



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

---

# **Application Notes for NICE Engage Platform 6.15 with Avaya Proactive Contact 5.2 with PG230 and Avaya Session Border Controller for Enterprise 8.0 – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for NICE Engage Platform 6.15 to interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Session Border Controller for Enterprise 8.0. NICE Engage Platform is a call recording solution.

In the compliance testing, NICE Engage Platform used the Event Services interface from Avaya Proactive Contact to obtain information on calls and agent states, and the SIPREC interface from Avaya Session Border Controller for Enterprise to capture media associated with Proactive Contact outbound calls for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 required for NICE Engage Platform (Engage) 6.15 to interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Session Border Controller for Enterprise (SBCE) 8.0. Engage is a call recording solution.

In the compliance testing, Engage used the Event Services interface from Proactive Contact to obtain information on calls and agent states, and the SIPREC interface from SBCE to capture media associated with Proactive Contact outbound calls for call recording.

When there is an active outbound call at the Proactive Contact agent, Engage is informed of the call via events from the Event Services interface and starts the call recording by use of associated media from the SBCE SIPREC interface. The Event Services events are also used to determine when to stop the call recordings.

Engage can be deployed with distributed components across multiple servers. The compliance testing used two Engage servers in the test configuration – one server running the Application Server, Database Server, and Interactions Center components, and the other server running the Advanced Interaction Recorder component. The Application Server component is responsible for the Engage web interface, the Interactions Center component is responsible for Event Services connection with Proactive Contact as well as SIPREC connection with SBCE, and the Advanced Interaction Recorder component is responsible for media recording.

The compliance testing covered the recording of basic outbound calls that were delivered by Proactive Contact for the PG230 deployment option only. The recording of inbound calls is outside the scope of this compliance test.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Engage application, the application automatically established Event Services connection with Proactive Contact.

For the manual part of testing, each outbound call was handled manually at the agent with generation of unique audio content for recording. Necessary agent actions such as hold and release line were performed from the Proactive Contact Agent application running on the agent desktops.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Engage.

The verification of tests included use of Engage logs for proper message exchanges and use of Engage web interface for proper logging and playback of call recordings.

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

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

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

For the testing associated with these Application Notes, the interfaces between Engage and Avaya products included encrypted Event Services and non-encrypted SIPREC connections as requested by NICE.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Engage:

- Handling of Event Services agent states and call events.
- Use of SIPREC to obtain media from SBCE.
- Proper recording, logging, and playback of calls for scenarios involving agent drop, customer drop, hold, reconnect, simultaneous calls, long duration, multiple agents, and manual call scenarios.

The serviceability testing focused on verifying the ability of Engage to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to Engage.

## 2.2. Test Results

All test cases were executed and verified. The following is an observation on Engage from the compliance testing.

- Recording of transfer, conference, and forward work scenarios are not supported in this release of Engage.

## 2.3. Support

Technical support on Engage can be obtained through the following:

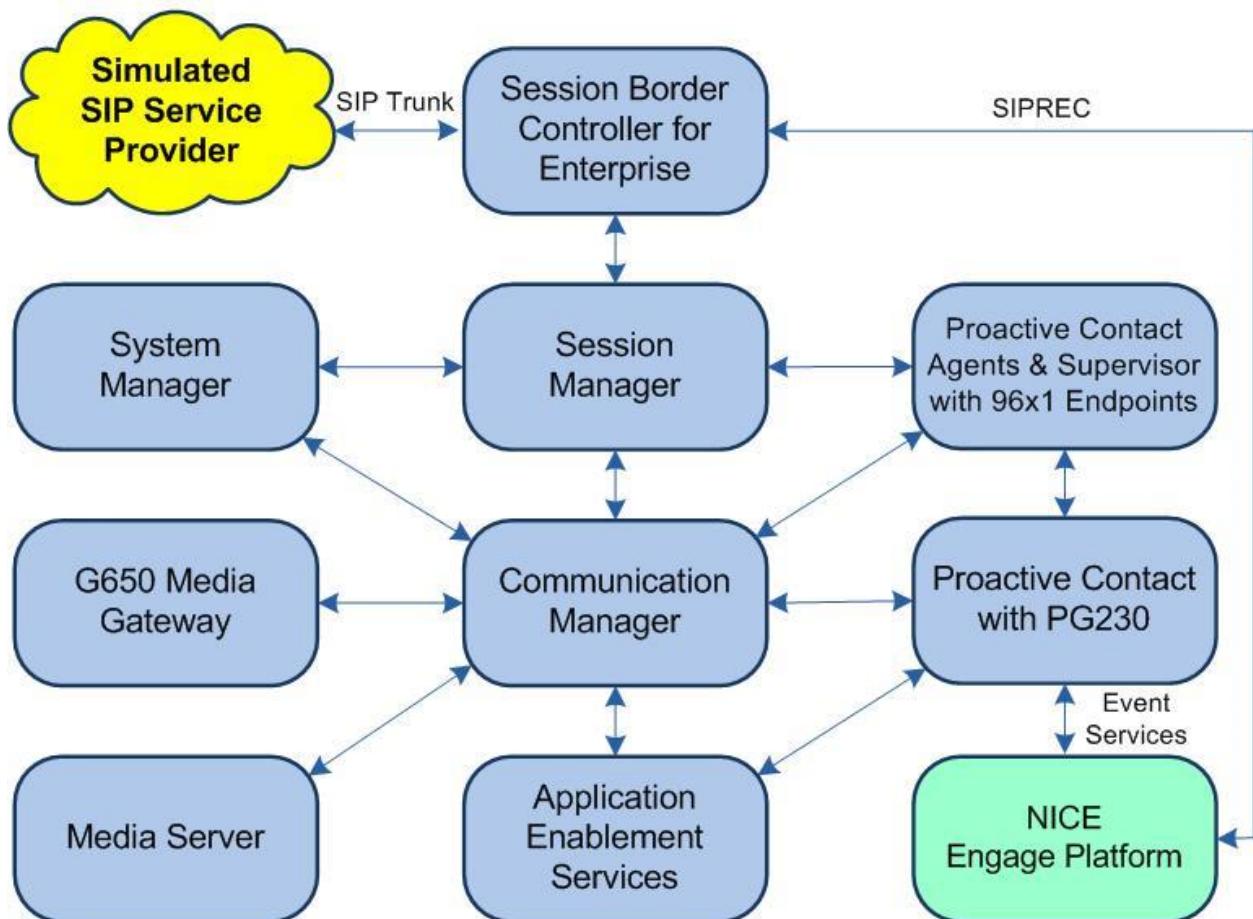
- **Web :** <http://www.extranice.com>

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of connectivity between Proactive Contact, Communication Manager, Session Manager, and SBCE are not the focus of these Application Notes and will not be described.

The agent station extensions used in the compliance testing are shown in the table below.

Device Type	Extension
Agent Station	65001 (H.323), 66006 (SIP)



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.1.1 (8.1.1.0.0.890.25763)
Avaya G650 Media Gateway <ul style="list-style-type: none"> <li>TN464HP DS1 Interface</li> </ul>	NA HW02 FW025
Avaya Aura® Media Server in Virtual Environment	8.0.1.121
Avaya Aura® Session Manager in Virtual Environment	8.1.1 (8.1.1.0.811021)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.0 (8.0.0.0.19-16991)
Avaya Proactive Contact with PG230 <ul style="list-style-type: none"> <li>QT1-PRI</li> </ul>	5.2.0.1 2.19
Avaya Proactive Contact Agent	5.2.0.1
Avaya 9611G IP Deskphone (H.323)	6.8202
Avaya 9641G IP Deskphone (SIP)	7.1.6.1.3
NICE Engage Platform on Windows Server 2016 <ul style="list-style-type: none"> <li>Application Server</li> <li>Interactions Center <ul style="list-style-type: none"> <li>Integrations.NSP.SipRecBase.dll</li> </ul> </li> <li>Database Server</li> <li>Avaya Proactive Contact Event SDK</li> </ul>	6.15.0001.77 Standard  6.15.202.2314  5.1.2
NICE Engage Platform on Windows Server 2016 <ul style="list-style-type: none"> <li>Advanced Interaction Recorder</li> </ul>	6.15.0001.77 Standard

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Administer system parameters features
- Administer IP codec set
- Administer SIP trunk group

### 5.1. Administer System Parameters Features

Log into the System Access Terminal. Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                               Page 5 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                        Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                        COR to Use for DPT: station
                        EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 27
```

## 5.2. Administer Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used by the agent stations. For **Audio Codec**, make certain only variants of G711 and/or G729 codec are configured, as shown below. Note that Engage supports the G711 and G729 codec variants.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size (ms)
1: G.711MU      n           2          20
2: G.729        n           2          20
3:
4:
5:
6:
7:

Media Encryption                                Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
```



### 5.3. Administer SIP Trunk Group

Use the “change trunk-group n” command, where “n” is the trunk group number used by Communication Manager with Session Manager for outbound calls initiated by Proactive Contact. Enter the following values for the specified fields and retain the default values for the remaining fields.

In this case, the pertinent trunk group number is “212”. Navigate to **Page 3**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **UI Treatment:** “shared”
- **Send UCID:** “y”

These settings enable the call ID received from PG230, as part of the user-to-user information element, to be passed to SBCE via Session Manager.

```
add trunk-group 212                                     Page 3 of 5
TRUNK FEATURES
    ACA Assignment? n                                     Measured: none
                                                         Maintenance Tests? y

    Suppress # Outpulsing? n   Numbering Format: private
                                                         UI Treatment: shared
                                                         Maximum Size of UII Contents: 128
                                                         Replace Restricted Numbers? n
                                                         Replace Unavailable Numbers? n

                                                         Hold/Unhold Notifications? y
    Modify Tandem Calling Number: no
    Send UCID? y

    Show ANSWERED BY on Display? y
```

## 6. Configure Avaya Proactive Contact

This section provides the procedures for configuring Proactive Contact. The procedures include the following areas:

- Obtain host name
- Administer master.cfg
- Administer PG230

The configuration of Proactive Contact is performed by Avaya Professional Services. The procedural steps are presented in these Application Notes for informational purpose.

### 6.1. Obtain Host Name

Log in to the Linux shell of the Proactive Contact server. Use the “hostname” command to obtain the host name, which will be used later to configure Engage.

In the compliance testing, the host name of the Proactive Contact server is “lzpds4b”, as shown below.

```
$ hostname  
lzpds4b
```

### 6.2. Administer master.cfg

Use Navigate to the `/opt/avaya/pds/etc` directory and open the **master.cfg** file.

Locate the **SEND\_CALLID\_OUTCALL** parameter and set it to “YES” as shown below. This setting enables the call ID generated by the dialer to be passed to the PG230.

```
SAMPLE:$VOICEDIR/sample  
SCRIPTS:$VOICEDIR/scripts  
SCRNBLD:$VOICEDIR/scrnbld  
SCRN_SPOOLER:pds_pg  
SEND_CALLID_OUTCALL:YES  
SFTPENABLE:NO  
SHELLDIR:$VOICEDIR/shell  
SHELLMSG:$VOICEDIR/language/sh_eng.msg  
SHORTSVRTIME:NO  
SILENCE_DETECTION:NO  
SIMULTANEOUS_ACQUIRES:NO  
SKIP_LOCK_TIME:0  
SM_UPDATE_TIMEOUT:30000  
SNMPENABLE:NO  
SSHA_ENCRYPTION:YES  
SSL:YES
```

### 6.3. Administer ISDN Message Template

Establish a telnet session with PG230 and navigate to the detailed screen for ISDN Message Template 1 shown below. Add an **USR-USER IE** for message template 1, if doesn't exist already. This setting enables the call ID received from the dialer to be passed to Communication Manager in the user-to-user information element.

I S D N   M E S S A G E   T E M P L A T E   S U M M A R Y											
I S D N   M E S S A G E   T E M P L A T E S											
Tmpl	Message	R/T	Tmpl	Message	R/T	Tmpl	Message	R/T	Tmpl	Message	R/T
1	SETUP	T	2	_____	-	3	SETUP	R	4	CALLPROC	T
IE	BEARER					REP ALL			IE	CHAN ID	
DATA	8090A2					PROCESS	CHAN ID		DATA	A98300	
IE	CHAN ID					D FLD 1	CD NUM		IE	USR-USR	
DATA	A98300					D ANI	CP NUM		DATA	04	
IE	CP NUM										
DATA	80										
D ANI											
IE	CD NUM										
DATA	80										
D FLD 1											
IE	USR-USR										
DATA	04										
D FLD 2											

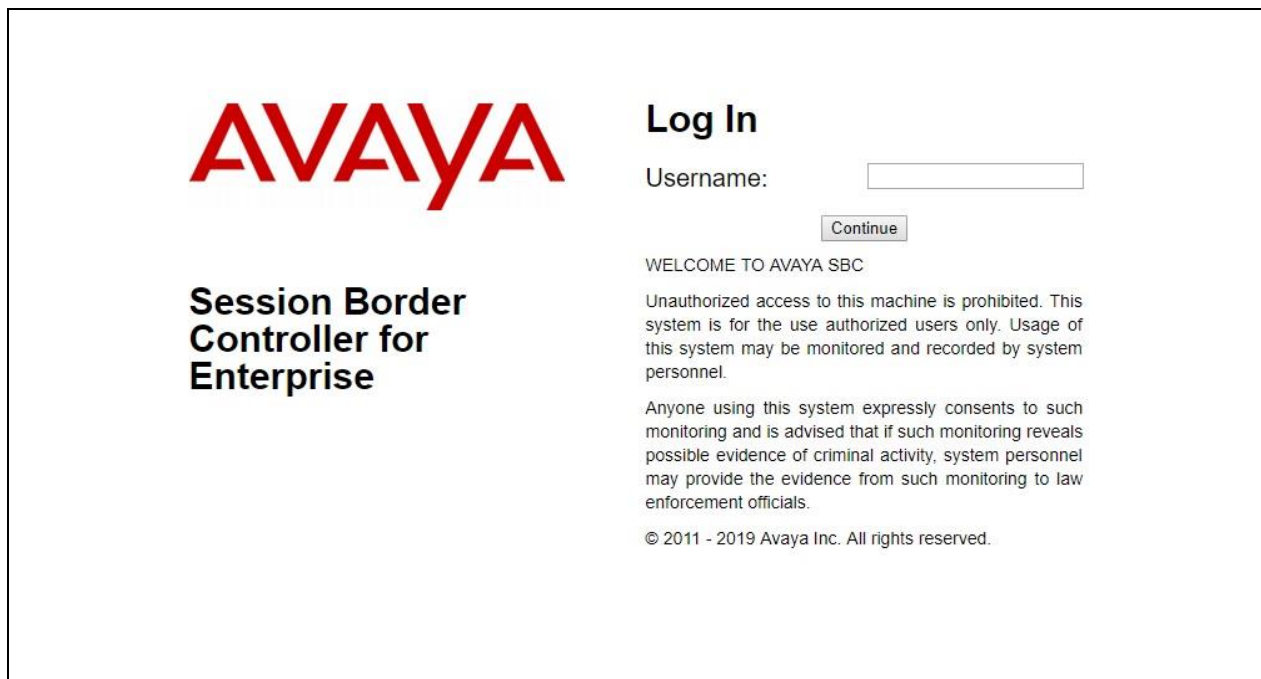
## 7. Configure Avaya Session Border Controller for Enterprise

This section provides the procedures for configuring SBCE. The procedures include the following areas:

- Launch web interface
- Administer SIP servers
- Administer routing
- Administer application rules
- Administer media rules
- Administer signaling rules
- Administer end point policy groups
- Administer session policies
- Administer session flows
- Administer end point flows

### 7.1. Launch Web Interface

Access the SBCE web interface by using the URL “https://ip-address/sbc” in an Internet browser window, where “ip-address” is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



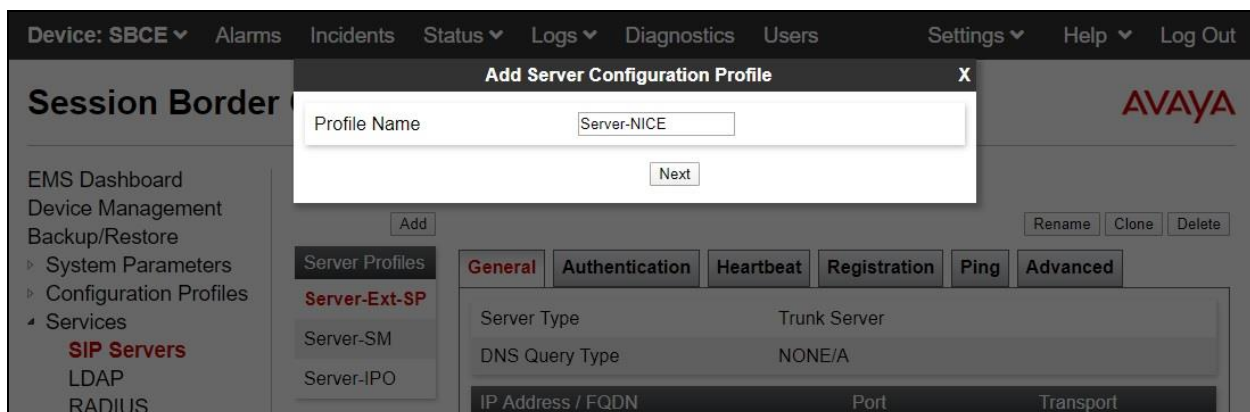
The image shows the login page of the Avaya Session Border Controller for Enterprise (SBCE) web interface. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a disclaimer about unauthorized access, a consent statement, and a copyright notice: "© 2011 - 2019 Avaya Inc. All rights reserved."

