Application Notes for NICE Engage Platform R7.1 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 using DMCC Multiple Registration for Stereo Recording - 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 R8.1, and Avaya Aura® Session Manager R8.1, and Avaya Aura® Application Enablement Services R8.1.

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 R7.1 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R8.1, an Avaya Aura® Session Manager R8.1, and Avaya Aura® Application Enablement Services R8.1. NICE Engage Platform uses Communication Manager's Multiple Registration 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 H.323, SIP and Digital endpoints, listed in **Section 4**.

Device Media Call Control (DMCC) allows 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.

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 Multiple Registration method to record the calls, using the TSAPI connection to monitor the events necessary to start and stop the recordings. The application uses the AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media streams via the recording device and records the call, in stereo.

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 Multiple Registration. 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.

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 Recording 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.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park, Call Pickup, Bridged Appearance and Service Observing.
- **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.

2.2. Test Results

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

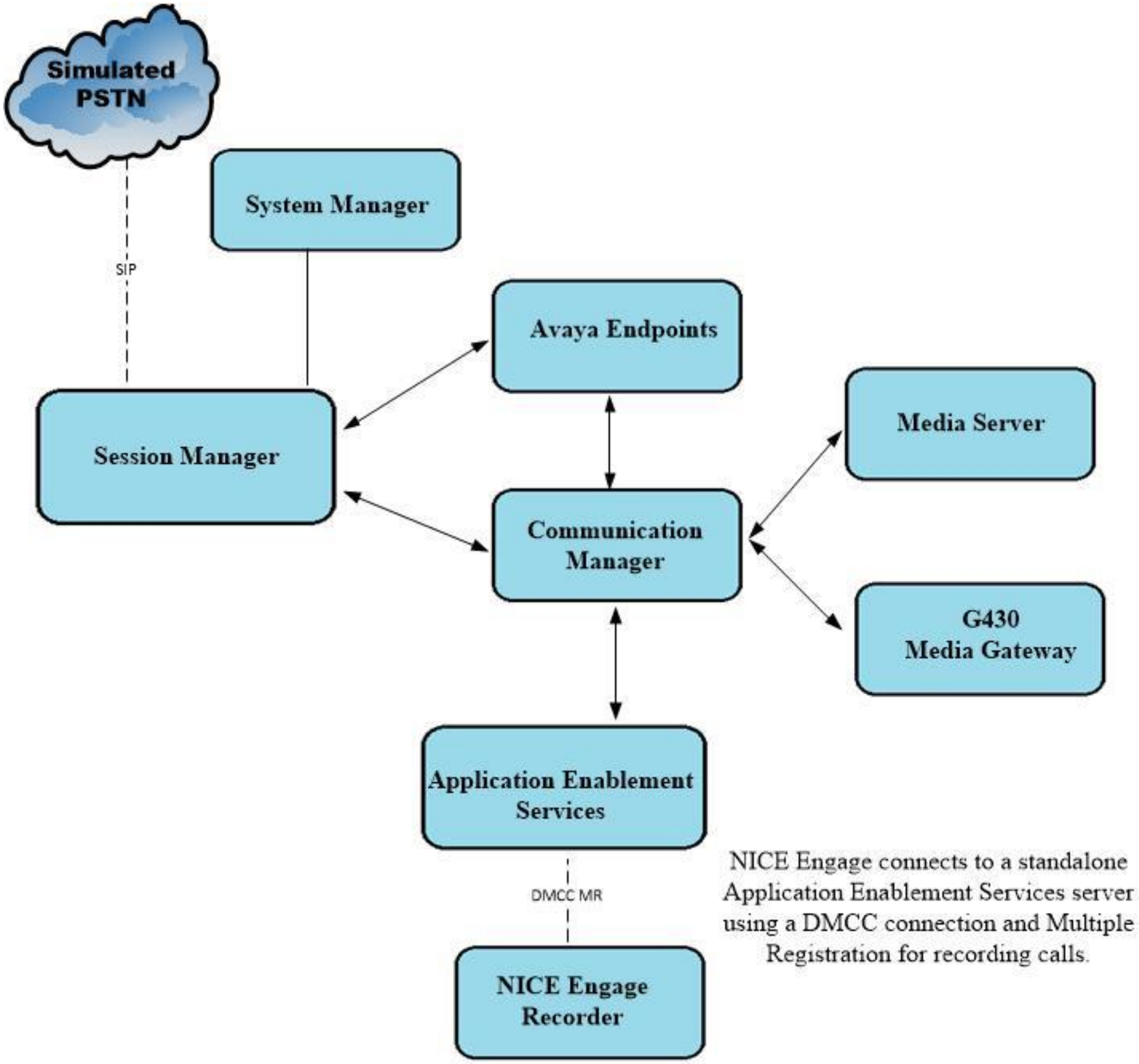
- When a call is Parked and Unparked, the first leg is recorded, the second leg (unparked call) is recorded but there is no RTP present when a SIP phone is unparking the call. Avaya is investigating the issue.
- Observing a station/user/extension that is not monitored from a station/user/extension that is monitored can cause no CTI events on the observer. Recordings will appear in NICE Business Analyser (NBA), according to pre-configured Total Recording Solution (TRS) insertion time out (default 5h). During testing, NICE decreased time out to get stored recordings shortly.

2.3. Support

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

3. Reference Configuration

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



NICE Engage connects to a standalone Application Enablement Services server using a DMCC connection and Multiple Registration for recording calls.

Figure 1: Connection of NICE Engage Platform R7.1 with Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Aura® Application Enablement Services R8.1

4. Equipment and Software Validated

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

Avaya Equipment	**Release/Version**
Avaya Aura® System Manager running on a virtual server	8.1.3.2 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.2.1012646 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	8.1.3.2 Build No. – 8.1.3.2.813207
Avaya Aura® Communication Manager running on a virtual server	8.1.3.2 – FP3SP2 R018x.01.0.890.0 Update ID 01.0.890.0-26989
Avaya Aura® Application Enablement Services	8.1.3.2
Avaya Aura® Media Server	8.0.2.184
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8502
Avaya J189 SIP Deskphone	4.0.10.1.2
Avaya 9408 Digital Deskphone	V2.0
Avaya Agent for Desktop	2.0.6.8.3002
NICE Equipment	**Release/Version**
NICE Engage Platform - NICE Engage Application Server - NICE Engage AIR - NICE Engage NDM Server	7.1

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

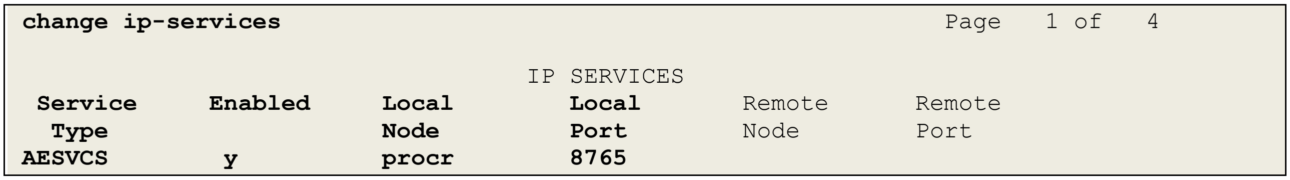
Display the procr IP address by using the command **display node-names ip proc** and note the IP address for the **procr**.

```
display node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.40.34
aes81vmpg           10.10.40.16
default             0.0.0.0
g450                10.10.40.15
procr               10.10.40.37
```

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**.

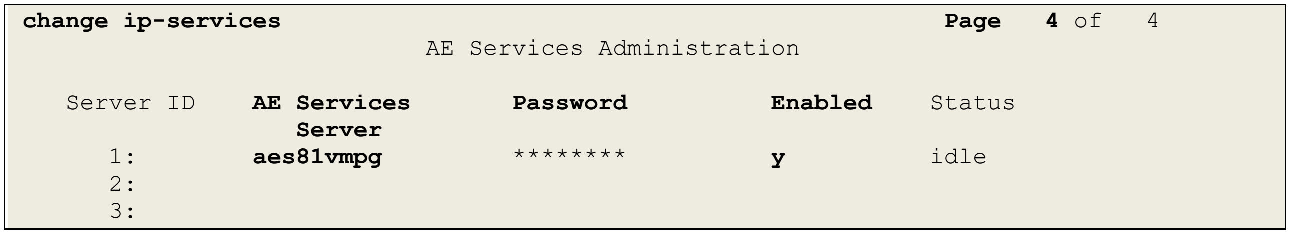


```
change ip-services                                            Page   1 of   4

                                  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 **aes81vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

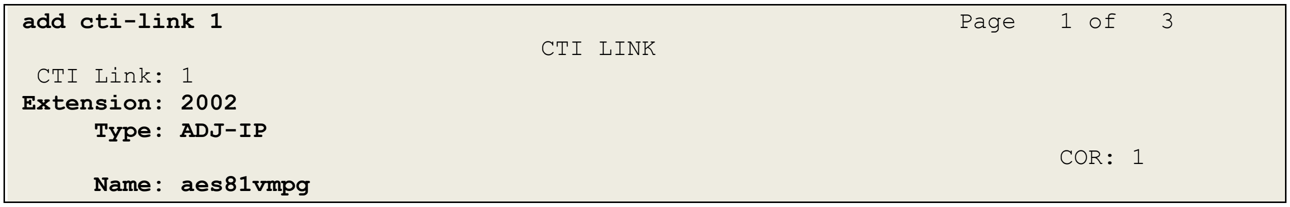
Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server; this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –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:        aes81vmpg          ********          y          idle
      2:
      3:
```

5.4. Configure CTI Link for TSAPI Service

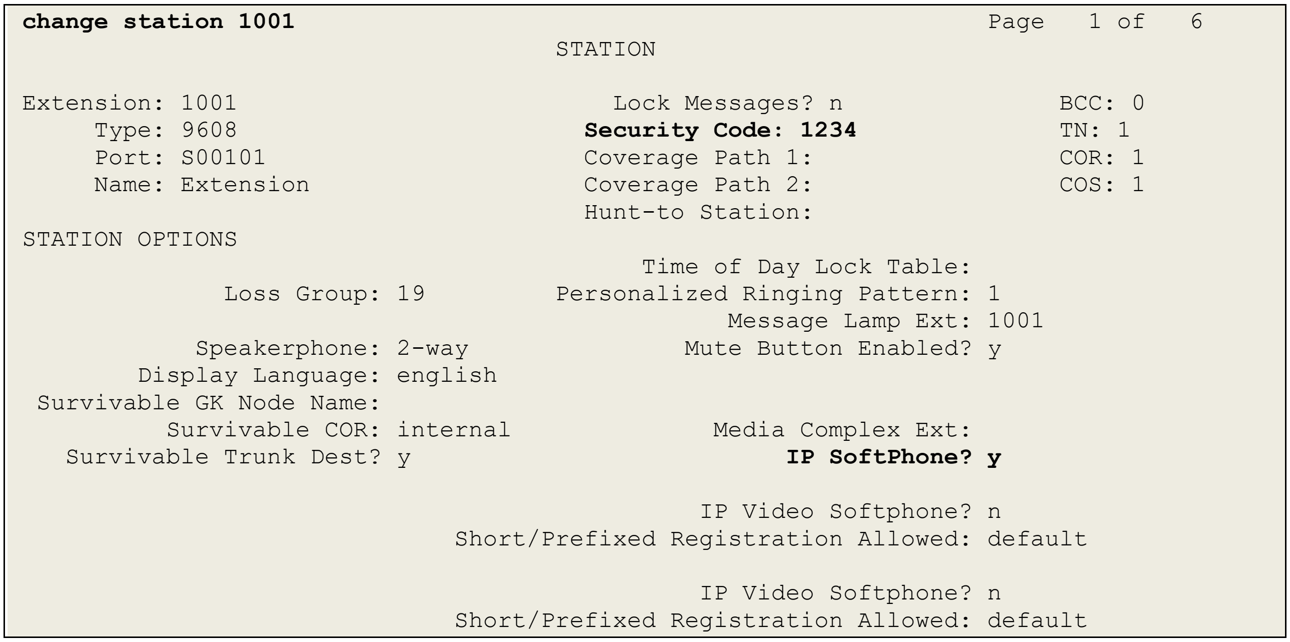
Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.



```
add cti-link 1                                                 Page   1 of   3
                                   CTI LINK
 CTI Link: 1
Extension: 2002
     Type: ADJ-IP
                                                                      COR: 1
     Name: aes81vmpg
```

5.5. Configure H.323 Stations for Multi-Registration

All endpoints that are to be monitored by NICE will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required during the NICE Recorder setup in **Section 7.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

