Application Notes for configuring NICE Engage Platform R6.6 to interoperate with Avaya Aura® Contact Center R7.0.1 and Avaya Aura® Communication Manager R7.0.1 using SIP and DMCC Recording to record calls - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the NICE Engage Platform to interoperate with the Avaya solution consisting of an Avaya Aura® Contact Center R7.0.1 and Avaya Aura® Communication Manager R7.0.1 using SIP Call Recording.

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

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

These Application Notes describe the configuration steps for the NICE Engage Platform R6.6 to interoperate with the Avaya solution consisting of an Avaya Aura® Contact Center R7.0.1, an Avaya Aura® Communication Manager R7.0.1, an Avaya Aura® Session Manager R7.0.1 and an Avaya Aura® Application Enablement Services R7.0.1. NICE Engage uses events from Avaya Aura® Contact Center’s Communication Control Toolkit (CCT) in order to understand when to start and stop the call recordings, basically to know what to record. NICE engage uses SIP recording to record all inbound calls to the Contact Center agents. These inbound calls are skillset calls which are made to the Control Directory Number (CDN) and are routed to the agent. Calls that are made out from the agents phone are recorded using Communication Manager’s Multiple Registrations feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to capture the audio for call recording on outbound calls from the agent’s phone.

SIP Call Recording works by tapping off the Avaya Media Server from the Contact Center, the media is recorded directly from the Avaya Media Server.

DMCC works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with the AES server monitors the digital and VoIP extensions. The application uses the AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call’s aggregated RTP media stream via the recording device and records the call.

The NICE Engage Platform is fully integrated into a LAN (Local Area Network), and includes easy-to-use Web based applications (i.e. Nice Application) that works with the Microsoft .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. This application registers an extension with Communication Manager and waits for that extension to be dialed. The NICE Engage Platform contains tools for audio retrieval, centralized system security authorization, system control, and system status monitoring. Also included is a call parameters database (Nice Application Server) that tightly integrates via CTI link PABXs and ACD’s including optional advanced audio archive database management, search tools, a wide variety of Recording-on-Demand capabilities, and comprehensive long-term call database for immediate retrieval.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the NICE Engage Platform to carry out call recording in a variety of scenarios using SIP and DMCC Multi-Registration with Contact Center, AES and Communication Manager. A range of Avaya endpoints were used in the compliance testing all of which are listed in Section 4.
DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

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

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

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

2.1. Interoperability Compliance Testing

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

- **Calls to and from agent phones** – Inbound calls to the agent’s private number and outbound calls from the agent’s private number.
- **Inbound Skillset calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers.
- **Hold/Transferred/Conference of Skillset calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **Observe CLID/Skillset/DNIS information on Call Recordings** – Ensure that the correct information is displayed on each recording. Information such as CLID, Skillset, DNIS, and Agent information.
- **Serviceability testing** - The behavior of NICE Engage Platform under different simulated failure conditions.

2.2. Test Results

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

1. Agent makes an outbound call using the hard phone.
   Initially there was an issue with this call not being recorded if the outgoing call is made from the hard phone, if the call is made using AAAD then it is recorded. NICE have implemented a fix for this issue and regression testing has been carried out. This fix will be included in the next service pack for NICE Engage release 6.6.
2. Transfer of a Skillset call to a Supervisor.
When an Avaya Contact Center agent (on a skillset call) makes a supervised transfer to a supervisor phone (a phone that is not being monitored by NICE) only leg 1 of the call is being recorded, where both leg1 and the consultation (leg 2) should be recorded. Note this issue only occurs with an agent logged into a H323 phone, for agents logged into a SIP phone this issue does not happen. This issue only occurs when the agent logged into the H323 phone initiates the transfer using the hard phone. If the transfer is made using the AAAD then there is no issue. NICE have implemented a fix for this issue and regression testing has been carried out. This fix will be included in the next service pack for NICE Engage release 6.6

3. Conference between PSTN, CDN and Agent DN with PSTN hanging up first.
Issue with leg 4 of the recording not being recorded for any endpoint making the transfer. NICE have stated that since NICE does not receive a DISCONNECTED event, it is not aware that the customer (PSTN) dropped. So the internal conversation (after customer dropped) will not be recorded by DMCC. This is per design with NICE obtaining events solely from CCT.

