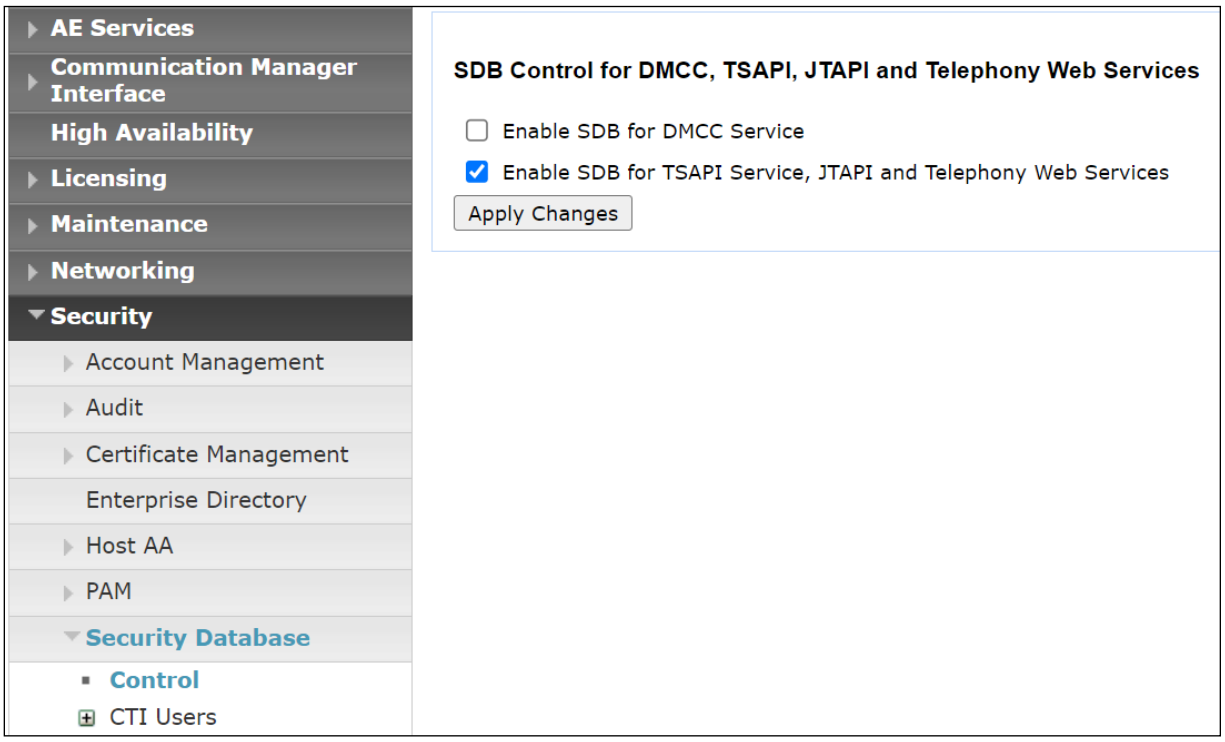
6.7. Configure Security

The CTI user permissions and the database security are set under **Security Database**.

6.7.1. Configure Database Control

The security database can be set differently depending on the requirements of the customer in question. For compliance testing, the DevConnect lab was setup as shown below, however this may be changed by opening **Control** and ticking the boxes shown.

Note: Since the CTI user was given unrestricted access, as per **Section** Error! Reference source not found., these values set here do not impact the overall setup.

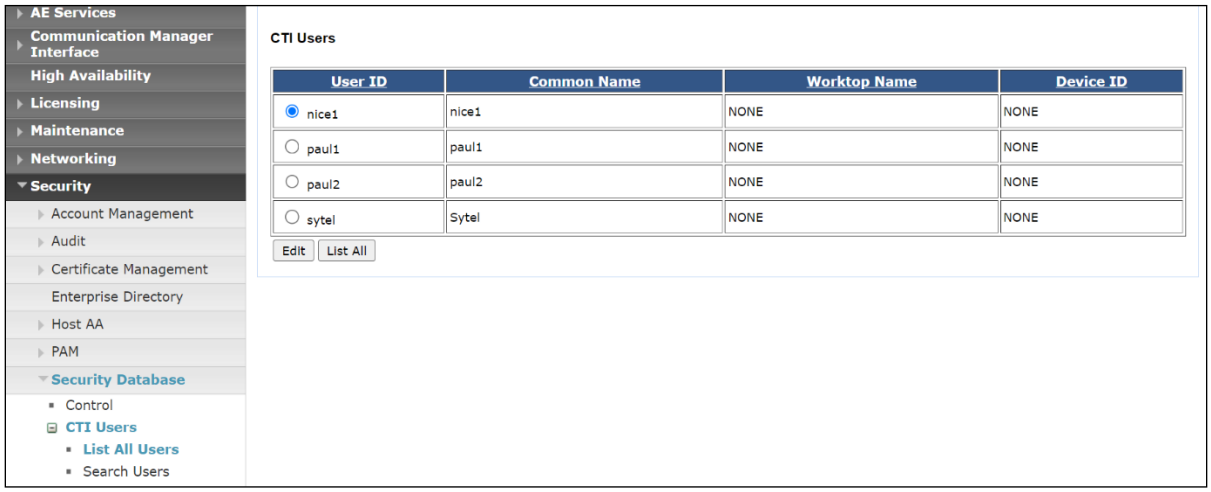


Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section** Error! Reference source not found. for more information on this.

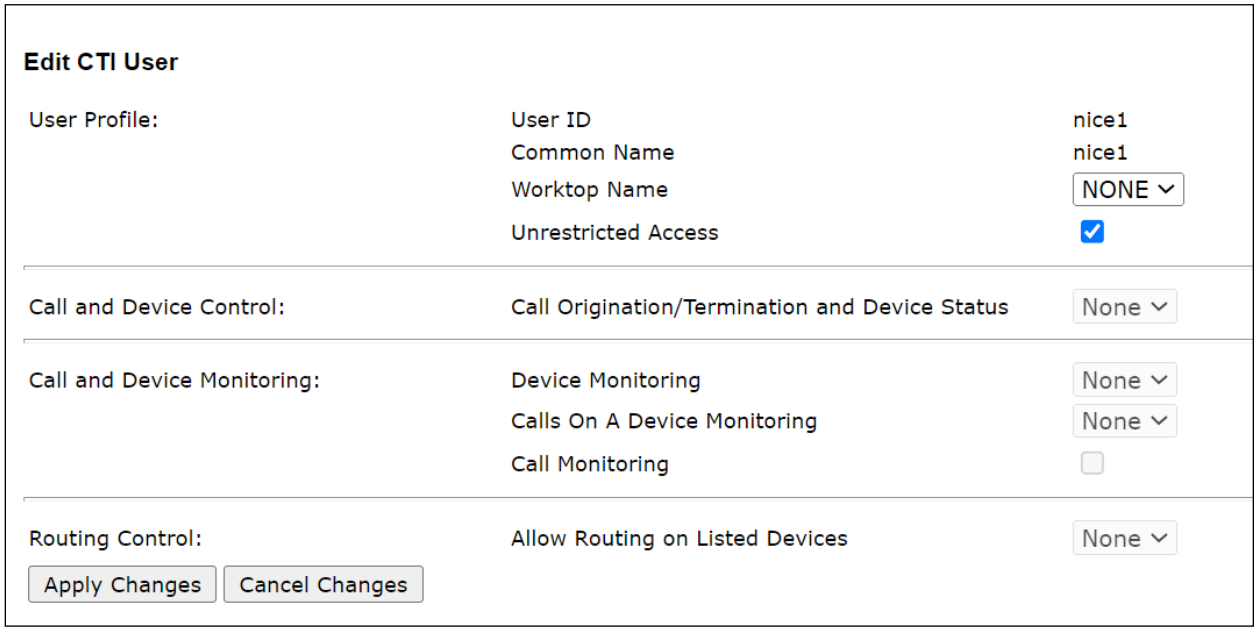
©2023 Avaya Inc. All Rights Reserved.

6.7.2. Associate Devices with CTI User

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



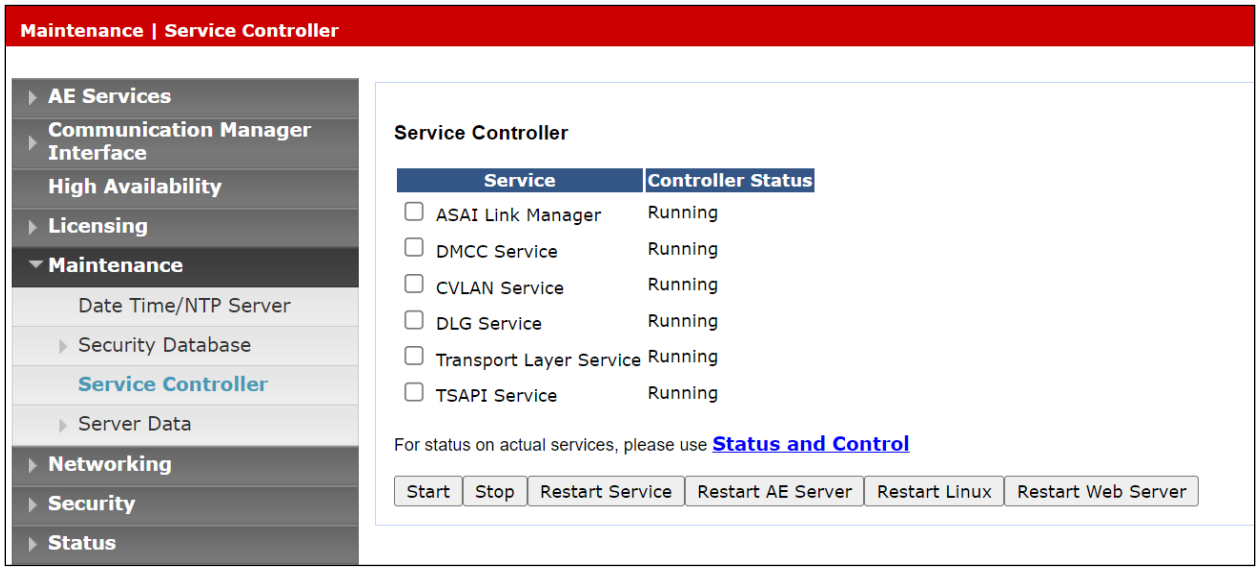
In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.



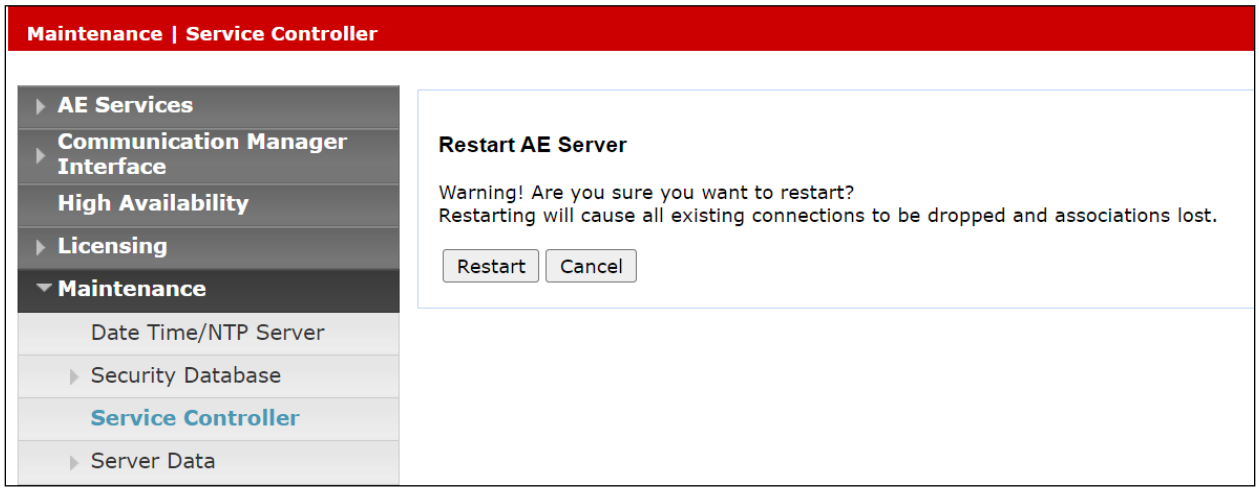
©2023 Avaya Inc. All Rights Reserved.

6.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.



A message confirming the restart will appear, click on **Restart** to proceed.

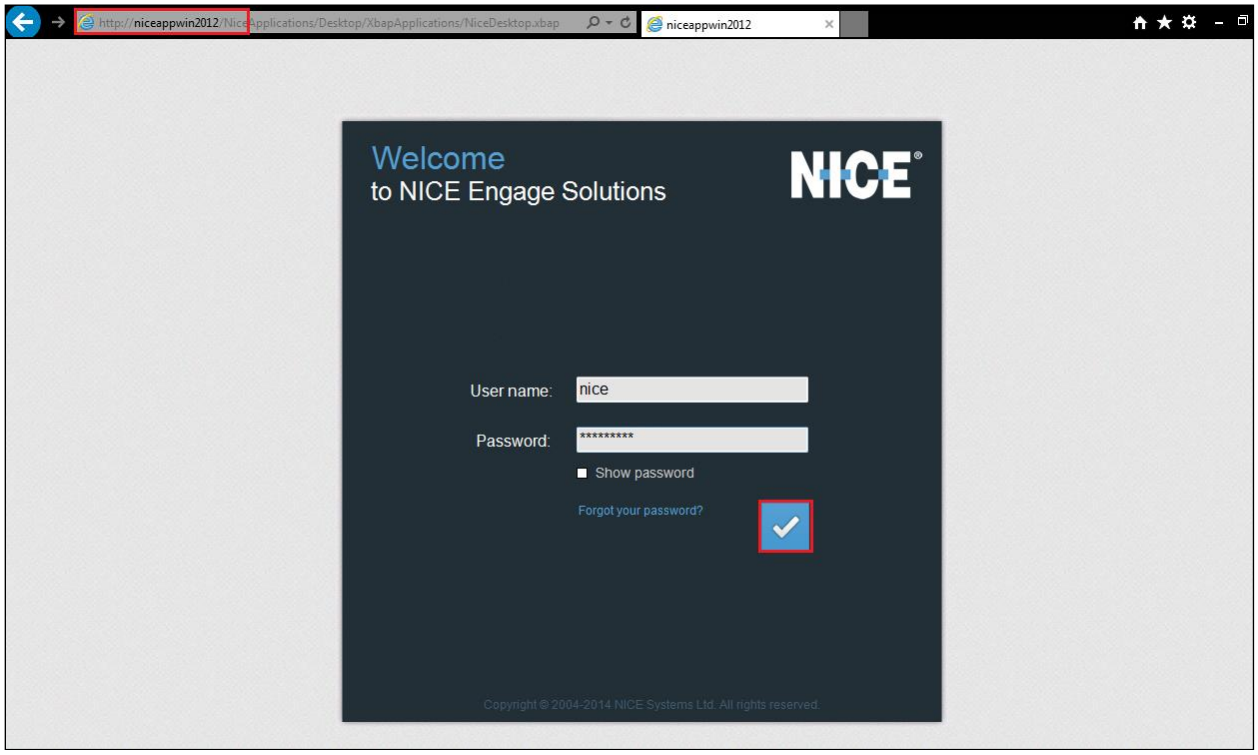


©2023 Avaya Inc. All Rights Reserved.

7. Configure NICE Engage Platform

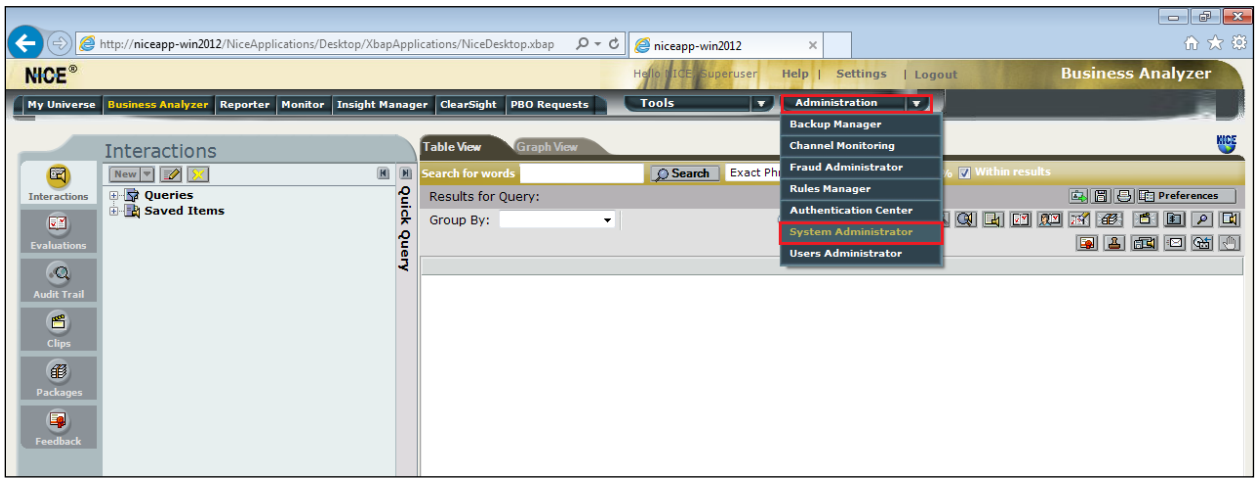
The installation of NICE Engage Platform is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of the NICE Engage Platform contact NICE as per the information provided in **Section 2.3**.

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**.

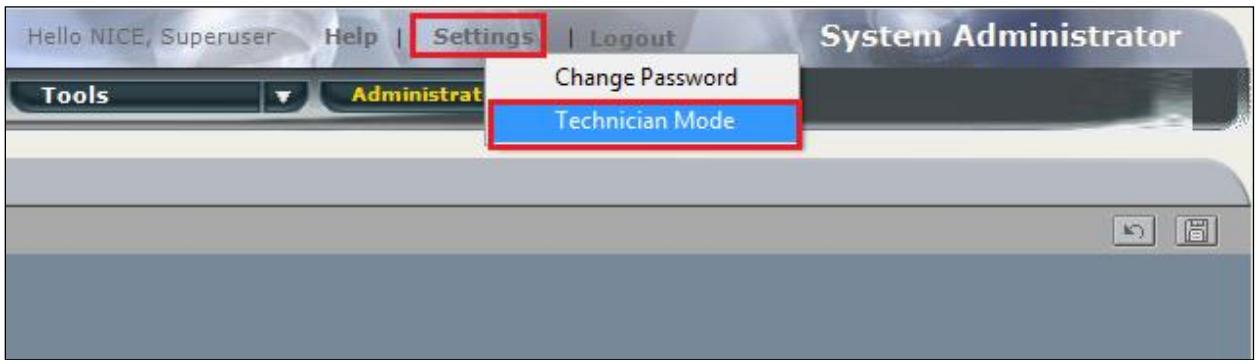


©2023 Avaya Inc. All Rights Reserved.

