Abstract

These Application Notes describe how to configure the NICE Call Recording System with the Avaya Application Enablement Services and Avaya Communication Manager to record incoming and outgoing phone calls. The configuration described in these Application Notes focuses on the NICE Call Recording system designed for Public Safety Answering Point call takers.

Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab at the request of the Solutions Marketing Team.
# TABLE OF CONTENTS

1. Introduction .................................................................................................................... 3
   1.1. Public Safety Solution Overview .............................................................................. 3
   1.2. NICE Call Flows ....................................................................................................... 4
   1.3. Interoperability Compliance Testing ........................................................................ 4
   1.4. Support .................................................................................................................... 4
2. Configuration .................................................................................................................... 5
   2.1. Public Safety Solution Reference Configuration ..................................................... 5
   2.2. Network Configuration ............................................................................................. 6
3. Equipment and Software Validated .................................................................................. 7
4. Configure Avaya Communication Manager .................................................................. 7
   4.1. Verify Avaya Communication Manager License ....................................................... 8
   4.2. Administer IP Node Name for C-LAN ..................................................................... 9
   4.3. Administer IP Interface for C-LAN ......................................................................... 10
   4.4. Administer Data Module for C-LAN ....................................................................... 11
   4.5. Administer IP Services for AES Transport Link ...................................................... 11
   4.6. Administer CTI Link for TSAPI Service ................................................................... 12
   4.7. Administer Stations for NICE ................................................................................ 12
   4.8. Administer COR for Virtual and Monitored Stations .............................................. 14
   4.9. Administer Feature Access code for Service Observing ........................................ 15
   4.10. Administer System Parameters ............................................................................. 15
5. Configure Avaya Application Enablement Services ....................................................... 17
   5.1. Verify Avaya Application Enablement Services License ....................................... 17
   5.2. Administer Local IP ............................................................................................... 19
   5.3. Administer Switch Connection .............................................................................. 19
   5.4. Administer TSAPI Link ......................................................................................... 21
   5.5. Administer Security Database ............................................................................... 22
   5.6. Obtain Tlink Name ............................................................................................... 24
   5.7. Administer NICE Users ......................................................................................... 24
   5.8. Administer Device Groups ................................................................................... 26
   5.9. Restart TSAPI Service ........................................................................................... 29
6. Configure NICE Call Recording System ...................................................................... 30
   6.1. Configure NiceCLS server .................................................................................... 30
   6.2. Configure the NICE Application Tools ................................................................. 41
7. General Test Approach and Test Results ...................................................................... 46
8. Verification ...................................................................................................................... 46
   8.1. Verify Avaya Communication Manager ................................................................. 46
   8.2. Verify Avaya Application Enablement Services .................................................... 47
   8.3. Verify Call Recording and Playback from the NICE Query and Monitor ................ 49
9. Terminology .................................................................................................................... 50
10. Conclusion ...................................................................................................................... 50
11. Additional References ................................................................................................. 50
1. Introduction

These Application Notes describe how to configure the NICE Call Recording System with the Avaya Application Enablement Services (AES) and Avaya Communication Manager to record incoming and outgoing phone calls. The configuration described in these Application Notes focuses on the NICE Call Recording system designed for Public Safety Answering Point call takers.

NICE Call Recording System for Public Safety is comprised of NICE CLS 8.90.4 and VoIP Logger 9.10.05. The integration with Avaya Communication Manager is achieved through the Application Enablement Services – Telephony Services Application Programming Interface (TSAPI) & Device, Media and Call Control Interface (DMCC) services.

The NICE CLS uses Avaya AES to register IP Softphones and receive call status and call events from Avaya Communication Manager. The VoIP Logger creates recording channels which emulate IP Softphones to receive audio streams. The NICE CLS Server manages an SQL database including extensive call details. Using NICE application tools, recorded calls with call detail information can be queried and played back.

For the Public Safety solution, NICE Call Recording application is achieved through the Avaya Communication Manager service observing feature. This option is selected at the installation phase in NICE application. (Note: NICE recording features can be enabled or disabled during the software installation only). This option allows automatic recording of entire calls for all configured stations. NICE application uses TSAPI of Avaya AES to observe and record the calls. This mode uses DMCC controlled IP softphones that are automatically allocated in NICE as shared ports for call recording.

1.1. Public Safety Solution Overview

The Avaya Public Safety Solution is designed to help government and private agencies responsible for the delivery of public safety services to enterprises and civilian populations. This includes:

- **Avaya Contact Center** applications such as expert agent selection to ensure the most qualified and most available resource rapidly attends to the case.

- **PlantCML Sentinel CM and Intelligent Work Station** integration which provides the public safety community with call-center solutions designed to streamline emergency call-taking. Sentinel CM is a 911 incident management solution, and integration with Avaya Communication Manager is achieved through the Avaya Application Enablement Services (AES) Telephony Services Application Programming Interface (TSAPI) & Device, Media and Call Control Interface (DMCC) services.

- **Raytheon JPS ACU-2000IP Intelligent Interconnect System** integration which provides seamless communication across traditionally disparate communications such as Land-based Mobile Radio (LMR). The ACU-2000IP is a radio IP/SIP gateway that
allows IP-PBX stations to interface with radios. Multiple interface cards allow all radios to be a part of the IP-PBX system. Integration with Avaya Communication Manager is achieved through the SIP Enablement Services (SES).

NICE CLS/VoIP Logger integration for secure recording of audio on the entire chain of service delivery from the conversations with the citizen, to command and control and dispatch, to resolution.

1.2. NICE Call Flows

1. NICE CLS connects to the AES DMCC services and requests to initiate the emulation of IP Softphones, registering one phone per recording channel.

2. NICE CLS receives a Start call event from the AES.

3. Based on the user defined recording rules, NICE CLS determines whether the call needs to be recorded. If so, NICE CLS allocates an IP address and port for recording on the VoIP Logger and sends a request, to Avaya Communication Manager via the AES to observe the call.

4. Avaya Communication Manager sends audio RTP streams to the NICE VoIP Logger and it records the audio in the allocated recording channel.