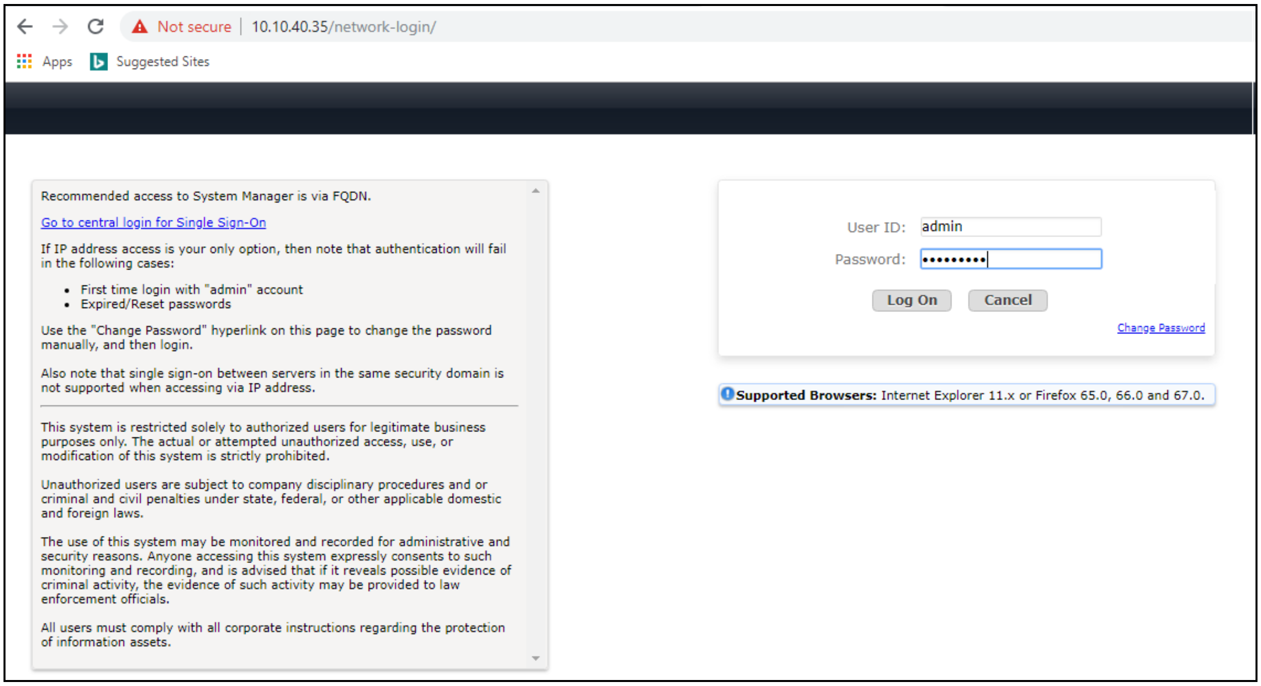


```
change station 1001                                                Page   1 of   6
                                     STATION

Extension: 1001                           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: 1001
            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

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

5.6. Configure SIP Stations for Multiple Registration

Each Avaya SIP endpoint or station that needs to be monitored for call recording will need to have “Type of 3PCC Enabled” is set to “Avaya” and “Softphone” set to “Yes”. Changes to SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN >/network-login**, where **<FQDN>** is the fully qualified domain name of System Manager or the IP address of System Manager can be used as an alternative to the FQDN. 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.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

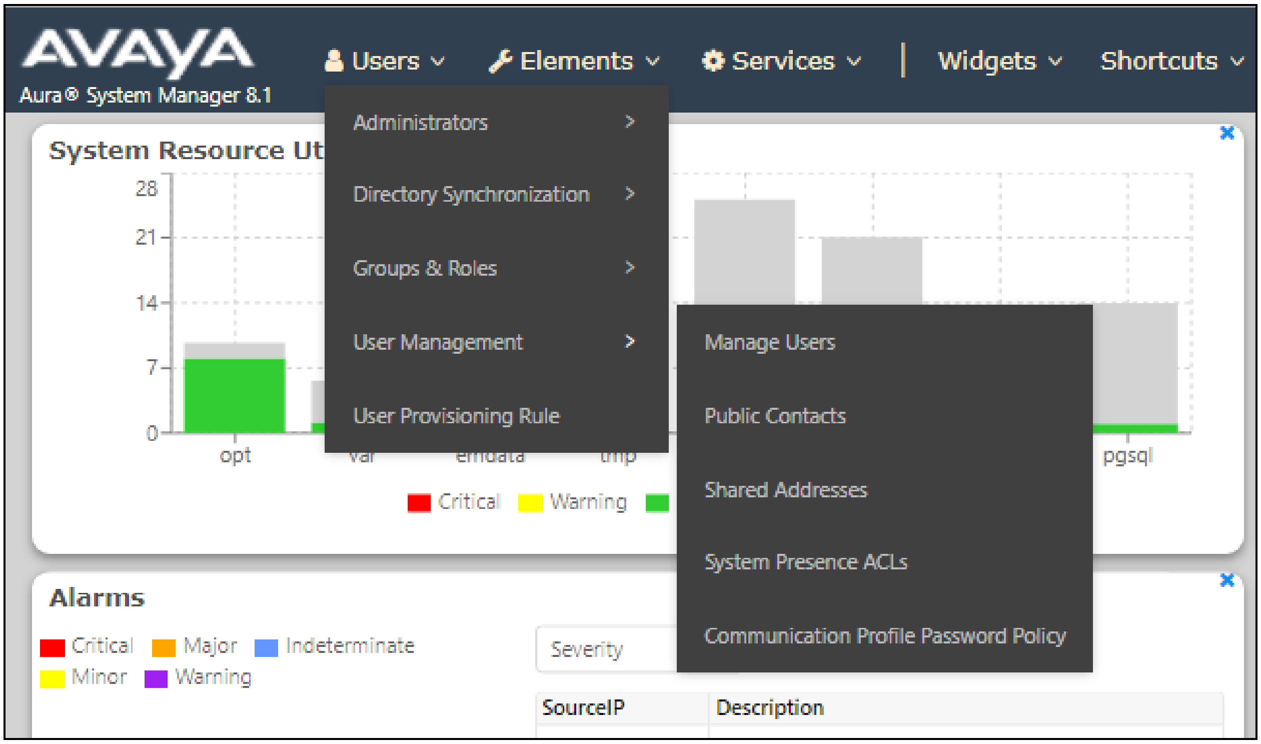
All users must comply with all corporate instructions regarding the protection of information assets.

User ID: admin

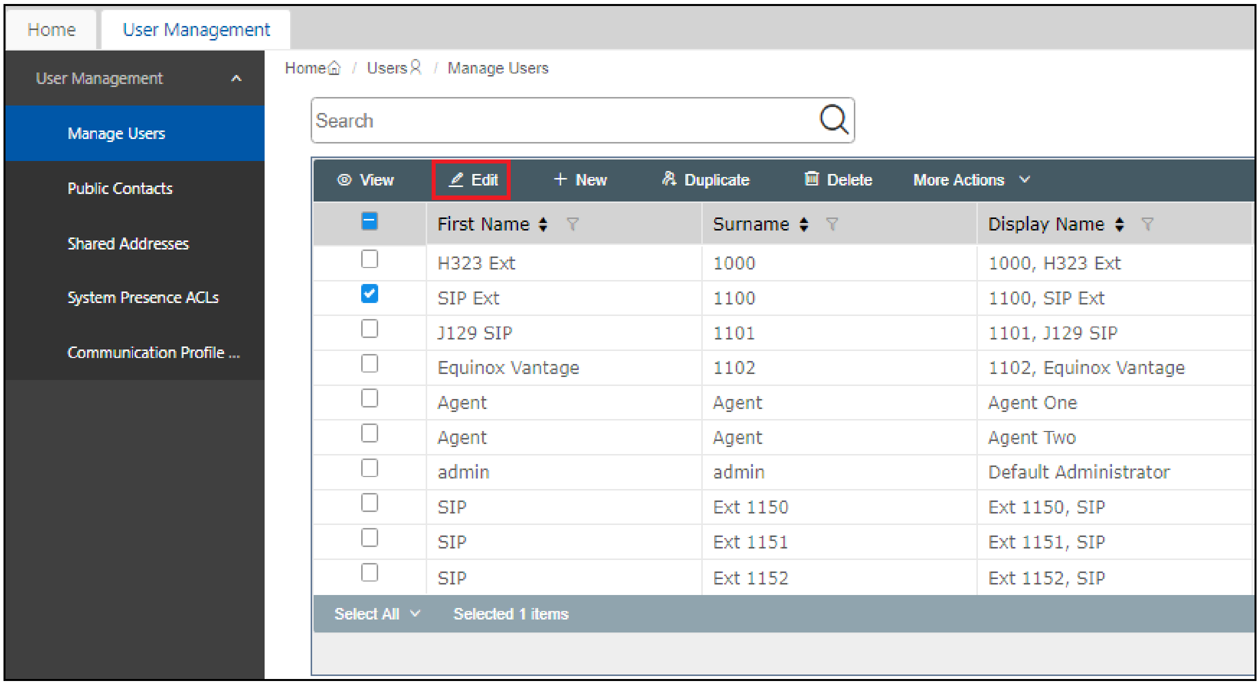
Password: •••••••••

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

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

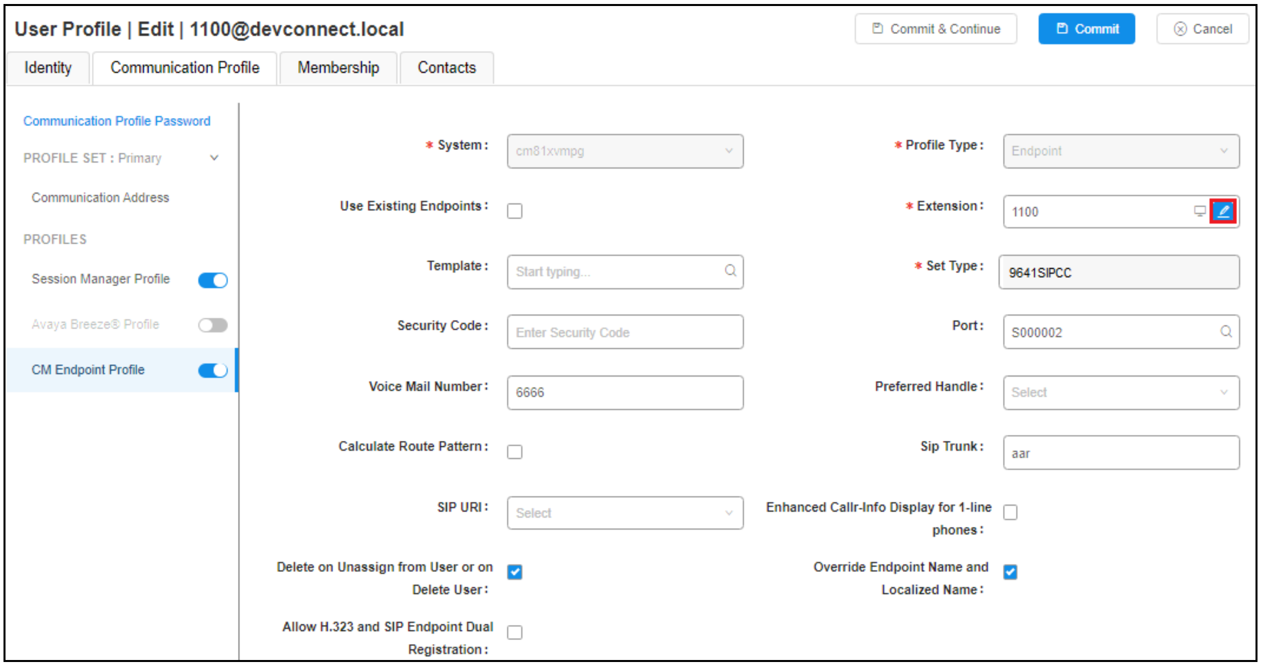


Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



	First Name	Surname	Display Name
☐	H323 Ext	1000	1000, H323 Ext
☑	SIP Ext	1100	1100, SIP Ext
☐	J129 SIP	1101	1101, J129 SIP
☐	Equinox Vantage	1102	1102, Equinox Vantage
☐	Agent	Agent	Agent One
☐	Agent	Agent	Agent Two
☐	admin	admin	Default Administrator
☐	SIP	Ext 1150	Ext 1150, SIP
☐	SIP	Ext 1151	Ext 1151, SIP
☐	SIP	Ext 1152	Ext 1152, SIP

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



User Profile | Edit | 1100@devconnect.local

* System : cm81xvmpg

* Profile Type : Endpoint

Use Existing Endpoints : ☐

* Extension : 1100

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000002

Voice Mail Number : 6666

Preferred Handle : Select

Calculate Route Pattern : ☐

Sip Trunk : aar

SIP URI : Select

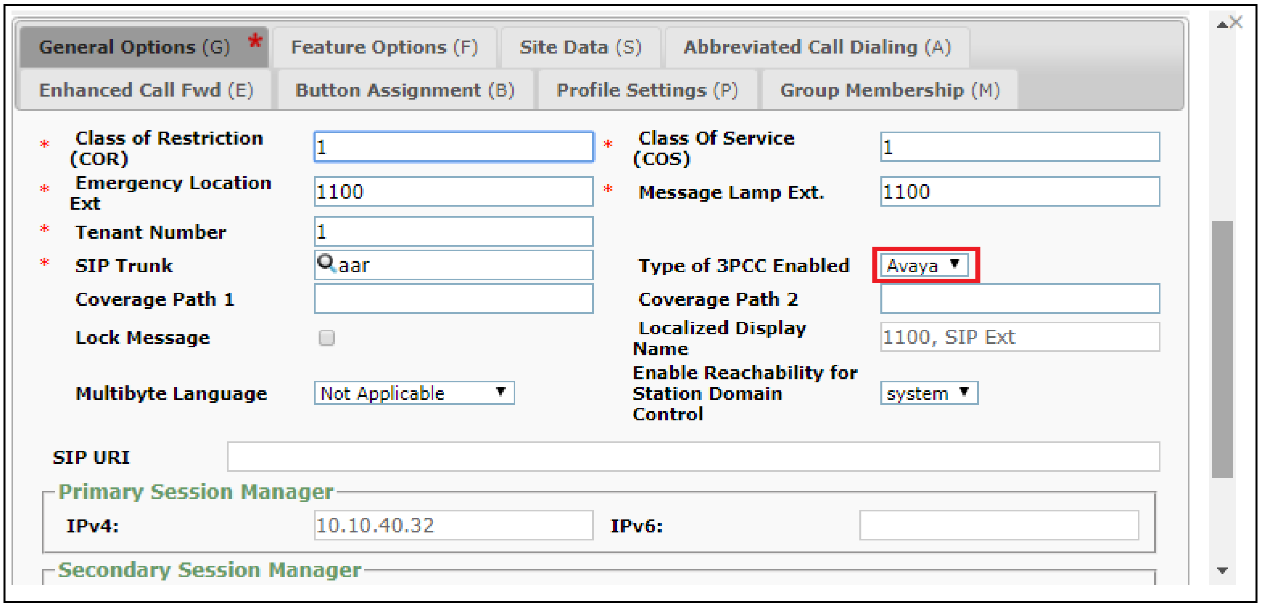
Enhanced Callr-Info Display for 1-line phones : ☐

Delete on Unassign from User or on Delete User : ☑

Override Endpoint Name and Localized Name : ☑

Allow H.323 and SIP Endpoint Dual Registration : ☐

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



* Class of Restriction (COR): 1

* Class Of Service (COS): 1

* Emergency Location Ext: 1100

* Message Lamp Ext.: 1100

* Tenant Number: 1

* SIP Trunk: aar

Type of 3PCC Enabled: Avaya

Coverage Path 1:

Coverage Path 2:

Lock Message: ☐

Localized Display Name: 1100, SIP Ext

Multibyte Language: Not Applicable

Enable Reachability for Station Domain Control: system

SIP URI:

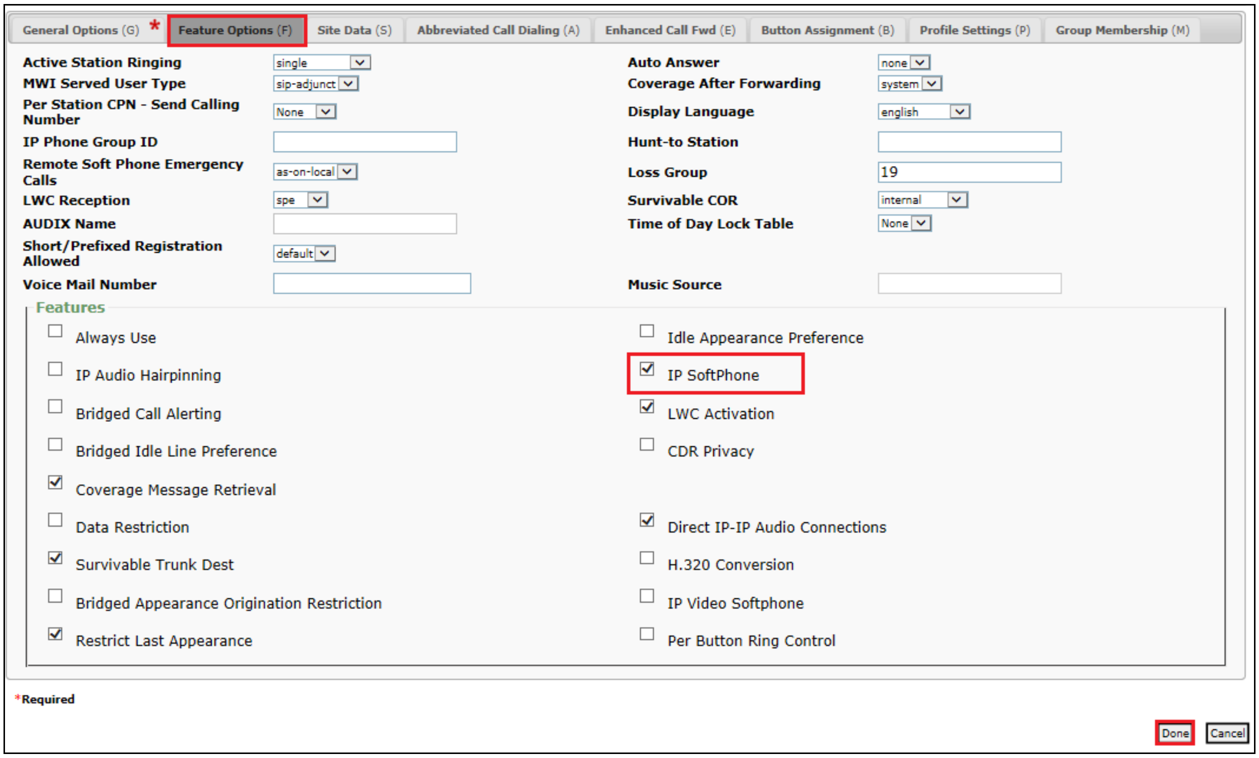
Primary Session Manager

IPv4: 10.10.40.32

IPv6:

Secondary Session Manager

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



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

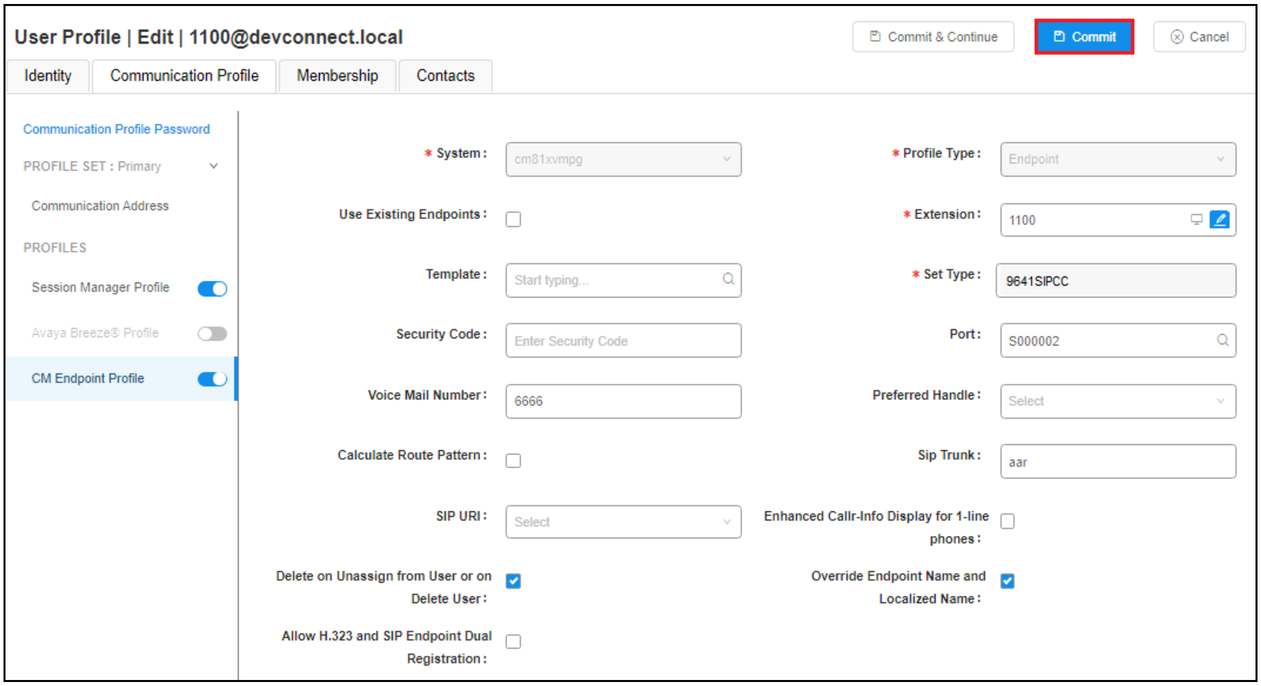
Active Station Ringing	single	Auto Answer	none
MWI Served User Type	sip-adjunct	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
IP Phone Group ID		Hunt-to Station	
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
AUDIX Name		Time of Day Lock Table	None
Short/Prefixed Registration Allowed	default		
Voice Mail Number		Music Source	

Features

□ Always Use	□ Idle Appearance Preference
□ IP Audio Hairpinning	☑ IP SoftPhone
□ Bridged Call Alerting	☑ LWC Activation
□ Bridged Idle Line Preference	□ CDR Privacy
☑ Coverage Message Retrieval	
□ Data Restriction	☑ Direct IP-IP Audio Connections
☑ Survivable Trunk Dest	□ H.320 Conversion
□ Bridged Appearance Origination Restriction	□ IP Video Softphone
☑ Restrict Last Appearance	□ Per Button Ring Control

*Required

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



User Profile | Edit | 1100@devconnect.local

Session Manager Profile ●
Avaya Breeze® Profile ○
CM Endpoint Profile ●

* System :	cm81xvmpg	* Profile Type :	Endpoint
Use Existing Endpoints :	□	* Extension :	1100
Template :	Start typing...	* Set Type :	9641SIPCC
Security Code :	Enter Security Code	Port :	S000002
Voice Mail Number :	6666	Preferred Handle :	Select
Calculate Route Pattern :	□	Sip Trunk :	aar
SIP URI :	Select	Enhanced Callr-Info Display for 1-line phones :	□
Delete on Unassign from User or on Delete User :	☑	Override Endpoint Name and Localized Name :	☑
Allow H.323 and SIP Endpoint Dual Registration :	□		

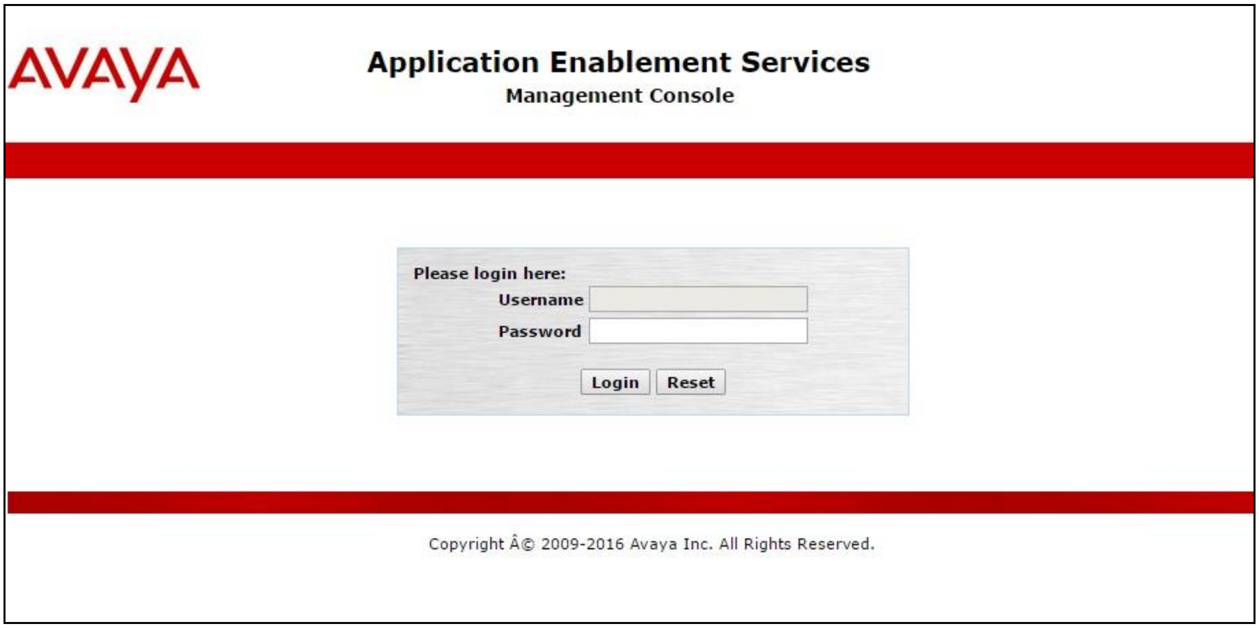
6. Configure Avaya Aura® Application Enablement Services

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

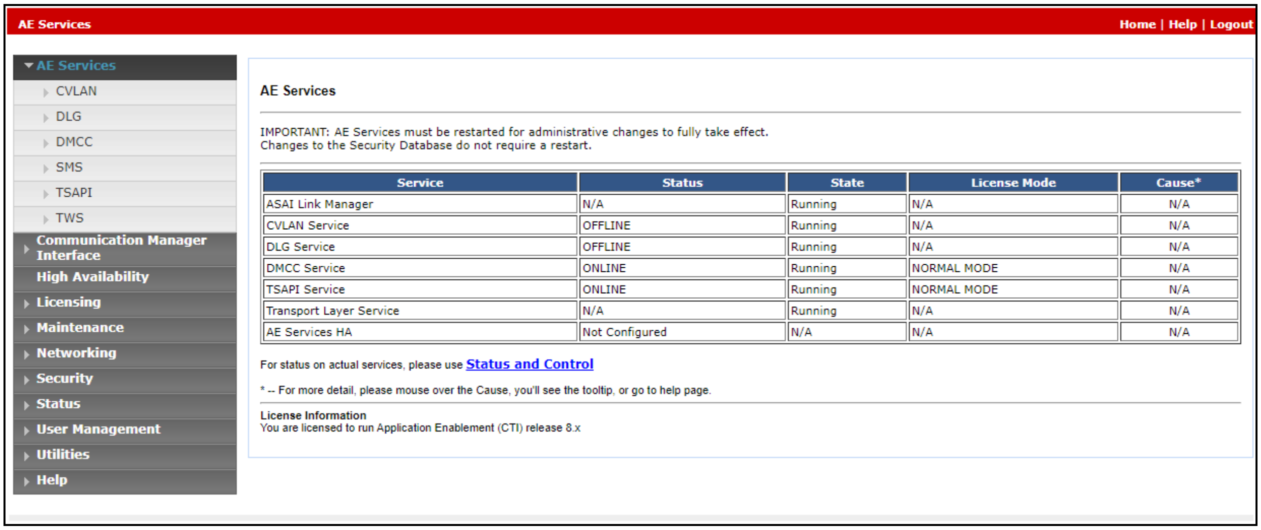
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Configure Networking Ports
- Create CTI User
- Configure Security Database

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.


AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Password
Login
Reset
Copyright Â© 2009-2016 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 and DMCC Services are licensed by ensuring that **TSAPI Service** and **DMCC Service** are in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the appropriate license.



AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

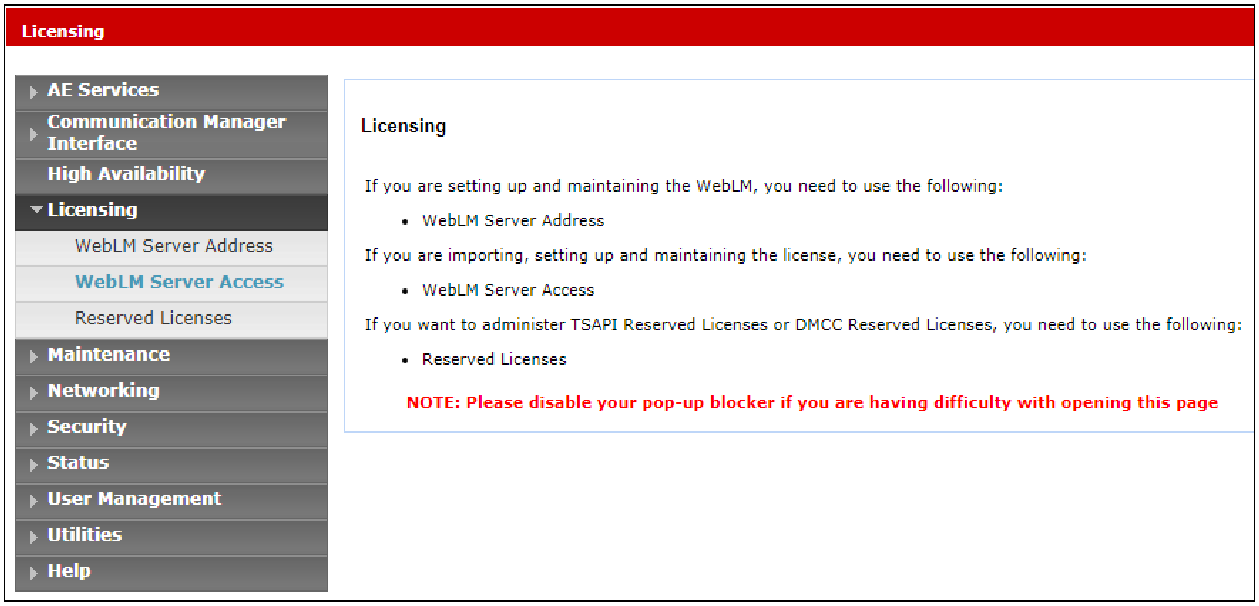
Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

For status on actual services, please use Status and Control

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

License Information