## 7.2. Administer SIP Servers

In the subsequent screen, select **Device** → **SBCE** from the top menu, followed by **Backup/Restore** → **Services** → **SIP Servers** from the left pane to display the existing SIP server profiles. Click **Add** to add a SIP server profile for Engage.



The **Add Server Configuration Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.



The **Edit SIP Server Profile – General** pop-up screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Server Type:** “Recording Server”
- **IP Address / FQDN:** IP address of Engage server with the Interactions Center component.
- **Port:** “5060”
- **Transport:** “UDP”

The screenshot shows the 'Edit SIP Server Profile - General' pop-up screen. The background is the Avaya EMS Dashboard. The pop-up has a title bar with 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main content area has a left sidebar with 'Session Border' and 'EMS Dashboard' sections. The 'Session Border' section is expanded, showing 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', and 'Services'. Under 'Services', 'SIP Servers' is selected. The main content area contains the following fields:

- Server Type: Recording Server (dropdown)
- SIP Domain: (text input)
- DNS Query Type: NONE/A (dropdown)
- TLS Client Profile: None (dropdown)
- Buttons: Add, Back, Next

Below the fields is a table with the following data:

IP Address / FQDN	Port	Transport
10.64.101.207	5060	UDP

Buttons: Delete, Back, Next

Navigate to the **Add SIP Server Profile - Advanced** screen. For **Interworking Profile**, select “avaya-ru” which is the default interworking profile for the system. Retain the check in **Enable Grooming** and the default values in the remaining fields.

The screenshot shows the 'Add SIP Server Profile - Advanced' pop-up screen. The background is the Avaya EMS Dashboard. The pop-up has a title bar with 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main content area has a left sidebar with 'Session Border' and 'EMS Dashboard' sections. The 'Session Border' section is expanded, showing 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', and 'Services'. Under 'Services', 'SIP Servers' is selected. The main content area contains the following fields:

- Enable Grooming: ☒
- Interworking Profile: avaya-ru (dropdown)
- Signaling Manipulation Script: None (dropdown)
- Securable: ☐
- Enable FGDN: ☐
- TCP Failover Port: 5060 (text input)
- TLS Failover Port: 5061 (text input)
- Tolerant: ☐
- URI Group: None (dropdown)
- Buttons: Back, Finish

### 7.3. Administer Routing

Select **Backup/Restore → Configuration Profiles → Routing** from the left pane to display the existing routing profiles. Click **Add** to add routing profile for Engage.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

## Session Border Controller for Enterprise AVAYA

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

**Routing**

Topology Hiding

Signaling Manipulation

Routing Profiles: default

**Add** Clone

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

**Routing Profile**

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	DNS/SRV	Auto-Detect	Auto-Detect	<a>Edit</a> <a>Delete</a>

The **Routing Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

## Session Border Controller for Enterprise AVAYA

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

**Routing**

Topology Hiding

Signaling Manipulation

**Routing Profile** X

Profile Name

Next

**Add** Clone

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

**Routing Profile**

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	DNS/SRV	Auto-Detect	Auto-Detect	<a>Edit</a> <a>Delete</a>



The **Routing Profile** pop-up screen is updated. Click **Add** to add a next hop entry. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **SIP Server Profile:** Select the SIP Server profile for Engage from **Section 7.2**.
- **Next Hop Address:** Select the address entry associated with Engage from **Section 7.2**.

The screenshot shows the 'Routing Profile' configuration window. The 'URI Group' is set to a dropdown menu. 'Time of Day' is set to 'default'. 'Load Balancing' is set to 'Priority'. 'Transport' is set to 'None'. 'LDAP Server Profile' is set to 'None'. 'LDAP Base DN (Search)' is set to 'None'. 'Matched Attribute Priority' is checked. 'Next Hop Priority' is checked. 'Ignore Route Header' is unchecked. 'ENUM' is unchecked. 'ENUM Suffix' is an empty text field. Below the form is a table with columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The first row has values: 1, (empty), (empty), (empty), Server-NICE, 10.64.101.207:5060 (UDP), and None. There are 'Add', 'Back', and 'Finish' buttons at the bottom.

## 7.4. Administer Application Rules

Select **Backup/Restore** → **Domain Policies** → **Application Rules** from the left pane to display the existing application rules. Click **Add** to add an application rule for Engage.

The screenshot shows the 'Application Rules: default' page. The 'Add' button is highlighted with a red box. Below the 'Add' button is a table with columns: Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The first row is 'Audio' with In checked, Out checked, Maximum Concurrent Sessions 200, and Maximum Sessions Per Endpoint 5. The second row is 'Video' with In unchecked and Out unchecked. There is a 'Miscellaneous' section below the table. The 'Add' button is also highlighted with a red box.



The **Application Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller

EMS Dashboard  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
    **Application Rules**  
        Border Rules  
        Media Rules  
        Security Rules

Application Rules

- default
- default-trunk
- default-subs...
- default-subs...
- default-serv...

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

#### Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		

The **Application Rule** pop-up screen is updated. Check **Audio In** and **Audio Out**, and enter desired values for **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**, as shown below.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller

EMS Dashboard  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
    **Application Rules**  
        Border Rules  
        Media Rules  
        Security Rules  
        Signaling Rules  
        Charging Rules  
        End Point Policy Groups  
        Session Policies  
▸ TLS Management

Application Rules

- default
- default-trunk
- default-subs...
- default-subs...
- default-serv...

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

#### Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100
Video	<input type="checkbox"/>	<input type="checkbox"/>		

##### Miscellaneous

CDR Support ☒ Off  
☐ RADIUS  
☐ CDR Adjunct

RADIUS Profile None ▾

Media Statistics Support ☐

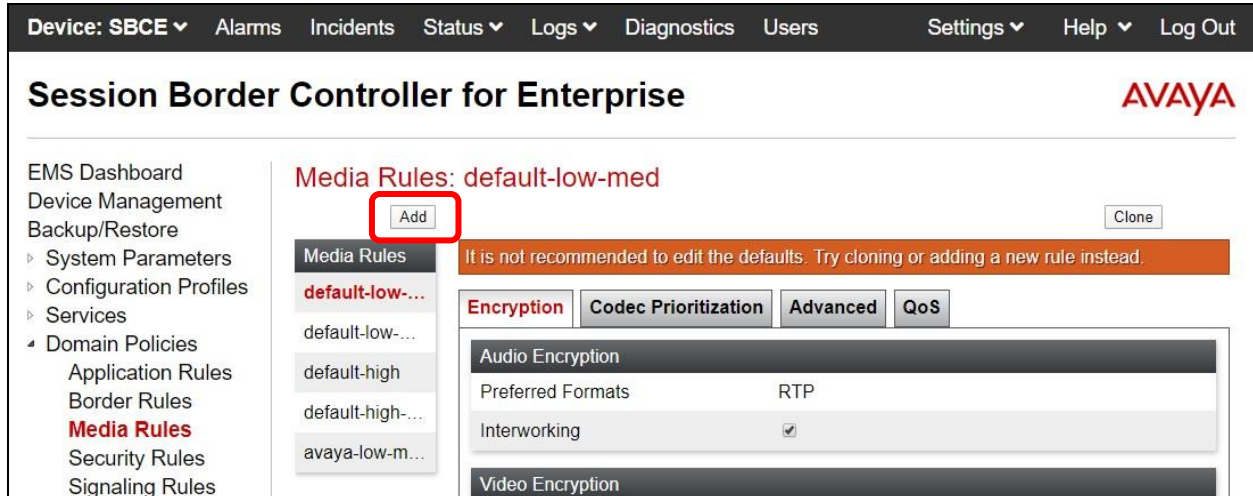
Call Duration ☒ Setup  
☐ Connect

RTP Keep-Alive ☐

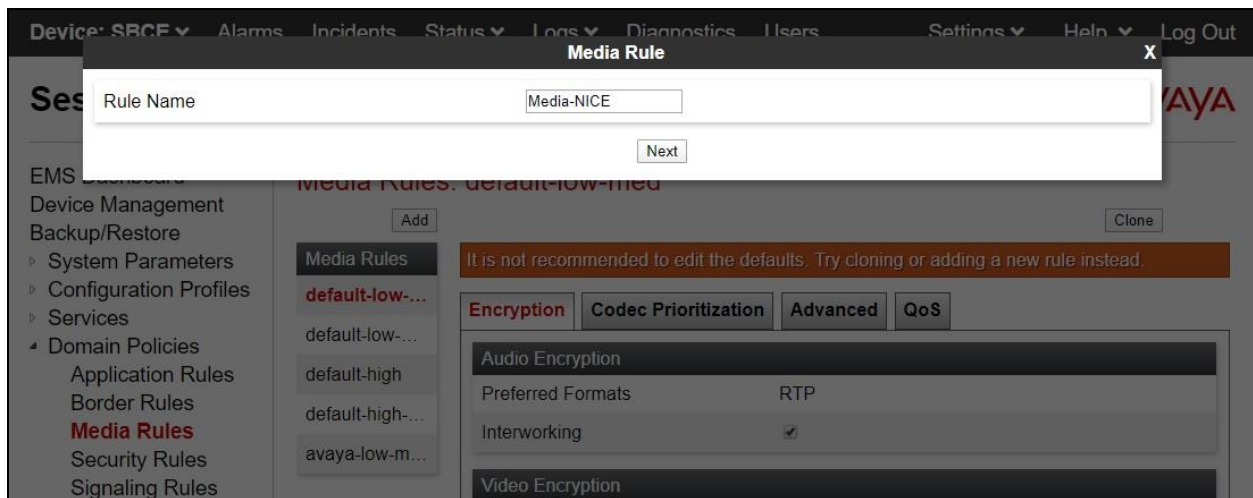
Back Finish

## 7.5. Administer Media Rules

Select **Backup/Restore** → **Domain Policies** → **Media Rules** from the left pane to display the existing media rules. Click **Add** to add a media rule for Engage.



The **Media Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.



The **Media Rule** pop-up screen is updated. Navigate to the **Audio Codec** page. Move the relevant G711 and G729 codec variants from the **Available** column to the **Selected** column, as shown below. Retain the default values in all remaining fields and pages.

The screenshot shows the 'Media Rule' configuration window with the following sections:

### Audio Codec

- Codec Prioritization: ☒ Allow Preferred Codecs Only: ☐
- Transcode: ☐ Transrating: ☐
- Preferred Codecs:
 

Available	P-Time (Optional)	Selected
QCELP (12)	10	PCMU (0) [T] G729 (18) [T]
CN (13)	20	
MPA (14)	30	
G728 (15)	60	
DVI4 (16)		
DVI4 (17)		
G729AB (18) [T]		
G726-32 [DT]		

### Video Codec

- Codec Prioritization: ☐ Allow Preferred Codecs Only: ☐
- Transcode When Needed: ☐ Transrating: ☐
- Preferred Codecs:
 

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

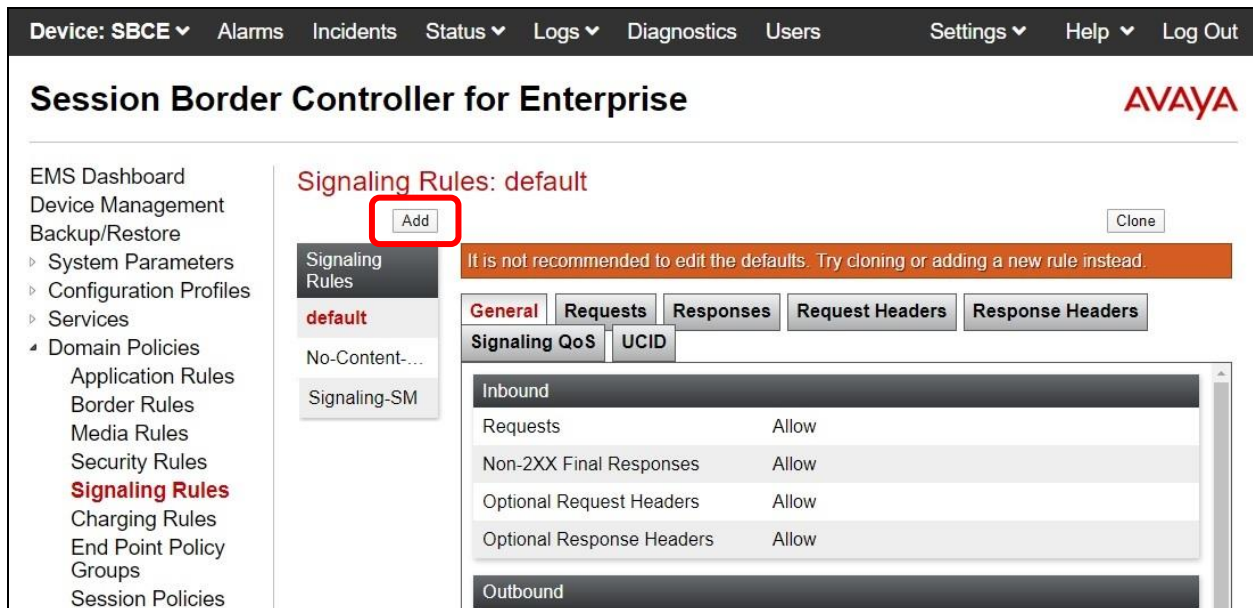
Buttons: Back, Next

## 7.6. Administer Signaling Rules

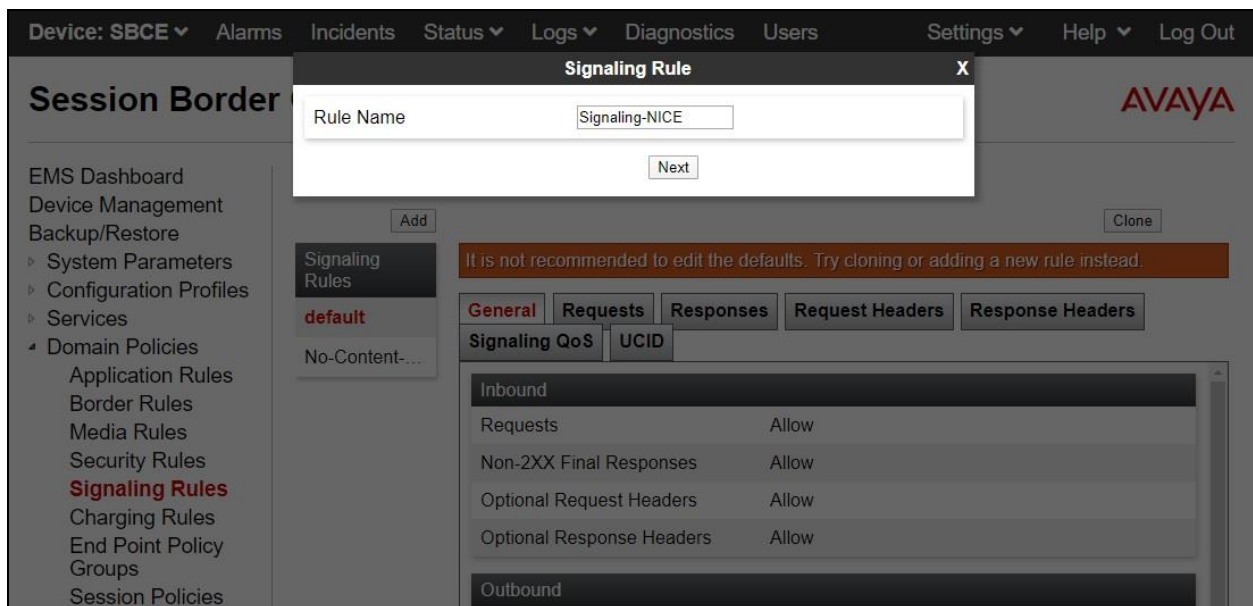
Select **Backup/Restore** → **Domain Policies** → **Signaling Rules** from the left pane to display the existing signaling rules.

