



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring NICE Engage Platform R6.5 to interoperate with Avaya Session Border Controller for Enterprise R7.1 and Avaya Aura® Communication Manager R7.0 using SIP 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 Session Border Controller, an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0.

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

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

# 1. Introduction

These Application Notes describe the configuration steps for the NICE Engage Platform R6.5 to interoperate with the Avaya solution consisting of an Avaya Session Border Controller for Enterprise R7.1, an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0. NICE Engage Platform uses SIP Recording and the Telephony Services API (TSAPI) to capture the audio and call details for call recording on various Communication Manager endpoints, listed in **Section 4**.

The NICE Engage Platform is fully integrated into a LAN (Local Area Network), and includes easy-to-use Web based applications (i.e. Nice Application) that works with .NET framework and can be used to retrieve telephone conversations from a comprehensive long-term calls database. The NICE Engage Platform uses SIP recording to record SIP trunk calls that pass through the Avaya Session Border Controller for Enterprise.

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

**Note:** These Application Notes focus on the setup of the Avaya Session Border Controller for Enterprise and the Avaya Aura® Application Enablement Services to allow for NICE SIP Call Recording to interoperate correctly. The initial configuration of the Avaya Session Border Controller for Enterprise is not the primary focus of these Application Notes and although this setup is outlined in **Section 12 (Appendix A)** for information on the installation and setup of the Avaya Session Border Controller for Enterprise please refer to **Section 11** of these Application Notes.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the NICE Engage Platform to carry out call recording of SIP trunk calls coming through the SBC using SIP trunk recording. A simulated enterprise site was configured using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to connect to a SIP trunking service to facilitate SIP trunk calls being made and received from the Communication Manager endpoints all of which are listed in **Section 4**.

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

## 2.1. Interoperability Compliance Testing

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

- **Inbound/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from SIP 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 one-X® Agent.
- **Serviceability testing** – The behavior of NICE Engage Platform under different simulated failure conditions.

## 2.2. Test Results

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

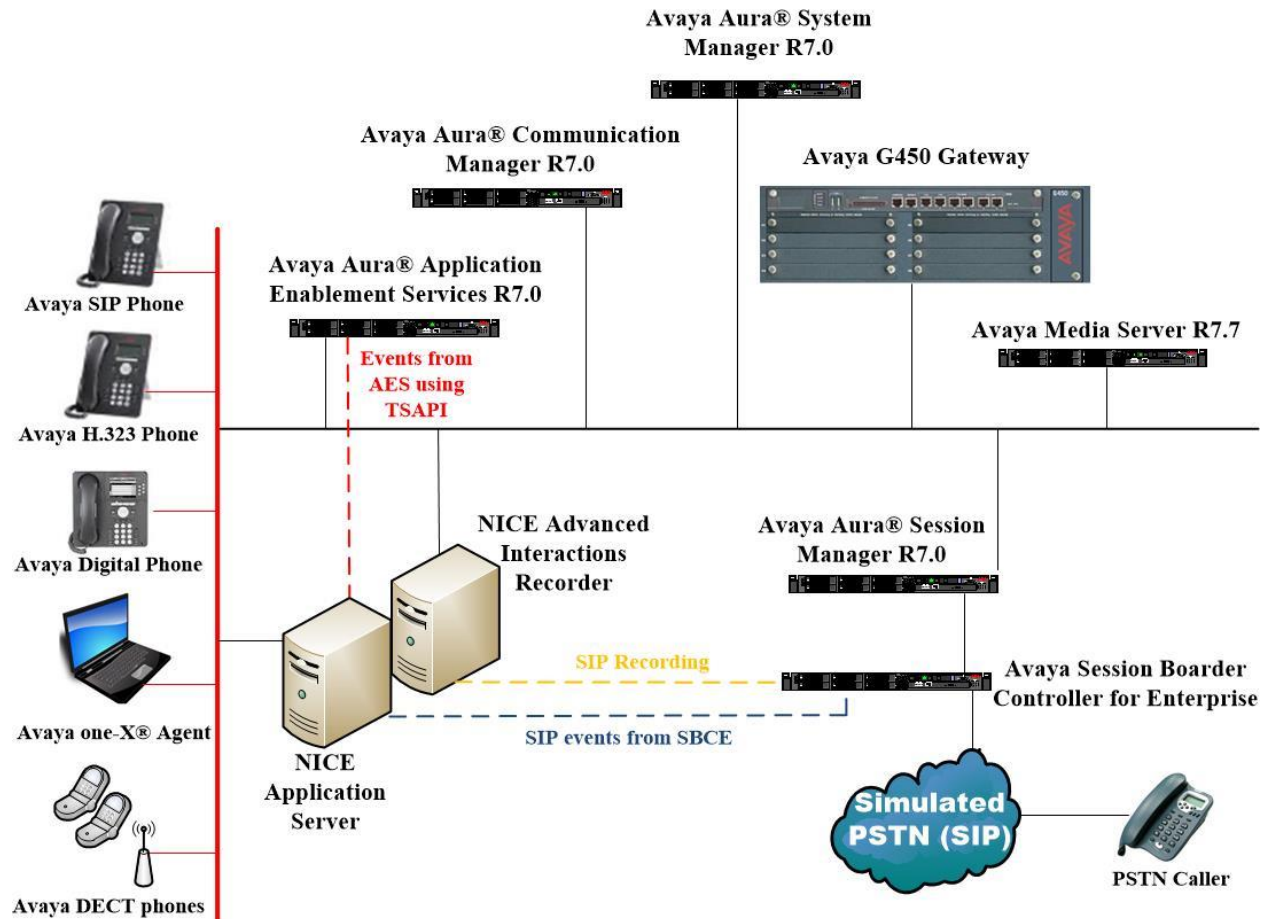
1. Conference Call with SIP trunk caller, the conference bit of the call is missing.  
Call Scenario: Communication Manager extension A calls Communication Manager extension B and Communication Manager extension B conferences in a SIP trunk user. Communication Manager extension A drops off the call first.  
Leg 3 or the conference portion of the call where all three are in conference is missing. This portion of the call is actually recorded and is inserted by TRS after the call is completed (by default after 4 hours) but it is not available immediately after the call.
2. Conference Call with SIP trunk caller, the last leg of the conference call is missing.  
Call Scenario: SIP Trunk user A calls into Communication Manager extension and Communication Manager extension A conferences in a SIP trunk user B. SIP Trunk user B drops off the call first.  
Leg 4 of the call is missing between SIP Trunk user A and Communication Manager extension A after SIP Trunk user B hangs up the call. This portion of the call is actually recorded and is inserted by TRS after the call is completed (by default after 4 hours) but it is not available immediately after the call.

## 2.3. Support

Technical support can be obtained for NICE Engage Platform from the website <http://www.nice.com/engage/services/support>

### 3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Engage Platform with the Avaya solution using SIP Call Recording to record calls. The NICE Application Server is setup to receive events from both the AES and SBC. SIP trunk calls that pass through the SBC are recorded using SIP recording.



**Figure 1: Connection of NICE Engage Platform R6.5 with Avaya Session Border Controller for Enterprise R7.1, Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager R7.0 and Avaya Aura® Application Enablement Services R7.0**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.1 Build No. – 7.0.0.0.16266 Software Update Revision No: 7.0.1.1.065378 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP1 Build No. – 7.0.1.1.701114
Avaya Aura® Communication Manager running on a virtual server	R7.0 R017x.00.0.441.0 00.0.441.0-23169
Avaya Aura® Application Enablement Services running on Virtual Server	R7.0 Build No – 7.0.1.0.3.15-0
Avaya Session Boarder Controller For Enterprise running on a virtual server	7.1.0.1-07-12090
Avaya G450 Gateway	37.19.0 /1
Avaya Media Server running on a virtual server	Media Server System R7.7.0.8 Media Server R7.7.0.200
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 7.0.0.39
Avaya Communicator for Windows	R2.1.3.80
Avaya one-X® Agent	R 2.5.50022.0
Avaya 9408 Digital Deskphone	FW Version 2
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
NICE Engage Platform <ul style="list-style-type: none"><li>- Application Server</li><li>- Advanced Interactions Recorder</li></ul>	R6.5

## 5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**.

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

### 5.1. Verify System Features

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

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	y		
Attendant Vectoring?	y		

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

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

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM70vmpg	10.10.40.12		
<b>aes70vmpg</b>	<b>10.10.40.26</b>		
default	0.0.0.0		
g450	10.10.40.15		
<b>procr</b>	<b>10.10.40.13</b>		

### 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 Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	y	procr	8765			

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

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

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

change ip-services				Page	4 of 4
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	aes70vmpg	*****	y	idle	
2:					
3:					

### 5.4. Configure CTI Link for TSAPI Service

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

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

## 5.5. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used.

```
change ip-network-region 1                                     Page 1 of 20
                                     IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: devconnect.local
    Name: default NR
MEDIA PARAMETERS                                           Intra-region IP-IP Direct Audio: yes
    Codec Set: 1                                           Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048                                     IP Audio Hairpinning? y
    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5
```

```
change ip-network-region 1                                     Page 2 of 20
                                     IP NETWORK REGION

RTCP Reporting to Monitor Server Enabled? y

RTCP MONITOR SERVER PARAMETERS
    Use Default Server Parameters? y
```



## IP NETWORK REGION

## INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY

Incoming LDN Extension:

Conversion To Full Public Number - Delete: Insert:

Maximum Number of Trunks to Use for IGAR:

Dial Plan Transparency in Survivable Mode? n

## BACKUP SERVERS (IN PRIORITY ORDER) H.323 SECURITY PROFILES

1 1 challenge

2 2

3 3

4 4

5

6 Allow SIP URI Conversion? y

## TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS

Near End Establishes TCP Signaling Socket? y

Near End TCP Port Min: 61440

Near End TCP Port Max: 61444

Source Region: 1 Inter Network Region Connection Management I M

dst codec direct WAN-BW-limits Video Intervening Dyn A G t

rgn set WAN Units Total Norm Prio Shr Regions CAC R L e

1 1 all

2

3

4

5

6

7

8

9

10

11

12

13

14

15

## 5.6. Configure Communication Manager SIP Trunk

The following shows the SIP Signaling Group and SIP trunk that was used during compliance testing. Use the command, **add signaling-group x**, where x is the signaling group number.

- Set the **Group Type** field to **sip**.
- For compliance testing **Transport Method** was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively.
- Set the **Near-end Node Name** to **procr**. Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm70vmpg**), as per **Section 5.2**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.5**. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was left blank so as any domain that tries to call Communication Manager is accepted.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** was set to **N** for compliance testing.
- The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2	
SIGNALING GROUP			
Group Number: 1		Group Type: sip	
IMS Enabled? n		Transport Method: tls	
Q-SIP? n			
IP Video? n		Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y		Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y			
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n			
Alert Incoming SIP Crisis Calls? n			
Near-end Node Name: procr		Far-end Node Name: sm70vmpg	
Near-end Listen Port: 5061		Far-end Listen Port: 5061	
Far-end Network Region: 1			
Far-end Domain:			
		Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3		IP Audio Hairpinning? n	
Enable Layer 3 Test? y		Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6	

Configure the Trunk Group form as shown below. This trunk group is used for calls to and from Communications Portal. Enter a descriptive name in the Group Name field. Set the Group Type field to sip. Enter a TAC code compatible with the Communication Manager dial plan. Set the Service Type field to tie. Specify the signaling group associated with this trunk group in the Signaling Group field, and specify the Number of Members supported by this SIP trunk group. Accept the default values for the remaining fields.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: r	
Group Name: SIPTRK	COR: 1	TN: 1	TAC: *801
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 10	

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with NEC to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 600			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n			

Settings on **Page 3** can be left as default. However the **Numbering Format** in the example below is set to **private**.

add trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private	
	UUI Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
	Hold/Unhold Notifications? y	
	Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y		

Settings on **Page 4** are as follows.

add trunk-group 1		Page 4 of 21
PROTOCOL VARIATIONS		
	Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n		
	Send Transferring Party Information? y	
	Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n		
	Send Diversion Header? n	
	Support Request History? y	
	Telephone Event Payload Type: 120	
	Convert 180 to 183 for Early Media? n	
	Always Use re-INVITE for Display Updates? n	
	Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n		
	Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active		
	Request URI Contents: may-have-extra-digits	

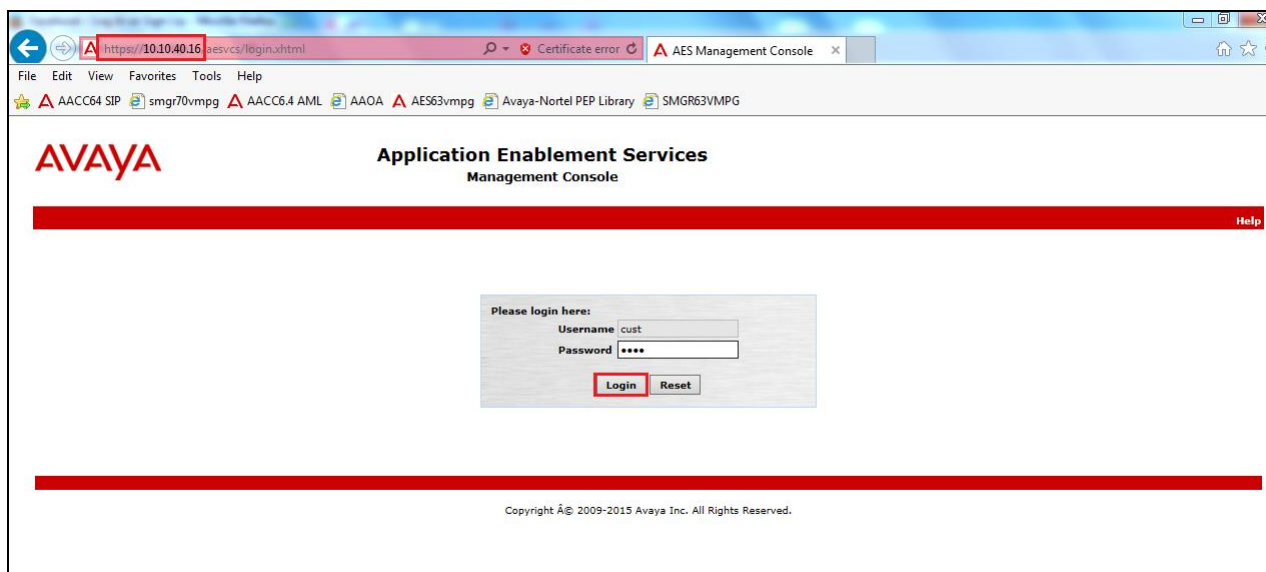
## 6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Associate Devices with CTI User

### 6.1. Verify Licensing

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



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

**AVAYA** Application Enablement Services Management Console

Welcome: User cust  
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222  
Number of prior failed login attempts: 1  
HostName/IP: aes70vmppg  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.0.0.0.13-0  
Server Date and Time: Tue Nov 24 16:15:51 GMT 2015  
HA Status: Not Configured

**AE Services** Home | Help | Logout

▼ AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI
- TWS
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

**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	N/A	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 7.x:

## 6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

**AVAYA** Application Enablement Services Management Console

Welcome: User cust  
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222  
Number of prior failed login attempts: 1  
HostName/IP: aes70vmppg  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.0.0.0.13-0  
Server Date and Time: Tue Nov 24 16:16:56 GMT 2015  
HA Status: Not Configured

**Communication Manager Interface | Switch Connections** Home | Help | Logout

▼ AE Services

- Communication Manager Interface
- Switch Connections
- Dial Plan
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

**Switch Connections**

cm70vmppg x **Add Connection**

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

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

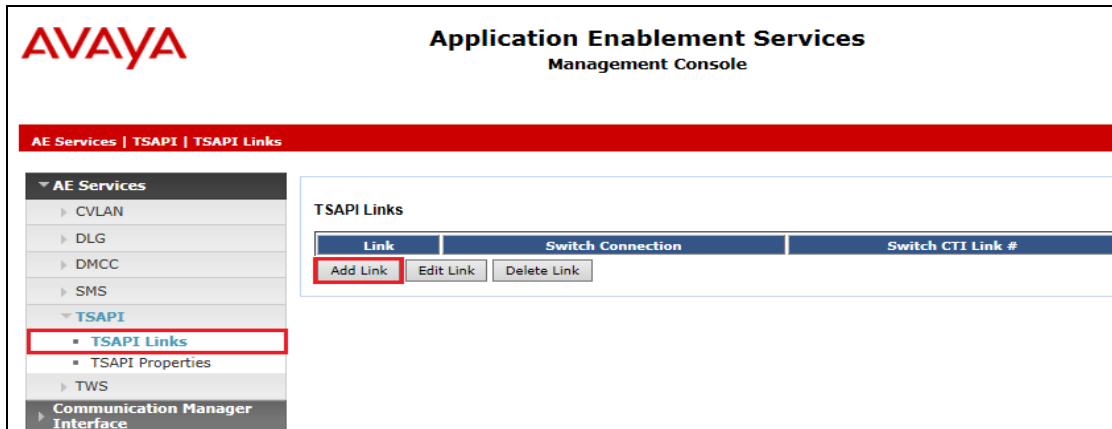
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface (selected), Switch Connections (highlighted with a red box), Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Connection Details - cm70vmppg' and contains the following fields: Switch Password (password field), Confirm Switch Password (password field), Msg Period (30 Minutes (1 - 72)), Provide AE Services certificate to switch (checkbox), Secure H323 Connection (checkbox), and Processor Ethernet (checked checkbox). The 'Apply' button is highlighted with a red box.

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.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface (selected), Switch Connections (highlighted with a red box), Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Edit Processor Ethernet IP - cm70vmppg' and contains the following fields: 10.10.40.13 (text field), Add/Edit Name or IP (button, highlighted with a red box), Name or IP Address (table header), 10.10.40.13 (table row), and Back (button).

### 6.3. Administer TSAPI link

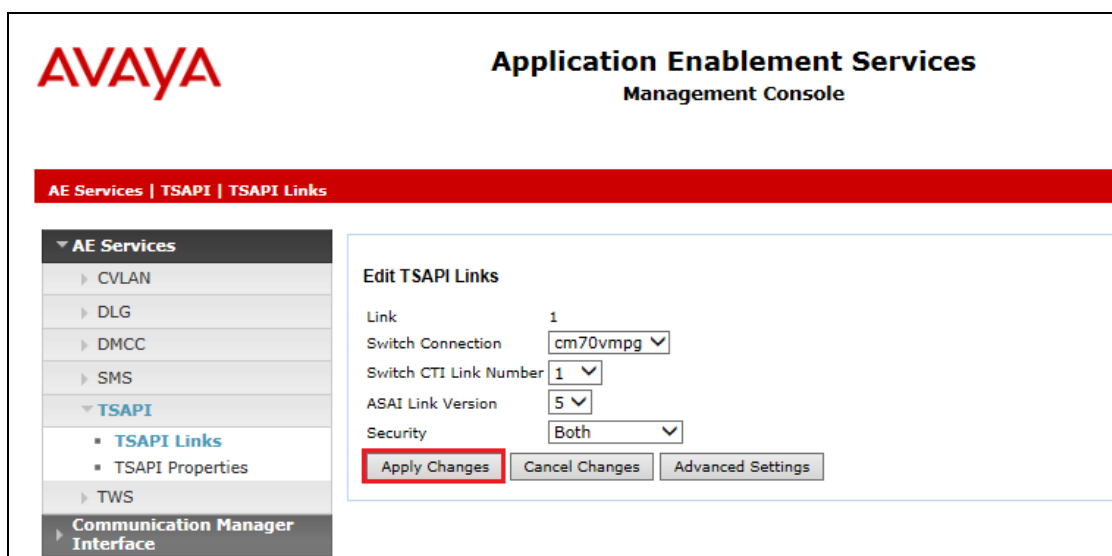
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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

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

Once completed, select **Apply Changes**.





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

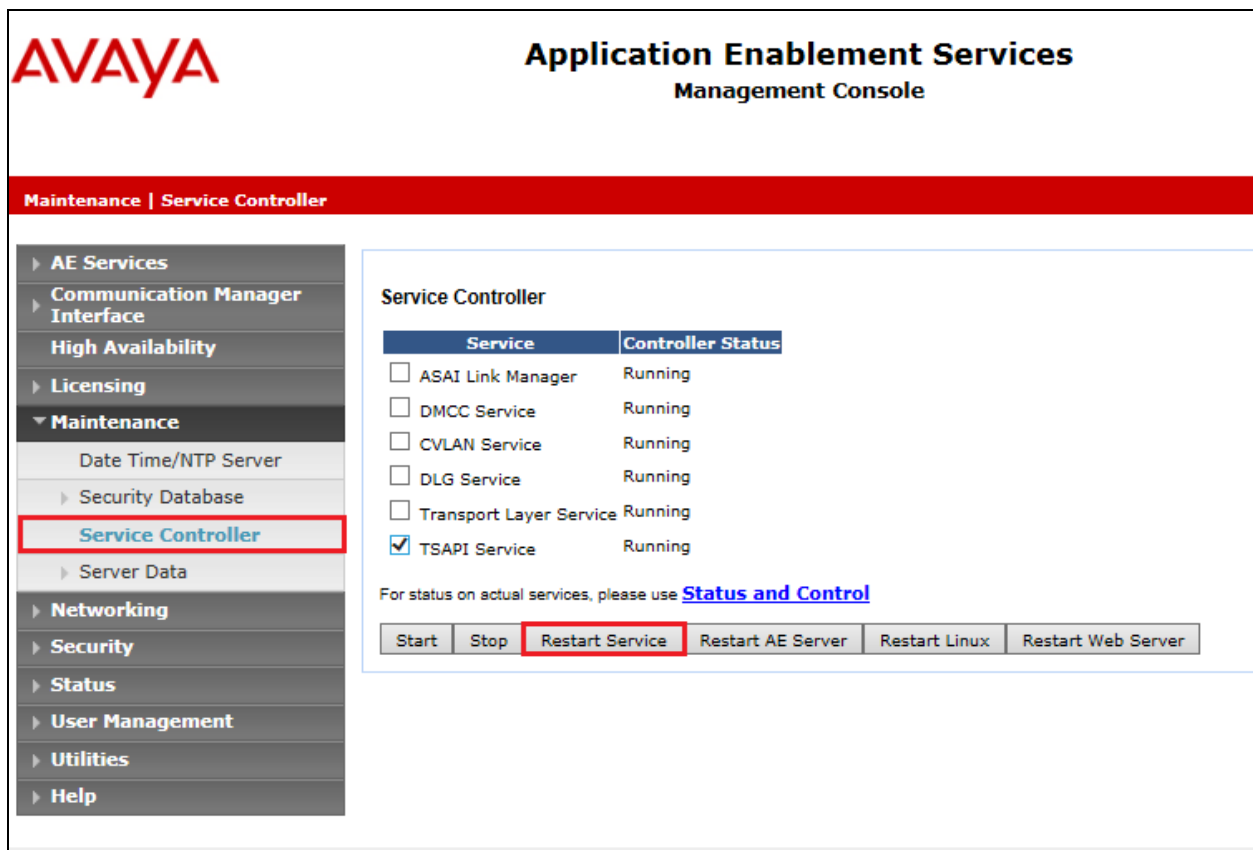
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), 'TSAPI Links', 'TSAPI Properties', 'TWS', and 'Communication Manager Interface'. The main content area displays a confirmation dialog titled 'Apply Changes to Link'. The dialog contains a warning message: 'Warning! Are you sure you want to apply the changes? These changes can only take effect when the TSAPI server restarts.' Below the warning is a yellow triangle icon and the text: 'Please use the Maintenance -> Service Controller page to restart the TSAPI server.' At the bottom of the dialog are two buttons: 'Apply' (highlighted with a red box) and 'Cancel'.