You are licensed to run Application Enablement (CTI) release 8.x

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.



Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

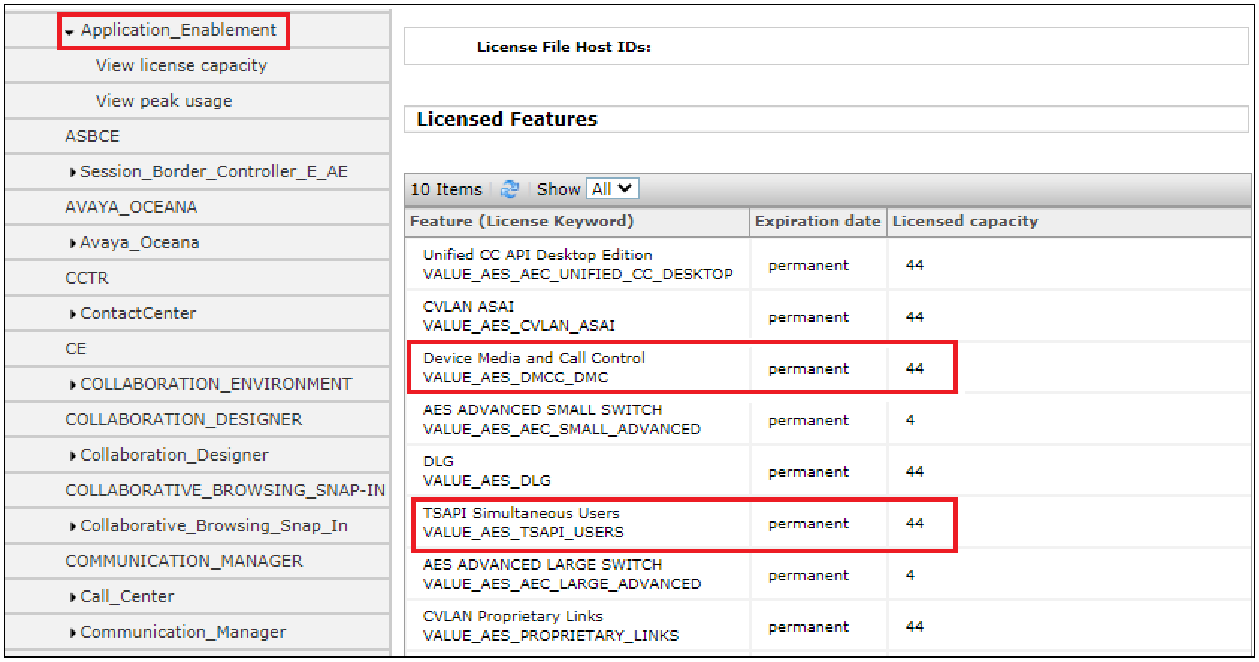
- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

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

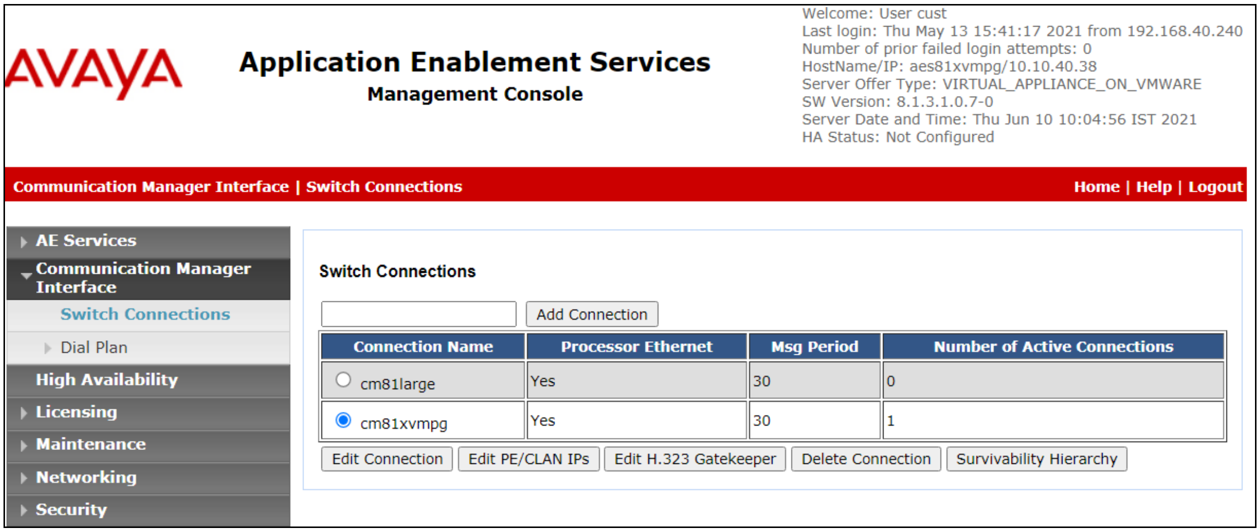


Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

6.2. Switch Connection to Avaya Aura® Communication Manager

Typically, the connection between the AES and Communication Manager is setup as part of the initial installation and would not usually be outlined in these Application Notes. Due to the nature of this particular setup with two connections from Communication Manager to two separate AES's the switch connection will be displayed on this section. From the AES Management Console navigate to **Communication Manager Interface → Switch Connections**, the connection to Communication Manager should be present as shown below but if one is not present one can be added by clicking on **Add Connection**.

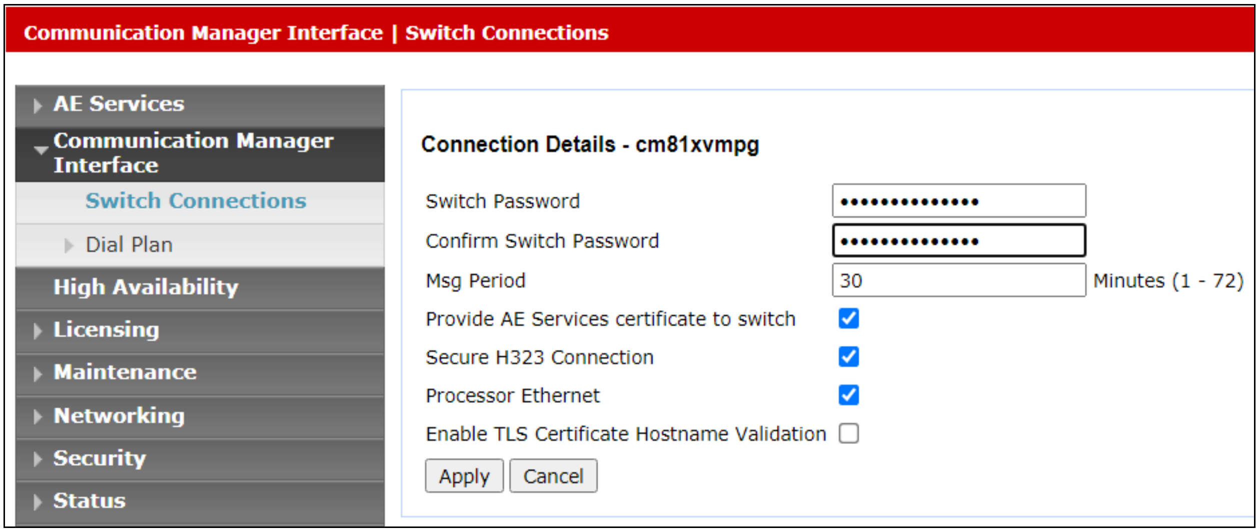


Welcome: User cust
Last login: Thu May 13 15:41:17 2021 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aes81xvmpg/10.10.40.38
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 10 10:04:56 IST 2021
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ cm81large	Yes	30	0
● cm81xvmpg	Yes	30	1

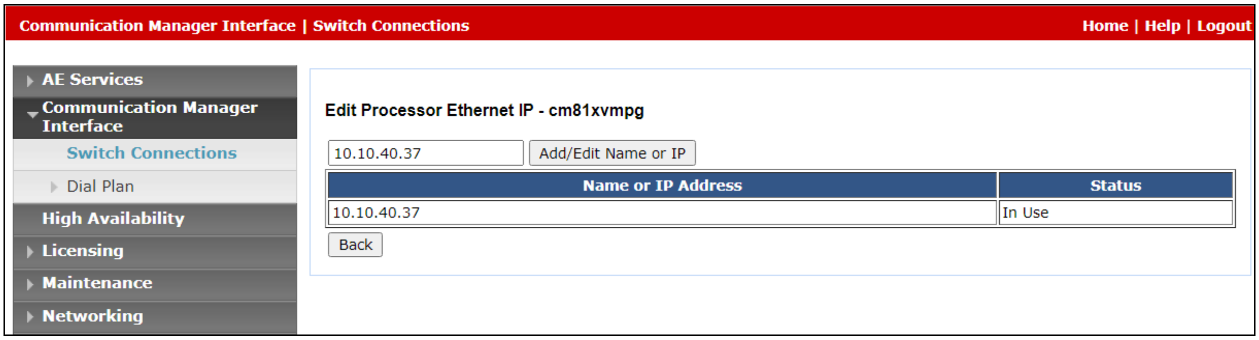
In the resulting screen, enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. A secure connection was established between the AES and Communication Manager, so the appropriate boxes were ticked, as shown below. Click **Apply** to save changes.



Connection Details - cm81xvmpg

Switch Password	••••••••••••••
Confirm Switch Password	••••••••••••••
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	☑
Secure H323 Connection	☑
Processor Ethernet	☑
Enable TLS Certificate Hostname Validation	□

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



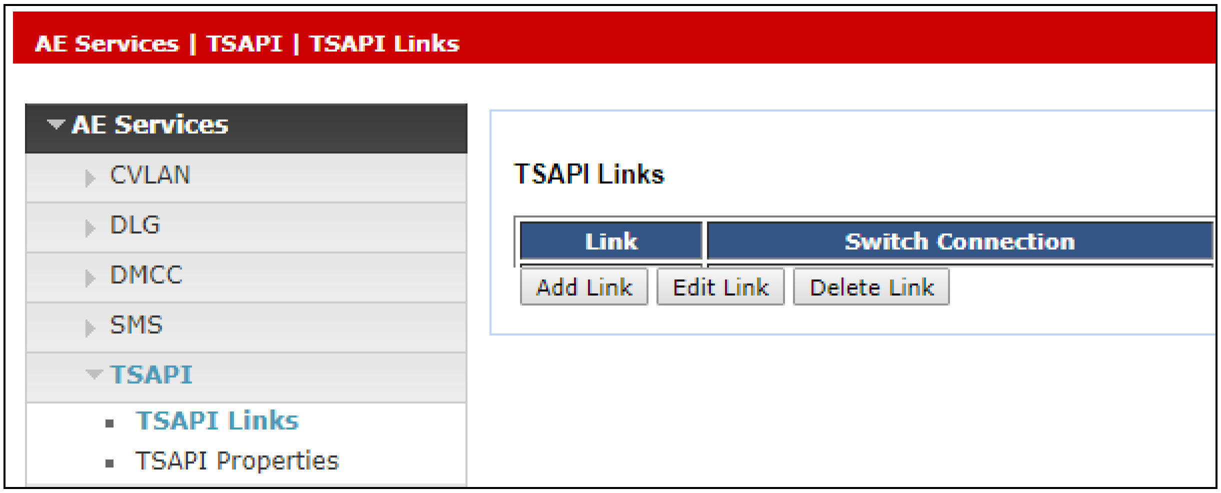
Edit Processor Ethernet IP - cm81xvmpg

10.10.40.37

Name or IP Address	Status
10.10.40.37	In Use

6.3. Administer TSAPI link

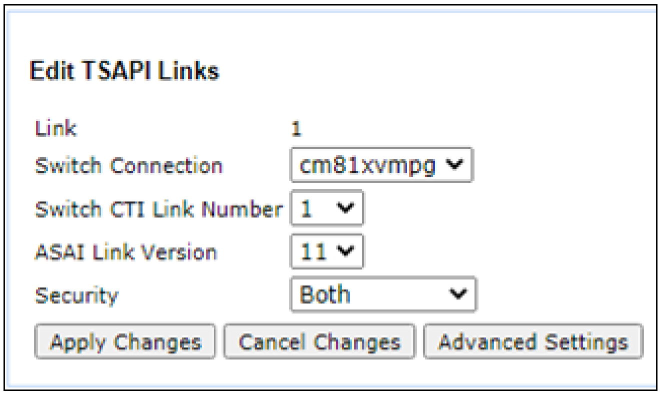
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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 **cm81xvmpg**, 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: 11** was used for compliance testing but the latest version available can be chosen).
- **Security:** This can be left at the default value of **both**.

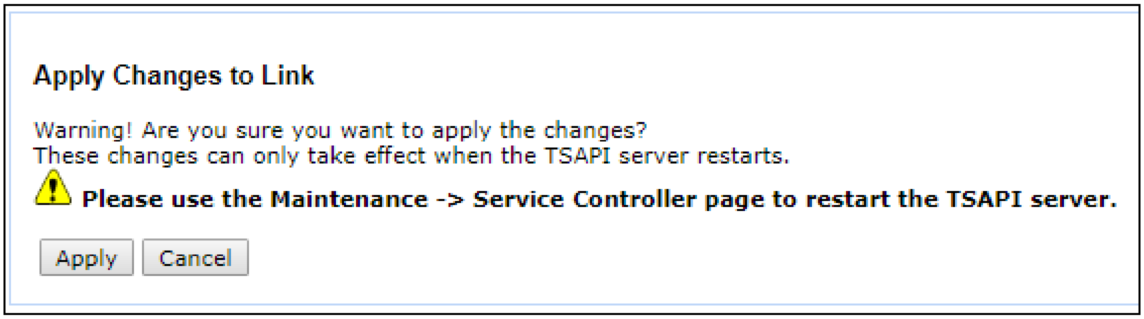
Once completed, select **Apply Changes**.



Edit TSAPI Links

Link	1
Switch Connection	cm81xvmpg
Switch CTI Link Number	1
ASAI Link Version	11
Security	Both

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

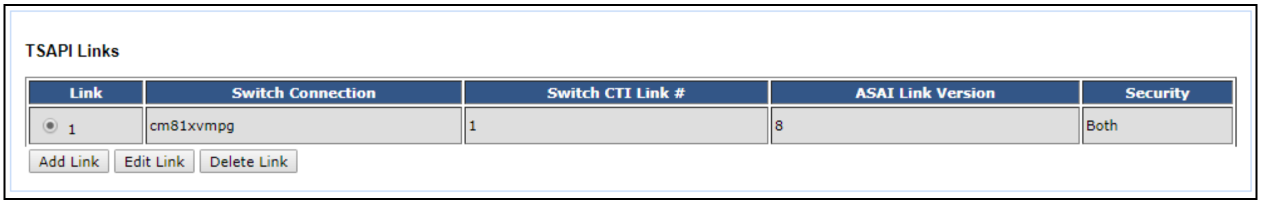


Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.

⚠ **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

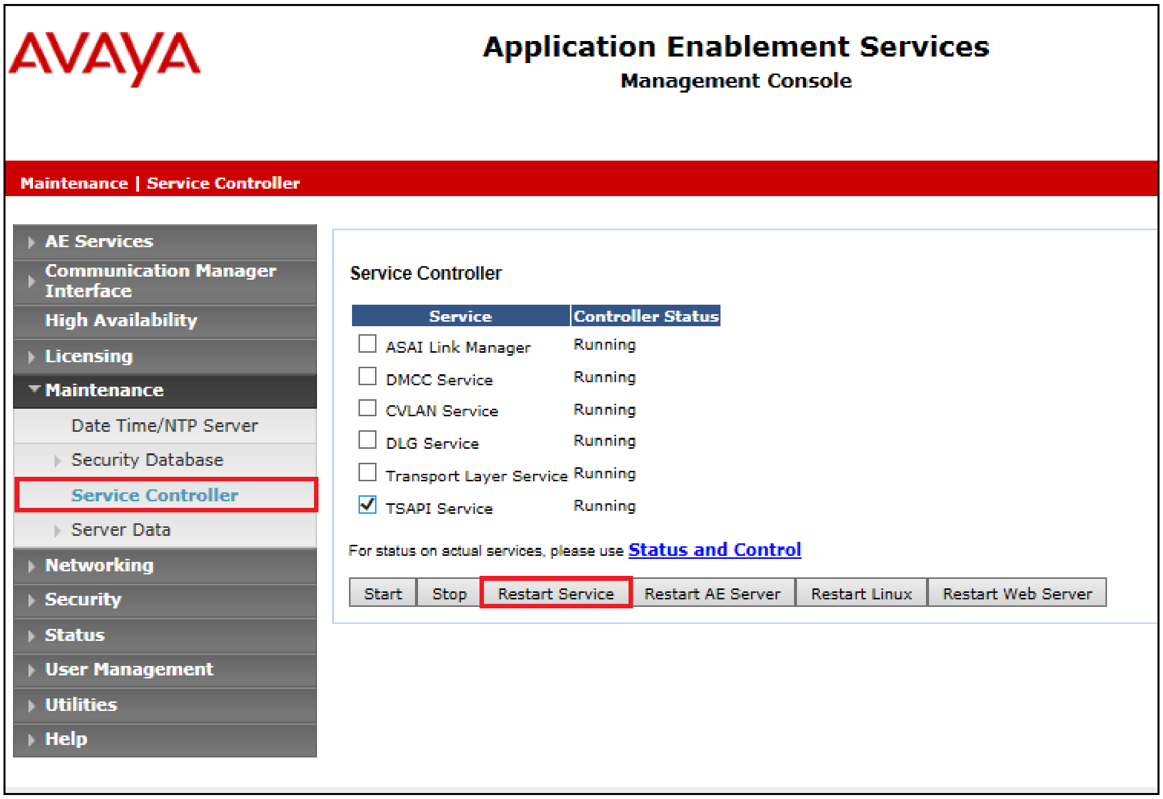
When the TSAPI Link is completed, it should resemble the screen below.



TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	cm81xvmpg	1	8	Both

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**.



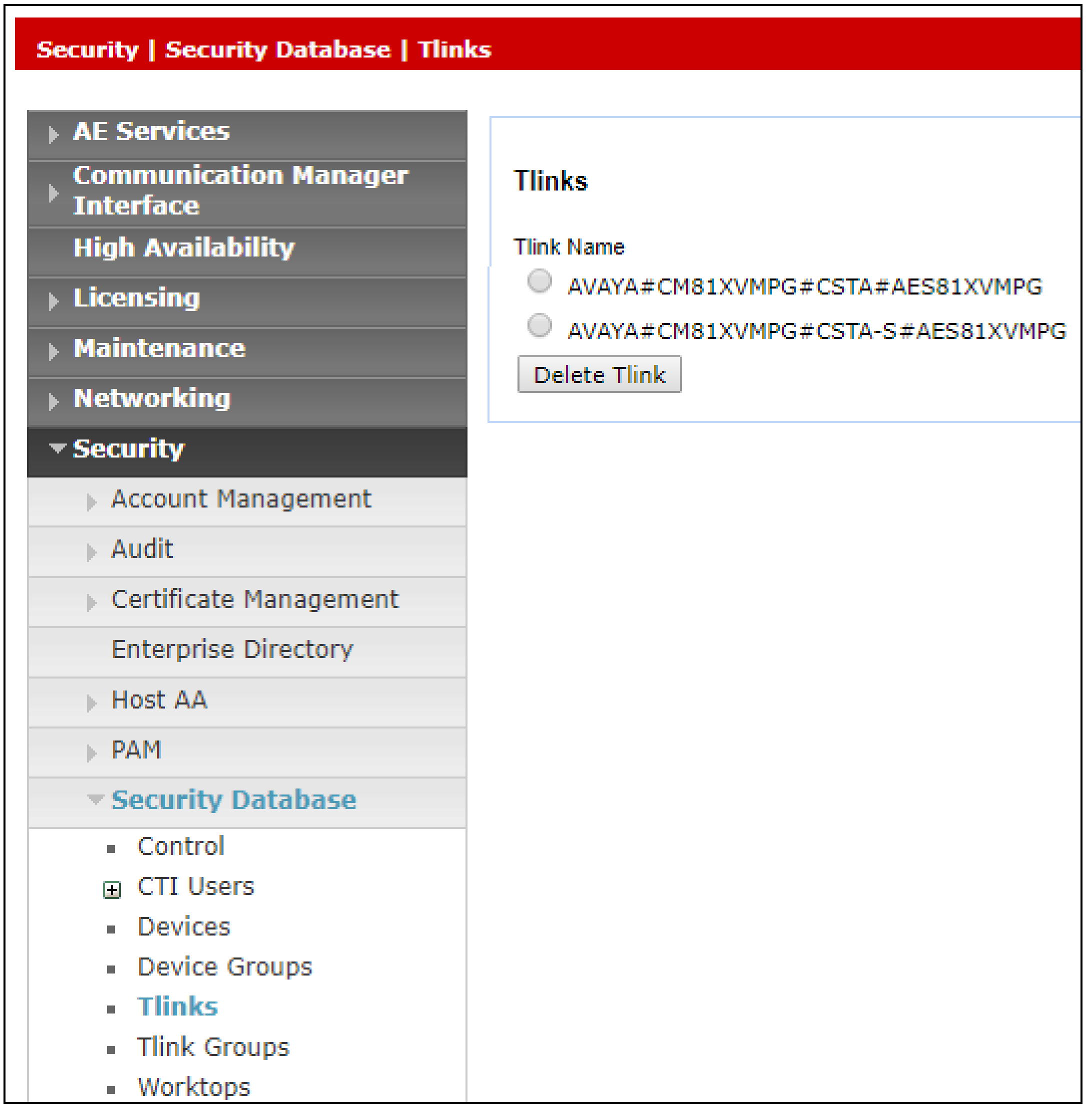
Service Controller

Service	Controller Status
☐ ASAI Link Manager	Running
☐ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.4. Identify Tlinks

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



Tlinks

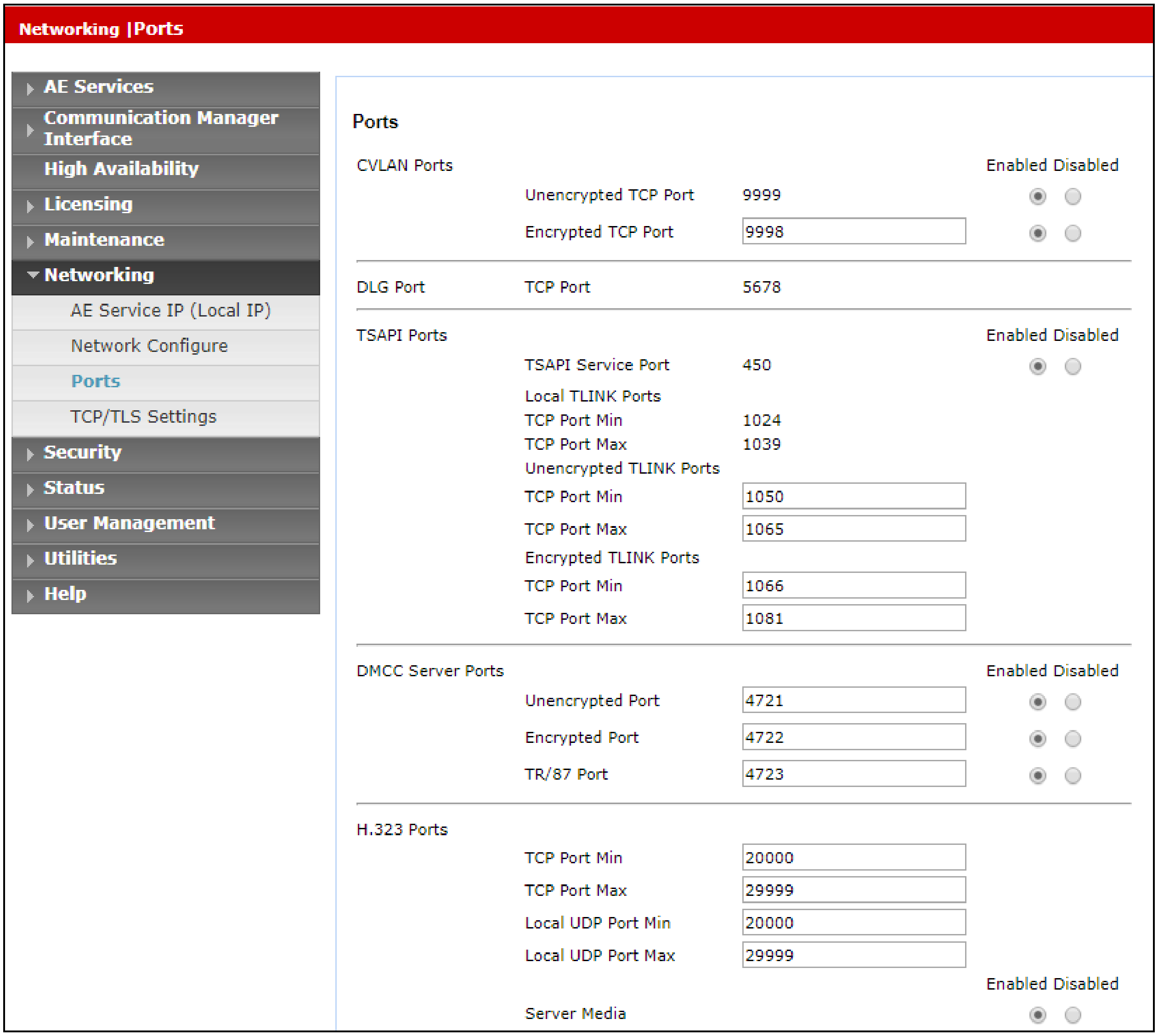
Tlink Name

○ AVAYA#CM81XVMPG#CSTA#AES81XVMPG

○ AVAYA#CM81XVMPG#CSTA-S#AES81XVMPG

6.5. Enable TSAPI and DMCC Ports

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



Ports

CVLAN Ports — Enabled Disabled
Unencrypted TCP Port 9999 ● ○
Encrypted TCP Port 9998 ● ○

DLG Port — TCP Port 5678

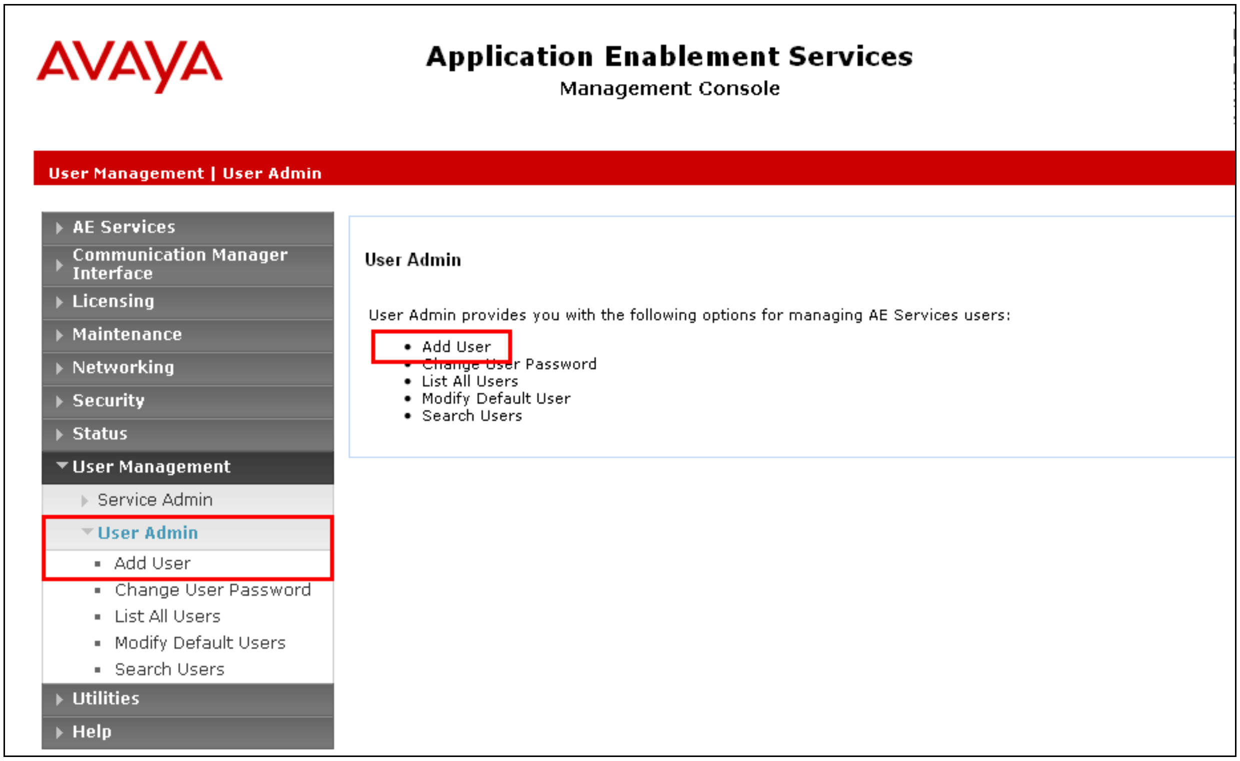
TSAPI Ports — Enabled Disabled
TSAPI Service Port 450 ● ○
Local TLINK Ports
TCP Port Min 1024
TCP Port Max 1039
Unencrypted TLINK Ports
TCP Port Min 1050
TCP Port Max 1065
Encrypted TLINK Ports
TCP Port Min 1066
TCP Port Max 1081

DMCC Server Ports — Enabled Disabled
Unencrypted Port 4721 ● ○
Encrypted Port 4722 ● ○
TR/87 Port 4723 ● ○

H.323 Ports
TCP Port Min 20000
TCP Port Max 29999
Local UDP Port Min 20000
Local UDP Port Max 29999
Enabled Disabled
Server Media ● ○

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.



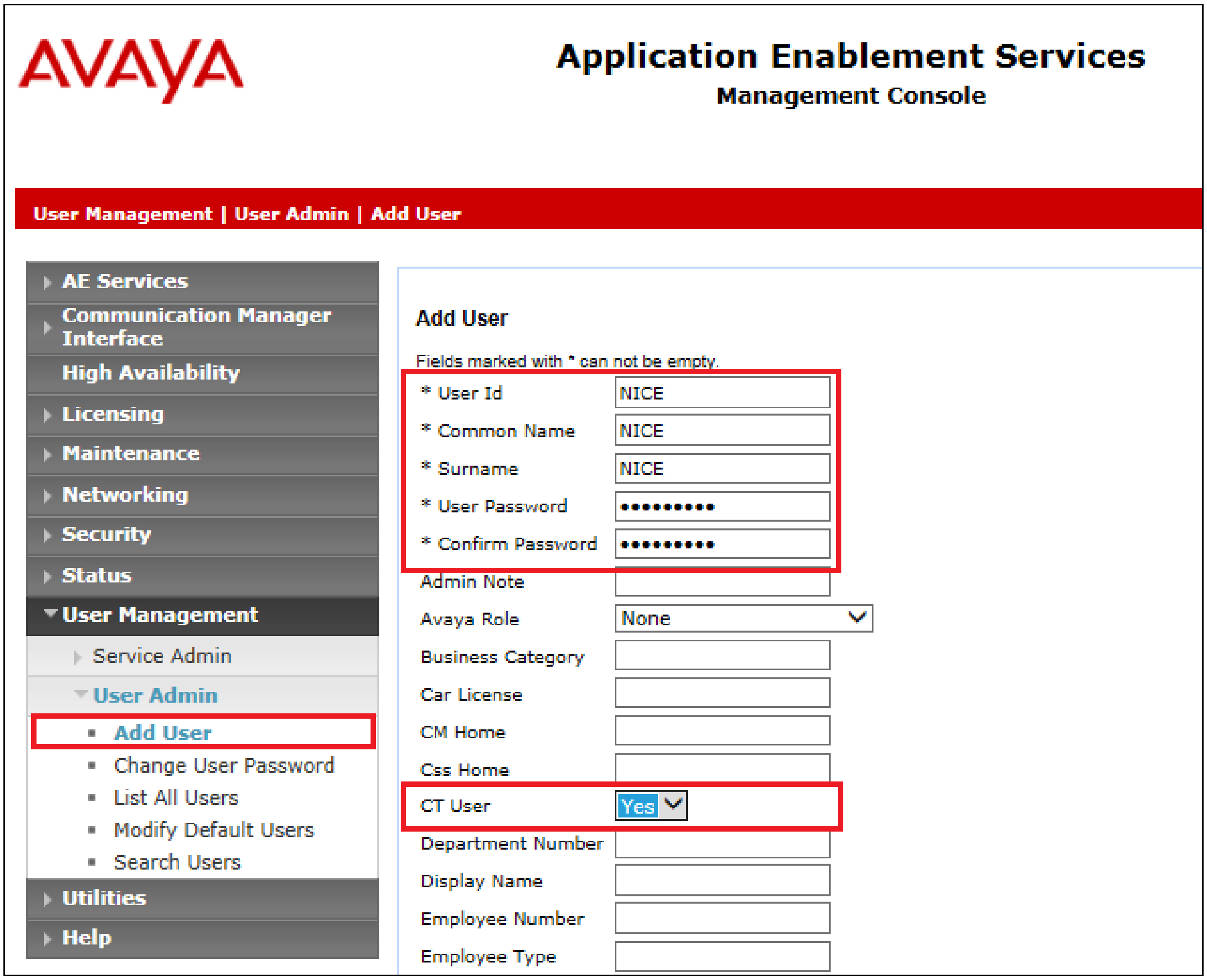
User Admin

User Admin provides you with the following options for managing AE Services users:

- Add User
- Change User Password
- List All Users
- Modify Default User
- Search Users

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.



Add User

Fields marked with * can not be empty.

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

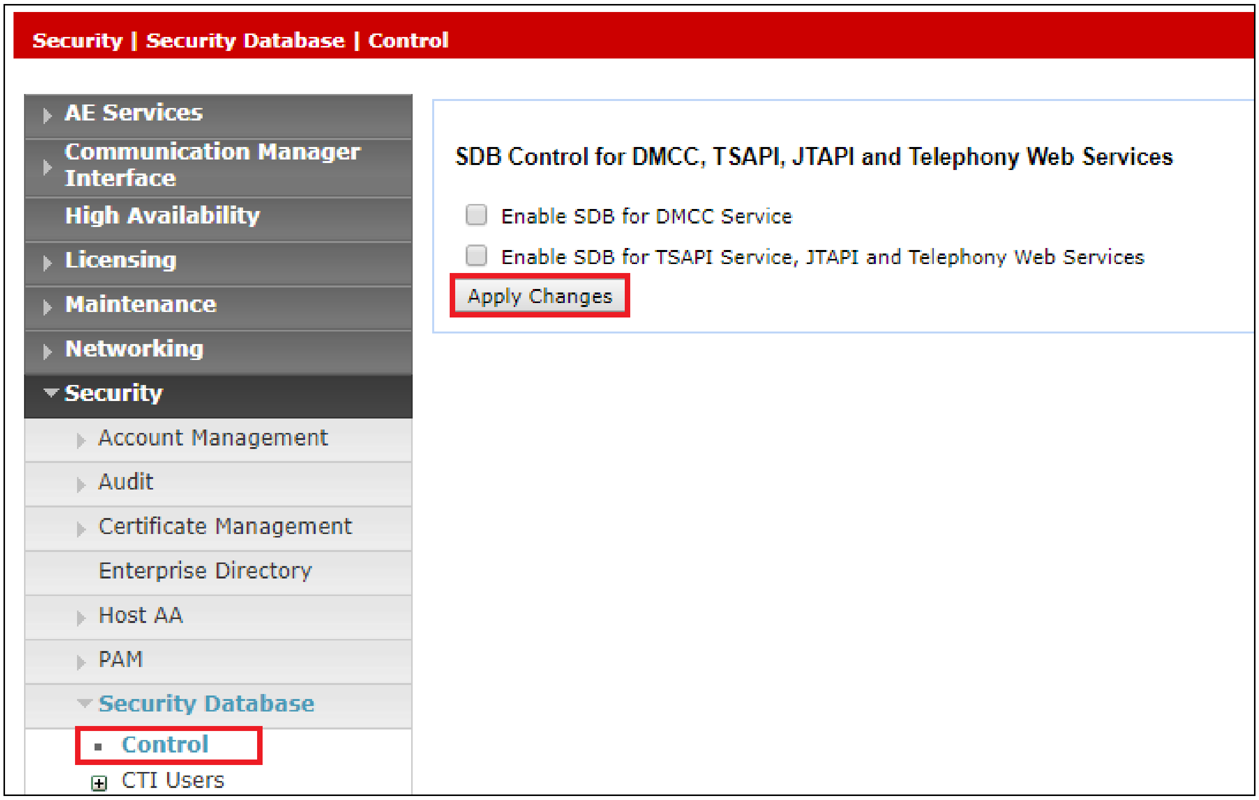
Scroll down and click on **Apply Changes** (not shown).

6.7. Configure Security Database

For compliance testing associated with these Application Notes the Security Database was not enabled and the user associated with NICE was given unrestricted access.

6.7.1. Disable the Security Database Control

Navigate to **Security** → **Security Database** → **Control** as shown below. Ensure that no boxes are ticked and click on **Apply Changes** if necessary.



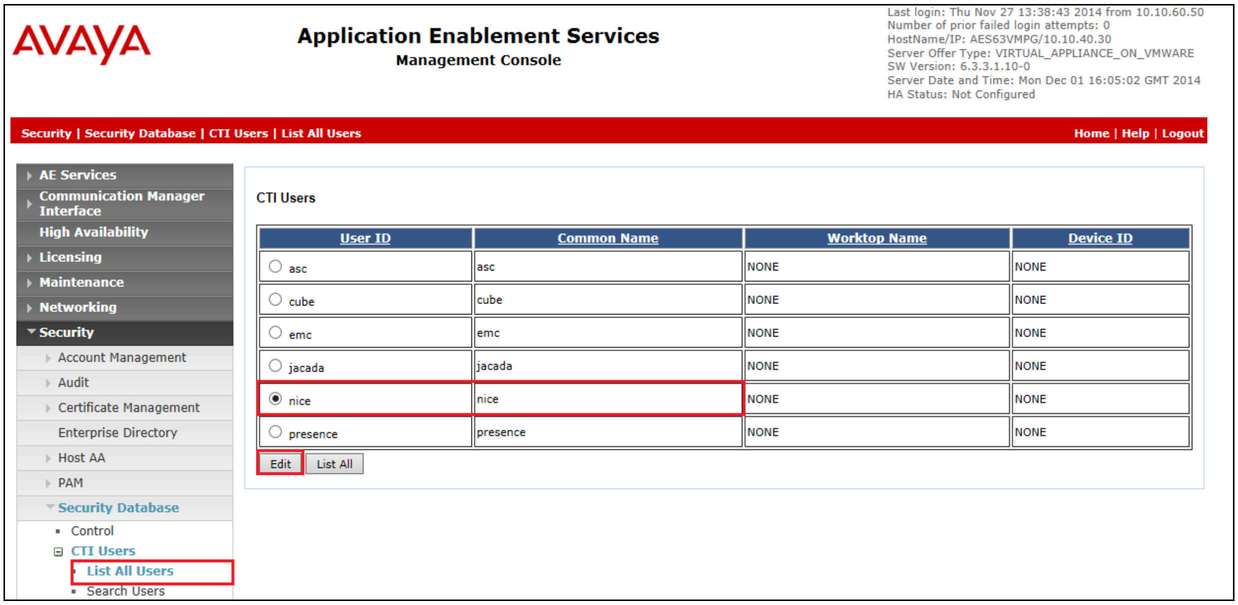
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

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**.

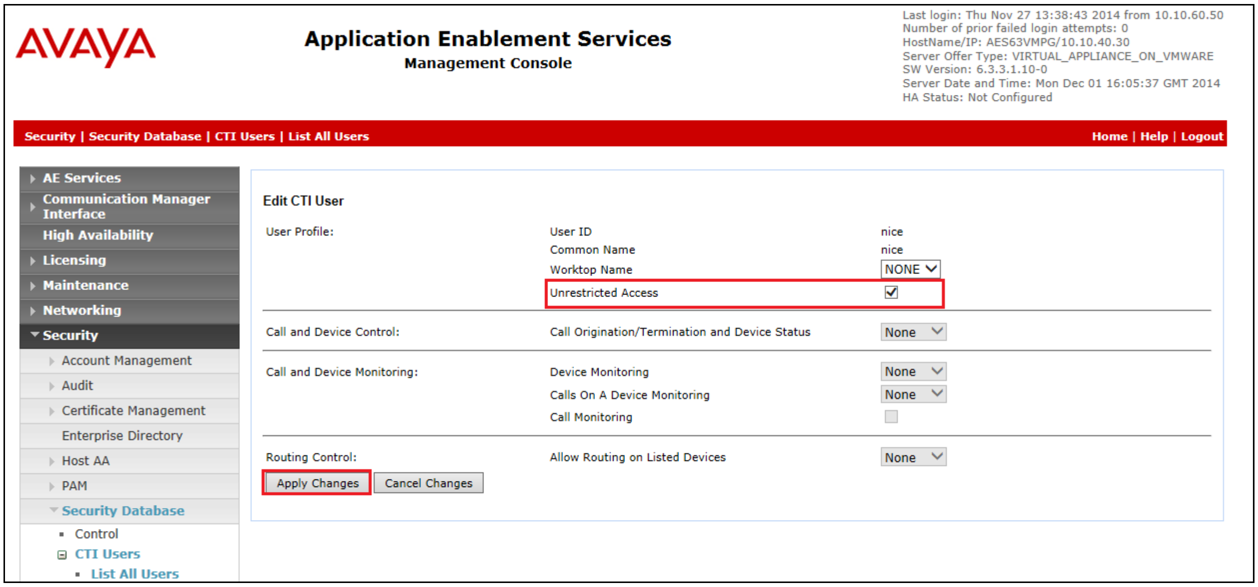


Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Dec 01 16:05:02 GMT 2014