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



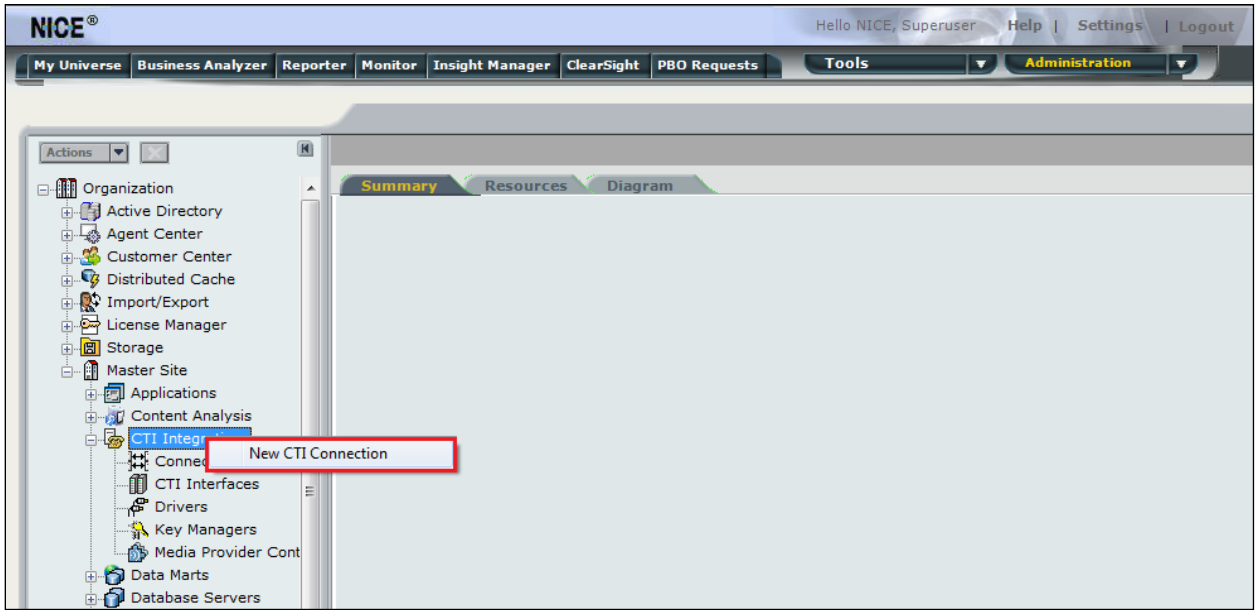
Before any changes can be made, switch to **Technician Mode** by clicking into **Settings** at the top of the screen as shown below.



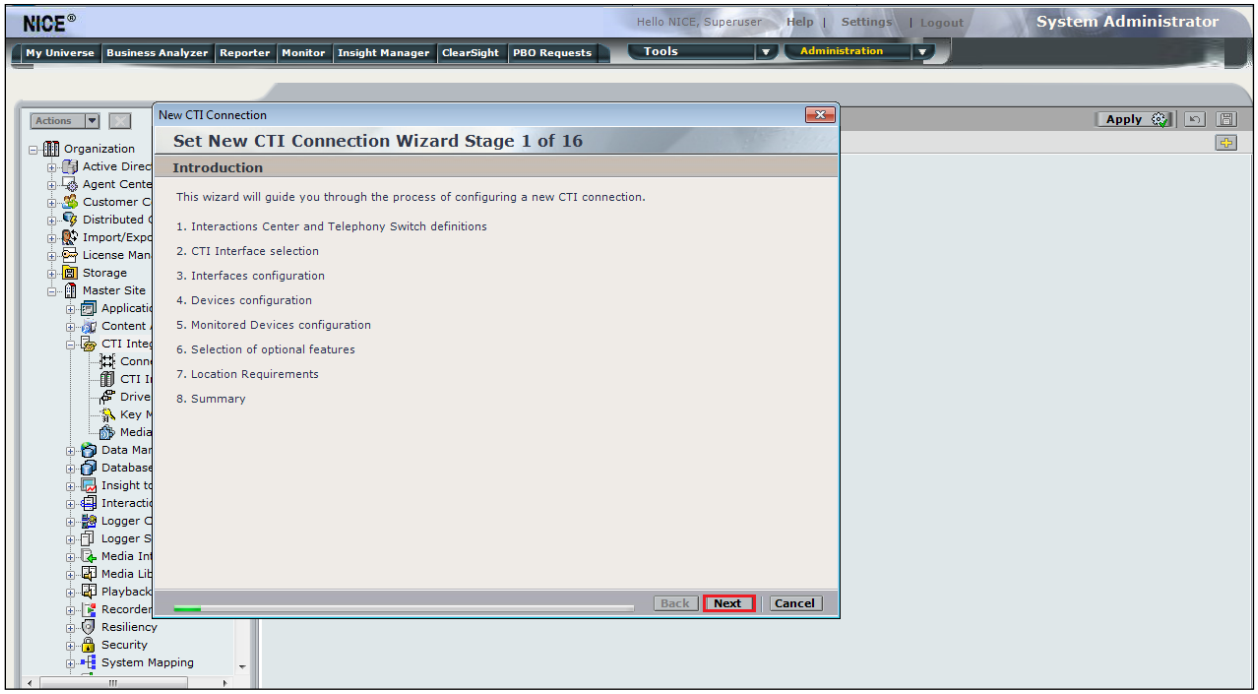
©2023 Avaya Inc. All Rights Reserved.

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.



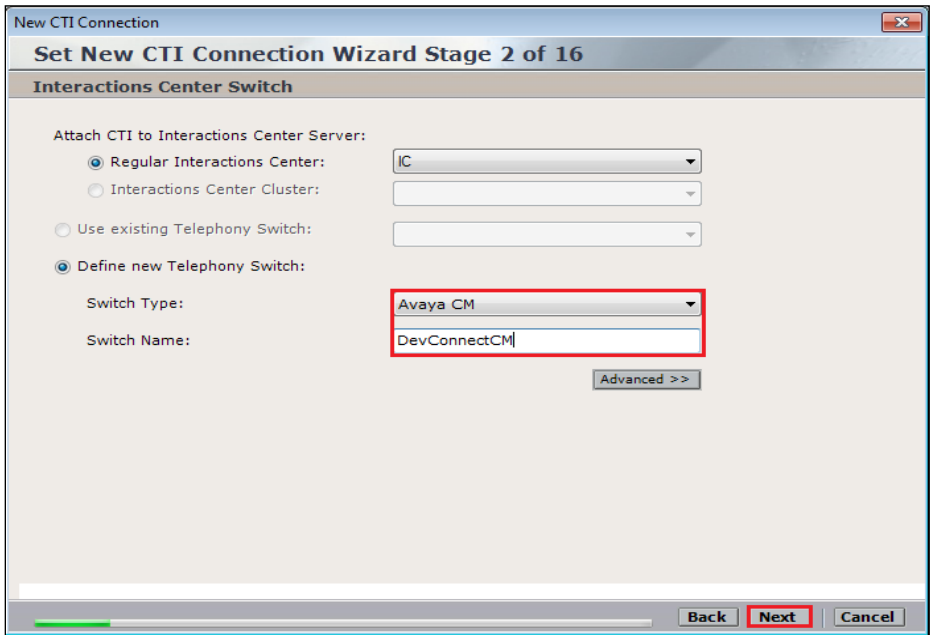
The **New CTI Connection Wizard** is opened, and this will go through the 16 steps required to set up the connection to the AES for DMCC Service Observe and Single Step Conference type of call recording. Click on **Next** to continue.



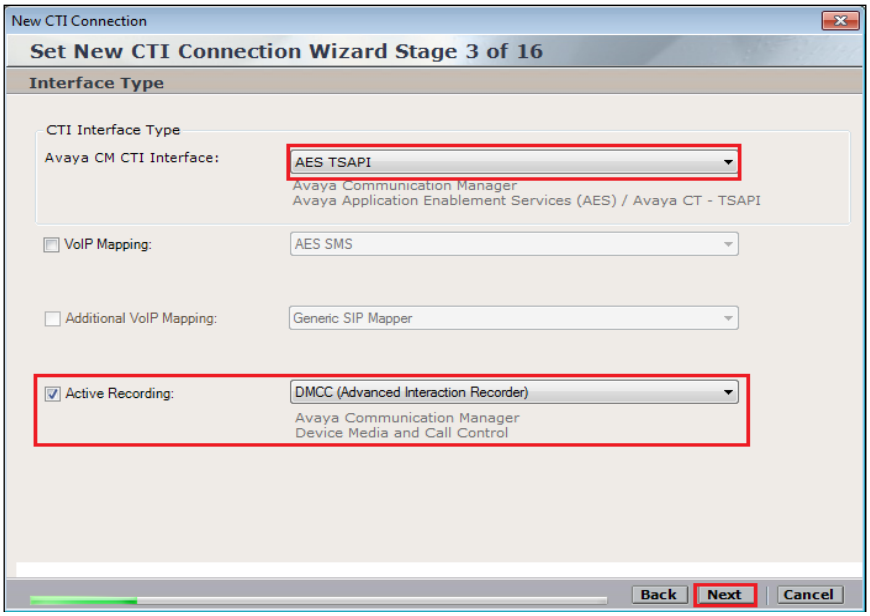
©2023 Avaya Inc. All Rights Reserved.

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.

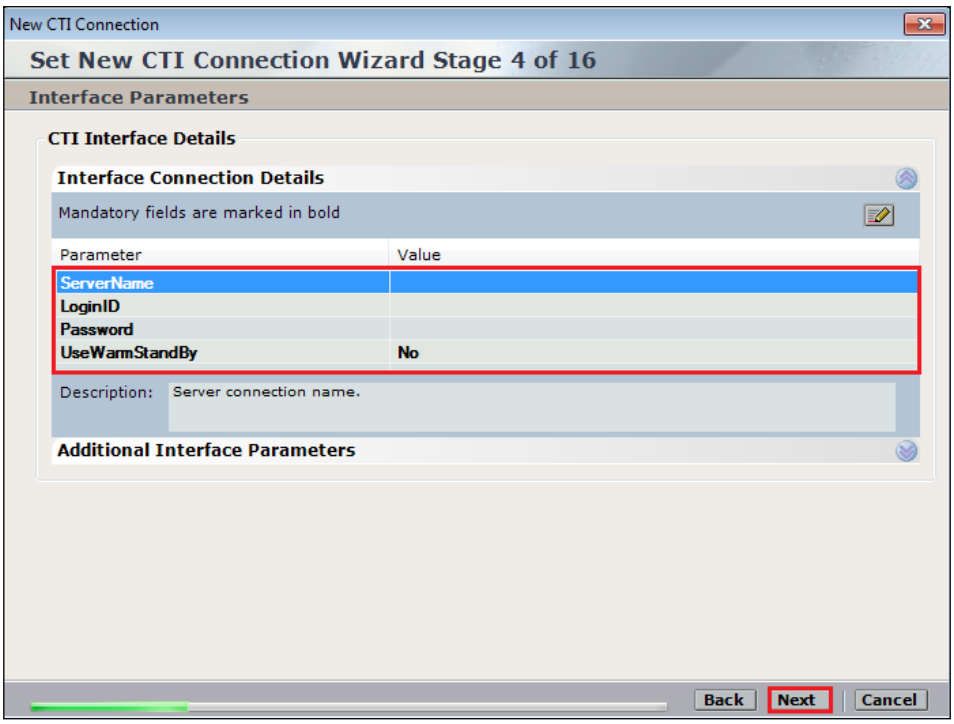


Select **AES TSAPI** for the **Avaya CM CTI Interface**, ensure that **Active Recording** is ticked and select the **DMCC (Advanced integration Recorder)** from the dropdown menu. Click on **Next** to continue.

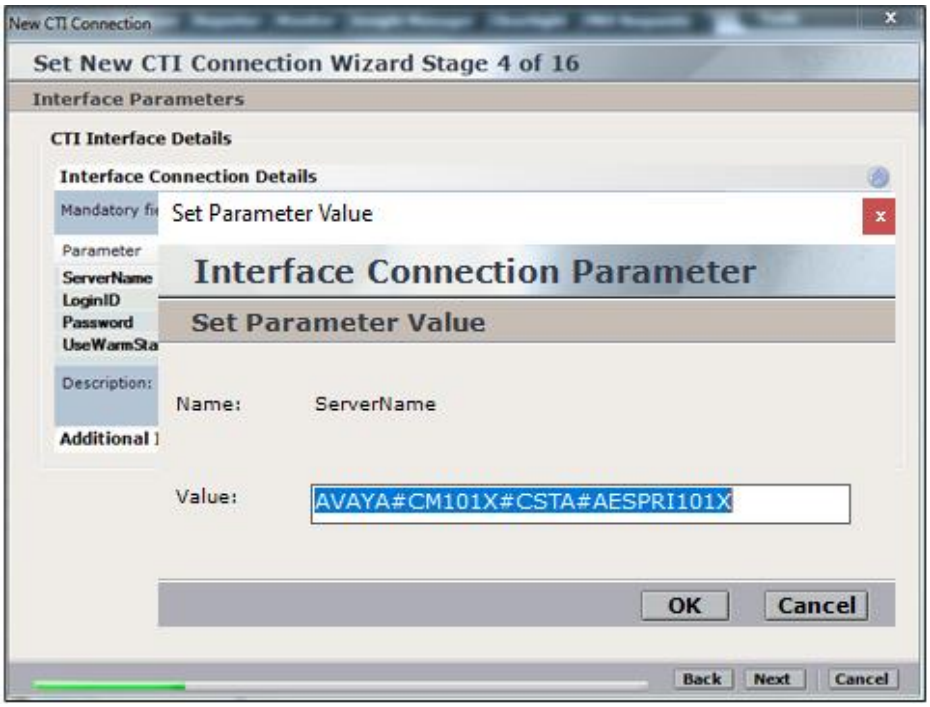


©2023 Avaya Inc. All Rights Reserved.

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

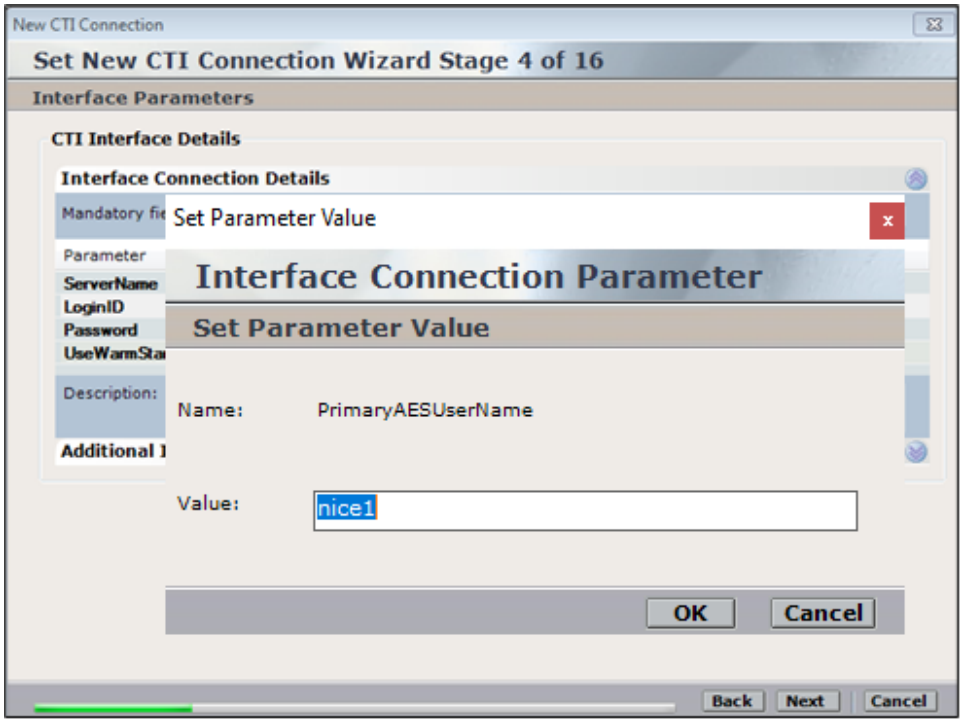


Double-click on **ServerName** and enter the TSAPI Tlink **Value** from **Section 6.4**.

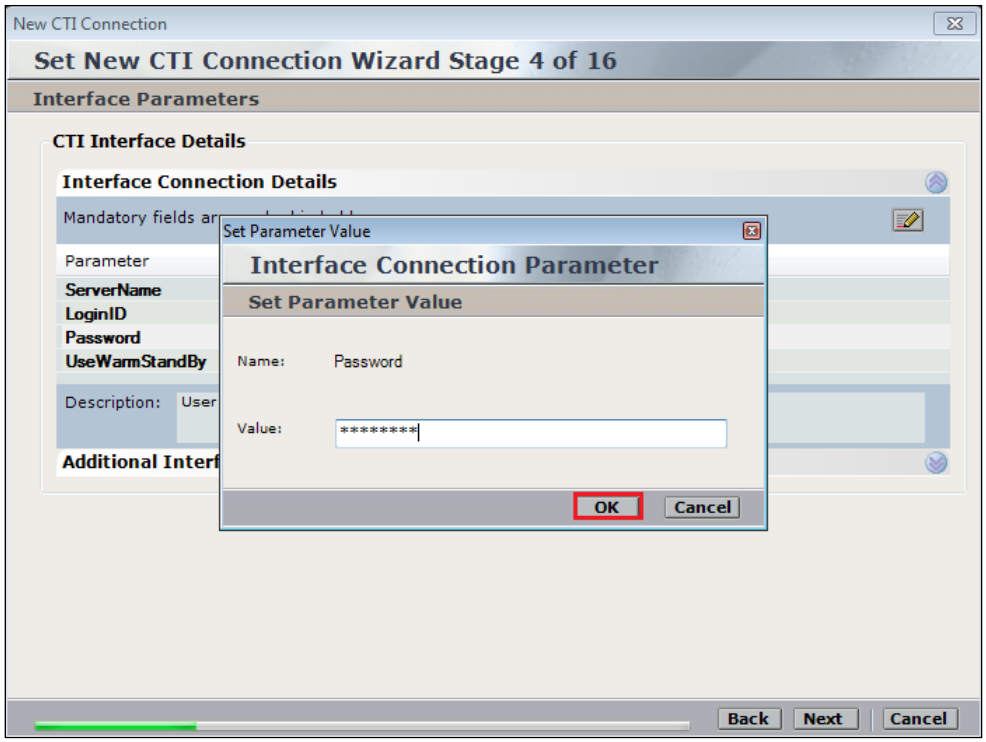


©2023 Avaya Inc. All Rights Reserved.

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

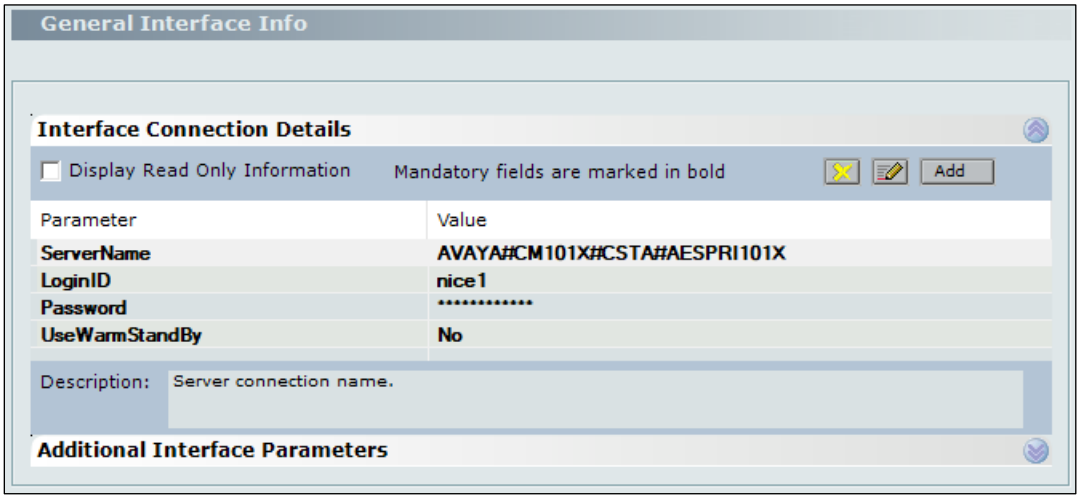


Double-click on password and enter the value for the password that was created in **Section 6.6**.

