Abstract

These Application Notes describe the procedures for configuring Cacti FocusRecord Enterprise to monitor and record calls placed between stations and agents as well as incoming calls to Vector Directory Numbers (VDN) on Avaya Communication Manager.

When the recording of a call is desired, Cacti FocusRecord Enterprise issues a Single Step Conference request through events acquired from Telephony Services Application Programming Interface (TSAPI). In the configuration discussed in these Application Notes, Cacti FocusRecord Enterprise employs Device, Media and Call Control (DMCC) API (formally known as CMAPI) virtual stations as recording ports. During compliance testing, Cacti FocusRecord Enterprise successfully recorded calls placed to and from stations, as well as calls placed to a hunt group and then redirected to agents.

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 a compliance-tested configuration comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) and Cacti FocusRecord Enterprise.

The FocusRecord Enterprise monitors, records, stores, and plays back phone calls for verification. The FocusRecord Enterprise uses TSAPI with an Avaya AES server to monitor stations, agents, and/or VDNs, i.e. to obtain recording triggers and call information. The FocusRecord Enterprise also uses the Device, Media and Call Control (DMCC) API (formally known as CMAPI) with the Avaya AES server to register DMCC softphones that FocusRecord Enterprise uses as recording ports. When recording of a call is desired, FocusRecord Enterprise issues a Single Step Conference request through events acquired from TSAPI.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide a T1/ISDN-PRI trunk between two Avaya Communication Manager systems.
2. Equipment and Software Validated
The following equipment and software/firmware were used for the sample configuration provided:

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software/Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8720 Server</td>
<td>Avaya Communication Manager 5.0 (R015x.00.0.825.4)</td>
</tr>
<tr>
<td>Avaya G650 Media Gateway</td>
<td>-</td>
</tr>
<tr>
<td>TN2312BP IP Server Interface</td>
<td>HW11 FW030</td>
</tr>
<tr>
<td>TN799DP C-LAN Interface</td>
<td>HW20 FW017</td>
</tr>
<tr>
<td>TN2302AP IP Media Processor</td>
<td>HW01 FW108</td>
</tr>
<tr>
<td>TN2602AP IP Media Processor</td>
<td>HW02 FW007</td>
</tr>
<tr>
<td>Avaya S8300 Server with Avaya G700 Media Gateway</td>
<td>Avaya Communication Manager 5.0 (R015x.00.0.825.4)</td>
</tr>
<tr>
<td>Avaya Application Enablement Services Server</td>
<td>R4.1.31.2</td>
</tr>
<tr>
<td>Avaya 4600 Series IP Telephones</td>
<td>4620SW 2.8 (H.323)</td>
</tr>
<tr>
<td></td>
<td>4625SW 2.8 (H.323)</td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephones</td>
<td>9630 1.5 (H.323)</td>
</tr>
<tr>
<td></td>
<td>9650 1.5 (H.323)</td>
</tr>
<tr>
<td>Avaya 6408D+ Digital Telephone</td>
<td>-</td>
</tr>
<tr>
<td>Cacti FocusRecord Enterprise on Windows 2003 Standard Edition with SP1</td>
<td>2.44</td>
</tr>
</tbody>
</table>

3. Configure Avaya Communication Manager
This section provides the procedures for configuring Computer Telephony Integration (CTI) links, hunt/skill groups, vectors, VDN, agents, agent login/logoff codes, and recording ports on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

3.1. Configure AES Link between Avaya Communication Manager and Avaya Application Enablement Services Server
The Avaya AES server forwards CTI requests, responses, and events between Cacti FocusRecord Enterprise and Avaya Communication Manager. The Avaya AES server communicates with Avaya Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Cacti FocusRecord Enterprise. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI links. See Section 4 for the details of configuring the AES side of the AES and CTI links.
Enter the **add cti-link m** command, where \( m \) is a number between 1 and 64, inclusive. Enter a valid Extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to **ADJ-IP** and assign a descriptive Name to the CTI link.

```
add cti-link 4
```