5. When the call ends, NICE CLS requests to stop recording the call.

1.3. Interoperability Compliance Testing

Interoperability compliance testing focused on NICE Call Recording System’s ability to work with Avaya Application Enablement Services Release 4.2.1 and Avaya Communication Manager Release 5. Call recording and playback was verified for incoming/outgoing calls. In addition, phone features like hold, conference calls and transfers were exercised while the call is being recorded. The call recording functionality was verified for incoming and outgoing trunk calls, IP, SIP, Analog and DCP stations.

1.4. Support

Technical support on NICE can be obtained at www.nice.com.
2. Configuration

2.1. Public Safety Solution Reference Configuration

The reference configurations for Public Safety Solution are shown below in Figure 1.

![Figure 1: Avaya Public Safety Solution Reference Configuration](image-url)
2.2. Network Configuration

The network implemented for the reference configuration is shown in Figure 2. The Public Safety Answering Point location consists of Avaya S8720 Servers controlling G650 Media Gateways. The PSAP location is also equipped with a pair of Avaya Application Enablement Services (AES) servers, Avaya IP phones, a pair of PlantCML Sentinel CM servers and multiple Sentinel 9-1-1 clients. Please refer to [4] for PlantCML Sentinel CM configuration details.

Figure 2: Network Configuration Diagram
3. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Device Description</th>
<th>Versions Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Communication Manager S8720 Servers</td>
<td>Release 5.0 (R015x.00.0.825.4)</td>
</tr>
<tr>
<td>Avaya G650 Media Gateway IPSI (TN2312BP)</td>
<td>- HW15 FW044</td>
</tr>
<tr>
<td></td>
<td>- CLAN (TN799DP)</td>
</tr>
<tr>
<td></td>
<td>- MedPro (TN2602AP )</td>
</tr>
<tr>
<td>Avaya AES</td>
<td>Release 4.2.1 (Build 20-5)</td>
</tr>
<tr>
<td>Avaya 4600 Series H.323 Telephones</td>
<td>R2.8</td>
</tr>
<tr>
<td>Avaya 9600 Series H.323 Telephones</td>
<td>R1.5</td>
</tr>
<tr>
<td>Avaya IP Softphone</td>
<td>R6.0</td>
</tr>
<tr>
<td>Avaya 6211 Analog Telephones</td>
<td>N/A</td>
</tr>
<tr>
<td>Avaya 2420 Digital Telephones</td>
<td>N/A</td>
</tr>
<tr>
<td>PlantCML Sentinel</td>
<td>Release 2 (Build 7)</td>
</tr>
<tr>
<td></td>
<td>OS for the IWS is Windows XP Professional SP 2</td>
</tr>
<tr>
<td>NICE Call Recording</td>
<td>8.90.4</td>
</tr>
<tr>
<td></td>
<td>9.10.05</td>
</tr>
</tbody>
</table>

4. Configure Avaya Communication Manager

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

- Verify Avaya Communication Manager License
- Administer IP node name for C-LAN
- Administer IP interface for C-LAN
- Administer data module for C-LAN
- Administer IP services for AES transport link
- Administer CTI link for TSAPI service
- Administer stations for NICE
- Administer system parameters
- Administer feature access codes
4.1. Verify Avaya Communication Manager License

Log into the System Access Terminal (SAT) to verify that Avaya Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters parameter-options” command to verify that the ASAI Link Core Capabilities, and Computer Telephony Adjunct Links customer option is set to “y” on Page 3. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

```
<table>
<thead>
<tr>
<th>服務</th>
<th>行動</th>
<th>權限</th>
<th>支援</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAI Link Core Capabilities</td>
<td>y</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Computer Telephony Adjunct Links</td>
<td>y</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
```

Navigate to Page 6, and verify that the Service Observing (Basic) and Service Observing (Remote/By FAC) are set to “y”. NICE Call Recording applications will use the Avaya Communication Manager feature Service Observing with Multiple Observers. Multiple observers on the same call is not supported for Service Observing by VDN feature.

```
<table>
<thead>
<tr>
<th>服務</th>
<th>行動</th>
<th>權限</th>
<th>支援</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCMS (Basic)</td>
<td>y</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Service Observing (Basic)</td>
<td>y</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Navigate to Page 10, and verify that there are sufficient **IP_API_A** licenses.

```
<table>
<thead>
<tr>
<th>產品 識別碼</th>
<th>版本限制</th>
<th>已使用</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_API_A</td>
<td>100</td>
<td>4</td>
</tr>
<tr>
<td>IP_API_B</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>IP_API_C</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>IP_Agent</td>
<td>300</td>
<td>0</td>
</tr>
<tr>
<td>IP_IR_A</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP_Phone</td>
<td>12000</td>
<td>5</td>
</tr>
<tr>
<td>IP_ROMax</td>
<td>12000</td>
<td>0</td>
</tr>
<tr>
<td>IP_Soft</td>
<td>300</td>
<td>0</td>
</tr>
<tr>
<td>IP_eCons</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
4.2. Administer IP Node Name for C-LAN

Enter the “change node-names ip” command, and add an entry for the C-LAN that will be used for connectivity to the AES server. For the sample configuration, use the following in the Name and IP Address. The actual node name and IP address may vary. Submit these changes.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAN-01A02</td>
<td>9.1.1.8</td>
</tr>
<tr>
<td>CLAN-01B02</td>
<td>9.1.1.9</td>
</tr>
</tbody>
</table>

change node-names ip

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES1</td>
<td>9.1.1.50</td>
</tr>
<tr>
<td>CLAN-01A02</td>
<td>9.1.1.8</td>
</tr>
<tr>
<td>CLAN-01B02</td>
<td>9.1.1.9</td>
</tr>
<tr>
<td>CLAN-RETAIL</td>
<td>30.1.1.4</td>
</tr>
<tr>
<td>FCSWinsuite</td>
<td>9.1.1.203</td>
</tr>
<tr>
<td>GVT-S8300-LSP</td>
<td>9.1.4.2</td>
</tr>
<tr>
<td>MedPro-01A03</td>
<td>9.1.1.5</td>
</tr>
<tr>
<td>MedPro-01B07</td>
<td>9.1.1.6</td>
</tr>
<tr>
<td>RedSky1</td>
<td>9.1.1.55</td>
</tr>
<tr>
<td>RedSky2</td>
<td>9.1.1.56</td>
</tr>
<tr>
<td>S8500-ESS</td>
<td>9.1.1.13</td>
</tr>
<tr>
<td>SES1</td>
<td>9.1.1.34</td>
</tr>
<tr>
<td>VAL-01A12</td>
<td>9.1.1.12</td>
</tr>
<tr>
<td>clan-trade</td>
<td>5.1.1.4</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>govmas1</td>
<td>9.1.1.31</td>
</tr>
</tbody>
</table>