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

The screenshot shows the Avaya Application Enablement Services Management Console after the TSAPI link configuration. The left sidebar is the same as the previous screenshot, but 'TSAPI Links' is now selected. The main content area displays a table titled 'TSAPI Links'. The table has five columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. There is one row in the table with the following values: '1', 'cm70vmpg', '1', '5', and 'Both'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'. In the top right corner, there is a status bar with the following information: 'Welcome! User: cust', 'Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222', 'Number of prior failed login attempts: 1', 'HostName/IP: aes70vmpg', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.0.0.0.13-0', 'Server Date and Time: Tue Nov 24 16:26:08 GMT 2015', and 'HA Status: Not Configured'. The 'Home | Help | Logout' links are also visible in the top right corner.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm70vmpg	1	5	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**.



**AVAYA** Application Enablement Services Management Console

Maintenance | Service Controller

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop **Restart Service** Restart AE Server Restart Linux Restart Web Server

## 6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the NICE Engage Platform in **Section 8.2**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar contains the breadcrumb "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services, with "Security Database" and its sub-item "Tlinks" highlighted with red boxes. The main content area, titled "Tlinks", shows a "Tlink Name" section with two radio button options: "AVAYA#CM70VMPPG#CSTA#AES70VMPPG" (selected) and "AVAYA#CM70VMPPG#CSTA-S#AES70VMPPG". A "Delete Tlink" button is located below these options.

## 6.5. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking** → **Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

AVAYA

Application Enablement Services  
Management Console

Networking | Ports

▶ AE Services

▶ Communication Manager  
Interface

High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

Enabled Disabled

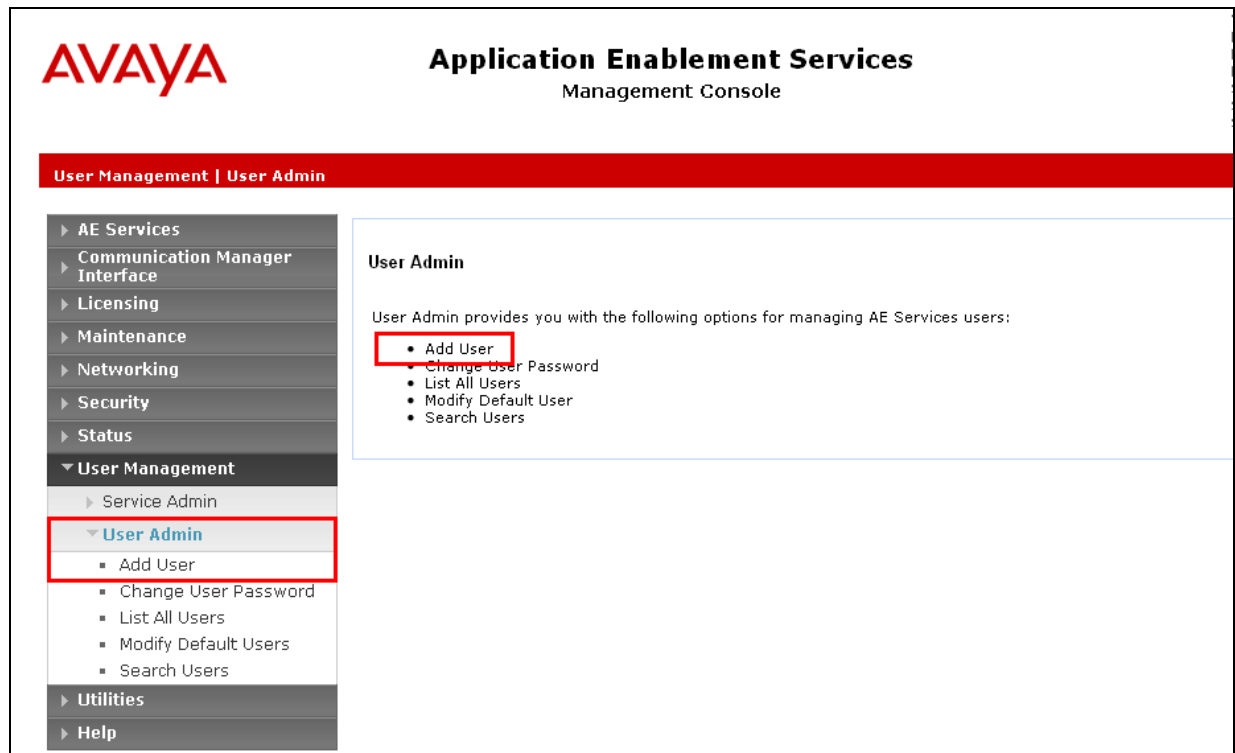
PG; Reviewed:  
SPOC 2/8/2017

Solution & Interoperability Test Lab Application Notes  
©2017 Avaya Inc. All Rights Reserved.

20 of 99  
NICE65\_ASBC71

## 6.6. Create CTI User

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



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

- **User Id** - This will be used by the NICE Engage Platform setup in **Section 8.2**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with NICE Engage Platform setup in **Section 8.2**.
- **CT User** - Select **Yes** from the drop-down menu.

**AVAYA** **Application Enablement Services**  
Management Console

User Management | User Admin | Add User

**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**.

**User Admin**

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

**Utilities**

**Help**

CM Home

Css Home

CT User: Yes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Home Phone

Home Postal Address

Initials

Labeled URI

Mail

MM Home

Mobile

Organization

Pager

Preferred Language: English

Room Number

Telephone Number

**Apply Changes** Cancel Changes

## 6.7. Associate Devices with CTI User

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

**AVAYA** Application Enablement Services Management Console

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

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

**CTI Users**

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> asc	asc	NONE	NONE
<input type="radio"/> cube	cube	NONE	NONE
<input type="radio"/> emc	emc	NONE	NONE
<input type="radio"/> jacada	jacada	NONE	NONE
<input checked="" type="radio"/> nice	nice	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE

**Edit** List All

**Security Database**

- Control
- CTI Users
  - List All Users
  - Search Users

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

**AVAYA**

**Application Enablement Services**  
Management Console

Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50  
Number of prior failed login attempts: 0  
HostName/IP: AES63VMPG/10.10.40.30  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 6.3.3.1:10-0  
Server Date and Time: Mon Dec 01 16:05:37 GMT 2014  
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Account Management

Audit

Certificate Management

Enterprise Directory

Host AA

PAM

Security Database

Control

CTI Users

List All Users

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

nice

nice

NONE

☒

Call and Device Control:

Call Origination/Termination and Device Status

None

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None

None

☐

Routing Control:

Allow Routing on Listed Devices

None

Apply Changes

Cancel Changes



## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE) in order to connect to the NICE SIP trunk recording server. The steps outlined here are only valid for the connection to NICE and are not designed to explain the setup of the SBC for SIP trunk calls. For further information on the setup and configuration of the Avaya SBC please refer to **Section 11** where a list of documentation can be found. The setup of the SBC for SIP trunk calls is outlined in **Section 12 (Appendix A)** of these Application Notes.

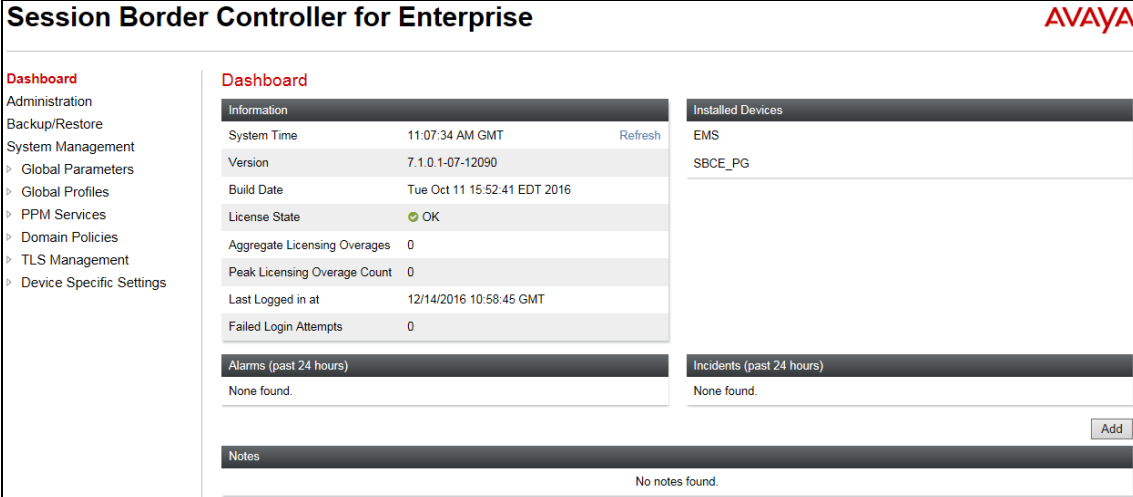
### 7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field and a "Continue" button. Below the login fields, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications 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." This is followed by a statement: "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." Then, "All users must comply with all corporate instructions regarding the protection of information assets." and finally, "© 2011 - 2016 Avaya Inc. All rights reserved."

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



The screenshot shows the main dashboard of the Avaya Session Border Controller for Enterprise. The top header includes the title "Session Border Controller for Enterprise" and the Avaya logo. On the left is a "Dashboard" menu with options: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into several sections: "Information" (System Time: 11:07:34 AM GMT, Version: 7.1.0.1-07-12090, Build Date: Tue Oct 11 15:52:41 EDT 2016, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 12/14/2016 10:58:45 GMT, Failed Login Attempts: 0), "Installed Devices" (listing EMS and SBCE\_PG), "Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (None found), and "Notes" (No notes found). There is a "Refresh" button next to the System Time and an "Add" button at the bottom right.

## 7.2. Configure Server Internetworking

Navigate to **Global Profiles** → **Server Internetworking** and click on **Add**.

The screenshot shows the 'Session Border Controller for Enterprise' configuration interface. On the left is a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Server, Interworking (highlighted), Media Forking, Routing, Server, and Configuration. The main area is titled 'Interworking Profiles: cs2100' and features an 'Add' button. Below this is a list of profiles: 'cs2100' and 'avaya-ru'. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' There are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a table of settings:

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None

Enter a suitable **Profile Name** and click on **Next**.

The 'Interworking Profile' dialog box is shown. It has a title bar with 'Interworking Profile' and a close button 'X'. Inside, there is a 'Profile Name' label and a text input field containing 'NICESIPREC' with a clear button 'x'. Below the input field is a 'Next' button.

The following are set and click on **Finish** to complete.

Editing Profile: NICESIPREC

X

General

Hold Support

☒ None  
☐ RFC2543 - c=0.0.0.0  
☐ RFC3264 - a=sendonly

180 Handling

☒ None ☐ SDP ☐ No SDP

181 Handling

☒ None ☐ SDP ☐ No SDP

182 Handling

☒ None ☐ SDP ☐ No SDP

183 Handling

☒ None ☐ SDP ☐ No SDP

Refer Handling

☐

URI Group

None ▾

Send Hold

☐

Delayed Offer

☐

3xx Handling

☐

Diversion Header Support

☐

Delayed SDP Handling

☐

Re-Invite Handling

☐

Prack Handling

☐

Allow 18X SDP

☐

T.38 Support

☐

URI Scheme

☒ SIP ☐ TEL ☐ ANY

Via Header Format

☒ RFC3261  
☐ RFC2543

Finish

### 7.3. Configure Server Configuration

Add a new **Server Configuration**. Navigate to **Global Profiles** → **Server Configuration** in the left window and click on **Add** in the main window.

Dashboard  
Administration  
Backup/Restore  
System Management  
  > Global Parameters  
  Global Profiles  
    Domain DoS  
    Server Interworking  
    Media Forking  
    Routing  
  **Server Configuration**

Server Configuration: PSTN

Add

Server Profiles  
PSTN  
Session Manager

Rename Clone Delete

General Authentication Heartbeat Advanced

Server Type Trunk Server

IP Address / FQDN	Port	Transport
10.10.16.77	5060	TCP

Edit

Enter a suitable **Profile Name** and click on **Next**.

Add Server Configuration Profile X

Profile Name NICESIPREC

Next

Enter the **Server Type** as **Recording Server** and enter the **IP Address** of the NICE Application Server, enter the **Port 5060** and the **Transport** must be set to **UDP**.

Edit Server Configuration Profile - General X

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type Recording Server

SIP Domain

TLS Client Profile None

Add

IP Address / FQDN	Port	Transport
10.10.40.125	5060	UDP

Delete

Finish

The next window shows the advanced configuration, ensure that **Enable Grooming** is set and the **Interworking Profile** is set to that created in **Section 7.2**.

**Edit Server Configuration Profile - Advanced**

Enable Grooming ☒

Interworking Profile NICESIPREC ▼

Signaling Manipulation Script None ▼

Securable ☐

Enable FGDN ☐

TCP Failover Port

TLS Failover Port

Finish

## 7.4. Configure Signaling Rules

Navigate to **Domain Policies** → **Signaling Rules**, click on **Add**.

**Signaling Rules: default**

Add Filter By Device... ▼

Signaling Rules

default

No-Content-Type-Ch...

It is not recommended to edit the defaults

General Requests Responses

Inbound

Requests

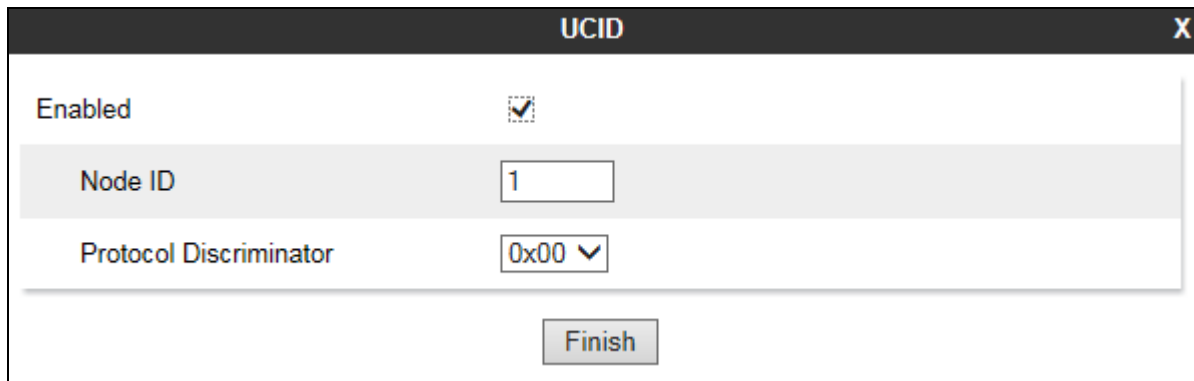
Enter a suitable name and click name **Next**.

**Signaling Rule**

Rule Name NICESIPREC X

Next

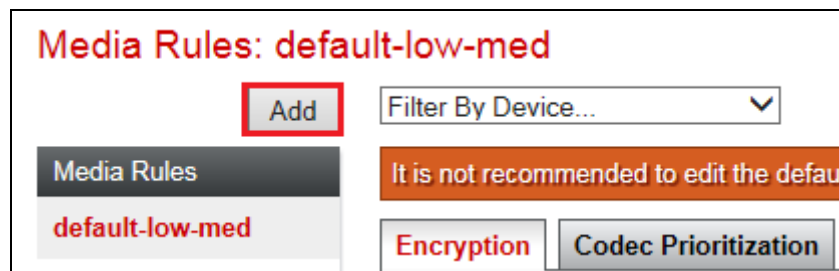
Click the Signaling Rule that the Avaya SBCE must use for the Recording Server. Click the UCID tab; click Edit (not shown). Select the **Enabled** check box. In the **Node ID** field, enter a node ID. Every entity that generates a UCID has a node ID. The node ID must be unique across a solution. In the **Protocol Discriminator** field, click **0x00**. Click **Finish**.



The image shows a window titled "UCID" with a close button (X) in the top right corner. Inside the window, there is a section labeled "Enabled" with a checked checkbox. Below this, there is a "Node ID" field containing the value "1". Underneath the "Node ID" field is a "Protocol Discriminator" dropdown menu showing "0x00" with a downward arrow. At the bottom of the window is a "Finish" button.

## 7.5. Configure Media Rules

Navigate to **Domain Policies** → **Media Rules** in the left window and click on **Add** in the main window.



The image shows a window titled "Media Rules: default-low-med". It features an "Add" button highlighted with a red box. To the right of the "Add" button is a "Filter By Device..." dropdown menu. Below the "Add" button is a "Media Rules" section with a "default-low-med" entry. To the right of this section is a warning message: "It is not recommended to edit the default". Below the warning message are two buttons: "Encryption" and "Codec Prioritization".

Enter a suitable name for the **Media Rule** and click on **Next**.



The image shows a window titled "Media Rule". It has a "Rule Name" field containing the text "NICESIPREC" and a small "x" button to its right. Below the "Rule Name" field is a "Next" button.

Enter the appropriate audio and video encryption information, and click Next.

**Media Encryption** X

**Audio Encryption**

Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

**Video Encryption**

Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

**Miscellaneous**

Capability Negotiation	<input type="checkbox"/>
------------------------	--------------------------

Finish

If the recorder only supports specific codecs, in the **Audio Codec** section, select the **Codec Prioritization** check box. In the Available column, select the preferred audio and DTMF dynamic codecs that the recorder supports, and click >. Click **Finish**.

**Codec Prioritization**

**Audio Codec**

Codec Prioritization ☒ Allow Preferred Codecs Only ☐

Transcode When Needed ☐

**Preferred Codes**

Available	Selected
Reserved (1)	PCMA (8)
Reserved (2)	PCMU (0)
GSM (3)	G729 (18)
G723 (4)	G729AB (18)
DV14 (5)	
DV14 (6)	
LPC (7)	
G722 (9)	

**Video Codec**

Codec Prioritization ☐ Allow Preferred Codecs Only ☐

Transcode When Needed ☐

**Preferred Codes**

Available	Selected
CellB (25)	
JPEG (26)	
nv (28)	
H261 (31)	
MPV (32)	
MP2T (33)	
H263 (34)	

**Finish**

## 7.6. Configure Session Policies

In the left window navigate to **Domain Policies** → **Session Policies** and in the main window click on **Add**.

**Session Border Controller for Enterprise**

Manipulation  
URI Groups  
SNMP Traps  
Time of Day Rules  
FGDN Groups  
Reverse Proxy  
Policy

► PPM Services

▾ Domain Policies

Application Rules  
Border Rules  
Media Rules  
Security Rules  
Signaling Rules  
End Point Policy  
Groups

**Session Policies**

**Session Policies: default**

**Add** Filter By Device...

**Session Policies**

**default**

**Media**

Media Anchoring ☒

Media Forking Profile **None**

Converged Conferencing ☐

Recording Server ☐

**Edit**

**It is not recommended to edit the defaults. Try cloning or adding a new policy instead.**



Enter a suitable name for the Session Policy and click on **Next** (not shown).

Select the **Media Anchoring** check box. Select the **Recording Server** check box. In the **Recording Type** field, select the type of recording required, **Full Time** is selected for NICE recording. In the **Routing Profile** field, click the routing profile that was setup for the NICE recording. Click **Finish**.

The screenshot shows a 'Media' configuration window with the following settings:

- Media Anchoring:** ☒
- Media Forking Profile:** None (dropdown)
- Converged Conferencing:** ☐
- Recording Server:** ☒
- Recording Type:** Full Time (dropdown)
- Play Recording Tone:** ☒
- Call Termination on Recording Failure:** ☐
- Routing Profile:** NICESIPREC (dropdown)
- Call Type for Media Unanchoring:** Media Tromboning Only (dropdown)

A **Finish** button is located at the bottom center of the window.

## 7.7. Configure Session Flows

In the left navigation pane, click **Device Specific Settings** → **Session Flows** (not shown). In the Application pane, click the Avaya SBCE Device for which a new session flow is to be created. The Content Area displays the session flows currently defined for that Avaya SBCE device. Click **Add**.

The screenshot shows the 'Session Flows: SBCE\_PG' page. On the left, a sidebar lists 'Devices' with 'SBCE\_PG' selected. The main area is titled 'Session Flows' and contains an 'Add' button in the top right corner. Below the button is a table with a header row and one data row. The header row is: Priority, Flow Name, URI Group #1, URI Group #2, Subnet #1, Subnet #2, Session Policy. The data row is empty. A tooltip message 'Hover over a row to see its description.' is displayed above the table.

The system displays the **Add Flow** screen. In the **Flow Name** field, type the name of the session flow. In the **URI Group #1** and **URI Group #2** field, select the URI group policy to identify the source or destination of the call. For recording all calls, leave the default value \* in the URI Group #1 and URI Group #2 fields. In the **Subnet #1** and **Subnet #2** fields, type the subnet addresses. For recording all calls, leave the default value \* in the Subnet #1 and Subnet #2 fields. In the **SBC IP Address** field, select the network name and IP address of the Avaya SBCE, again this can be set to \* for all addresses. In the **Session Policy** field, select the session policy that you created for the Recording Server. Click **Finish**.

Edit Flow: NICESIPREC

X

Flow Name

NICESIPREC

X

URI Group #1

\*

▼

URI Group #2

\*

▼

Subnet #1

Ex: 192.168.0.1/24

\*

SBC IP Address

\*

▼

\*

▼

Subnet #2

Ex: 192.168.0.1/24

\*

SBC IP Address

\*

▼

\*

▼

Session Policy

NICESIPREC

▼

Has Remote SBC

☐

Finish

## 7.8. Configure End Point Flows

In the left navigation pane, click **Device Specific Settings** → **End Point Flows** (not shown). In the Application pane, click the Avaya SBCE Device for which a new end point flow is to be created. Click on the **Server Flows** tab, the Content Area displays the end point flows currently defined for that Avaya SBCE device. Click **Add**.

**End Point Flows: SBCE\_PG**

**Devices**  
SBCE\_PG

**Subscriber Flows** **Server Flows**

Add

Click here to add a row description.