HA Status: Not Configured

CTI Users

User ID	Common Name	Worktop Name	Device ID
○ asc	asc	NONE	NONE
○ cube	cube	NONE	NONE
○ emc	emc	NONE	NONE
○ jacada	jacada	NONE	NONE
● nice	nice	NONE	NONE
○ presence	presence	NONE	NONE

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



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

Edit CTI User

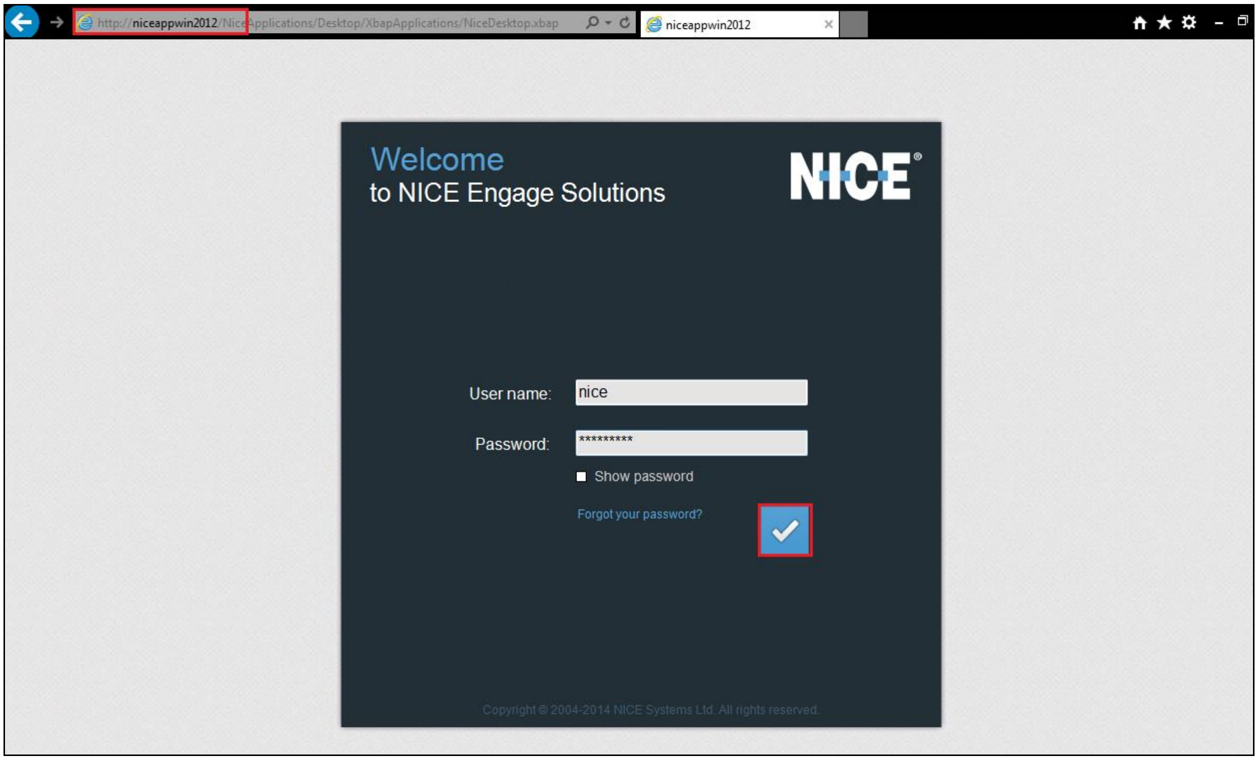
User Profile:	User ID	nice
	Common Name	nice
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

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**.



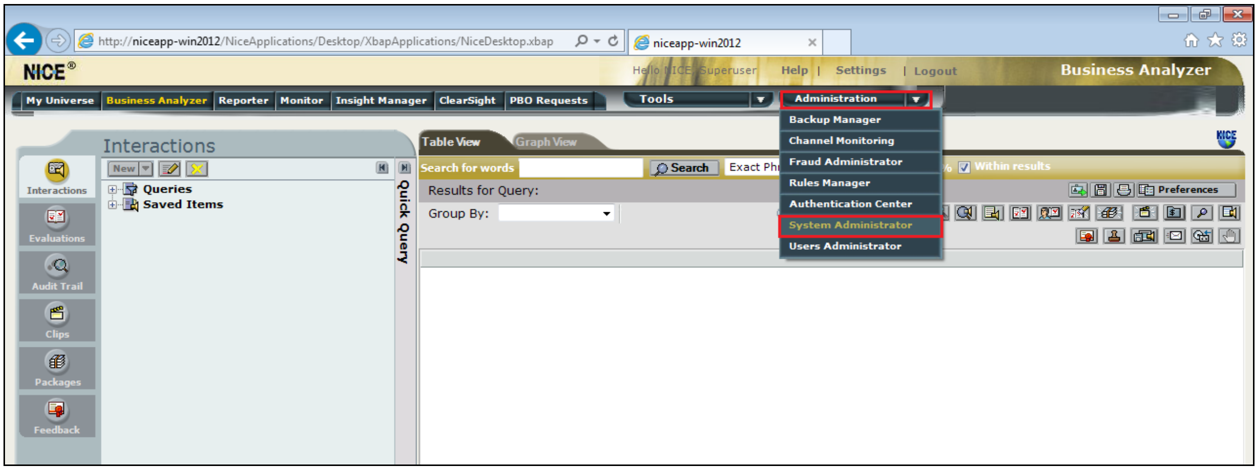
http://niceappwin2012/NiceApplications/Desktop/XbapApplications/NiceDesktop.xbap

User name: nice

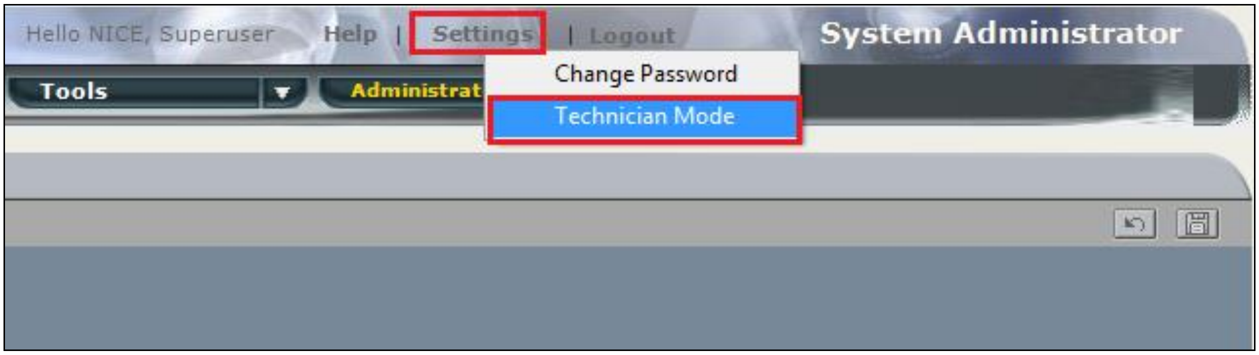
Password: *********

□ Show password

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

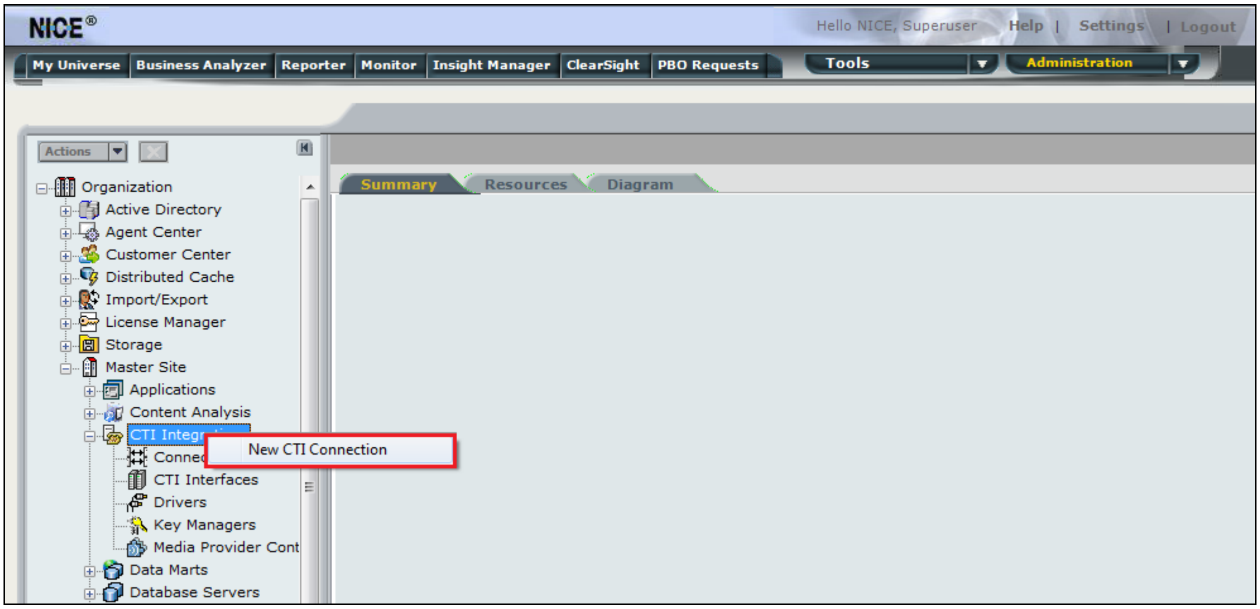


Before any changes can be made, switch to **Technician Mode** by clicking into **Settings** at the top of the screen as shown below.

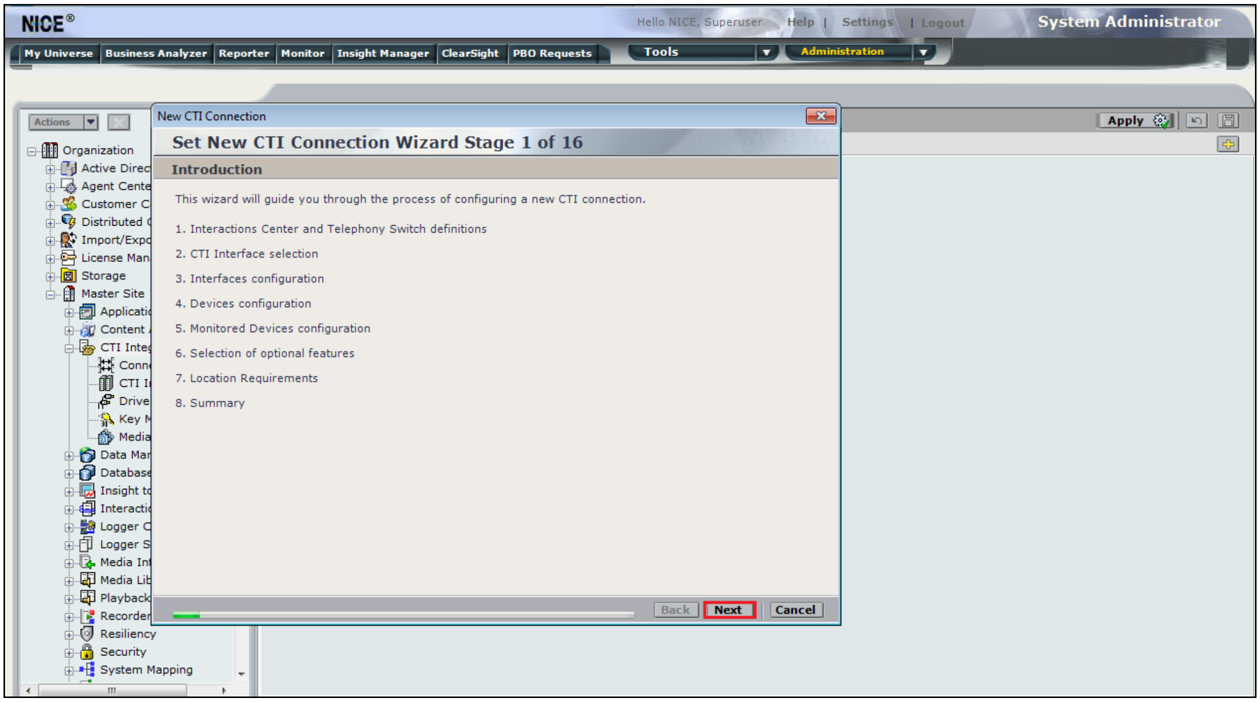


7.1. New CTI Connection

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



Set New CTI Connection Wizard Stage 1 of 16

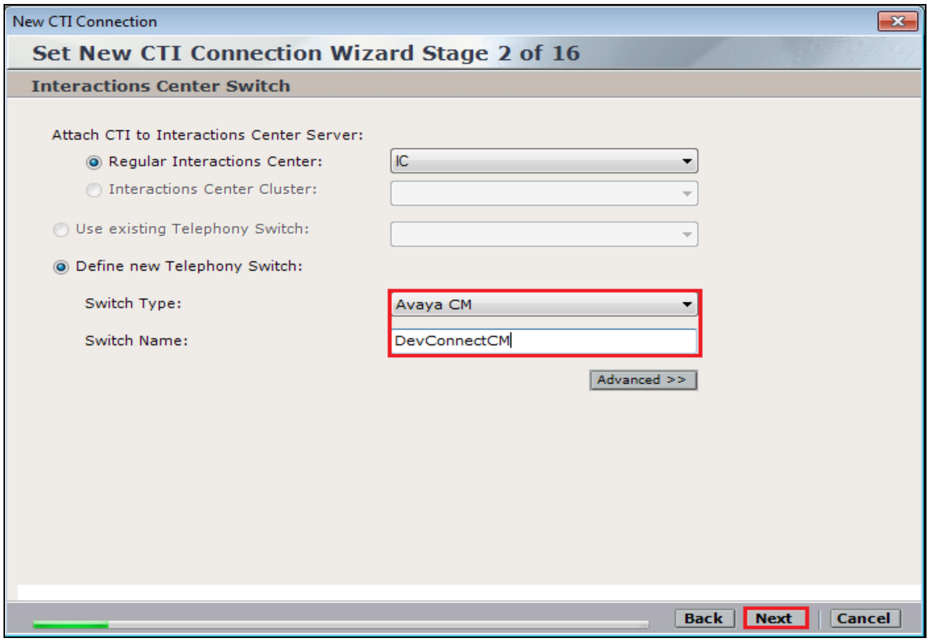
Introduction

This wizard will guide you through the process of configuring a new CTI connection.

1. Interactions Center and Telephony Switch definitions
2. CTI Interface selection
3. Interfaces configuration
4. Devices configuration
5. Monitored Devices configuration
6. Selection of optional features
7. Location Requirements
8. Summary

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.


New CTI Connection

Set New CTI Connection Wizard Stage 2 of 16

Interactions Center Switch

Attach CTI to Interactions Center Server:

● Regular Interactions Center: IC

○ Interactions Center Cluster:

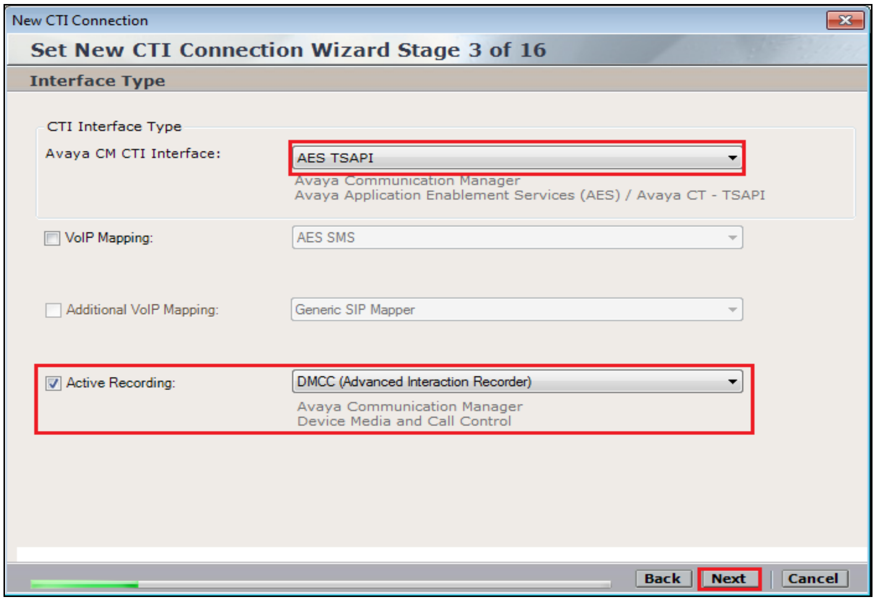
○ Use existing Telephony Switch:

● Define new Telephony Switch:

Switch Type: Avaya CM

Switch Name: DevConnectCM

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


New CTI Connection

Set New CTI Connection Wizard Stage 3 of 16

Interface Type

CTI Interface Type

Avaya CM CTI Interface: AES TSAPI

Avaya Communication Manager
Avaya Application Enablement Services (AES) / Avaya CT - TSAPI

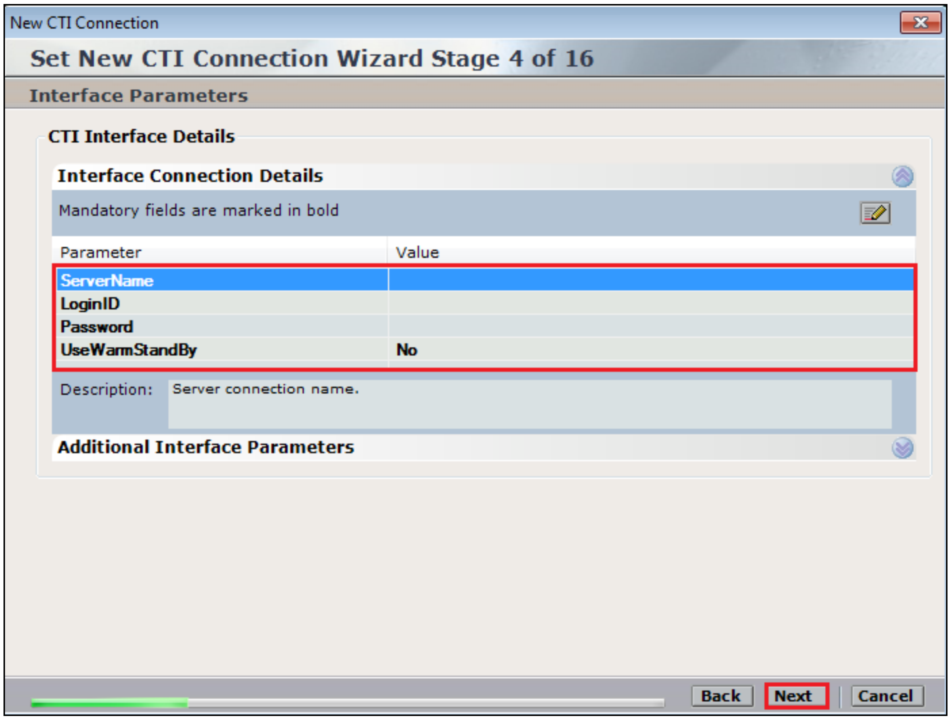
□ VoIP Mapping: AES SMS

□ Additional VoIP Mapping: Generic SIP Mapper

☑ Active Recording: DMCC (Advanced Interaction Recorder)

Avaya Communication Manager
Device Media and Call Control

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



New CTI Connection

Set New CTI Connection Wizard Stage 4 of 16

Interface Parameters

CTI Interface Details

Interface Connection Details

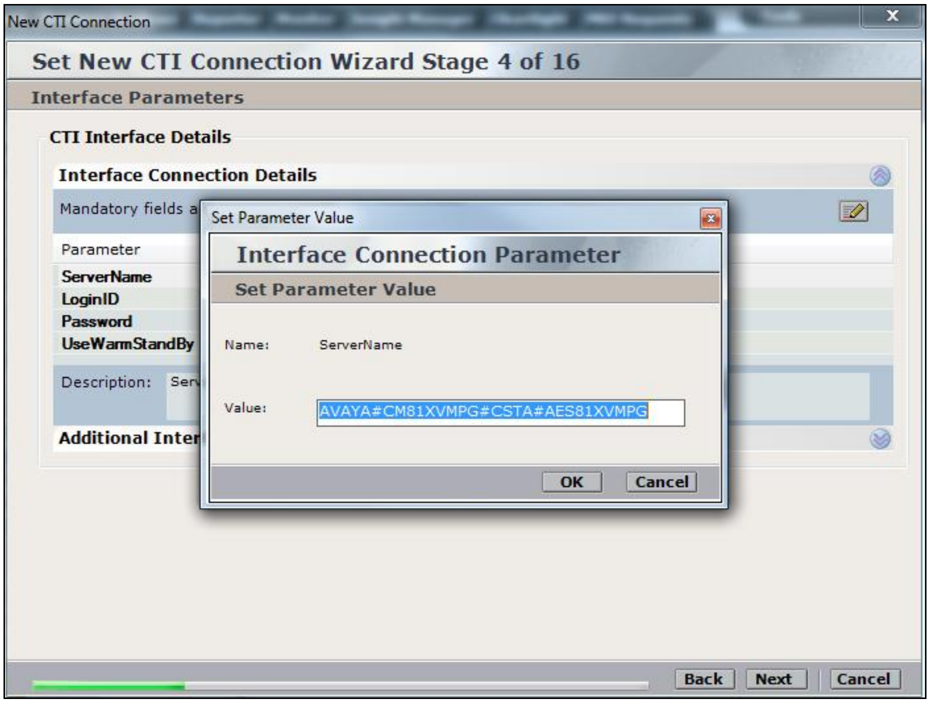
Mandatory fields are marked in bold

Parameter	Value
ServerName	
LoginID	
Password	
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

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



Set Parameter Value

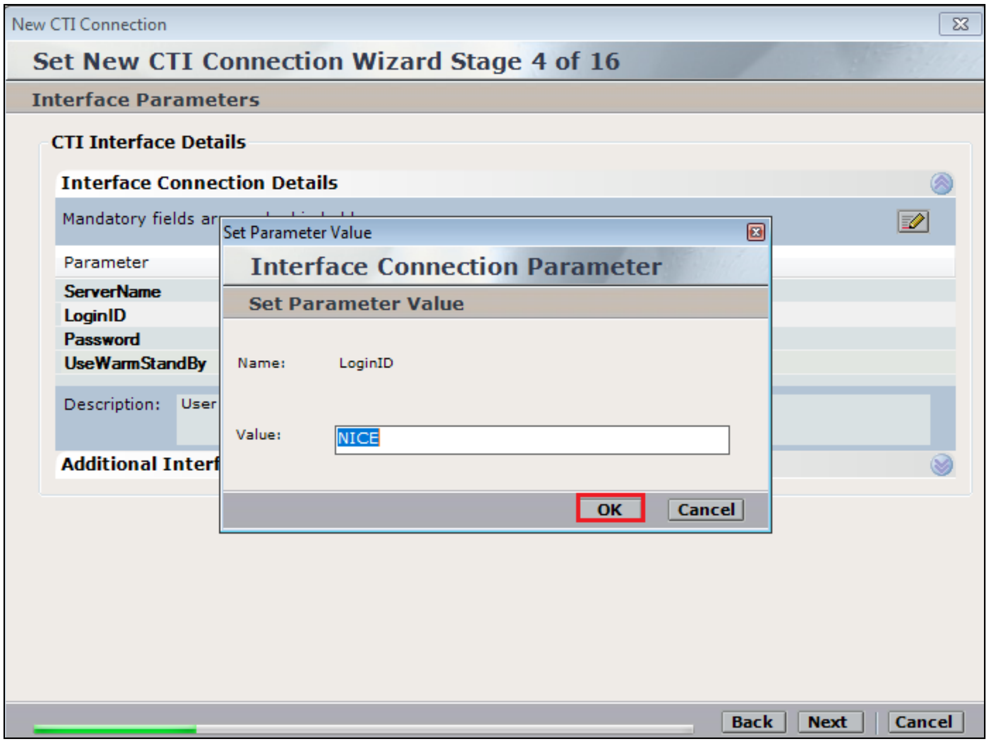
Interface Connection Parameter

Set Parameter Value

Name: ServerName

Value: AVAYA#CM81XVMPG#CSTA#AES81XVMPG

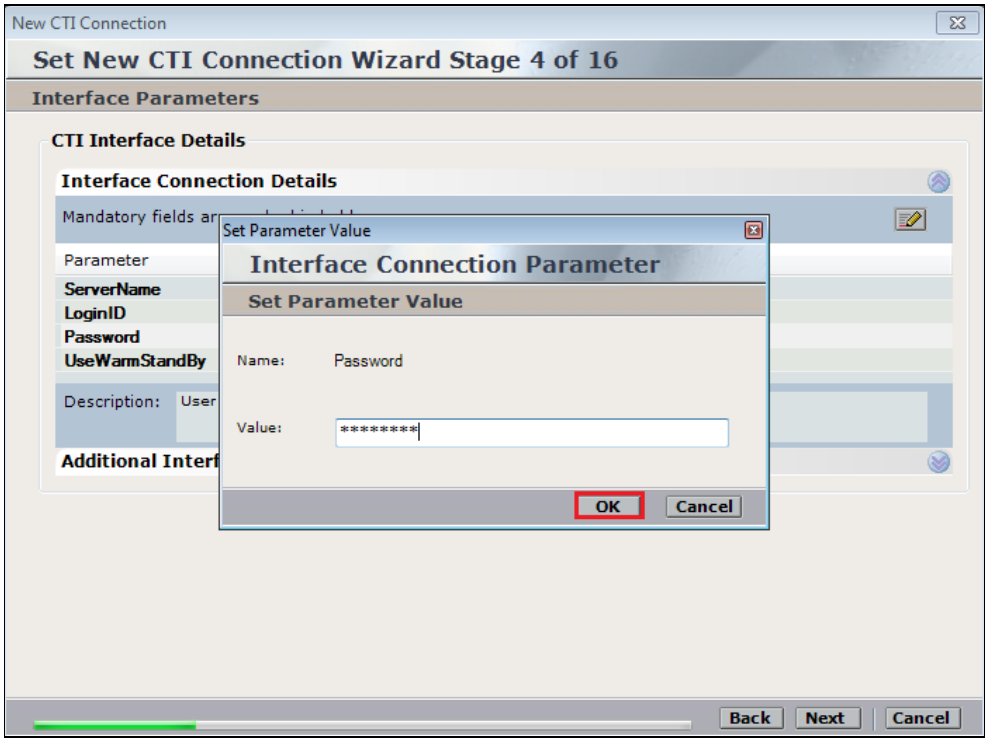
Double-click on **LoginID** and enter the username that was created in **Section 6.6**. Click on **OK**.



Name: LoginID

Value: NICE

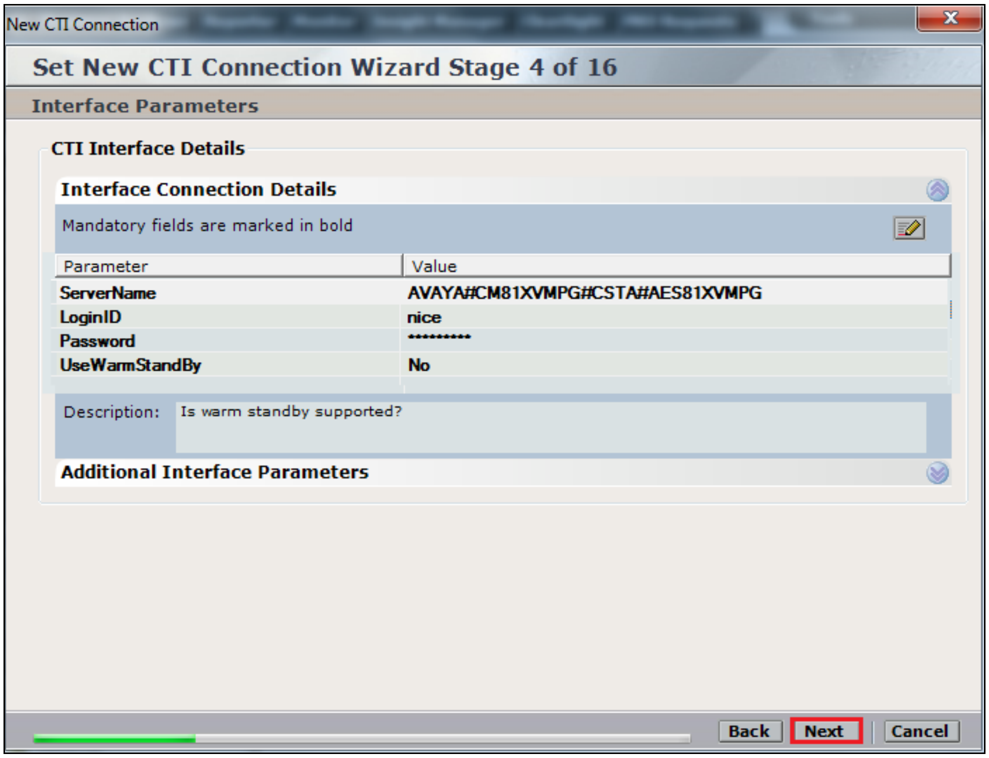
Double-click on password and enter the value for the password that was created in **Section 6.6**.



Name: Password

Value: *********

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



New CTI Connection

Set New CTI Connection Wizard Stage 4 of 16

Interface Parameters

CTI Interface Details

Interface Connection Details

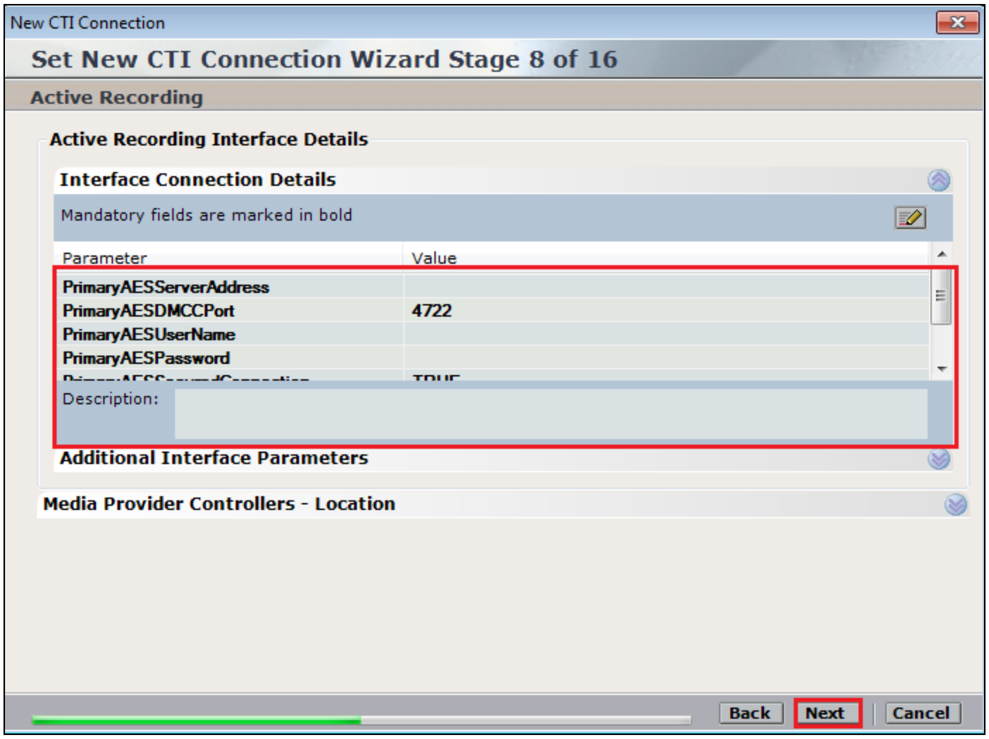
Mandatory fields are marked in bold

Parameter	Value
ServerName	**AVAYA#CM81XVMPG#CSTA#AES81XVMPG**
LoginID	**nice**
Password	*********
UseWarmStandBy	**No**

Description: Is warm standby supported?

Additional Interface Parameters

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



New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Mandatory fields are marked in bold

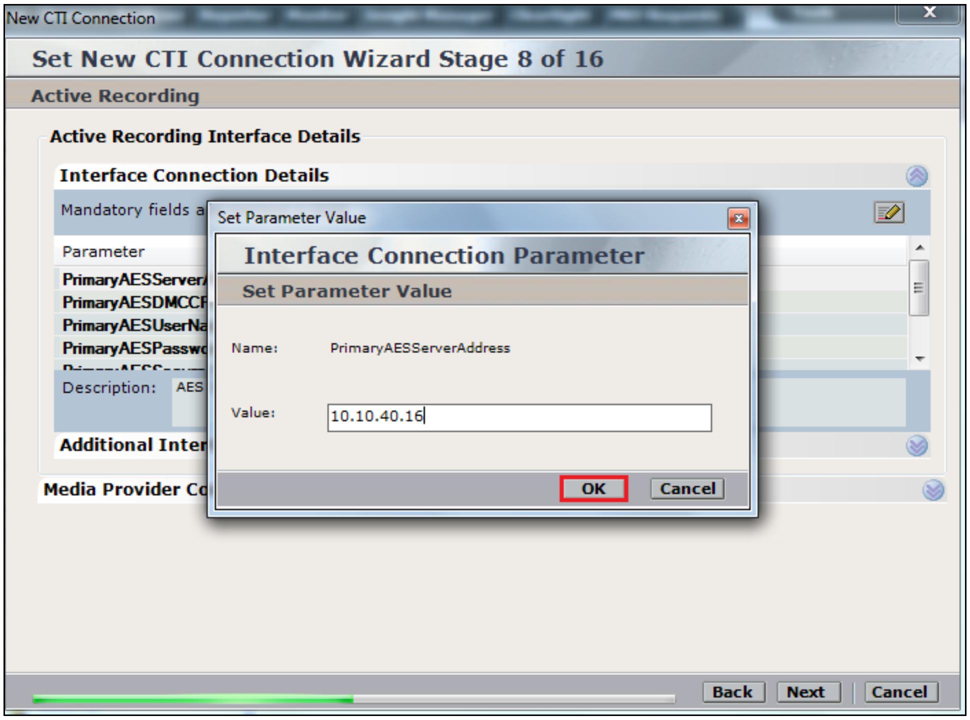
Parameter	Value
PrimaryAESServerAddress	
PrimaryAESDMCCPort	**4722**
PrimaryAESUserName	
PrimaryAESPassword	
PrimaryAESSecuredConnection	**TRUE**

Description:

Additional Interface Parameters

Media Provider Controllers - Location

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



New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Set Parameter Value

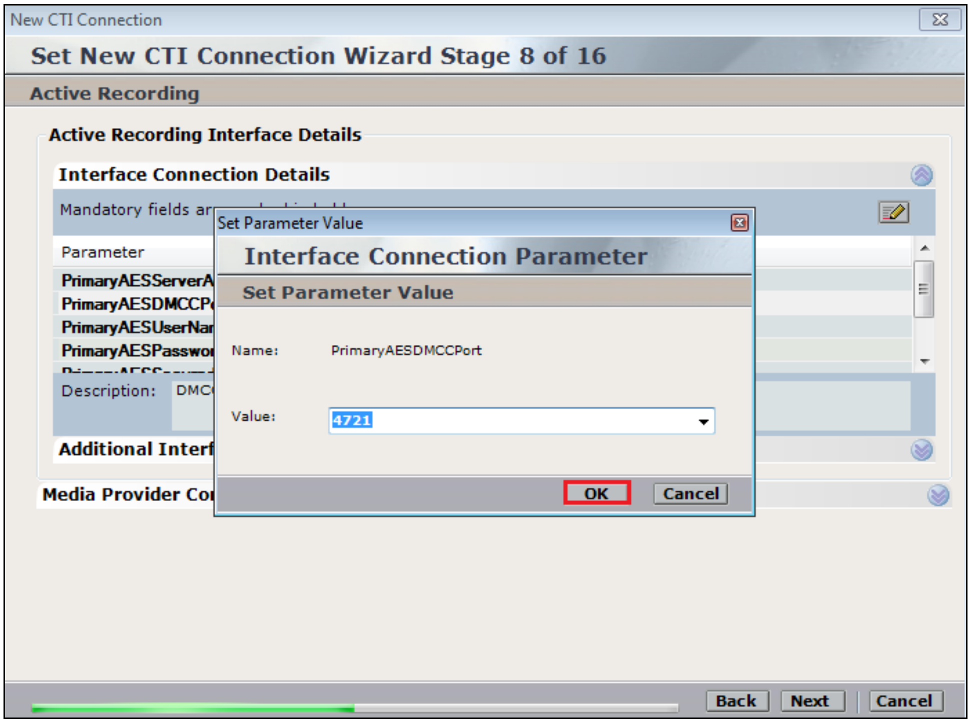
Interface Connection Parameter

Set Parameter Value

Name: PrimaryAESServerAddress

Value: 10.10.40.16

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



New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

Active Recording Interface Details

Interface Connection Details

Set Parameter Value

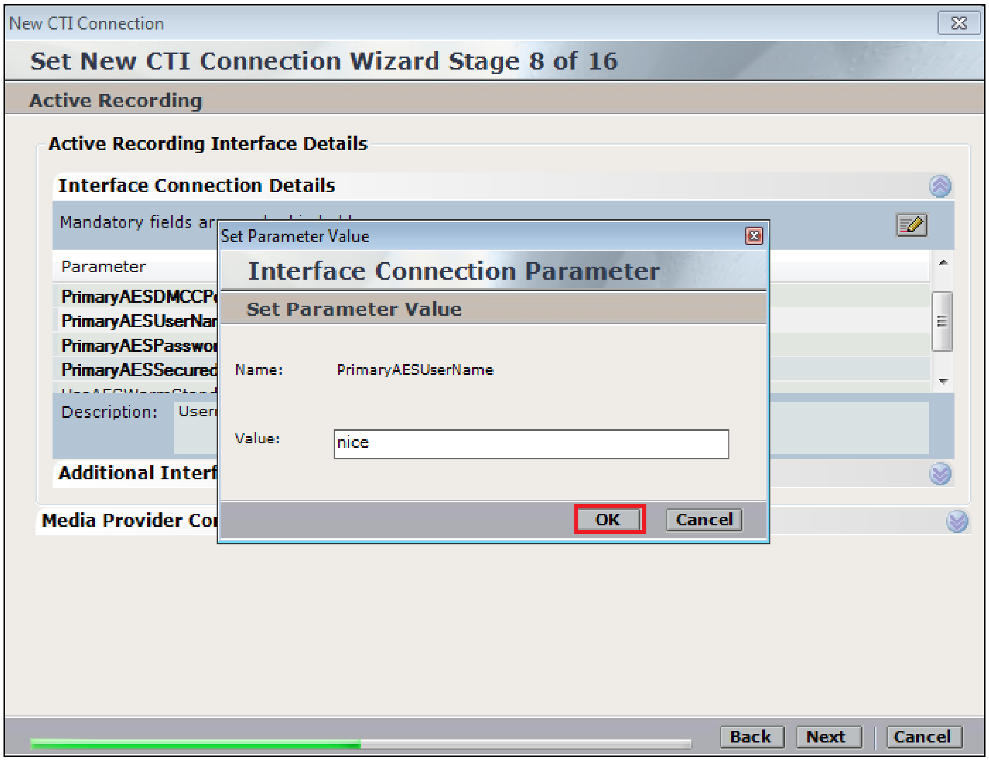
Interface Connection Parameter

Set Parameter Value

Name: PrimaryAESDMCCPort

Value: 4721

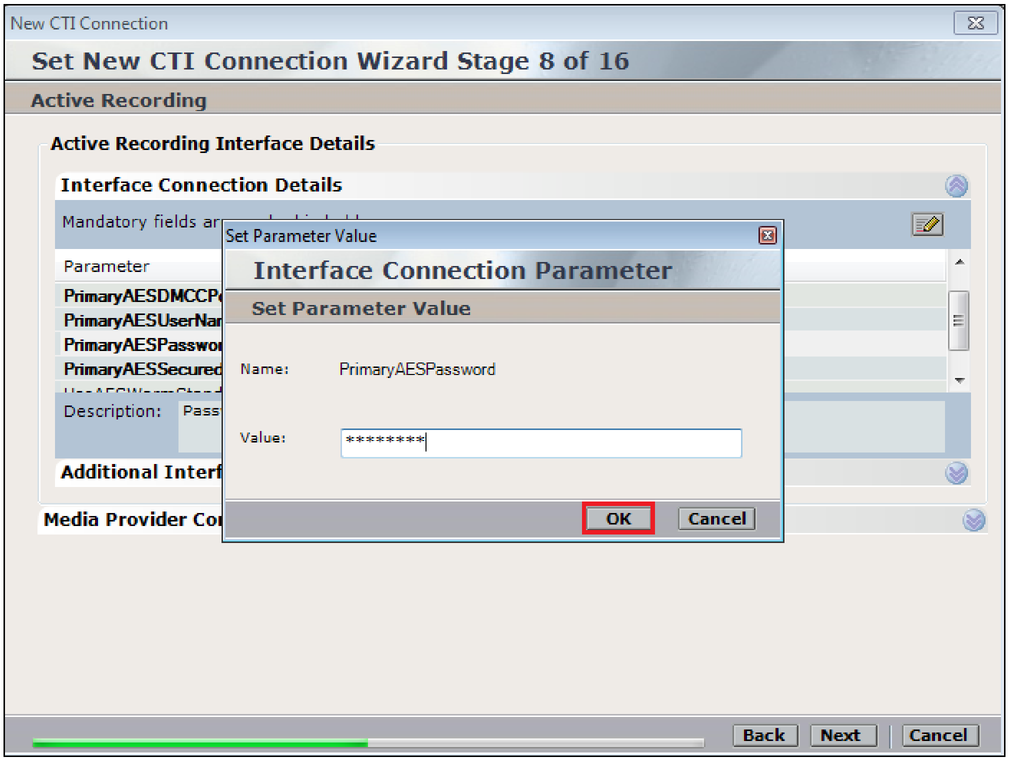
As before, enter the username that was created in **Section 6.6** and click on **OK**.



Name: PrimaryAESUserName

Value: nice

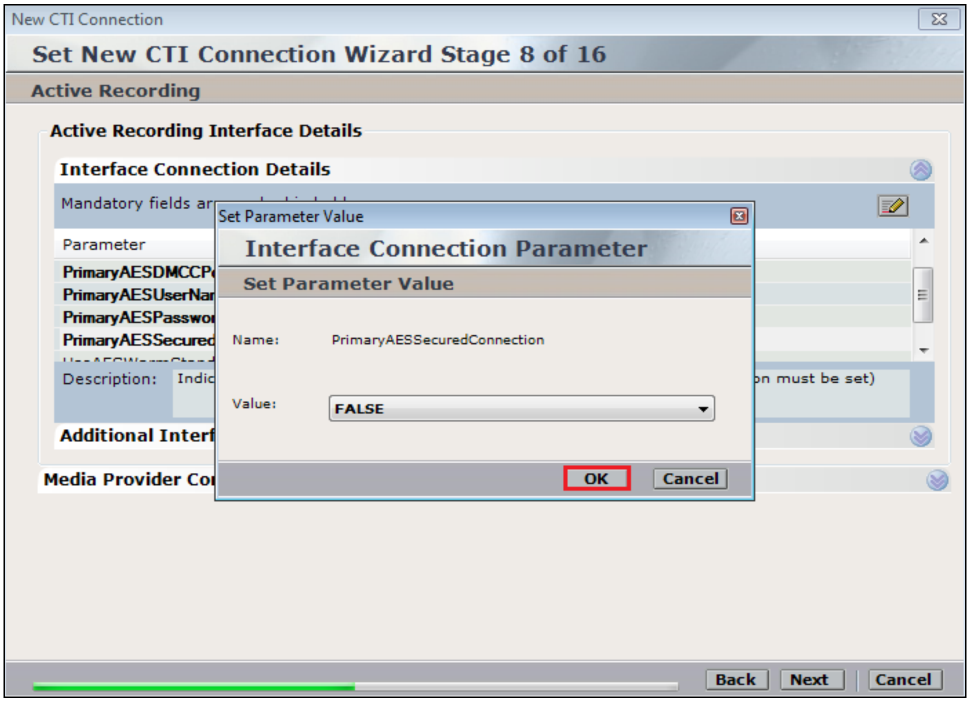
Enter the password that was created in **Section 6.6** and click on **OK**.



Name: PrimaryAESPassword

Value: *********

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

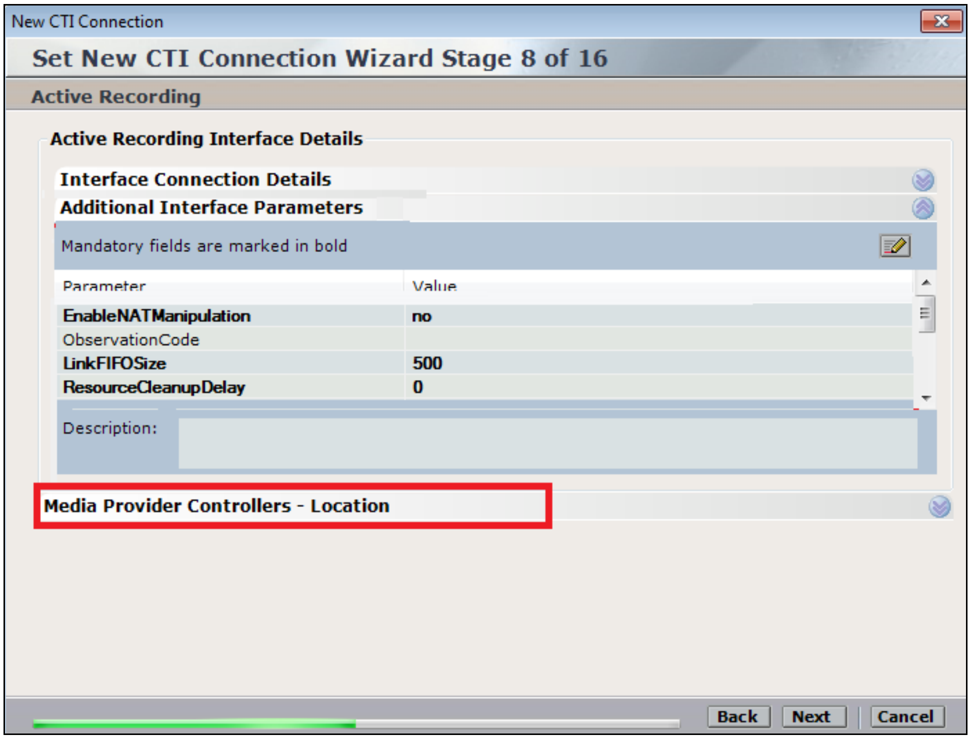


Set Parameter Value – Interface Connection Parameter – Set Parameter Value

Name: PrimaryAESSecuredConnection

Value: FALSE

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