### 7.6.1. Engage Signaling Rule

Click **Add** to add a signaling rule for Engage.



The **Signaling Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.



The **Signaling Rule** pop-up screen is updated. Navigate to the **UCID** page. Check **Enabled**. For **Node ID**, enter a unique number across the customer system, in this case “12”. Retain the default value in the remaining field.

The screenshot shows the Avaya Session Border Controller (SBCE) configuration interface. A 'Signaling Rule' pop-up window is open, displaying the 'UCID' tab. The 'Enabled' checkbox is checked. The 'Node ID' field is set to '12', and the 'Protocol Discriminator' is set to '0x00'. The background shows the 'Session Border' configuration page with a sidebar menu and a main content area with tabs for 'General', 'Requests', 'Responses', 'Request Headers', and 'Response Headers'.

## 7.6.2. Session Manager Signaling Rule

Select the existing signaling rule for Session Manager, in this case **Signaling-SM**. Select the **UCID** tab. Make certain that **UCID** is checked, and that **Node ID** is configured, as shown below.

The screenshot shows the Avaya Controller for Enterprise configuration interface. The 'Signaling Rules: Signaling-SM' page is displayed. The 'UCID' tab is selected. The 'Enabled' checkbox is checked. The 'Node ID' field is set to '11', and the 'Protocol Discriminator' is set to '0x00'. The background shows the 'Controller for Enterprise' configuration page with a sidebar menu and a main content area with tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'.



## 7.7. Administer End Point Policy Groups

Select **Backup/Restore** → **Domain Policies** → **End Point Policy Groups** from the left pane to display the existing policy groups. Click **Add** to add a policy group for Engage.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Device Management  
Backup/Restore  
‣ System Parameters  
‣ Configuration Profiles  
‣ Services  
‣ Domain Policies  
 Application Rules  
 Border Rules  
 Media Rules  
 Security Rules  
 Signaling Rules  
 Charging Rules  
**End Point Policy Groups**  
 Session Policies  
‣ TLS Management  
‣ Network & Flows  
‣ DMZ Services

**Policy Groups: default-low**

**Add** Clone

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

Hover over a row to see its description.

**Policy Group** Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
1	default	default	default-low-med	default-low	default	None	Off <span>Edit</span>

The **Policy Group** pop-up screen is displayed. Enter a desired **Group Name** as shown below.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Device Management  
Backup/Restore  
‣ System Parameters  
‣ Configuration Profiles  
‣ Services  
‣ Domain Policies  
 Application Rules

**Policy Groups: default-low**

**Add** Clone

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

Hover over a row to see its description.

**Policy Group**

**Policy Group** X

Group Name

Next

The **Policy Group** pop-up screen is updated. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Application Rule:** Select the Engage application rule from **Section 7.4**.
- **Media Rule:** Select the Engage media rule from **Section 7.5**.
- **Signaling Rule:** Select the Engage signaling rule from **Section 7.6.1**.

The screenshot shows the 'Policy Group' configuration window. The left sidebar contains the navigation menu with 'Domain Policies' expanded. The main area displays the 'Policy Group' configuration form with the following fields and values:

Field	Value
Application Rule	Application-NICE
Border Rule	default
Media Rule	Media-NICE
Security Rule	default-low
Signaling Rule	Signaling-NICE
Charging Rule	None
RTCP Monitoring Report Generation	Off

Buttons: Back, Finish

## 7.8. Administer Session Policies

Select **Backup/Restore** → **Domain Policies** → **Session Policies** from the left pane to display the existing routing profiles. Click **Add** to add routing profile for Engage.

The screenshot shows the 'Session Policies' configuration page. The left sidebar contains the navigation menu with 'Domain Policies' expanded. The main area displays the 'Session Policies' configuration form with the following fields and values:

Field	Value
Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None
Converged Conferencing	<input type="checkbox"/>
Recording Server	<input type="checkbox"/>
Media Server	<input type="checkbox"/>

Buttons: Add, Clone, Edit

The **Session Policy** pop-up screen is displayed. Enter a desired **Policy Name** as shown below.

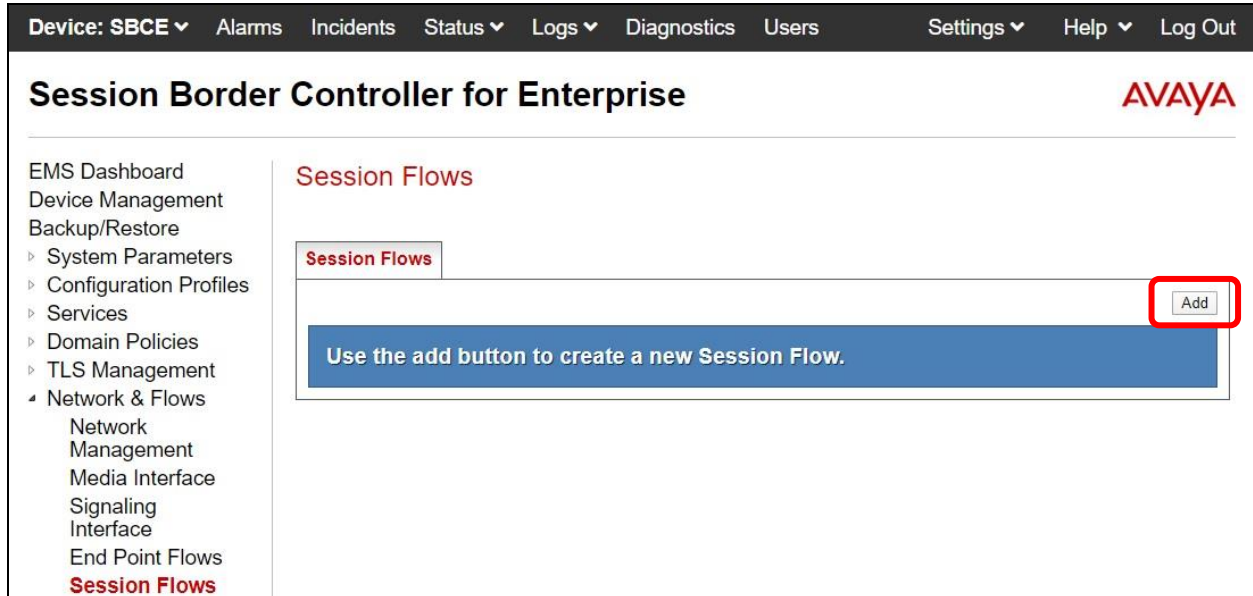
The **Session Policy** pop-up screen is updated. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Media Anchoring:** Check this field.
- **Recording Server:** Check this field.
- **Recording Type:** Select the desired type, in this case “Full Time”.
- **Play Recording Tone:** Check this field if customer desires recording tone to be played.
- **Routing Profile:** Select the Engage routing profile from **Section 7.3**.

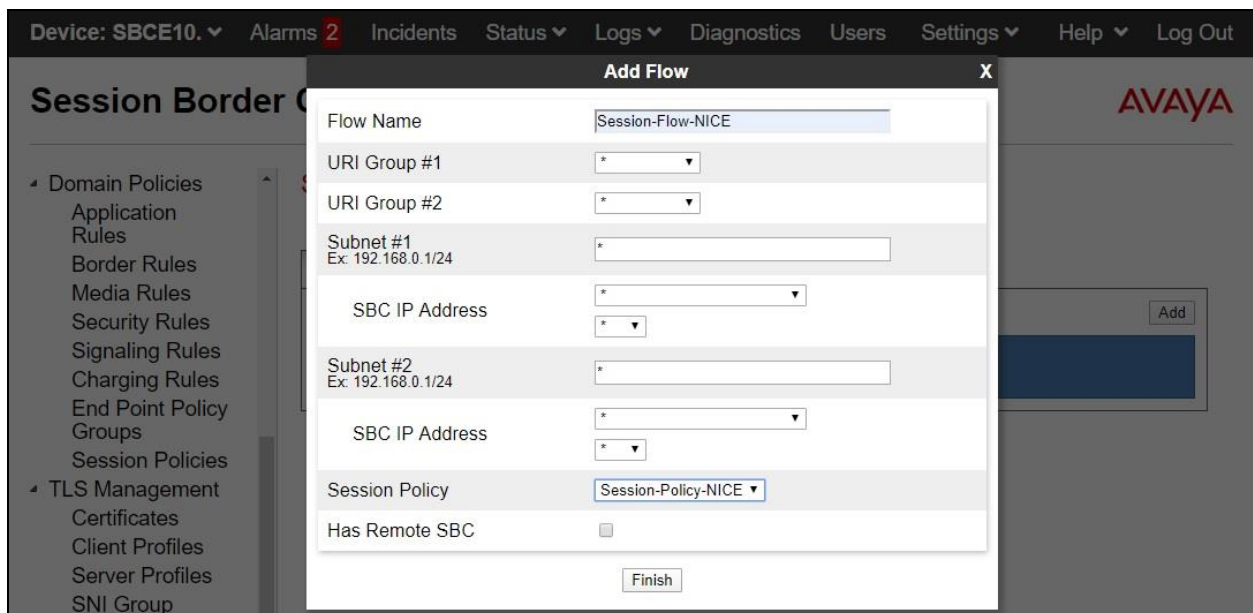


## 7.9. Administer Session Flows

Select **Backup/Restore** → **Network & Flows** → **Session Flows** from the left pane to display the existing session flows. Click **Add** to add a session flow for Engage.



The **Add Flow** pop-up screen is displayed. For **Flow Name**, enter a desired name. For **Session Policy**, select the session policy for Engage from **Section 7.8**.



## 7.10. Administer End Point Flows

Select **Backup/Restore** → **Network & Flows** → **End Point Flows** from the left pane. Select the **Server Flows** tab and click **Add** to add a server flow for Engage.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
    Network Management  
    Media Interface  
    Signaling Interface  
    **End Point Flows**  
    Session Flows  
    Advanced Options  
▸ DMZ Services  
▸ Monitoring & Logging

#### End Point Flows

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

Modifications made to a Server Flow will only take effect on new sessions.

Hover over a row to see its description.

##### SIP Server: Server-Ext-SP

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Flow2-Ext	*	Private-Signaling	Public-Signaling	default-low	Route-SM	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

##### SIP Server: Server-SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Flow2-SM	*	Public-Signaling	Private-Signaling	default-low	Route-Ext-SP	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

The **Add Flow** pop-up screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Flow Name:** A descriptive name.
- **SIP Server Profile:** The SIP server profile for Engage from **Section 7.2**.
- **Received Interface:** The external signaling interface in this case “Public-Signaling”.
- **Signaling Interface:** The internal signaling interface in this case “Private-Signaling”.
- **Media Interface:** The internal media interface in this case “Private-Media”.
- **End Point Policy Group:** The end point policy group for Engage from **Section 7.7**.

The screenshot displays the 'Add Flow' configuration window in the Avaya Session Border Controller (SBCE) interface. The window is titled 'Add Flow' and has a close button 'X' in the top right corner. The configuration fields and their values are as follows:

Field	Value
Flow Name	Flow2-NICE
SIP Server Profile	Server-NICE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public-Signaling
Signaling Interface	Private-Signaling
Media Interface	Private-Media
Secondary Media Interface	None
End Point Policy Group	Endpt-Policy-NICE
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

A 'Finish' button is located at the bottom of the configuration window. The background shows the SBCE interface with a sidebar menu on the left and a top navigation bar. The sidebar menu includes options like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'Network Management', 'Media Interface', 'Signaling Interface', 'End Point Flows', 'Session Flows', 'Advanced Options', 'DMZ Services', and 'Monitoring & Logging'. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'.

## 8. Configure NICE Engage Platform

This section provides the procedures for configuring Engage. The procedures include the following areas:

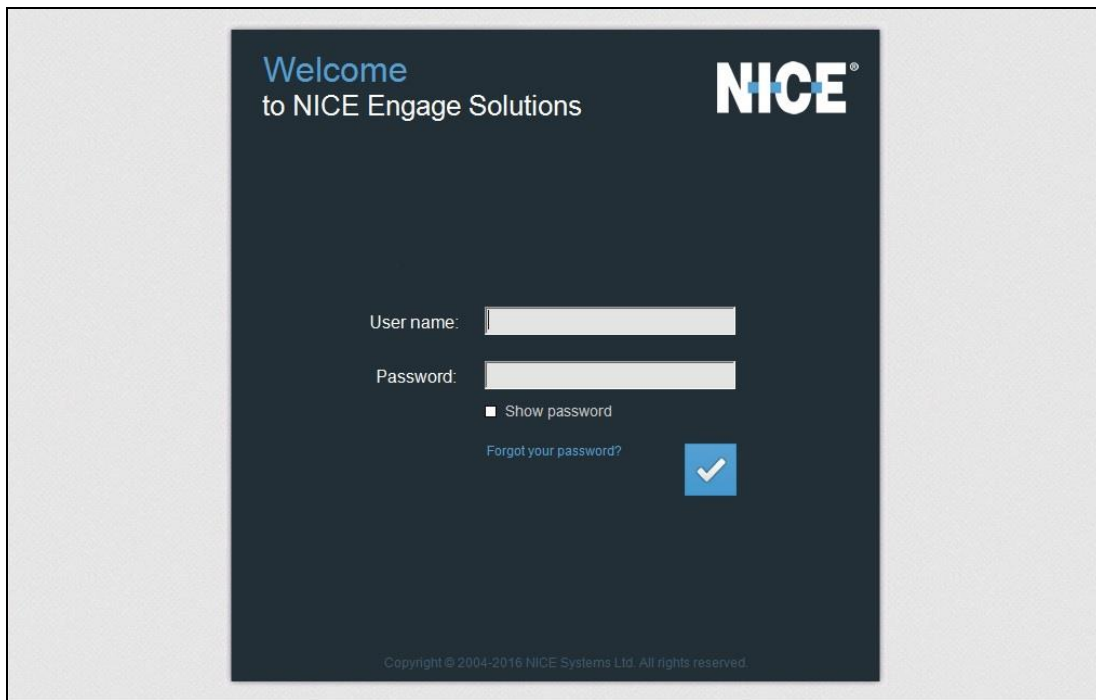
- Launch Engage web interface
- Administer CTI for PC
- Administer media provider controllers
- Administer drivers
- Administer Interactions Center
- Restart services
- Administer system mapping
- Administer agent users

The configuration of Engage is performed by NICE engineers. The procedural steps are presented in these Application Notes for informational purpose.