**Server Configuration: PSTN**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
<input type="text" value="1"/>	PSTN	*	Internal_Sig	External_Sig	default-low	Session Manager	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

**Server Configuration: Session Manager**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
<input type="text" value="1"/>	Session Manager	*	External_Sig	Internal_Sig	default-low	PSTN	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

- In the **Flow Name** field enter a descriptive name for the server flow for the Recording flow.
- In the **Server Configuration** drop-down menu, select the server configuration for NICE defined in **Section 7.3**.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 12.3 (Appendix A)**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 12.3 (Appendix A)**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 12.3 (Appendix A)**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile for NICE defined in **Section 12.6 (Appendix A)**.
- Click **Finish**.

Edit Flow: NICESIPREC
X

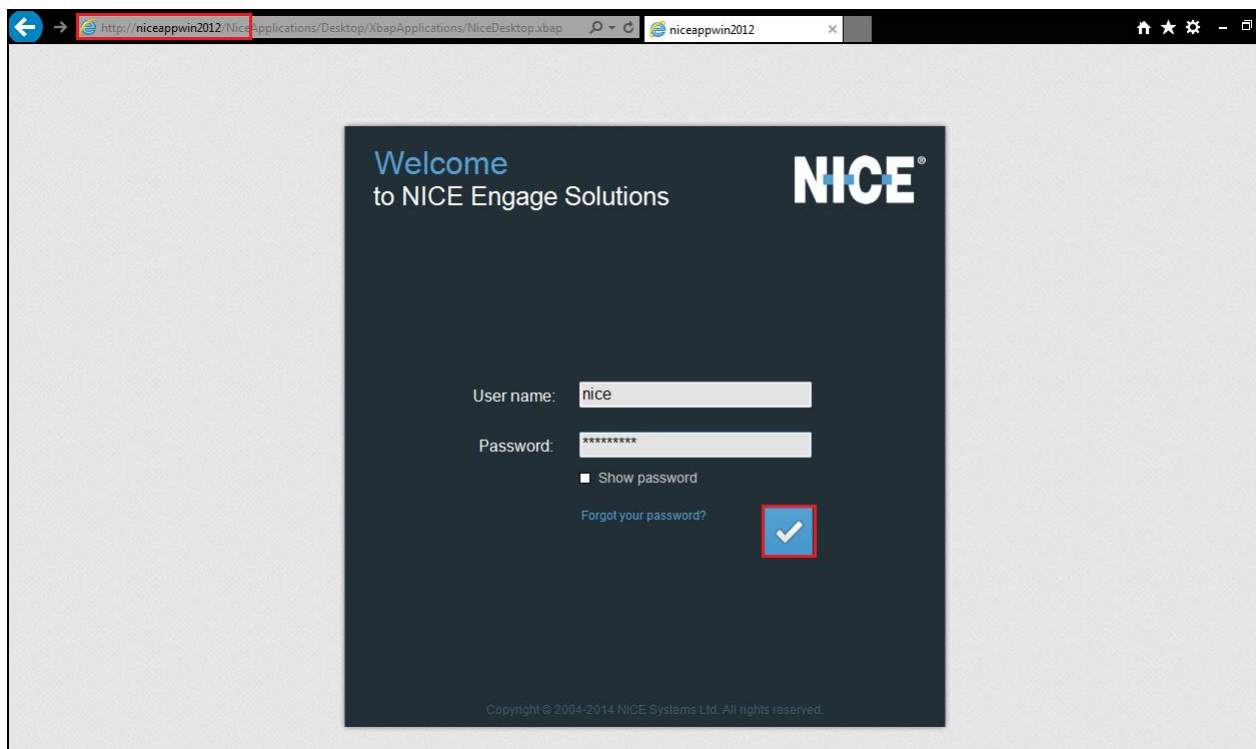
Flow Name	NICESIPREC
Server Configuration	NICESIPREC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External_Sig
Signaling Interface	Internal_Sig
Media Interface	Internal_Media
Secondary Media Interface	None
End Point Policy Group	SIPREC_Policy_Group
Routing Profile	NICESIPREC
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

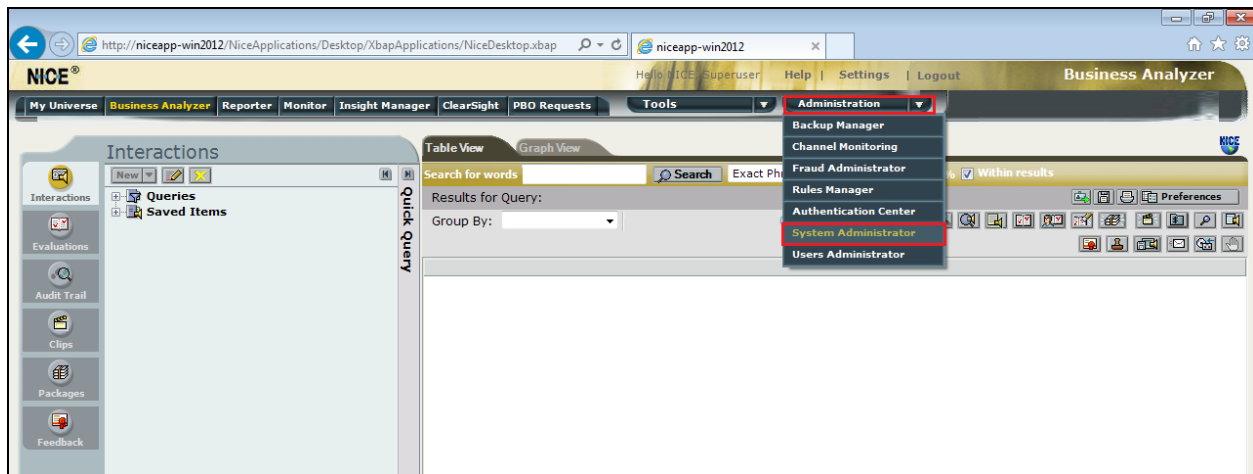
## 8. Configure NICE Engage Platform

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

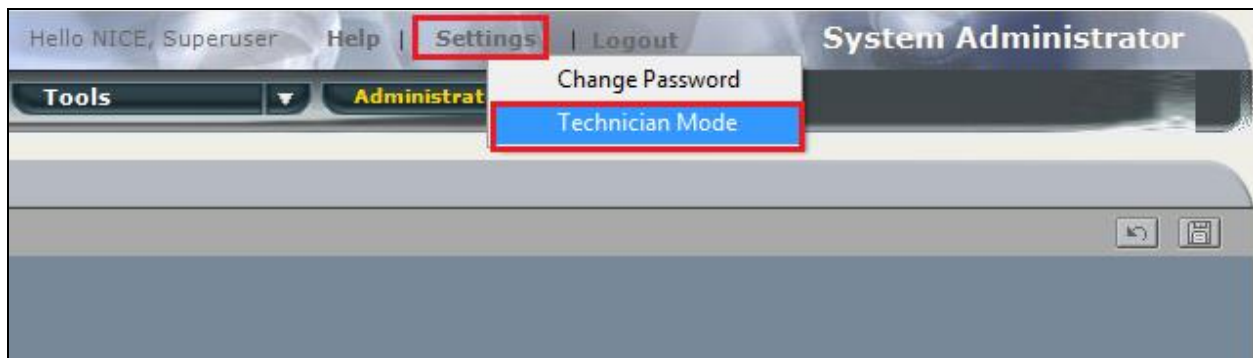
The following sections will outline the process involved in connecting the NICE Engage Platform to the Avaya Solution. All configuration of the NICE Engage Platform for connection with the AES and SBC is performed using a web browser connecting to the NICE Engage Application Server. Open a web browser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



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

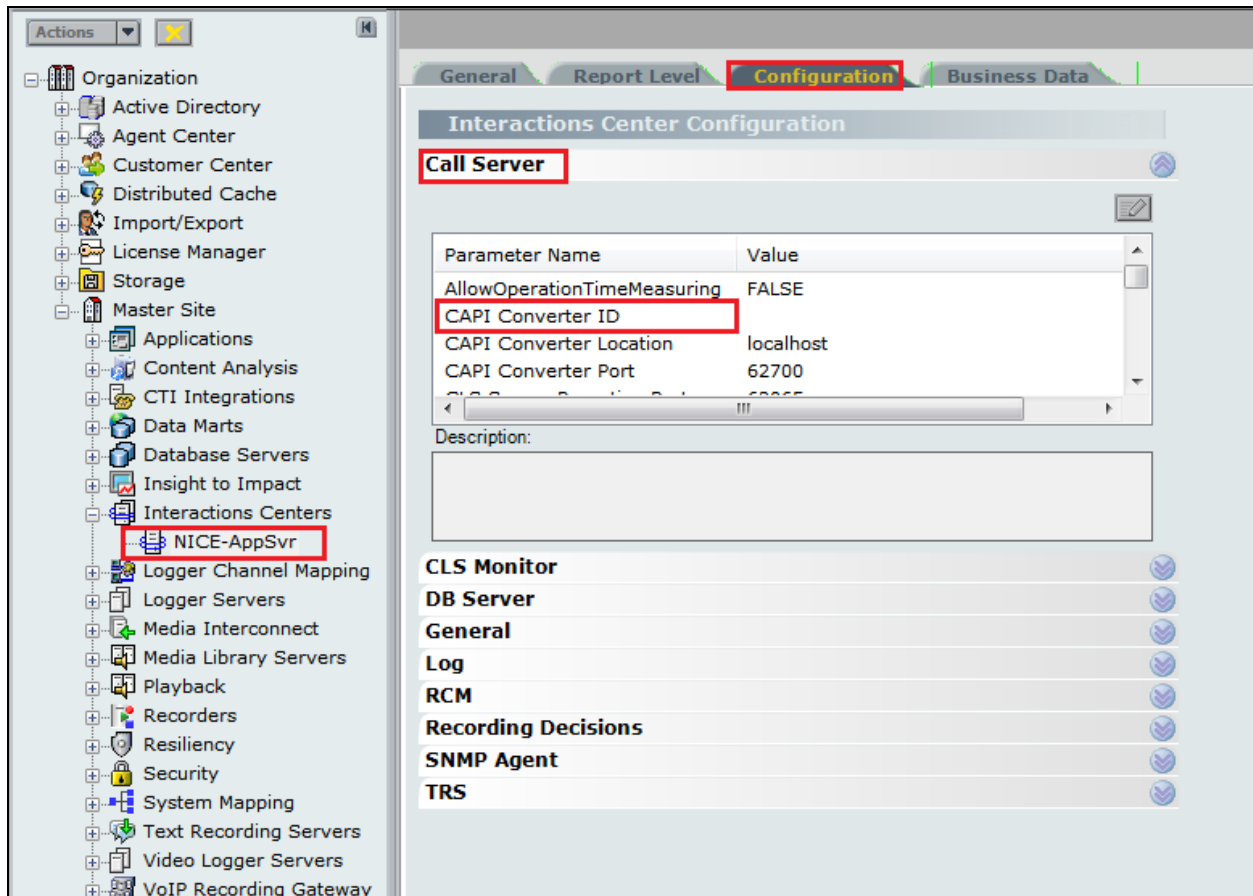


Before any changes can be made, switch to **Technician Mode** by clicking into **Settings** at the top of the screen as shown below.



## 8.1. Configure Interactions Center

Navigate to **Interactions Centers** → **NICE-AppSvr** in the left window, (the name may be different than NICE-AppSvr depending on the system installed). From the main window, click on the **Configuration** tab, in the resulting window underneath click on **Call Server** and scroll to **CAPI Converter ID** as shown below.



Enter the value **CAPIC** and click on **OK**.

The screenshot shows the 'Interactions Center Configuration' dialog box with the 'Call Server' tab selected. A 'Parameter value' sub-dialog is open, allowing the user to change a parameter value. The 'New Value' field contains the text 'CAPIC'. The 'OK' button is highlighted with a red rectangular box.

Parameter Name	Value
AllowOperationTimeMeasuring	FALSE
CAPI Converter ID	
CAPI Converter Location	localhost
CAPI Converter Port	62700
CAPI Converter ID	68865

Description:  
The identifying ID string for the CAPI Converter. Must be unique and limited to 32 characters. An empty ID indicates that there is no CAPI Converter in the system.

**Parameter value**

Old Value:

New Value: CAPIC

OK Cancel



Scroll to **IgnoreSwitchIdForUsers** and change the **New Value** to **TRUE** as shown below.

The screenshot shows the 'Interactions Center Configuration' window with the 'Call Server' tab selected. A table lists parameters, with 'IgnoreSwitchIdForUsers' highlighted. A dialog box titled 'Parameter value' is open, showing the 'Old Value' as 'FALSE' and the 'New Value' as 'TRUE'. The 'OK' button in the dialog is highlighted.

Parameter Name	Value
IgnoreSwitchId	FALSE
IgnoreSwitchIdForUsers	FALSE
InsertAllDualRecordings	FALSE
LoginTableMaxEntries	20000

Description:  
If true, the Call Server ignores the switch id when completing userID information.

**Parameter value**

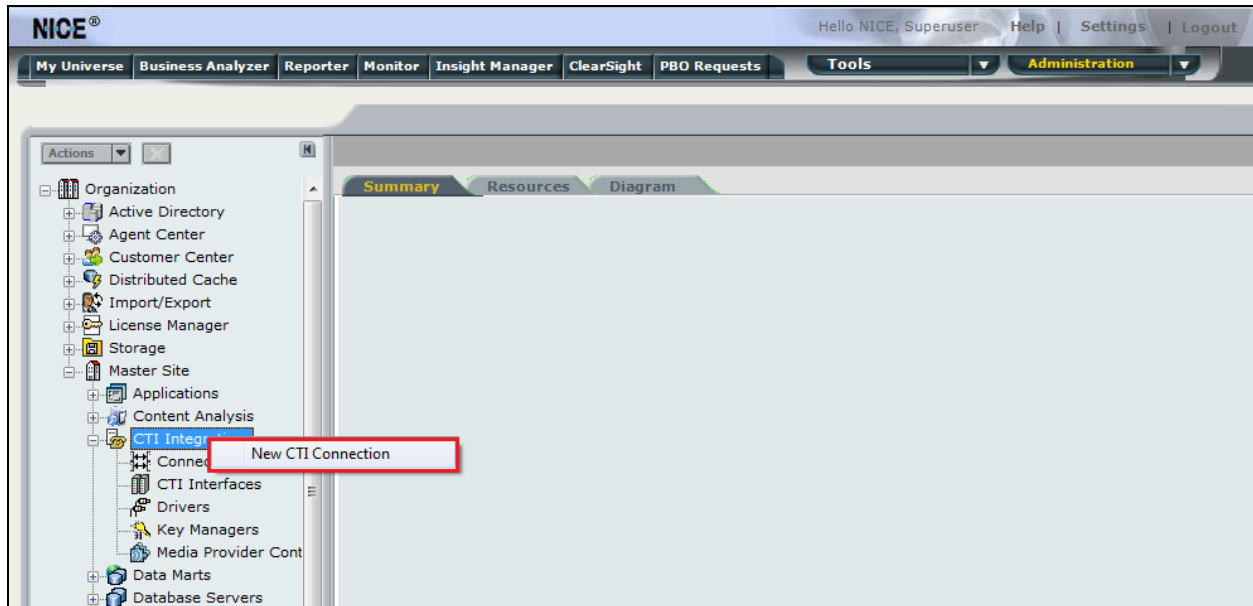
Old Value: FALSE

New Value: TRUE

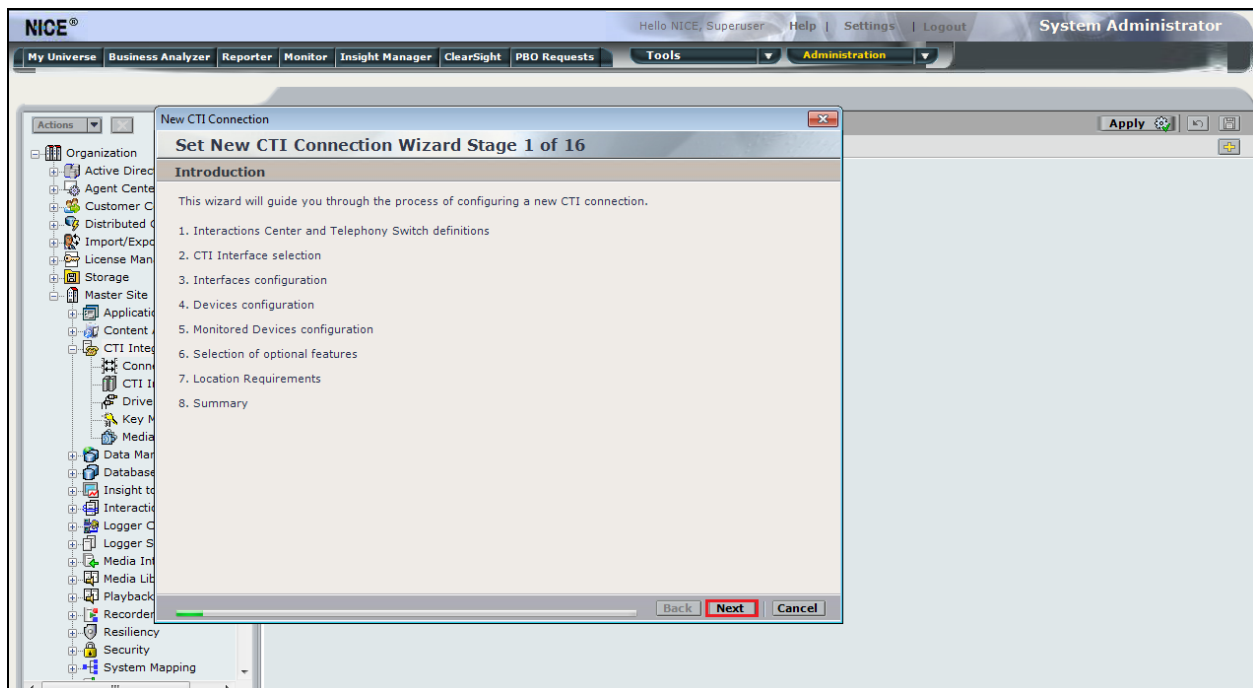
OK Cancel

## 8.2. New CTI Connection for AES

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 to receive events. Click on **Next** to continue.



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

The **Telephony Switch** must be selected 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 17

Interactions Center Switch

Attach CTI to Interactions Center Server:

☒ Regular Interactions Center: NICE-AppSvr

☐ Interactions Center Cluster:

☐ Use existing Telephony Switch: Avaya POM

☒ Define new Telephony Switch:

Switch Type: Avaya CM

Switch Name: Avaya SBC

Advanced >>

Back Next Cancel

Select **AES TSAPI** for the **Avaya CM CTI Interface**, ensure that nothing else is ticked and click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 3 of 17

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: AES SMS

☒ Active Recording: DMCC (Advanced Interaction Recorder)

Back Next Cancel

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
<b>ServerName</b>	
<b>LoginID</b>	
<b>Password</b>	
<b>UseWarmStandBy</b>	No

Description: Server connection name.

Additional Interface Parameters

Back Next Cancel

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

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
<b>ServerName</b>	
<b>LoginID</b>	
<b>Password</b>	
<b>UseWarmStandBy</b>	No

Description: Server connection name.

Additional Interface Parameters

Back Next Cancel

Set Parameter Value

Interface Connection Parameter

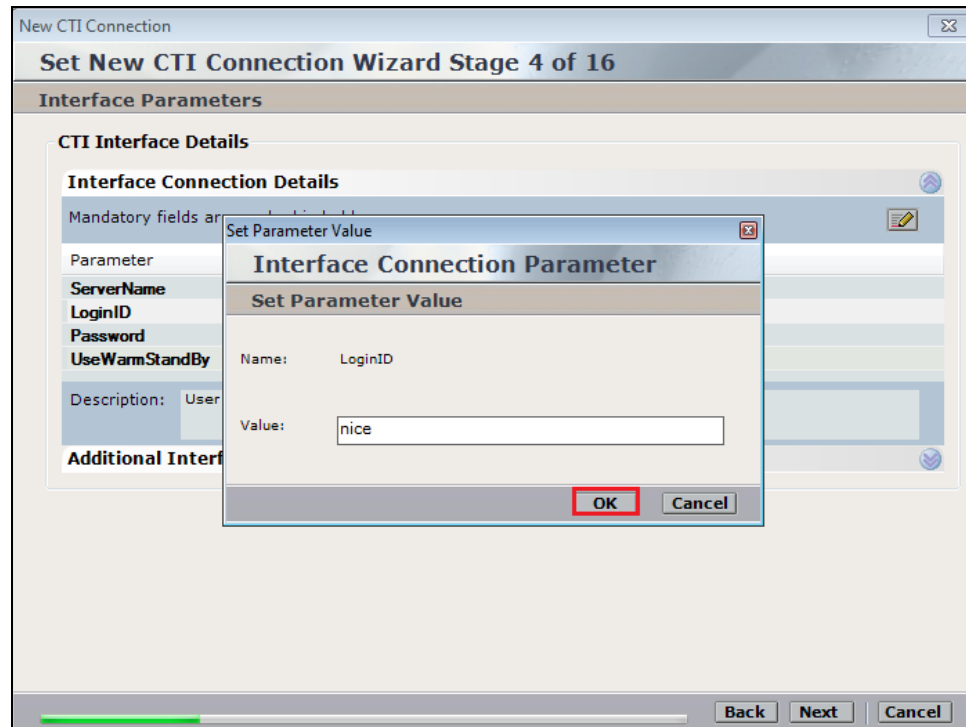
Set Parameter Value

Name: ServerName

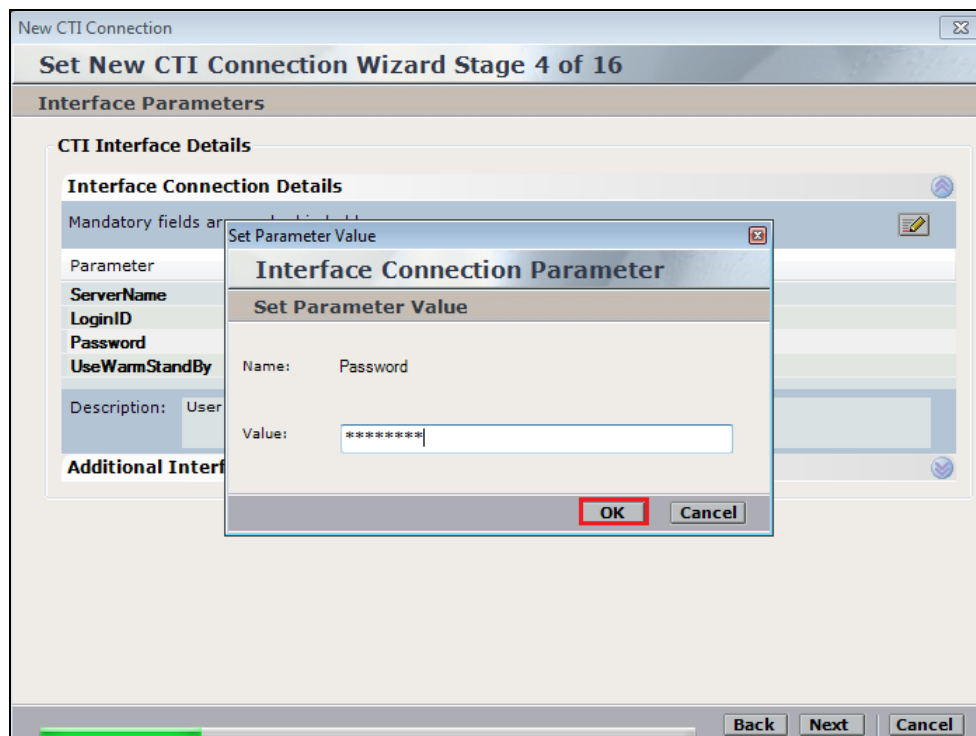
Value: AVAYA#CM70VMGP#CSTA#AES70VMGP

OK Cancel

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



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



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

The screenshot shows the 'Set New CTI Connection Wizard Stage 4 of 16' window. The 'Interface Parameters' section is active, displaying 'CTI Interface Details'. A table lists parameters: ServerName (AVAYA#CM70VMPG#CSTA#AES70VMPG), LoginID (nice), Password (\*\*\*\*\*), and UseWarmStandBy (No). The 'Next' button at the bottom is highlighted with a red box.