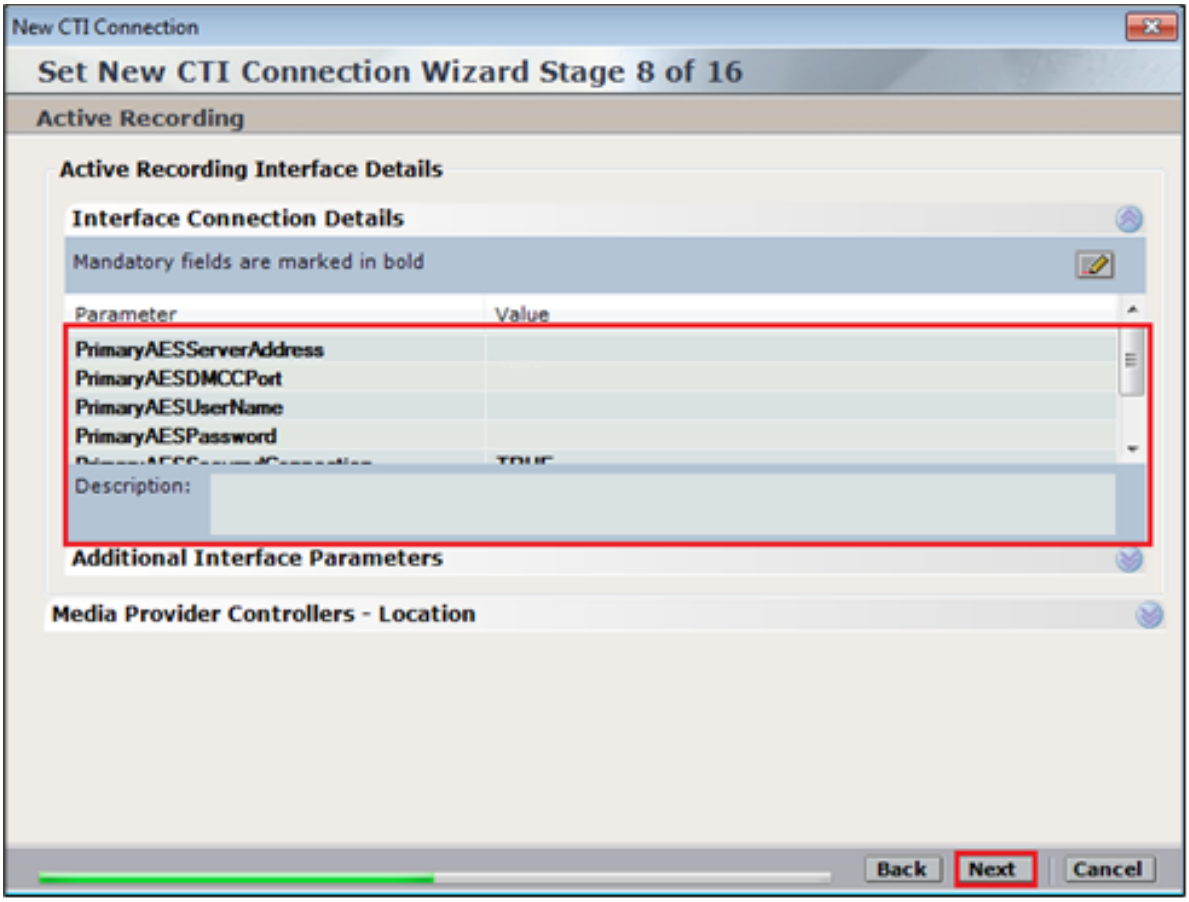


©2023 Avaya Inc. All Rights Reserved.

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

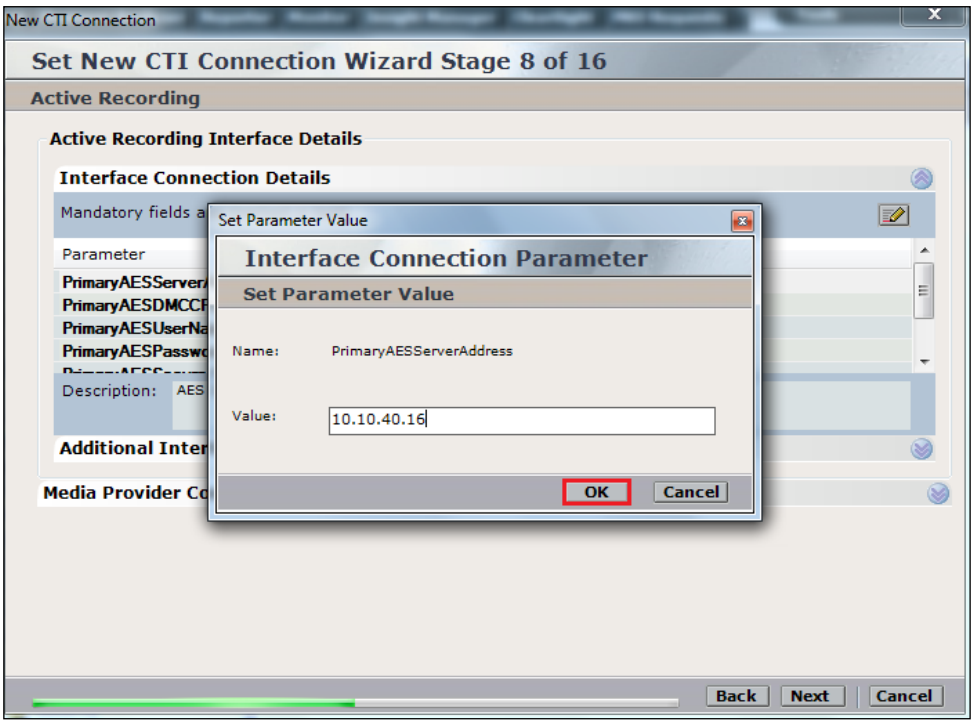


The values below must be filled in by double-clicking on each **Parameter**.

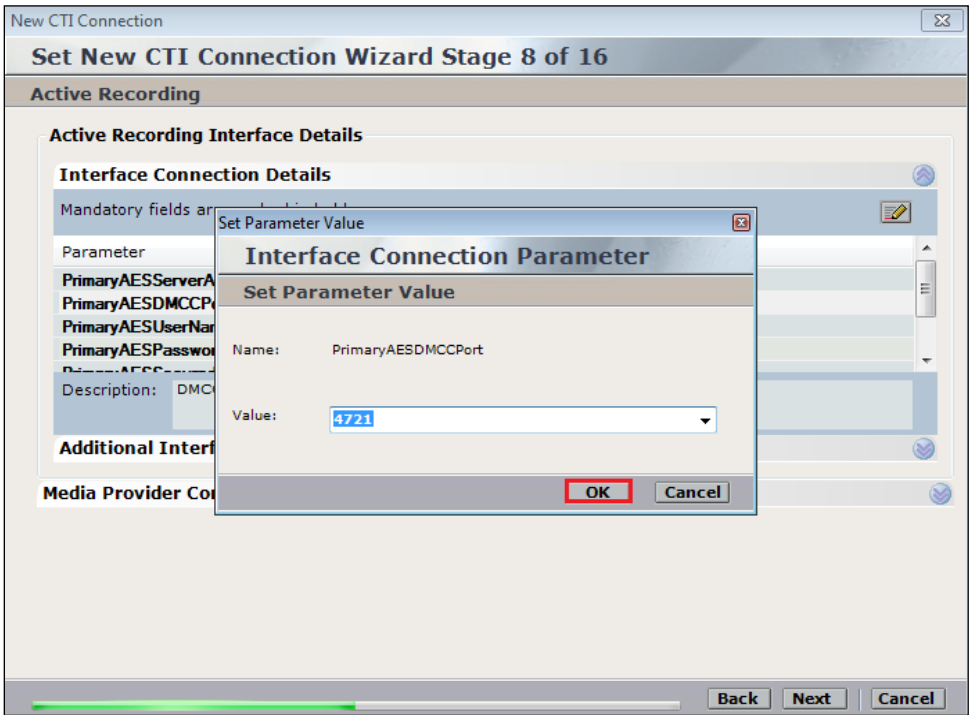


©2023 Avaya Inc. All Rights Reserved.

Enter the **Value** for the **AESServerAddress**, note this is the IP address of the AES server as per **Section 5.2**. Click on **OK**.

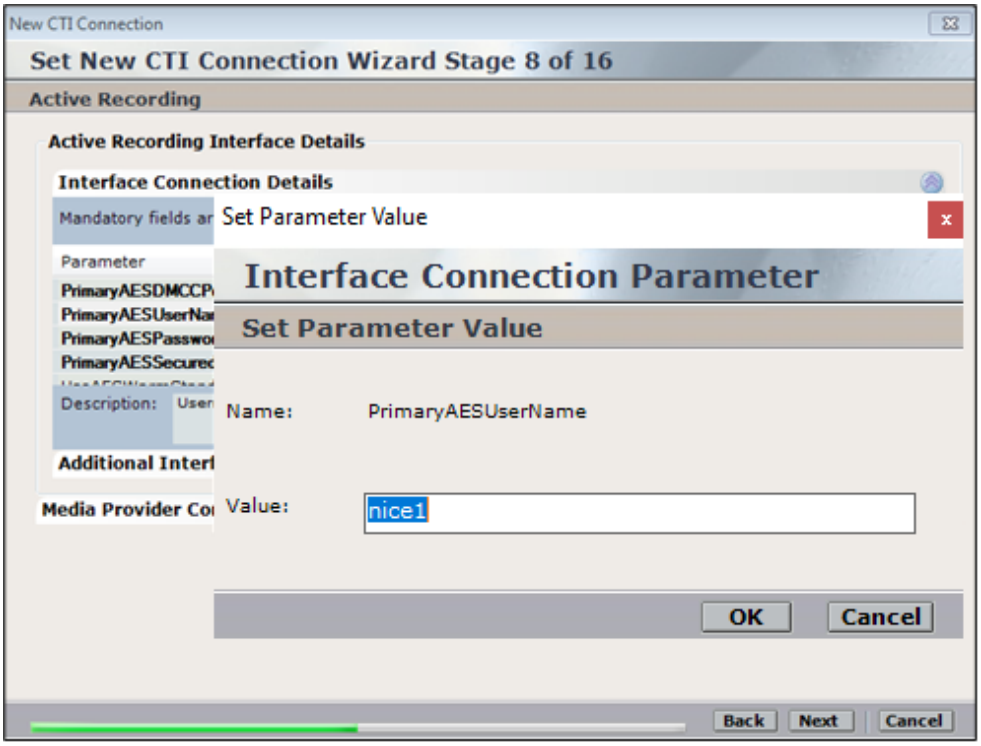


Enter the **Value** for the Primary**AESDMCCPort**, note this will be the same port that was configured in **Section 6.5**. In **this** example the unencrypted port **4721** is entered.

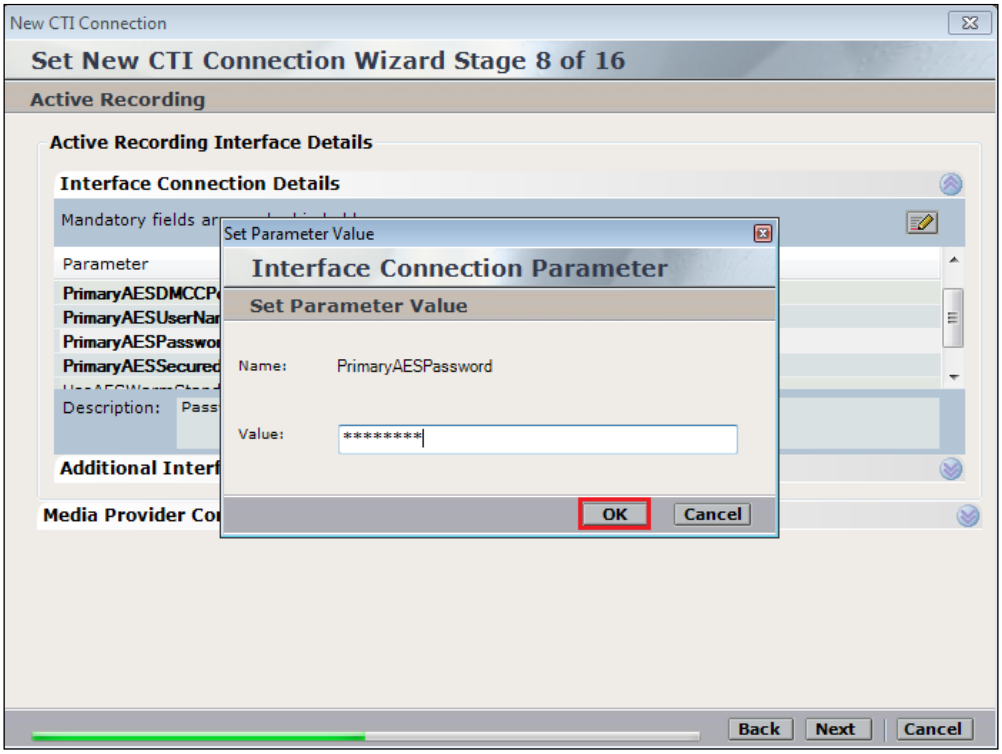


©2023 Avaya Inc. All Rights Reserved.

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

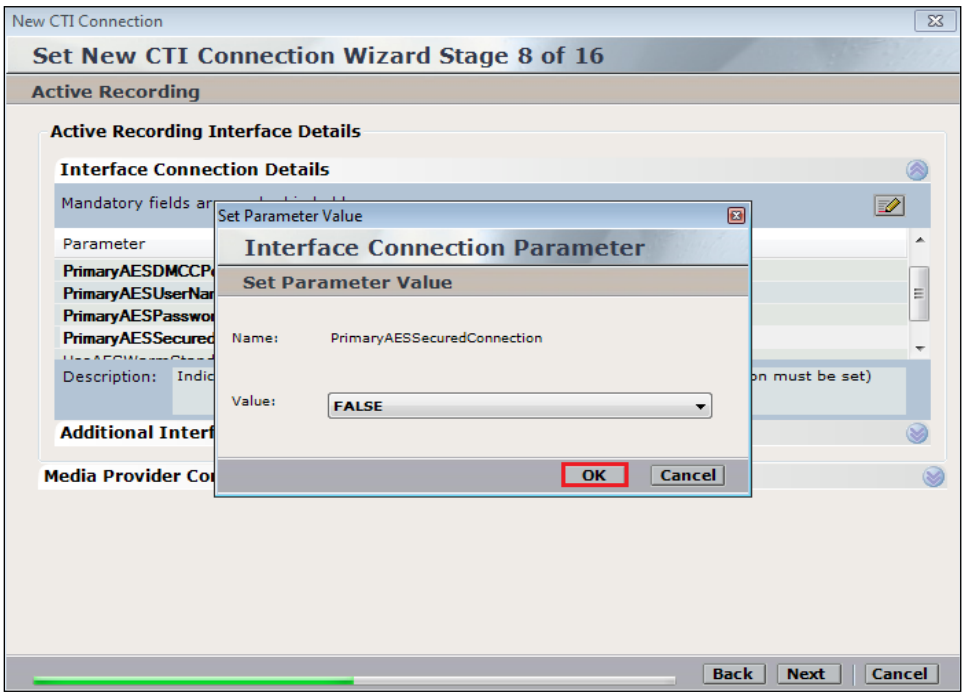


Enter the password that was created in **Section 6.6** and click on **OK**.

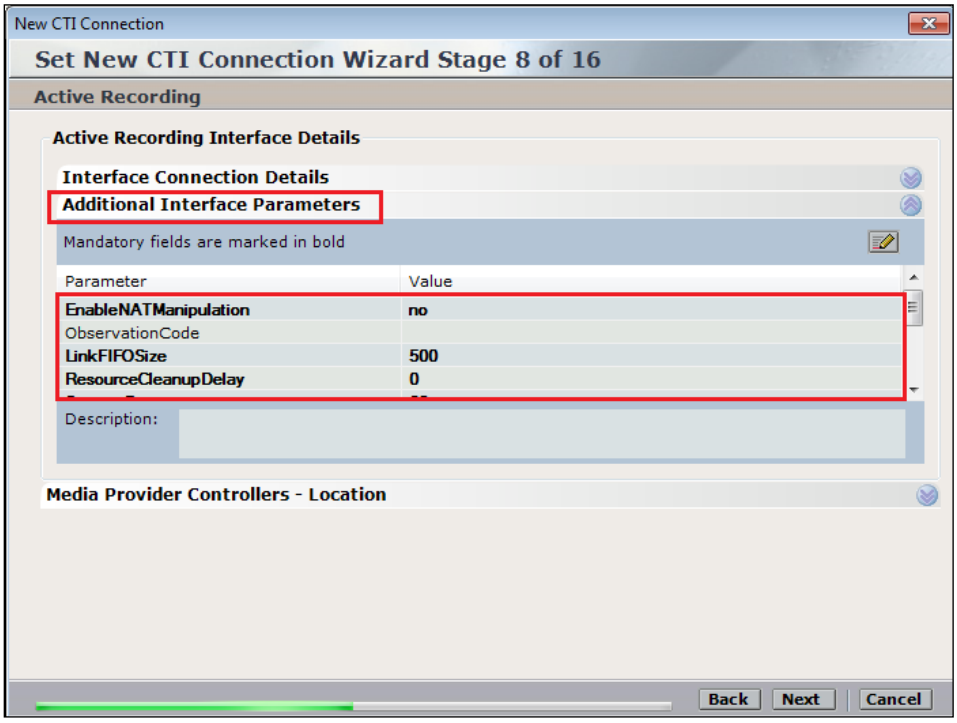


©2023 Avaya Inc. All Rights Reserved.

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

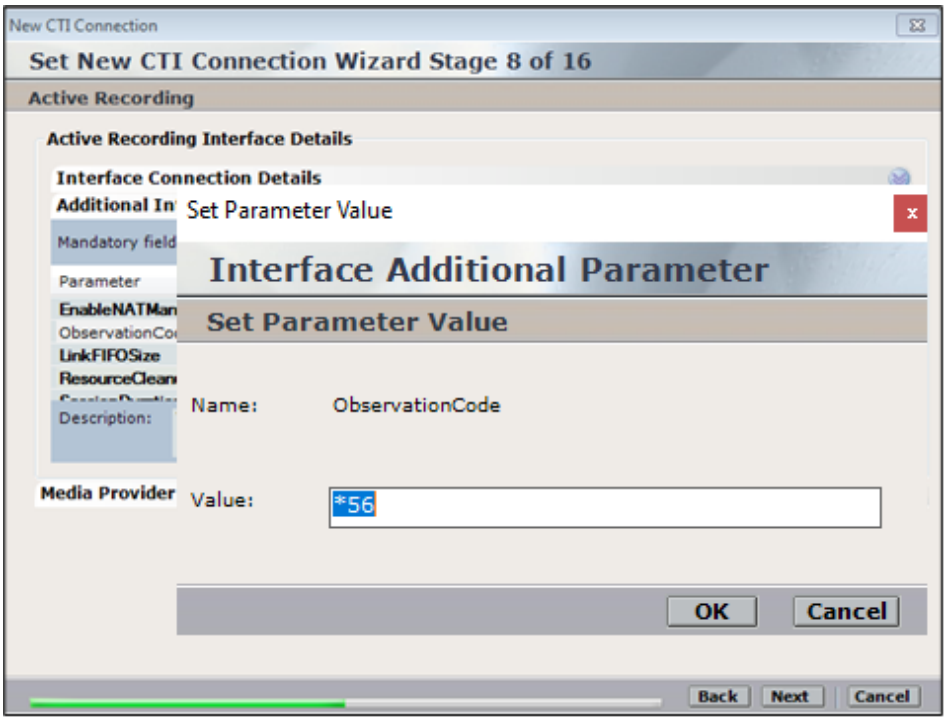


Click on **Additional Interface Parameters**, to change the Service Observing Code double-click on **ObservationCode**.