CTI Link: 4

- Extension: 20006
- Type: ADJ-IP

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAN</td>
<td>192.45.80.87</td>
</tr>
<tr>
<td>CLAN-AES</td>
<td>192.45.80.89</td>
</tr>
<tr>
<td>MEDPRO</td>
<td>192.45.80.88</td>
</tr>
<tr>
<td>MEDPRO2</td>
<td>192.45.80.161</td>
</tr>
<tr>
<td>S8300G700</td>
<td>192.45.87.11</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>procr</td>
<td>192.45.80.214</td>
</tr>
</tbody>
</table>

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoint (Avaya IP Telephones and IP Softphones, and AES Device and Media Control API stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

```
change node-names ip
```

**IP NODE NAMES**

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAN</td>
<td>192.45.80.87</td>
</tr>
<tr>
<td>CLAN-AES</td>
<td>192.45.80.89</td>
</tr>
<tr>
<td>MEDPRO</td>
<td>192.45.80.88</td>
</tr>
<tr>
<td>MEDPRO2</td>
<td>192.45.80.161</td>
</tr>
<tr>
<td>S8300G700</td>
<td>192.45.87.11</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>procr</td>
<td>192.45.80.214</td>
</tr>
</tbody>
</table>

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the CLAN-AES board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was utilized for the Local Port field.

```
change ip-services
```

**IP SERVICES**

<table>
<thead>
<tr>
<th>Service Type</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-AES</td>
<td>8765</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On **Page 4**, enter the hostname of the Avaya AES server for the AE Services Server field. The server name may be obtained by logging in to the Avaya AES server using ssh, and run `uname -a`. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the Avaya AES server in **Section 4.1**.

```
change ip-services
```

**AE Services Administration**

<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>server1</td>
<td>xxxxxxxxxx</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>
3.2. Configure Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the `display system-parameters customer-options` command. On Page 6, verify that the ACD and Vectoring (Basic) fields are set to `y`. If not, contact an authorized Avaya account representative to obtain these licenses.

```
<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACD?</td>
<td>y</td>
</tr>
<tr>
<td>BCMS (Basic)?</td>
<td>y</td>
</tr>
<tr>
<td>Service Level Maximizer?</td>
<td>n</td>
</tr>
<tr>
<td>BCMS/VuStats Service Level?</td>
<td>n</td>
</tr>
<tr>
<td>Service Observing (Basic)?</td>
<td>y</td>
</tr>
<tr>
<td>BSR Local Treatment for IP &amp; ISDN?</td>
<td>n</td>
</tr>
<tr>
<td>Service Observing (Remote/By FAC)?</td>
<td>y</td>
</tr>
<tr>
<td>Business Advocate?</td>
<td>n</td>
</tr>
<tr>
<td>Service Observing (VDNs)?</td>
<td>n</td>
</tr>
<tr>
<td>Call Work Codes?</td>
<td>n</td>
</tr>
<tr>
<td>Timed ACW?</td>
<td>N</td>
</tr>
<tr>
<td>DTMF Feedback Signals For VRU?</td>
<td>n</td>
</tr>
<tr>
<td>Dynamic Advocate?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (Prompting)?</td>
<td>n</td>
</tr>
<tr>
<td>Expert Agent Selection (EAS)?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (G3V4 Enhanced)?</td>
<td>n</td>
</tr>
<tr>
<td>EAS-PHD?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (3.0 Enhanced)?</td>
<td>n</td>
</tr>
<tr>
<td>Forced ACD Calls?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (ANI/II-Digits Routing)?</td>
<td>n</td>
</tr>
<tr>
<td>Least Occupied Agent?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (G3V4 Advanced Routing)?</td>
<td>n</td>
</tr>
<tr>
<td>Lookahead Interflow (LAI)?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (CINFO)?</td>
<td>n</td>
</tr>
<tr>
<td>Multiple Call Handling (On Request)?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (Best Service Routing)?</td>
<td>n</td>
</tr>
<tr>
<td>Multiple Call Handling (Forced)?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (Holidays)?</td>
<td>n</td>
</tr>
<tr>
<td>PASTE (Display PBX Data on Phone)?</td>
<td>n</td>
</tr>
<tr>
<td>Vectoring (Variables)?</td>
<td>n</td>
</tr>
</tbody>
</table>

(NOTE: You must logoff & login to effect the permission changes.)
```