Parameter	Value
ServerName	AVAYA#CM70VMPG#CSTA#AES70VMPG
LoginID	nice
Password	*****
UseWarmStandBy	No

Description: Is warm standby supported?

Additional Interface Parameters

Back Next Cancel

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

The screenshot shows the 'Set New CTI Connection Wizard Stage 11 of 17' window. The 'Devices' section is active, displaying 'Available Devices'. It indicates '0 devices' are currently listed. An 'Add' button is highlighted with a red box. Below is a table with columns: Device Number/IP, CTI Trunk ID, and Type.

Available Devices

Provide telephony switch available devices

0 devices

Add Add Range Add From Switch

Device Number/IP	CTI Trunk ID	Type

Back Next Cancel

The **Device Type** should be **Extension** and insert the extension number of a phoneset that is to be recorded the example below showing extension **7000**. Repeat this process for all the devices that are to be monitored.

The screenshot shows a dialog box titled "Available Device" with a sub-header "Add Device". It contains several input fields: "Name" (empty), "Device Type:" (dropdown menu set to "Extension"), "Device Number:" (text box containing "7000"), and "IP:" (empty). Below these is a section titled "Advanced Device Parameters" which includes a checkbox for "Display Read Only Information" and a table with two columns: "Name" and "Value". The table is currently empty. At the bottom of the dialog is a "Description:" label followed by a text area. The "OK" button at the bottom right is highlighted with a red rectangular box.

Name	Value

Once all the devices to be monitored are added, click on **Next** to continue.

New CTI Connection

**Set New CTI Connection Wizard Stage 11 of 17**

**Devices**

**Available Devices**

Provide telephony switch available devices

3 devices

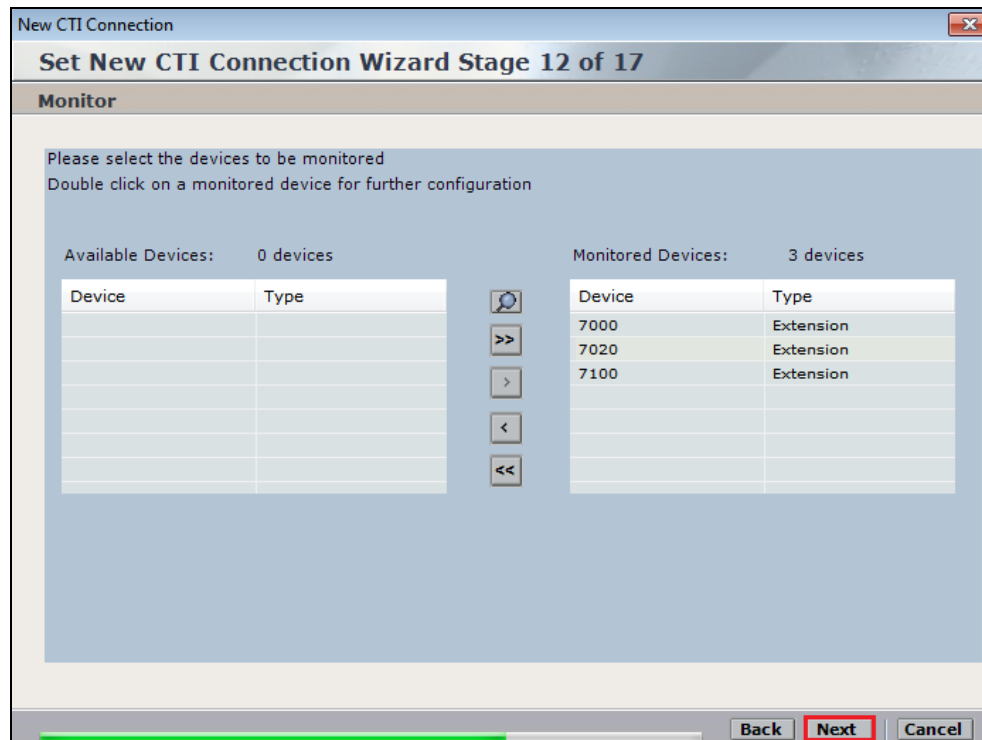
Search X Add Add Range Add From Switch

Device Number	CTI Trunk ID	Type
7000		Extension
7020		Extension
7100		Extension

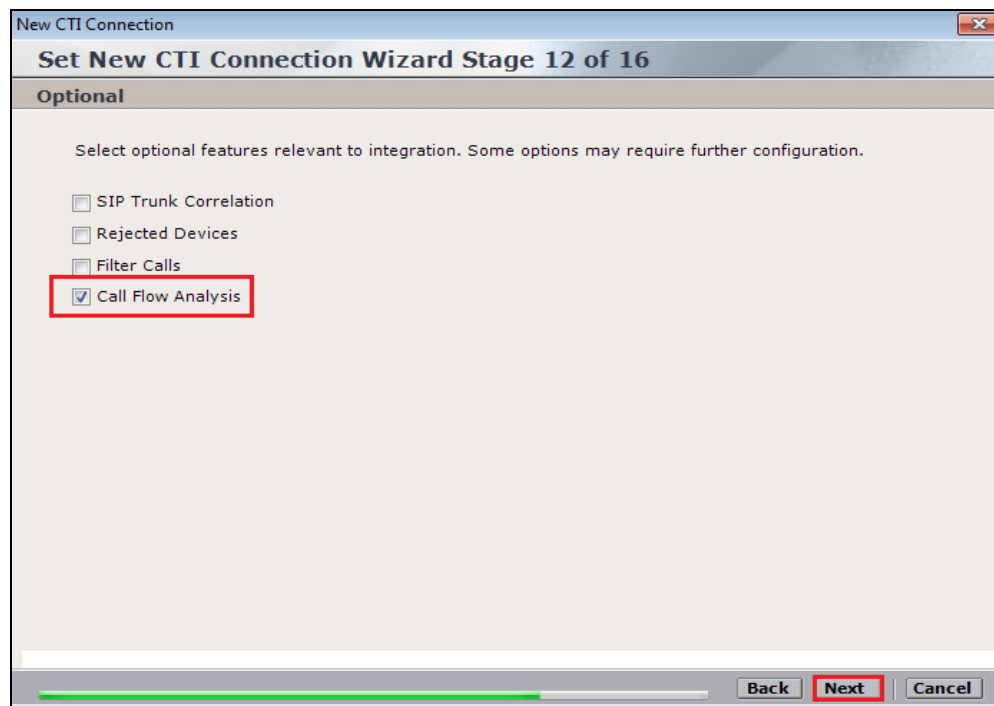
Back Next Cancel



The devices should already appear in the right column but ensure that they are selected as shown and click on **Next** to continue.



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



Select a different **Port** number as shown below. Port **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

Back Next Cancel

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

New CTI Connection

**Set New CTI Connection Wizard Stage 17 of 17**

**Summary**

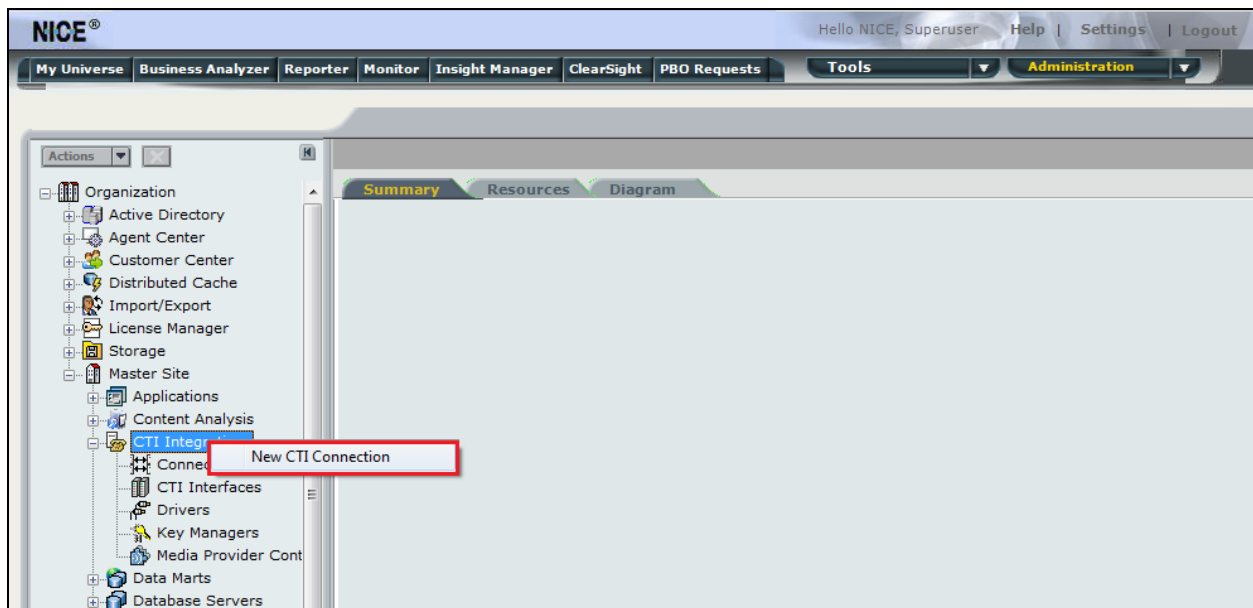
Click Finish to save and apply the configuration of the following CTI:

**Avaya SBC Connection**

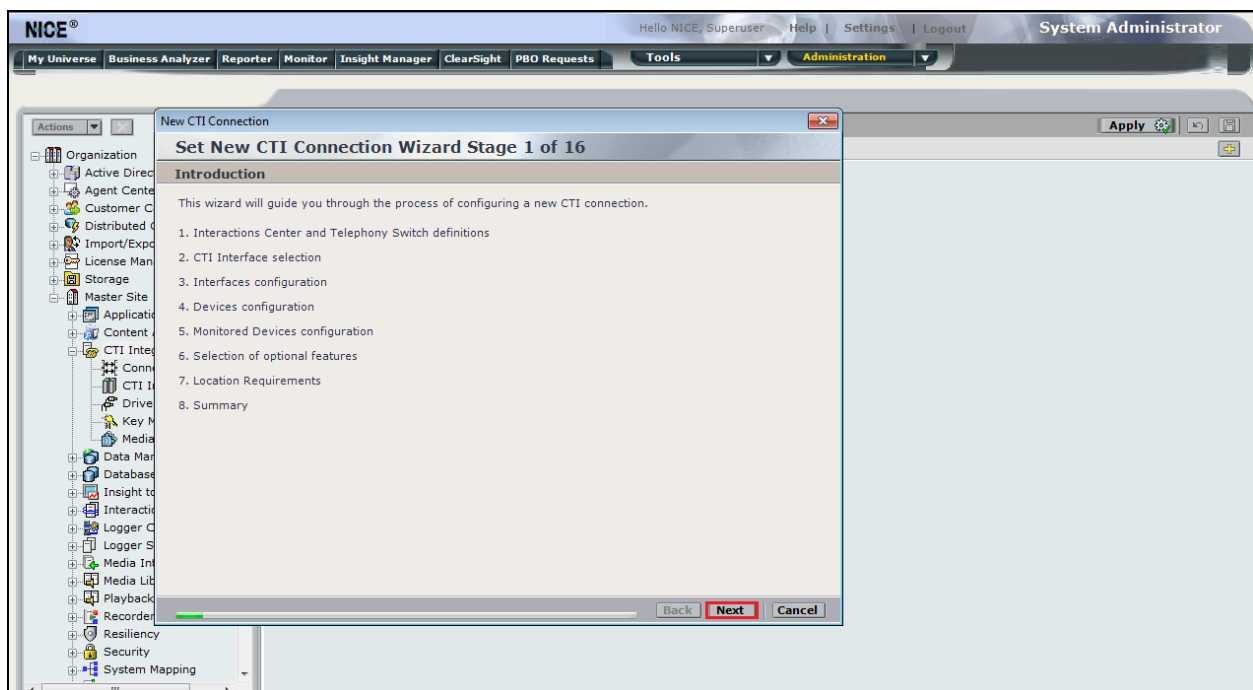
Back Finish Cancel

### 8.3. New CTI Connection for SIP Recording

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 SBC for SIP Recording. Click on **Next** to continue.



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

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

New CTI Connection

Set New CTI Connection Wizard Stage 2 of 17

Interactions Center Switch

Attach CTI to Interactions Center Server:

☒ Regular Interactions Center: NICE-AppSvr

☐ Interactions Center Cluster:

☐ Use existing Telephony Switch: Avaya POM

☒ Define new Telephony Switch:

Switch Type: SIPREC

Switch Name: SIPREC\_ASBC

Advanced >>

Back Next Cancel

The **SIPREC CTI** Interface should show as **SIPREC** and **Active Recording** should be ticked and **SIPREC** chosen from the dropdown menu. Click on **Next** to continue.

The screenshot shows the 'Set New CTI Connection Wizard Stage 3 of 17' window. The 'Interface Type' section contains the following fields:

- CTI Interface Type:** A dropdown menu with 'SIPREC' selected. Below the dropdown, the text 'SIPREC' and 'SIPREC' is visible.
- VoIP Mapping:** An unchecked checkbox followed by an empty dropdown menu.
- Active Recording:** A checked checkbox (highlighted with a red rectangle) followed by a dropdown menu with 'SIPREC' selected. Below the dropdown, the text 'SIPREC' and 'SIPREC' is visible.

At the bottom of the window, there are 'Back', 'Next' (highlighted with a red rectangle), and 'Cancel' buttons.

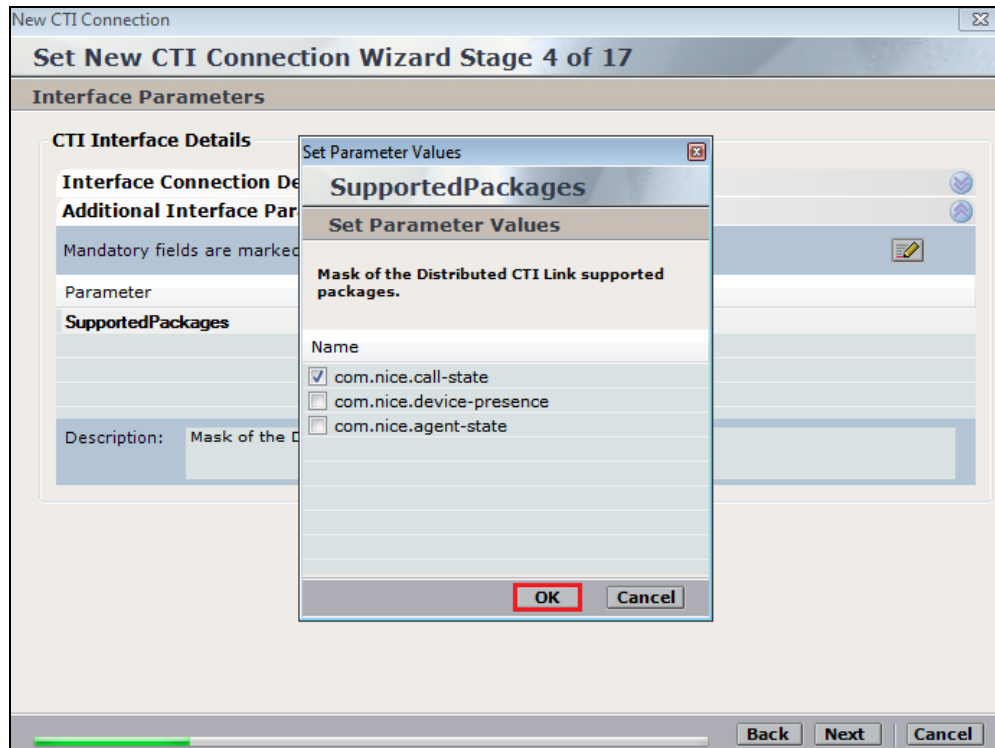
Click on **Additional Interface Parameters** and double click on **SupportedPackages**.

The screenshot shows the 'Set New CTI Connection Wizard Stage 4 of 17' window. The 'Interface Parameters' section contains the following fields:

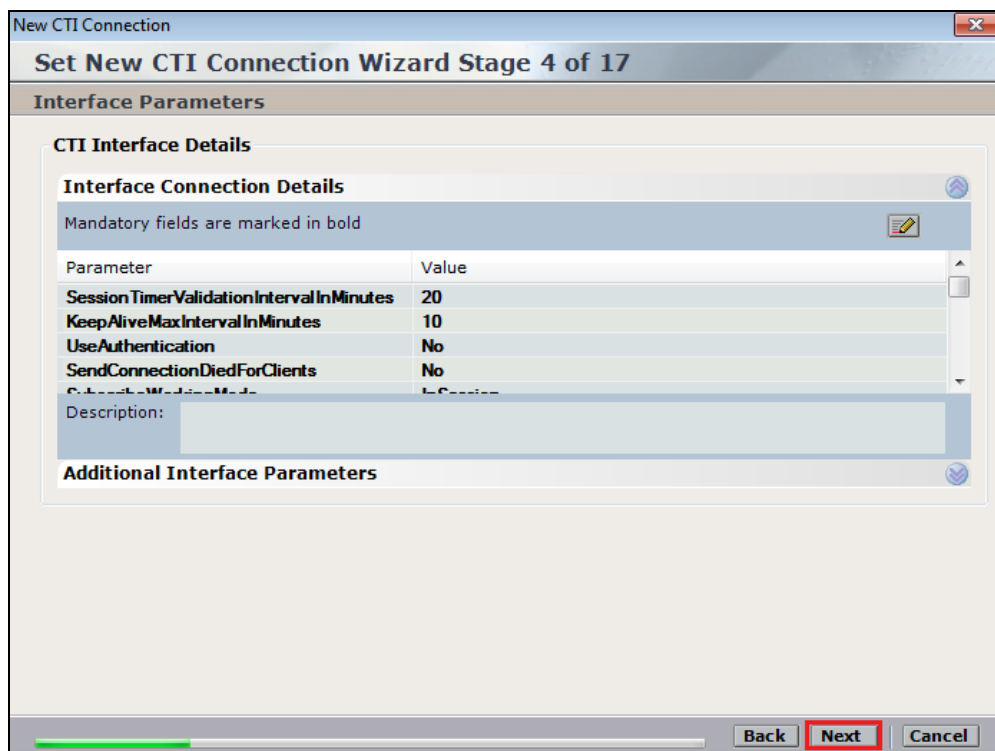
- CTI Interface Details:** A section header.
- Interface Connection Details:** A section header.
- Additional Interface Parameters:** A section header (highlighted with a red rectangle).
- Mandatory fields are marked in bold:** A note with a pencil icon.
- Parameter Value Table:** A table with two columns: 'Parameter' and 'Value'. The first row has 'SupportedPackages' (highlighted with a red rectangle) in the 'Parameter' column and '0' in the 'Value' column.
- Description:** A text box containing the text 'Mask of the Distributed CTI Link supported packages.'

At the bottom of the window, there are 'Back', 'Next', and 'Cancel' buttons.

Tick the **com.nice.call-state** box as shown below and click on **OK**.



Click on **Next** to continue.



Click on **Media Provider Controllers – Location**. The **Server IP/Hostname** and **Connection Manager Port** should automatically be populated as shown below. The port number may need to be altered if that default port is already been used. Click on the + icon in the main window

New CTI Connection

Set New CTI Connection Wizard Stage 9 of 17

Active Recording

**Media Provider Controllers - Location**

Media Provider Location

Server IP/Hostname: NICEAIRServer

Connection Manager Port: 62094

Media Provider Controllers:

IP/Hostname	CM Port

Back Next Cancel

Click on **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 9 of 17

Active Recording

**Media Provider Controllers - Location**

Media Provider Location

Server IP/Hostname:

Connection Manager Port: 62094

Media Provider Controllers:

IP/Hostname	CM Port
NICEAIRServer	62094

Back **Next** Cancel

The devices that are to be monitored need to be added again. Click on **Add** to add them one at a time or if there is a range of devices to be added, **Add Range** can be selected.

New CTI Connection

**Set New CTI Connection Wizard Stage 11 of 17**

**Devices**

**Available Devices**

Provide telephony switch available devices

0 devices

Device Number	Unique Device ID	Type



From the **Device Type** drop-down list, select **Extension**. Leave the **Device Number** field blank. In the **Unique Device ID** field, enter the Unique Device ID number.

**Note:** The Unique Device ID is a number that is defined and assigned to a specific device. It has no connection to the PBX. (Best practice is to define devices 1, 2, 3...). The number has no real meaning and used to correlate CTI events and recording between SIPREC and TSAPI interfaces. Each extension defined here can be used for only one simultaneous call recording.