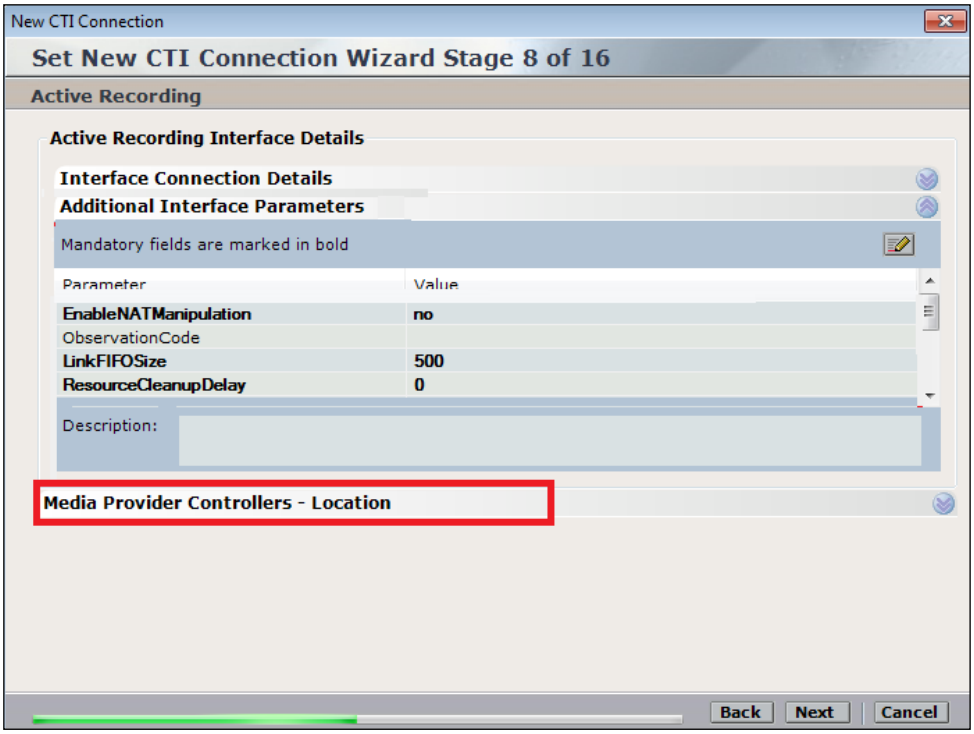


©2023 Avaya Inc. All Rights Reserved.

Enter the **Value** that was created in **Section 5.5**. This was the Service Observing Listen Only Access Code ***56**. Click on **OK** to continue.

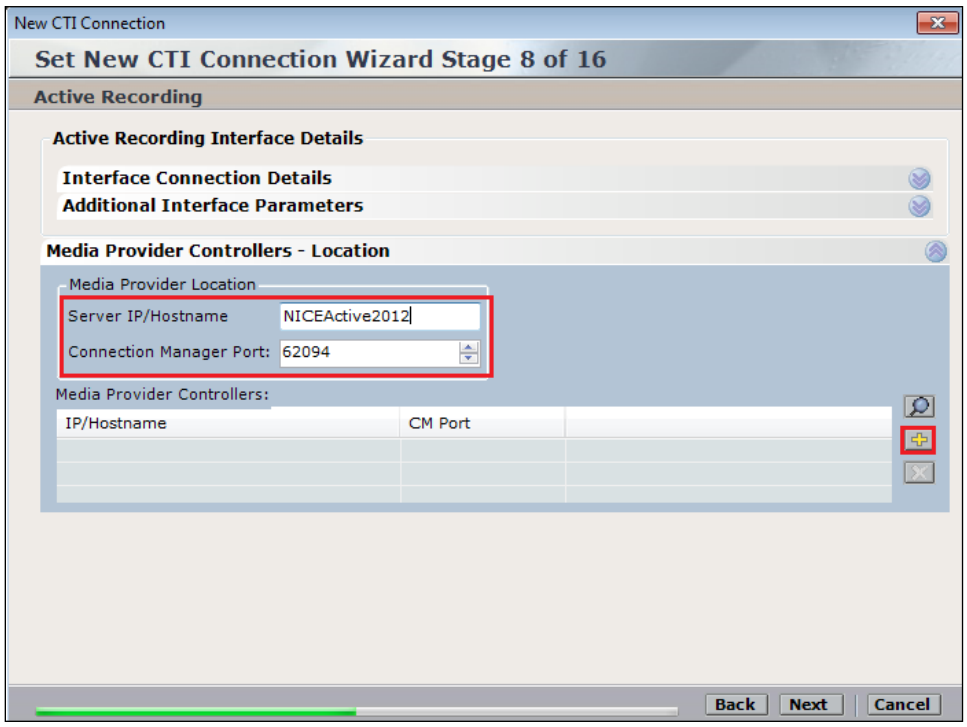


Click on **Media Provider Controllers – Location** to expand this.

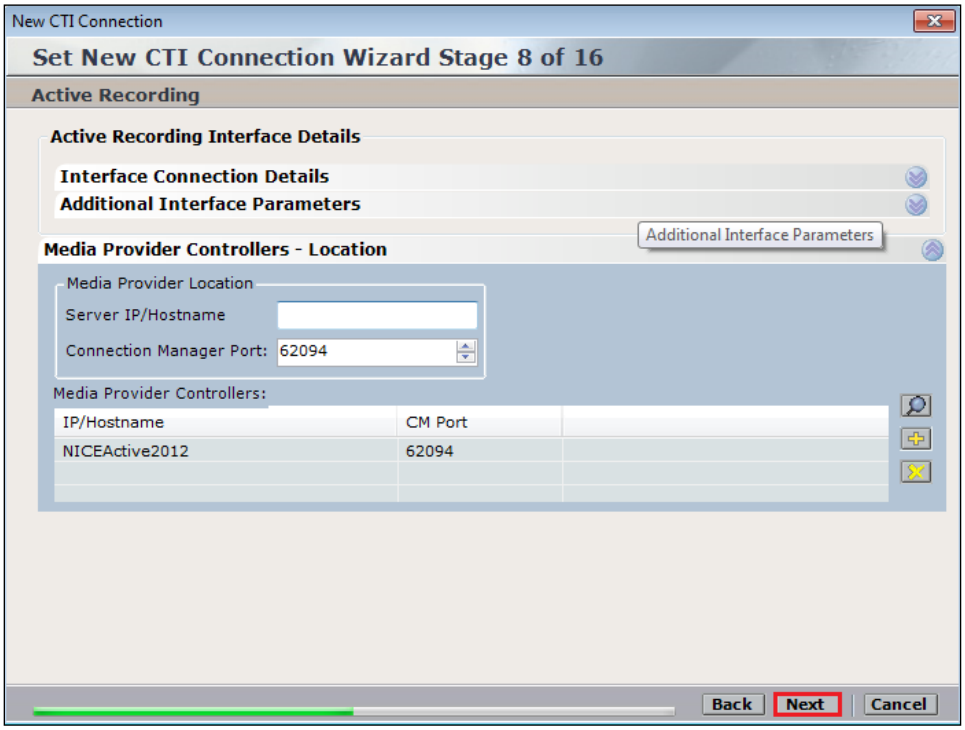


©2023 Avaya Inc. All Rights Reserved.

Enter the **IP/Hostname** of the Nice Advanced Interactions Server, then click on the + icon to add this.

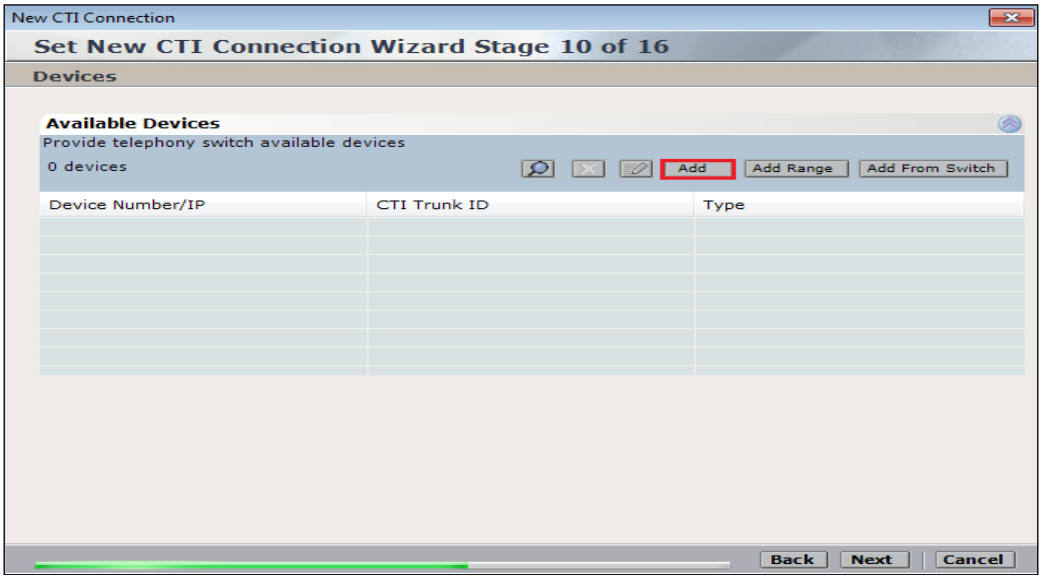


Click on **Next** to continue.

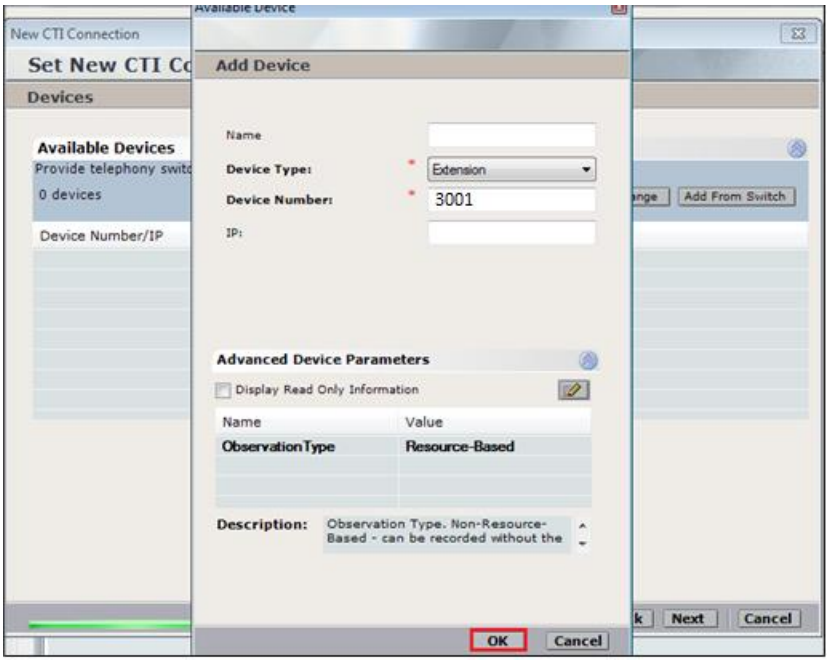


©2023 Avaya Inc. All Rights Reserved.

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

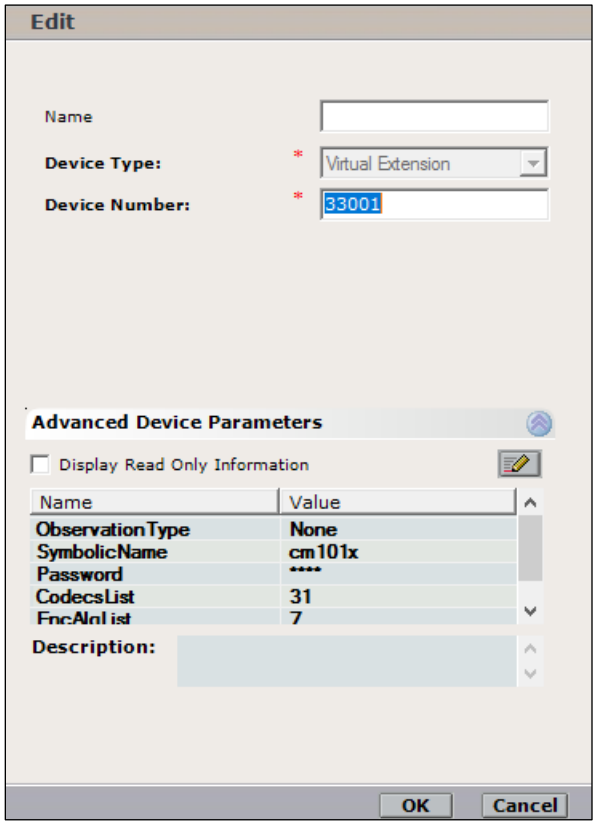


The **Device Type** should be **Extension** and insert the extension number of a phoneset that is to be recorded the example below showing extension **3001**. Expand **Advanced Device Parameters** and ensure that the **Value** for **Observation Type** is set to **Resourced-Based**. Click on **OK** to continue.



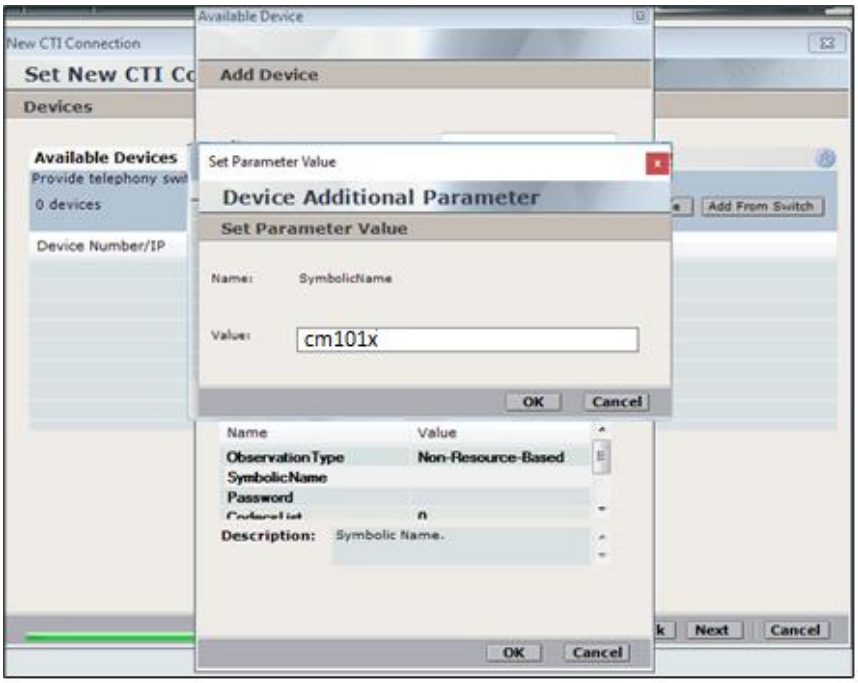
©2023 Avaya Inc. All Rights Reserved.

For Service Observe and Single Step Conference virtual extensions need to be added. These are the virtual extensions that were created in **Section 5.8**. Ensure that **Device Type** is set to **Virtual Extension** and add the correct extension for **Device Number**. Each of the **Parameters** highlighted at the bottom of the screen need to be configured and these are done by double-clicking on each parameter.

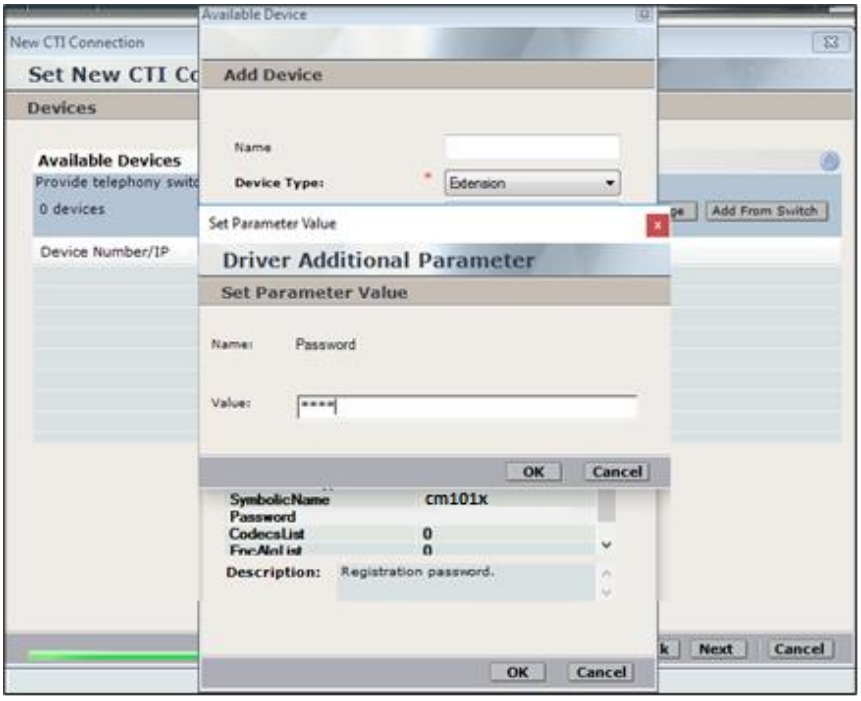


©2023 Avaya Inc. All Rights Reserved.

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**.

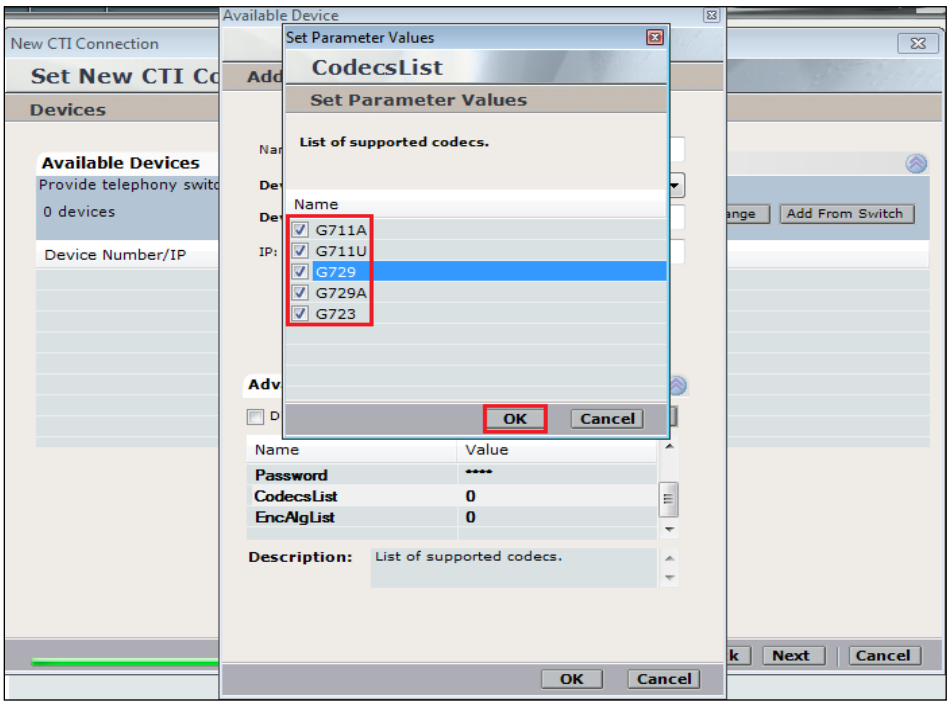


Enter the correct **Password** and note this is the password for the extension that is being added here. This is the station password which was entered during the creation of the station. A printout of an extension can be found in **Section 5.6** of these Application Notes.

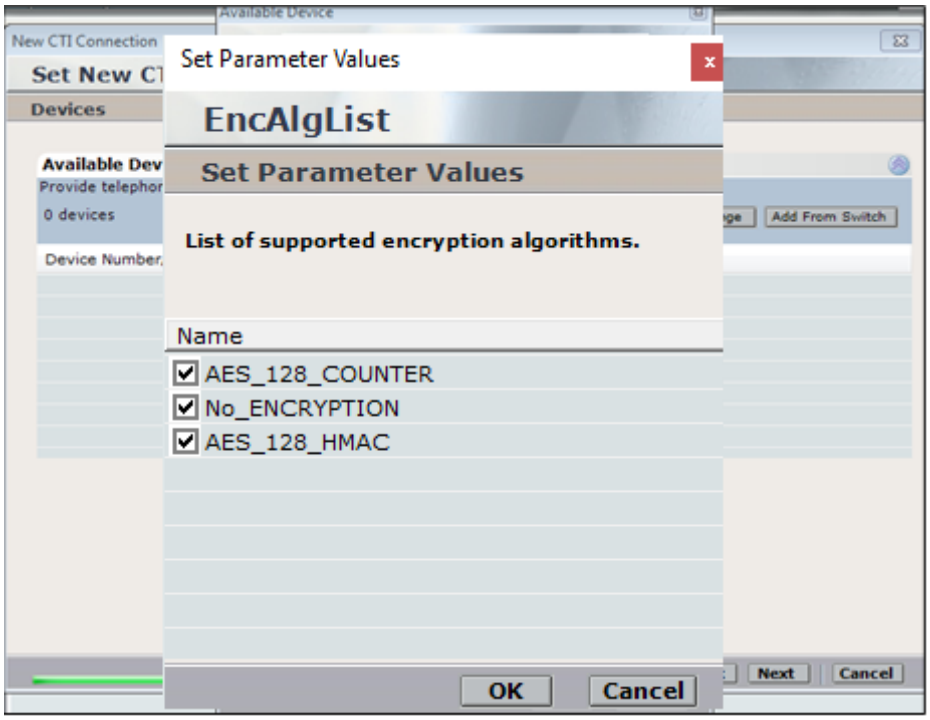


©2023 Avaya Inc. All Rights Reserved.