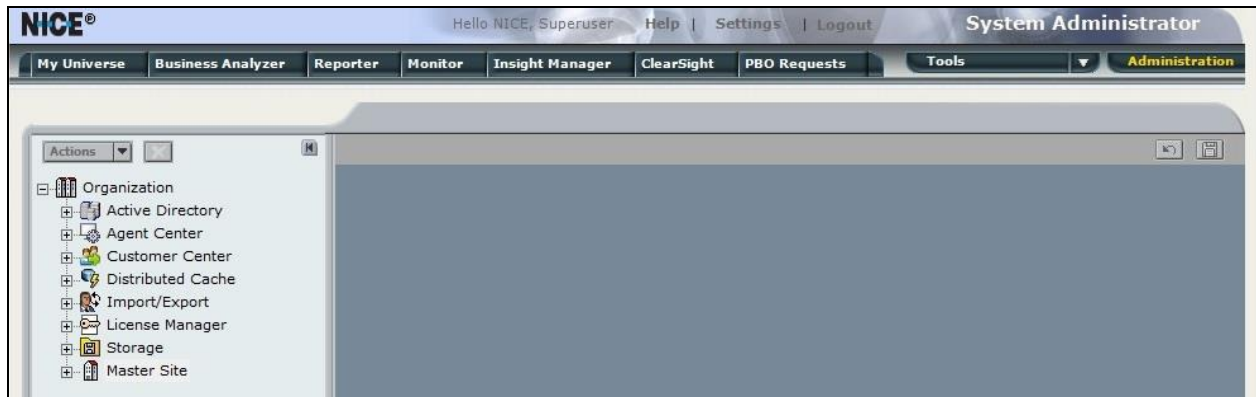
Prior to configuration, a pertinent interactions center is assumed to be pre-configured.

### 8.1. Launch Engage Web Interface

Access the Engage web interface by using the URL “http://hostname/nice” in an Internet Explorer browser window, where “hostname” is the host name of the Engage server with the Application Server component. The **Welcome** screen below is displayed. Log in using the appropriate credentials.

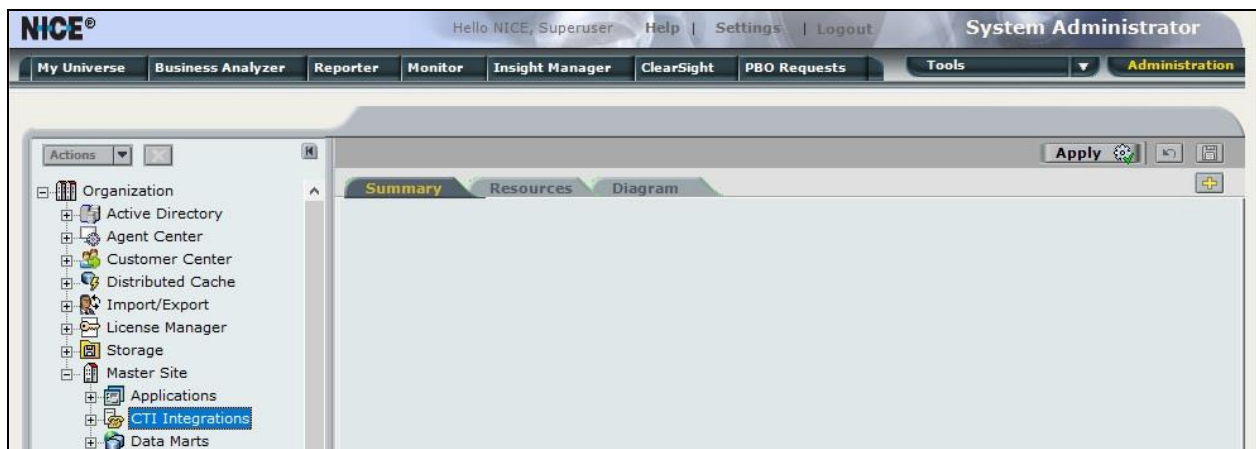


The NICE screen below is displayed next. Select **Administration** → **System Administrator** followed by **Settings** → **Technician Mode** from the top menu.

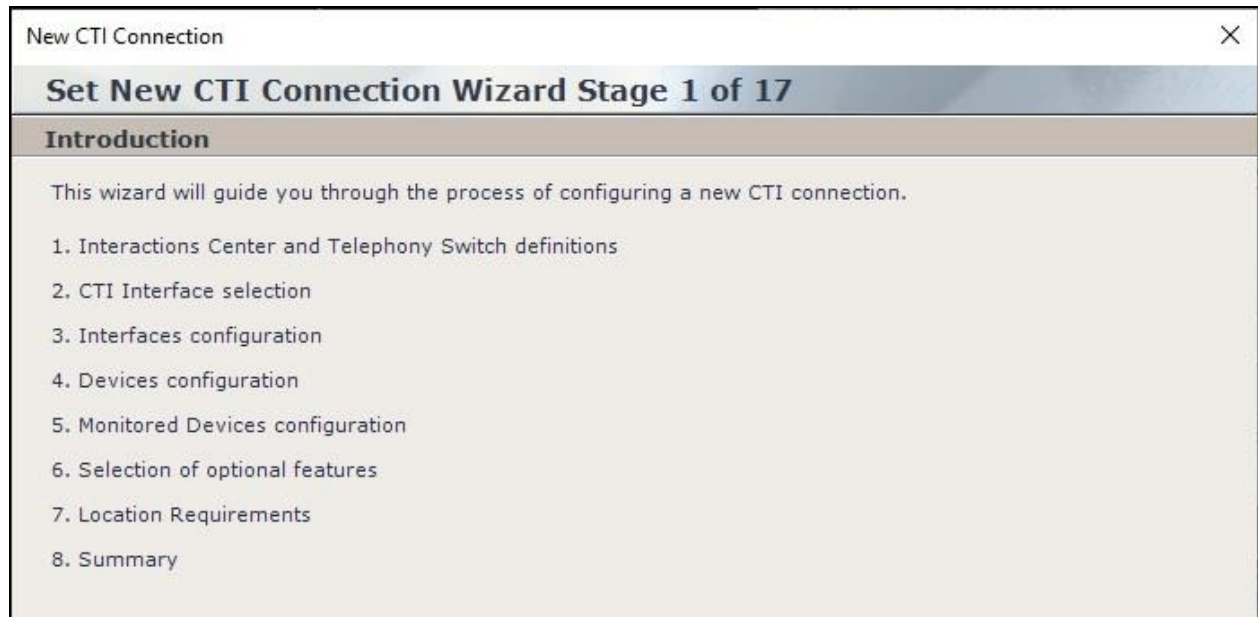


## 8.2. Administer CTI for PC

Expand **Organization** → **Master Site** as shown below. Right click on **CTI Integrations** and select **New CTI Connection** to add a connection with Proactive Contact.



The **New CTI Connection** pop-up screen is displayed. Click **Next** (not shown).



New CTI Connection

### Set New CTI Connection Wizard Stage 1 of 17

#### Introduction


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

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

The **Stage 2** screen is displayed as shown below.

For **Regular Interactions Center**, select the pertinent center, in this case “IC\_on\_AppServer (NiceApp)” which was pre-configured.

For **Switch Type**, select “Avaya PC/ POM”, which auto populates **Switch Name** with the same value.



New CTI Connection

### Set New CTI Connection Wizard Stage 2 of 17

#### Interactions Center Switch

Attach CTI to Interactions Center Server:

☒ Regular Interactions Center: IC\_on\_AppServer (NiceApp)

☐ Interactions Center Cluster:

☐ Use existing Telephony Switch:

☒ Define new Telephony Switch:

Switch Type: Avaya PC/ POM

Switch Name: Avaya PC/ POM



Proceed to **Stage 3**. Retain “Event Service” as the default value for **Avaya PC/ POM CTI Interface** as shown below.

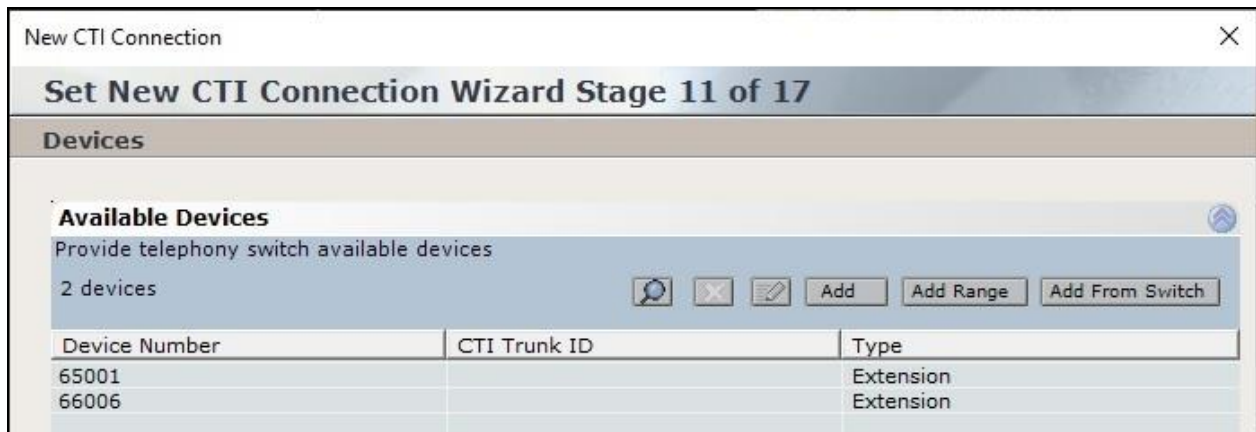
Proceed to **Stage 4**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **AvayaPD Version:** The closest version number, in this case “PC512”.
- **Event Service Host Name:** The Proactive Contact host name from **Section 6.1**.
- **Naming Service Host Name:** The Proactive Contact host name from **Section 6.1**.
- **AvayaPD Client Username:** The Proactive Contact Event Service client credentials.
- **AvayaPD Client Password:** The Proactive Contact Event Service client credentials.

Parameter	Value
<b>AvayaPD Version</b>	PC512
<b>Event Service Host Name</b>	lzpds4b
<b>Naming Service Host Name</b>	lzpds4b
<b>AvayaPD Client Username</b>	client1
<b>AvayaPD Client Password</b>	*****
<b>Client Port ID</b>	6666

Description: Avaya PC Client Password - The CTILink will use this parameter in order to login to the Avaya PC server.

Proceed to **Stage 11**. Select **Add** to add a device entry for each agent station extension from **Section 3**. Set **Device Number** to the agent station extension and **Type** to “Extension” as shown below.



Device Number	CTI Trunk ID	Type
65001		Extension
66006		Extension

Proceed to **Stage 13**, and check **Call Flow Analysis**.

Proceed to complete the wizard.



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

- ☐ SIP Trunk Correlation
- ☐ AOD VRSP Correlation
- ☐ Rejected Devices
- ☐ Filter Calls
- ☒ Call Flow Analysis

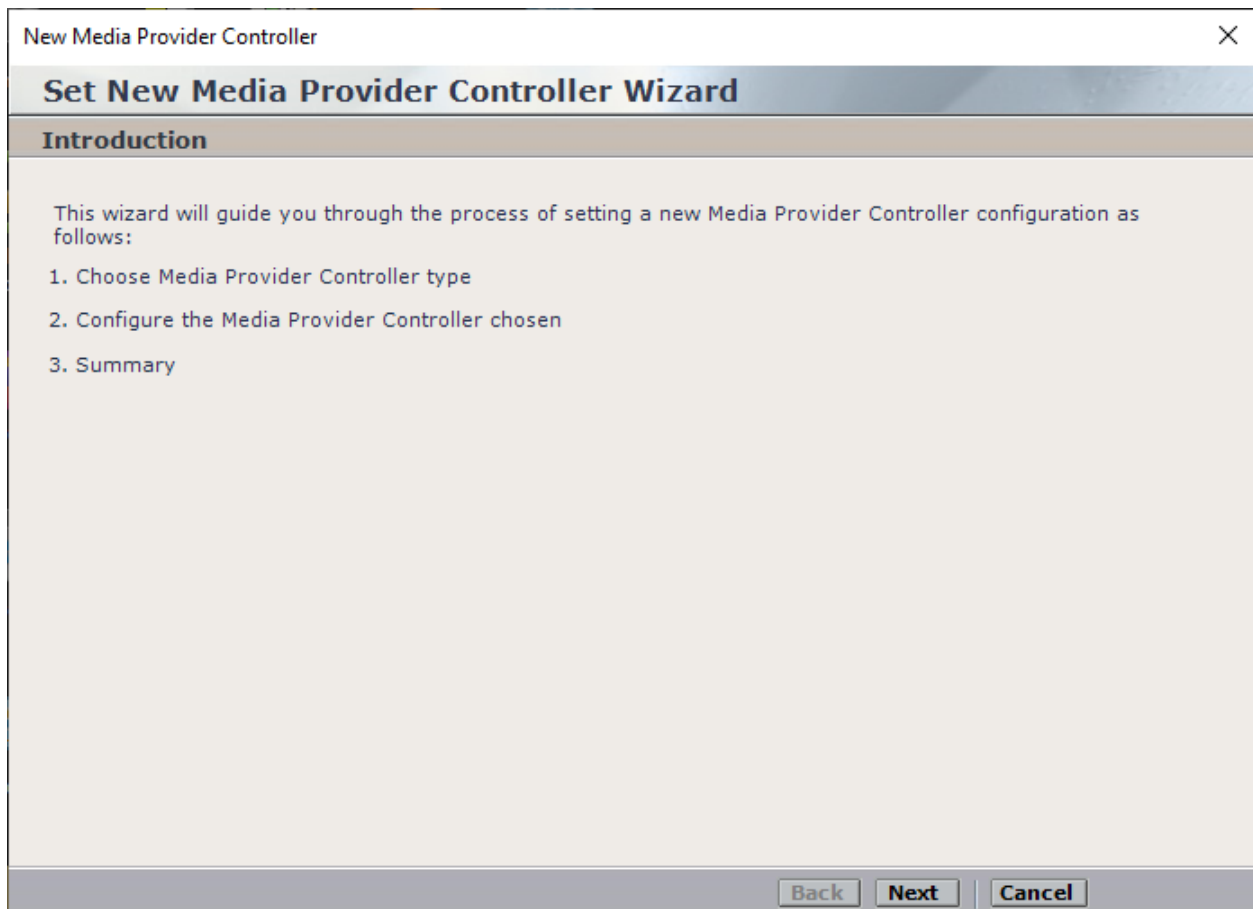


### 8.3. Administer Media Provider Controllers

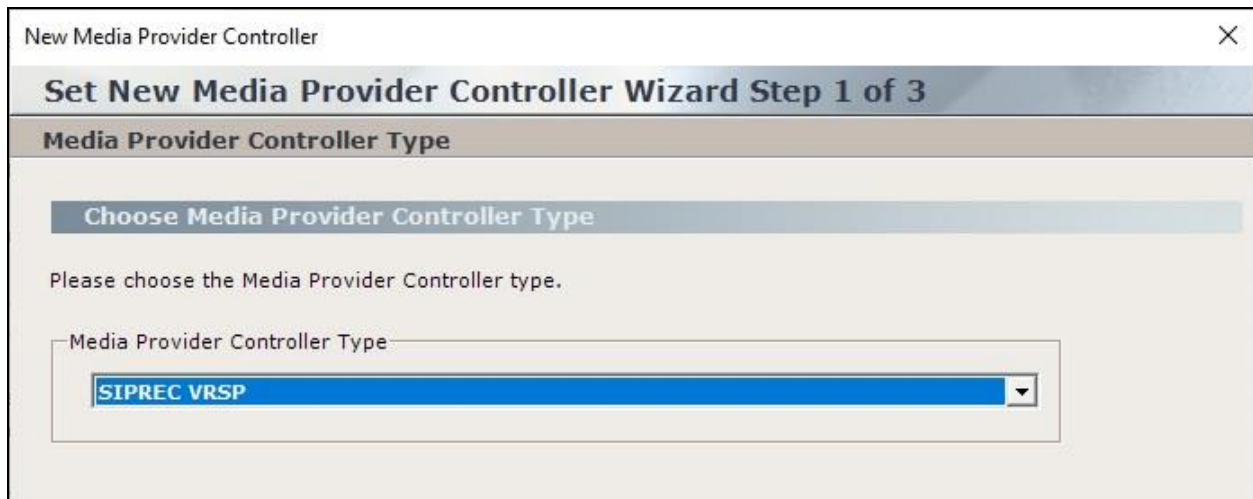
The NICE screen is displayed again. Expand **CTI Integrations** in the left pane. Right click on **Media Provider Controllers** and select **New Media Provider Controller** to add a media controller for SBCE.