(16 of 17 administered node-names were displayed)

Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
### 4.3. Administer IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface <board location>” command. In the sample configuration, “1a02” for CLAN-01A02 and “1b02” for CLAN-01B02” will be used. Note that the actual slot number may vary. Enter the C-LAN node name assigned from Section 4.2 into the Node Name field. The IP Address field will be populated automatically.

Enter proper values for the Subnet Mask and Gateway Address fields. Set the Enable Ethernet Port field to “y”, and select the appropriate Network Region for the C-LAN dedicated for AES connectivity. Default values may be used in the remaining fields. For the sample configuration, Network Region 1 is used. Submit these changes.

<table>
<thead>
<tr>
<th>add ip-interface 1a02</th>
<th>IP INTERFACES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type:</strong> C-LAN</td>
<td><strong>Slot:</strong> 01A02</td>
</tr>
<tr>
<td><strong>Code/Suffix:</strong> TN799 D</td>
<td><strong>Node Name:</strong> CLAN-01A02</td>
</tr>
<tr>
<td><strong>IP Address:</strong> 9.1.1.8</td>
<td><strong>Subnet Mask:</strong> 255.255.255.0</td>
</tr>
<tr>
<td><strong>Gateway Address:</strong> 9.1.1.1</td>
<td><strong>Enable Ethernet Port:</strong> y</td>
</tr>
<tr>
<td><strong>Allow H.323 Endpoints:</strong> y</td>
<td><strong>Allow H.248 Gateways:</strong> n</td>
</tr>
<tr>
<td><strong>Network Region:</strong> 1</td>
<td><strong>VLAN:</strong> n</td>
</tr>
<tr>
<td><strong>Gatekeeper Priority:</strong> 1</td>
<td><strong>Target socket load and Warning level:</strong> 400</td>
</tr>
<tr>
<td><strong>Receive Buffer TCP Window Size:</strong> 8320</td>
<td><strong>ETHERNET OPTIONS</strong></td>
</tr>
<tr>
<td><strong>Auto:</strong> y</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>add ip-interface 1b02</th>
<th>IP INTERFACES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type:</strong> C-LAN</td>
<td><strong>Slot:</strong> 01B02</td>
</tr>
<tr>
<td><strong>Code/Suffix:</strong> TN799 D</td>
<td><strong>Node Name:</strong> CLAN-01B02</td>
</tr>
<tr>
<td><strong>IP Address:</strong> 9.1.1.9</td>
<td><strong>Subnet Mask:</strong> 255.255.255.0</td>
</tr>
<tr>
<td><strong>Gateway Address:</strong> 9.1.1.1</td>
<td><strong>Enable Ethernet Port:</strong> y</td>
</tr>
<tr>
<td><strong>Allow H.323 Endpoints:</strong> y</td>
<td><strong>Allow H.248 Gateways:</strong> n</td>
</tr>
<tr>
<td><strong>Network Region:</strong> 1</td>
<td><strong>VLAN:</strong> n</td>
</tr>
<tr>
<td><strong>Gatekeeper Priority:</strong> 1</td>
<td><strong>Target socket load and Warning level:</strong> 400</td>
</tr>
<tr>
<td><strong>Receive Buffer TCP Window Size:</strong> 8320</td>
<td><strong>ETHERNET OPTIONS</strong></td>
</tr>
<tr>
<td><strong>Auto:</strong> y</td>
<td></td>
</tr>
</tbody>
</table>
4.4. Administer Data Module for C-LAN

Add a new data module using the “add data-module n” command, where “n” is an available extension for each C-LAN module. Enter the following values:

- **Name:** A descriptive name
- **Type:** “ethernet”
- **Port:** Same slot number from Section 4.3, suffixed with port “17”
- **Link:** An available link number

```
add data-module 40000
DATA MODULE
Data Extension: 40000 Name: CLAN-01A02
  Type: ethernet
  Port: 01A0217
  Link: 1
Network uses 1's for Broadcast Addresses? Y
```

```
add data-module 49999
DATA MODULE
Data Extension: 49999 Name: CLAN-01B02
  Type: ethernet
  Port: 01b0217
  Link: 2
Network uses 1's for Broadcast Addresses? Y
```

4.5. Administer IP Services for AES Transport Link

Administer the transport link to the AES server with the “change ip-services” command. Add an entry with the following values for fields on Page 1:

- **Service Type:** “AESVCS”
- **Enabled:** “y”
- **Local Node:** C-LAN node name from Section 4.2
- **Local Port:** Retain the default value of “8765”

```
change ip-services
IP SERVICES
<table>
<thead>
<tr>
<th>Service</th>
<th>Enabled</th>
<th>Local Node</th>
<th>Local Port</th>
<th>Remote Node</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AESVCS</td>
<td>y</td>
<td>CLAN-01A02</td>
<td>8765</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AESVCS</td>
<td>y</td>
<td>CLAN-01B02</td>
<td>8765</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Proceed to Page 4, and enter the following values:

- **AE Services Server**: Name obtained from the AES server.
- **Password**: Same password to be administered on the AES server.
- **Enabled**: “y”

Note that the name and password entered for the **AE Services Server** and **Password** fields are case sensitive, and must match the name and password on the AES server. The administered name for the AES server 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. The same password entered in the screen below will need to be set on the AES server, as described in Section 5.3.

<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>govae2</td>
<td>*</td>
<td>y</td>
<td></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>

### 4.6. Administer CTI Link for TSAPI Service

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields. Submit these changes.