4. Conference between PSTN, CDN, Supervisor with PSTN hanging up first.
Issue with leg 4 of the recording not being recorded for any endpoint making the transfer. NICE have stated that since NICE does not receive a DISCONNECTED event, it is not aware that the customer (PSTN) dropped. So the internal conversation (after customer dropped) will not be recorded by DMCC. This is per design with NICE obtaining events solely from CCT.

2.3. Support
Technical support can be obtained for NICE Engage Platform from the website http://www.nice.com/support-and-maintenance
3. Reference Configuration

The configuration in Figure 1 will be used to compliance test NICE Engage with Avaya Aura® Contact Centre R7.0.1 and Avaya Aura® Communication Manager R7.0.1. The NICE Engage Call Recorder has a user defined called Call-Record. The NICE recorder connects to the Avaya Contact Centre CCT using this user. The connection to the CCT allows the NICE Recorder receive CTI events from the Contact Center. The CTI events determine what agent is to be recorded and the RTP recording comes from the Avaya Media Server. When recording calls outside the contact centre environment the NICE application uses DMCC to record the calls.

![Figure 1: Connection of NICE Recording with Avaya Aura® Contact Centre R7.0.1](image)

Figure 1: Connection of NICE Recording with Avaya Aura® Contact Centre R7.0.1
## 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® System Manager running on a virtual server</td>
<td>System Manager 7.0.1.2 Build No. - 7.0.0.0.16266</td>
</tr>
<tr>
<td></td>
<td>Software Update Revision No: 7.0.1.2.086007 Service Pack 2</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager running on a virtual server</td>
<td>Session Manager R7.0 SP2 Build No. – 7.0.1.2.701230</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager running on a virtual server</td>
<td>R7.0.1 R017x.00.0.441.0 00.0.441.0-23523</td>
</tr>
<tr>
<td>Avaya Media Server running on a virtual server</td>
<td>Media Server SYSTEM R7.7.0.21 Media Server R7.7.0.350</td>
</tr>
<tr>
<td>Avaya Aura® Contact Center running on an Windows 2012 R2 Server</td>
<td>R7.0.1.0 Feature Pack 1</td>
</tr>
<tr>
<td>Avaya 9608 H323 Deskphone</td>
<td>Release 6.6.028</td>
</tr>
<tr>
<td>Avaya 9608 SIP Deskphone</td>
<td>Release 7.0.0.39</td>
</tr>
<tr>
<td>Avaya Aura® Agent Desktop Display</td>
<td>R7.0.1.0 Feature Pack 1</td>
</tr>
<tr>
<td>NICE Engage</td>
<td></td>
</tr>
<tr>
<td>- NICE Engage Application Server</td>
<td>R6.6</td>
</tr>
<tr>
<td>- NICE Engage Active Server</td>
<td></td>
</tr>
<tr>
<td>- NICE Engage NDM Server</td>
<td></td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in Section 10.

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

5.1. Verify System Features

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

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

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

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

```plaintext
<table>
<thead>
<tr>
<th>IP NODE NAMES</th>
<th>Page 1 of 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>IP Address</td>
</tr>
<tr>
<td>sm70vmpg</td>
<td>10.10.40.12</td>
</tr>
<tr>
<td>aes70vmpg</td>
<td>10.10.40.26</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>g450</td>
<td>10.10.40.15</td>
</tr>
<tr>
<td>procr</td>
<td>10.10.40.13</td>
</tr>
</tbody>
</table>
```
5.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the change ip-services command. On Page 1 add an entry with the following values:

- **Service Type:** Should be set to AESVCS.
- **Enabled:** Set to y.
- **Local Node:** Set to the node name assigned for the procr in Section 5.2
- **Local Port:** Retain the default value of 8765.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Enabled</th>
<th>Local Node</th>
<th>Local Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AESVCS</td>
<td>y</td>
<td>procr</td>
<td>8765</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Server ID</th>
<th>AE Services Server</th>
<th>Password</th>
<th>Enabled</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>aes70vmpg</td>
<td>********</td>
<td>y</td>
<td>idle</td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.4. Configure CTI Link for TSAPI Service