The **New Media Provider Controller** pop-up screen is displayed as shown below. Click **Next**



The **Step 1** screen is displayed. For **Media Provider Controller Type**, select “SIPREC VRSP” as shown below.



New Media Provider Controller

### Set New Media Provider Controller Wizard Step 1 of 3

#### Media Provider Controller Type

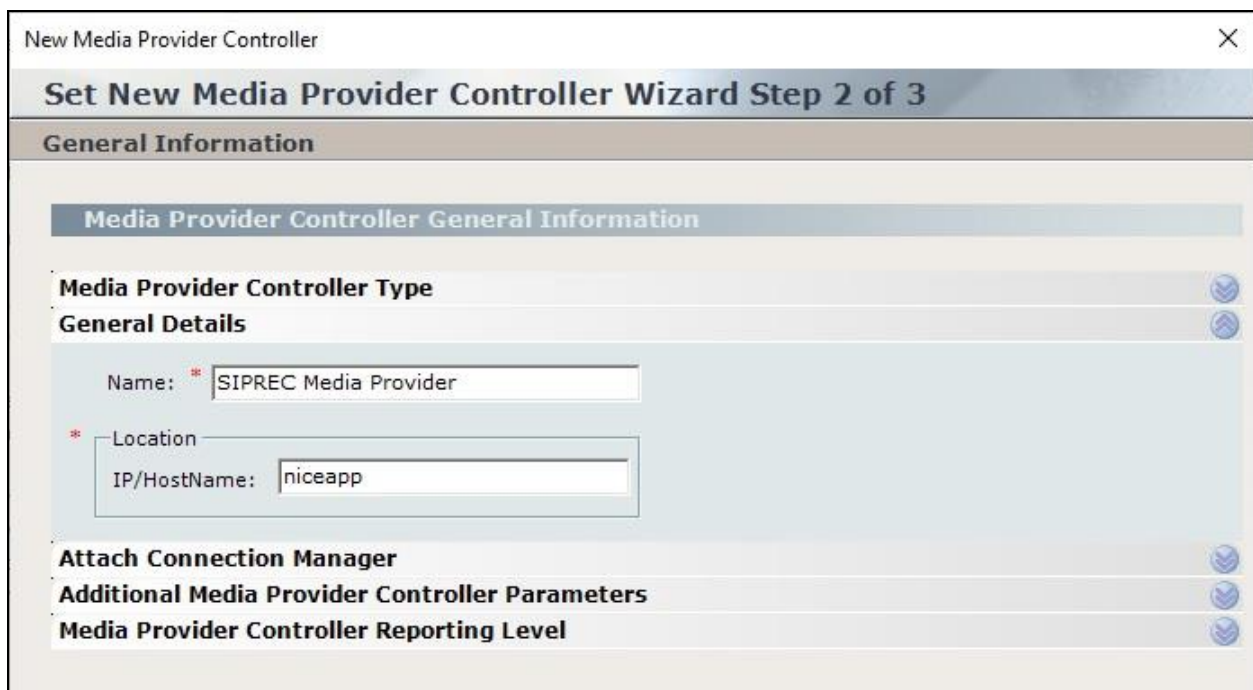
##### Choose Media Provider Controller Type

Please choose the Media Provider Controller type.

Media Provider Controller Type

SIPREC VRSP

The **Step 2** screen is displayed next. Enter a descriptive **Name**. For **IP/HostName**, enter the IP address or the hostname of the Engage server with the Interactions Center component.



New Media Provider Controller

### Set New Media Provider Controller Wizard Step 2 of 3

#### General Information

##### Media Provider Controller General Information

**Media Provider Controller Type**

**General Details**

Name: \* SIPREC Media Provider

\* Location

IP/HostName: niceapp

**Attach Connection Manager**

**Additional Media Provider Controller Parameters**

**Media Provider Controller Reporting Level**

Expand the **Attach Connection Manager** sub-section. Select the **1 – Avaya PC/ POM NiceApp CM** entry from the **Available Connection Managers** column and move to the **Attached Connection Manager** column as shown below.

New Media Provider Controller

**Set New Media Provider Controller Wizard Step 2 of 3**

**General Information**

**Media Provider Controller General Information**

**Media Provider Controller Type**

**General Details**

**Attach Connection Manager**

Available Connection Managers

Attached Connection Manager

1 - Avaya PC/ POM NiceApp CM

**Additional Media Provider Controller Parameters**

Expand the **Additional Media Provider Controller Parameters** sub-section. Set **MetadataType** to “Draft15”, as shown below.

New Media Provider Controller

**Set New Media Provider Controller Wizard Step 2 of 3**

**General Information**

**Media Provider Controller General Information**

**Media Provider Controller Type**

**General Details**

**Attach Connection Manager**

**Additional Media Provider Controller Parameters**

☐ Display Read Only Information Mandatory fields are marked in bold

Parameter Name	Parameter Value
VRSP Version	Ver_2
UnitAssembly	Integrations.NSP.DynamicSipRecVrsp.dll
<b>MetadataType</b>	<b>Draft 15</b>
SipRefreshMethod	Update
AodApiPort	41042
CustomerDomainInSiprecMetadata	
AgentDomainInSiprecMetadata	
ResponseToSDPInactive	AllRecvOnly

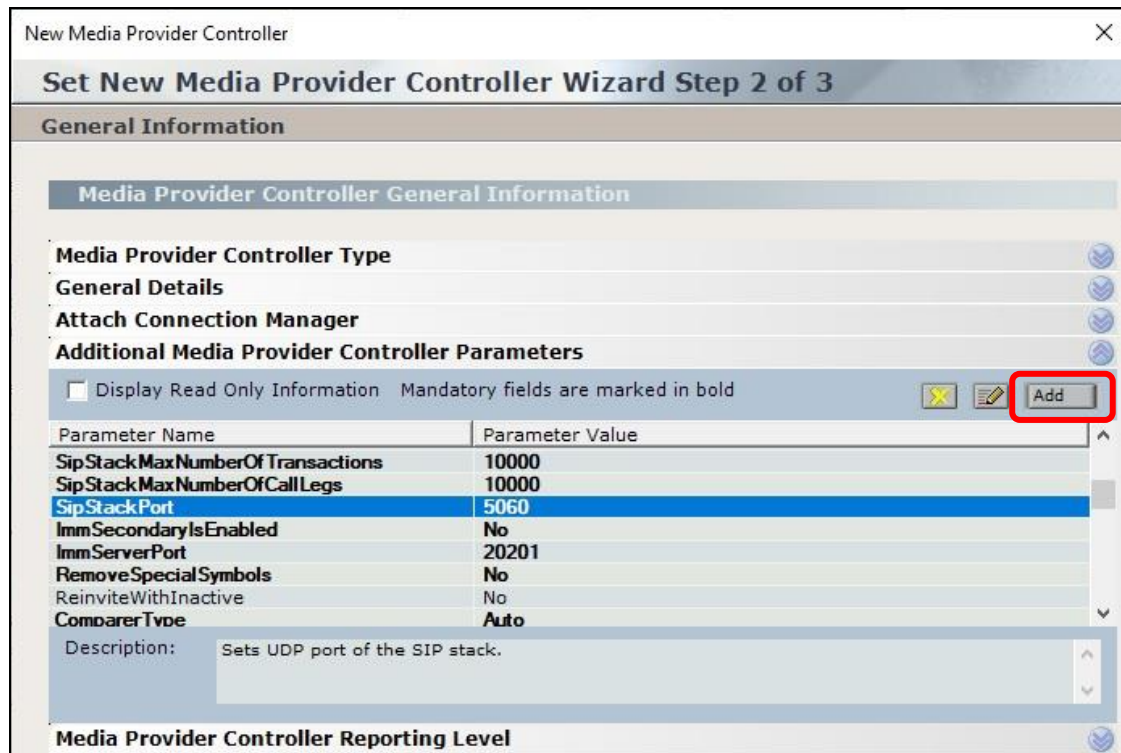
Description: Metadata type to set the data translator type.

**Media Provider Controller Reporting Level**

Back Next Cancel

Navigate down to **SipStackPort** and set the parameter value to the port value for Engage SIP server from **Section 7.2**, in this case “5060”.

Select **Add** to add an additional parameter.



New Media Provider Controller

Set New Media Provider Controller Wizard Step 2 of 3

General Information

Media Provider Controller General Information

Media Provider Controller Type

General Details

Attach Connection Manager

Additional Media Provider Controller Parameters

☐ Display Read Only Information Mandatory fields are marked in bold

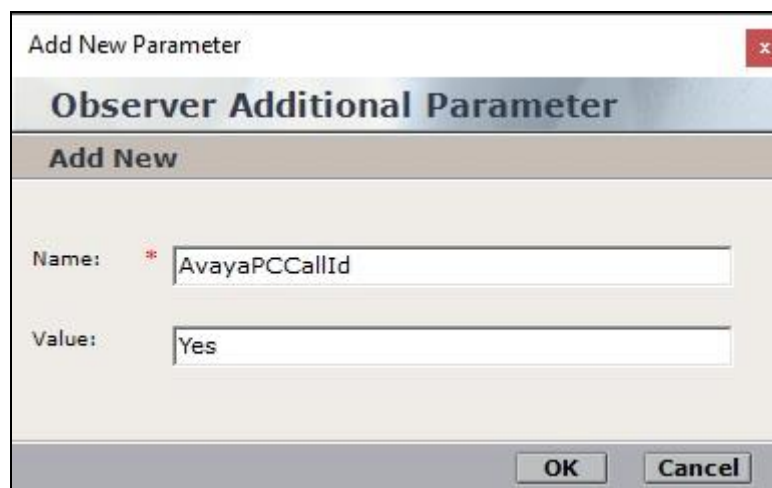
Parameter Name	Parameter Value
SipStackMaxNumberOfTransactions	10000
SipStackMaxNumberOfCallLegs	10000
<b>SipStackPort</b>	<b>5060</b>
ImmSecondaryIsEnabled	No
ImmServerPort	20201
RemoveSpecialSymbols	No
ReinviteWithInactive	No
ComparatorType	Auto

Description: Sets UDP port of the SIP stack.

Media Provider Controller Reporting Level

The **Add New Parameter** pop-up box is displayed. Add the **AvayaPCCallId** parameter and set the value to “Yes” as shown below.

Proceed to complete the wizard.



Add New Parameter

Observer Additional Parameter

Add New

Name: \* AvayaPCCallId

Value: Yes

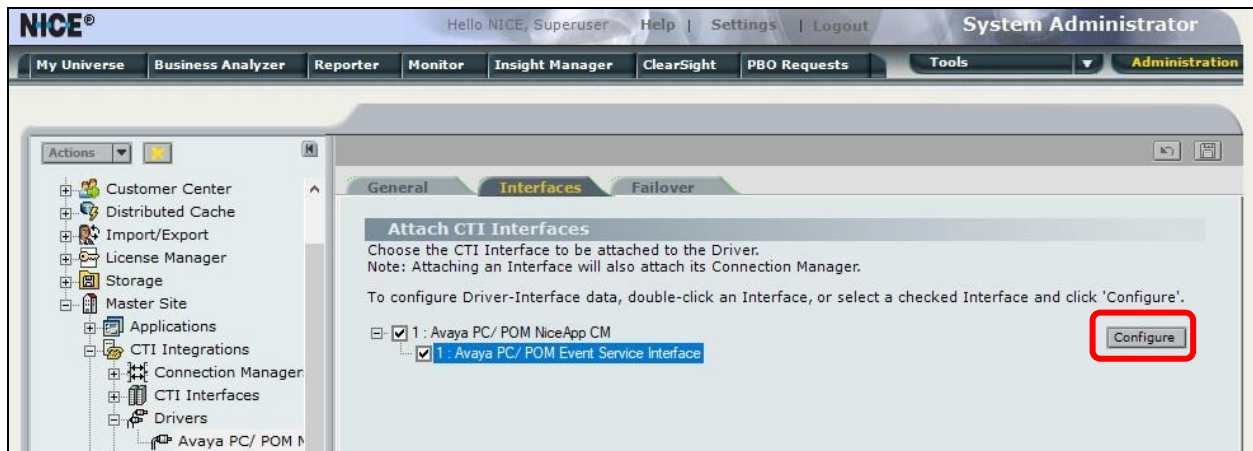
OK Cancel



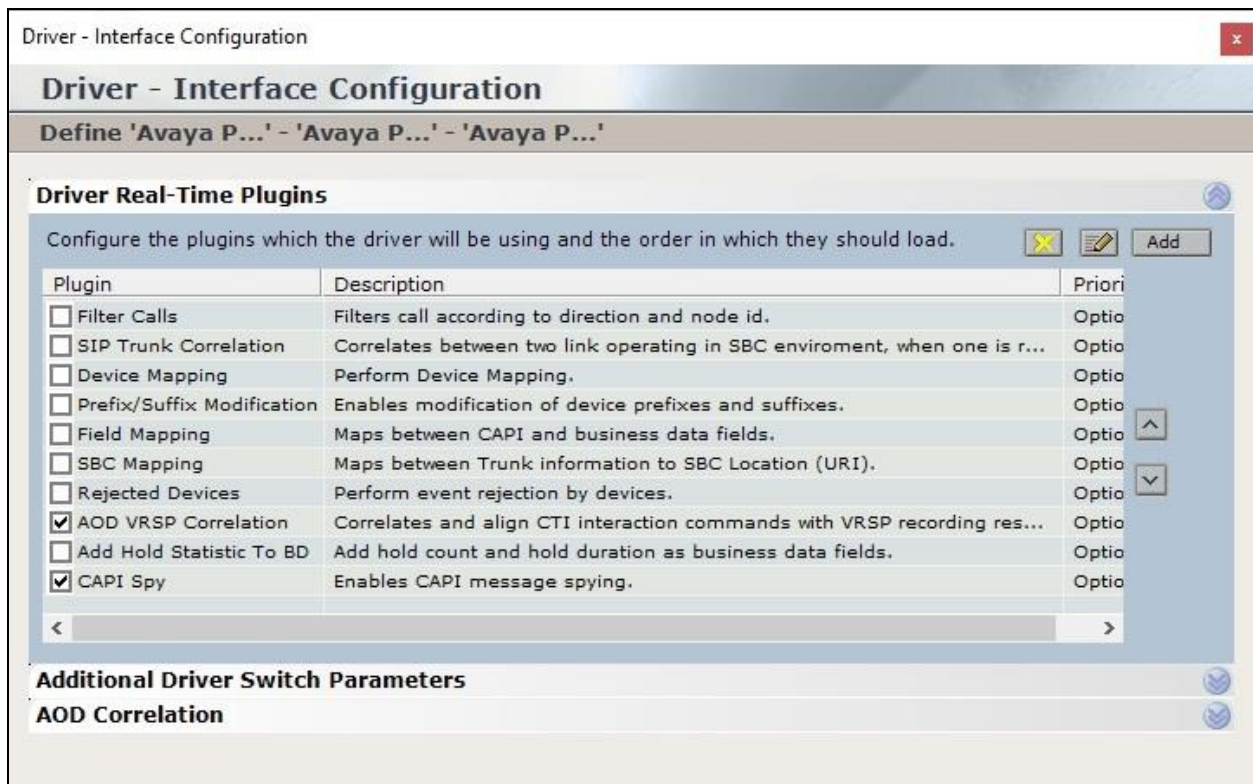
## 8.4. Administer Drivers

The **NICE** screen is displayed again. Expand **Drivers** in the left pane and select **Avaya PC/ POM NiceApp Driver** in the left pane.