```
add cti-link 2
CTI Link: 2
Extension: 55001
Type: ADJ-IP
Name: TSAPI GOVAES2
```

### 4.7. Administer Stations for NICE

Add stations for use by the NiceLog recording channels. These are virtual stations that will be used by the NICE call recording system. It is assumed that the other stations that will be monitored by the NICE call recording system are already configured. There is a one-to-one mapping for the virtual station and the monitored station, i.e. one virtual station is needed for every monitored station. Both virtual and monitored stations extensions will be used later in Section 5.5 and Section 6.1 Step 12.
Issue “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** Enter station type “4624”.
- **Name:** A descriptive name.
- **Security Code:** Enter a valid code. All the NiceLog stations will use the same code.
- **COR:** Enter a COR which has “Can be Service Observed” and “Can be a Service Observer” enabled as “y”
- **IP SoftPhone:** “y”

```
add station 46001

STATION

Extension: 46001
Type: 4624
Port: IP
Name: NICE

STATION OPTIONS
Loss Group: 19
Data Option: none
Display Language: english

Feature Options
LWC Reception: spe
LWC Activation? y
LWC Log External Calls? n
CDR Privacy? n
Redirect Notification? y
Per Button Ring Control? n
Bridged Call Alerting? n
Active Station Ringing: single
H.320 Conversion? n

Multimedia Mode: enhanced
Audible Message Waiting? n

MWI Served User Type: Display Client Redirection? n
AUDIX Name: Select Last Used Appearance? n
```

Proceed to **Page 2**, and set the **Multimedia Mode** to “enhanced”, **Auto Answer** to “none” and **Data Restriction** to “n”.

```
add station 46001

STATION

Lock Messages? n
BCC: 0

Security Code: 1234
TN: 1

Coverage Path 1: COR: 1
Coverage Path 2: COS: 1

Hunt-to Station:

STATION OPTIONS

Personalized Ringing Pattern: 1
Message Lamp Ext: 46001
Mute Button Enabled? y
Expansion Module? n

Media Complex Ext:
IP SoftPhone? y

Auto Select Any Idle Appearance? n
Coverage Msg Retrieval? y
Auto Answer: none
Data Restriction? n