**Port Support** can be left as **Single Port** and click OK to continue.

**Available Device**

**Edit**

Name:

**Device Type:** \*

**Device Number:**

**Unique Device ID:**

**IP:**

**Port Support:**

**Advanced Device Parameters**

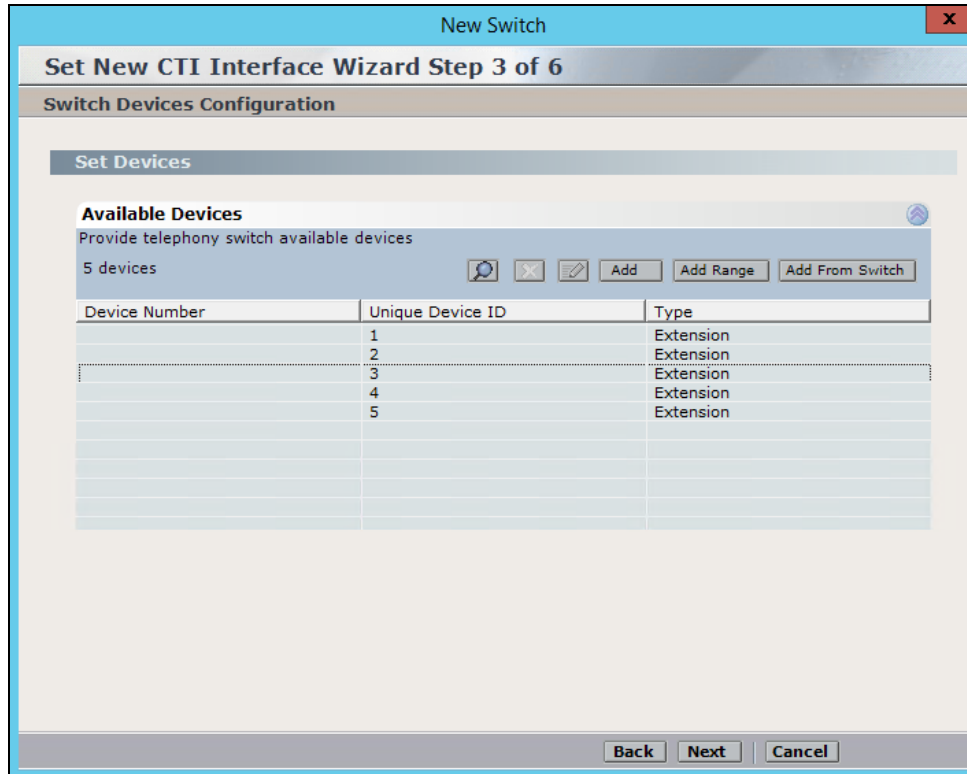
☐ Display Read Only Information

Name	Value

**Description:**

**OK** **Cancel**

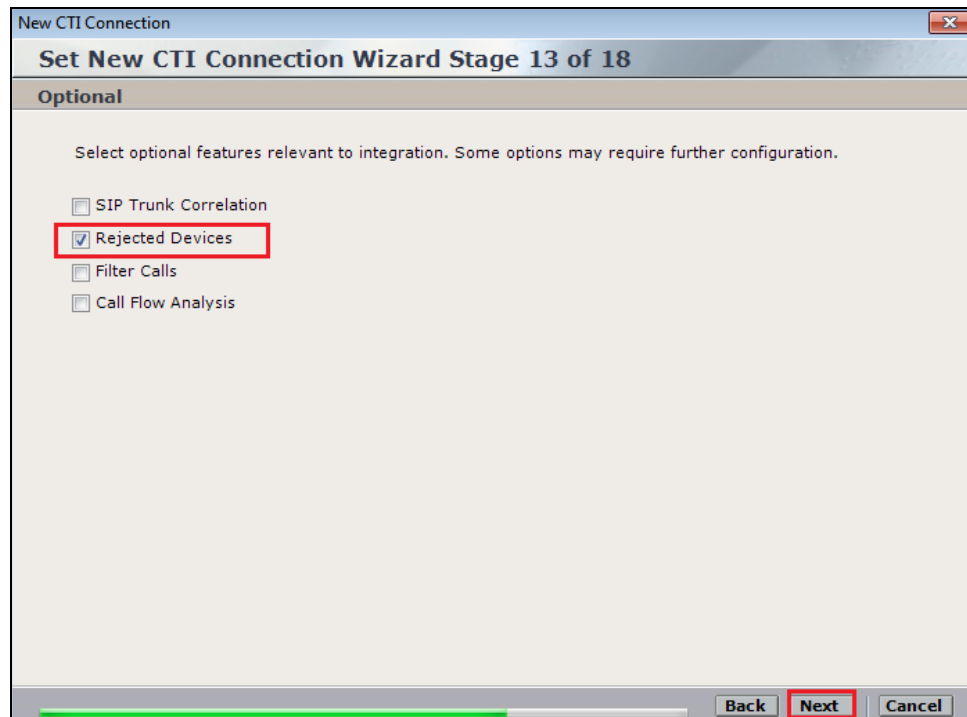
With all the extensions added, click on **Next** to continue.



The screenshot shows the 'Set New CTI Interface Wizard Step 3 of 6' window. The title bar is 'New Switch'. The main title is 'Set New CTI Interface Wizard Step 3 of 6'. The subtitle is 'Switch Devices Configuration'. Below this is a 'Set Devices' section. It includes a sub-section 'Available Devices' with the text 'Provide telephony switch available devices' and '5 devices'. There are buttons for 'Add', 'Add Range', and 'Add From Switch'. Below this is a table with three columns: 'Device Number', 'Unique Device ID', and 'Type'. The table contains five rows of data, all with 'Extension' as the type. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Device Number	Unique Device ID	Type
	1	Extension
	2	Extension
	3	Extension
	4	Extension
	5	Extension

Ensure that **Rejected Devices** is ticked. Click on **Next** to continue.



The screenshot shows the 'Set New CTI Connection Wizard Stage 13 of 18' window. The title bar is 'New CTI Connection'. The main title is 'Set New CTI Connection Wizard Stage 13 of 18'. The subtitle is 'Optional'. Below this is a section with the text 'Select optional features relevant to integration. Some options may require further configuration.' There are four checkboxes: 'SIP Trunk Correlation', 'Rejected Devices' (which is checked and highlighted with a red box), 'Filter Calls', and 'Call Flow Analysis'. At the bottom are 'Back', 'Next' (highlighted with a red box), and 'Cancel' buttons.

Avaya SBCE reports some intermediate SIP messages (SIP call between agent and specific device on Avaya SBCE – **ASBCE** and **ASBCE@asbce.com**) that are not necessary for recording. In order to ignore them both devices should be mentioned in the **Rejected Devices** list, as shown below.

New CTI Connection

**Set New CTI Connection Wizard Stage 15 of 18**

**Rejected Devices**

Please select the devices to be rejected

Available Devices: 0 devices

Device	Type

Rejected Devices: 2 devices

Device	Type
ASBCE	RejectedDevice
ASBCE@asbce.com	RejectedDevice

Back **Next** Cancel

The port may need to be altered here depending on if the default one has been used but a message will be displayed if this is the case. Click on **Next** to continue.

New CTI Connection

**Set New CTI Connection Wizard Stage 16 of 17**

**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: 62096

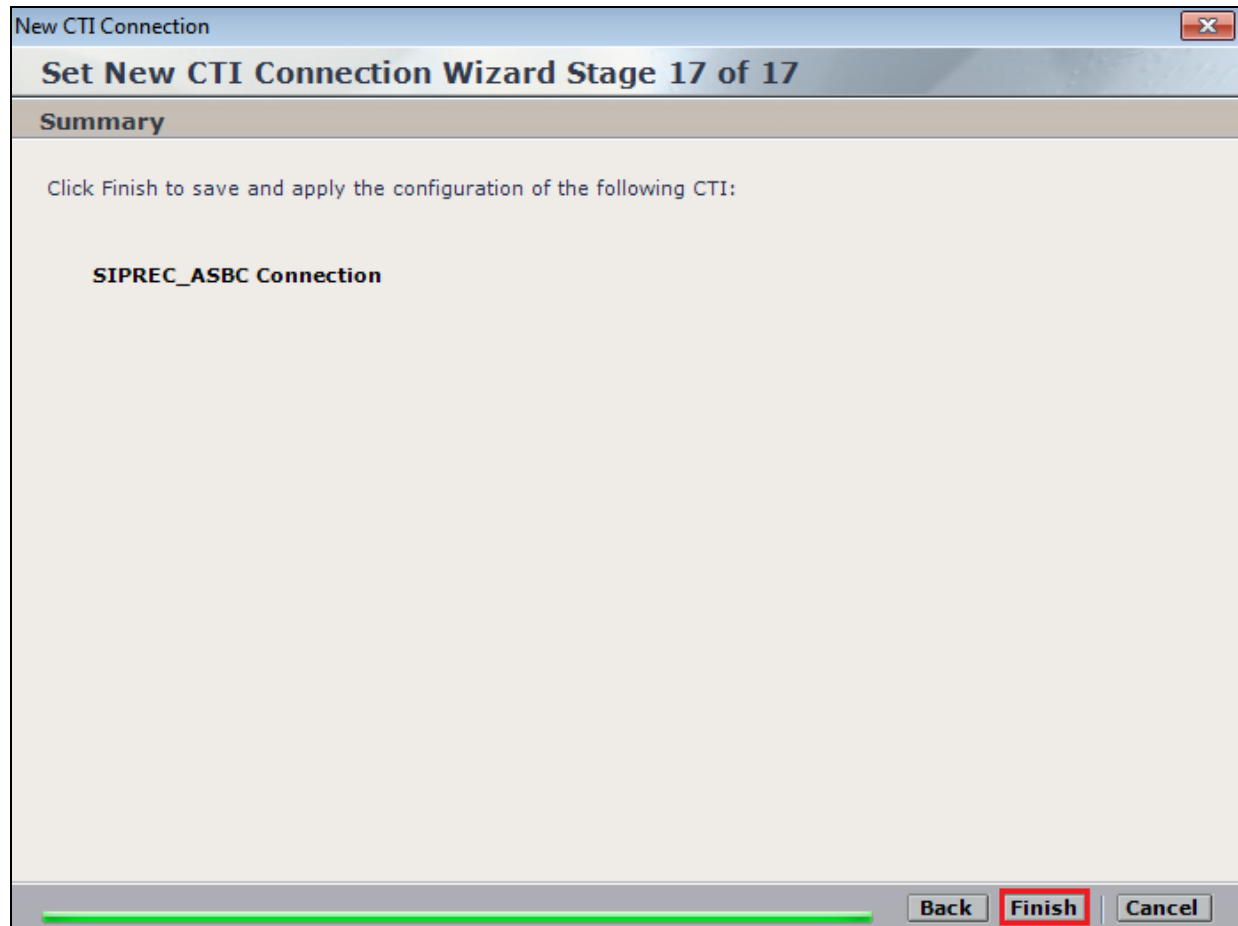
☐ Select available Connection Manager

Ports in use:

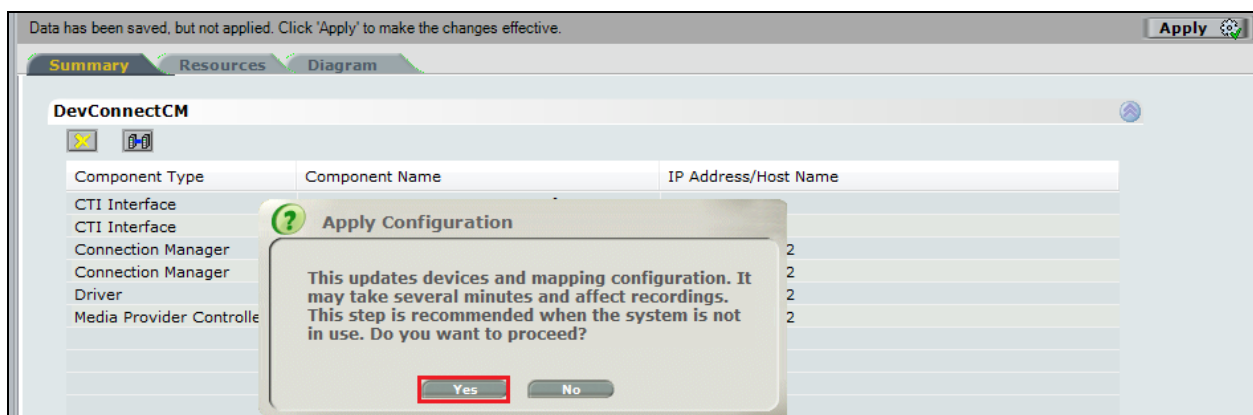
62094  
62095

Back **Next** Cancel

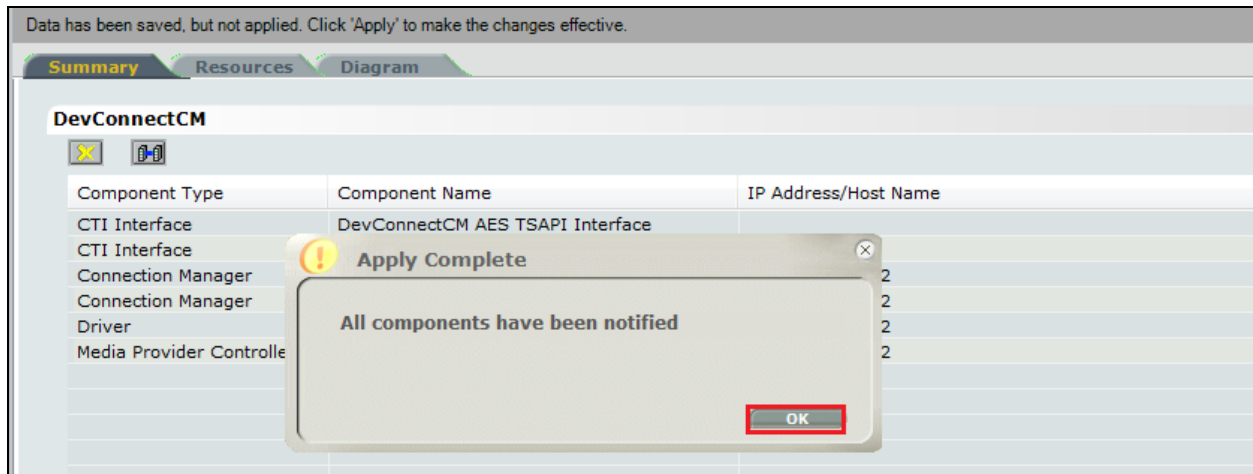
Click on **Finish** to complete the connection setup.



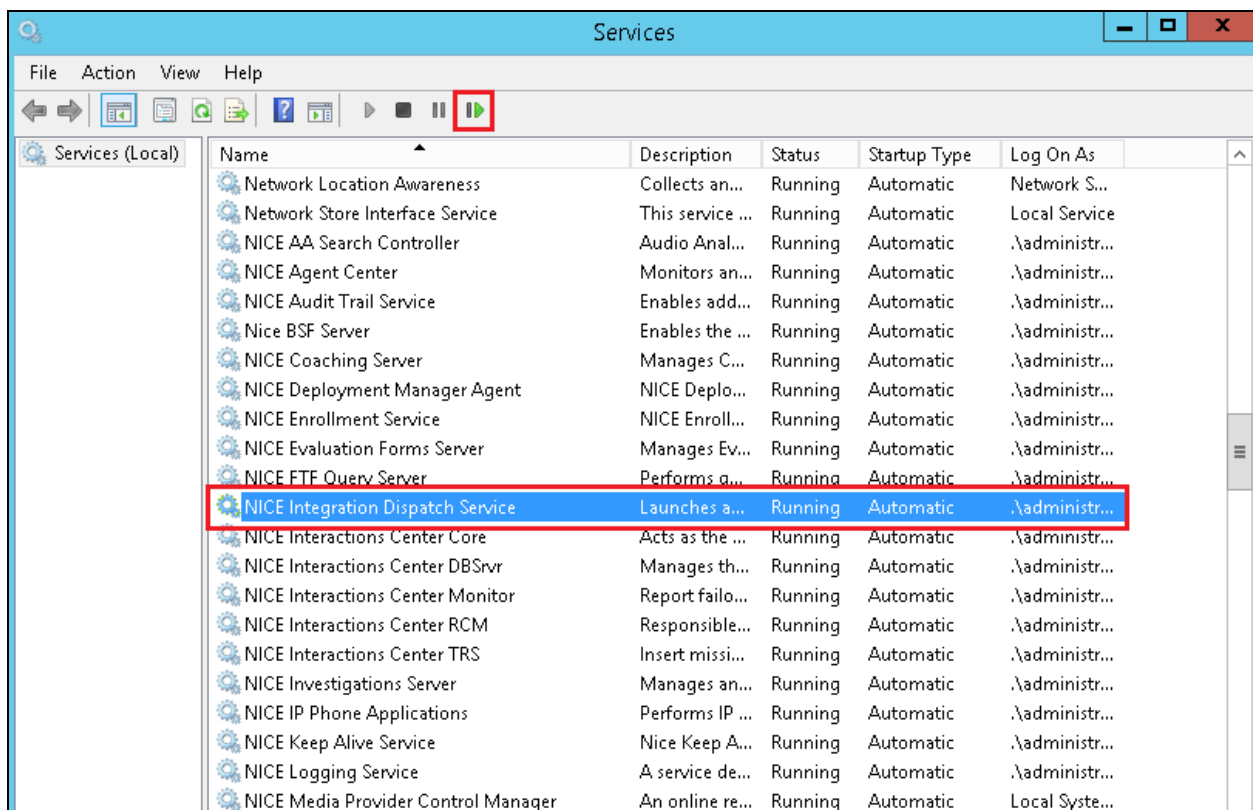
Click on **Apply** at the top right of the screen to save the new connection and click on **Yes** to proceed



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

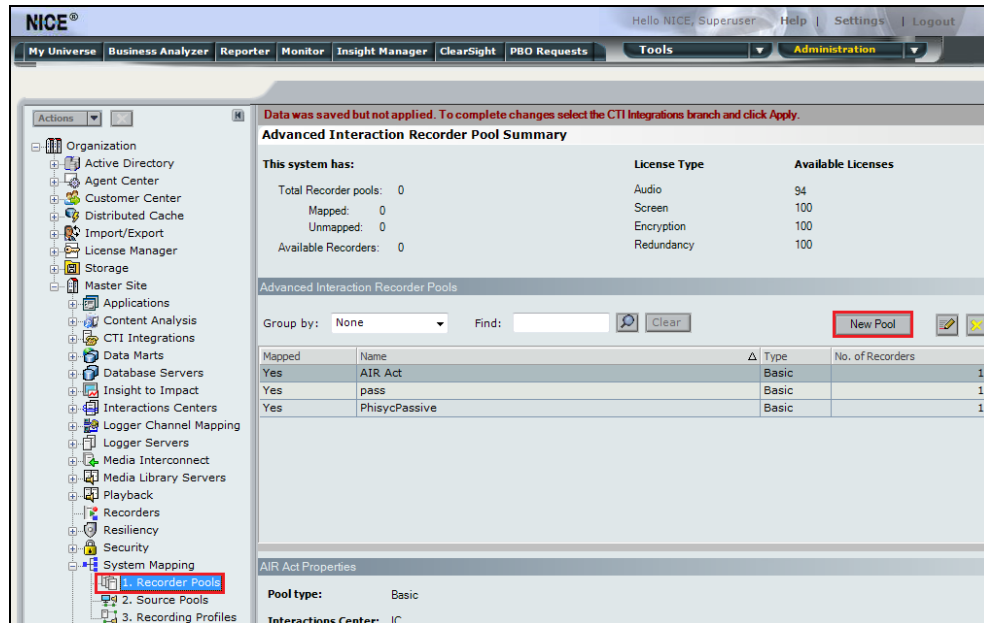


From the NICE Application Server, open **Services** and restart the **NICE Integration Dispatch Service**.

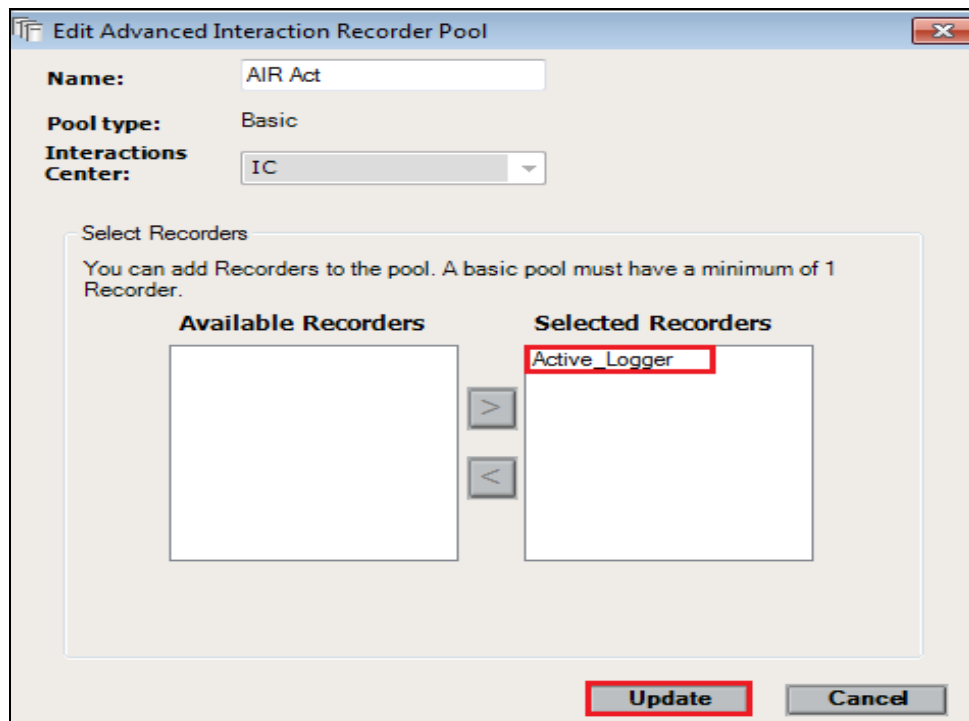


## 8.4. System Mapping

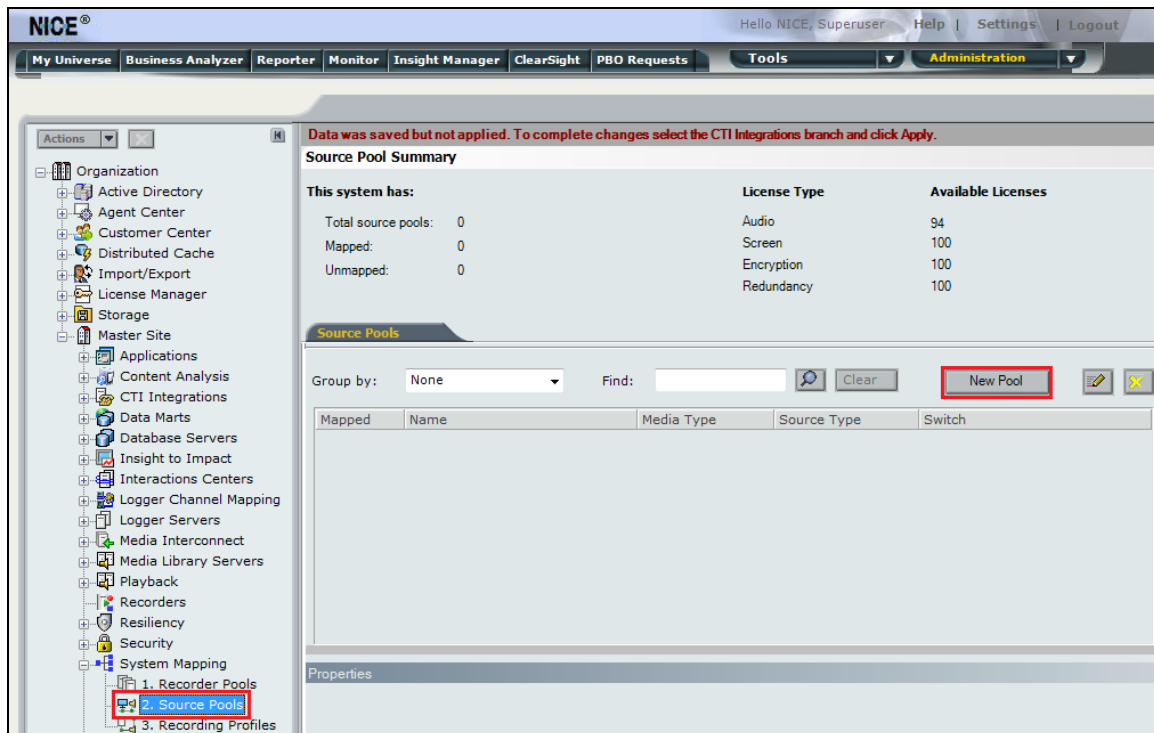
In the left window navigate to **Master Site** → **System Mapping** → **Recorder Pools** and in the main window, click on **New Pool**.