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

```
add cti-link 1
```

CTI Link: 1
Extension: 2002
Type: ADJ-IP
Name: aes70vmpg

COR: 1
5.5. Configure Network Region

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

```
change ip-network-region 1

IP NETWORK REGION
Region: 1
Location: 1
Name: default
Authoritative Domain: devconnect.local

MEDIA PARAMETERS
Codec Set: 1
Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048
UDP Port Max: 3329

DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26

802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5

AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5

RTCP REPORTING TO MONITOR SERVER PARAMETERS
RTCP Reporting to Monitor Server Enabled? y

Use Default Server Parameters? y
```
INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
Incoming LDN Extension:
Conversion To Full Public Number - Delete: Insert:
Maximum Number of Trunks to Use for IGAR:
Dial Plan Transparency in Survivable Mode? n
BACKUP SERVERS (IN PRIORITY ORDER)    H.323 SECURITY PROFILES
1    1    challenge
2    2
3    3
4    4
5
6    Allow SIP URI Conversion? y
TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
Near End Establishes TCP Signaling Socket? y
Near End TCP Port Min: 61440
Near End TCP Port Max: 61444

Source Region: 1    Inter Network Region Connection Management    I    M
G    A    t
dst codec direct WAN-BW-limits Video Intervening Dyn A G c
rgn set WAN Units Total Norm Prio Shr Regions CAC R L e
1    1    all
2
3
4
5
6
7
8
9
10
11
12
13
14
15
5.6. Configure H323 Stations for Multi-Registration

All endpoints that are to be monitored by NICE will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multi-Registration to work. Type `change station x` where x is the extension number of the station to be monitored also note this extension number for configuration required in Section 8.2 and Section 8.3. Note the Security Code and ensure that IP SoftPhone is set to y.

<table>
<thead>
<tr>
<th>change station x</th>
<th>PAGE 1 of 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension: x</td>
<td>Lock Messages? n BCC: 0</td>
</tr>
<tr>
<td>Type: 9608</td>
<td>Security Code: 1234 TN: 1</td>
</tr>
<tr>
<td>Port: S00101</td>
<td>Coverage Path 1: COR: 1</td>
</tr>
<tr>
<td>Name: Extension</td>
<td>Coverage Path 2: COS: 1</td>
</tr>
</tbody>
</table>

**STATION**

<table>
<thead>
<tr>
<th>Time of Day Lock Table:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss Group: 19</td>
</tr>
<tr>
<td>Personalized Ringing Pattern: 1</td>
</tr>
<tr>
<td>Message Lamp Ext: 1591</td>
</tr>
</tbody>
</table>

**STATION OPTIONS**

<table>
<thead>
<tr>
<th>Mute Button Enabled? y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speakerphone: 2-way</td>
</tr>
<tr>
<td>Display Language: english</td>
</tr>
<tr>
<td>Survivable GK Node Name:</td>
</tr>
<tr>
<td>Survivable COR: internal</td>
</tr>
<tr>
<td>Survivable Trunk Dest? y</td>
</tr>
</tbody>
</table>

**Survivable Trunk Dest**

<table>
<thead>
<tr>
<th>Media Complex Ext:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IP SoftPhone? y</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IP Video Softphone? n</th>
</tr>
</thead>
</table>

| Short/Prefixed Registration Allowed: default |

| Display Language: english |

<table>
<thead>
<tr>
<th>Survivable Trunk Dest? y</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Media Complex Ext:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IP SoftPhone? y</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IP Video Softphone? n</th>
</tr>
</thead>
</table>

| Short/Prefixed Registration Allowed: default |
5.7. Configure SIP Stations for Multi-Registration

Any SIP extension that is to be recorded requires some configuration changes to allow call recording using multiple registration. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering http://<FQDN>/SMGR, where <FQDN> is the fully qualified domain name of System Manager or http://<IP Address>/SMGR. Log in using appropriate credentials.

Note: The following shows changes of a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.