Idle Appearance Preference? n
Bridged Idle Line Preference? n
Restrict Last Appearance? y
Conf/Trans on Primary Appearance? n
Per Station CPN - Send Calling Number?
```
On Page 4, assign the “conf-dsp” and “serv-obsrv” to any available buttons:

<table>
<thead>
<tr>
<th>add station 46001</th>
<th>STATION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SITE DATA</td>
</tr>
<tr>
<td></td>
<td>Room:</td>
</tr>
<tr>
<td></td>
<td>Jack:</td>
</tr>
<tr>
<td></td>
<td>Cable:</td>
</tr>
<tr>
<td></td>
<td>Floor:</td>
</tr>
<tr>
<td></td>
<td>Building:</td>
</tr>
<tr>
<td></td>
<td>ABBREVIATED DIALING</td>
</tr>
<tr>
<td></td>
<td>List1:</td>
</tr>
<tr>
<td></td>
<td>BUTTON ASSIGNMENTS</td>
</tr>
<tr>
<td>1: call-appr</td>
<td>7:</td>
</tr>
<tr>
<td>2: call-appr</td>
<td>8:</td>
</tr>
<tr>
<td>3: call-appr</td>
<td>9:</td>
</tr>
<tr>
<td>4: conf-dsp</td>
<td>10:</td>
</tr>
<tr>
<td>5: serv-obsrv</td>
<td>11:</td>
</tr>
<tr>
<td>6:</td>
<td>12:</td>
</tr>
</tbody>
</table>

Repeat the “add station n” command to add the desired number of stations. For the compliance testing, eight virtual stations were administered which were used to monitor the corresponding stations.

<table>
<thead>
<tr>
<th>NICE Virtual Stations</th>
<th>Monitored Stations</th>
</tr>
</thead>
<tbody>
<tr>
<td>46001</td>
<td>23002</td>
</tr>
<tr>
<td>46002</td>
<td>41002</td>
</tr>
<tr>
<td>46003</td>
<td>51001</td>
</tr>
<tr>
<td>46004</td>
<td>51002</td>
</tr>
<tr>
<td>46005</td>
<td>52001</td>
</tr>
<tr>
<td>46006</td>
<td>52002</td>
</tr>
<tr>
<td>46007</td>
<td>53000</td>
</tr>
<tr>
<td>46008</td>
<td>53001</td>
</tr>
</tbody>
</table>

Note: The VDN and Agents-ID extensions do not require a virtual station.

4.8. Administer COR for Virtual and Monitored Stations

Issue “change cor n” command, where “n” is the COR number assigned to the virtual stations created in Section 4.7. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Can Be Service Observed:** Enter “Y”.
- **Can Be A Service Observer:** Enter “Y”.

Note: All monitored stations also need the above values enabled in their respective COR forms.
4.9. Administer Feature Access code for Service Observing

Enter the “change feature-access-code” command. Navigate to Page 5, and set Service Observing Listen Only Access Code. This will be used in Section 6.1 Step 8.

<table>
<thead>
<tr>
<th>FEATURE ACCESS CODE (FAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Call Distribution Features</td>
</tr>
<tr>
<td>After Call Work Access Code: *52</td>
</tr>
<tr>
<td>Assist Access Code: *50</td>
</tr>
<tr>
<td>Auto-In Access Code: *17</td>
</tr>
<tr>
<td>Aux Work Access Code: *19</td>
</tr>
<tr>
<td>Login Access Code: *15</td>
</tr>
<tr>
<td>Logout Access Code: *16</td>
</tr>
<tr>
<td>Manual-in Access Code: *18</td>
</tr>
<tr>
<td>*<em>Service Observing Listen Only Access Code: <em>30</em></em></td>
</tr>
<tr>
<td>Service Observing Listen/Talk Access Code: *31</td>
</tr>
<tr>
<td>Service Observing No Talk Access Code: *32</td>
</tr>
<tr>
<td>Add Agent Skill Access Code:</td>
</tr>
<tr>
<td>Remove Agent Skill Access Code:</td>
</tr>
<tr>
<td>Remote Logout of Agent Access Code:</td>
</tr>
</tbody>
</table>

4.10. Administer System Parameters

Enter the “change system-parameters features” command. Navigate to Page 5, and set Create Universal Call ID (UCID) to “y” and UCID Network Node ID to an unassigned node ID.

<table>
<thead>
<tr>
<th>FEATURE-RELATED SYSTEM PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM PRINTER PARAMETERS</td>
</tr>
<tr>
<td>Endpoint:</td>
</tr>
<tr>
<td>Lines Per Page: 60</td>
</tr>
<tr>
<td>SYSTEM-WIDE PARAMETERS</td>
</tr>
<tr>
<td>Switch Name:</td>
</tr>
<tr>
<td>Emergency Extension Forwarding (min): 10</td>
</tr>
<tr>
<td>Enable Inter-Gateway Alternate Routing? n</td>
</tr>
<tr>
<td>Enable Dial Plan Transparency in Survivable Mode? n</td>
</tr>
<tr>
<td>COR to Use for DPT: station</td>
</tr>
<tr>
<td>MALICIOUS CALL TRACE PARAMETERS</td>
</tr>
<tr>
<td>Apply MCT Warning Tone? n</td>
</tr>
<tr>
<td>MCT Voice Recorder Trunk Group:</td>
</tr>
<tr>
<td>SEND ALL CALLS OPTIONS</td>
</tr>
<tr>
<td>Send All Calls Applies to: station</td>
</tr>
<tr>
<td>Auto Inspect on Send All Calls? n</td>
</tr>
<tr>
<td>UNIVERSAL CALL ID</td>
</tr>
<tr>
<td>Create Universal Call ID (UCID)? y</td>
</tr>
<tr>
<td>UCID Network Node ID: 123</td>
</tr>
</tbody>
</table>
Navigate to **Page 6**, and set **Conference Tone** and **Intrusion Tone** to “n”.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Network Trunks on Conference Call</td>
<td>5</td>
<td>Auto Start? n</td>
</tr>
<tr>
<td>Conference Parties with Public Network Trunks</td>
<td>6</td>
<td>Auto Hold? y</td>
</tr>
<tr>
<td>Conference Parties without Public Network Trunks</td>
<td>6</td>
<td>Attendant Tone? y</td>
</tr>
<tr>
<td>Night Service Disconnect Timer (seconds)</td>
<td>180</td>
<td>Bridging Tone? n</td>
</tr>
<tr>
<td>Short Interdigit Timer (seconds)</td>
<td>3</td>
<td>Conference Tone? n</td>
</tr>
<tr>
<td>Unanswered DID Call Timer (seconds)</td>
<td></td>
<td>Intrusion Tone? n</td>
</tr>
<tr>
<td>Line Intercept Tone Timer (seconds)</td>
<td>30</td>
<td>Mode Code Interface? y</td>
</tr>
<tr>
<td>Long Hold Recall Timer (seconds)</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Reset Shift Timer (seconds)</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Station Call Transfer Recall Timer (seconds)</td>
<td>0</td>
<td>Recall from VDN? n</td>
</tr>
<tr>
<td>DID Busy Treatment: tone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Night Service Disconnect Timer</td>
<td>180</td>
<td></td>
</tr>
</tbody>
</table>

Navigate to **Page 13**, and set **Send UCID to ASAI** to “y”.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Callr-info: next-call</td>
<td>next-call</td>
<td></td>
</tr>
<tr>
<td>Allow Ringer-off with Auto-Answer?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Reporting for PC Non-Predictive Calls?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Copy ASAI UUI During Conference/Transfer?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>Call Classification After Answer Supervision?</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td><strong>Send UCID to ASAI?</strong></td>
<td><strong>Y</strong></td>
<td></td>
</tr>
</tbody>
</table>
5. Configure Avaya Application Enablement Services

This section provides the procedures for configuring Avaya Application Enablement Services. The procedures include the following areas:

- Verify Avaya Application Enablement Services License
- Administer local IP
- Administer switch connection
- Administer TSAPI link
- Administer security database
- Obtain Tlink name
- Administer NICE users
- Administer device groups
- Restart TSAPI service

5.1. Verify Avaya Application Enablement Services License

Access the AES OAM web based interface by using the URL “https://ip-address:8443/MVAP” in an Internet browser window, where “ip-address” is the IP address of the AES server. The Login screen is displayed as shown below. Note that the AES OAM includes two separate administrative accounts, one to access CTI OAM Admin and a separate one to access User Management. Log in using the CTI OAM Admin user name and password.
The **Welcome to OAM** screen is displayed, as shown below. Select **CTI OAM Administration** from the left pane.

![Welcome to OAM Screen](image1)

The **Welcome to CTI OAM Screens** is displayed. Verify that AES is licensed for the TSAPI service, as shown below. If the TSAPI service is not licensed, contact the Avaya sales team or business partner for a proper license file.

![Welcome to CTI OAM Screens](image2)
5.2. Administer Local IP
Select Administration > Network Configuration > Local IP from the left pane. The Local IP screen is displayed into the right pane, as shown below. In the Client Connectivity field, select the AES server IP address that will be used to interface to NICE Call Recording system. In the Switch Connectivity field, select the AES server IP address that will be used to connect to Avaya Communication Manager. In the sample configuration, the same NIC interface is used for the Client Connectivity and Switch Connectivity. Note that in some cases, they might be different. Click on Apply Changes.