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

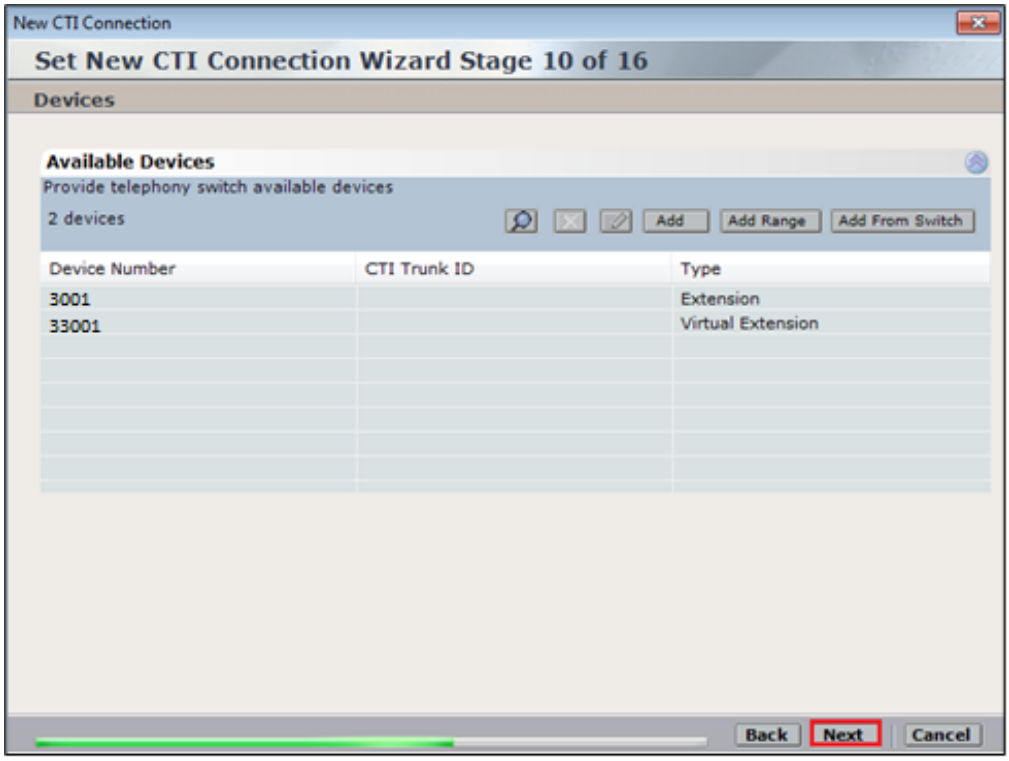


Double-click on **EncAlgList**. To cover all options, all types of encryptions were ticked. Click on **OK** to continue.

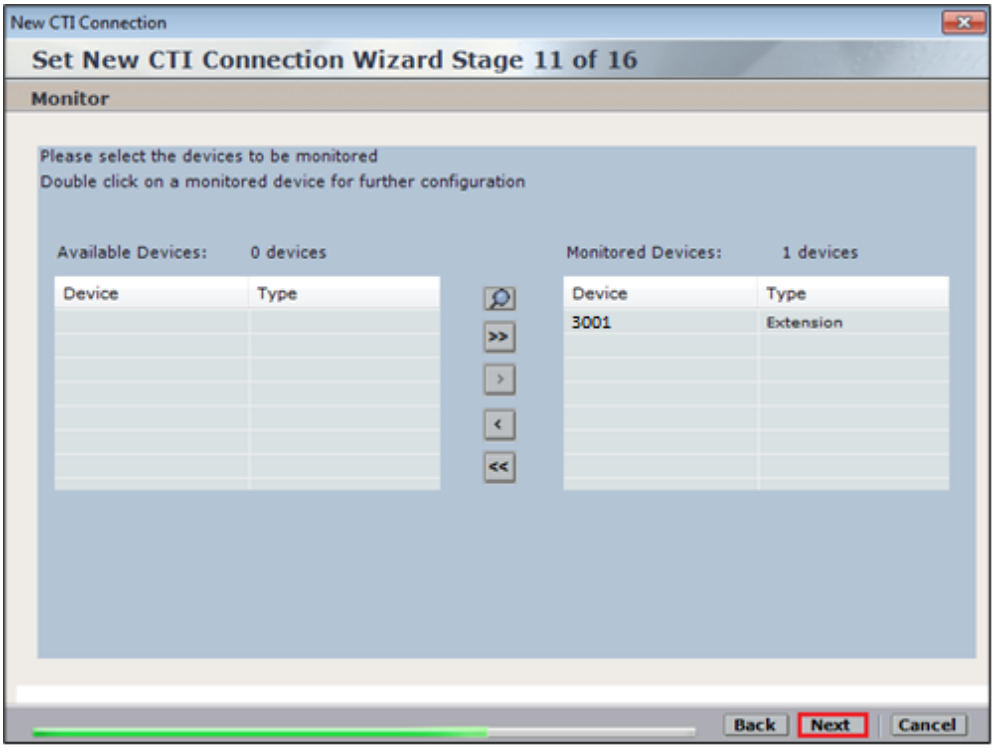


©2023 Avaya Inc. All Rights Reserved.

Click on **Next** to continue.

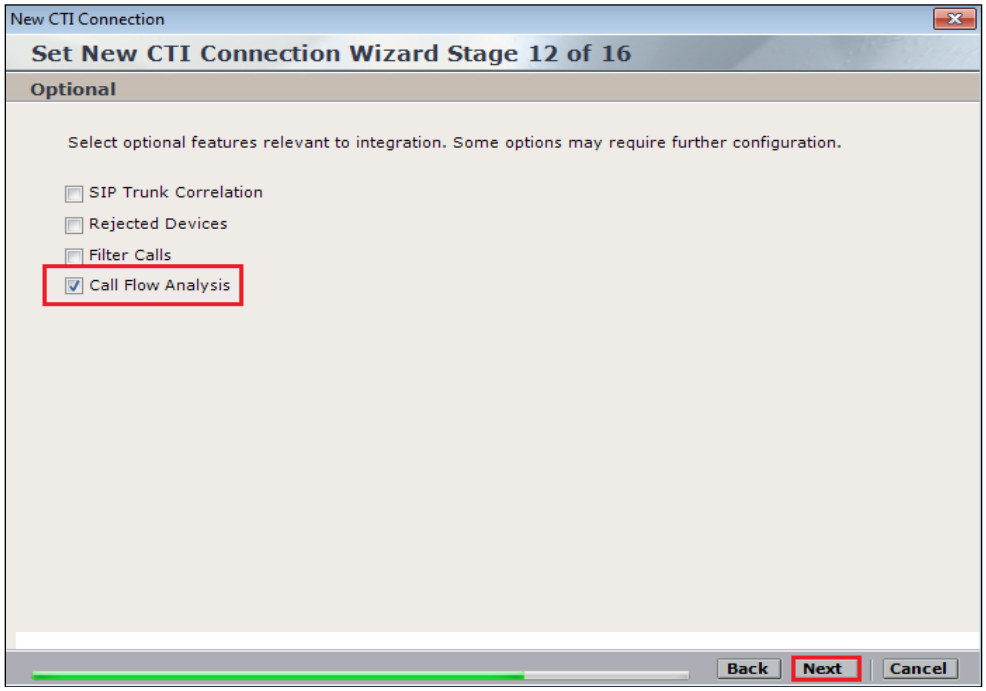


Select the new extension and click on the >> icon as shown. Click on **Next** to continue.

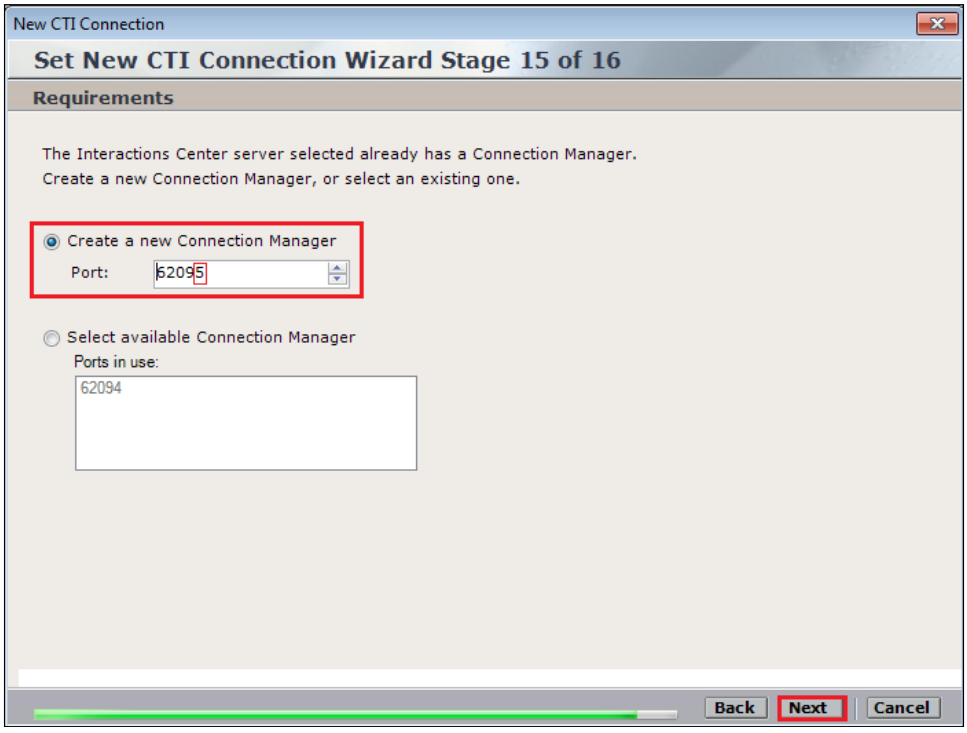


©2023 Avaya Inc. All Rights Reserved.

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

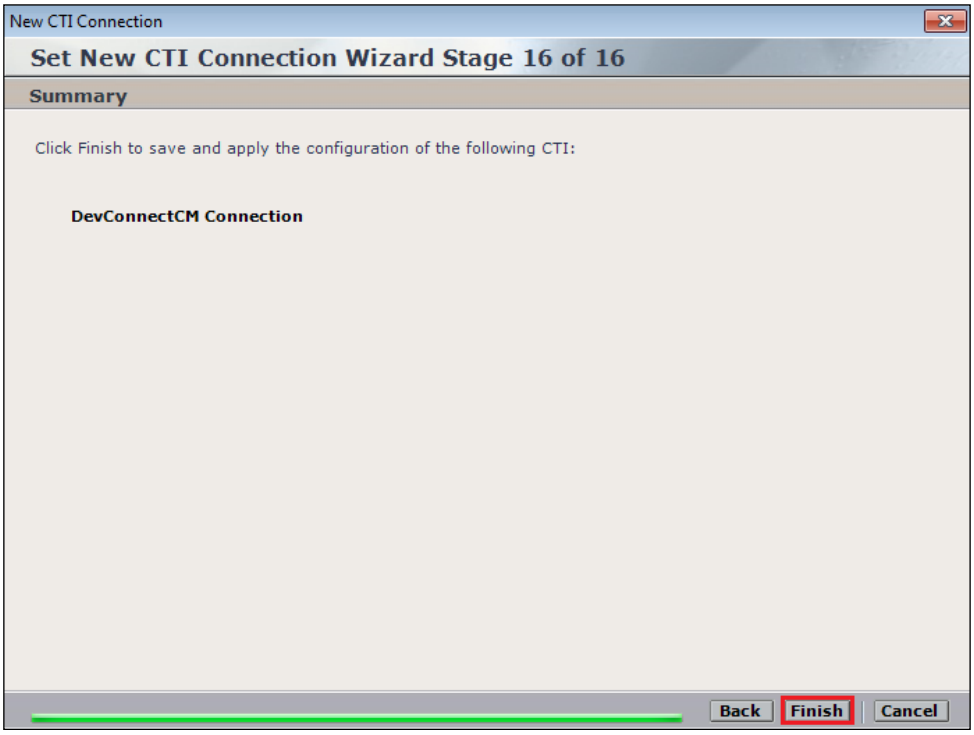


Select a different **Port** number as shown below **62095** is chosen simply because **62094** was already in use.

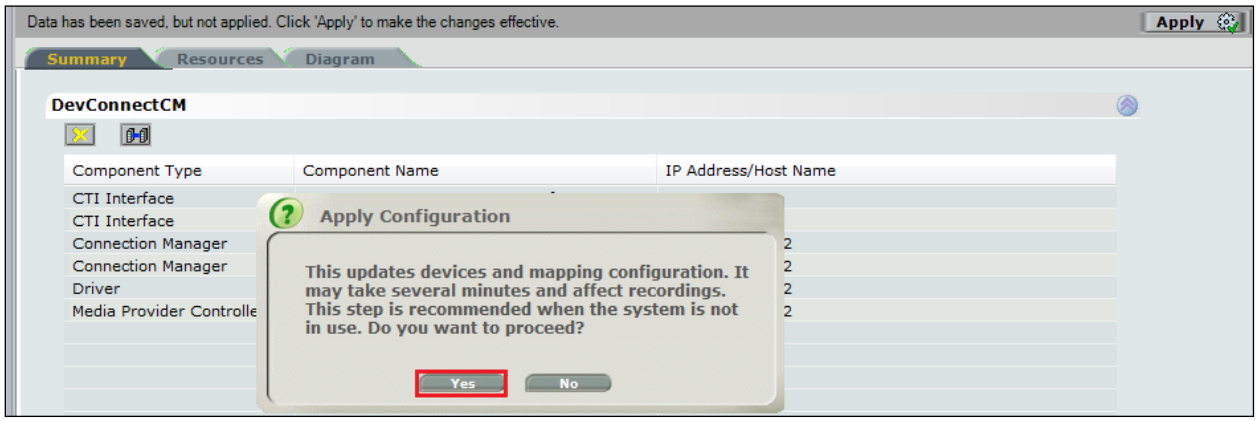


©2023 Avaya Inc. All Rights Reserved.

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

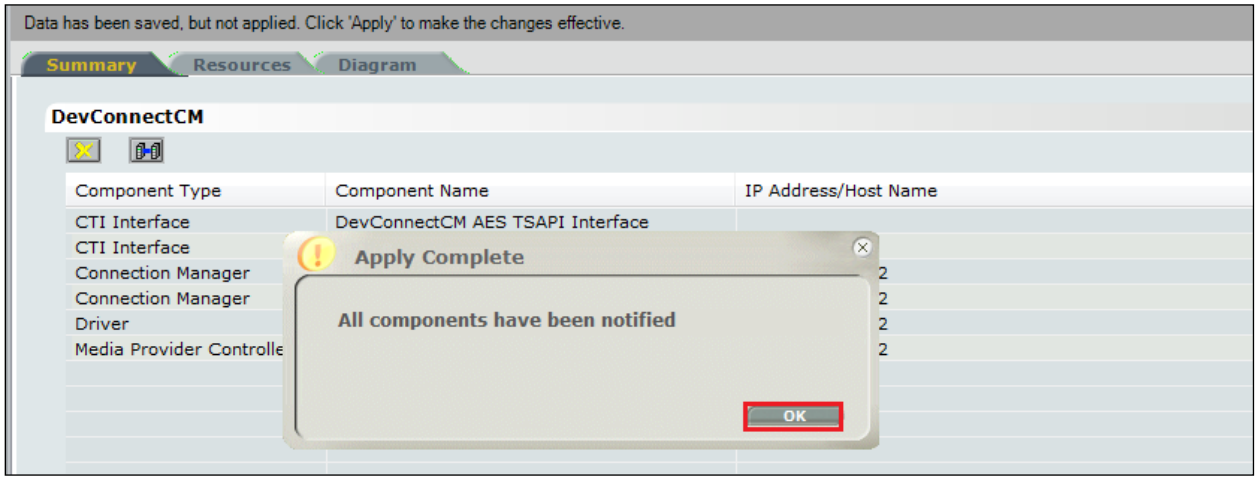


Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed

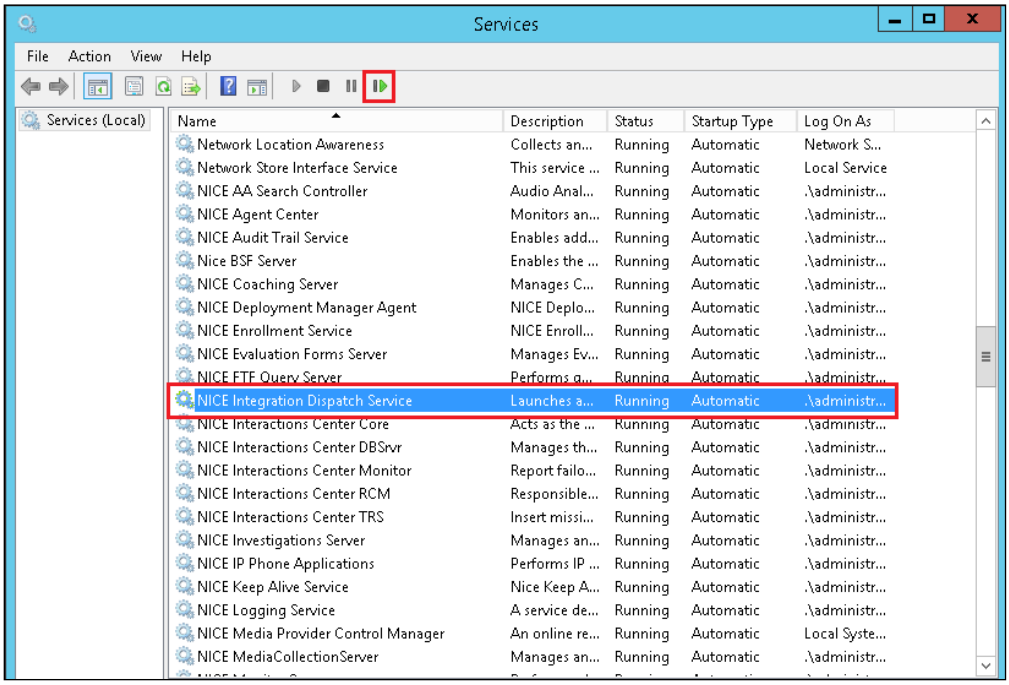


©2023 Avaya Inc. All Rights Reserved.