From the home page click on User Management highlighted below.
Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.

Click on the **Communication Profile** tab. Ensure that the **Communication Profile Password** is known and if not click on edit to change it.
From the same page scroll down to **CM Endpoint Profile** click on **Endpoint Editor** to make further changes.
In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done**, at the bottom of the screen, once this is set.
Click on **Commit** once this is done to save the changes.
6. Configure Avaya Aura® Application Enablement Services

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

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

6.1. Verify Licensing

To access the AES Management Console, enter `https://<ip-addr>` as the URL in an Internet browser, where `<ip-addr>` is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the Login button.
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface ➔ Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.
In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the `change ip-services` command, described in **Section 5.3**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

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

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

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

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

Once completed, select Apply Changes.
Another screen appears for confirmation of the changes made. Choose **Apply**.

When the TSAPI Link is completed, it should resemble the screen below.
The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to Maintenance → Service Controller. On the Service Controller screen, tick the TSAPI Service and select Restart Service.
6.4. Enable TSAPI and DMCC Ports

To ensure the DMCC and TSAPI ports are enabled, navigate to Networking → Ports. Ensure that the TSAPI ports are set to Enabled as shown below. Ensure that the DMCC Server Ports are also Enabled and take note of the Encrypted Port 4722 which will be used later in Section 8.3.
6.5. Create CTI User
A User ID and password needs to be configured for the NICE Engage Platform to communicate with the Application Enablement Services server. Navigate to the User Management → User Admin screen then choose the Add User option.
In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the NICE Engage Platform setup in **Section 8.3**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with NICE Engage Platform setup in **Section 8.3**.
- **CT User** - Select **Yes** from the drop-down menu.

Scroll down and click on **Apply Changes**.
6.6. Associate Devices with CTI User

Navigate to Security → Security Database → CTI Users → List All Users. Select the CTI user added in Section 6.5 and click on Edit Users.

In the main window ensure that Unrestricted Access is ticked. Once this is done click on Apply Changes.
7. Configure Avaya Aura® Contact Center

A new CCT user must be added for NICE in order for NICE to log into Web Services and receive events from CCT. This new user must have all monitored agents associated with it also. This new user must be created on the domain and if there is no domain then created on the Contact Center server itself as is the case as shown below.

7.1. Create a new domain user

Open Computer Management and right-click on Users and select New User.

![Computer Management](image)
Enter the **User name** and the **Password** as shown below, this password should never expire. Click on **Create** at the bottom of the screen.

![New User form](image)

**7.2. Create a CCT user**

Open a web browser and navigate to `https://<Contact Center Server>`. Enter the appropriate **User ID** and **Password** and click on **Login**.

![Contact Center - Manager](image)
Click on **Configuration**, as shown below.

Navigate to the CCT server on the left window and click on the URL in the main window. This can be a http session or the more secure https session.

Right-click on **Users** in the left window and click on **Add new User**, as shown below.
Enter the user’s details such as the **Login User Name** which will be in the format domain\username as shown below, where the domain name is the Contact Center’s hostname. This will be the same username that was created in **Section 7.1**.
Click on **Agent Assignments** to open this and add the required agents that are to be monitored. Then click on **Save** at the bottom of the screen.

**Note:** This step is optional and required only if After Call Work and CCT Agent Name information is required. It does not affect CTI events or recording.
7.3. Configure CCT Web Services
Open the CCT console from the Contact Center server.

Navigate to CCT Web Services in the left window and click on Enable CCT Web Services, click on Enable SIP Call Recording and enter the CCT user that was created in Section 7.1. In the right window under CCT Web Services click on Apply Changes to save these changes.
8. Configure NICE Engage Platform

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

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

![Login to NICE Engage Solutions](image.png)
Once logged in expand the **Administration** dropdown menu and click on **System Administrator** as highlighted.

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

Navigate to Master Site → Interactions Centers → <Interaction> in the left window, (the name may be different than AvayaIC_on_appSvr depending on the system installed). From the main window, click on the Configuration tab, in the resulting window underneath click on Call Server and scroll to ExcludeUnmonitoredFromRecording as shown below. Ensure that this is set to TRUE.
8.2. New CCT CTI Connection (using CTI Connection Wizard)

Navigate to Master Site → CTI Integration in the left window then right-click on CTI Integration and select New CTI Connection as shown below.