5.3. Administer Switch Connection
Select Administration > Switch Connections from the left pane. The Switch Connections screen is displayed, as shown below. Enter a descriptive name for the switch connection and click on Add Connection. In this case, “govaes2” is used. Note that the actual switch connection name may vary.

Next, the Set Password – govaes2 screen is displayed. Enter the following values for the specified fields:

- **Switch Password:** Same password from Section 4.5.
- **Confirm Switch Password:** Re-enter the same password from Section 4.5.
- **SSL:** Retain the check.

Click on Apply.
The **Switch Connections** screen is displayed next, as shown below. Select the newly added switch connection name from the listing, and click on **Edit CLAN IPs**.

The **Edit CLAN IPs – govaes2** screen is displayed next. Enter the host name or IP address of the C-LAN used for AES connectivity from Section 4.2. Click on **Add Name or IP**. In the sample configuration two C-LANs will be administered.
5.4. Administer TSAPI Link

To administer a TSAPI link, select **Administration > CTI Link Admin > TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click on **Add Link**.

![TSAPI Links Screen](image1)

The **Add / Edit TSAPI Links** screen is displayed next. The **Link** field is only local to the AES server, and may be set to any available number. For **Switch Connection**, select the name of the switch connection from **Section 5.3**. For **Switch CTI Link Number**, select the CTI link number from **Section 4.6**. Accept the default values for **ASA1 Link Version** and **Security**. Click on **Apply Changes**.

![Add / Edit TSAPI Links Screen](image2)

The **Apply Changes to Link** screen is displayed (not shown). Click on **Apply**.

![Apply Changes Screen](image3)
5.5. Administer Security Database

Enable the security database on AES, as this functionality is utilized by NICE. Select Administration > Security Database > SDB Control to display the SDB Control for DMCC and TSAPI screen shown below. Click on Enable SDB for DMCC Service and Enable SDB TSAPI Service, JTAPI and Telephony Service. Click on Apply Changes.

All devices that are monitored by NICE need to be configured in the AES security database. These include all the virtual stations that were created in Section 4.7 and also the station extensions which will be monitored by NICE call recording.

Select Administration > Security Database > Devices, and add each device by entering the device extension and clicking on Add Device.

The Add / Edit Device screen is used to enter the associated field values for each device, as shown below. Only enter the Device Type as PHONE in this list. This should include both the virtual stations administered in Section 4.7 and the corresponding monitored stations.
A sample listing of the configured devices used for the compliance testing is shown below. Note that the total number of devices may vary, as this depends on the number of extensions to be monitored and controlled. The list below contains all the devices (PHONE, VDN and AGENT ID) administered on the AES. Not all these devices will be used by NICE. Only selected devices will be administered for the NICE Device Group, as described in Section 5.8.
5.6. Obtain Tlink Name

Select Administration > Security Database > Tlinks from the left pane. The Tlinks screen shows a listing of the Tlink names. A new Tlink name is automatically generated by the AES server, upon creation of a new switch connection. Locate the Tlink Name associated with the newly created switch connection, which would utilize the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring the NICE server in Section 6.1 Step 7.

5.7. Administer NICE Users

Administer an user account for the NICE server. Follow the login procedures in Section 5.1, and log in with the User Management user name and password. The Welcome to the User Management home page screen is displayed, as shown below.
Select **User Management > Add User** from the left pane. In the **Add User** screen shown below, enter values for the **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password** fields to create a user account for the NICE server. Retain the default value of “None” for **Avaya Role**, and select “Yes” from the **CT User** drop-down list. Click on **Apply** at the bottom of the screen (not shown below). Make a note of the User Id and Password, to be used later for configuring the NICE server in **Section 6.1 Step 7**.
Follow the login procedures in Section 5.1, and log in with the CTI OAM Admin user name and password. Select Administration > Security Database > CTI Users > List All Users to get a listing of all CTI users, as shown below.

5.8. Administer Device Groups

Administer a device group to be used by NICE, to control user access of devices. Select Administration > Security Database > Device Groups from the left pane. In the Device Groups screen shown below, enter a descriptive value, and click on Add Device Group.
For the sample configuration, a device group of “NICE” was created. Click on **Edit Device Group**. The **Add / Edit Device Group** screen is displayed, as shown below. Select all devices that were created in Section 5.5, and click on **Apply Changes**.

The **Apply Changes to Device Group Properties** screen is displayed next. Click on **Apply** to confirm the changes.
Select Administration > Security Database > CTI Users > List All Users to view the listing of all CTI users again, as shown below. Select the user ID created for the NICE server, and click on Edit.

The Edit CTI User screen is displayed, as shown below. Select the newly created device group for the Call Origination and Termination, Device / Device, Call / Device, and Allow Routing on Listed Device fields. Click on Call / Call, followed by Apply Changes.
5.9. Restart TSAPI Service

Select Maintenance > Service Controller. The Service Controller screen shows a listing of the services and associated status. Check the TSAPI Service, and click on Restart Service.

The following Restart Service screen is displayed. Click on Restart to confirm the restart.
6. Configure NICE Call Recording System

These Application Notes assume that the NICE call recording system depicted in Figure 2 is already installed. Refer to [3] for detailed information about the installation procedure. It is also assumed that the Avaya AES 4.2.1 TSAPI Client application is already installed on the NICE server. Refer to [1] for detailed information.

6.1. Configure NiceCLS server

The steps in this section describe the system configuration of the NiceCLS server. For detailed NiceCLS configuration information, please refer to [3].

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On the NiceCLS server, launch the NiceCLS Server Controller by navigating to Programs → NiceCLS Server 8.93 → NiceCLS Server Controller.</td>
</tr>
</tbody>
</table>

![NiceCLS Server Controller](image1)

2. In the NiceCLS Server Controller window, click on Configuration → Server Features. The Server Features screen appears. Check the Total Recording, Click OK.

![Server Features](image2)
### Step 3
In the NiceCLS Server Controller window, click on **Switch → Driver Setup → Avaya-Definity G3-Passageway.**

![NiceCLS Server Controller](image)

The **Generic CTI Driver Setup** screen appears. Enter the following values, and then click **Next**.

- **Driver to be Configured**: Select “1- LucentTS” from the drop down list.
- **SwitchID**: Retain the default value “1”. This value will be used in **Step 16**.

![Generic CTI Driver Setup](image)

### Step 4
The **Generic CTI Driver Features** screen appears. Click **Next**.

### Step 5
The **Devices Mapping** screen appears. Click **Finish**.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>The AVAYA Quick Setup – Welcome screen appears. Select “LucentTS” from the <strong>Choose the driver you would like to configure</strong> drop down list, and then click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>

![AVAYA Quick Setup - Welcome](image)

*Welcome to AVAYA Quick Setup.*

*The Setup Wizard will guide you through the driver's configuration setup.*

*Choose the driver you would like to configure:*