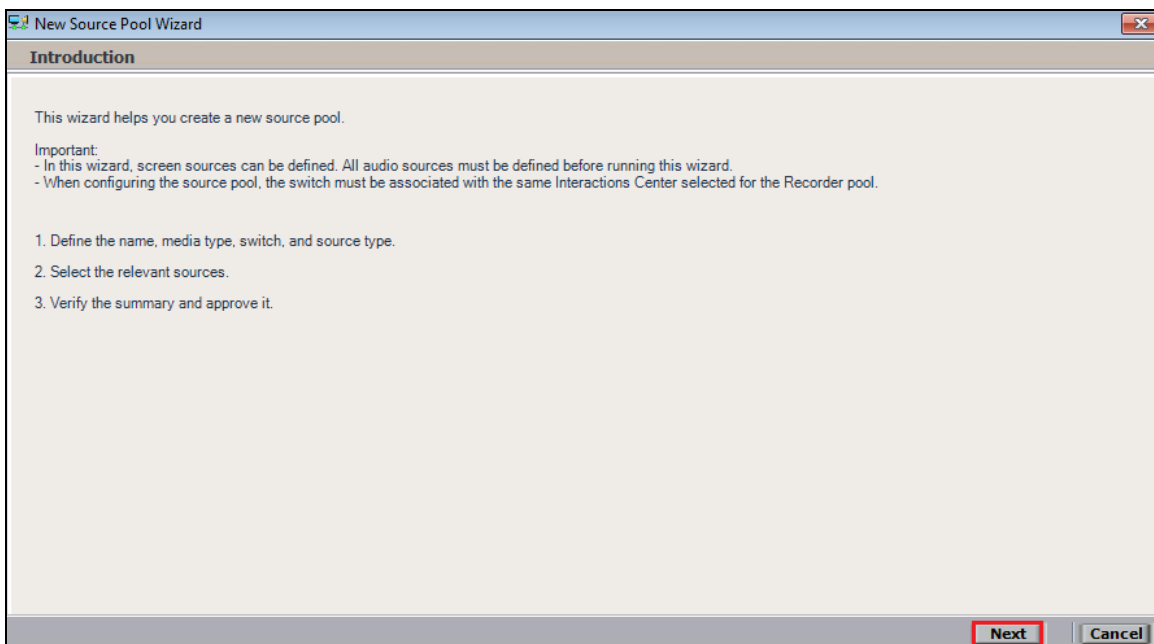
Enter a suitable **Name** for the **Recorder Pool** and select the **Active\_Logger** from the list of **Available Recorders** and click on **Update** to continue.



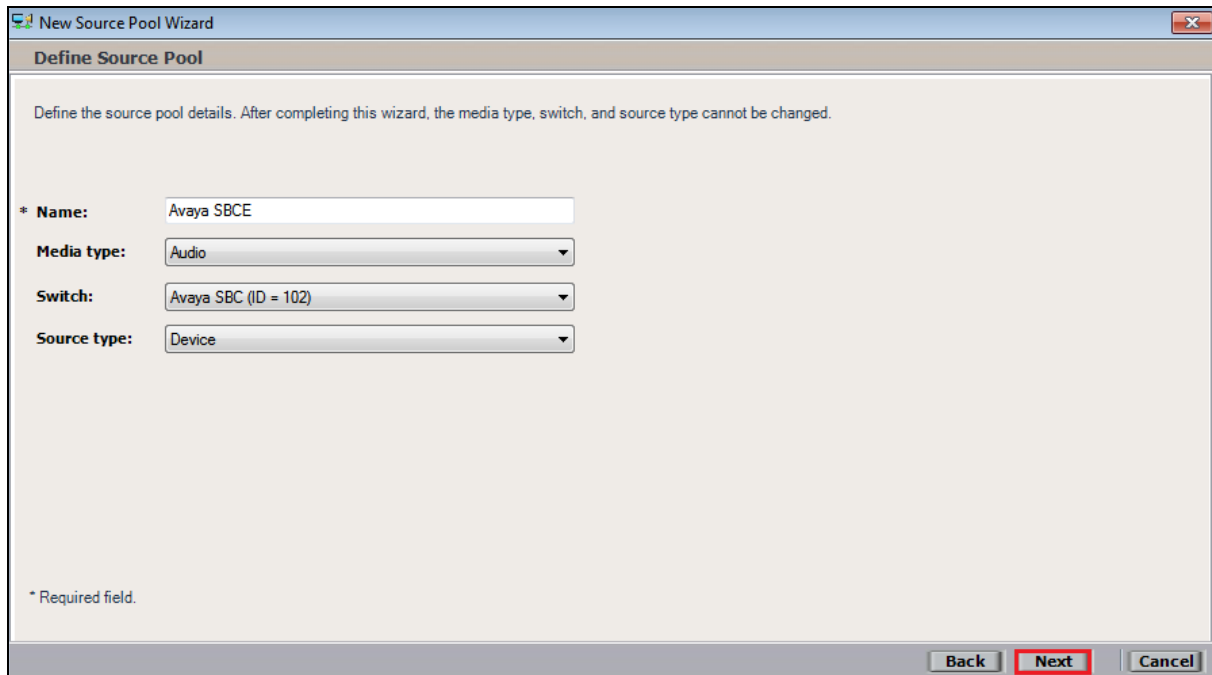
From the left navigation window select **Source Pools** and from the main window click on **New Pool**.



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



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



New Source Pool Wizard

Define Source Pool

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

\* **Name:**

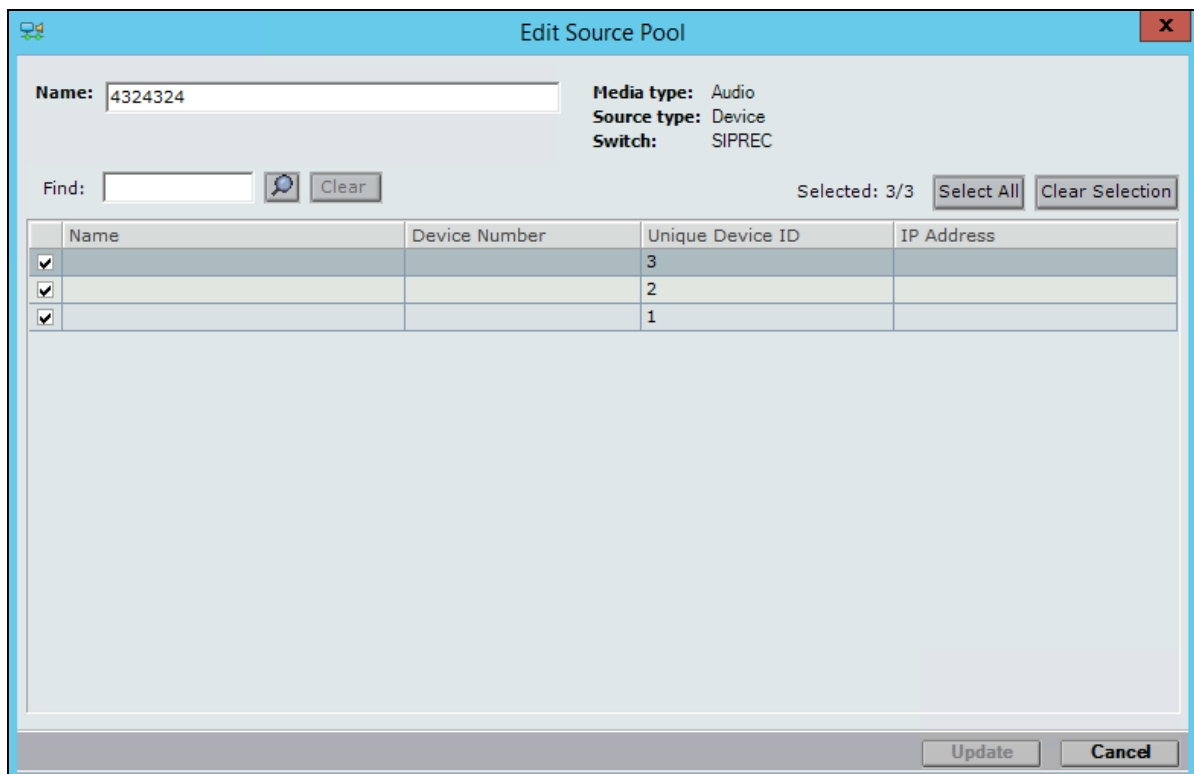
**Media type:**

**Switch:**

**Source type:**

\* Required field.

Select the extensions that were added in **Section 8.1**. Click on **Next** to continue.



Edit Source Pool

**Name:**

**Media type:** Audio  
**Source type:** Device  
**Switch:** SIPREC

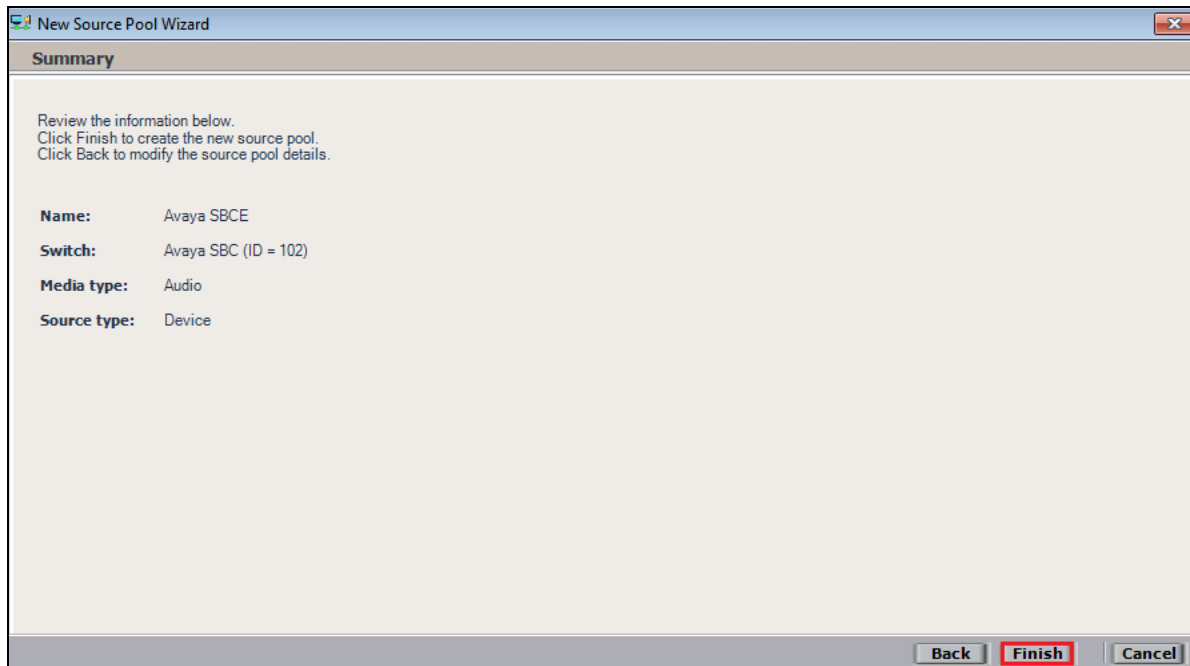
Find:

Selected: 3/3

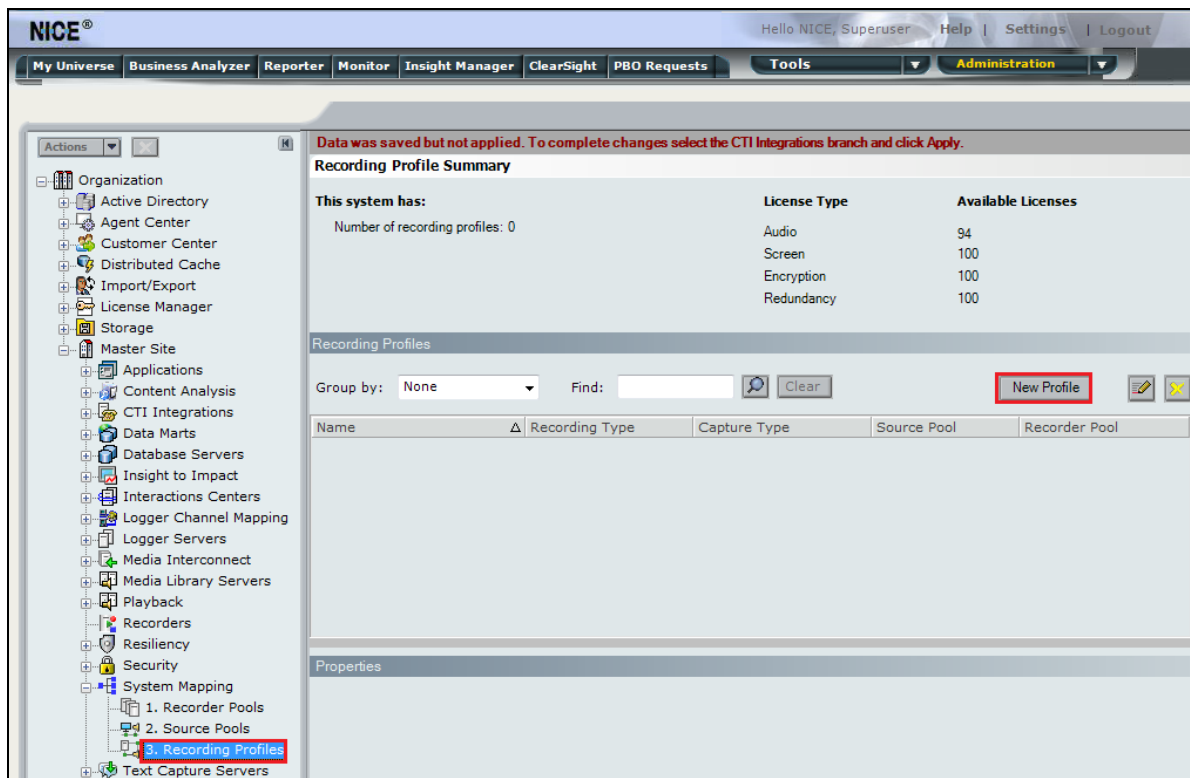
	Name	Device Number	Unique Device ID	IP Address
<input checked="" type="checkbox"/>			3	
<input checked="" type="checkbox"/>			2	
<input checked="" type="checkbox"/>			1	



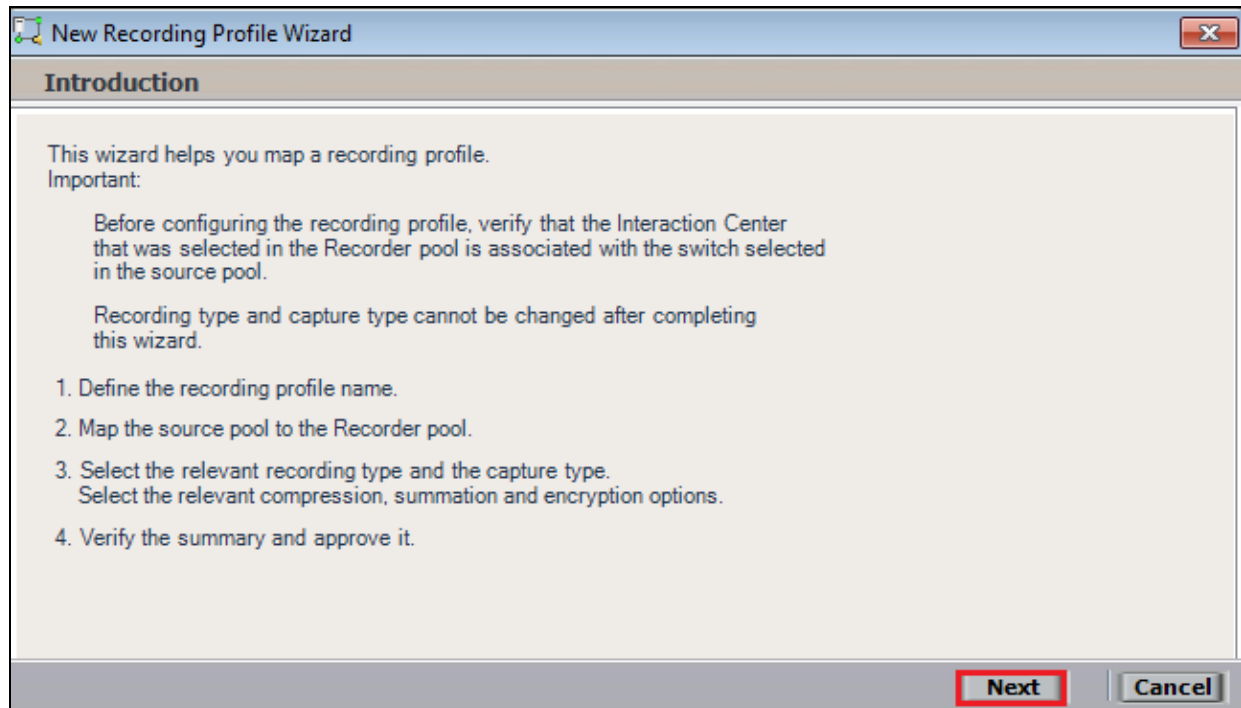
Click on **Finish** to complete the New Source Pool Wizard.



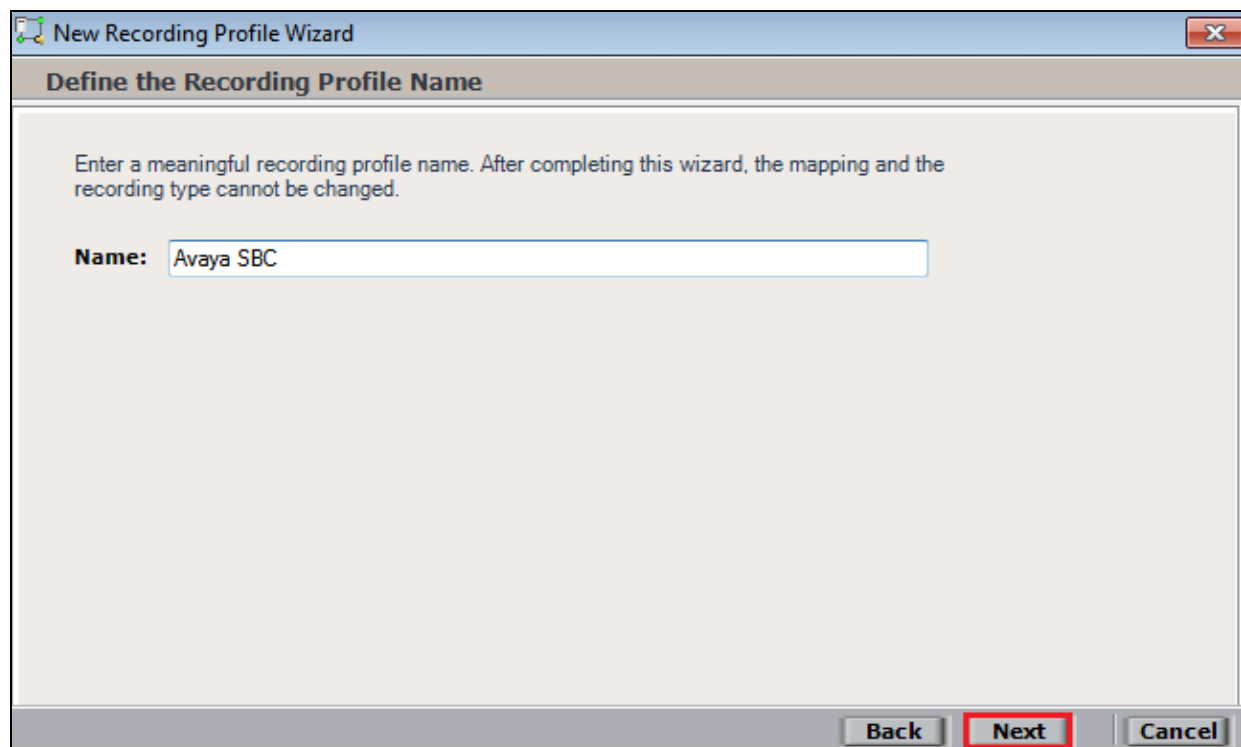
From the left window navigate to **Master Site** → **System Mapping** → **Recording Profiles** and in the main window click on **New Profile**.



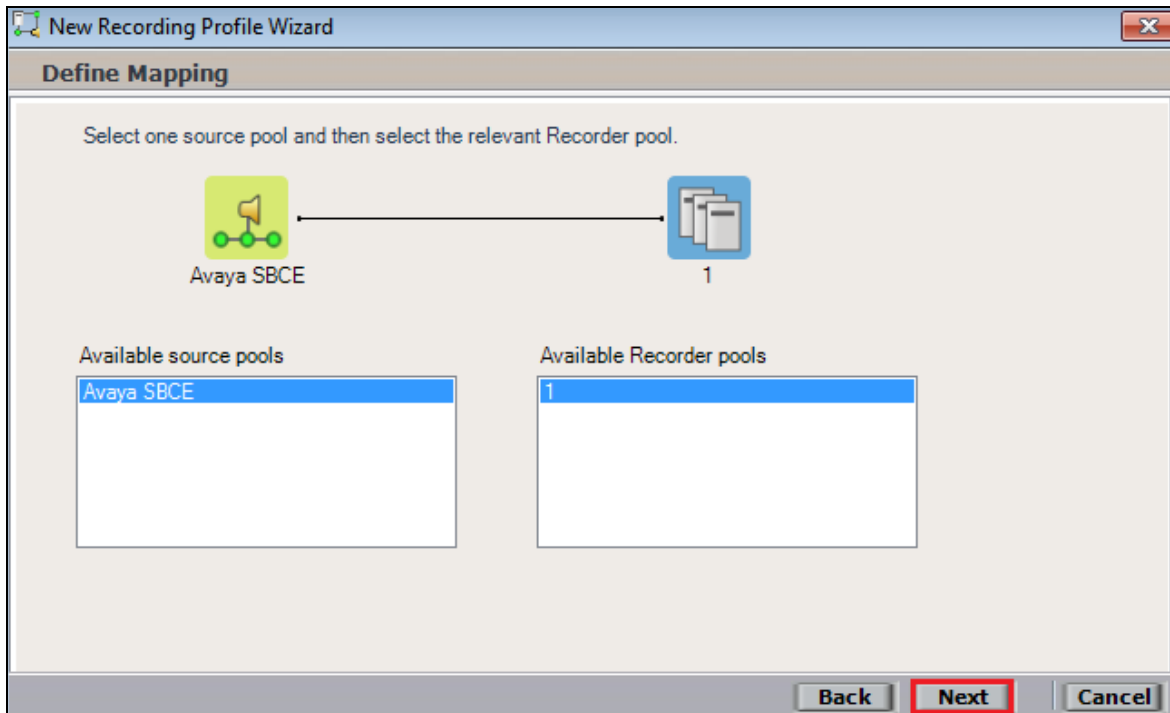
Click on **Next** to continue with the **New Recording Profile Wizard**.