The New CTI Connection Wizard is opened and this will go through the 17 steps required to setup the connection to the AES to receive events. Click on Next to continue.
The value for **Regular Interactions Center** is a value that was already created during the installation of the NICE Engage platform. This value is therefore pre-chosen for the CTI connection being created below.

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

Select **CCT** for the **Avaya CM CTI Interface**, ensure **Active Recording** box is checked and that **CCT** is chosen then click on **Next** to continue.
The following few steps involve entering the CCT information into the NICE configuration. Double-click on each **Parameter** to enter a value for that parameter. The first parameter is **Username** as shown below. This **nicecct** is the username setup in **Section 7.1** and **Section 7.2**.

Double-click on **Password** and enter the **Value** from **Section 7.1**.
Double-click on **Domain** and enter the **Value** for the domain. In the example below there was no domain used so this value is the hostname of the Contact Center server.

Double-click on **Address** and enter the IP address or hostname of the Contact Center server. Like in the case above this is the hostname of the Contact Center server.
The other values can be left as default which is shown below. Click on **Next** once these values are all filled in.

Enter the hostname of the NICE Application Server for the **Server IP/Hostname**, choose a suitable **Connection Manager port** and Click on + icon as shown below.
Once it is added, click on **Next** to continue.
The devices that are to be monitored are now chosen. Click on Add to add these devices. Fill in the details of the extension that is to be monitored. In the example below Communication Manager extension/station 7000 was added. Repeat this for all the Communication Manager extensions that need to be added. If there are many, a range of extensions can be added together using the Add Range button below and this will save time in doing them one by one.
Check the box for **Call Flow Analysis** in the next screen.

Select the next available Connection Manager port and click on **Next** to continue. Note that the next available port will be displayed by default.
Click on **Finish** to complete the new CTI Connection for CCT.
8.3. New DMCC CTI Interface (using CTI Interface Wizard)

Navigate to Master Site → CTI Integrations → CTI Interfaces → New CTI Interface in the left window.

This will open the CTI Interface Wizard, click on Next to continue.
Enter a suitable Name and select the Telephony Switch that was created in Section 8.2. Click on Next to continue.

The following steps involve entering the information for connecting to the AES for DMCC recording. Double-click on PrimaryAESServerAddress and enter the IP address of the AES.
Double-click on **PrimaryAESUserName** and enter the username created in Section 6.5.

![Interface Connection Details](image1.png)

Double-click on the **PrimaryAESPassword** and enter the AES password created in Section 6.5.

![Interface Connection Details](image2.png)
For this setup a secure connection was configured so the **PrimaryAESDMCCPort** is set to 4722 and the **PrimaryAESSecuredConnection** is set to **TRUE**, these are set as this by default so there is no need to set these. Click on **Next** to continue.
Any Communication Manager extensions/stations that are to be recorded or monitored are added in the section. Click on **Add**, to add one extension or the possibility to add a whole range of extensions is possible by clicking on **Add Range**.

Double-click on **Observation Type** above.
Opening **ObservationType** from the previous page gives the following window where the **Value** is set to **Non-Resource-Based**.

Choosing Non-Resource-Based above will result in the screen below where other values can be set. Double-click on **SymbolicName** and enter the host name of Communication Manager.
Double-click on **Password** and enter the password for the extension that was configured in **Section 5.6**.

![Add Device](image1)

Double-click on **CodecsList** and select the required Codecs.

![CodecsList](image2)
Double-click on EncAlgList and check the box for **No_ENCRYPTION** as shown below. This is because as stated in **Section 2**, calls using TLS/SRTP are not being tested on this occasion.
With all the information on this/these extension(s) added, click on **OK** to continue.
As explained before either one or many extensions can be added using **Add** or **Add Range**. When the required extensions have been added click on **Next** to continue.

Click on **Finish** to complete the setup of the CTI Interface for DMCC.
8.4. New DMCC Connection (using Connection Manager)

Navigate to Master Site → Connection Manager → New Connection Manager, in the left window.