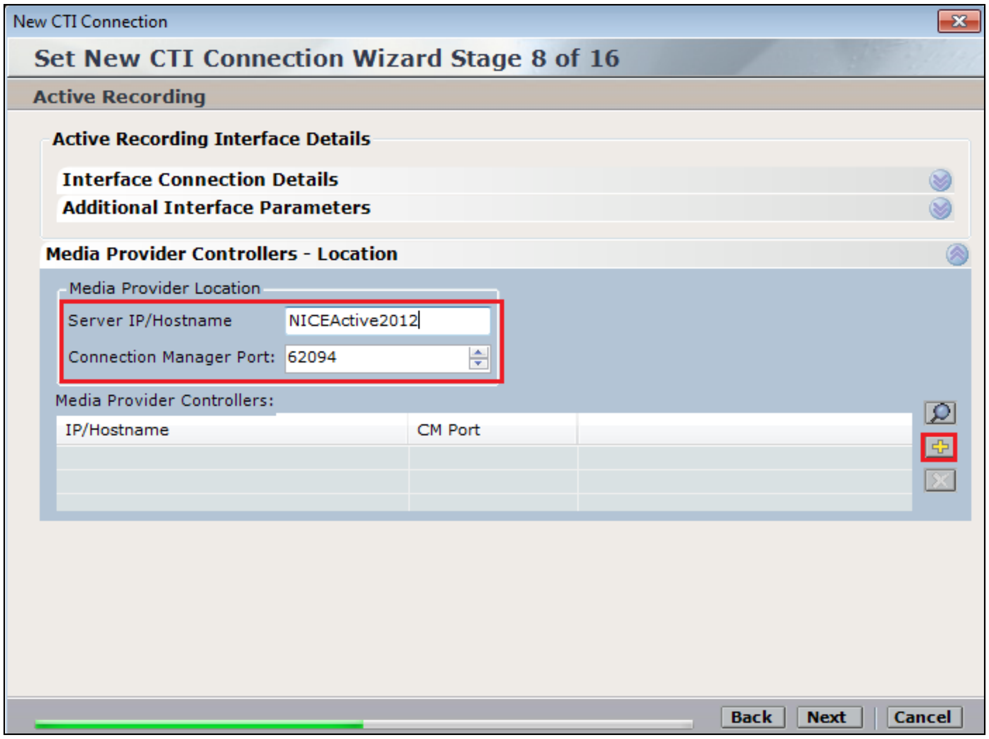
Mandatory fields are marked in bold

Parameter	Value
EnableNATManipulation	**no**
ObservationCode	
LinkFIFOSize	**500**
ResourceCleanupDelay	**0**

Description:

New CTI Connection
Set New CTI Connection Wizard Stage 8 of 16
Active Recording
Active Recording Interface Details
Interface Connection Details
Additional Interface Parameters
Media Provider Controllers - Location
Back
Next
Cancel

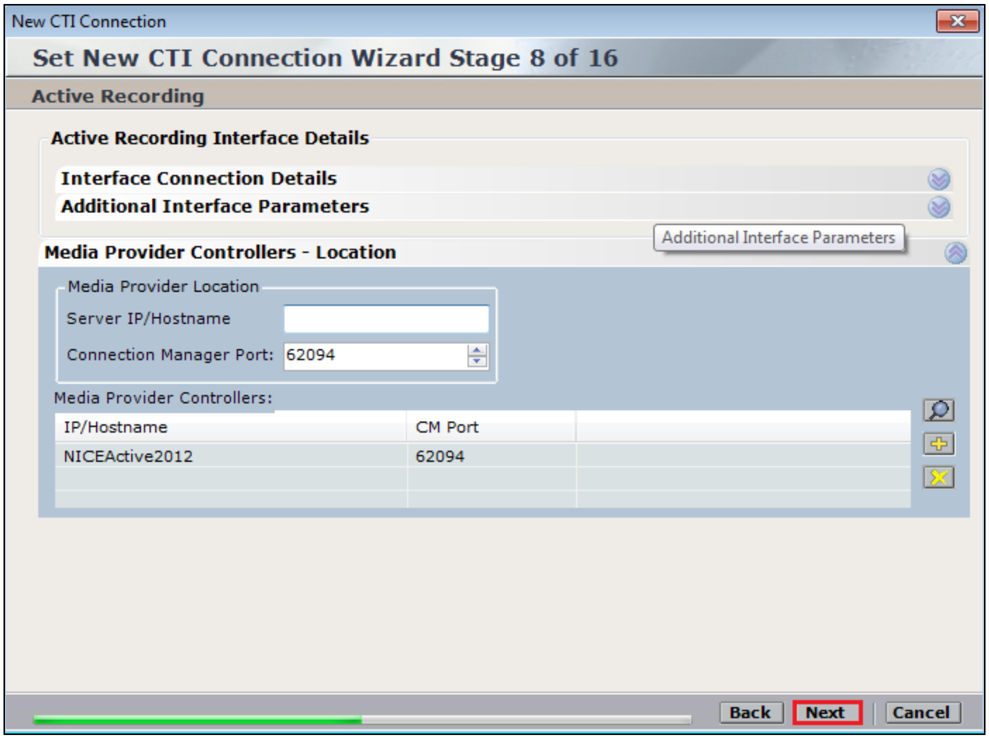
Enter the **IP/Hostname** of the Nice Advanced Interactions Server, then click on the **+** icon to add this.



New CTI Connection
Set New CTI Connection Wizard Stage 8 of 16
Active Recording
Active Recording Interface Details
Interface Connection Details
Additional Interface Parameters
Media Provider Controllers - Location
Media Provider Location
Media Provider Controllers:
IP/Hostname
CM Port
Back
Next
Cancel

Server IP/Hostname: NICEActive2012
Connection Manager Port: 62094

Click on **Next** to continue.

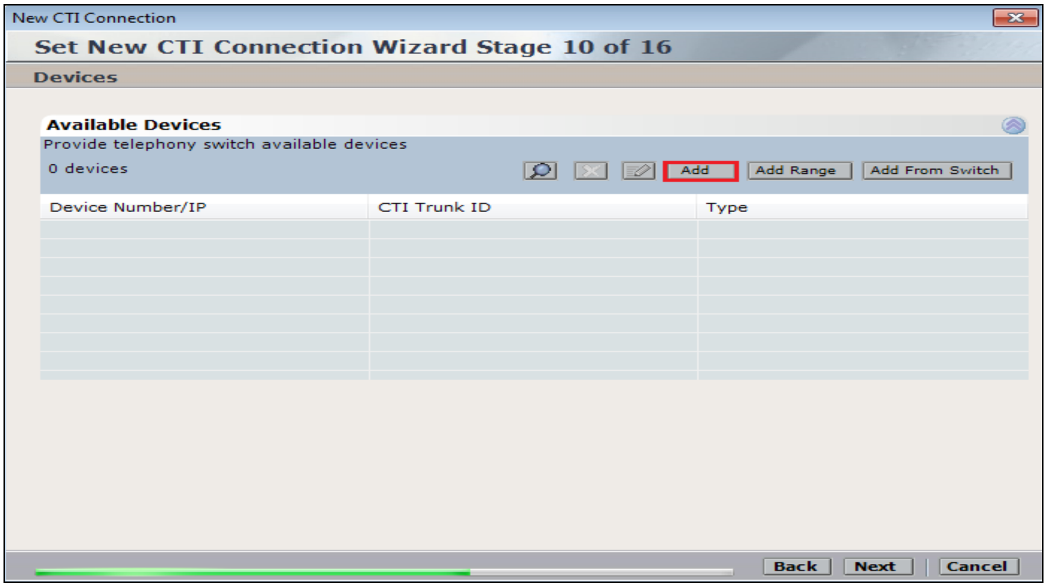


New CTI Connection
Set New CTI Connection Wizard Stage 8 of 16
Active Recording
Active Recording Interface Details
Interface Connection Details
Additional Interface Parameters
Additional Interface Parameters
Media Provider Controllers - Location
Media Provider Location
Media Provider Controllers:
Back
Next
Cancel

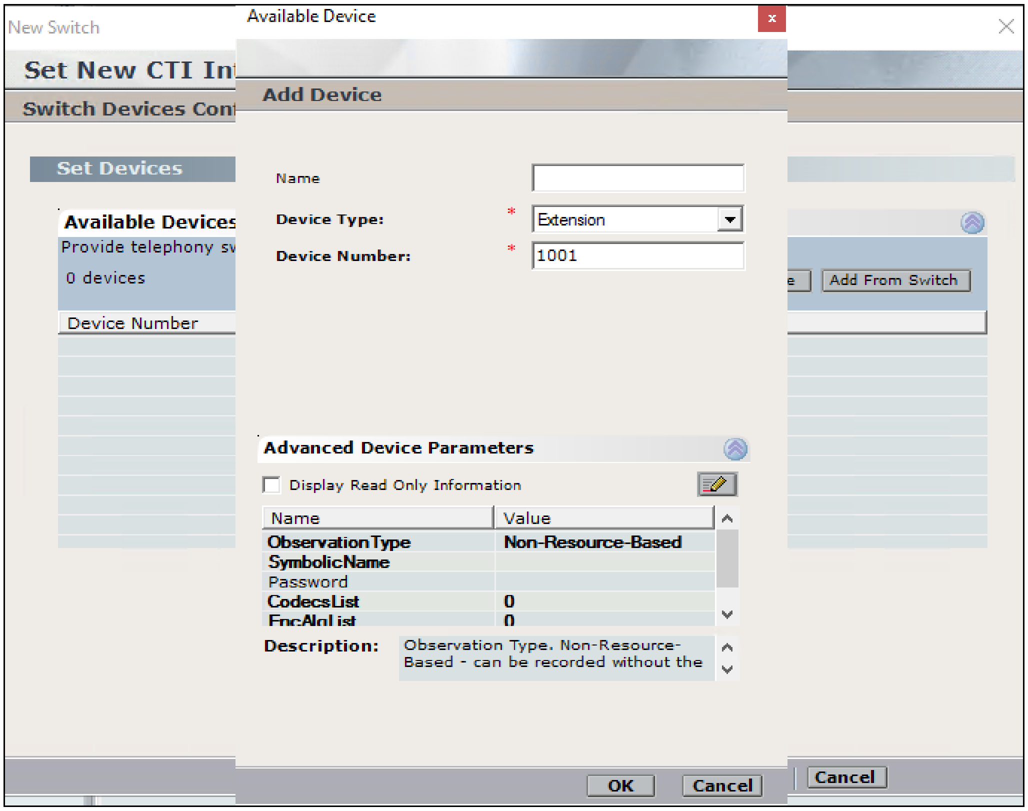
Server IP/Hostname:
Connection Manager Port: 62094

IP/Hostname	CM Port
NICEActive2012	62094

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 **1001**. Expand **Advanced Device Parameters** and ensure that the **Value** for **Observation Type** is set to Non-**Resourced-Based**. Click on **OK** to continue.



Available Device

Add Device

Name	
Device Type: *	Extension
Device Number: *	1001

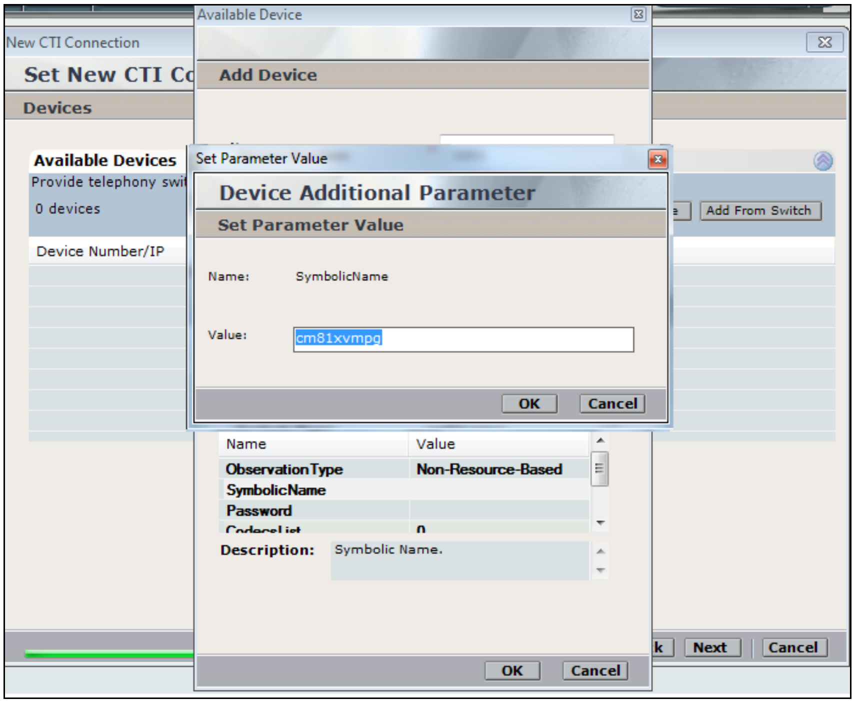
Advanced Device Parameters

□ Display Read Only Information

Name	Value
ObservationType	Non-Resource-Based
SymbolicName	
Password	
CodecsList	0
EncAlgList	0

Description: Observation Type. Non-Resource-Based - can be recorded without the

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**.



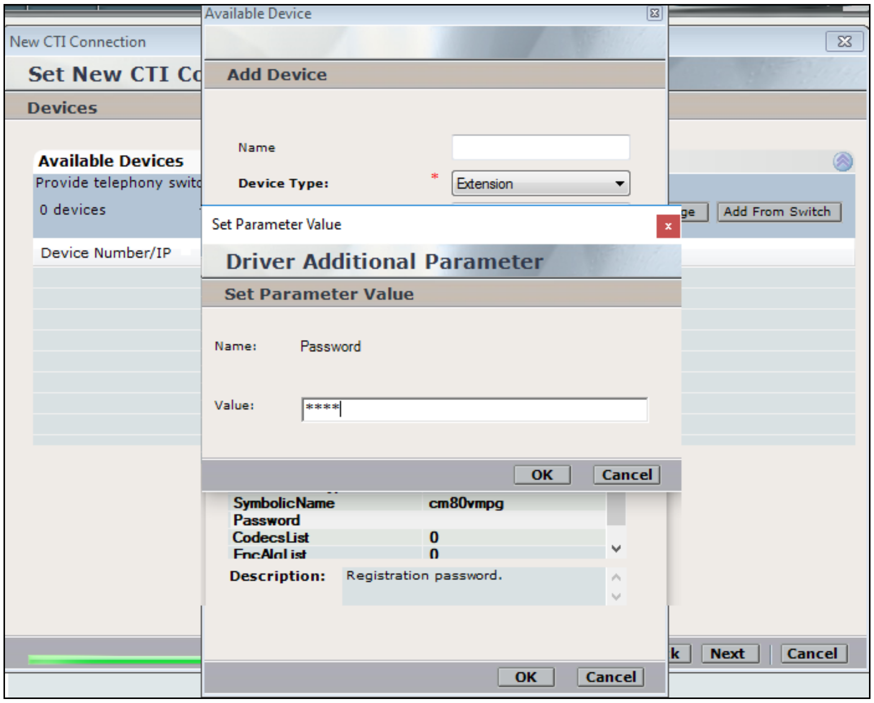
Name: SymbolicName

Value: cm81xvmpg

Name	Value
ObservationType	Non-Resource-Based
SymbolicName	
Password	
CodecsList	0

Description: Symbolic Name.

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



Name

Device Type: * Extension

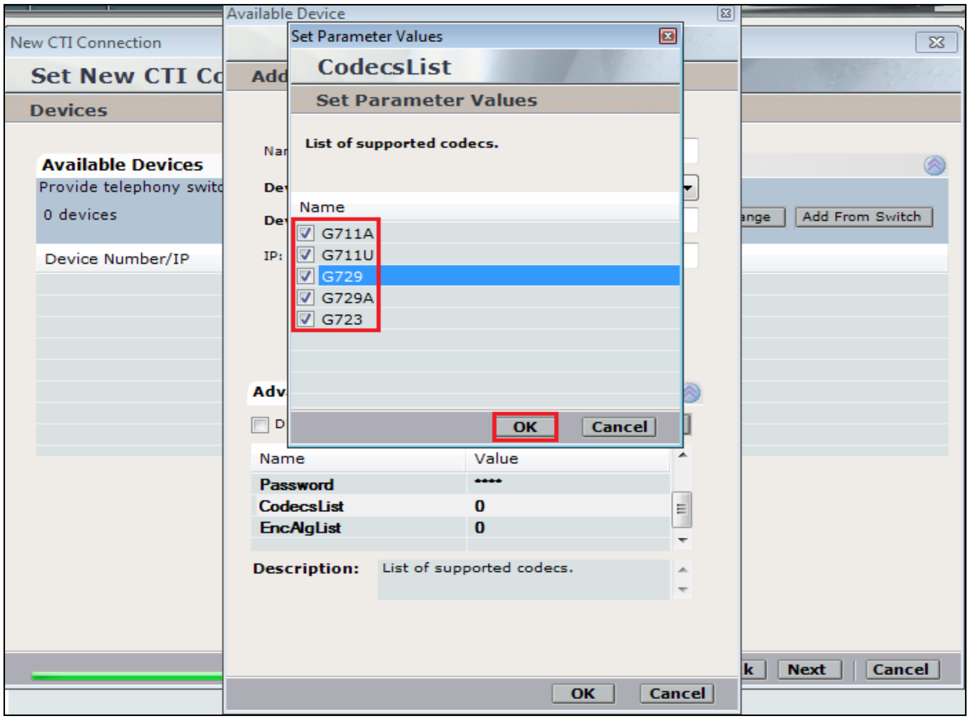
Name: Password

Value: ****

SymbolicName	cm80vmpg
Password	
CodecsList	0
EncAlgList	0

Description: Registration password.

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



Set Parameter Values

CodecsList

Set Parameter Values

List of supported codecs.

Name

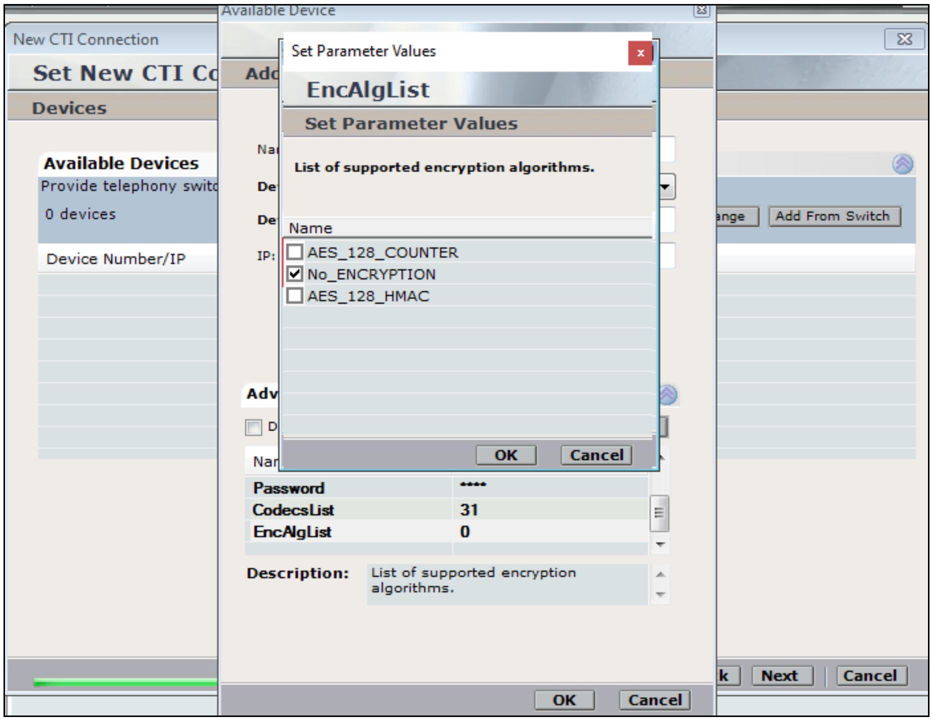
☑ G711A
☑ G711U
☑ G729
☑ G729A
☑ G723

OK Cancel

Name	Value
Password	****
CodecsList	0
EncAlgList	0

Description: List of supported codecs.

Double-click on **EncAlgList** and since no SRTP was being recorded on this occasion **No_ENCRYPTION** was ticked. Click on **OK** to continue.



Set Parameter Values

EncAlgList

Set Parameter Values

List of supported encryption algorithms.

Name

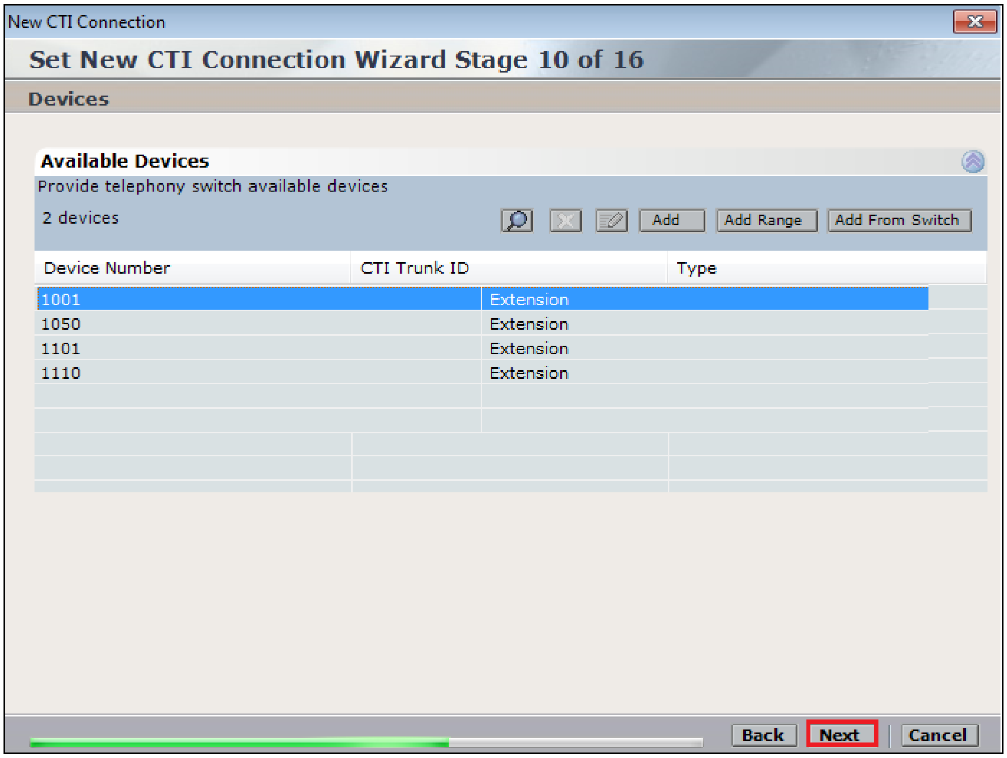
☐ AES_128_COUNTER
☑ No_ENCRYPTION
☐ AES_128_HMAC

OK Cancel

Name	Value
Password	****
CodecsList	31
EncAlgList	0

Description: List of supported encryption algorithms.

Click on **Next** to continue.



New CTI Connection

Set New CTI Connection Wizard Stage 10 of 16

Devices

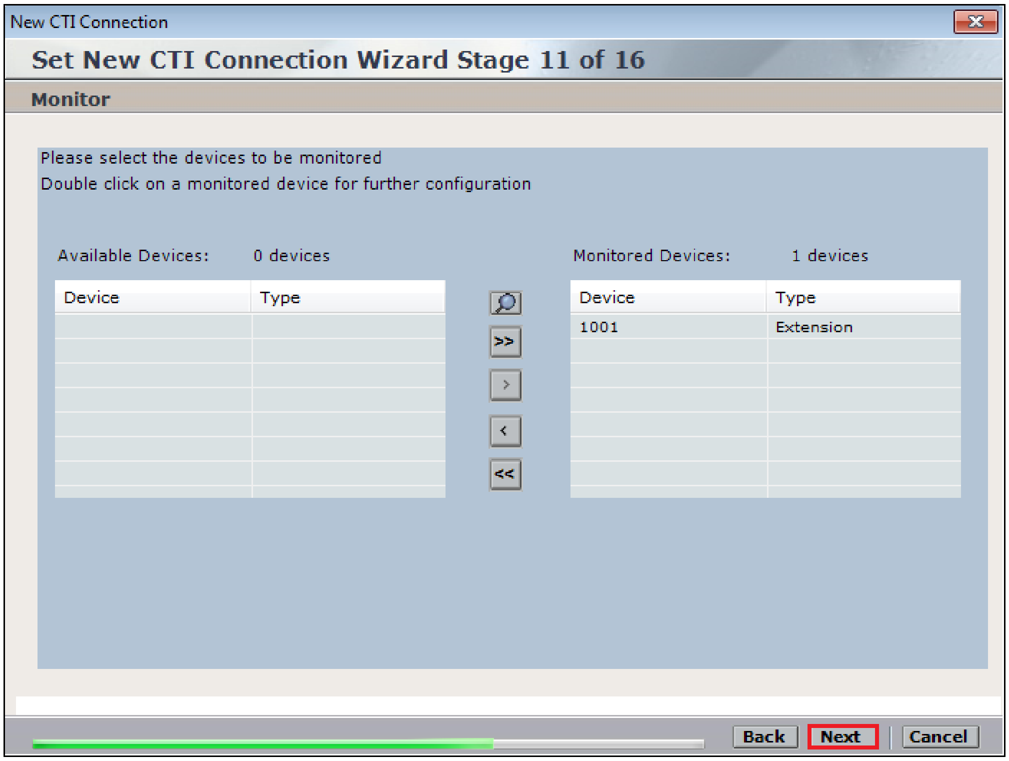
Available Devices

Provide telephony switch available devices

2 devices

Device Number	CTI Trunk ID	Type
1001		Extension
1050		Extension
1101		Extension
1110		Extension

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



New CTI Connection

Set New CTI Connection Wizard Stage 11 of 16

Monitor

Please select the devices to be monitored

Double click on a monitored device for further configuration

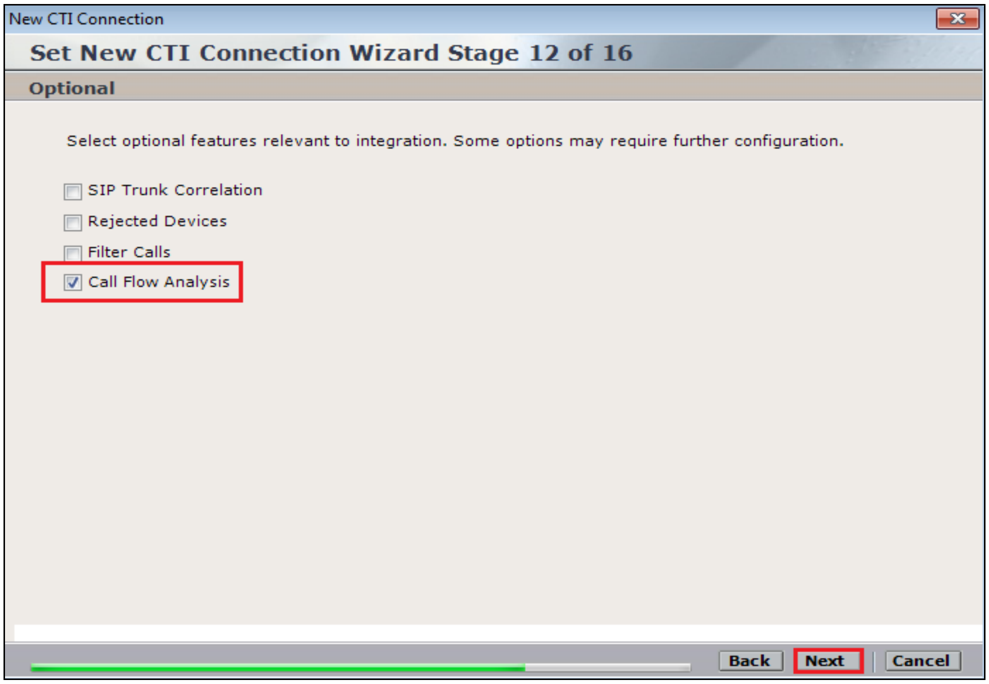
Available Devices: 0 devices

Device	Type

Monitored Devices: 1 devices

Device	Type
1001	Extension

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



New CTI Connection

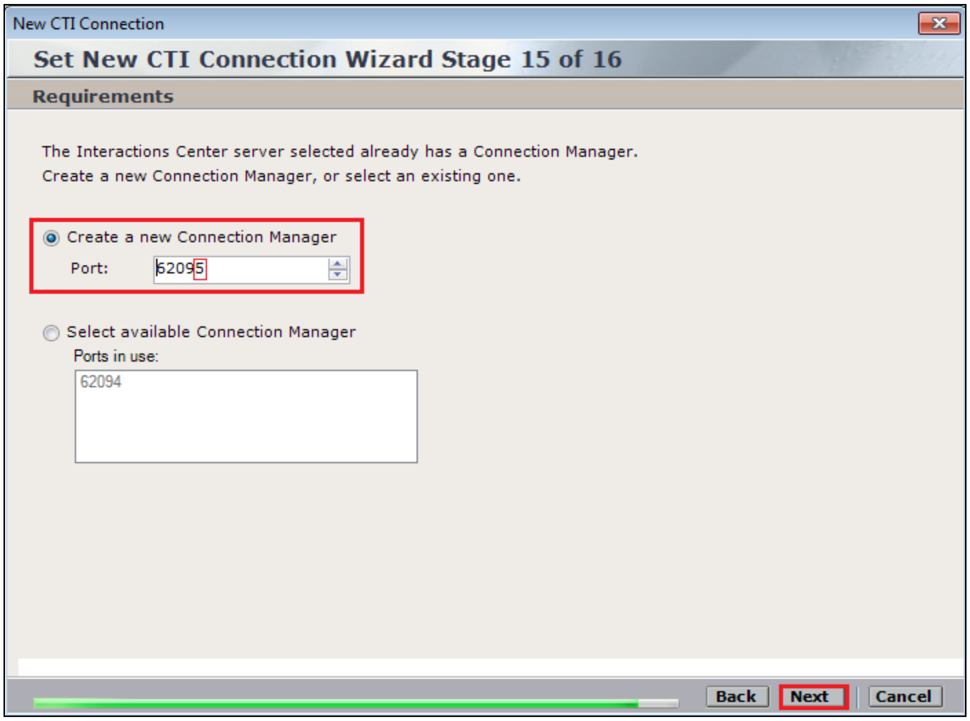
Set New CTI Connection Wizard Stage 12 of 16

Optional

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

- □ SIP Trunk Correlation
- □ Rejected Devices
- □ Filter Calls
- ☑ Call Flow Analysis

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



New CTI Connection

Set New CTI Connection Wizard Stage 15 of 16

Requirements

The Interactions Center server selected already has a Connection Manager.
Create a new Connection Manager, or select an existing one.

● Create a new Connection Manager

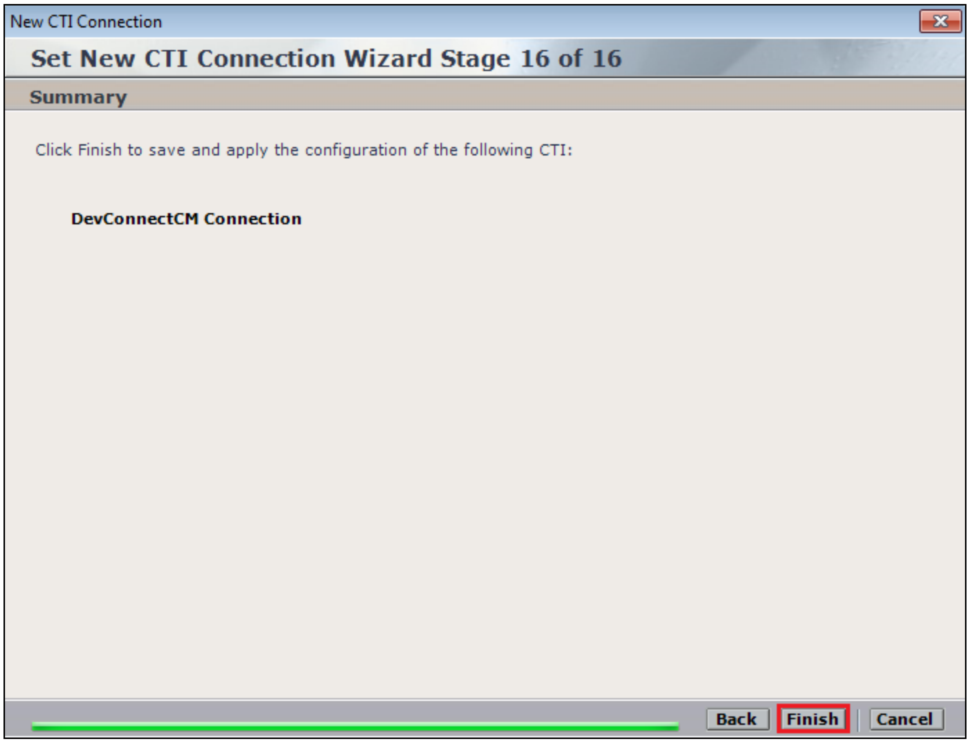
Port: 62095

○ Select available Connection Manager

Ports in use:

62094

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



New CTI Connection

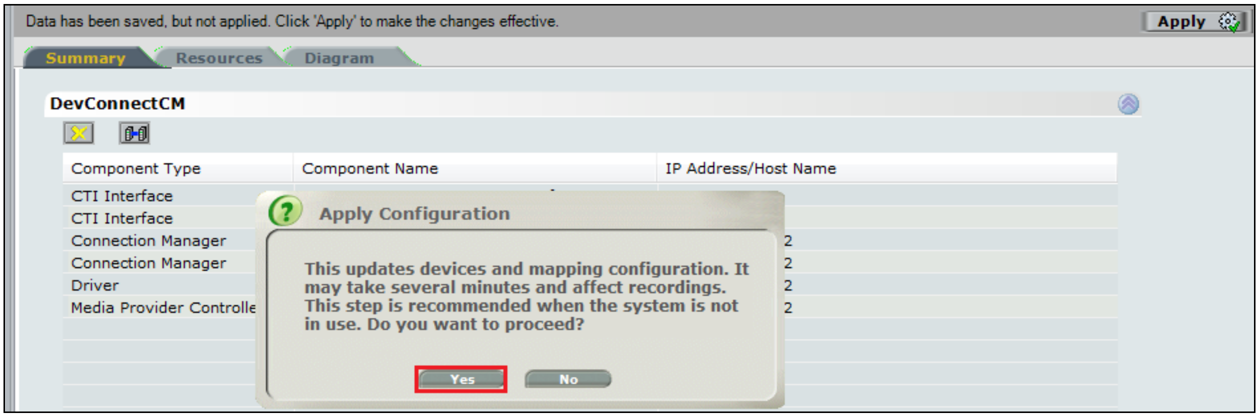
Set New CTI Connection Wizard Stage 16 of 16

Summary

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

DevConnectCM Connection

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



Data has been saved, but not applied. Click 'Apply' to make the changes effective.

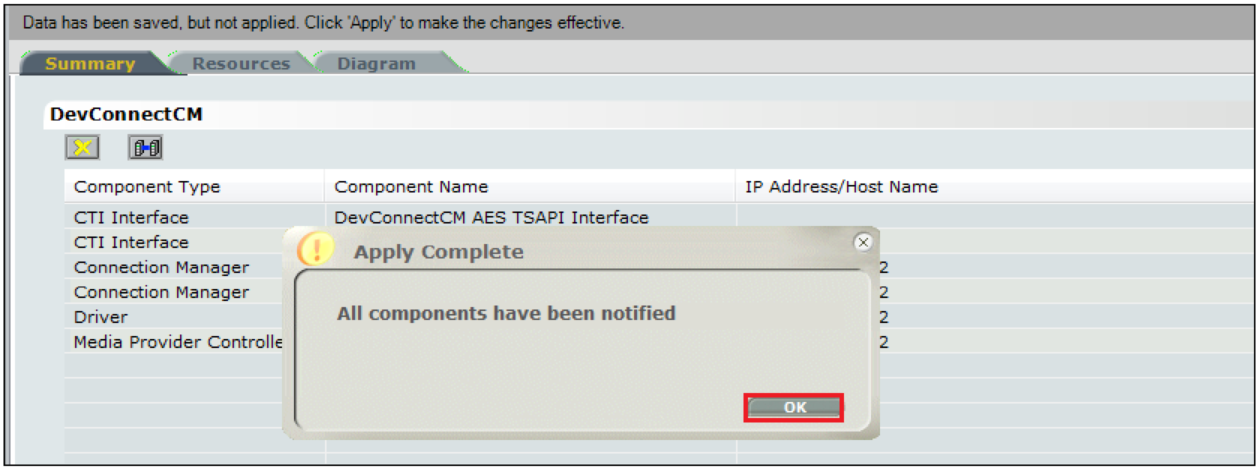
DevConnectCM

Component Type	Component Name	IP Address/Host Name
CTI Interface		
CTI Interface		
Connection Manager		2
Connection Manager		2
Driver		2
Media Provider Controlle		2

Apply Configuration