Enter a suitable **Name** for the **Recording Profile** and click on **Next** to continue.



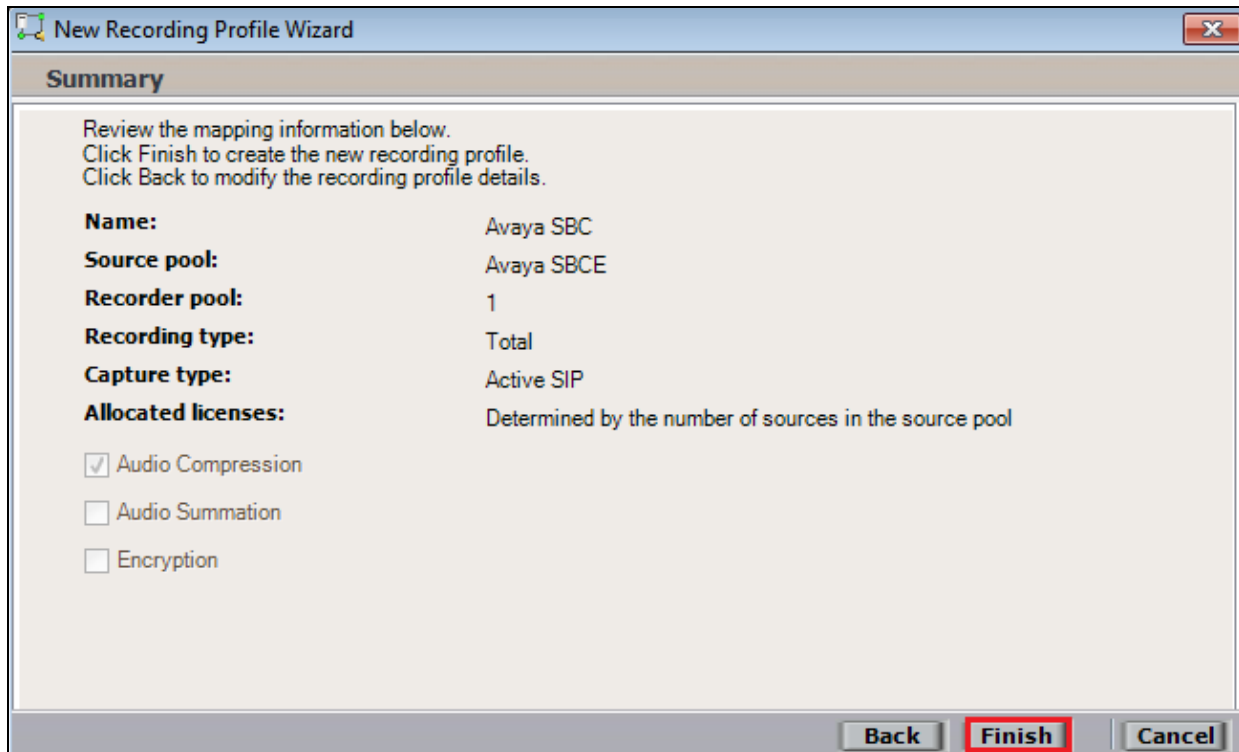
Highlight the **Available source pools** and the **Available Recorder pools** and click on **Next**.



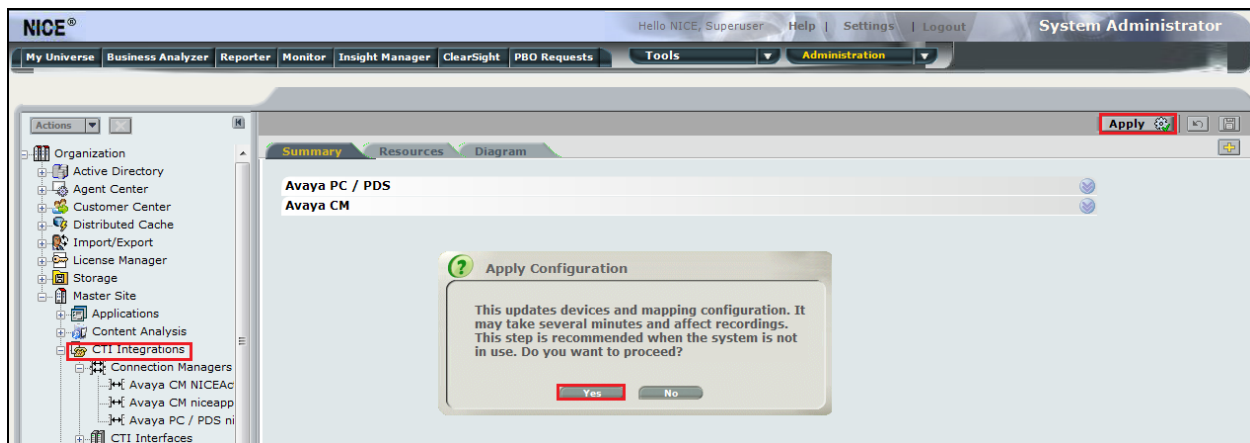
The **Recording type** should be set to **Total** and the **Capture type** should be set to **Active SIP**, **Audio Compression** is selected by default. Select **Audio Summation** check box. Click on **Next** to continue.



Click on **Finish** to complete these changes.



To implement these new changes, navigate to **Master Site → CTI Integrations** and from the main window click on **Apply**. Then click on **Yes** to proceed.



This concludes the setup of the NICE Application Server for SIP Call Recording.

## 9. Verification Steps

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

### 9.1. Verify Avaya Aura® Communication Manager CTI Service State

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

status aesvcs cti-link							
AE SERVICES CTI LINK STATUS							
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd	
1	4	no	aes70vmppg	established	18	18	

### 9.2. Verify TSAPI Link

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

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome! User: Cost  
Last login: Tue Nov 24 16:15:05 2015 from 10.10.40.222  
Number of prior failed login attempts: 0  
HostName/IP: aes70vmppg  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.0.0.0.13-0  
Server Date and Time: Wed Nov 25 14:33:01 GMT 2015  
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

User Management

Utilities

Help

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
<input checked="" type="radio"/>	1	cm70vmppg	1	Talking	Mon Nov 23 10:28:15 2015	Online	17	8	15	15	30

Online Offline

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

TSAPI Service Status TLink Status User Status

### 9.3. Verify Session Border Controller Link

This section provides steps that may be performed to verify that the link to the Session Border Controller is running correctly.

**Note:** The IP addresses below may not be the same as those mentioned in previous sections; they only serve as an example to show how to check that the link between the SBC and Session Manager is up and running.

1. From System Manager **Home** screen click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

**Session Manager Entity Link Connection Status**

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: [Session\\_Manager](#)

Summary View

Status Details for the selected Session Manager:

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<a href="#">CM SIP Endpoints</a>	10.10.9.12	5061	TLS	FALSE	UP	200 OK	UP
<a href="#">ASBCE</a>	10.10.9.81	5060	TCP	FALSE	UP	200 OK	UP
<a href="#">CM Trunk</a>	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
<a href="#">Messaging</a>	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

2. From Communication Manager SAT interface run the command **status trunk n** where **n** is the previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 2
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00011	in-service/idle	no
0002/002	T00012	in-service/idle	no
0002/003	T00013	in-service/idle	no
0002/004	T00014	in-service/idle	no
0002/005	T00015	in-service/idle	no
0002/006	T00016	in-service/idle	no
0002/007	T00017	in-service/idle	no
0002/008	T00018	in-service/idle	no
0002/009	T00019	in-service/idle	no
0002/010	T00020	in-service/idle	no

3. To define a trace on the Avaya SBCE, navigate to **Device Specific Settings** → **Advanced Options** → **Troubleshooting** → **Trace** in the main menu on the left hand side and select the **Packet Capture** tab.
  - Select the SIP Trunk interface from the **Interface** drop down menu.
  - Select the signalling interface IP address or **All** from the **Local Address** drop down menu.
  - Enter the IP address of the network SBC in the **Remote Address** field or enter a \* to capture all traffic.
  - Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example.
  - Specify the filename of the resultant pcap file in the **Capture Filename** field.
  - Click on **Start Capture**.

Trace: GSSCP\_V9

Devices  
GSSCP\_V9

Packet Capture

Captures

Packet Capture Configuration

Status

Ready

Interface

B1

Local Address  
IP[:Port]

192.168.122.59 :

Remote Address  
\*, \*.Port, IP, IP:Port

\*

Protocol

All

Maximum Number of Packets to Capture

10000

Capture Filename  
Using the name of an existing capture will overwrite it.

SIP\_Trunk\_Test.pcap

Start Capture

Clear

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

Trace: GSSCP\_V9

Devices  
GSSCP\_V9

Packet Capture

Captures

Refresh

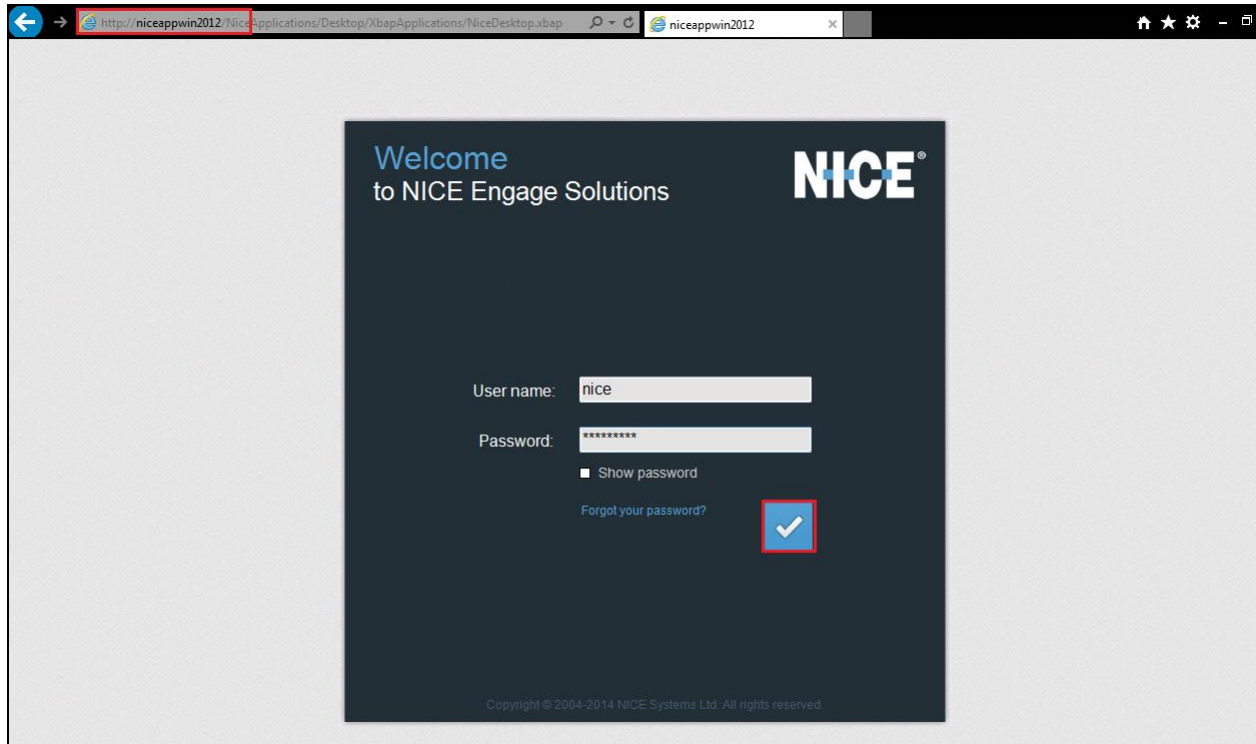
File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20160817083716.pcap	69,632	August 17, 2016 9:04:44 AM IST	Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response to OPTIONS in the form of a 200 OK will be seen from the PSTN network.

## 9.4. Verify calls are being recorded

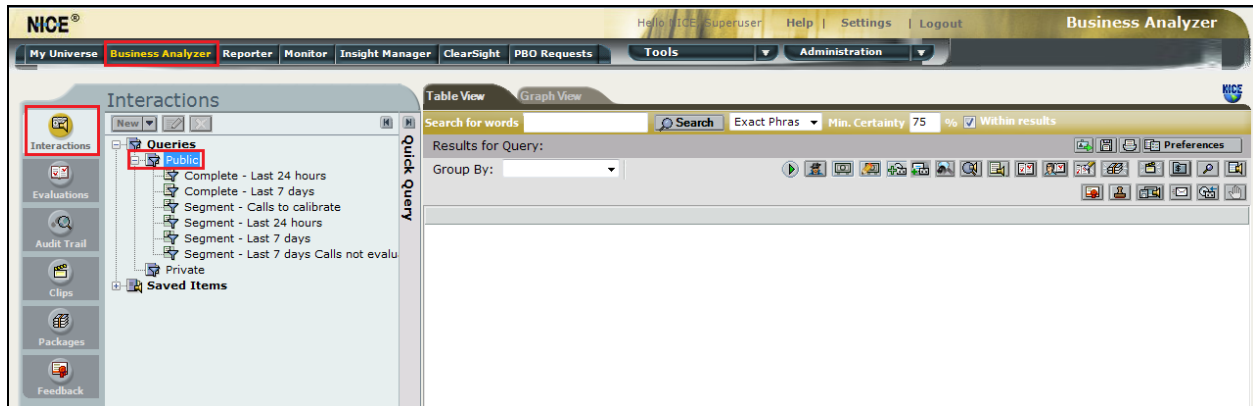
From any of the monitored Avaya endpoints make a series of inbound and outbound calls. Once these calls are completed they should be available for playback through a web browser to the NICE Application Server.

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

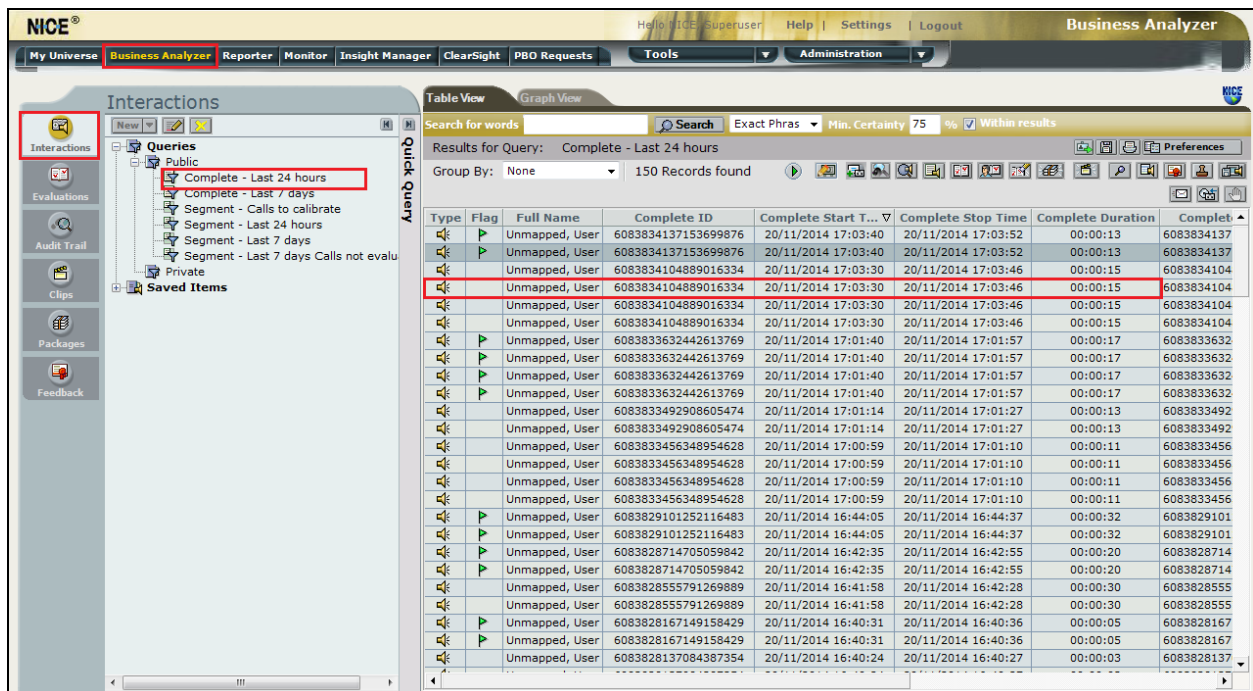




Click on **Business Analyser** at the top of the screen. Select **Interactions** from the left window and then navigate to **Queries** → **Public**.



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



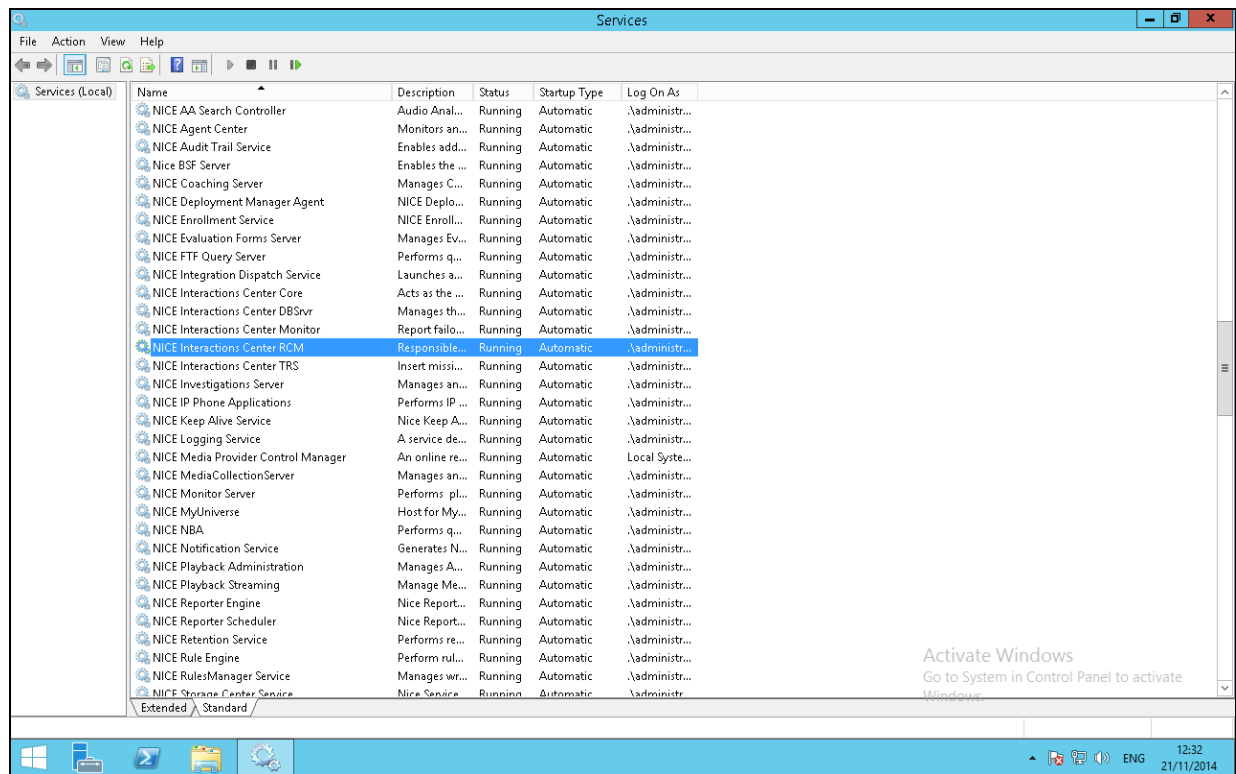
The NICE player is opened and the recording is presented for playback. Click on the **Play/Pause** icon highlighted below to play back the recording.

The screenshot displays the NICE Business Analyzer interface. The top navigation bar includes 'My Universe', 'Business Analyzer', 'Reporter', 'Monitor', 'Insight Manager', 'ClearSight', 'PBO Requests', 'Tools', and 'Administration'. The 'Business Analyzer' tab is active. The main area shows a recording playback interface with a timeline and a list of events. The 'Play/Pause' button is highlighted with a red box. The interface also includes a sidebar with 'Interactions', 'Evaluations', 'Audit Trail', 'Clips', 'Packages', and 'Feedback'. The bottom section shows a table of events with columns for 'Time', 'Agent', and 'Event'.

Time	Agent	Event
12:41:49	7101, Avaya 9630 S...	
12:41:52	7100, Avaya 9641 S...	
12:41:56		
12:41:59		
12:42:03		
12:42:08		

## 9.5. 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.



## 10. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform to successfully interoperate with Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 using SIP recording to record calls coming through the Session Border Controller. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

## 11. Additional References

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

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

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 7.0
- [4] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1 Issue 2
- [5] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1 Issue 1

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

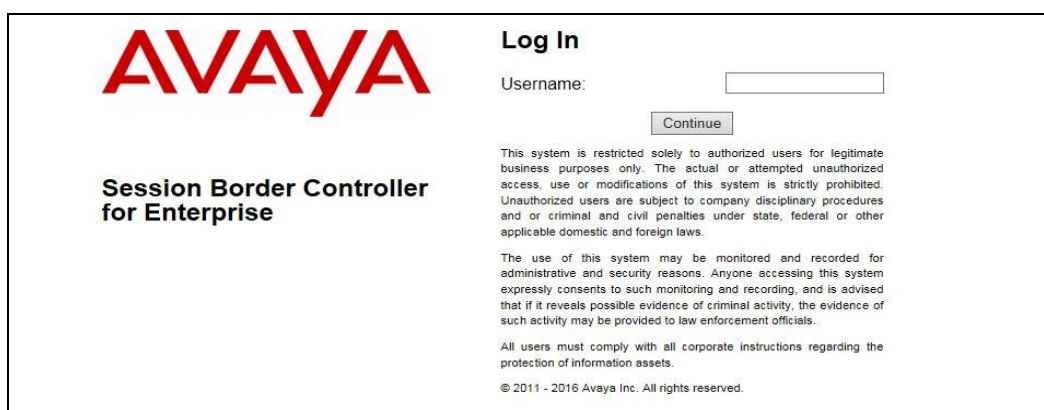
## 12. Appendix A

This section shows the complete setup for the Avaya Session Border Controller for Enterprise (Avaya SBCE) in order to allow SIP trunk calls pass from the WAN (external) to the LAN (internal). The Avaya SBCE provides security and manipulation of signaling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

**Note:** In the example below a SIP trunk was setup to another Communication Manager on a different subnet. The internal profile was named Session Manager and the external profile was named PSTN.