The **Connection Manager Wizard** is opened. Click on **Next** to continue.
Enter a suitable **Name** and enter the **Hostname** of the NICE call recorder, the IP address could also be entered. Enter the appropriate **Port** number and click on **Next** to continue.

Add the CTI Interface for **DMCC Recording** (created in **Section 8.3**) and click on **Next** to continue.
Click on **Finish** to complete the setup.
8.5. Add a new Media Provider Controller for DMCC (using Media Provider Controller Wizard)

From the left window navigate to Master Site → CTI Integrations → Media Providers → New Media Provider Controller.

Click on Next to continue.
Select the **Media Provider Controller Type** as shown below and click on **Next** to continue.

![Media Provider Controller Type](image1)

Enter a suitable **Name** and enter the **Hostname** or IP address of the NICE recorder. Click on **Next** to continue.

![General Information](image2)
Select the DMCC Connection Manager that was created in Section 8.4 and click on Next to continue.

Click on Finish to complete the setup of the Media Provider Controller.
8.6. System Mapping
This section involves mapping the connections to the recorders and it involves adding a new Recorder Pool, a new Source Pool and a new Recording Profile.

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

Enter a suitable Name for the Recorder Pool and select the Active_Logger from the list of Available Recorders and click on Update to continue.
8.6.2. Add a new Source Pool

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

Click on Next to continue to add a new Source Pool.
Enter a suitable Name and select the Switch connection that was created in Section 8.2. Media type should be set to Audio and Source type should be set to Device. Click on Next to continue.

Select the monitored extensions that were added in Section 8.2 and Section 8.3 and click on Next to continue.
Click on **Finish** to complete the **New Source Pool Wizard**.

### 8.6.3. Add a new Recording Profile

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

Enter a suitable **Name** for the **Recording Profile** and click on **Next** to continue.
Highlight the **Available source pools** and the **Available Recorder pools** and click on **Next**.

The **Recording type** should be set to **Interaction-based** and the **Capture type** should be set to **Active SIP Mono**. The **Secondary capture type** box is checked and in here **Active DMCC MR** is chosen. **Audio Compression** is selected by default. Click on **Next** to continue.
Click on **Finish** to complete these changes.

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

This concludes the setup of the NICE Application Server for SIP and DMCC call recording.
9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager CTI Service State

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

```
status aesvcs cti-link
```

<table>
<thead>
<tr>
<th>CTI Link</th>
<th>Version</th>
<th>Mnt</th>
<th>Busy</th>
<th>AE Services</th>
<th>Service State</th>
<th>Mgs Sent</th>
<th>Mgs Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>no</td>
<td>aes70vmpg</td>
<td>established</td>
<td>18</td>
<td>18</td>
<td></td>
</tr>
</tbody>
</table>

9.2. Verify DMCC link on AES

Verify the status of the DMCC link by selecting Status \(\rightarrow\) Status and Control \(\rightarrow\) DMCC Service Summary to display the DMCC Service Summary – Session Summary screen. The screen below shows that the user NICE is connected from the IP address 10.10.40.126, which is the NICE Application server.
9.3. Verify calls are being recorded

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

Open a browser session to the NICE Application Server as is shown below. Enter the proper credentials and click on Login.
Click on **Business Analyser** at the top of the screen. Select **Interactions** from the left window and then navigate to **Queries → Public**.

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

If these recordings are not present or cannot be played back the NICE services may not be running or may need to be restarted. There are two separate servers as a part of this NICE Engage Platform. The NICE Application Server and the NICE Advanced Interactions Server can be logged into and checked to ensure all services beginning with NICE are running correctly. As a last resort both servers may need a reboot after the initial configuration.
10. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform to successfully interoperate with Avaya Aura® Contact Center R7.0.1 and Avaya Aura® Communication Manager R7.0.1 using SIP recording and DMCC Multi-Registration to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in Section 2.2.

11. Additional References

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

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

[4] Avaya Aura® Session Manager Overview, Doc # 03603323Avaya Aura ® Contact Centre SIP Commissioning, Doc # NN44400-511, Release 7.0

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