This updates devices and mapping configuration. It may take several minutes and affect recordings. This step is recommended when the system is not in use. Do you want to proceed?

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



Data has been saved, but not applied. Click 'Apply' to make the changes effective.

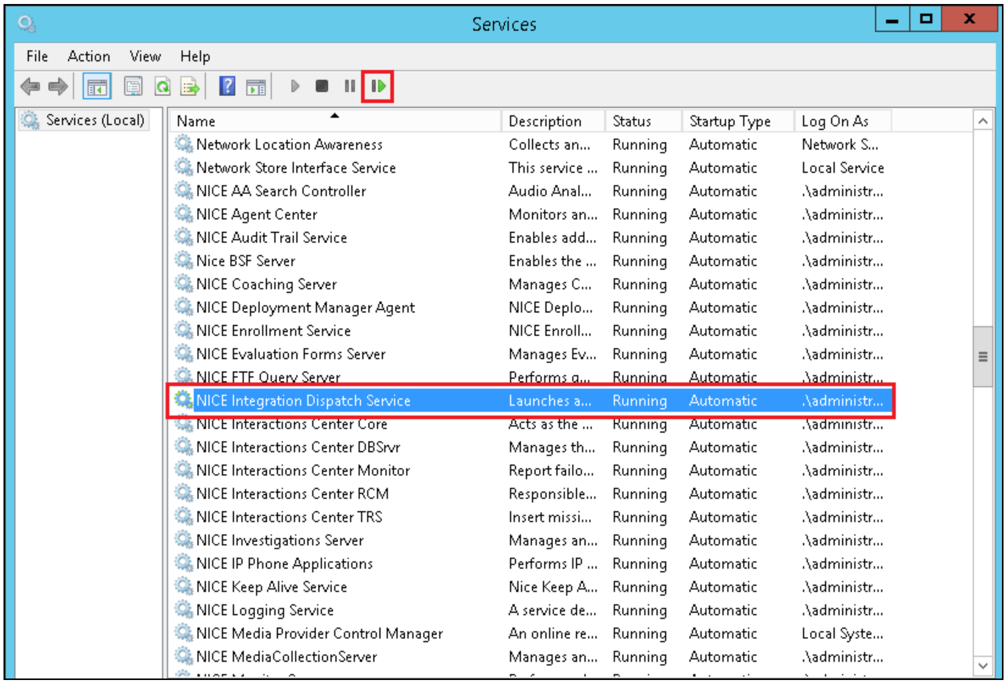
DevConnectCM

Component Type	Component Name	IP Address/Host Name
CTI Interface	DevConnectCM AES TSAPI Interface	
CTI Interface		
Connection Manager		2
Connection Manager		2
Driver		2
Media Provider Controlle		2

Apply Complete

All components have been notified

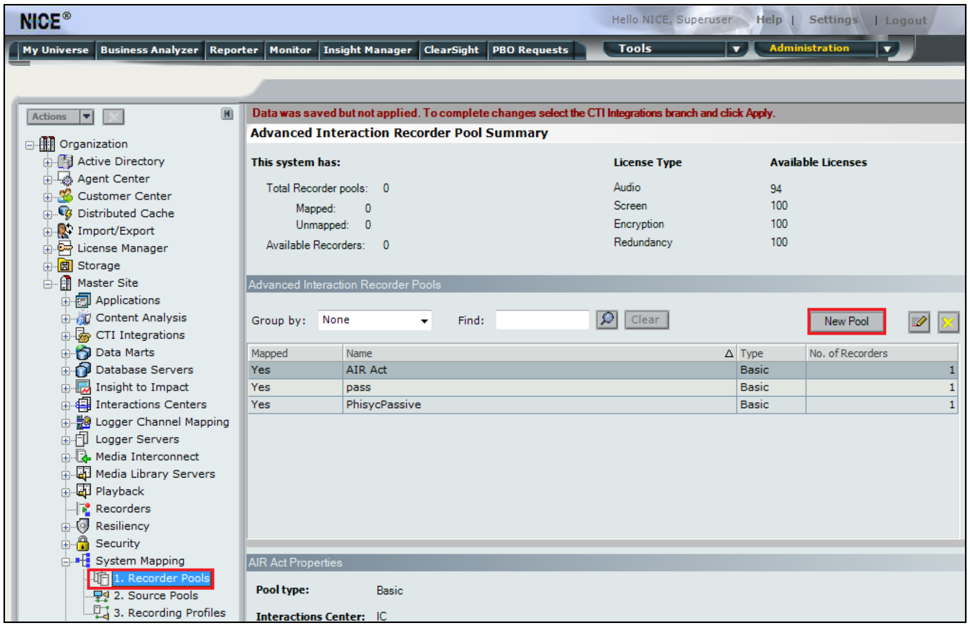
From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.



Name	Description	Status	Startup Type	Log On As
Network Location Awareness	Collects an...	Running	Automatic	Network S...
Network Store Interface Service	This service ...	Running	Automatic	Local Service
NICE AA Search Controller	Audio Anal...	Running	Automatic	.\administr...
NICE Agent Center	Monitors an...	Running	Automatic	.\administr...
NICE Audit Trail Service	Enables add...	Running	Automatic	.\administr...
Nice BSF Server	Enables the ...	Running	Automatic	.\administr...
NICE Coaching Server	Manages C...	Running	Automatic	.\administr...
NICE Deployment Manager Agent	NICE Deplo...	Running	Automatic	.\administr...
NICE Enrollment Service	NICE Enroll...	Running	Automatic	.\administr...
NICE Evaluation Forms Server	Manages Ev...	Running	Automatic	.\administr...
NICE FTF Query Server	Performs q...	Running	Automatic	.\administr...
NICE Integration Dispatch Service	Launches a...	Running	Automatic	.\administr...
NICE Interactions Center Core	Acts as the ...	Running	Automatic	.\administr...
NICE Interactions Center DBSrvr	Manages th...	Running	Automatic	.\administr...
NICE Interactions Center Monitor	Report failo...	Running	Automatic	.\administr...
NICE Interactions Center RCM	Responsible...	Running	Automatic	.\administr...
NICE Interactions Center TRS	Insert missi...	Running	Automatic	.\administr...
NICE Investigations Server	Manages an...	Running	Automatic	.\administr...
NICE IP Phone Applications	Performs IP ...	Running	Automatic	.\administr...
NICE Keep Alive Service	Nice Keep A...	Running	Automatic	.\administr...
NICE Logging Service	A service de...	Running	Automatic	.\administr...
NICE Media Provider Control Manager	An online re...	Running	Automatic	Local Syste...
NICE MediaCollectionServer	Manages an...	Running	Automatic	.\administr...

7.2. System Mapping

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



Data was saved but not applied. To complete changes select the CTI Integrations branch and click Apply.

Advanced Interaction Recorder Pool Summary

This system has:

Total Recorder pools: 0
Mapped: 0
Unmapped: 0
Available Recorders: 0

License Type	Available Licenses
Audio	94
Screen	100
Encryption	100
Redundancy	100

Advanced Interaction Recorder Pools

Group by: None Find: Clear New Pool

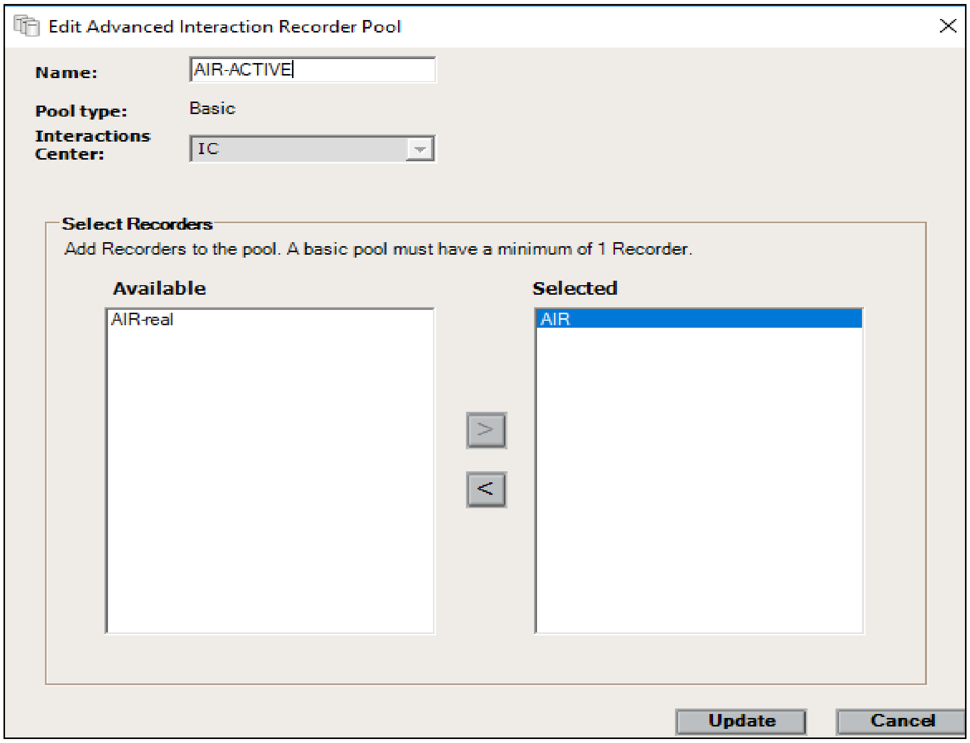
Mapped	Name	Type	No. of Recorders
Yes	AIR Act	Basic	1
Yes	pass	Basic	1
Yes	PhisycPassive	Basic	1

AIR Act Properties

Pool type: Basic

Interactions Center: IC

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


Edit Advanced Interaction Recorder Pool

Name: AIR-ACTIVE

Pool type: Basic

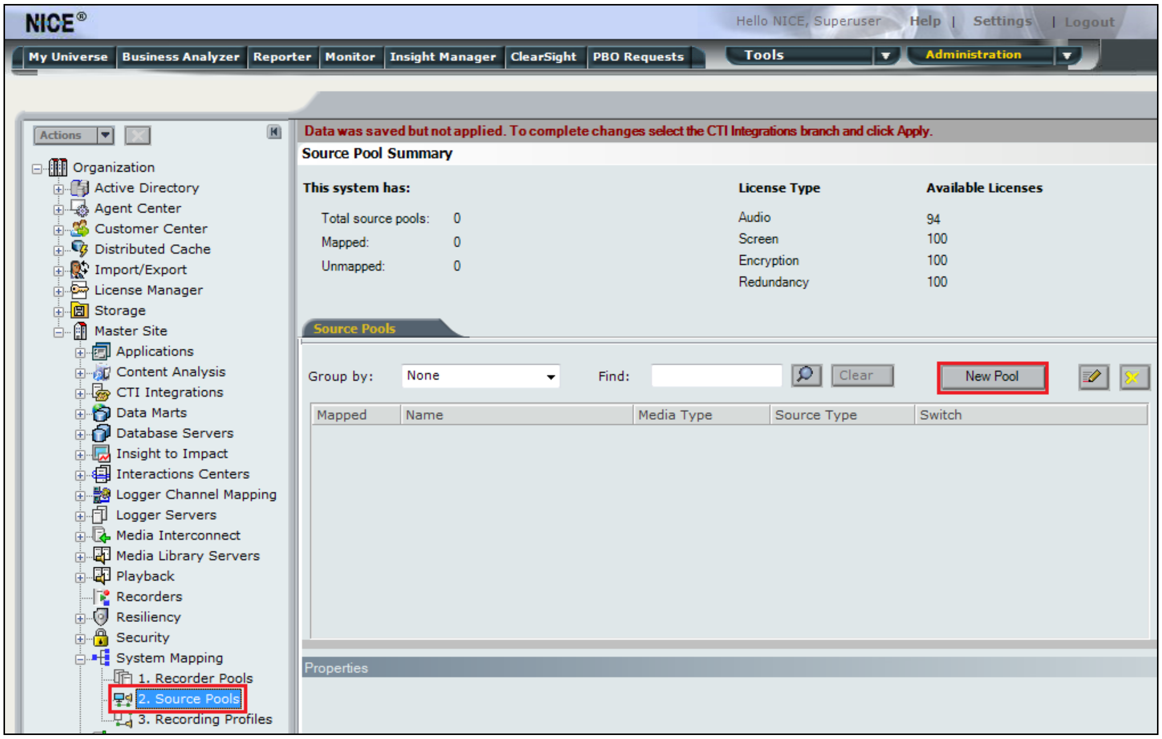
Interactions Center: IC

Select Recorders

Add Recorders to the pool. A basic pool must have a minimum of 1 Recorder.

Available	Selected
AIR-real	AIR

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



Data was saved but not applied. To complete changes select the CTI Integrations branch and click Apply.

Source Pool Summary

This system has:

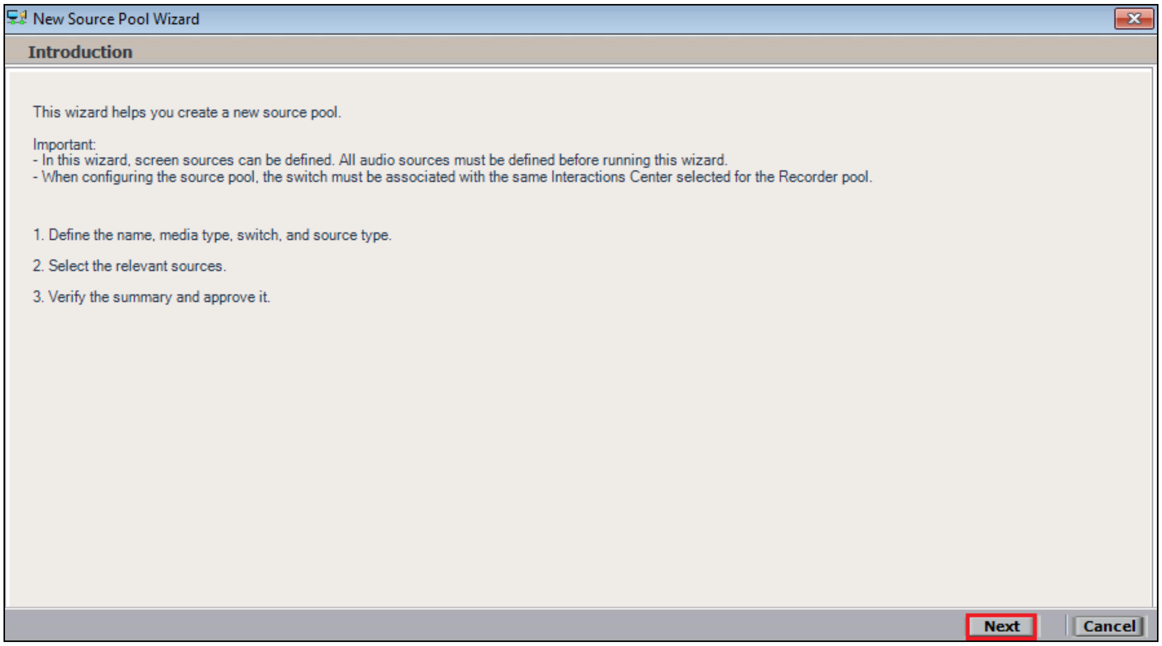
Total source pools:	0
Mapped:	0
Unmapped:	0

License Type	Available Licenses
Audio	94
Screen	100
Encryption	100
Redundancy	100

Group by: None   Find:

Mapped	Name	Media Type	Source Type	Switch

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



Introduction

This wizard helps you create a new source pool.

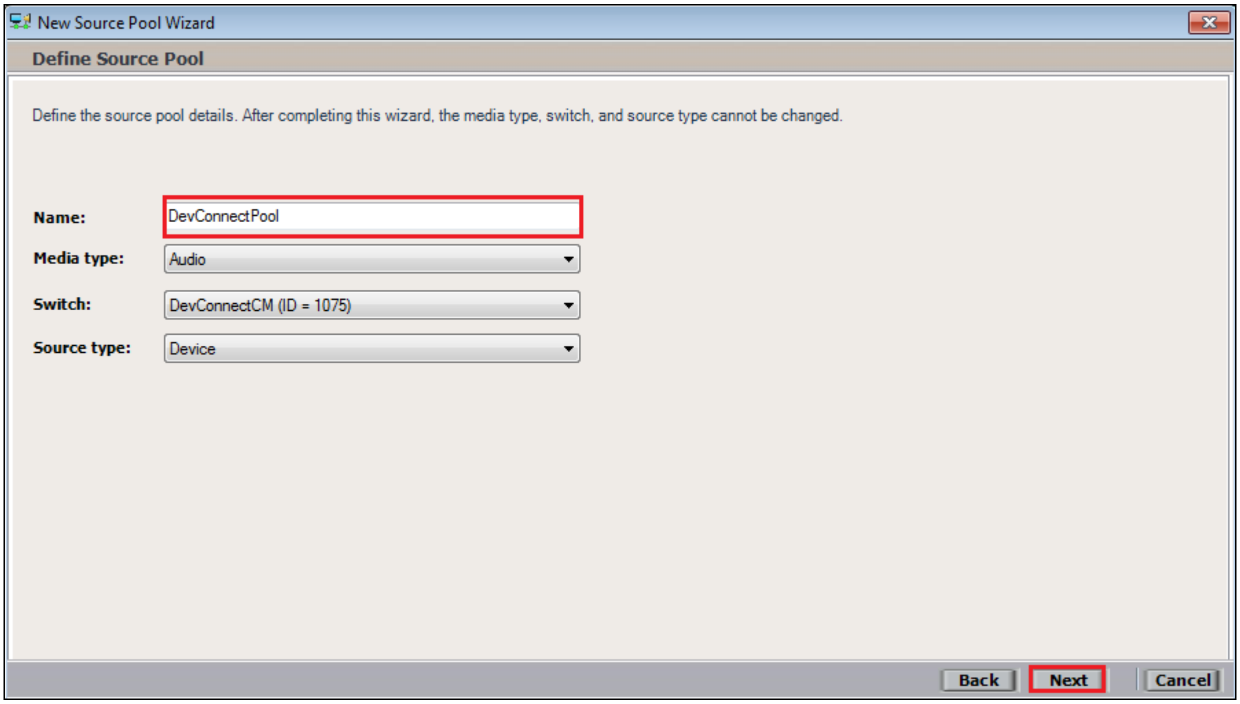
Important:
- In this wizard, screen sources can be defined. All audio sources must be defined before running this wizard.
- When configuring the source pool, the switch must be associated with the same Interactions Center selected for the Recorder pool.

1. Define the name, media type, switch, and source type.

2. Select the relevant sources.

3. Verify the summary and approve it.

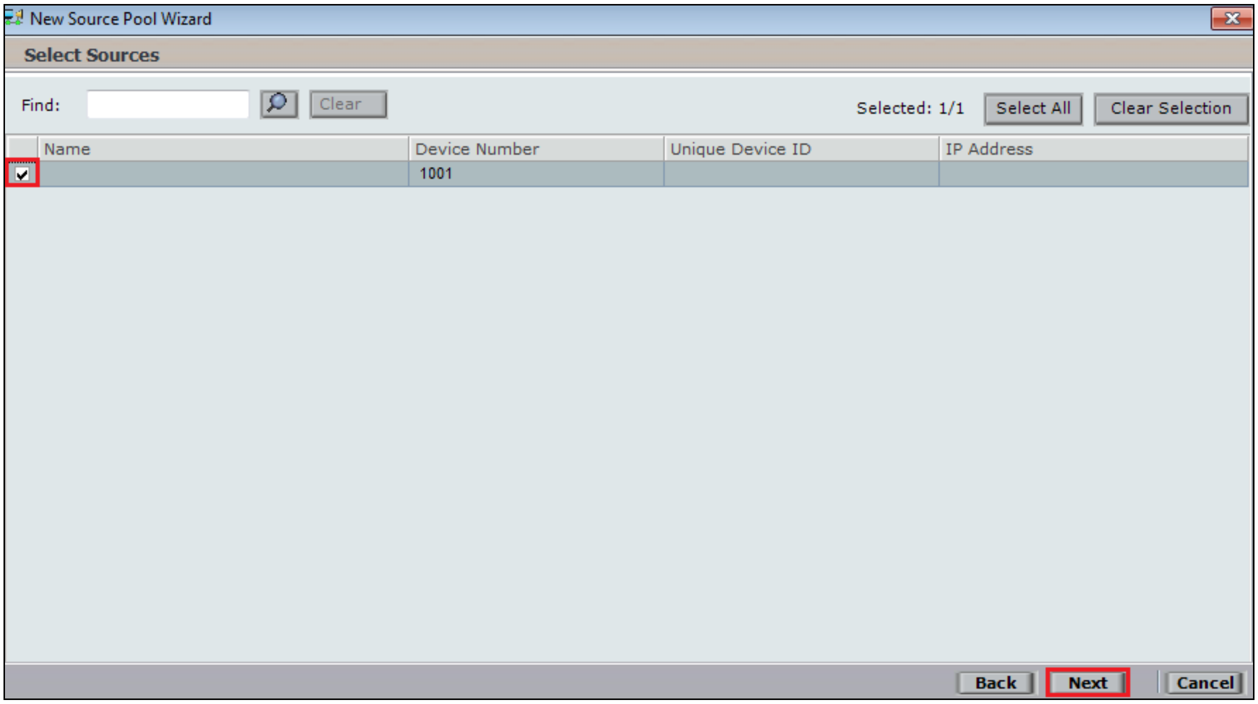
Enter a suitable **Name** and the other values were left as default. Click on **Next** to continue.



Define the source pool details. After completing this wizard, the media type, switch, and source type cannot be changed.

Name:	DevConnectPool
Media type:	Audio
Switch:	DevConnectCM (ID = 1075)
Source type:	Device

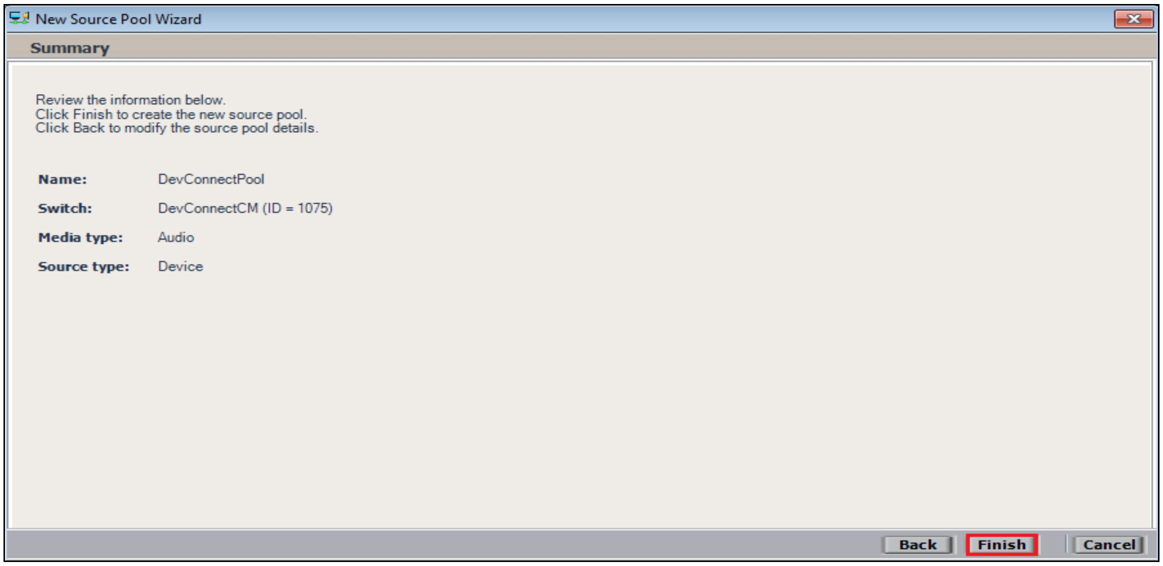
Select the extensions that were created in **Section 7.1**, note only one extension number is shown in the example below but this is not typical. Click on **Next** to continue.



Selected: 1/1

	Name	Device Number	Unique Device ID	IP Address
☑		1001		

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

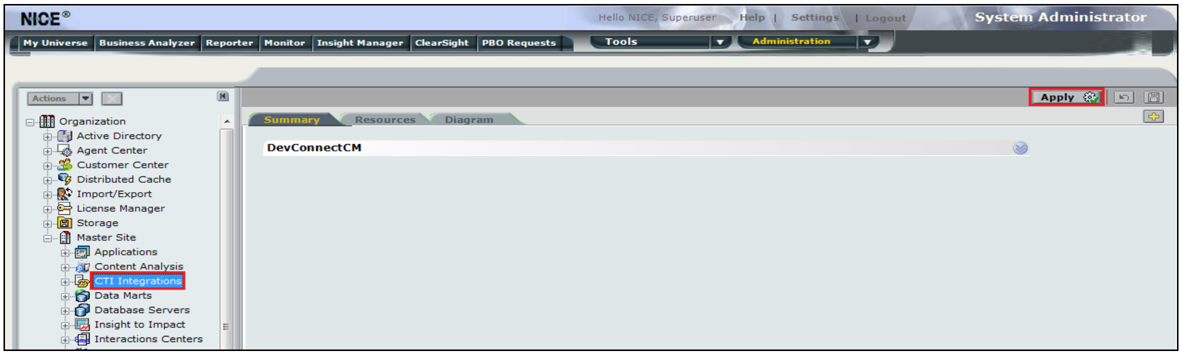


Summary

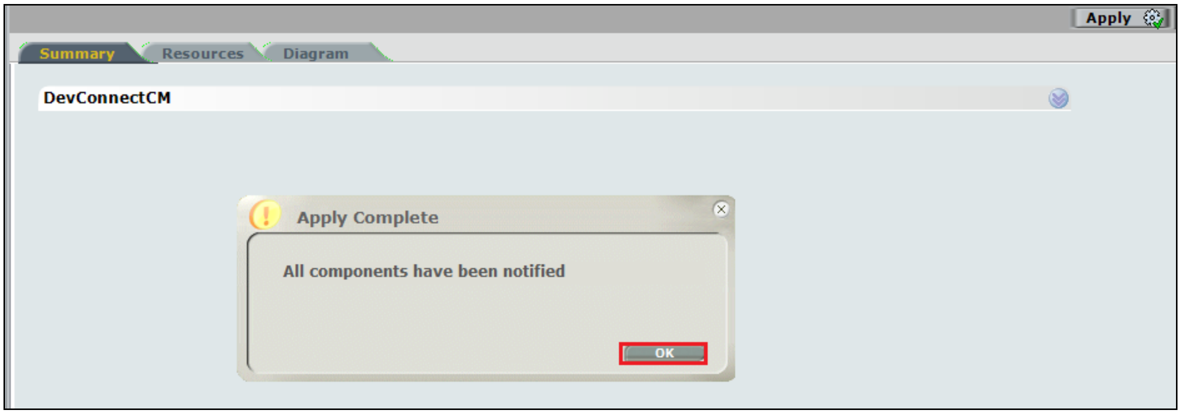
Review the information below.
Click Finish to create the new source pool.
Click Back to modify the source pool details.

Name:	DevConnectPool
Switch:	DevConnectCM (ID = 1075)
Media type:	Audio
Source type:	Device

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.



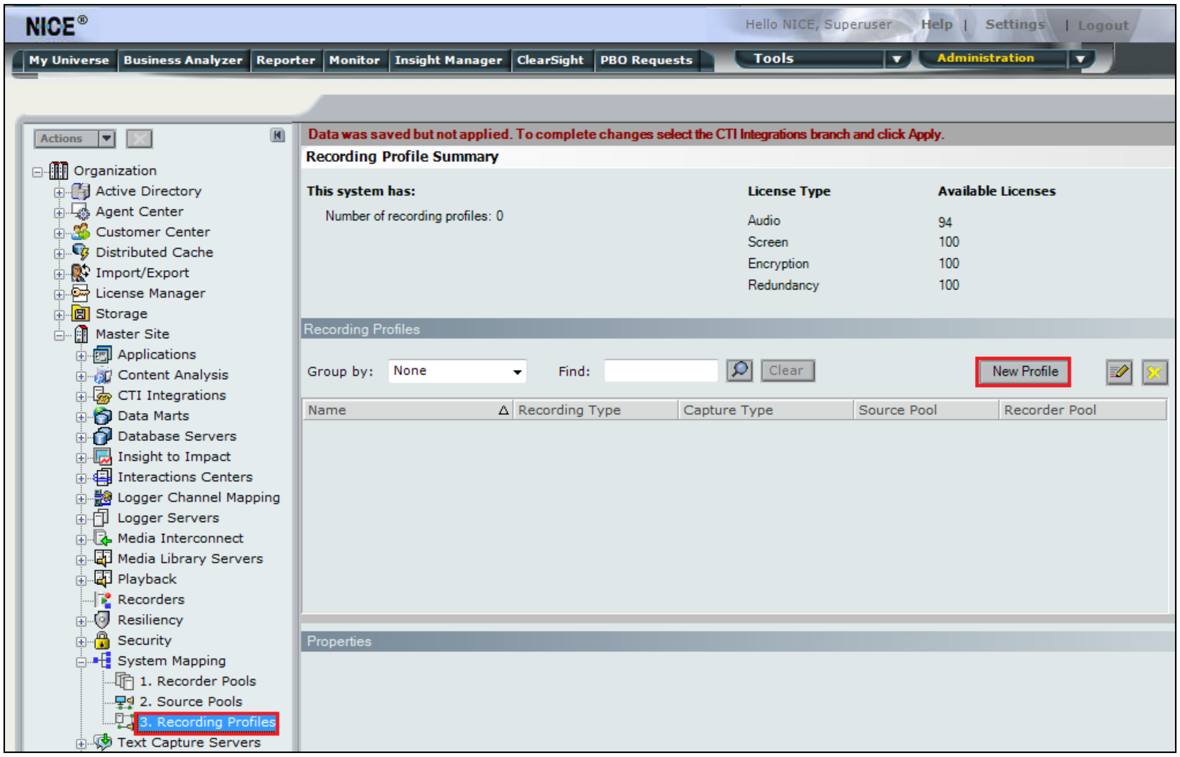