- LucentTS
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Select “AVAYA#GOVAES2#CSTA#GOVAES2” from the Select Server drop down list. The Select Server information was created after performing configuration in Section 5.6. Enter the login ID and password administered in Section 5.7.</td>
</tr>
</tbody>
</table>

**Click Test Connection.**

**Click OK.**
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>The AVAYA Quick Setup – Recording Method screen appears. Select “Service Observation with DS1’s” from the Recording Method drop down list. Enter the administered feature access code for Service Observing from Section 4.9 and then click Finish.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="AVAYA Quick Setup - Recording Method" /></td>
</tr>
<tr>
<td>9.</td>
<td>In the NiceCLS Server Controller, click on Configuration → Logger Definition Tool. The Logger Definition Tool screen appears. In the Logger Definition Tool, click on Edit → Switches.</td>
</tr>
</tbody>
</table>
10. The **Switch Configuration** screen appears. From the **Switch Name** drop down list, select “LucentTS”, and then click **OK**.

![Switch Configuration screen](image)

11. In the **Logger Definition Tool**, click on **Edit → Loggers**. The **Logger Configuration** screen appears. Enter the following values, and then click **OK**.

- **Recording Type**: Select “CMAPI Total SO” (Service Observing).
- **Input Channels**: Enter the number of stations that will be recorded.
- **Line Type**: Select “VOIP” from the **Line Type** drop down list.
- **Address**: Select the default value.
- **Status**: Select the default value.

![Logger Configuration](image)
12. In the **Logger Definition Tool**, enter the following values, and then click **OK**.

- **Recorded Device Type**: Select “Virtual Device” from the drop down list.
- **Virtual Extension**: Enter the IP Softphone extension administered in **Section 4.7**.
- **Station**: Enter the monitored station extension number.

![Logger Definition Tool](image_url)
13. In the **Logger Definition Tool**, click on File ➔ Build Map File.

14. The **Logger Mapping** screen appears. Click **OK** to confirm the change.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>From the NiceCLS Server Controller, click on <strong>Switch → Driver Setup → CMAPI - Site Configuration</strong>. The NICE CMAPI Configuration Utility screen appears. Click on <strong>Switches</strong>, and then click <strong>New</strong>.</td>
</tr>
</tbody>
</table>
| 16.  | The **Switch Configuration** screen appears. Enter the following values, and then click **OK**.  
  - **Switch Name**: A descriptive name, for example **NICE**.  
  - **CLAN Board IP Address**: The C-LAN IP address administered in **Section 4.3**. Enter only one C-LAN IP address.  
  - **Switch ID**: Enter the switch ID “1”. The value administered in **Step 3**.  
  - **Default Password**: The security code administered in **Section 4.7**.  
  - **Codec**: Select **g711U**. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 17.  | In the **NICE CMAPI Configuration Utility**, click on CMAPI, and then click **New** (not shown). The **New CMAPI Properties** screen appears. Enter the following values, and then click **OK**.  
  - **Name**: A descriptive name.  
  - **ID**: Enter the AES server ID “1”.  
  - **Related Switch**: Select “NICE” which was entered in **Step 16**.  
  - **IP Address**: Enter the AES server IP address.  
  - **Port**: Retain the default value “4721”.  

The updated screen is shown below:
18. From the NICE CMAPI Configuration Utility, click on Proxies, and then click New (not shown). The New Proxy Properties screen appears. Enter the following values, and then click OK.

- **Name**: A descriptive name.
- **Address**: Enter the local IP address of the NICE call recording system (9.1.1.15).
- **Port**: Retain the default value “1327”.
- **Related CMAPI**: Select “NICECMAPI”, which was entered in Step 17.
- **Proxy ID**: Enter a unique ID, for example 1.

The updated screen is shown below:

19. In the NICE CMAPI Configuration Utility, click on Save. The Update Registry Settings window appears. Check the Create entries for dispatcher and Update file location in registry checkboxes. Click OK.
20. In the NiceCLS Server Controller, click on **Server → Run NICE CLS.**

This will start the CLS Manager and the following screen will appear.

![CLS Manager](image)

6.2. Configure the NICE Application Tools

This section describes the steps necessary to configure the NICE Application Tools which include NICE Administrator, NICE Monitor and NICE Query. These client tools are used to manage NiceCLS and NiceLog. These Application Notes assume that the NICE Application Tools are already installed at the appropriate workstation.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>To start NICE Administrator, navigate to <strong>Programs → NICE Applications → NICE Administrator.</strong> Enter the proper credentials to log in.</td>
</tr>
</tbody>
</table>
Step | Description
--- | ---
2. | In the NICE Administrator window, click **New → NiceLog**. The New NiceLog appears in the Resource List in the left panel. Click **General** tab, and enter the following values:
   - **Name**: Enter a descriptive logger name, for example “AvayaLogg”.
   - **Network type**: Retain the default value “TCP/IP”.
   - **Network address**: Enter the IP Address of the Logger.
   - **For retrieval**: Enable the checkbox.

Click on **Save** icon

The updated screen is shown below:

![Updated Screen](image)

**Note**: After the NICE Administrator system connects with the NiceLog, the system populates the NiceLog information.
Step | Description
--- | ---
3. | In the NICE Administrator window, click **New → NiceCLS Server**. The New CLS Server window appears in the general area. Enter the following values and then click on the **Save** icon.

- **Name**: Enter a descriptive name.
- **Network Type**: Select “TCP/IP” from the drop down list.
- **Network address**: Enter the network address of the NiceCLS server.

The updated screen is shown below:

![Updated NICE Administrator Screen]

**Note**: After the NICE Administrator system connects with the NiceCLS, the system populates the NiceCLS information.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Click on <strong>Loggers</strong> tab. Move the Logger, administered in <strong>Step 2</strong>, from the <strong>Available Loggers</strong> list to the <strong>Member Logger</strong> list. Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 5.   | In the NICE Administrator, click **New → User**. Enter the following values, and then click **Save**.  
  - **First name**: Enter a descriptive name.  
  - **Last name**: Enter a descriptive name.  
  - **Login name**: Enter login name.  
  - **Password**: Enter the password that will be used by the NICE Application Tools.  
  - **User must change password at next logon**: Disable the checkbox.  
  - **Make user an agent**: Enable the checkbox.  
  - **CLS Server**: Select the CLS Server administered in **Step 3** from the drop down list.  
  - **Extension**: Enter the station extension which will be monitored.  
  - **Switch ID**: Enter “1”.  
  Repeat this step as necessary to add additional Users.  
| 6.   | To start NICE Query, navigate to **Programs → NICE Applications → NICE Query**. Enter the proper credentials to log in.  
| 7.   | In the NICE Query, click **New → Query**. Enter the following values, and then click **OK**.  
  - **Query name**: Enter a descriptive name.  
|
7. General Test Approach and Test Results
Feature functionality testing was performed manually. Call recording and playback was verified for incoming/outgoing calls. In addition, phone features like hold, conference calls and transfers were exercised while the call was being recorded.

8. Verification
This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Application Enablement Services, and NICE call recording application.

8.1. Verify Avaya Communication Manager
On Avaya Communication Manager, verify the status of the administered CTI links by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link numbers administered in Section 4.6, as shown below.

