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.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Station</td>
<td>65001 (H.323), 66006 (SIP)</td>
</tr>
</tbody>
</table>

Figure 1: Compliance Testing Configuration
### 4. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager in Virtual Environment</td>
<td>8.1.1 (8.1.1.0.890.25763)</td>
</tr>
<tr>
<td>Avaya G650 Media Gateway</td>
<td>NA HW02 FW025</td>
</tr>
<tr>
<td>• TN464HP DS1 Interface</td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Media Server in Virtual Environment</td>
<td>8.0.1.121</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager in Virtual Environment</td>
<td>8.1.1 (8.1.1.0.811021)</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise in Virtual Environment</td>
<td>8.0 (8.0.0.0.19-16991)</td>
</tr>
<tr>
<td>Avaya Proactive Contact with PG230</td>
<td>5.2.0.1</td>
</tr>
<tr>
<td>• QT1-PRI</td>
<td>2.19</td>
</tr>
<tr>
<td>Avaya Proactive Contact Agent</td>
<td>5.2.0.1</td>
</tr>
<tr>
<td>Avaya 9611G IP Deskphone (H.323)</td>
<td>6.8202</td>
</tr>
<tr>
<td>Avaya 9641G IP Deskphone (SIP)</td>
<td>7.1.6.1.3</td>
</tr>
<tr>
<td>NICE Engage Platform on Windows Server 2016</td>
<td>6.15.0001.77 Standard</td>
</tr>
<tr>
<td>• Application Server</td>
<td></td>
</tr>
<tr>
<td>• Interactions Center</td>
<td></td>
</tr>
<tr>
<td>• Integrations.NSP.SipRecBase.dll</td>
<td>6.15.202.2314</td>
</tr>
<tr>
<td>• Database Server</td>
<td></td>
</tr>
<tr>
<td>• Avaya Proactive Contact Event SDK</td>
<td>5.1.2</td>
</tr>
<tr>
<td>NICE Engage Platform on Windows Server 2016</td>
<td>6.15.0001.77 Standard</td>
</tr>
<tr>
<td>• Advanced Interaction Recorder</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>change system-parameters features</th>
<th>Page 5 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEATURE-RELATED SYSTEM PARAMETERS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SYSTEM PRINTER PARAMETERS</strong></td>
<td></td>
</tr>
<tr>
<td>Endpoint:</td>
<td>Lines Per Page: 60</td>
</tr>
<tr>
<td><strong>SYSTEM-WIDE PARAMETERS</strong></td>
<td></td>
</tr>
<tr>
<td>Switch Name:</td>
<td></td>
</tr>
<tr>
<td>Emergency Extension Forwarding (min): 10</td>
<td></td>
</tr>
<tr>
<td>Enable Inter-Gateway Alternate Routing? n</td>
<td></td>
</tr>
<tr>
<td>Enable Dial Plan Transparency in Survivable Mode? n</td>
<td></td>
</tr>
<tr>
<td>COR to Use for DPT: station</td>
<td></td>
</tr>
<tr>
<td>EC500 Routing in Survivable Mode: dpt-then-ec500</td>
<td></td>
</tr>
<tr>
<td><strong>MALICIOUS CALL TRACE PARAMETERS</strong></td>
<td></td>
</tr>
<tr>
<td>Apply MCT Warning Tone? n</td>
<td>MCT Voice Recorder Trunk Group:</td>
</tr>
<tr>
<td>Delay Sending RE Lease (seconds): 0</td>
<td></td>
</tr>
<tr>
<td><strong>SEND ALL CALLS OPTIONS</strong></td>
<td></td>
</tr>
<tr>
<td>Send All Calls Applies to: station</td>
<td>Auto Inspect on Send All Calls? n</td>
</tr>
<tr>
<td>Preserve previous AUX Work button states after deactivation? n</td>
<td></td>
</tr>
<tr>
<td><strong>UNIVERSAL CALL ID</strong></td>
<td></td>
</tr>
<tr>
<td>Create Universal Call ID (UCID)? y</td>
<td>UCID Network Node ID: 27</td>
</tr>
</tbody>
</table>
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

Codec Set: 1

        IP MEDIA PARAMETERS

        Codec Audio Silence Frames Packet
        Codec Suppression Per Pkt Size(ms)

1: G.711 MU  n  2  20
2: G.729  n  2  20
3:
4:
5:
6:
7:

Media Encryption
Encrypted SRTCP: 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.