The following screen shows the changes were saved correctly. Click on **OK** to continue.



Apply Complete

All components have been notified

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



Data was saved but not applied. To complete changes select the CTI Integrations branch and click Apply.

Recording Profile Summary

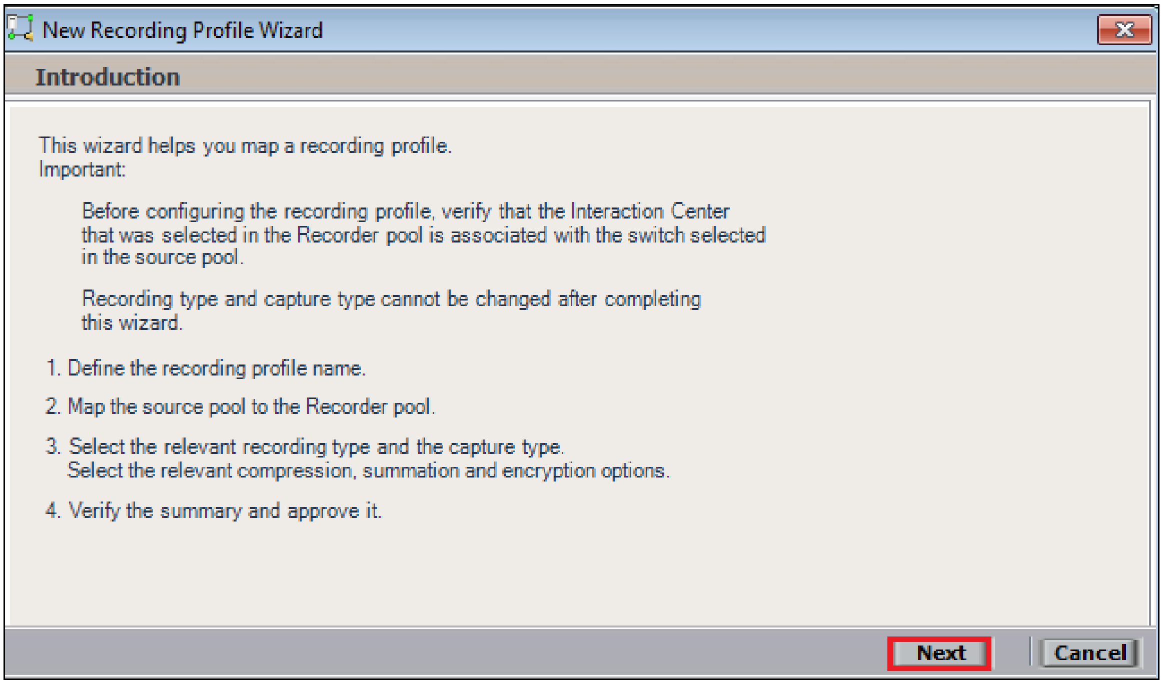
This system has:

Number of recording profiles: 0

License Type	Available Licenses
Audio	94
Screen	100
Encryption	100
Redundancy	100

Name	Recording Type	Capture Type	Source Pool	Recorder Pool

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



Introduction

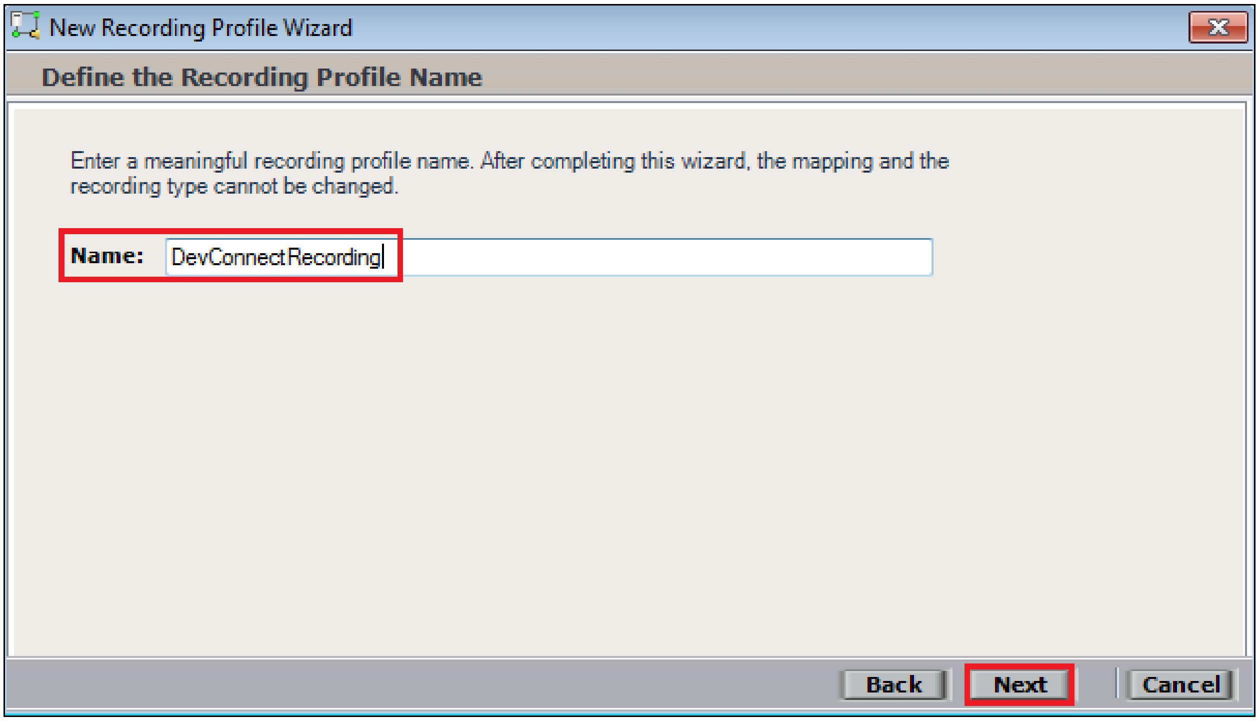
This wizard helps you map a recording profile.
Important:

Before configuring the recording profile, verify that the Interaction Center that was selected in the Recorder pool is associated with the switch selected in the source pool.

Recording type and capture type cannot be changed after completing this wizard.

1. Define the recording profile name.
2. Map the source pool to the Recorder pool.
3. Select the relevant recording type and the capture type.
   Select the relevant compression, summation and encryption options.
4. Verify the summary and approve it.

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



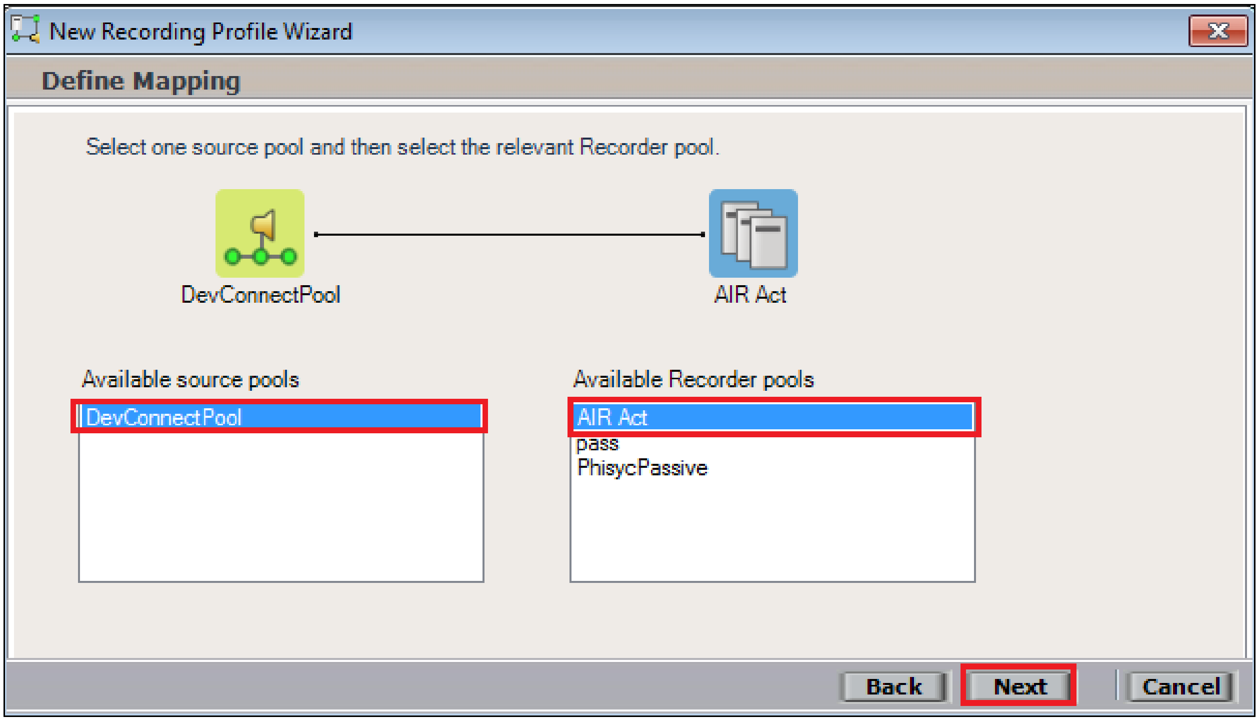
New Recording Profile Wizard

Define the Recording Profile Name

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

Name: DevConnectRecording

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



New Recording Profile Wizard

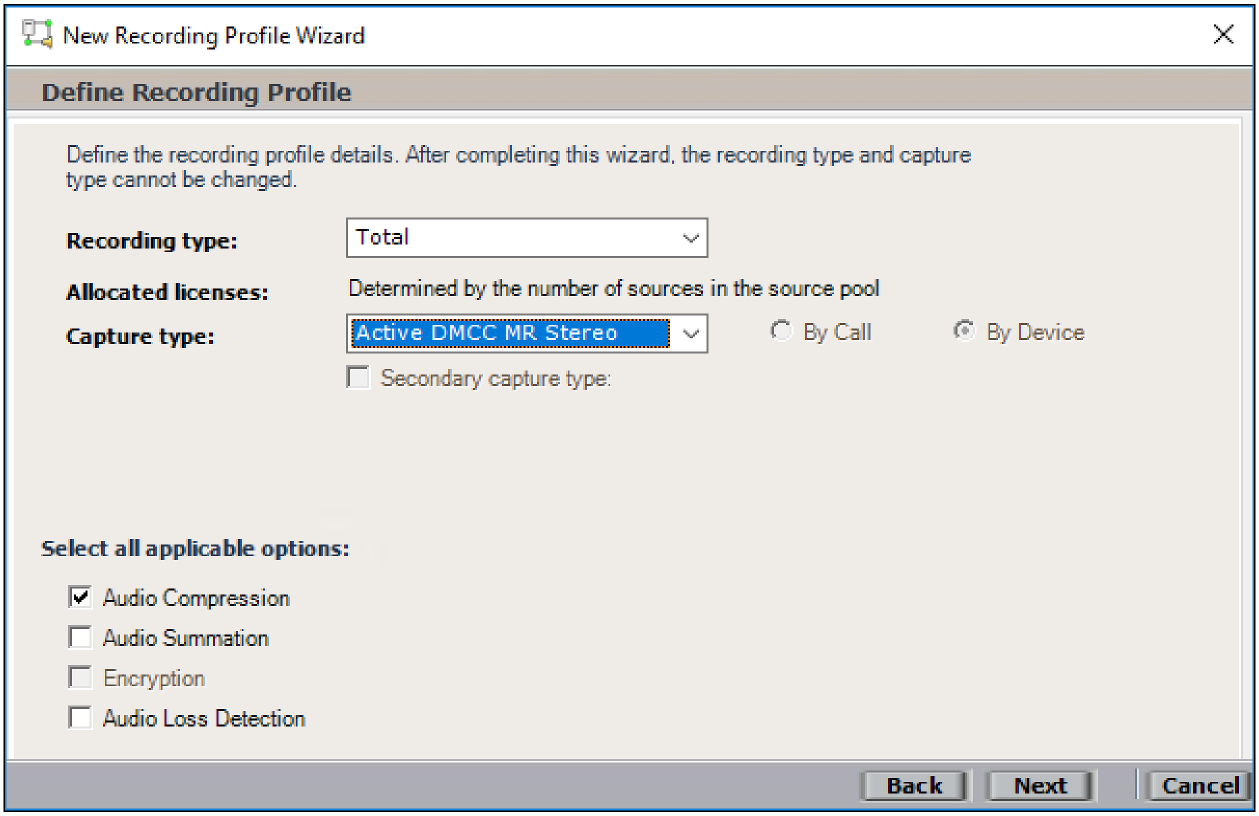
Define Mapping

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

Available source pools: DevConnectPool

Available Recorder pools: AIR Act, pass, PhisycPassive

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



New Recording Profile Wizard

Define Recording Profile

Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.

Recording type: Total

Allocated licenses: Determined by the number of sources in the source pool

Capture type: Active DMCC MR Stereo ○ By Call ● By Device

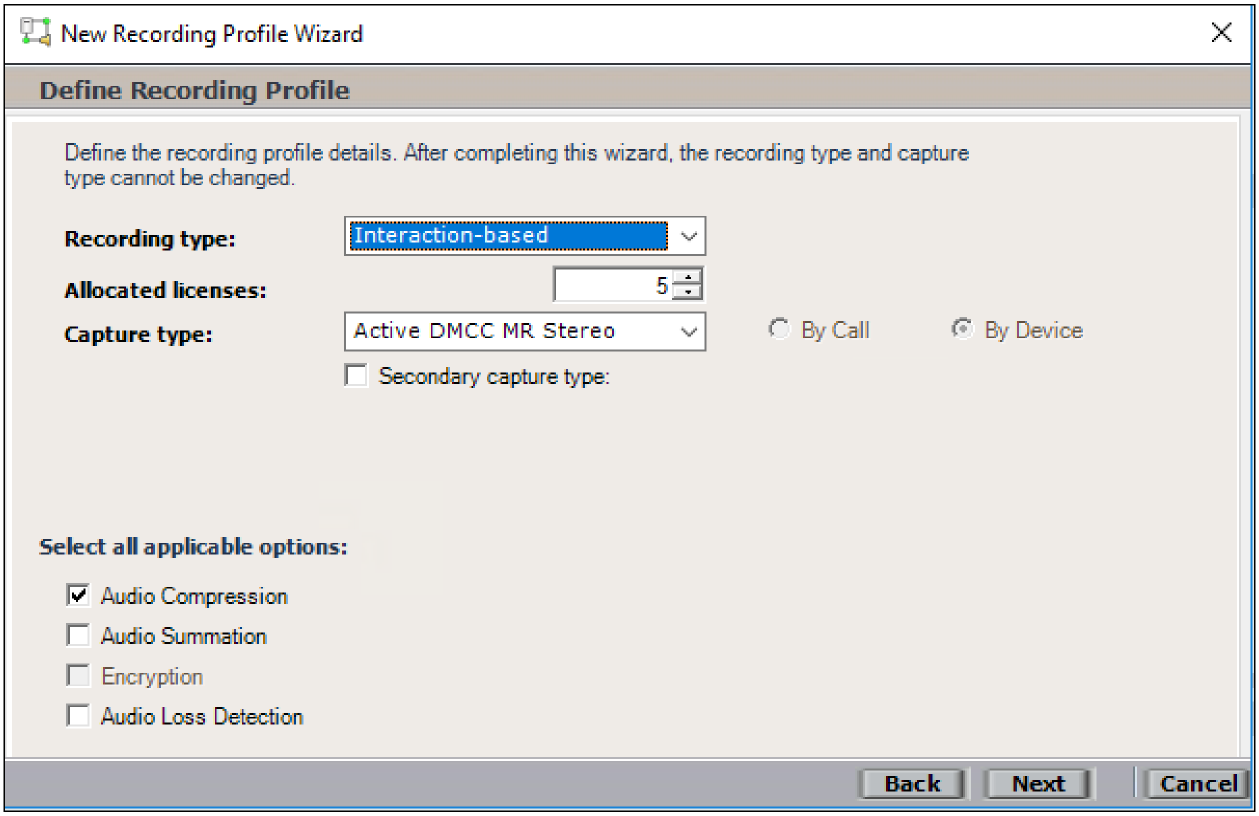
□ Secondary capture type:

Select all applicable options:

☑ Audio Compression
□ Audio Summation
□ Encryption
□ Audio Loss Detection

Note: Avaya would recommend that **Total** "recording type" is used as it is not recommended to have recorders registering and unregistering to cope with an "interaction-based" type of recording.

Interaction-based recording can be configured by selecting **Interaction-based** as the **Recording type** and **Active DMCC MR Stereo** as the **Capture type** and **By Device** is selected beside it. **Audio Compression** is selected as default and can be left like this. Click on **Next** to continue.



Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.

Recording type: Interaction-based

Allocated licenses: 5

Capture type: Active DMCC MR Stereo ○ By Call ● By Device

□ Secondary capture type:

Select all applicable options:

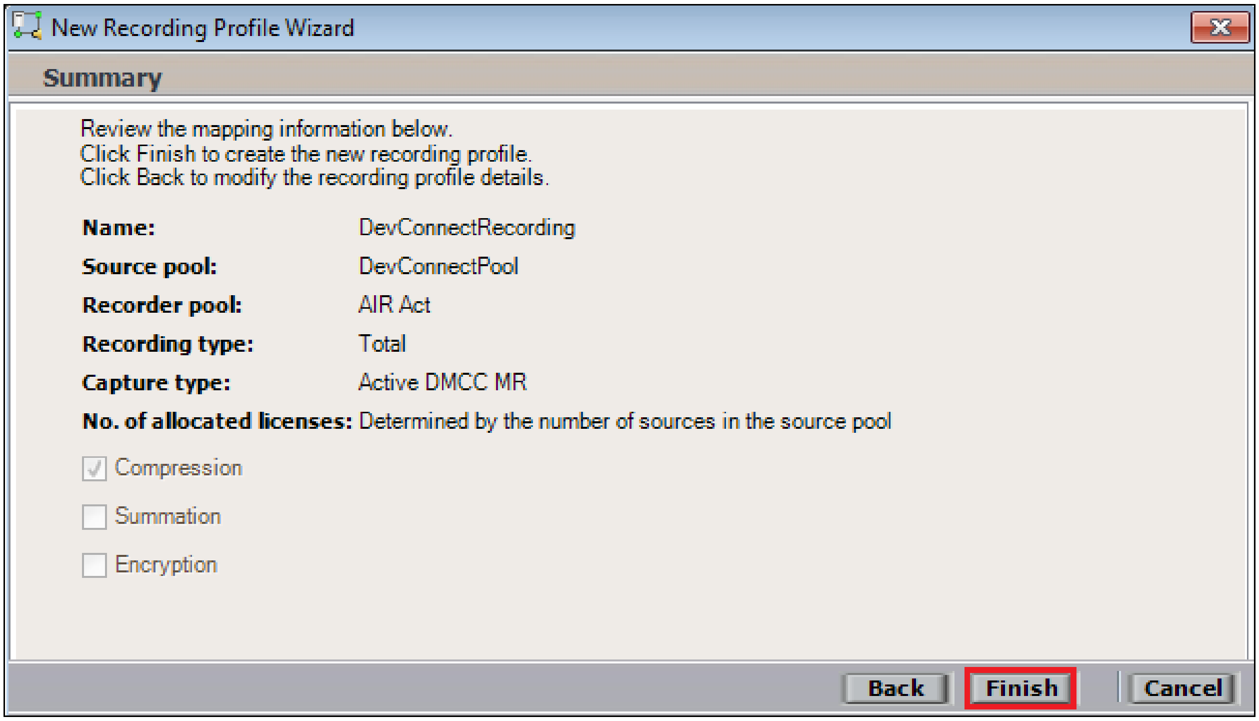
☑ Audio Compression

□ Audio Summation

□ Encryption

□ Audio Loss Detection

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



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

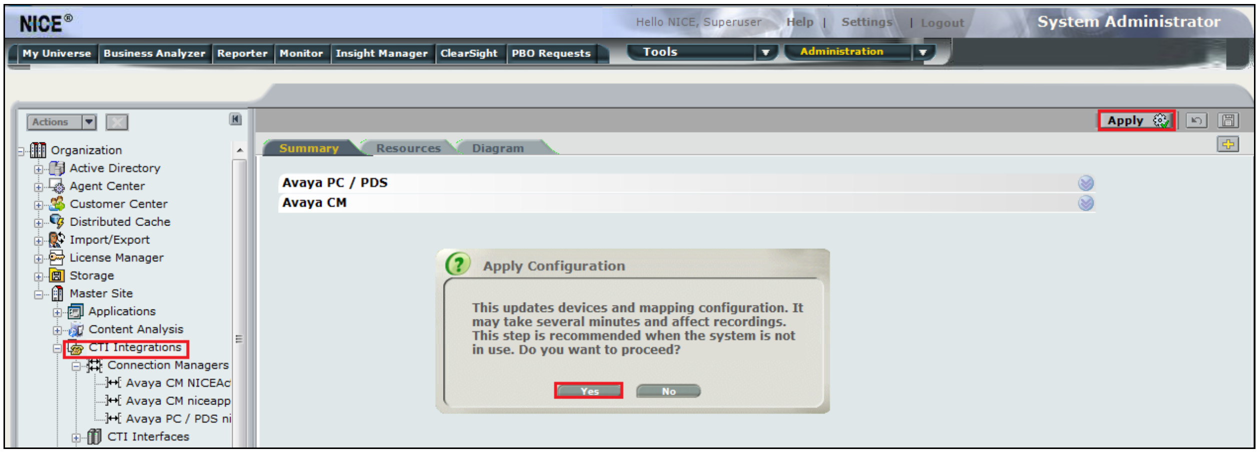
Name:	DevConnectRecording
Source pool:	DevConnectPool
Recorder pool:	AIR Act
Recording type:	Total
Capture type:	Active DMCC MR
No. of allocated licenses:	Determined by the number of sources in the source pool

☑ Compression

□ Summation

□ Encryption

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



This updates devices and mapping configuration. It may take several minutes and affect recordings. This step is recommended when the system is not in use. Do you want to proceed?

This concludes the setup of the NICE Application Server for DMCC Multiple Registration recording.

8. Verification Steps

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

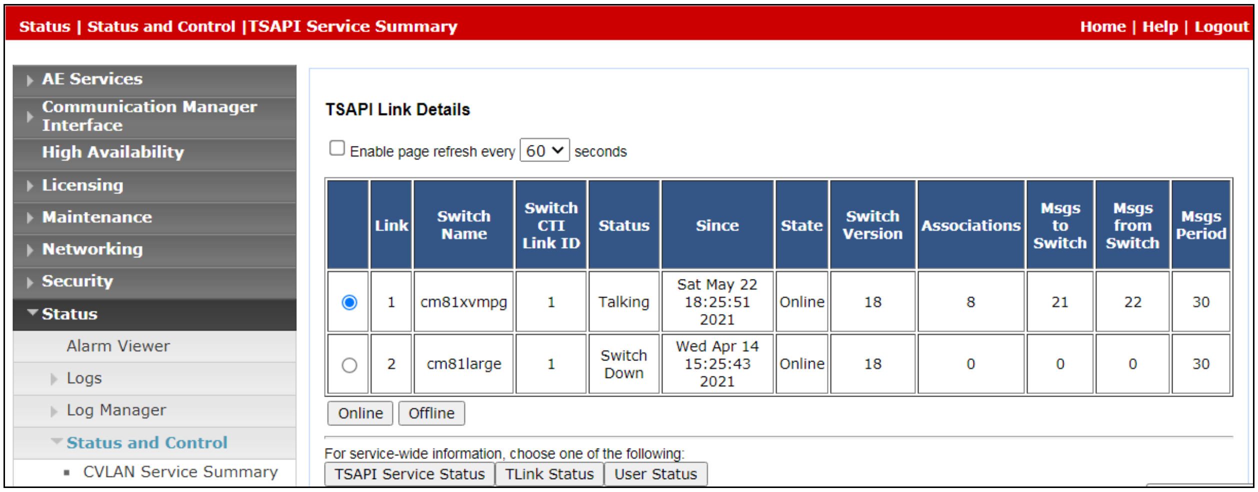
8.1. Verify Avaya Aura® Communication Manager CTI Service State

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        11        no      aes81vmpg      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**.



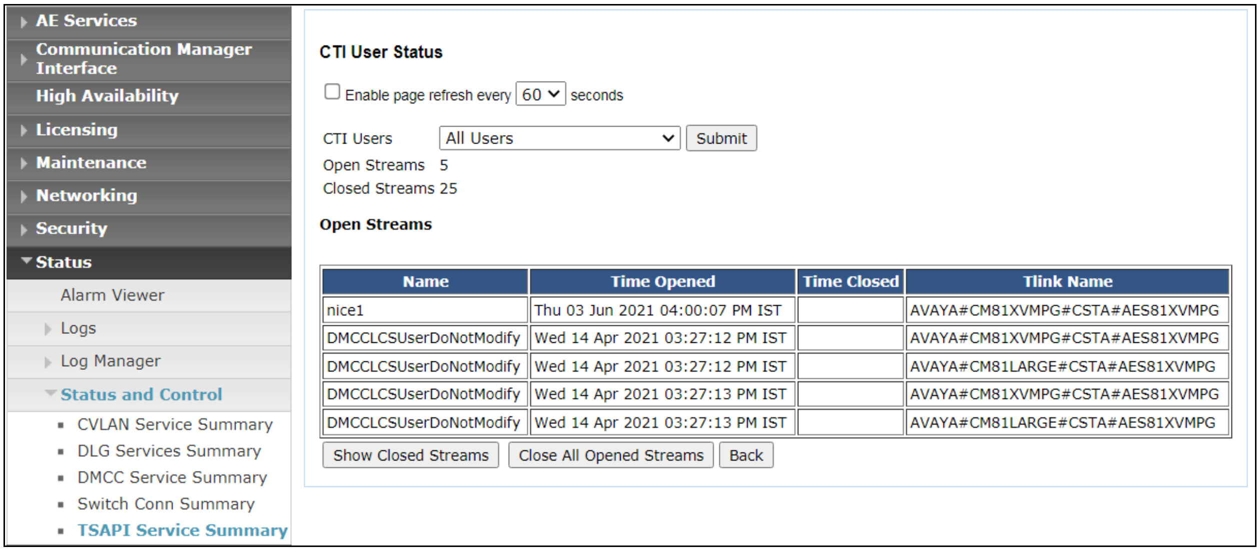
TSAPI Link Details

□ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm81xvmpg	1	Talking	Sat May 22 18:25:51 2021	Online	18	8	21	22	30
○	2	cm81large	1	Switch Down	Wed Apr 14 15:25:43 2021	Online	18	0	0	0	30

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

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.



CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users: All Users — Submit

Open Streams 5

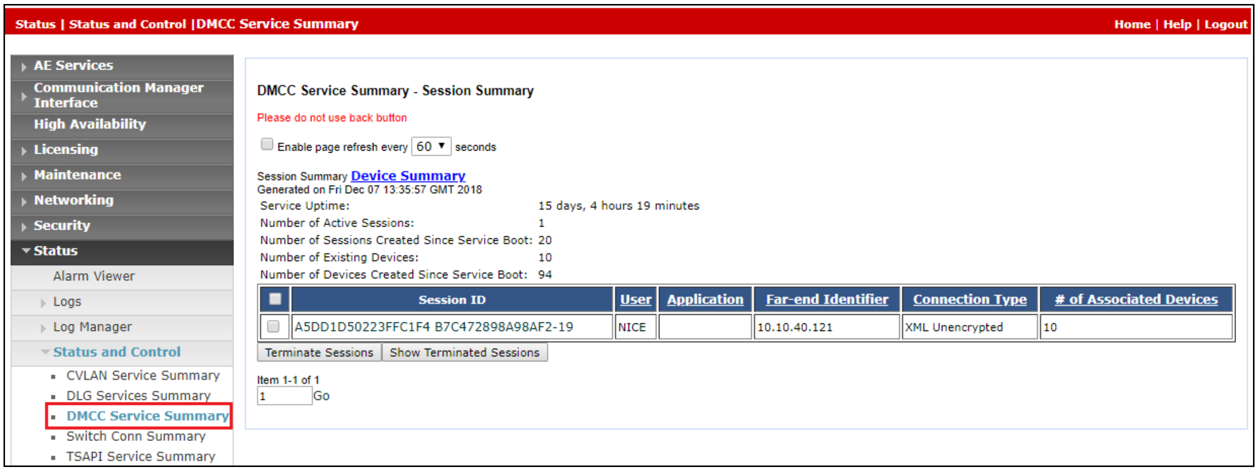
Closed Streams 25

Open Streams

Name	Time Opened	Time Closed	Tlink Name
nice1	Thu 03 Jun 2021 04:00:07 PM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:12 PM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:12 PM IST		AVAYA#CM81LARGE#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:13 PM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:13 PM IST		AVAYA#CM81LARGE#CSTA#AES81XVMPG

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 **10.10.40.121**, which is the NICE Application server.



DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Fri Dec 07 13:35:57 GMT 2018

Service Uptime:	15 days, 4 hours 19 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	20
Number of Existing Devices:	10
Number of Devices Created Since Service Boot:	94

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	A5DD1D50223FFC1F4 B7C472898A98AF2-19	NICE		10.10.40.121	XML Unencrypted	10