```
status aesvcs cti-link

AE SERVICES CTI LINK STATUS
CTI Version Mnt AE Services Service State Msgs Msgs
Link Busy Server       Sent Rcvd
1   4   no   govaes1  established 611 611
2   4   no   govaes2  established 611 611
```

Issue the **list registered-ip-stations** command from the Avaya Communication Manager SAT to verify the NiceLog recording channels are registered in Avaya Communication Manager

```
list registered-ip-stations

REGISTERED IP STATIONS
Station Ext/ Orig Port Type ID Phone Station Rel Rgn IP Address IP Address Net Gatekeeper TCP
Set Prod Prod Skt
23001 4625 IP_Phone 2.8300 9.1.1.1.85 1 9.1.1.1.8 y
40030 4621 IP_Phone 2.8000 9.1.1.1.153 1 9.1.1.1.8 y
44000 4625 IP_Phone 2.6000 9.1.1.1.143 1 9.1.1.1.8 y
44002 4625 IP_Phone 2.6000 9.1.1.1.177 1 9.1.1.1.9 y
44004 4625 IP_Phone 2.6000 9.1.1.1.175 1 9.1.1.1.8 y
46001 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
46002 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
46003 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
46004 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
46005 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
46006 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
46007 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
46008 4624 IP_API_A 3.2040 9.1.1.1.51 1 9.1.1.1.8 y
```
8.2. Verify Avaya Application Enablement Services

On Avaya AES, verify the status of the switch connection by selecting **Status and Control > Switch Conn Summary** from the left pane. Verify that the **Conn State** is “Talking” for the switch connection administered in **Section 5.3**, as shown below.

Verify the status of the TSAPI link by selecting **Status and Control > Services Summary** from the left pane. Click on **TSAPI Service**, followed by **Details** (not shown below). The **TSAPI Link Details** screen is displayed. Verify the **Conn Status** is “Talking” for the TSAPI link administered in **Section 5.4**, as shown below.
Verify the status of the DMCC by selecting **Status and Control > Services Summary** from the left pane. Click on **DMCC Service**, followed by **Details** (not shown below). The **DMCC Service Summary – Session Summary** screen is displayed. Verify the nice cmaipi session is listed.

Select **Session Summary Device Summary**. The details of all the devices registered with NICE application will be displayed. These should match the “list registered-ip-stations” from **Section 8.1**.
8.3. Verify Call Recording and Playback from the NICE Query and Monitor

Make several calls. Verify that the recorded calls can be queried and playback from the NICE Query.

From the NICE Tool bar click on the NICE Query icon and run query.

From the NICE Tool bar click on the NICE Monitor icon.
9. Terminology

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Avaya Application Enablement Services</td>
</tr>
<tr>
<td>ALI</td>
<td>Automatic Location Information</td>
</tr>
<tr>
<td>ANI</td>
<td>Automatic Number Identification</td>
</tr>
<tr>
<td>CAMA</td>
<td>Centralized Automated Message Accounting</td>
</tr>
<tr>
<td>DMCC</td>
<td>Device, Media and Call Control</td>
</tr>
<tr>
<td>IWS</td>
<td>Intelligent Workstation</td>
</tr>
<tr>
<td>NENA</td>
<td>National Emergency Number Association</td>
</tr>
<tr>
<td>PSAP</td>
<td>Public Safety Answering Point</td>
</tr>
<tr>
<td>SES</td>
<td>SIP Enablement Services</td>
</tr>
<tr>
<td>TSAPI</td>
<td>Telephony Services Application Programming Interface</td>
</tr>
</tbody>
</table>

10. Conclusion

These Application Notes demonstrate how to provision NICE Call Recording System for Public Safety which includes NICE CLS 8.90.4 and VoIP Logger 9.10.05 with Avaya Communication Manager, and Avaya Application Enablement Services to record and monitor incoming and outgoing calls on Avaya Communication Manager.

11. Additional References


4. Application Notes for PlantCML Sentinel CM with Avaya Communication Manager and Avaya Application Enablement Services.

©2009 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.