Enter the `add hunt-group n` command, where `n` is an unused hunt group number. On Page 1 of the HUNT GROUP form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan. Set the ACD, Queue, and Vector fields to `y`. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.
On Page 2, set the Skill field to y, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

```plaintext
add hunt-group 1

HUNT GROUP
| Skill? y |
| AAS? n  |
| Measured: internal |
| Supervisor Extension: |

Controlling Adjunct: none

VuStats Objective:

Redirect on No Answer (rings):
Redirect to VDN:
Forced Entry of Stroke Counts or Call Work Codes? n
```

Enter the `add agent-loginID` command, where `p` is a valid extension in the provisioned dial plan. On Page 1 of the agent-loginID form, enter a descriptive Name and Password.

```plaintext
add agent-loginID 50021

AGENT LOGINID
| Login ID: 50021 |
| Name: Agent-1 |
| TN: 1 |
| COR: 1 |
| Coverage Path: |
| Security Code: |

LoginID for ISDN/SIP Display? n
Password:
Password (enter again):

Auto Answer: station
MIA Across Skills: system
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time: :
On Page 2, set the Skill Number (SN) to the hunt group number previously created. The Skill Level (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.

```
add agent-loginID 50021
```

<table>
<thead>
<tr>
<th>SN</th>
<th>SL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Enter the `add vector q` command, where q is an unused vector number. Enter a descriptive Name, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

```
add vector 1
```

```
Number: 1
Name: Queue to skill
Meet-me Conf? n

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

wait-time 2 secs hearing ringback
queue-to skill 1 pri m
```

Enter the `add vdn r` command, where r is an extension valid in the provisioned dial plan. Specify a descriptive Name for the VDN and the Vector Number configured in the previous step. In the example below, incoming calls to the extension 50000 will be routed to `testVDN50000`, which in turn will invoke the actions specified in vector 1.

```
add vdn 50000
```

```
Extension: 50000
Name: testVDN50000
Vector Number: 1
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none

1st Skill*:
2nd Skill*:
3rd Skill*:
```

```
change feature-access-codes

FEATURE ACCESS CODE (FAC)

Automatic Call Distribution Features

After Call Work Access Code: 120
Assist Access Code: 121
Auto-In Access Code: 122
Aux Work Access Code: 123
Login Access Code: 124
Logout Access Code: 125
Manual-in Access Code: 126
Service Observing Listen Only Access Code: 127
Service Observing Listen/Talk Access Code: 128
Add Agent Skill Access Code: 130
Remove Agent Skill Access Code: 131
Remote Logout of Agent Access Code: 132
```

Enter the `add abbreviated-dialing group g` command, where `g` is the number of an available abbreviated dialing group. In the DIAL CODE list, enter the Feature Access Codes, created previously, for ACD Login and Logout.

```
add abbreviated-dialing group 1

ABBREVIATED DIALING LIST

Group List: 1    Group Name: Call Center
Size (multiple of 5): 5    Program Ext:
Privileged? n

DIAL CODE
11: 124
12: 125
13:
```
3.3. Recording Stations

The recording ports in this configuration are DMCC stations that essentially appear as IP Softphones, to Avaya Communication Manager. Each DMCC station requires an IP_API_A license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for AES DMCC stations. Enter the `display system-parameters customer-options` command and verify that there are sufficient IP_API_A licenses. If not, contact an authorized Avaya account representative to obtain these licenses.