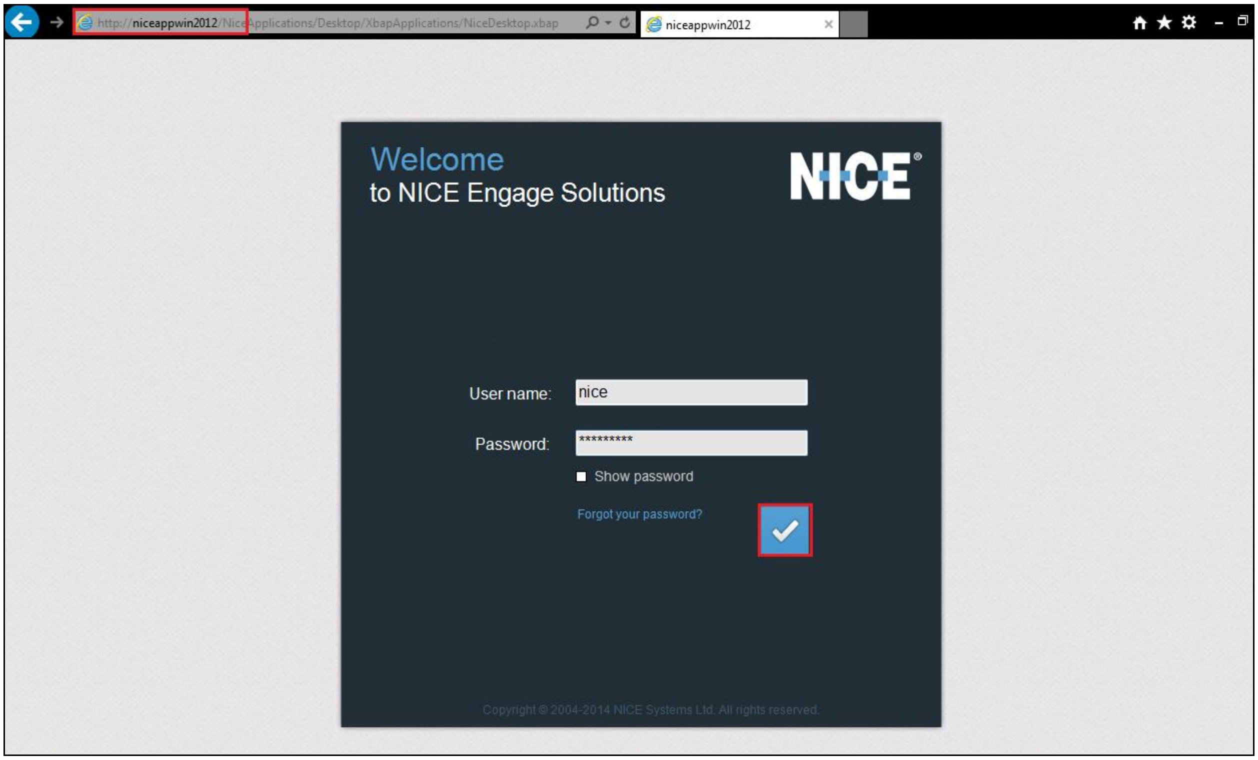
Item 1-1 of 1

1 Go

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**.



http://niceappwin2012/NiceApplications/Desktop/XbapApplications/NiceDesktop.xbap

niceappwin2012

Welcome
to NICE Engage Solutions

User name: nice

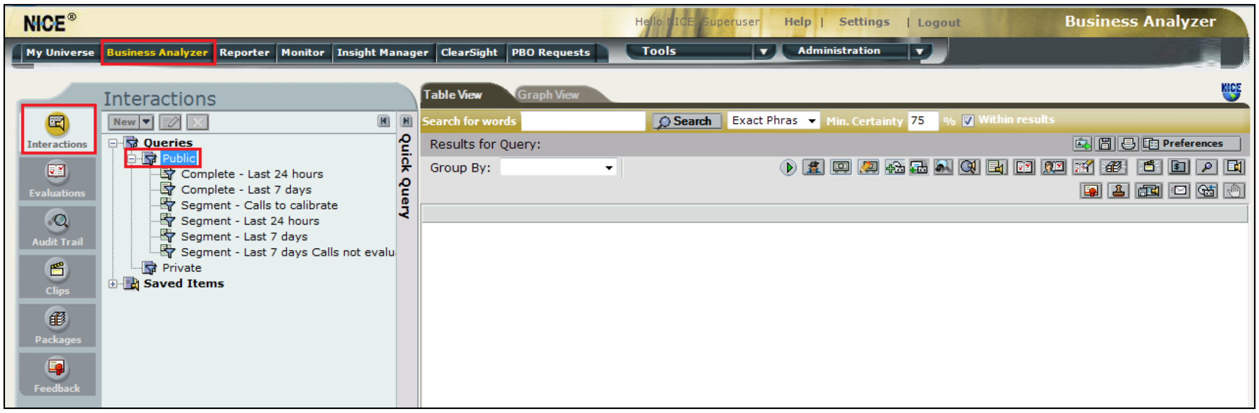
Password: *********

□ Show password

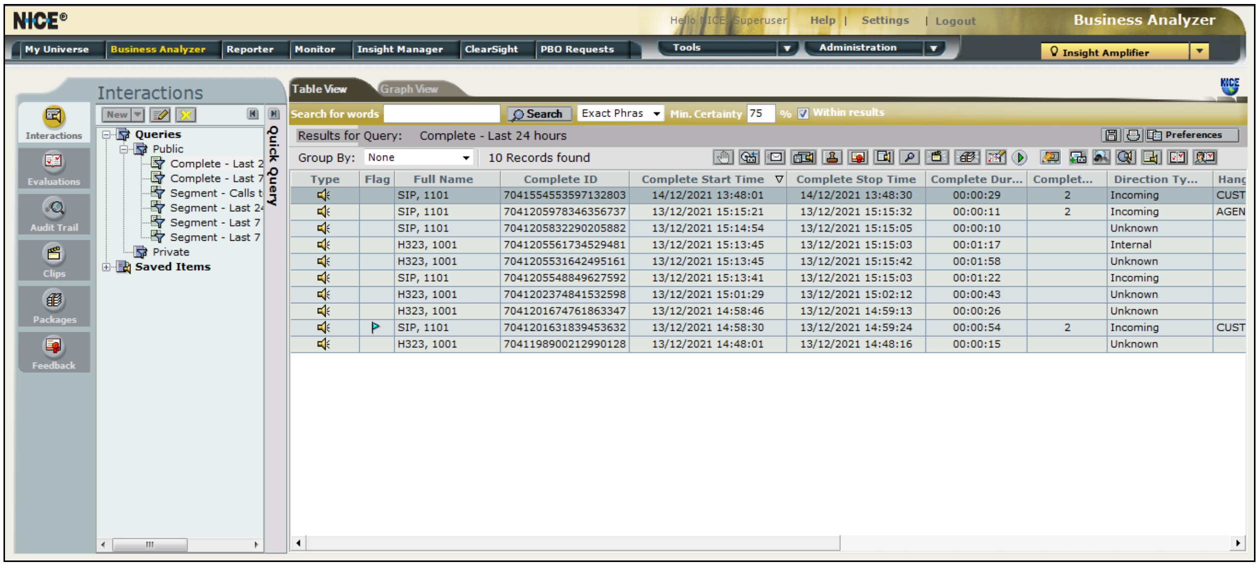
Forgot your password?

Copyright © 2004-2014 NICE Systems Ltd. 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.



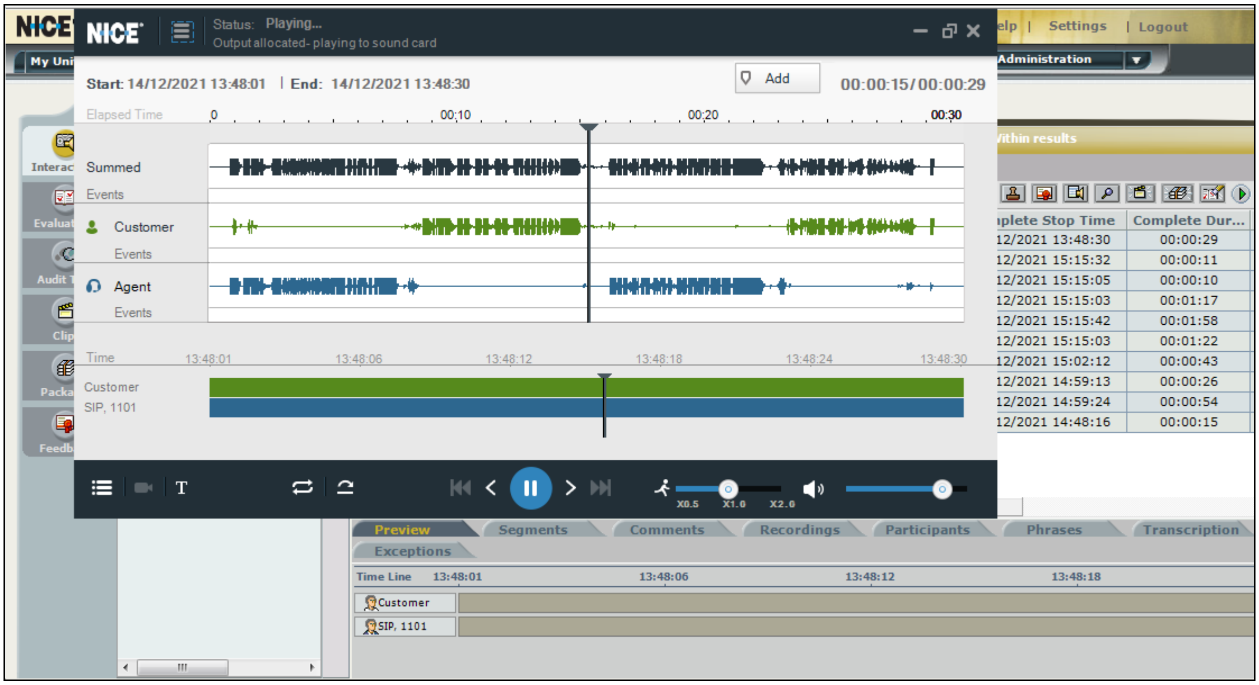
Results for Query: Complete - Last 24 hours

Group By: None 10 Records found

Type	Flag	Full Name	Complete ID	Complete Start Time	Complete Stop Time	Complete Dur...	Complet...	Direction Ty...	Hang
🔈		SIP, 1101	7041554553597132803	14/12/2021 13:48:01	14/12/2021 13:48:30	00:00:29	2	Incoming	CUST
🔈		SIP, 1101	7041205978346356737	13/12/2021 15:15:21	13/12/2021 15:15:32	00:00:11	2	Incoming	AGEN
🔈		SIP, 1101	7041205832290205882	13/12/2021 15:14:54	13/12/2021 15:15:05	00:00:10		Unknown	
🔈		H323, 1001	7041205561734529481	13/12/2021 15:13:45	13/12/2021 15:15:03	00:01:17		Internal	
🔈		H323, 1001	7041205531642495161	13/12/2021 15:13:45	13/12/2021 15:15:42	00:01:58		Unknown	
🔈		SIP, 1101	7041205548849627592	13/12/2021 15:13:41	13/12/2021 15:15:03	00:01:22		Incoming	
🔈		H323, 1001	7041202374841532598	13/12/2021 15:01:29	13/12/2021 15:02:12	00:00:43		Unknown	
🔈		H323, 1001	7041201674761863347	13/12/2021 14:58:46	13/12/2021 14:59:13	00:00:26		Unknown	
🔈	⚑	SIP, 1101	7041201631839453632	13/12/2021 14:58:30	13/12/2021 14:59:24	00:00:54	2	Incoming	CUST
🔈		H323, 1001	7041198900212990128	13/12/2021 14:48:01	13/12/2021 14:48:16	00:00:15		Unknown	

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.

Note: The recording below shows two separate streams in stereo, with the **Customer** on one side and the **Agent** on the other.


Status: Playing...
Output allocated- playing to sound card

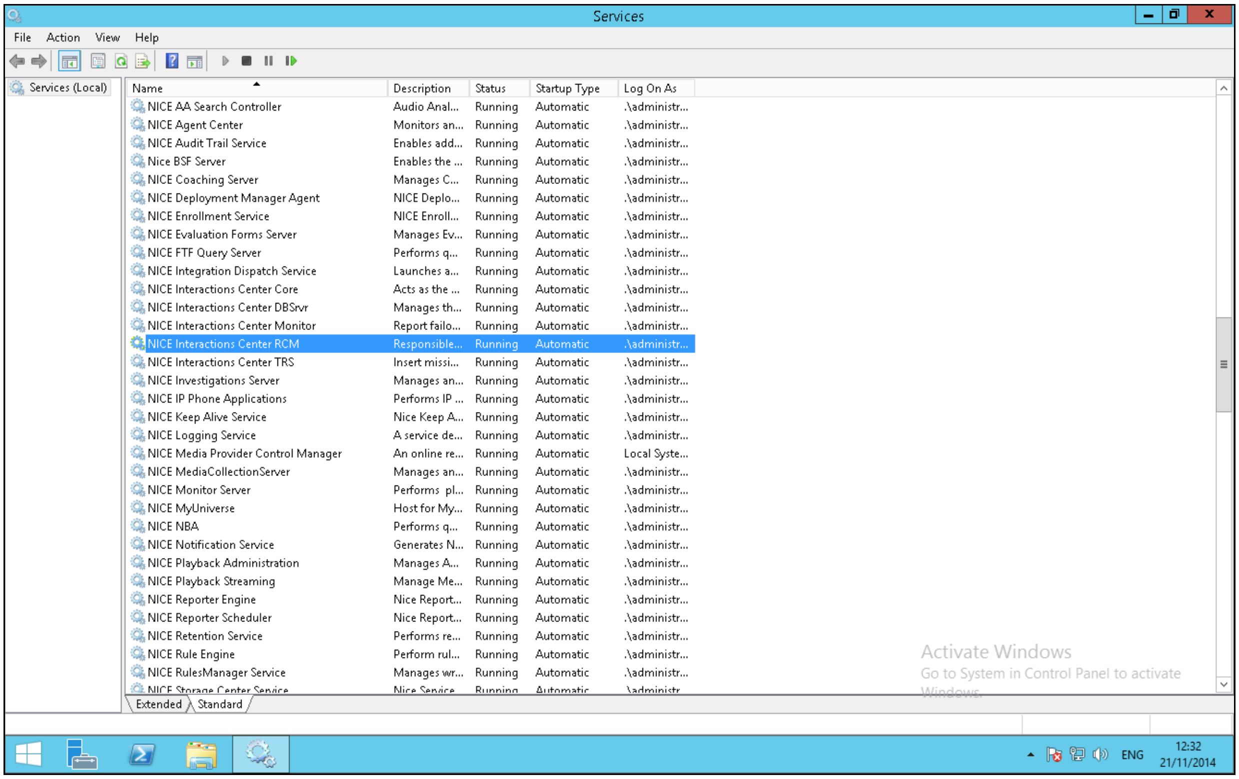
Start: 14/12/2021 13:48:01 | End: 14/12/2021 13:48:30

00:00:15/00:00:29

plete Stop Time	Complete Dur...
12/2021 13:48:30	00:00:29
12/2021 15:15:32	00:00:11
12/2021 15:15:05	00:00:10
12/2021 15:15:03	00:01:17
12/2021 15:15:42	00:01:58
12/2021 15:15:03	00:01:22
12/2021 15:02:12	00:00:43
12/2021 14:59:13	00:00:26
12/2021 14:59:24	00:00:54
12/2021 14:48:16	00:00:15

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 Recorder 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.



Name	Description	Status	Startup Type	Log On As
NICE AA Search Controller	Audio Anal...	Running	Automatic	.\administr...
NICE Agent Center	Monitors an...	Running	Automatic	.\administr...
NICE Audit Trail Service	Enables add...	Running	Automatic	.\administr...
Nice BSF Server	Enables the ...	Running	Automatic	.\administr...
NICE Coaching Server	Manages C...	Running	Automatic	.\administr...
NICE Deployment Manager Agent	NICE Deplo...	Running	Automatic	.\administr...
NICE Enrollment Service	NICE Enroll...	Running	Automatic	.\administr...
NICE Evaluation Forms Server	Manages Ev...	Running	Automatic	.\administr...
NICE FTF Query Server	Performs q...	Running	Automatic	.\administr...
NICE Integration Dispatch Service	Launches a...	Running	Automatic	.\administr...
NICE Interactions Center Core	Acts as the ...	Running	Automatic	.\administr...
NICE Interactions Center DBSrvr	Manages th...	Running	Automatic	.\administr...
NICE Interactions Center Monitor	Report failo...	Running	Automatic	.\administr...
NICE Interactions Center RCM	Responsible...	Running	Automatic	.\administr...
NICE Interactions Center TRS	Insert missi...	Running	Automatic	.\administr...
NICE Investigations Server	Manages an...	Running	Automatic	.\administr...
NICE IP Phone Applications	Performs IP ...	Running	Automatic	.\administr...
NICE Keep Alive Service	Nice Keep A...	Running	Automatic	.\administr...
NICE Logging Service	A service de...	Running	Automatic	.\administr...
NICE Media Provider Control Manager	An online re...	Running	Automatic	Local Syste...
NICE MediaCollectionServer	Manages an...	Running	Automatic	.\administr...
NICE Monitor Server	Performs pl...	Running	Automatic	.\administr...
NICE MyUniverse	Host for My...	Running	Automatic	.\administr...
NICE NBA	Performs q...	Running	Automatic	.\administr...
NICE Notification Service	Generates N...	Running	Automatic	.\administr...
NICE Playback Administration	Manages A...	Running	Automatic	.\administr...
NICE Playback Streaming	Manage Me...	Running	Automatic	.\administr...
NICE Reporter Engine	Nice Report...	Running	Automatic	.\administr...
NICE Reporter Scheduler	Nice Report...	Running	Automatic	.\administr...
NICE Retention Service	Performs re...	Running	Automatic	.\administr...
NICE Rule Engine	Perform rul...	Running	Automatic	.\administr...
NICE RulesManager Service	Manages wr...	Running	Automatic	.\administr...
NICE Storage Center Service	Nice Service...	Running	Automatic	.\administr...

9. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform R7.1 to successfully interoperate with Avaya Aura® Communication Manager R8.1 using Avaya Aura® Application Enablement Services R8.1 to connect to using DMCC Multiple Registration to record calls in stereo. All feature functionality and serviceability test cases were completed successfully with 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 8.1

[4] *Avaya Aura® Session Manager Overview and Specifications*

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

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.