Select the **Interfaces** tab in the right pane, followed by the **Avaya PC/ POM Event Service Interface** entry as shown below. Click **Configure**.



The **Driver – Interface Configuration** screen is displayed next. Expand **Driver Real-Time Plugins** and check **AOD VRSP Correlation**. Retain the default values in the remaining fields.



Expand **AOD Correlation** and select the entry associated with the media provider controller from **Section 8.3**. In the **Correlation settings** sub-section, enter “OriginalCID” as shown below.

**Driver - Interface Configuration**

Define 'Avaya P...' - 'Avaya P...' - 'Avaya P...'

**Driver Real-Time Plugins**

**Additional Driver Switch Parameters**

**AOD Correlation**

Select SIPREC AOD VRSP(s) for correlation:

	Name	Location	TCP port	Resource ID
<input checked="" type="checkbox"/>	SIPREC Media Provider	niceapp	41042	82
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

**Correlation settings**

Business data field for correlation with SIPREC: \*

☐ Filter non-correlated calls

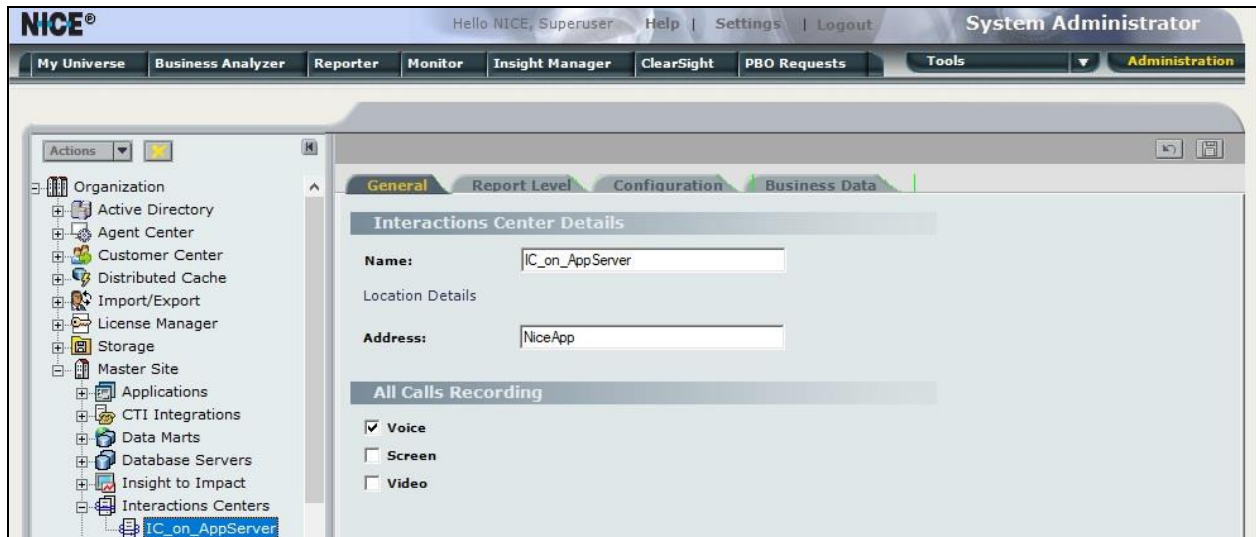
☐ Correlate internal calls

OK Cancel

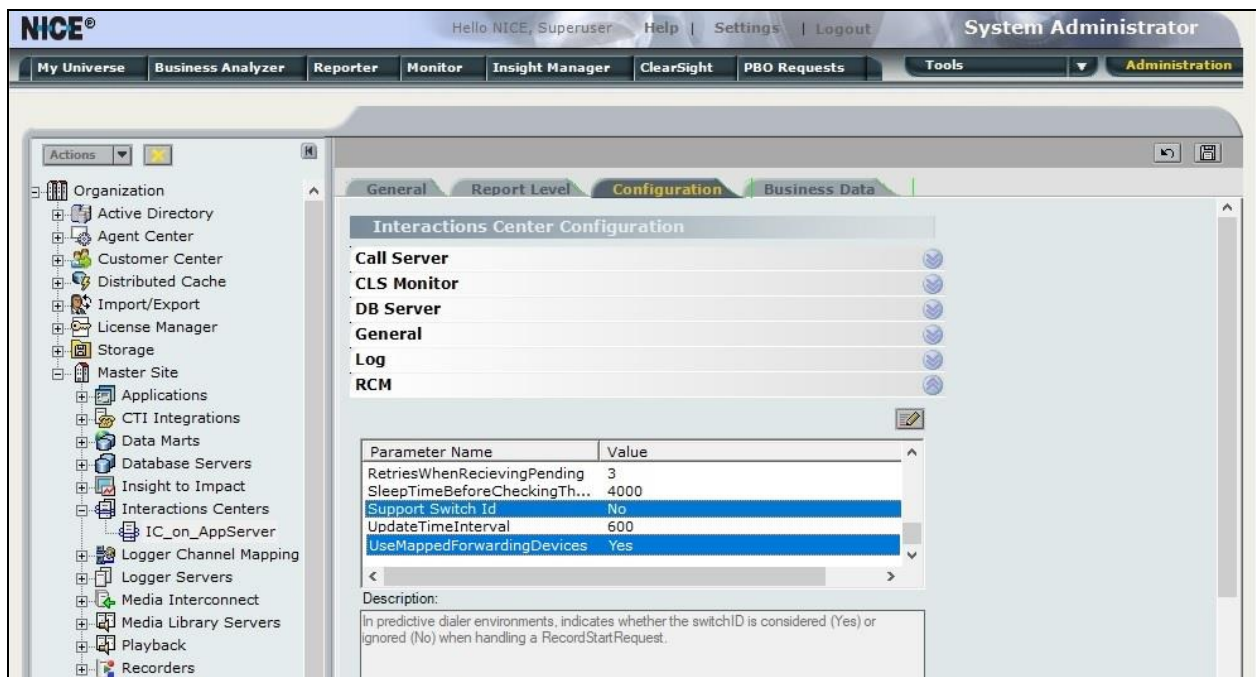
## 8.5. Administer Interactions Center

From the **NICE** screen, expand **Master Site** → **Interactions Centers** and select the pertinent center, in this case “IC\_on\_AppServer”, which was pre-configured.

Select the **General** tab in the right pane, and check **Voice** as shown below.

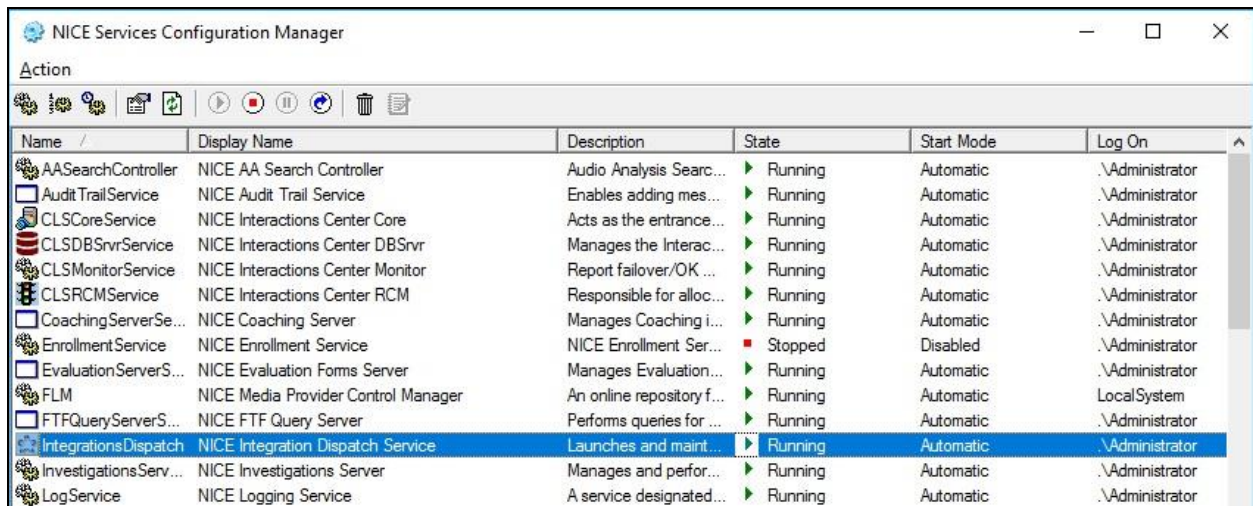


Select the **Configuration** tab and expand **RCM** in the right pane. Locate the **Support Switch Id** parameter and set it to “No”. Locate the **UseMappedForwardingDevices** parameter and set it to “Yes” as shown below.



## 8.6. Restart Services

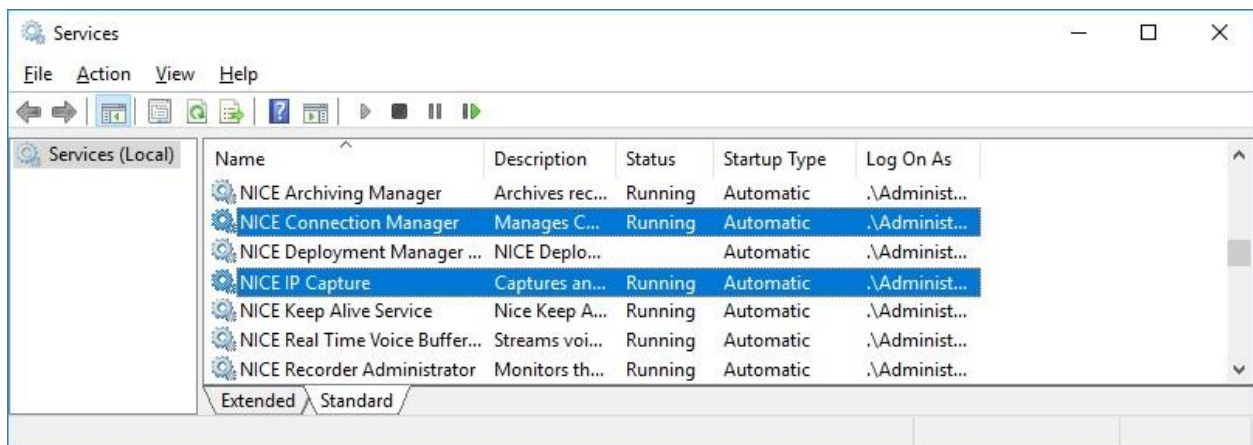
From the Engage server running the Interactions Center component, navigate to **Windows → Nice Systems** and launch **Nice Service Configuration Manager**. The **NICE Services Configuration Manager** screen below is displayed. Restart the **IntegrationsDispatch** service.



Name	Display Name	Description	State	Start Mode	Log On
AASearchController	NICE AA Search Controller	Audio Analysis Search...	Running	Automatic	.\Administrator
AuditTrailService	NICE Audit Trail Service	Enables adding mes...	Running	Automatic	.\Administrator
CLSCoreService	NICE Interactions Center Core	Acts as the entrance...	Running	Automatic	.\Administrator
CLSDBSvrService	NICE Interactions Center DBSvr	Manages the Interac...	Running	Automatic	.\Administrator
CLSMonitorService	NICE Interactions Center Monitor	Report failover/OK ...	Running	Automatic	.\Administrator
CLSRCMSvc	NICE Interactions Center RCM	Responsible for alloc...	Running	Automatic	.\Administrator
CoachingServerSe...	NICE Coaching Server	Manages Coaching i...	Running	Automatic	.\Administrator
EnrollmentService	NICE Enrollment Service	NICE Enrollment Ser...	Stopped	Disabled	.\Administrator
EvaluationServerS...	NICE Evaluation Forms Server	Manages Evaluation...	Running	Automatic	.\Administrator
FLM	NICE Media Provider Control Manager	An online repository f...	Running	Automatic	LocalSystem
FTFQueryServerS...	NICE FTF Query Server	Performs queries for ...	Running	Automatic	.\Administrator
IntegrationsDispatch	NICE Integration Dispatch Service	Launches and maint...	Running	Automatic	.\Administrator
InvestigationsServ...	NICE Investigations Server	Manages and perfor...	Running	Automatic	.\Administrator
LogService	NICE Logging Service	A service designated...	Running	Automatic	.\Administrator

From the Engage server running the Advanced Interaction Recorder component, navigate to **Windows → Windows System → Windows Administrative Tools → Services** to display the **Services** screen below.

Restart the **NICE Connection Manager** and **NICE IP Capture** services shown below.



Name	Description	Status	Startup Type	Log On As
NICE Archiving Manager	Archives rec...	Running	Automatic	.\Administ...
NICE Connection Manager	Manages C...	Running	Automatic	.\Administ...
NICE Deployment Manager ...	NICE Deplo...		Automatic	.\Administ...
NICE IP Capture	Captures an...	Running	Automatic	.\Administ...
NICE Keep Alive Service	Nice Keep A...	Running	Automatic	.\Administ...
NICE Real Time Voice Buffer...	Streams voi...	Running	Automatic	.\Administ...
NICE Recorder Administrator	Monitors th...	Running	Automatic	.\Administ...