- **UUI 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.

```plaintext
add trunk-group 212
TRUNK FEATURES
ACA Assignment? n  Measured: none
Maintenance Tests? y
Suppress # Outpulsing? n  Numbering Format: private
Send UCID? y
UUI Treatment: shared
Maximum Size of UUI Contents: 128
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
Hold/Unhold Notifications? y
Modify Tandem Calling Number: no
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 “lzpdss4b”, as shown below.

```
$ hostname
lzpdss4b
```

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.

<table>
<thead>
<tr>
<th>Tmpl Message R/T</th>
<th>Tmpl Message R/T</th>
<th>Tmpl Message R/T</th>
<th>Tmpl Message R/T</th>
<th>CALLPROC T</th>
</tr>
</thead>
<tbody>
<tr>
<td>SETUP T</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

**ISDN MESSAGE TEMPLATE SUMMARY**

<table>
<thead>
<tr>
<th>IE</th>
<th>BEARER</th>
<th>REP ALL</th>
<th>IE</th>
<th>CHAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA 8090A2</td>
<td>PROCESS</td>
<td>CHAN ID</td>
<td>DATA A98300</td>
<td></td>
</tr>
<tr>
<td>IE</td>
<td>CHAN ID</td>
<td>D FLD 1</td>
<td>CD NUM</td>
<td>IE</td>
</tr>
<tr>
<td>DATA A98300</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IE</td>
<td>CP NUM</td>
<td>D ANI</td>
<td>CP NUM</td>
<td>DATA 04</td>
</tr>
<tr>
<td>DATA 80</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D ANI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IE</td>
<td>CD NUM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA 80</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D FLD 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IE</td>
<td>USR-USR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA 04</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D FLD 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
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”

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.

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

![Routing Profile](image)

### 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.

![Application Rules](image)
The Application Rule pop-up screen is displayed. Enter a desired Rule Name as shown below.

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.
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.
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.

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.
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.

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

![Policy Group pop-up screen](image)

### 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.

![Session Policies](image)
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.
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.
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).

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

![Set New CTI Connection Wizard](image)

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.
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.

![New CTI Connection](image)

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

Proceed to complete the wizard.
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](image)

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](image)
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.

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

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.
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**.

![Configuration Interface](image)

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.
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.

![NICE Services Configuration Manager](image)

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.

![Services](image)
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.

```
Name: DevConnect Pool
Pool type: Basic
Interactions Center: IC_on_AppServer
```

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.
8.7.2. Source Pool

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

![NICE screen with Source Pool](image)

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

![New Source Pool Wizard](image)

**Introduction**

This wizard helps you create a new source pool.

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

1. Define the name, media type, switch, and source type.
2. Select the relevant sources.
3. Verify the summary and approve it.
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.

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

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

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

The screen below is displayed next. Enter a descriptive **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](image-url)
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.

![Create New User Wizard Step 1 of 8](image)

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

![Create New User Wizard Step 4 of 8](image)
Proceed to **Step 5** and click **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.

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.
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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Local Address</th>
<th>Remote Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>lzpds4b:enserver_ssl</td>
<td>10.64.101.207:58456</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp</td>
<td>lzpds4b:enserver_ssl</td>
<td>lzpds4b:32638</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp</td>
<td>lzpds4b:32638</td>
<td>lzpds4b:enserver_ssl</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>

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.


©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.