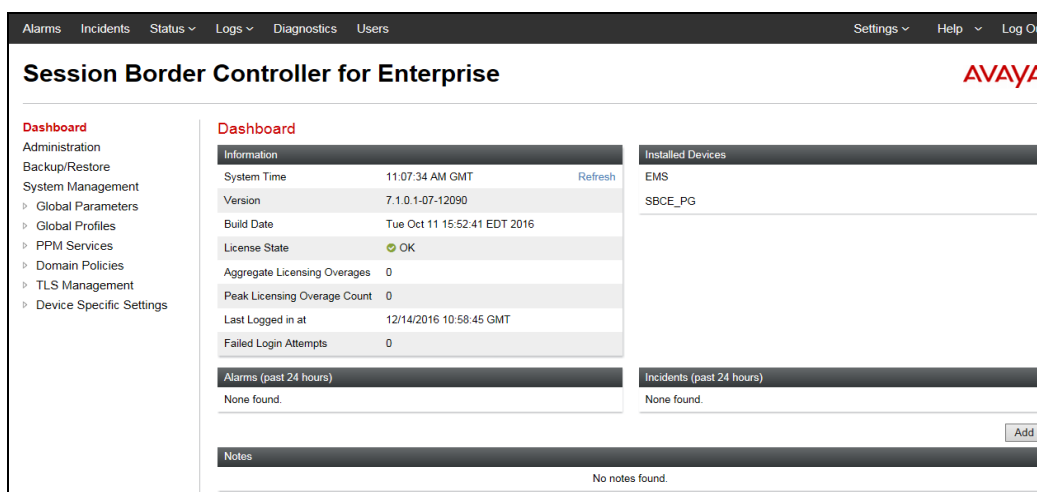
### 12.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



The login screen features the Avaya logo on the left and a 'Log In' section on the right. The 'Log In' section includes a 'Username:' label, a text input field, and a 'Continue' button. Below the input field, there is a disclaimer: 'This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications 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.' This is followed by a consent statement: '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.' A final note states: 'All users must comply with all corporate instructions regarding the protection of information assets.' At the bottom, the copyright notice '© 2011 - 2016 Avaya Inc. All rights reserved.' is displayed.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



The dashboard is titled 'Session Border Controller for Enterprise' and features the Avaya logo in the top right corner. A navigation menu on the left lists various sections: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into several panels. The 'Information' panel displays system details: System Time (11:07:34 AM GMT), Version (7.1.0.1-07-12090), Build Date (Tue Oct 11 15:52:41 EDT 2016), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (12/14/2016 10:58:45 GMT), and Failed Login Attempts (0). The 'Alarms (past 24 hours)' and 'Incidents (past 24 hours)' panels both show 'None found.' The 'Notes' panel at the bottom also shows 'No notes found.' The 'Installed Devices' panel lists 'EMS' and 'SBCE\_PG'. A 'Refresh' button is located next to the System Time, and an 'Add' button is at the bottom right of the dashboard.

## 12.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side and click on **Add**.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address
------	---------	-----------------------------	-----------	------------

Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

IP Address	Public IP	Gateway Override
10.10.16.151	Use IP Address	Use Default

Click on **Add** to define the internal interface. Enter details in the dialogue box (not shown):

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address for the Avaya SBCE in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:

Network Management: SBCE\_PG

Devices: SBCE\_PG

Interfaces Networks

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Internal_A1	10.10.40.1	255.255.255.0	A1	10.10.40.151	Edit	Delete
External_B1	10.10.16.1	255.255.255.0	B1	10.10.16.151	Edit	Delete

Add

Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.

Network Management: SBCE\_PG

Devices: SBCE\_PG

Interfaces Networks

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Disabled

Add VLAN

Message from webpage

Are you sure you wish to change the status of Interface to Enabled?

OK Cancel

**Note:** to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box (not shown) will appear that will indicate when the restart is complete.

## 12.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TCP used for transport of signalling between Session Manager and the Avaya SBCE, and TCP for transport of signalling between the Avaya SBCE and the PSTN SIP Trunk. A signalling and media interface was required on both the internal and external sides of the Avaya SBCE. This document shows the configuration for TCP, if additional security is required it's recommended to use TLS and port 5061.

### 12.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** in the main menu on the left hand side. Details of transport protocol and ports for the external and internal SIP signalling are entered here.

- Select **Add** (not shown) and enter details of the external signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 12.2**. In the test environment, this was IP address **10.10.16.151** for the Avaya SBCE interface on the SIP Trunk.
- Enter the TCP port number in the **TCP Port** field, **5060** is used for the PSTN SIP Trunk.
- Click on **Finish**.

Add Signaling Interface	
Name	External_Sig
IP Address	External_B1 (B1, VLAN 0) 10.10.16.151
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	
<b>Finish</b>	



The internal signalling interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TCP** port number, **5060** is used for Session Manager.

The following screenshot shows details of the signalling interfaces:

**Signaling Interface: SBCE\_PG**

Devices  
SBCE\_PG

**Signaling Interface**

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Internal_Sig	10.10.40.151 Internal_A1 (A1, VLAN 0)	5060	5060	---	None	Edit Delete
External_Sig	10.10.16.151 External_B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete

**Note:** In the test environment, the internal IP address was **10.10.40.151**.

### 12.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** in the main menu on the left hand side. Details of the RTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select **Add** and enter details of the external media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 12.2**. In the test environment, this was IP address **10.10.16.151**.
- Define the **RTP Port Range** for the media path with the PSTN SIP Trunking, during testing this was left at default values of **35000 - 40000**.

System Management

- ▶ Global Parameters
- ▶ Global Profiles
- ▶ PPM Services
- ▶ Domain Policies
- ▶ TLS Management
- ▶ Device Specific Settings
  - Network Management
  - Media Interface**

**Add Media Interface**

Name: External\_Media

IP Address: External\_B1 (B1, VLAN 0)

10.10.16.151

Port Range: 35000 - 40000

Finish

The internal media interfaces are defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

Media Interface: SBCE\_PG

Devices  
SBCE\_PG

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP Network	Port Range	
Internal_Media	10.10.40.151 Internal_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
External_Media	10.10.16.151 External_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

**Note:** In the test environment, the internal IP address was **10.10.40.151** and the port range was left at default values.

## 12.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the PSTN SIP Trunking service is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the PSTN SIP Trunking service, click on **Add** (not shown). A pop-up menu is generated. In the **Name** field enter a descriptive name for the PSTN network and click **Next**.

System Management

- Global Parameters
- Global Profiles
  - Domain DoS
  - Server Interworking**

Interworking Profile X

Profile Name NICESIPREC X

Next

PSTN's preferred method of fax transmission is via G.711 so T.38 support is not necessary. This document shows how to define it however, as it may be required in the future.

Check the **T.38 Support** box and click on **Next**.

**Interworking Profile**

**General**

Hold Support: ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling: ☒ None ☐ SDP ☐ No SDP

181 Handling: ☒ None ☐ SDP ☐ No SDP

182 Handling: ☒ None ☐ SDP ☐ No SDP

183 Handling: ☒ None ☐ SDP ☐ No SDP

Refer Handling: ☐

URI Group:

Send Hold: ☒

Delayed Offer: ☒

3xx Handling: ☐

Diversion Header Support: ☐

Delayed SDP Handling: ☐

Re-Invite Handling: ☐

Prack Handling: ☐

Allow 18X SDP: ☐

**T.38 Support: ☒**

URI Scheme: ☒ SIP ☐ TEL ☐ ANY

Via Header Format: ☒ RFC3261 ☐ RFC2543

Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

**Interworking Profile**

All fields are optional.

**SIP Timers**

Min-SE:  seconds, [90 - 86400]

Init Timer:  milliseconds, [50 - 1000]

Max Timer:  milliseconds, [200 - 8000]

Trans Expire:  seconds, [1 - 64]

Invite Expire:  seconds, [180 - 300]

**Interworking Profile**

**Privacy**

Privacy Enabled: ☐

User Name:

P-Asserted-Identity:

P-Preferred-Identity:

Privacy Header:

In the final dialogue box, leave the **Record Routes** at the default setting of **None** and ensure that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk. Click on **Finish**.

Repeat the process to define Server Interworking for Session Manager using the same parameter settings apart from **Record Routes** which is set to **Both Sides** as the Session Manager uses the Record-Route header.

## 12.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. The PSTN SIP Trunk is connected as a Trunk Server. Session Manager is connected as a Call Server.

To define the PSTN SIP Trunking Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** (not shown) and enter an appropriate name in the pop-up menu.

Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the PSTN SIP Trunking IP address.
- In the **Port** box, enter the port to be used for the SIP Trunk.
- In the **Transport** drop down menu, select **TCP**.
- Click on **Next**.

IP Address / FQDN	Port	Transport
10.10.16.77	5060	TCP

Click on **Next** and **Next** again. Leave the fields in the dialogue boxes at default values.

Authentication	Heartbeat
Enable Authentication	Enable Heartbeat
User Name	Method: OPTIONS
Realm	Frequency
Password	From URI
Confirm Password	To URI

Click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for PSTN SIP Trunking defined in **Section 12.4**.
- Leave the other fields at default settings.
- Click **Finish**.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	NICESIPREC
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061

Use the process described to define the Call Server configuration for Session Manager if not already defined.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box (not shown).
- Ensure that the Interworking Profile defined for Session Manager in **Section 12.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box (not shown).

The following screenshots show the **General** and **Advanced** tabs of the completed Server Configuration:

**Server Configuration: PSTN**

Buttons: Add, Rename, Clone, Delete

Server Profiles: PSTN, Session Manager, NICESIPREC

Tabs: General, Authentication, Heartbeat, Advanced

General Tab:

Server Type: Trunk Server

IP Address / FQDN	Port	Transport
10.10.16.77	5060	TCP

Edit

Advanced Tab:

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile: None

Signaling Manipulation Script: None

Securable ☐

Enable FGDN ☐

Edit

## 12.6. Define Routing

Routing information is required for routing to the PSTN SIP Trunking on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling. To define routing to PSTN SIP Trunking, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** (not shown) and enter an appropriate name in the dialogue box.

Global Profiles

- Domain DoS
- Server Interworking
- Media Forking
- Routing**

**Routing Profile** X

Profile Name: PSTN x

Next

Click on **Next** and enter details for the Routing Profile for the SIP Trunk:

- During testing, **Load Balancing** was not required and was left at the default value of **Priority**.
- Click on **Add** to specify an IP address for the SIP Trunk.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration defined in **Section 12.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

Profile : PSTN - Edit Rule

URI Group: \*  
Time of Day: default  
Load Balancing: Priority  
NAPTR: ☐  
Transport: None  
Next Hop Priority: ☒  
Next Hop In-Dialog: ☐  
Ignore Route Header: ☐  
ENUM: ☐  
ENUM Suffix:   
  
Add  
  
Priority / Weight: 1  
Server Configuration: PSTN  
Next Hop Address: 10.10.16.77:5060 (TCP)  
Transport: None  
Delete  
  
Finish

Repeat the process for the Routing Profile for Session Manager. In the test environment, this was called “PSTN” and the Server Configuration was “PSTN”.

## 12.7. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop or external interfaces.

To define Topology Hiding for PSTN SIP Trunking, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Click on **Add** (not shown) to bring up a dialogue box, assign an appropriate name and click on **Next** to configure Topology Hiding for each header as required:

Topology Hiding Profile

Profile Name: PSTN  
Next

Enter details in the **Topology Hiding Profile** pop-up menu.

- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing the default **IP/Domain** was used for all headers that hide both domain names and IP addresses.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

The following screenshot shows the completed **Topology** Hiding configuration for the PSTN SIP Trunk.

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---



To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for PSTN SIP Trunking. Do this by highlighting the profile defined for PSTN and clicking on **Clone**. Enter an appropriate name for Session Manager and click on **Next** (not shown). Make any changes where required, in the test environment the settings were left at the same values.

**Topology Hiding Profiles: Session Manager**

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco\_th\_profile

PSTN

**Session Manager**

Click here to add a description.

**Topology Hiding**

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

Edit

## 12.8. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 12.9**. During testing of PSTN SIP Trunking, a Signalling Rule was used so an End Point Policy Group was also required to apply it to the Server Flow.

### 12.8.1. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to handle any incompatible signalling that may be encountered on the SIP Trunk of a particular Service Provider. To define a signalling rule to remove the Proxy-Require header, navigate to **Domain Policies → Signaling Rules** in the main menu on the left hand side. Click on **Add** (not shown) and enter details in the Signaling Rule pop-up box. In the **Rule Name** field enter a descriptive name for the signalling rule, in this case **NICESIPREC**.

**Signaling Rule** X

Rule Name

Next

Click on **Next** 3 times leaving the settings at default values then click on **Finish**.

The figure displays three sequential screenshots of the 'Signaling Rule' configuration interface, showing the progression from Inbound/Outbound settings to Content-Type Policy, QoS, and finally UCID settings.

**Signaling Rule (Inbound/Outbound):**

- Inbound:**
  - Requests: Allow (403 Forbidden)
  - Non-2XX Final Responses: Allow (486 Busy Here)
  - Optional Request Headers: Allow (403 Forbidden)
  - Optional Response Headers: Allow (486 Busy Here)
- Outbound:**
  - Requests: Allow (403 Forbidden)
  - Non-2XX Final Responses: Allow (486 Busy Here)
  - Optional Request Headers: Allow (403 Forbidden)
  - Optional Response Headers: Allow (486 Busy Here)

**Signaling Rule (Content-Type Policy):**

- Enable Content-Type Checks: ☒
- Action: Allow
- Multipart Action: Allow
- Exception List: Separate with line breaks

**Signaling Rule (QoS):**

- Enabled: ☒
- ToS:
  - Precedence: Routine (000)
  - ToS: Minimize Delay (1000)
- DSCP:
  - Value: CS3 (101110)

**Signaling Rule (UCID):**

- Enabled: ☐
- Node ID:
- Protocol Discriminator: 0x00

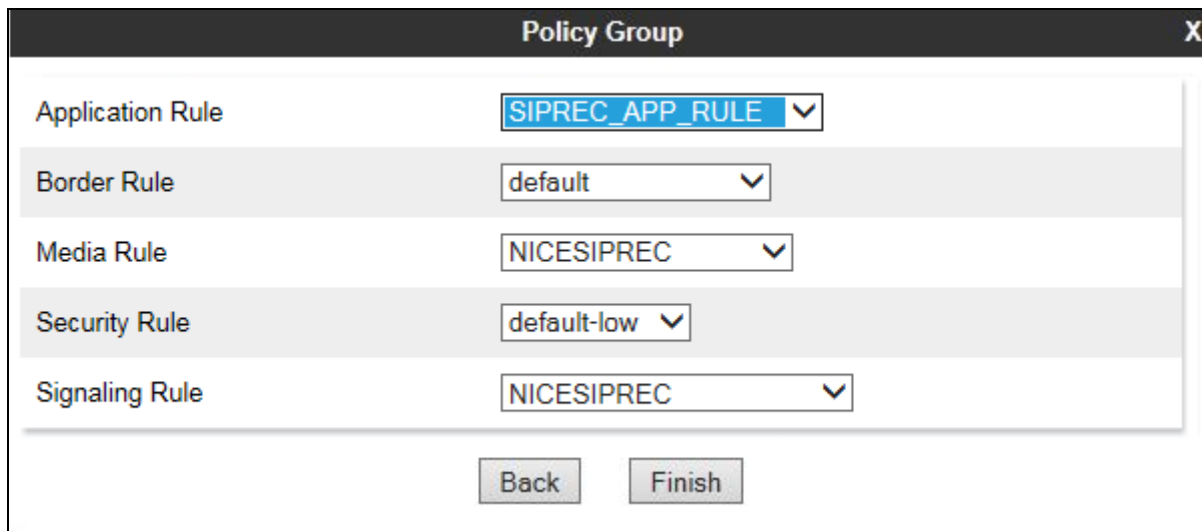
## 12.8.2. End Point Policy Groups

End Point Policy Groups are required to implement the signalling rules. To define one for use in the SIP Trunk server flow to remove the Proxy-Require header, navigate to **Domain Policies** → **End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up box.

The figure shows the 'End Point Policy Groups' configuration dialog. The left sidebar lists 'Media Rules', 'Security Rules', 'Signaling Rules', and 'End Point Policy Groups' (highlighted). The main area shows the 'Policy Group' configuration with a 'Group Name' field containing 'NICESIPREC' and a 'Next' button.

Click on **Next** to configure the Policy Set. Enter details as follows:

- Leave the **Border Rule** and **Security Rule** at their default values.
- Select the **Application Rule** and **Signaling Rule** created in the previous sections in the drop down menu.
- Click on **Finish**.



The screenshot shows a 'Policy Group' configuration window. It contains five rows, each with a label and a dropdown menu. The 'Application Rule' dropdown is set to 'SIPREC\_APP\_RULE'. The 'Border Rule' dropdown is set to 'default'. The 'Media Rule' dropdown is set to 'NICESIPREC'. The 'Security Rule' dropdown is set to 'default-low'. The 'Signaling Rule' dropdown is set to 'NICESIPREC'. At the bottom of the window, there are two buttons: 'Back' and 'Finish'.

Label	Value
Application Rule	SIPREC_APP_RULE
Border Rule	default
Media Rule	NICESIPREC
Security Rule	default-low
Signaling Rule	NICESIPREC

Buttons: Back, Finish

## 12.9. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the PSTN SIP Trunking service. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the PSTN SIP Trunk and vice versa.

To define a Server Flow for the PSTN SIP Trunk, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab (not shown).
- Select **Add Flow** (not shown) and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for the PSTN SIP Trunk, in the test environment **Network** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the PSTN SIP Trunk defined in **Section 12.5**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 12.3**. This is the interface that signalling bound for the SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 12.3**. This is the interface that signalling bound for the SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 12.3**. This is the interface that media bound for the SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 12.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the PSTN SIP Trunk defined in **Section 12.7** and click **Finish**.

Edit Flow: PSTN	
Flow Name	PSTN
Server Configuration	PSTN
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal_Sig
Signaling Interface	External_Sig
Media Interface	External_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Session Manager
Topology Hiding Profile	PSTN
Signaling Manipulation Script	None
Remote Branch Office	Any
<b>Finish</b>	

To define a Server Flow for Session Manager, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab (not shown).
- Select **Add Flow** (not shown) and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Session Manager** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 12.5**.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 12.3**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 12.3**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 12.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the PSTN SIP Trunking defined in **Section 12.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 12.7** and click **Finish**.

**Edit Flow: Session Manager** [X]

Flow Name	Session Manager [X]
Server Configuration	Session Manager [v]
URI Group	* [v]
Transport	* [v]
Remote Subnet	* [ ]
Received Interface	External_Sig [v]
Signaling Interface	Internal_Sig [v]
Media Interface	Internal_Media [v]
Secondary Media Interface	None [v]
End Point Policy Group	default-low [v]
Routing Profile	PSTN [v]
Topology Hiding Profile	Session Manager [v]
Signaling Manipulation Script	None [v]
Remote Branch Office	Any [v]

**Finish**

The information for all **Server Flows** is shown on a single screen on the Avaya SBCE.

End Point Flows: SBCE\_PG

Devices

SBCE\_PG

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: PSTN

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
<input type="text" value="1"/>	PSTN	*	Internal_Sig	External_Sig	default-low	Session Manager	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

Server Configuration: Session Manager

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
<input type="text" value="1"/>	Session Manager	*	External_Sig	Internal_Sig	default-low	PSTN	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

## 13. Appendix B

### Avaya one-X® Agent Softphone

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

display station 2100	Page 1 of 5	
STATION		
Extension: 2100	Lock Messages? n	BCC: 0
Type: 9630	Security Code: *	TN: 1
Port: S00031	Coverage Path 1:	COR: 1
Name: one-X Agent1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern:	1
	Message Lamp Ext:	2100
Speakerphone: 2-way	Mute Button Enabled?	y
Display Language: english	Button Modules:	0
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone?	y
	IP Video Softphone?	n
	Short/Prefixed Registration Allowed:	default
	Customizable Labels?	Y

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

display station 2100	STATION	Page 3 of 5
<p>Conf/Trans on Primary Appearance? n</p> <p>Bridged Appearance Origination Restriction? n</p>		
<p>Call Appearance Display Format: disp-param-default</p> <p>IP Phone Group ID:</p> <p>Enhanced Callr-Info Display for 1-Line Phones? n</p>		
ENHANCED CALL FORWARDING		
	Forwarded Destination	Active
Unconditional For Internal Calls To: 1000		n
External Calls To: 1000		n
Busy For Internal Calls To:		n
External Calls To:		n
No Reply For Internal Calls To:		n
External Calls To:		n
SAC/CF Override: n		

display station 2100	STATION	Page 4 of 5
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5: manual-in	Grp:
2: call-appr	6: after-call	Grp:
3: call-appr	7: aux-work	RC: Grp:
4: auto-in	8:	
	Grp:	
voice-mail		



## Avaya 9608 H.323 Deskphone

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

display station 2001	Page 1 of 5	
STATION		
Extension: 2001	Lock Messages? n	BCC: 0
Type: 9608	Security Code: *	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: Ext2001	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 2001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: yes	
	Customizable Labels? y	

display station 2001	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	
	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	EC500 State: enabled
Multimedia Mode: enhanced	Audible Message Waiting? n
MWI Served User Type: sip-adjunct	Display Client Redirection? n
	Select Last Used Appearance? n
	Coverage After Forwarding? s
	Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y
Emergency Location Ext: 2001	Always Use? n IP Audio Hairpinning? n

display station 2001Page 3 of 5

STATION

Conf/Trans on Primary Appearance? n

Bridged Appearance Origination Restriction? n

Require Mutual Authentication if TLS? n

Offline Call Logging? y

Call Appearance Display Format: disp-param-default

IP Phone Group ID:

Enhanced Callr-Info Display for 1-Line Phones? n

ENHANCED CALL FORWARDING

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

SAC/CF Override: n

display station 2001Page 4 of 5

STATION

SITE DATA

Room:	Headset? n
Jack:	Speaker? n
Cable:	Mounting: d
Floor:	Cord Length: 0
Building:	Set Color:

ABBREVIATED DIALING

List1:	List2:	List3:
--------	--------	--------

BUTTON ASSIGNMENTS

1: call-appr	5: call-park
2: call-appr	6:
3: call-appr	7:
4: extnd-call	8:
voice-mail	

---

**©2017 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](mailto:devconnect@avaya.com).