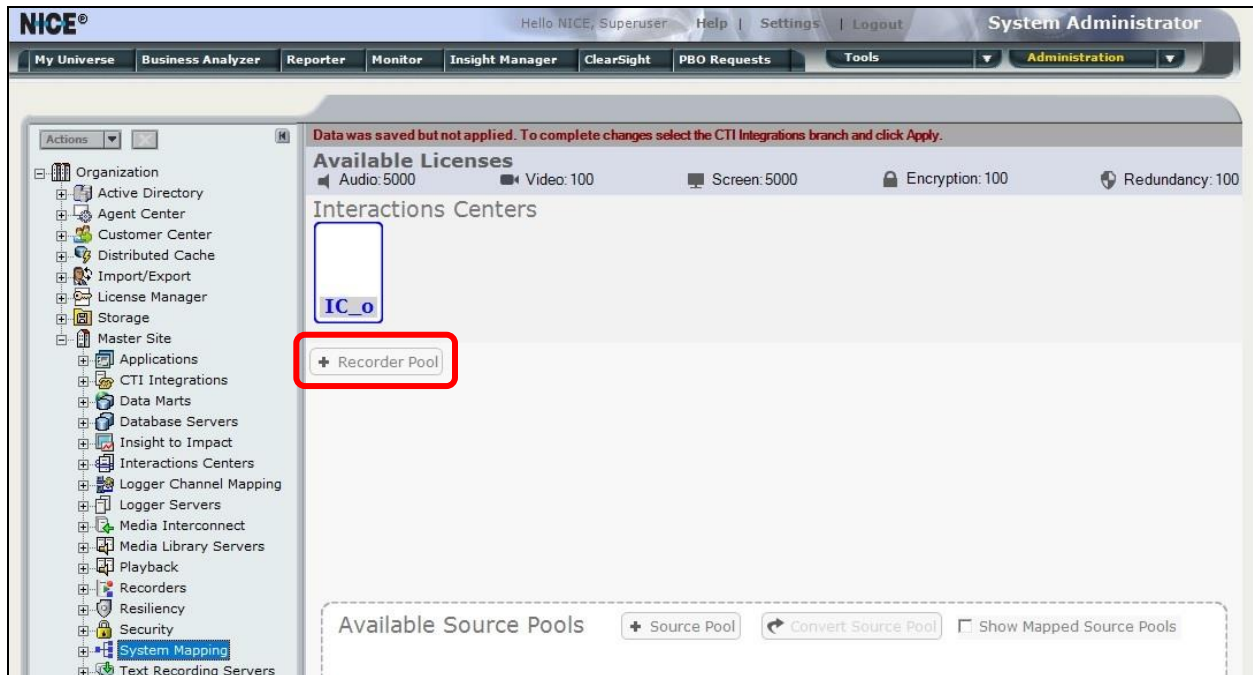


## 8.7. Administer System Mapping

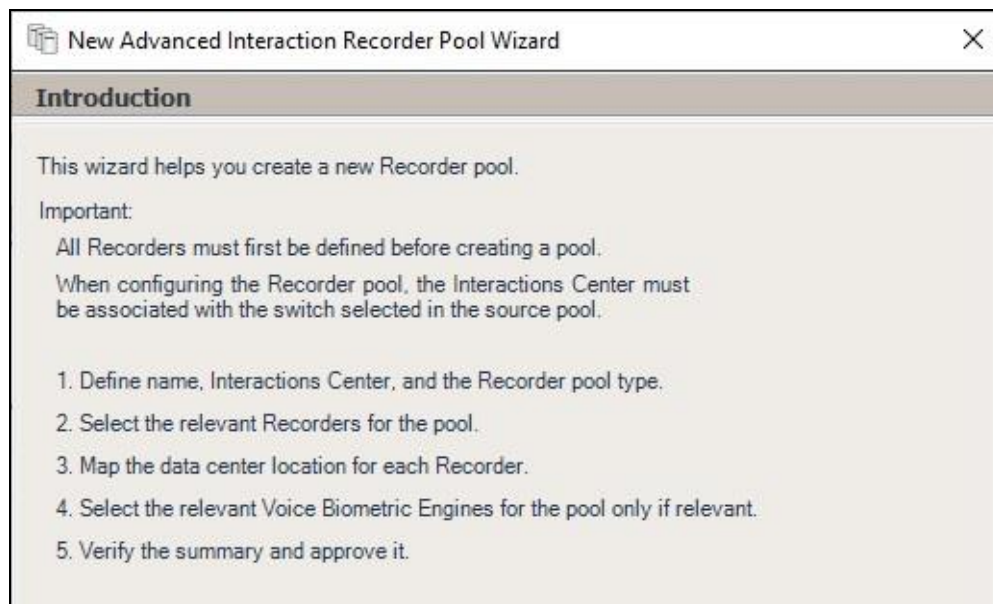
From the NICE screen, select **Master Site** → **System Mapping**.

### 8.7.1. Recorder Pool

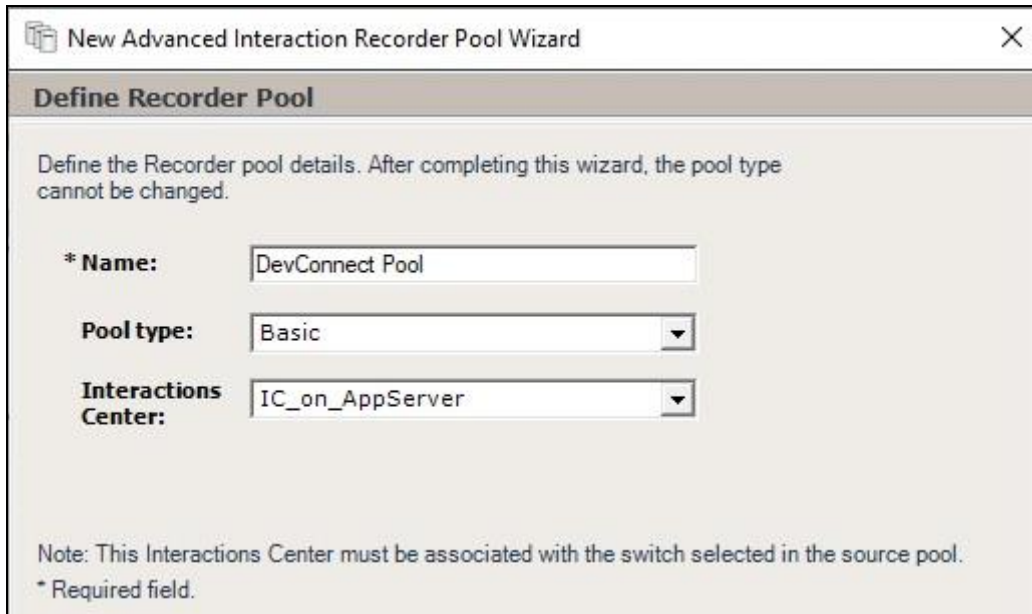
The screen below is displayed. In the right pane, select **+ Recorder Pool**.



The **New Advanced Interaction Recorder Pool Wizard** pop-up screen is displayed as shown below. Click **Next** (not shown).



The screen below is displayed next. Enter a descriptive **Name** and retain the default values in the remaining fields.



The screenshot shows the 'Define Recorder Pool' step of the wizard. It includes a title bar, a close button, and a header. The main area contains instructions and three input fields: a required text field for the name, and two dropdown menus for pool type and interactions center. A note and a legend are at the bottom.

**New Advanced Interaction Recorder Pool Wizard** [X]

**Define Recorder Pool**

Define the Recorder pool details. After completing this wizard, the pool type cannot be changed.

\* **Name:**

**Pool type:**

**Interactions Center:**

Note: This Interactions Center must be associated with the switch selected in the source pool.

\* Required field.

In the next screen, select the relevant and pre-existing recorder from the left pane and move to the right. The screenshot below shows the result of the move.

Proceed to complete the wizard.



The screenshot shows the 'Select Recorders' step of the wizard. It features two list boxes, 'Available' and 'Selected', with arrows between them. The 'Selected' list box contains the entry 'AIR'.

**New Advanced Interaction Recorder Pool Wizard** [X]

**Select Recorders**

Select the relevant Recorders for the pool. A basic pool must have a minimum of 1 Recorder.

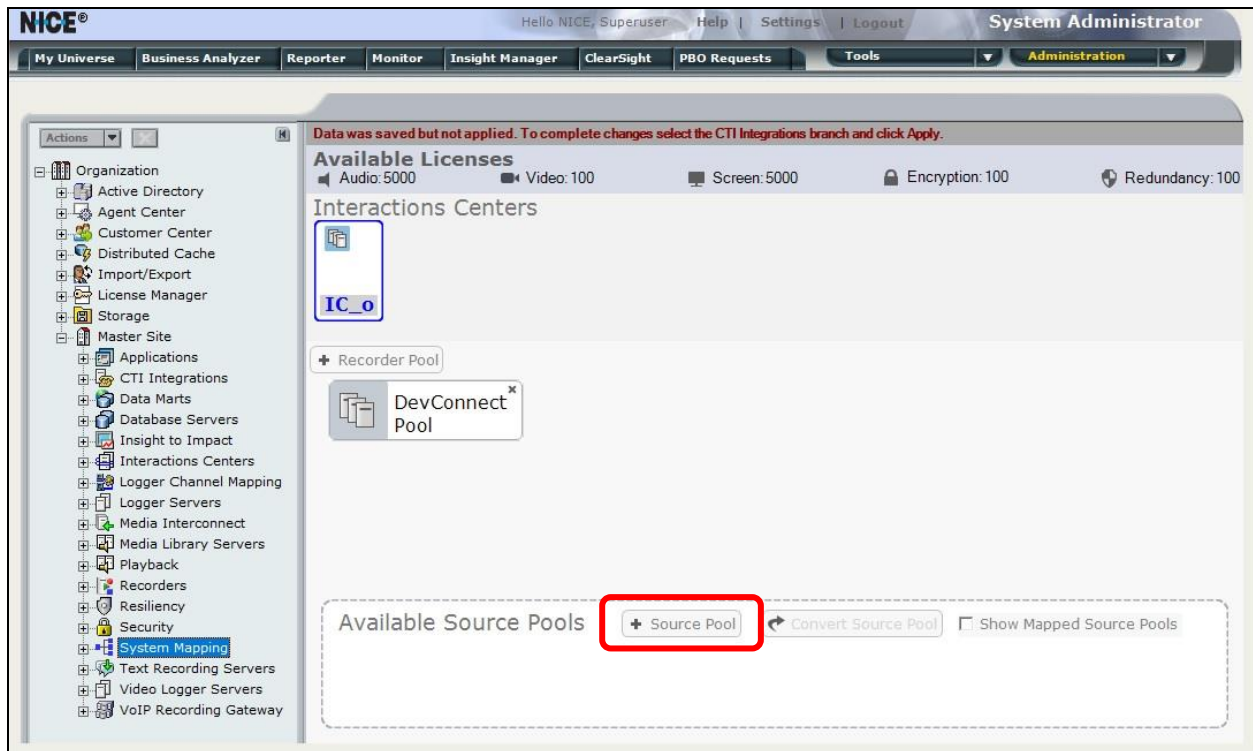
**Available**

**Selected**

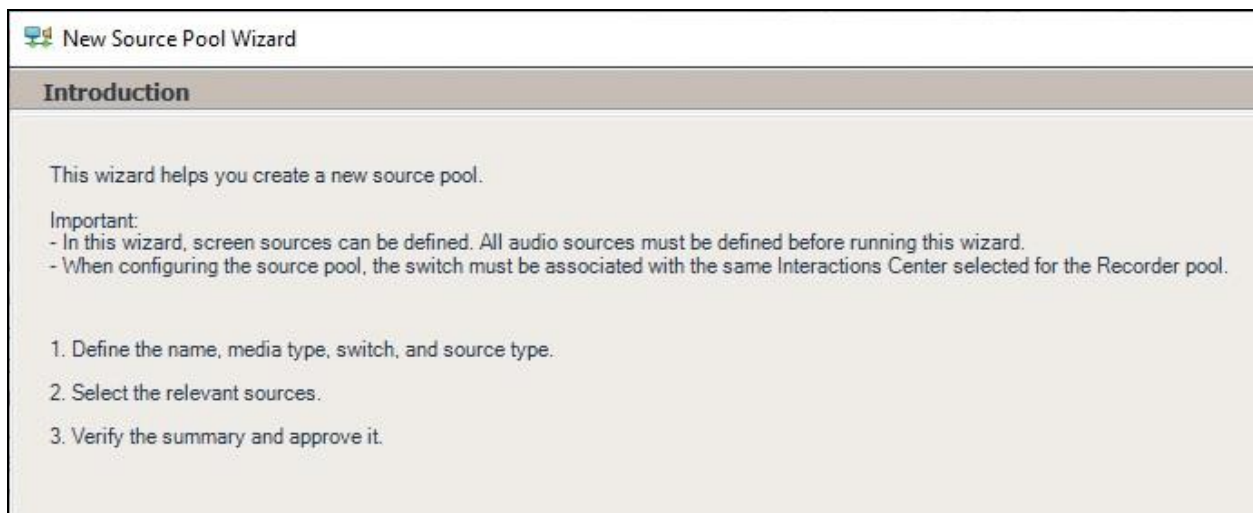
AIR

## 8.7.2. Source Pool

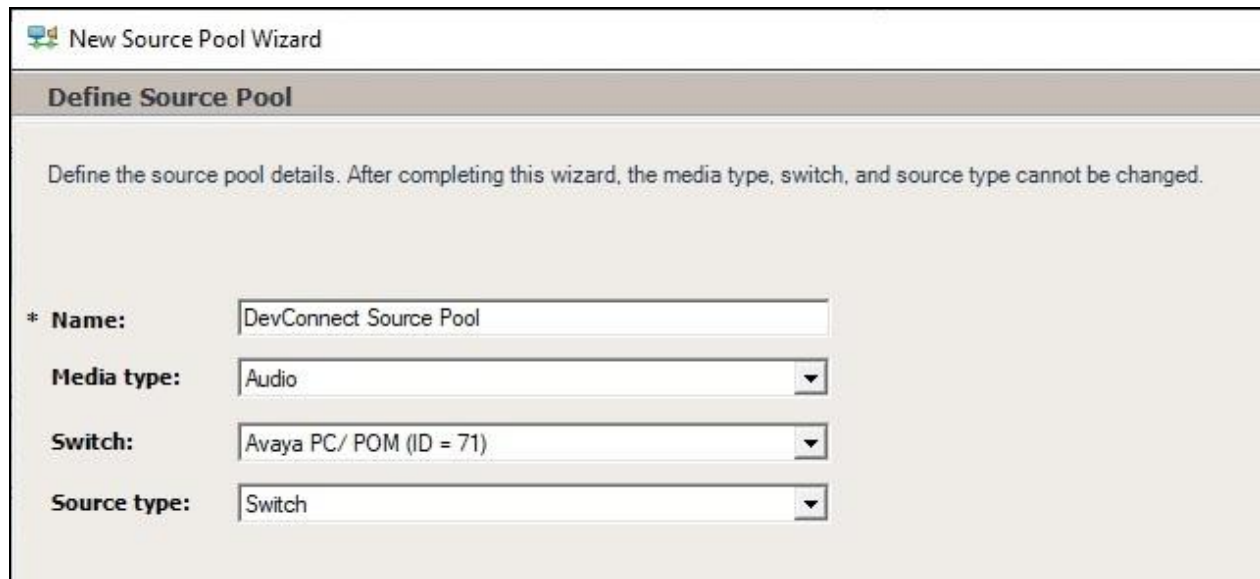
The NICE screen is updated as shown below. Select **+ Source Pool** to add a source pool.



The **New Source Pool Wizard** pop-up screen is displayed. Click **Next** (not shown).