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



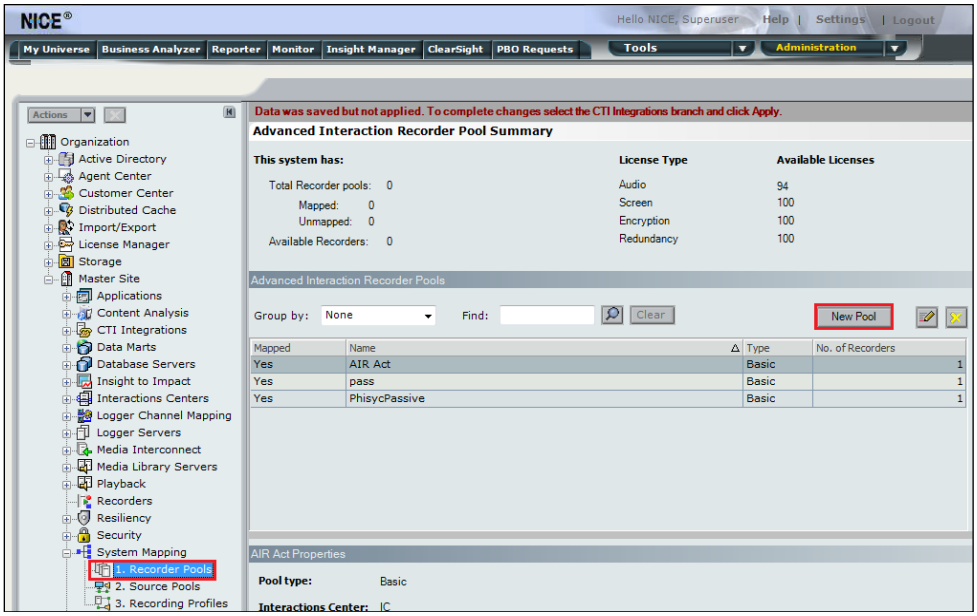
From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.



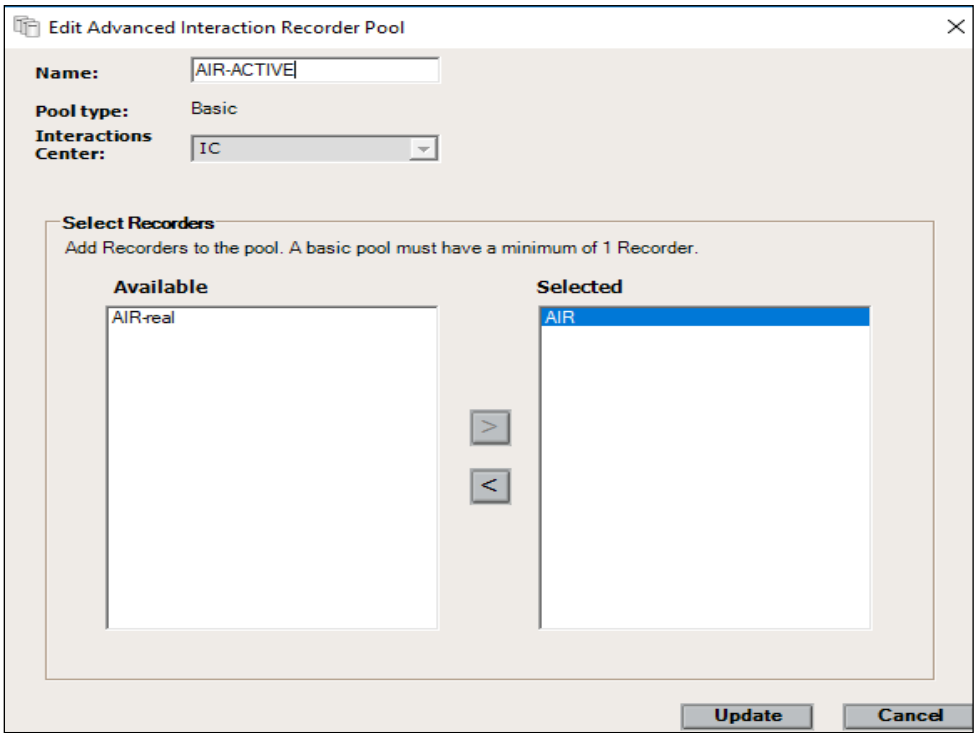
©2023 Avaya Inc. All Rights Reserved.

7.2. System Mapping

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

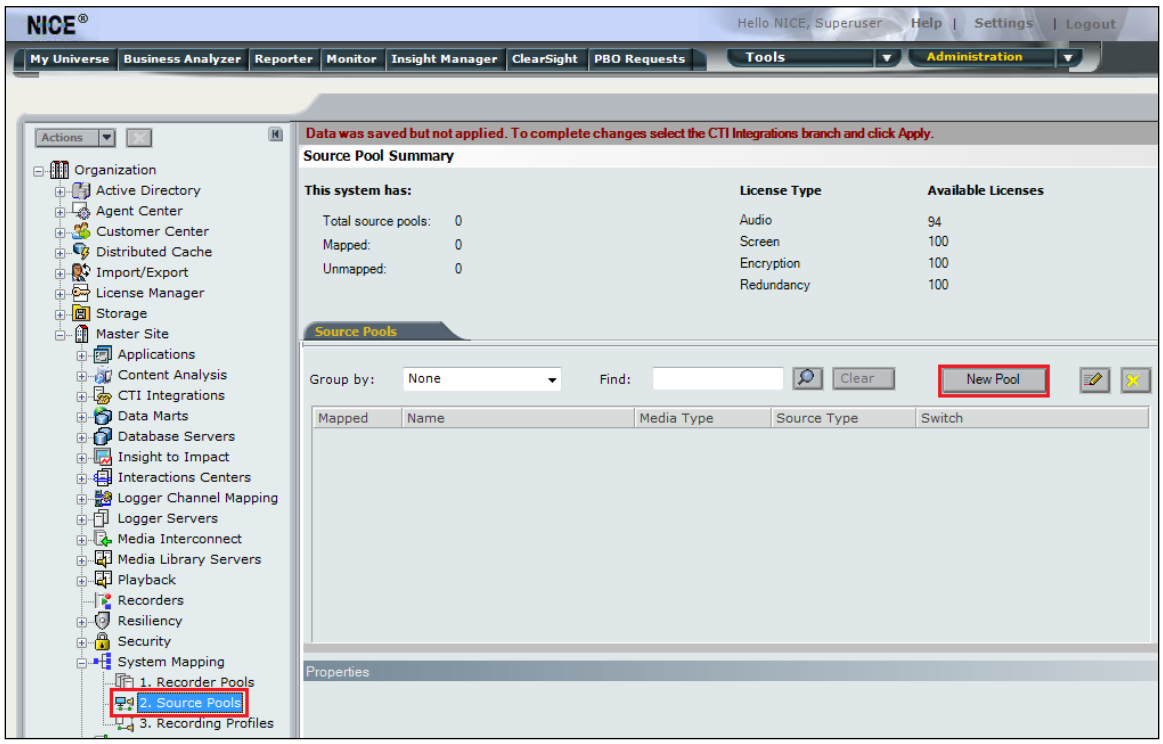


Enter a suitable **Name** for the **Recorder Pool** and select the **AIR** from the list of **Available Recorders** and click on **Update** to continue.

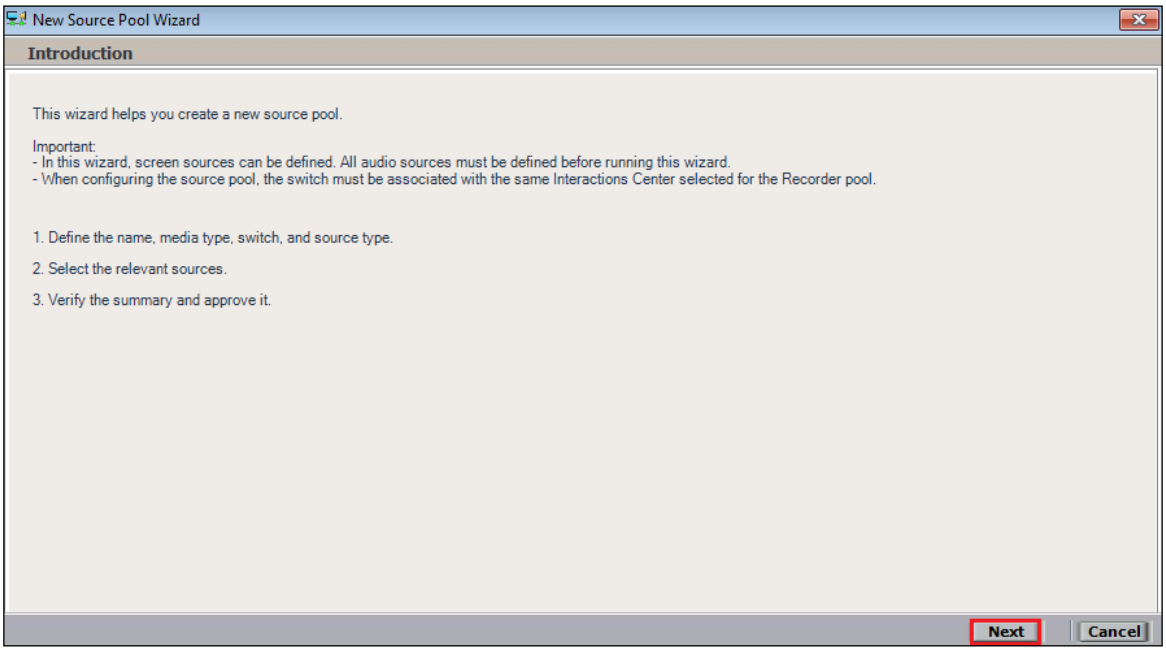


©2023 Avaya Inc. All Rights Reserved.

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

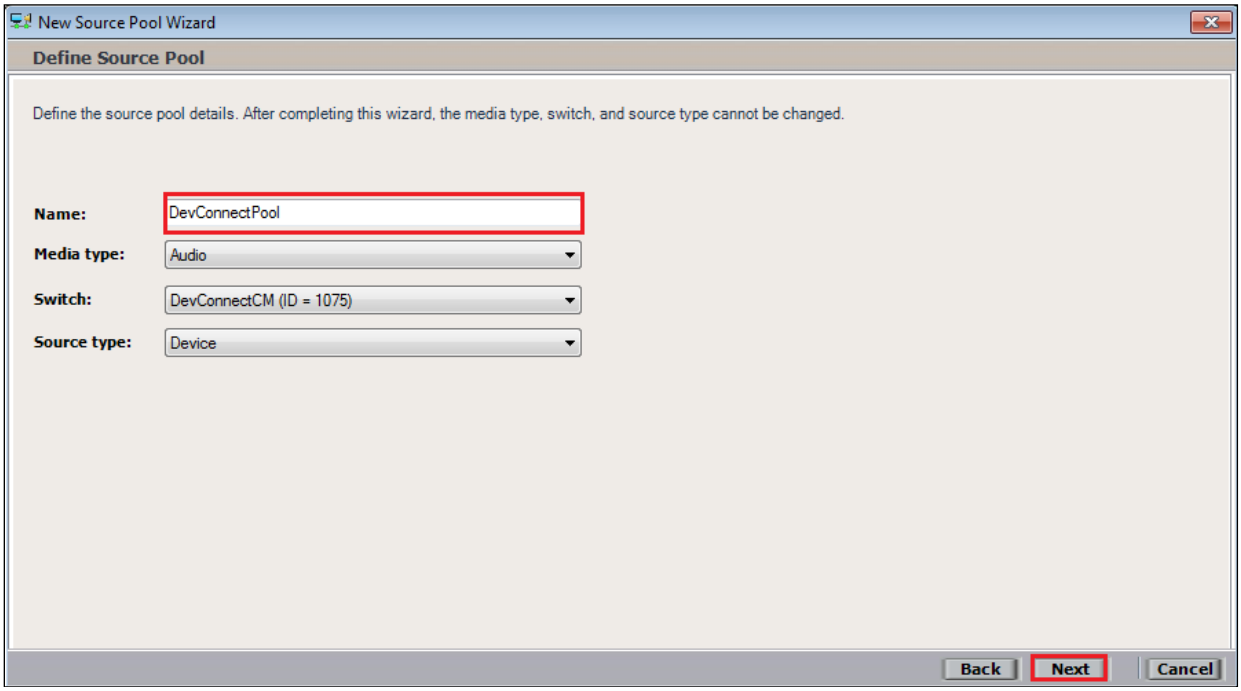


Click on **Next** to continue to add a new **Source Pool**.

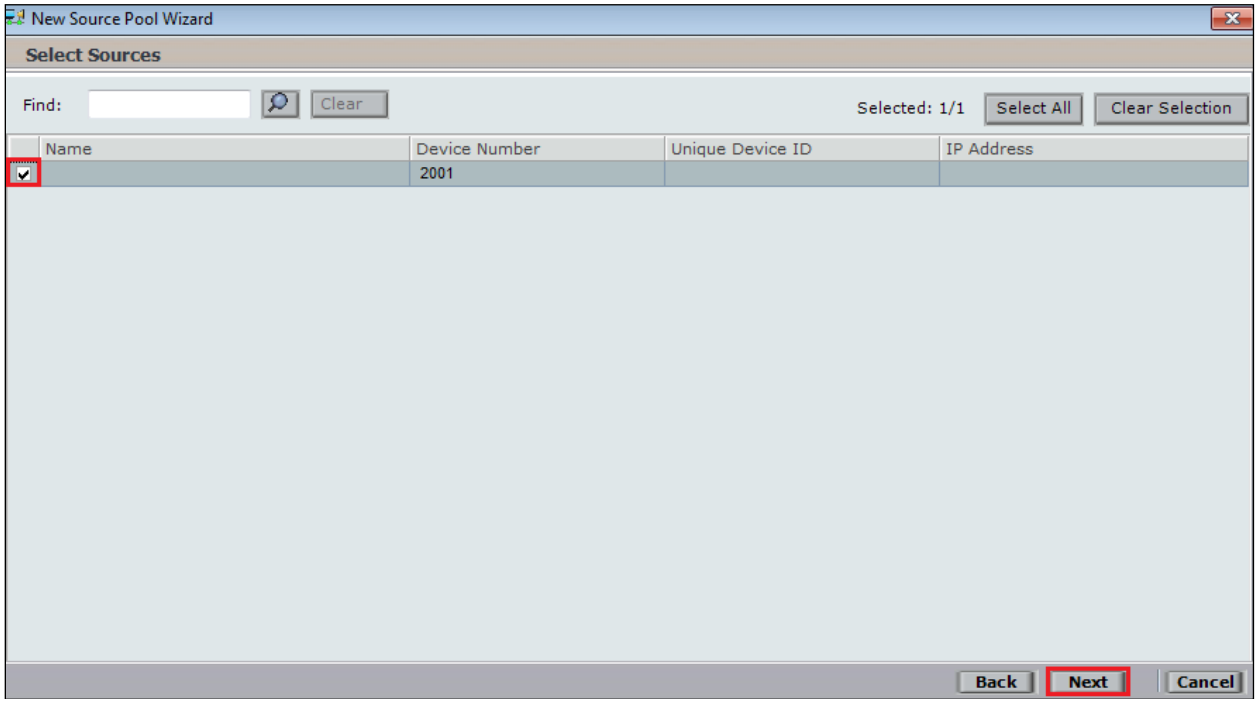


©2023 Avaya Inc. All Rights Reserved.

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

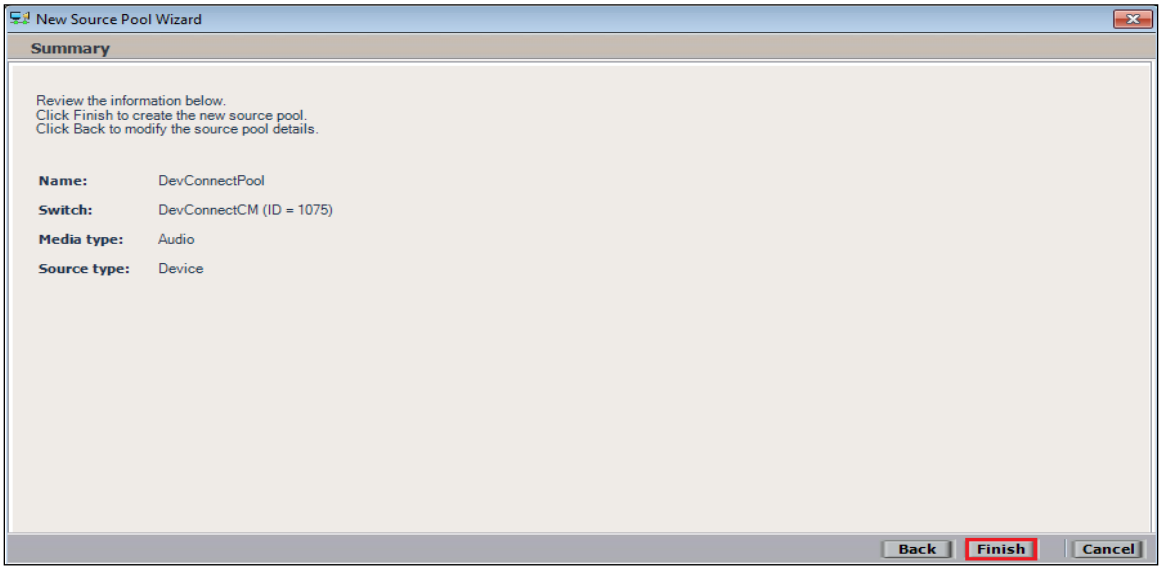


Select the extensions that were created in **Section 7.1**, note only one extension number is shown in the example below but this is not typical. Click on **Next** to continue.

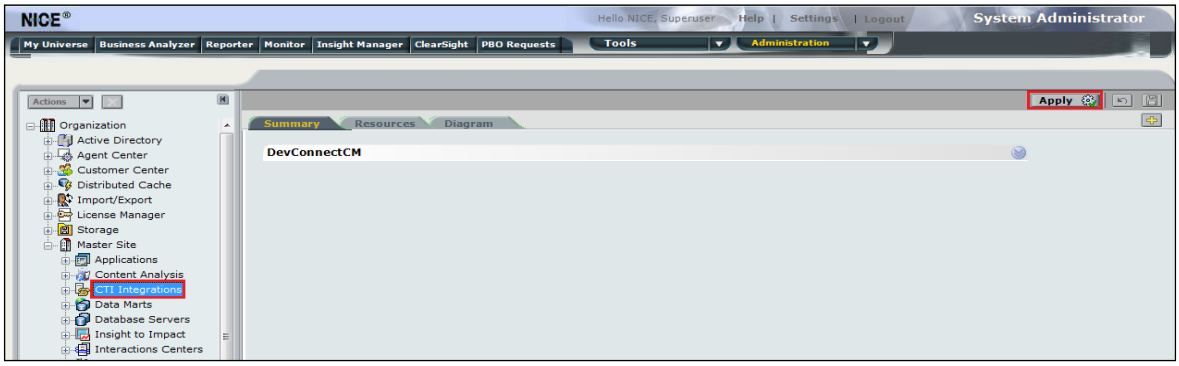


©2023 Avaya Inc. All Rights Reserved.

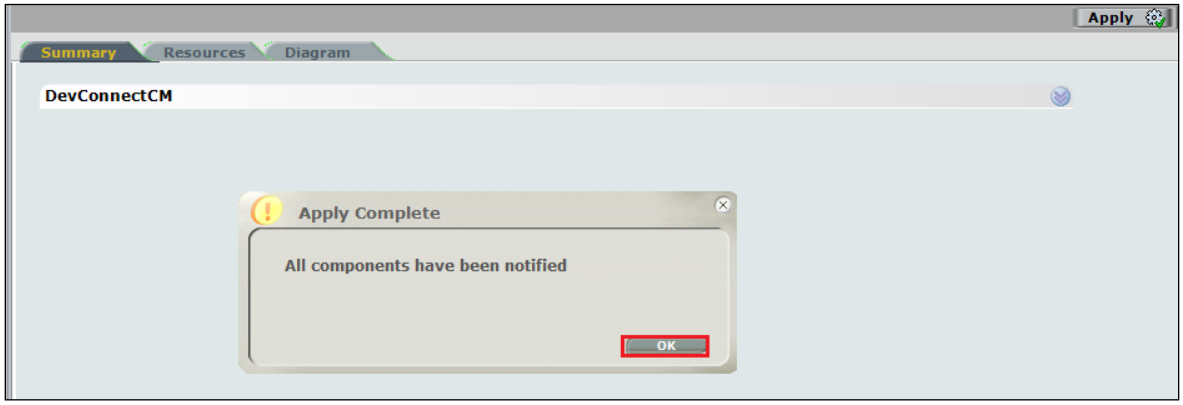
Click on **Finish** to complete the **New Source Pool Wizard**.



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.