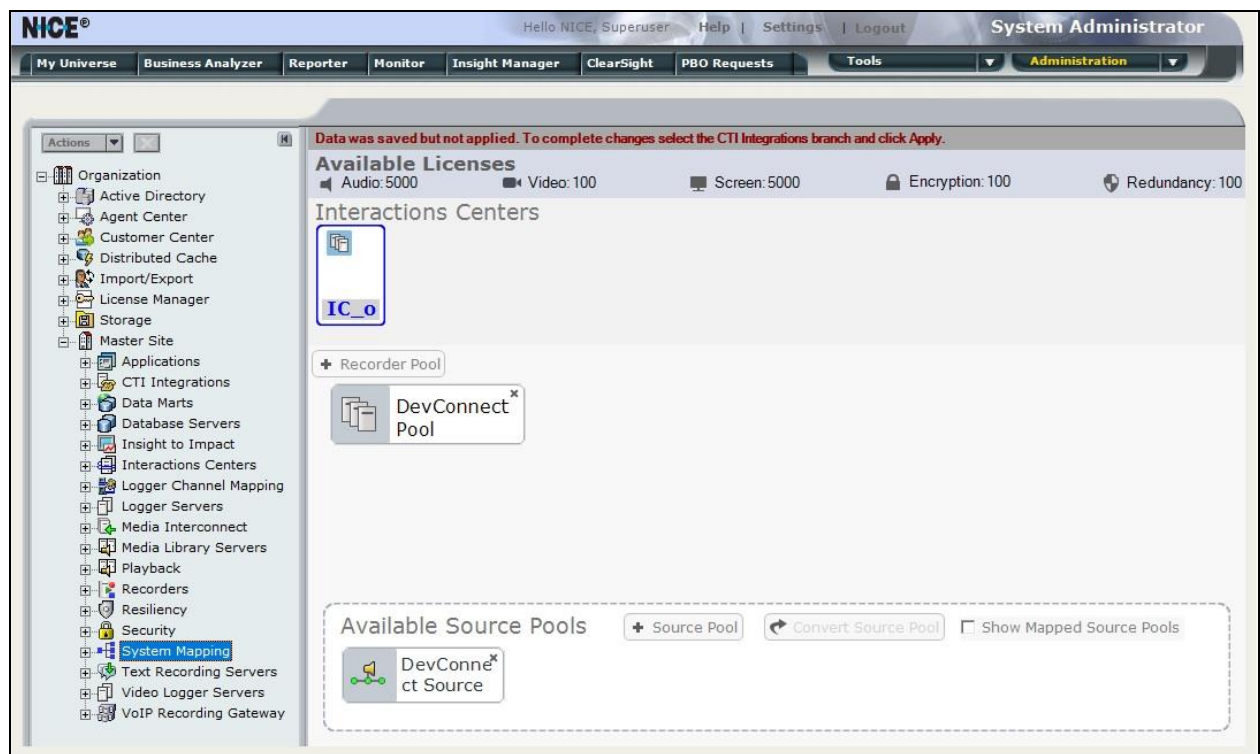
The screen below is displayed next. Enter a descriptive **Name**. For **Source type**, select “Switch”. Retain the default values in the remaining fields, and complete the wizard.



The screenshot shows the 'New Source Pool Wizard' window. The title bar says 'New Source Pool Wizard'. Below the title bar is a section titled 'Define Source Pool'. A message states: 'Define the source pool details. After completing this wizard, the media type, switch, and source type cannot be changed.' The form contains four fields: 'Name' with the value 'DevConnect Source Pool', 'Media type' with a dropdown menu showing 'Audio', 'Switch' with a dropdown menu showing 'Avaya PC/ POM (ID = 71)', and 'Source type' with a dropdown menu showing 'Switch'.

### 8.7.3. Recording Profile

The **NICE** screen is updated as shown below. Drag the created source pool below and drop on top of the created recorder pool, in this case **DevConnect Source** and **DevConnect Pool** respectively.



The screenshot shows the NICE System Administrator interface. The top navigation bar includes 'My Universe', 'Business Analyzer', 'Reporter', 'Monitor', 'Insight Manager', 'ClearSight', 'PBO Requests', 'Tools', and 'Administration'. The left sidebar shows a tree view of the system components, with 'System Mapping' highlighted. The main content area displays 'Available Licenses' (Audio: 5000, Video: 100, Screen: 5000, Encryption: 100, Redundancy: 100) and 'Interactions Centers'. A 'Recorder Pool' is shown with a 'DevConnect Pool' icon. Below this, 'Available Source Pools' are listed, including 'DevConnect Source'. A message at the top states: 'Data was saved but not applied. To complete changes select the CTI Integrations branch and click Apply.'

The **New Recording Profile Wizard** pop-up screen is displayed. Click **Next** (not shown).



The screenshot shows the 'Introduction' step of the 'New Recording Profile Wizard'. The title bar at the top reads 'New Recording Profile Wizard'. Below the title bar, the section is titled 'Introduction'. The text explains that the wizard helps map a recording profile and includes an 'Important' note about verifying the Interaction Center and switch selection. It also states that recording type and capture type cannot be changed after completion. A numbered list of four steps is provided: 1. Define the recording profile name, 2. Map the source pool to the Recorder pool, 3. Select the relevant recording type and capture type, and 4. Verify the summary and approve it.

New Recording Profile Wizard

### Introduction

This wizard helps you map a recording profile.

**Important:**

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

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

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

The screen below is displayed next. Enter a descriptive **Name**.



The screenshot shows the 'Define the Recording Profile Name' step of the 'New Recording Profile Wizard'. The title bar at the top reads 'New Recording Profile Wizard'. Below the title bar, the section is titled 'Define the Recording Profile Name'. The text prompts the user to enter a meaningful recording profile name, noting that the mapping and recording type cannot be changed after completion. A text input field is shown with the label 'Name:' and the text 'DevConnect Recording Profile' entered.

New Recording Profile Wizard

### Define the Recording Profile Name

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

**Name:**

In the next screen, enter the following values for the specified fields and retain the default values for the remaining fields. Proceed to complete the wizard.

- **Recording type:** “Total”
- **Capture type:** “Active SIP”
- **Audio Compression:** Check this option.

**Define Recording Profile**

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

**Recording type:** Total

**Allocated licenses:** 2

**Capture type:** Active SIP

☒ By Call ☐ By Device

☐ Secondary capture type:

**Select all applicable options:**

☒ Audio Compression

☐ Audio Summation

☐ Encryption

☐ Audio Loss Detection

Back Next Cancel

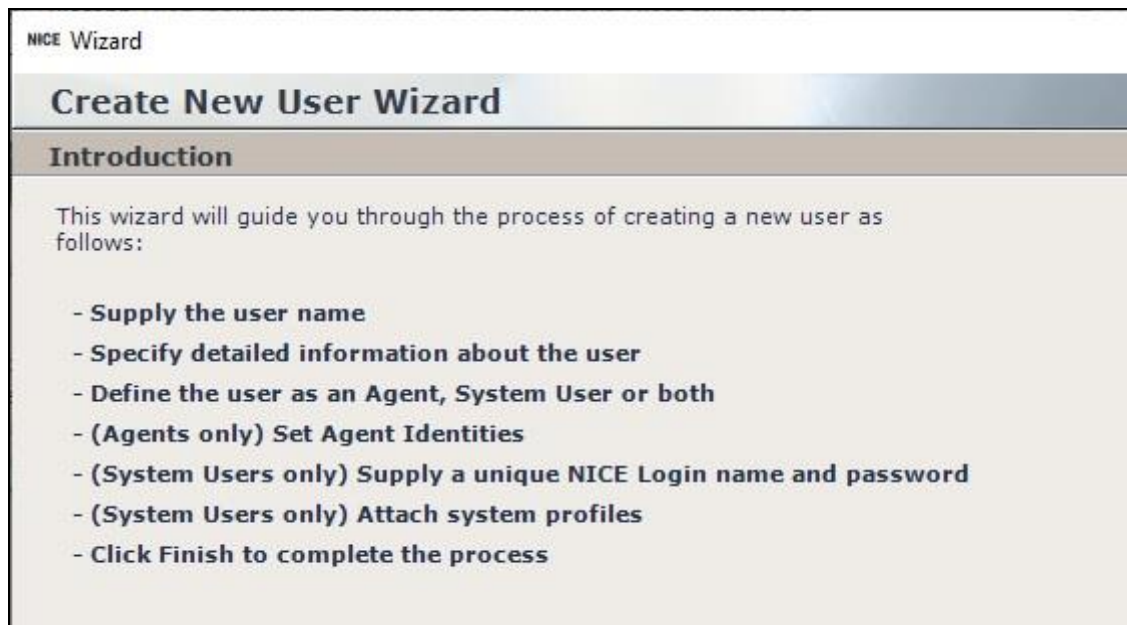


## 8.8. Administer Agent Users

The NICE screen is displayed again. Select **Administration** → **User Administrator** from the top menu, followed by **New User**.



The **Create New User Wizard** pop-up screen is displayed. Click **Next** (not shown).





The **Step 1** screen displayed next. Enter pertinent values for **First Name**, **Last Name**, and **Windows User Name** for the first agent user from **Section 3**. Retain the default values in the remaining fields.

NICE Wizard

### Create New User Wizard Step 1 of 8

#### General Information

Enter the following information. A red asterisk (\*) indicates required fields.

**First Name:** \* Agent1

**Middle Name:**

**Last Name:** \* Avaya

**Email Address:**

**Windows User Name:** \* agent1

**Domain:**

Select a site to associate to the user:

**Site:** Master Site

Proceed to **Step 4** and check the **Agent** user type shown below.

NICE Wizard

### Create New User Wizard Step 4 of 8

#### User Type

Choose one or both user types:

☒ **Agent (User interactions will be recorded/monitored)**

☐ **System User (User will log into NICE applications)**

Proceed to **Step 5** and click **Add**.

NICE Wizard

### Create New User Wizard Step 5 of 8

#### Agent Details

**RTA Agent:** ☐

RTA Agents have permissions to initiate customer authentication, enrollment and consent updates.

Site	Switch	Agent ID	Extension	Email	Alias

**Add**

The **Agent Identity Dialog** pop-up box is displayed. For **Switch**, select the switch name from **Section 8.2**. Select **Extension** and enter the first agent user extension from **Section 3**. Retain the default values in the remaining fields and proceed to complete the wizard.

### Agent Identity Dialog

**Site:** Master Site

**Switch:** Avaya PC/ POM

☐ **Agent ID:**

☒ **Extension:** 65001

☐ **Email:**

☐ **Alias:**

**OK** **Cancel**

Repeat this section to add an agent user for each agent station extension in **Section 3**. In the compliance testing, two agent users were created as shown below.

NICE®

Hello NICE, Superuser | Help | Settings | Logout

**Users Administrator**

My Universe | Business Analyzer | Reporter | Monitor | Insight Manager | ClearSight | PBO Requests | Tools | Administration

Click to scroll Contents list

**All Users**

**General** | Profiles

**All Users**

Search Users:

1 - 6 of 6 User(s)

Name	Type	RTA Agent	Description	Domain	Location
Avaya, Agent1	Agent	No			
Avaya, Agent2	Agent	No			

Reset Password | New User | Delete

## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Proactive Contact, SBCE, and Engage.

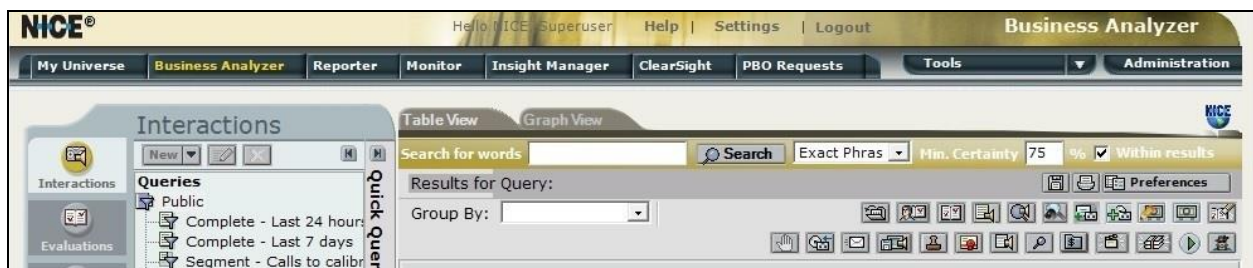
### 9.1. Verify Event Services Connection

Log in to the Linux shell of Proactive Contact and issue the “netstat | grep ensERVER” command. Verify that there is an entry showing an **ESTABLISHED** connection with the IP address of the Engage server running the Interactions Center component, in this case “10.64.101.207”, as shown below.

tcp	0	0	lzpds4b:enserver_ssl	10.64.101.207:58456	ESTABLISHED
tcp	0	0	lzpds4b:enserver_ssl	lzpds4b:32638	ESTABLISHED
tcp	0	0	lzpds4b:32638	lzpds4b:enserver_ssl	ESTABLISHED

### 9.2. Verify SIPREC Recording

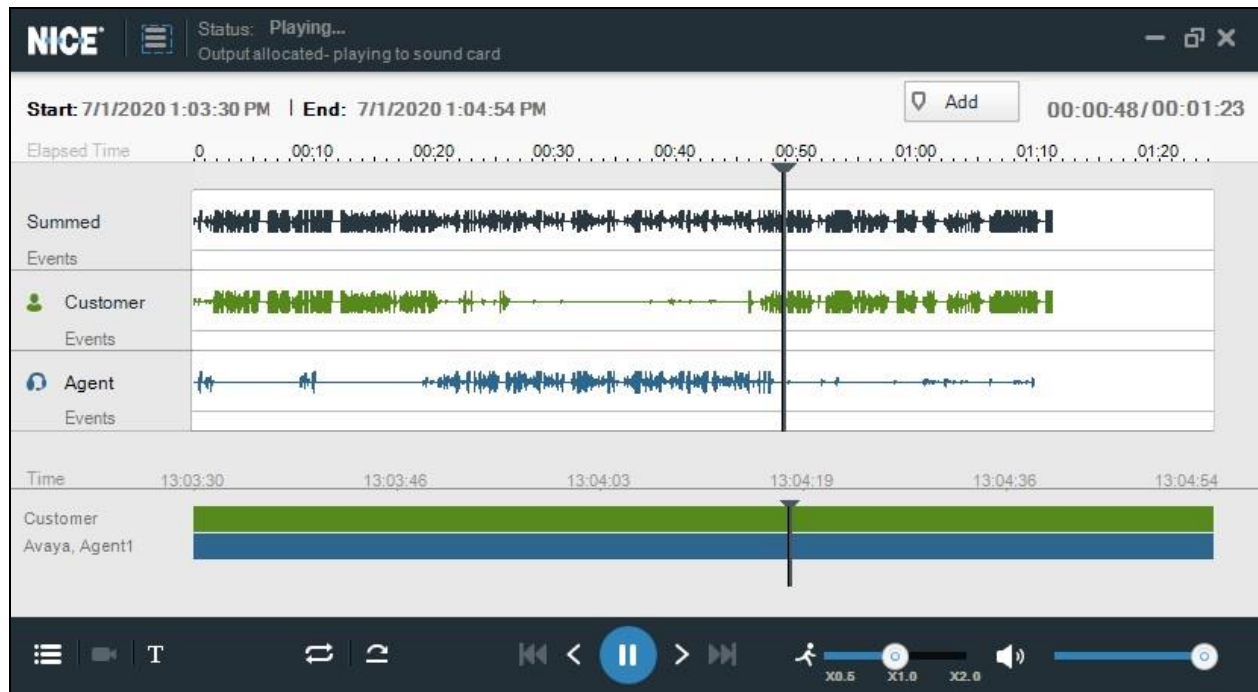
Start an outbound job on Proactive Contact and log an agent in to handle and complete an outbound call. From the NICE screen, select **Business Analyzer** from the top menu to display the screen below. Select **Queries → Public → Complete – Last 24 hours** from the left pane.



Verify that there is an entry in the right pane reflecting the last outbound call, with proper values in the relevant fields. Double click on the entry.



Verify that the pop-up screen below is displayed and that the recording can be played back.



## 10. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform 6.15 to successfully interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Session Border Controller for Enterprise 8.0. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

## 11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 5, November 2019, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 8.1.1, Issue 2, October 2019, available at <http://support.avaya.com>.
3. *Administering Avaya Proactive Contact*, Release 5.2, Issue 1, July 2018, available at <http://support.avaya.com>.
4. *Administering Avaya Session Border Controller for Enterprise*, Release 8.0.x, Issue 4, August 2019, available at <http://support.avaya.com>.
5. *System Administrator Configuration Guide, NICE Engage Platform 6.x*, Revision A4, September 2018, available at <http://www.extranice.com>.
6. *Avaya PC Active-Passive Connectivity Guide, NICE Engage Platform 6.x*, Revision C8, January 2018, available at <http://www.extranice.com>.
7. *Avaya SBCE Switch-Side Preparation Guide, NICE Engage Platform 6.x*, Revision A1, December 2017, available at <http://www.extranice.com>.

---

**©2020 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).