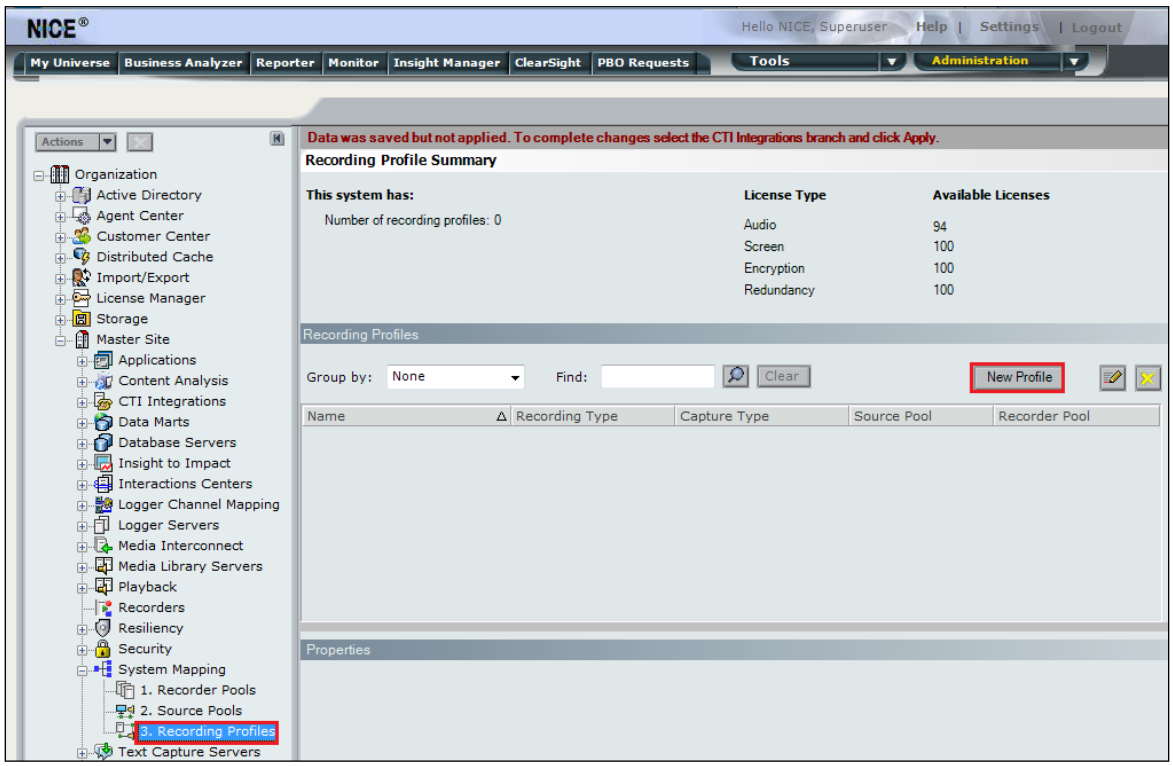


The following screen shows the changes were saved correctly. Click on **OK** to continue.

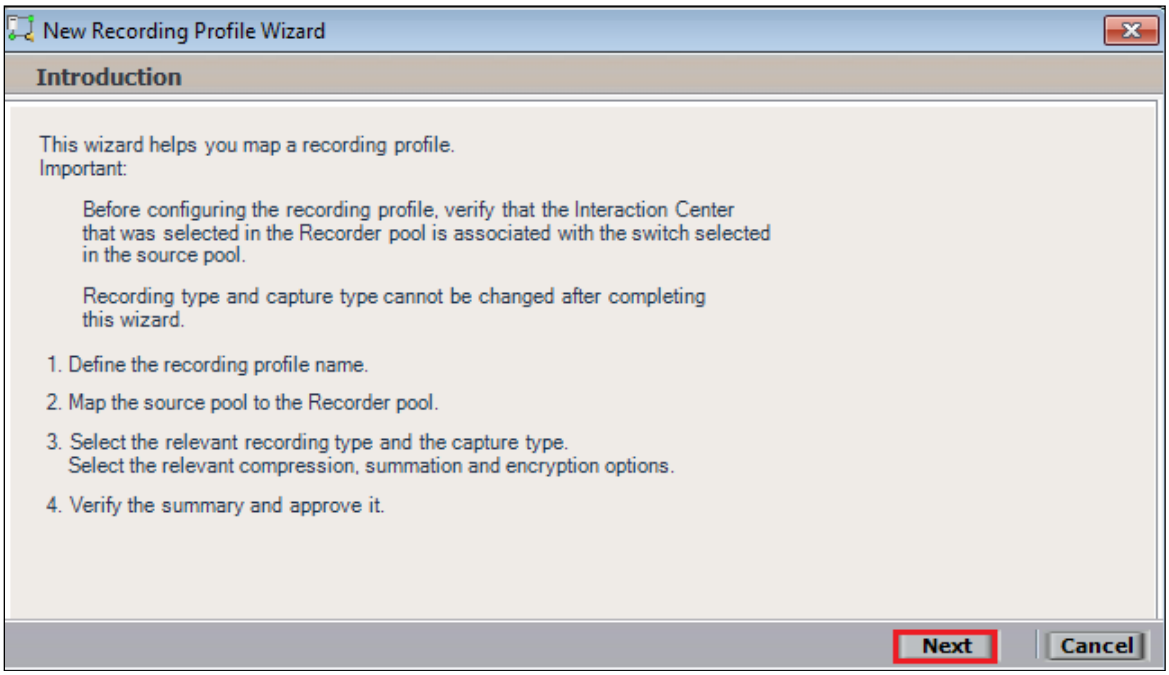


©2023 Avaya Inc. All Rights Reserved.

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

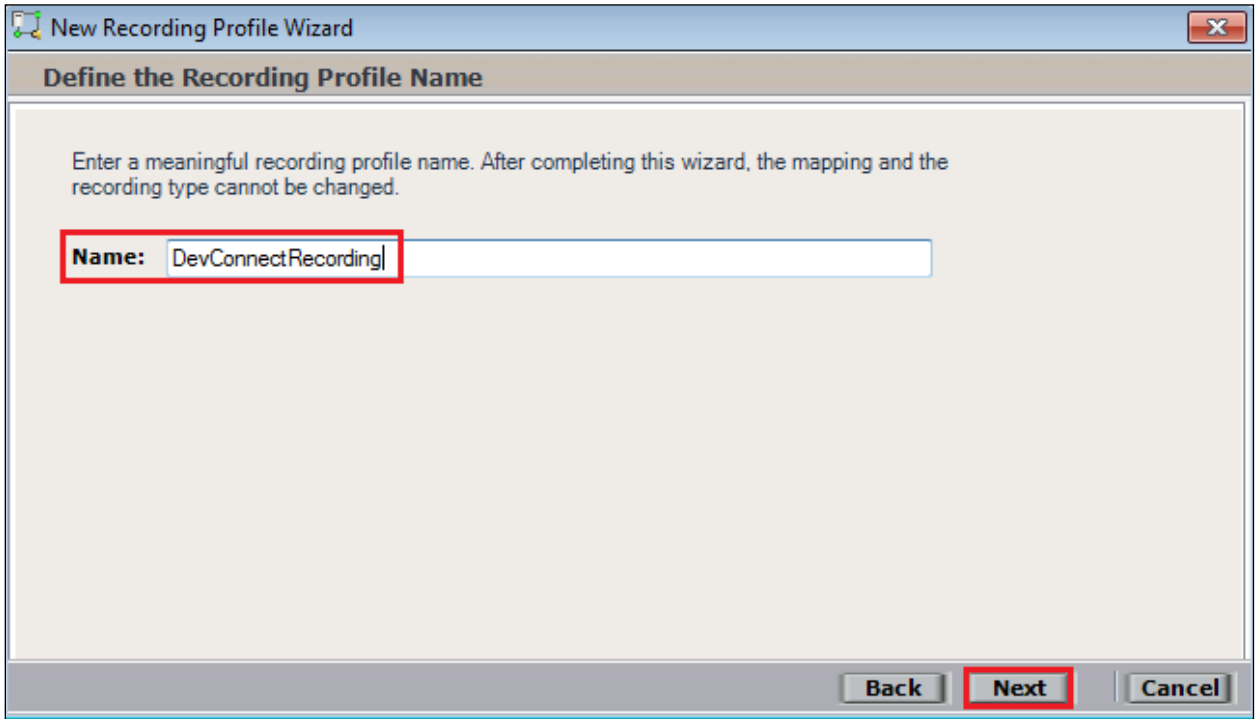


Click on **Next** to continue with the **New Recording Profile Wizard**.

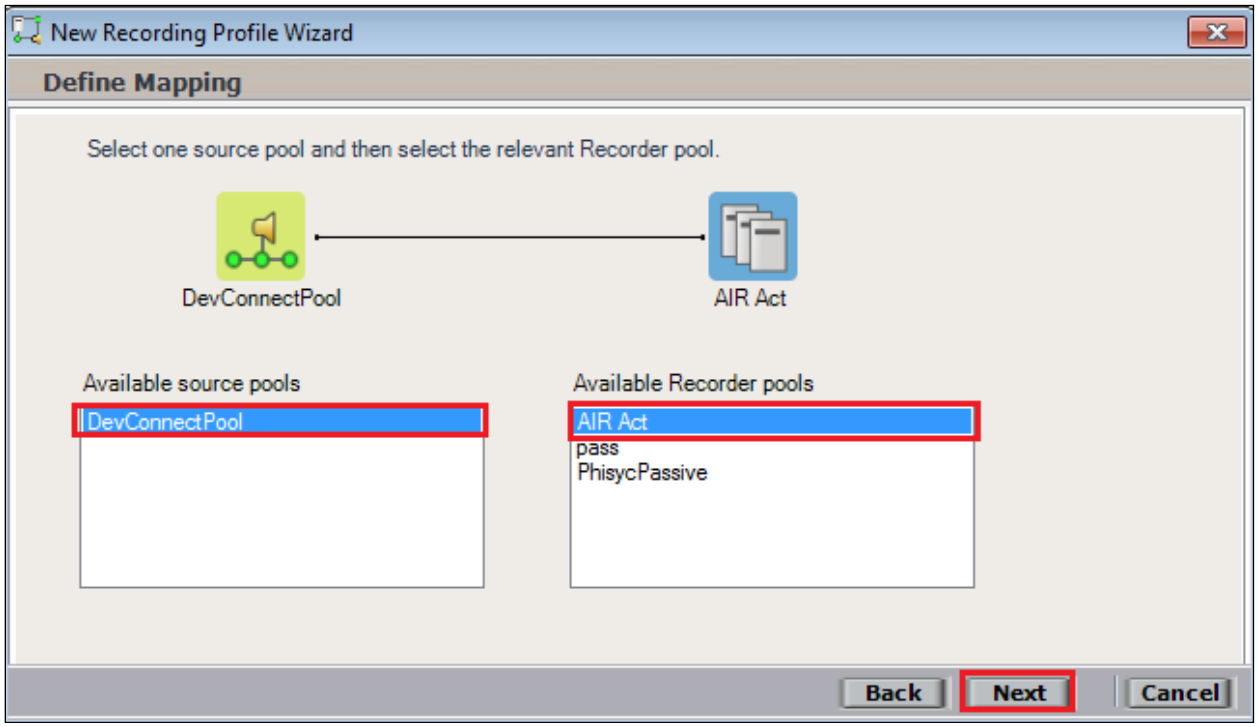


©2023 Avaya Inc. All Rights Reserved.

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

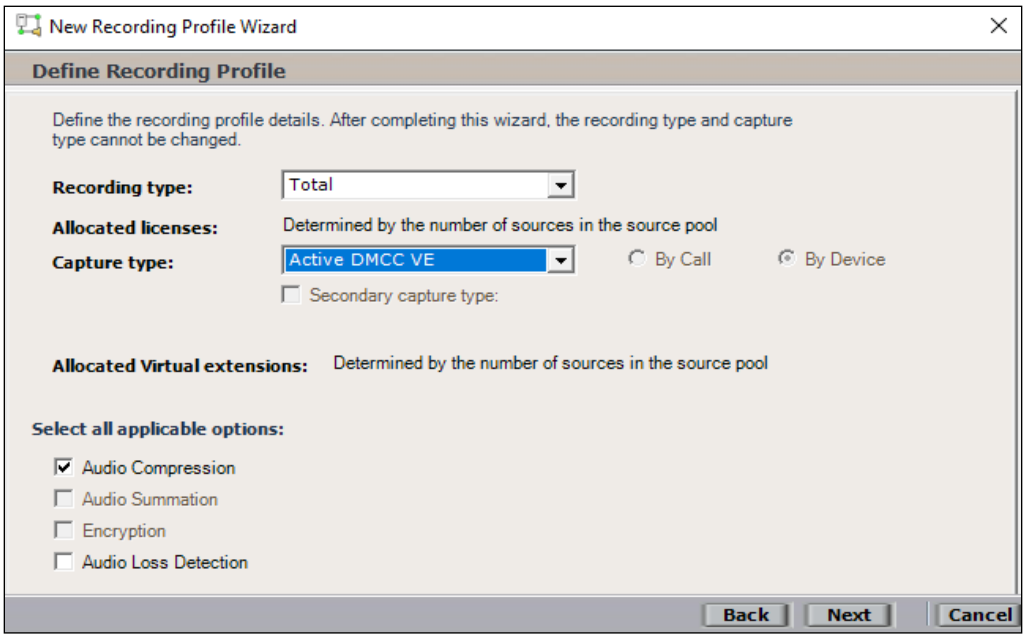


Select the correct **source pool** and **Recorder pool**, and then click **Next** to continue.

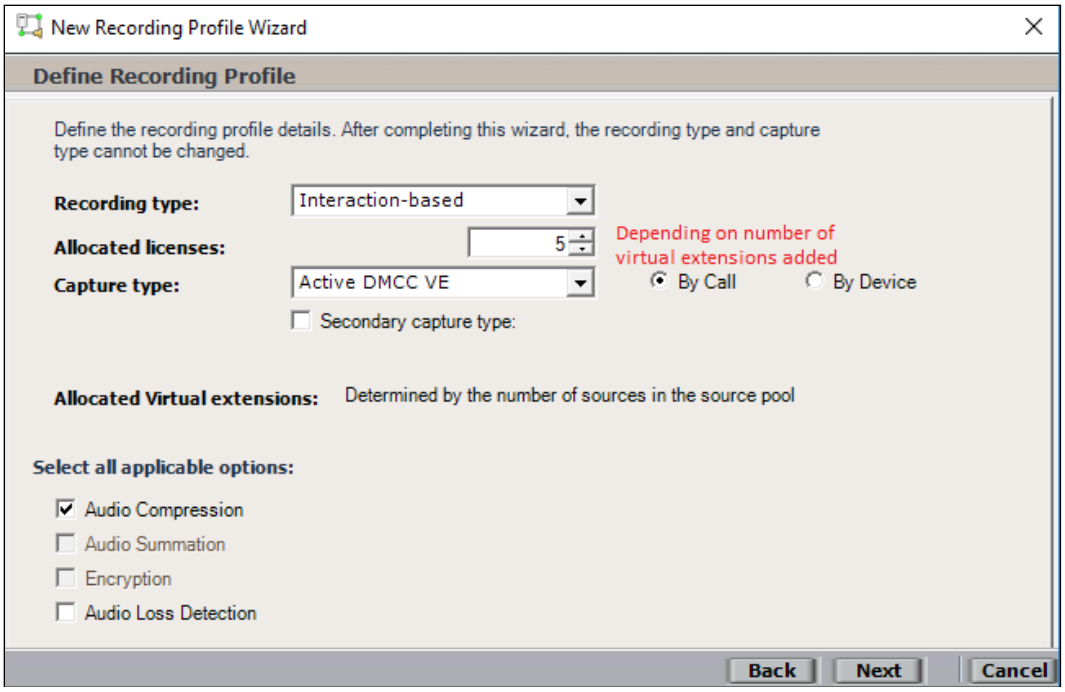


©2023 Avaya Inc. All Rights Reserved.

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

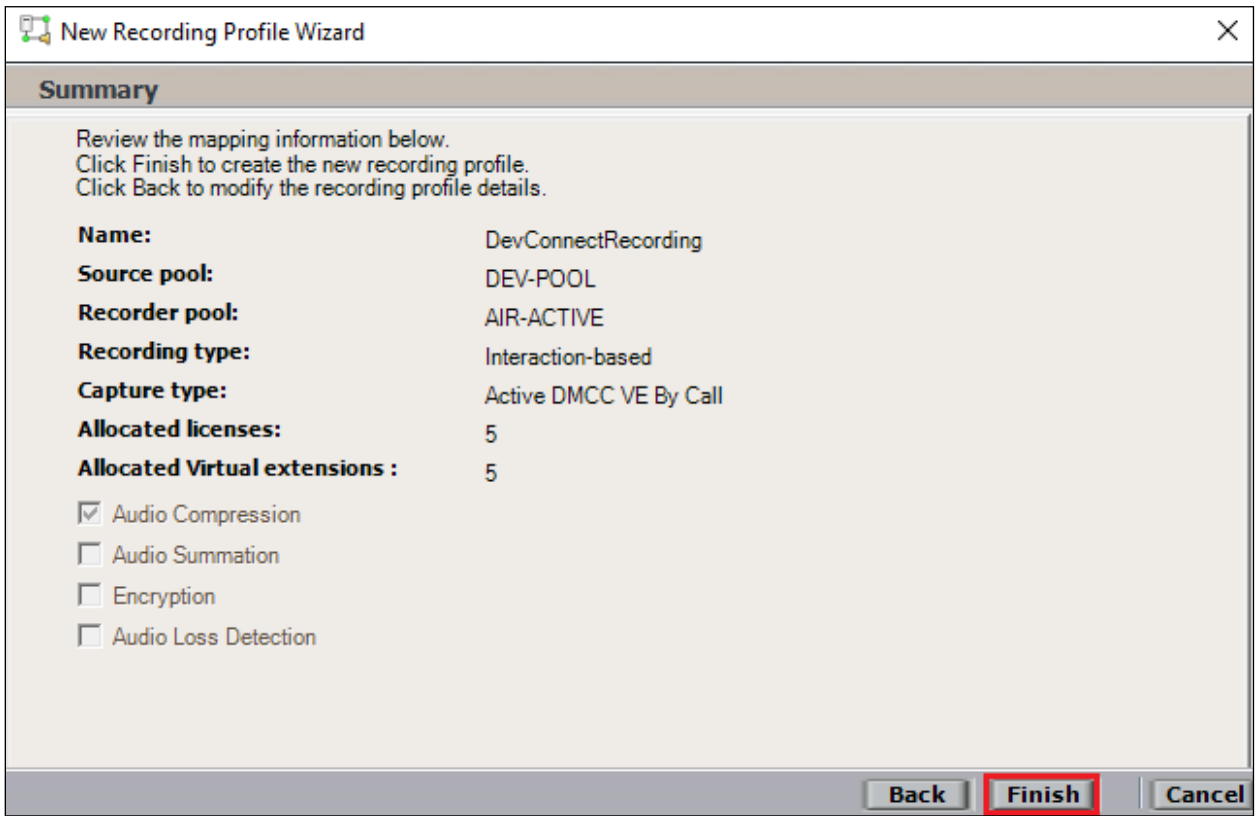


Note: The only difference in the setup for Single Step Conference is with both the choice of **Recording type** which is set to **Interaction-based** and **Capture type** which will be **Active DMCC VE** and **By Call** as shown below.

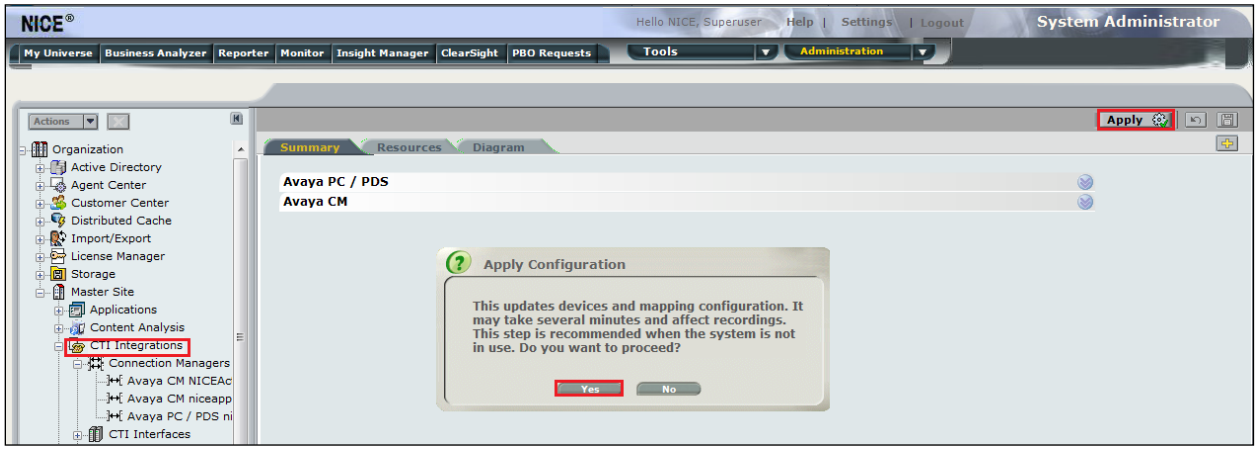


©2023 Avaya Inc. All Rights Reserved.

Click on **Finish** to complete the **New Recording Profile Wizard**. The screen below shows that for Service Observe.



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



This concludes the setup of the NICE Application Server for DMCC Service Observe and Single Step Conference recording.

©2023 Avaya Inc. All Rights Reserved.

8. Verification Steps

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

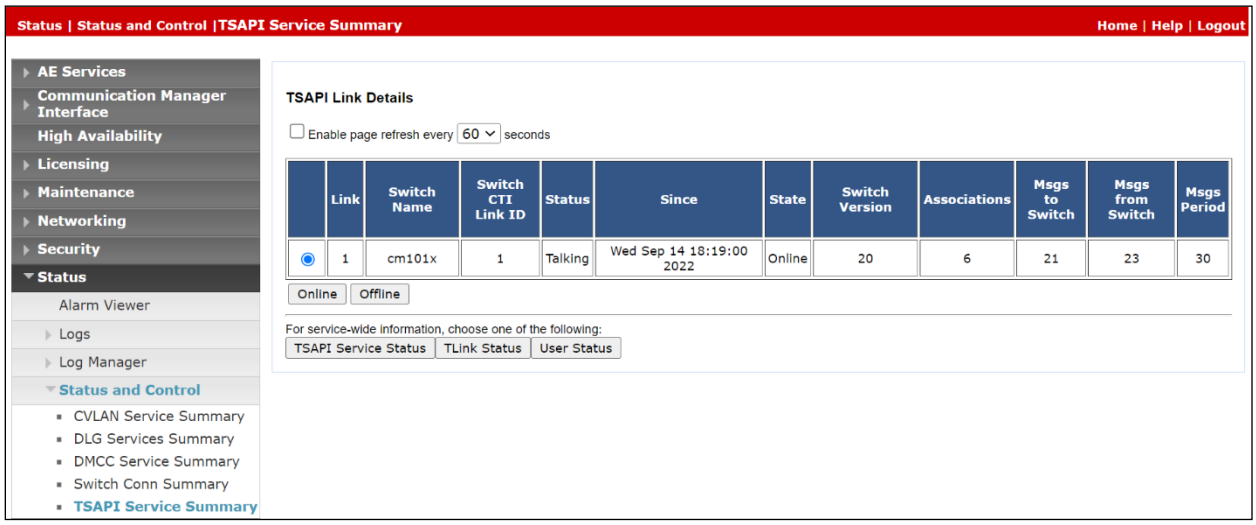
8.1. Verify Avaya Aura® Communication Manager CTI Service State

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         12        no       aespri101x         established    865       865
```

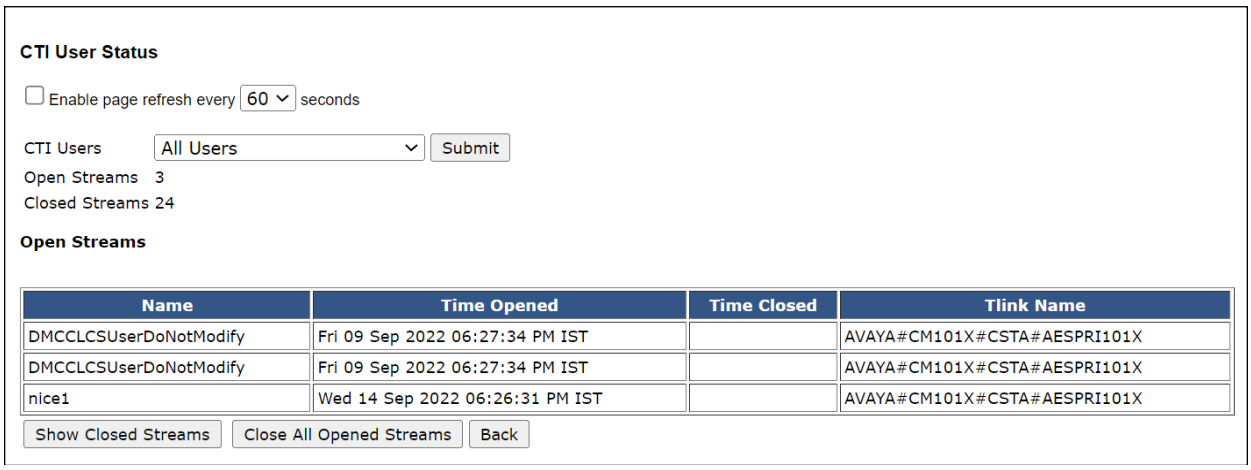
8.2. Verify TSAPI Link

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**.



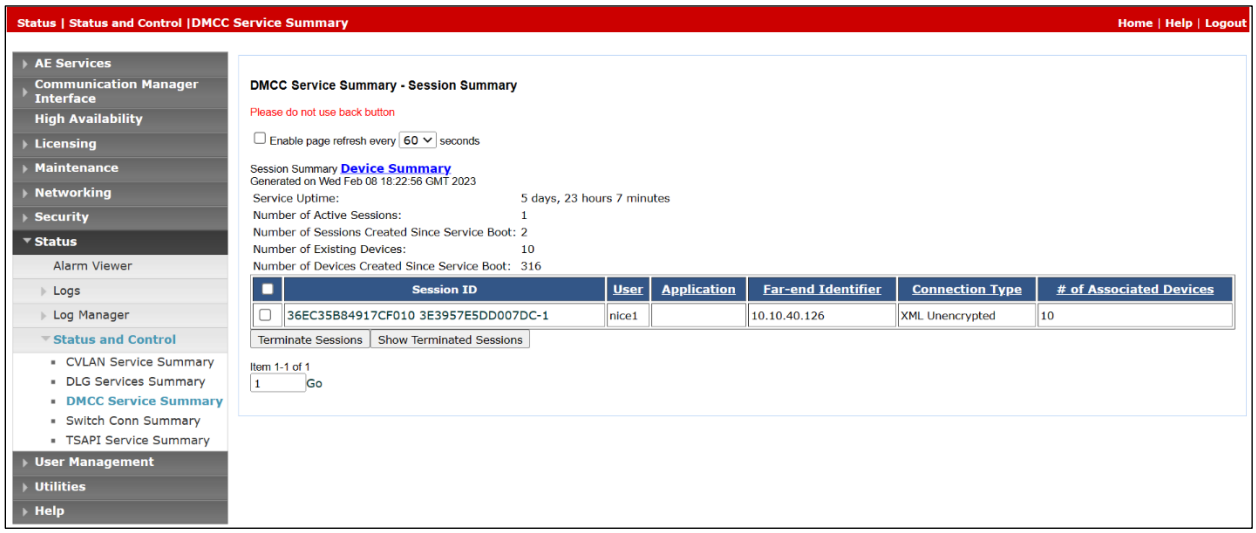
©2023 Avaya Inc. All Rights Reserved.

Clicking on **User Status** from the screen on the previous page should display something similar to that shown below, where the NICE user and corresponding **Tlink Name** are shown.



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.

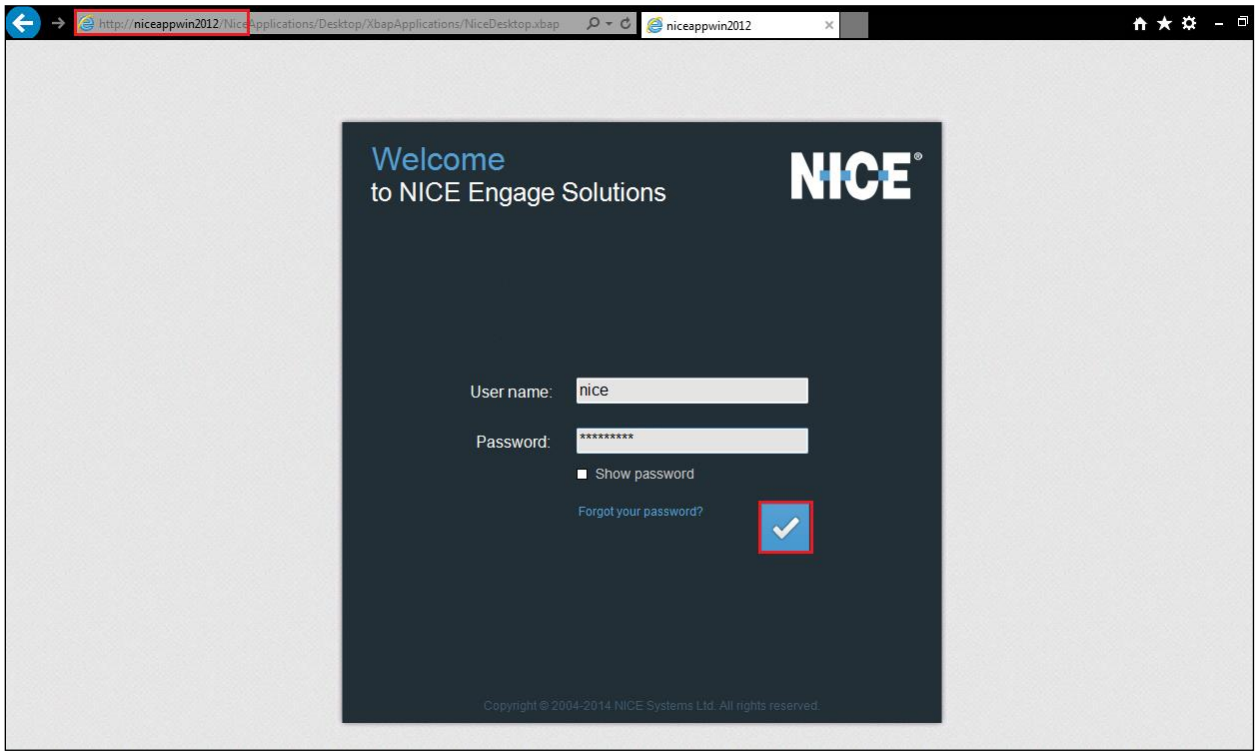


©2023 Avaya Inc. All Rights Reserved.

8.4. Verify calls are being recorded

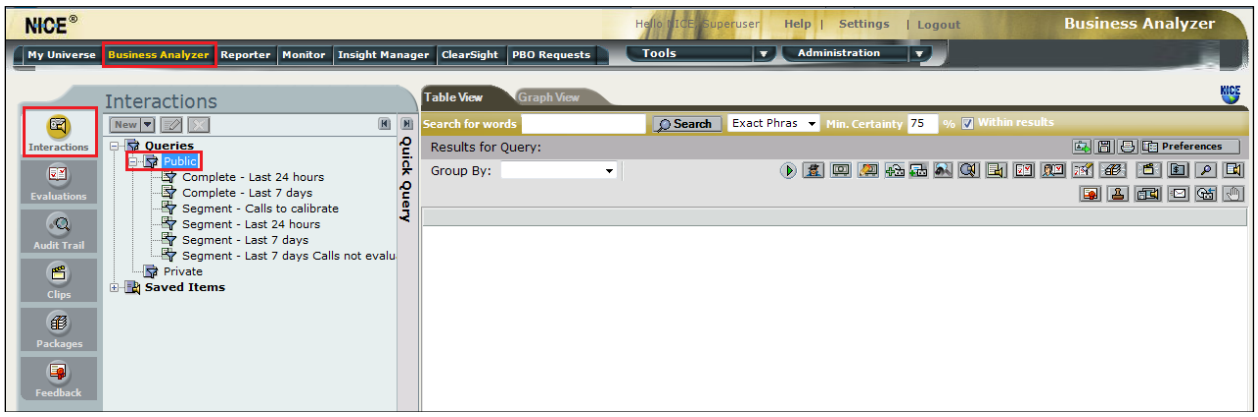
From any of the monitored Avaya endpoints make a series of inbound and outbound calls. Once these calls are completed, they should be available for playback through a web browser to the NICE Application Server.

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

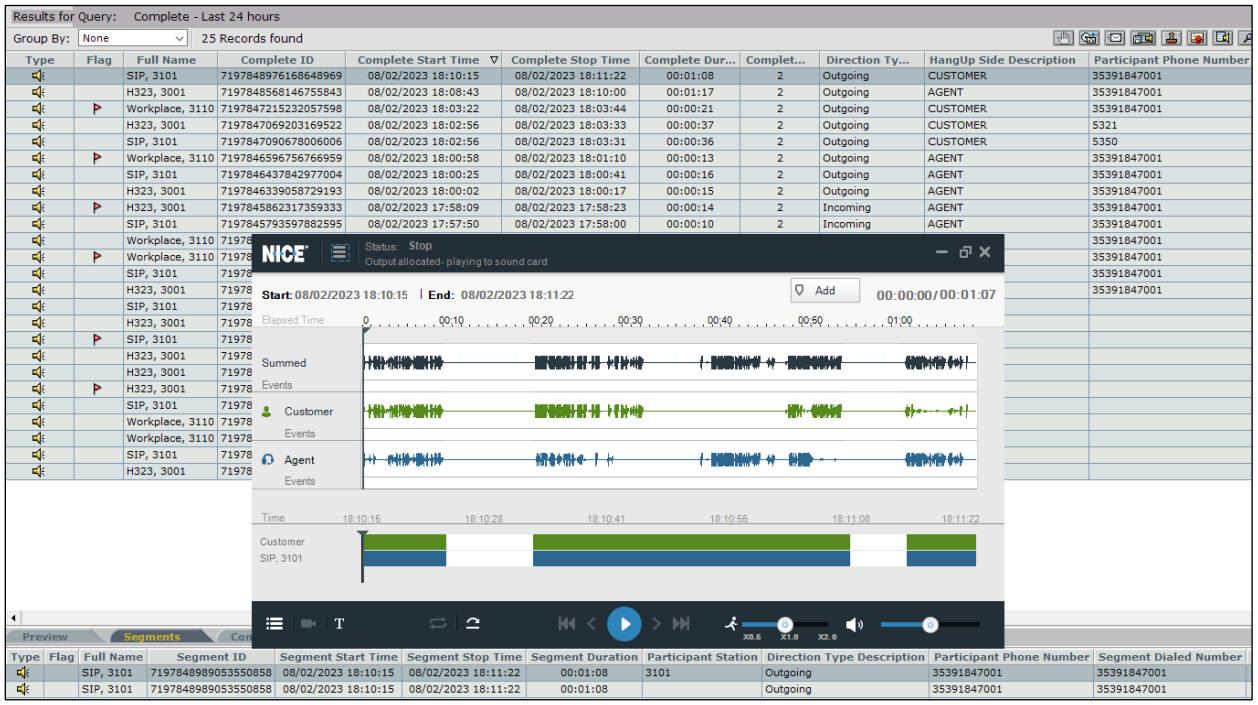


©2023 Avaya Inc. All Rights Reserved.

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



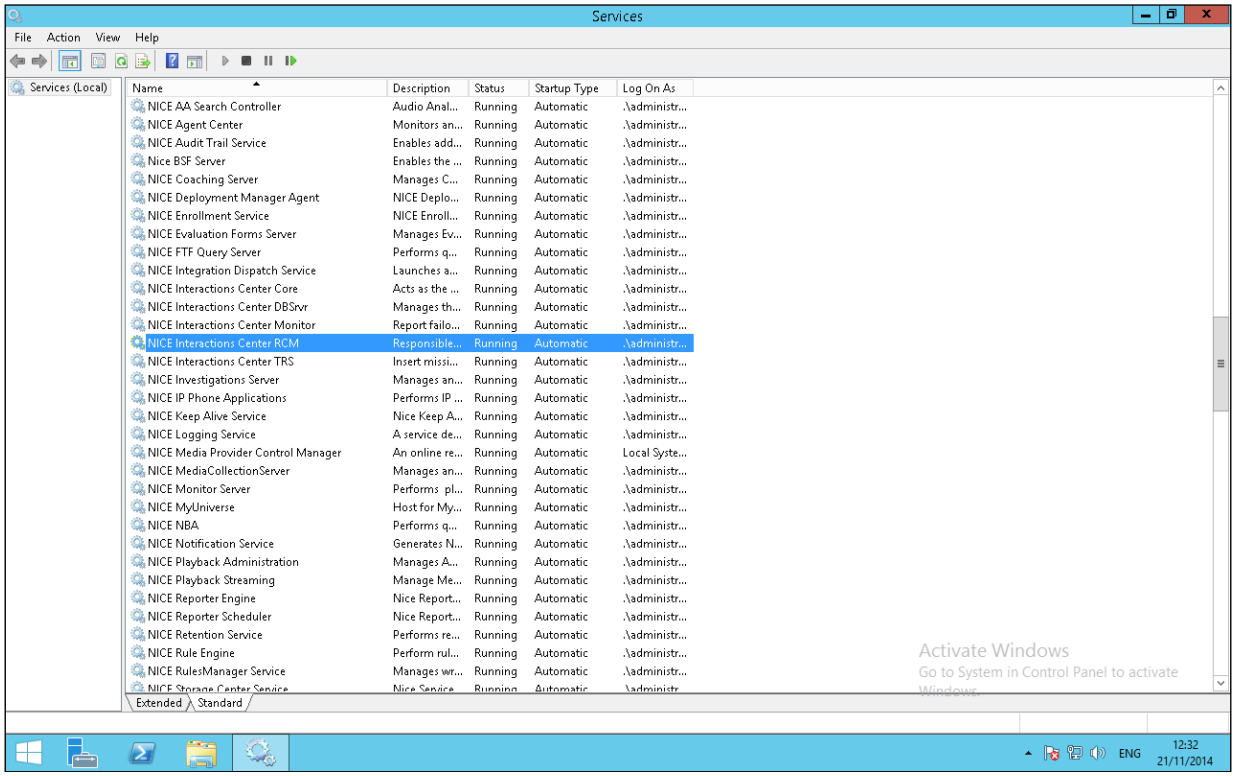
Click on **Complete – Last 24 hours**. This should reveal all the recordings that took place over the previous 24 hours. Select the required recording from the list and double-click on this to play the recording. The NICE player is opened, and the recording is presented for playback. Click on the **Play/Pause** icon highlighted below to play back the recording.



©2023 Avaya Inc. All Rights Reserved.

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.



©2023 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform R7.3 to successfully interoperate with Avaya Aura® Communication Manager R10.1 using Avaya Aura® Application Enablement Services R10.1 to connect to using DMCC Service Observation and Single Step Conference 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® System Manager*. Release 10.1.x, Issue 6, June 2022.
[2] *Administering Avaya Aura® Session Manager*. Release 10.1.x, Issue 3, April 2022.
[3] *Administering Avaya Aura® Communication Manager*. Release 10.1, Issue 1, December 2021.
[4] *Administering Avaya Aura® Application Enablement Services*. Release 10.1.x, Issue 4, April 2022.
[5] *Implementing and Administering Avaya Aura® Media Server*. Release 10.1.x, Issue 2, July 2022.
[6] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[7] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

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

©2023 Avaya Inc. All Rights Reserved.

©2023 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.