```
<table>
<thead>
<tr>
<th>Product ID</th>
<th>Rel. Limit</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_API_A</td>
<td>200</td>
<td>0</td>
</tr>
<tr>
<td>IP_API_B</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP_API_C</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP_Agent</td>
<td>50</td>
<td>0</td>
</tr>
<tr>
<td>IP_PR_A</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP_Phone</td>
<td>12000</td>
<td>3</td>
</tr>
<tr>
<td>IP_ROMax</td>
<td>12000</td>
<td>0</td>
</tr>
<tr>
<td>IP_Soft</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>IP_eCons</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

(NOTE: You must logoff & login to effect the permission changes.)
```

Enter the `add station` command, where `s` is an extension valid in the provisioned dial plan. On Page 1 of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, specify the Security Code, and set the IP SoftPhone field to `y`. Repeat this as necessary, with the same Security Code, to configure additional DMCC stations.

For the compliance test, stations from 23001 to 23023 were created for the purpose of recording.
3.4. Recorded (Monitored) Stations

Enter the `add station s` command, where `s` is an extension valid in the provisioned dial plan. During the compliance test, these stations were utilized as monitored and recorded stations. On Page 1 of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, and specify the Security Code. For the compliance test, recorded stations from 22001 to 22005 and 21101 to 21123 were created.

```
add station 22001

Extension: 22001                      Lock Messages? n   BCC: 0
  Type: 4621
  Security Code: *
  Port: S00142
  Name: 72001

STATION OPTIONS
  Time of Day Lock Table:
    Loss Group: 19   Personalized Ringing Pattern: 1
  Speakerphone: 2-way   Mute Button Enabled? y
  Display Language: english   Expansion Module? n
  Survivable GK Node Name:
  Survivable COR: internal   Media Complex Ext:
  Survivable Trunk Dest? y   IP SoftPhone? n

Customizable Labels? y
```

On Page 3 of the STATION form, for ABBREVIATED DIALING List 2, enter the abbreviated dialing group configured in Section 3.3. Configure the following BUTTON ASSIGNMENTS in addition to the call-appr (call appearance) buttons:

- auto-in
- aux-work
- abrv-dial – for Login
- abrv-dial – for Logout.

```
add station 22001

SITE DATA

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

ABBREVIATED DIALING

List1: personal 1       List2: group 1

List3:

BUTTON ASSIGNMENTS

1: call-appr
2: call-appr
3: call-appr
4: call-appr
5: auto-in Grp:
6: aux-work RC: Grp:
7: abrv-dial List: 2 DC: 11
8: abrv-dial List: 2 DC: 12

```
4. Configure Avaya Application Enablement Services

The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a switch connection, a CTI user, a DMCC server port, and creating a CTI link for TSAPI.

4.1. Configure Switch Connection

Launch a web browser, enter https://<IP address of Avaya AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the AES CTI OAM pages.
Select the **CTI OAM Administration** link from the left pane of the screen.

Click on **Administration → Network Configuration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.
The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in Section 3.1. Default values may be used in the remaining fields. Click on Apply.

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on Edit CLAN IPs.
Enter the CLAN-AES IP address which configured for AES connectivity in Section 3.1 and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards (or procr) enabled with Application Enablement Services.

4.2. Configure the CTI Users

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter `https://<IP address of Avaya AES server>:8443/MVAP` in the URL, and log in with the appropriate credentials for accessing the OAM Home page.
The Welcome to OAM page is displayed next. Select User Management from the left pane.

From the Welcome to User Management page, navigate to the User Management → Add User page to add a CTI user.

On the Add User page, provide the following information:

- User Id
- Common Name
- Surname
- User Password
- Confirm Password

Above information (User ID and User Password) must match with information configured in the Cacti FocusRecord Enterprise Configuration page in Section 5.

Select Yes using the drop down menu on the CT User field. This enables the user as a CTI user. Click the Apply button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.
Once the user is created, select OAM Home in upper right and navigate to the Administration → Security Database → CTI Users → List All Users page. Select the User ID created previously, and click the Edit button to set the permission of the user.
Provide the user with unrestricted access privileges by clicking the *Enable* button on the Unrestricted Access field. Click the *Apply Changes* button.

Navigate to the **Administration → Network Configuration → Ports** page to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to *Enabled*. Click the *Apply Changes* button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.
4.3. Configure the TSAPI CTI Link

Navigate to the Administration ➔ CTI Link Admin ➔ TSAPI Links page to set the TSAPI CTI Link. Click on Add Link.

Select a Switch Connection using the drop down menu. The Switch Connection is configured in Section 4.1. Select the Switch CTI Link Number using the drop down menu. The CTI link number should match with the number configured in the cti-link form in Section 3.1. Click the Apply Changes button. Default values may be used in the remaining fields.

5. Configure Cacti FocusRecord Enterprise

Cacti installs, configures, and customizes the FocusRecord Enterprise application for their end customers. This section only describes the interface configuration for the FocusRecord Enterprise application to communicates with Avaya AES and Avaya Communication Manager. Refer to [3] for configuring the Cacti FocusRecord Enterprise application.

Navigate to Start ➔ Programs ➔ CAppMan to access the Cacti_Application_Manager page. In the Cacti_Application_Manager page, select Cacti_Focus_DMCC_01 and click the Settings button.
The following screen shows the Cacti_Focus_DMCC_01 Settings page. Provide the following information:

- **DMCCSvrIp** – Enter the IP address of Avaya AES.
- **DMCCSvrPort** – Enter the DMCC port utilized. During the compliance test, unencrypted, default DMCC port was utilized, as shown in Section 4.2.
- **DMCC_Login** – Enter the user name created in Section 4.2.
- **DMCC_Passwd** – Enter the password created in Section 4.2.
- **SwitchName** – Enter the switch connection name created in Section 4.1.
- **IpPhoneDevice** – Enter the recording (DMCC stations) extension range created in Section 3.3.
The following screen shows the second part of DMCC Configuration.

- **IpPhoneDevicePasswd** – Enter the recording (DMCC stations) extension password, created in **Section 3.3**.
- **RtpIpAddress** – Enter the IP address of the recording device, in this case, Cacti FocusRecord Enterprise
- **CodecType** – Enter the audio codec type. This must match the value in the IP Codec Set form used in the IP NETWORK REGION form.

Click on **Save** to save the changes.

To configure for the TSAPI service, navigate to **Start ➔ Programs ➔ CAppMan** to access the Cacti_Application_Manager page. In the Cacti_Application_Manager page, select **Cacti_AES_Tsapi_Client_01** and click the **Settings** button.
The following screen shows the Cacti_AES_Tsapi_Client_01 Settings page. Provide the following information:

- Tsapi_SveID – Enter the Tlink name used. The Tlink name can be obtained by accessing Avaya AES through the web, and navigate to Administration → Security Database → Tlinks.
- Tsapi_loginID – Enter the user name created in Section 4.2
- Tsapi_Passwd – Enter the password created in Section 4.2.
- Tsapi_AppName – Enter the switch connection name created in Section 4.1.
- Monitor_Devices – Enter the monitoring (recorded) extension range created in Section 3.4.

Click on Save to save the changes.
6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability, and performance testing. The feature testing evaluated the ability of Cacti FocusRecord Enterprise to monitor and record calls placed to and from stations and agents. The serviceability testing introduced failure scenarios to see if Cacti FocusRecord Enterprise can resume recording after failure recovery. The performance testing stressed Cacti FocusRecord Enterprise by continuously placing calls over extended periods of time.

6.1. General Test Approach

The general approach was to place various types of calls to and from stations, agents, and hunt group number, monitor and record them using Cacti FocusRecord Enterprise, and verify the recordings. For feature testing, the types of calls included internal calls, inbound and outbound trunk calls, transferred calls, bridged calls, and conferenced calls. Performance tests verified that Cacti FocusRecord Enterprise could record calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES.
7.1. Verify Avaya Communication Manager

Verify the status of the administered AES link by using the `status aesvcs link` command.

```
status aesvcs link

AE SERVICES LINK STATUS
Srsvr/ AE Services Remote IP Remote Local Node Msgs Msgs
Link Server Port                    Sent Rcvd
01/01 server1         192. 45. 80.102 36538 CLAN-AES 17 18
```

Verify the status of the administered TSAPI CTI link by using the `status aesvcs cti-link` command.

```
status aesvcs cti-link

AE SERVICES CTI LINK STATUS
CTI Version Mnt AE Services Service Msgs Msgs
Link           Busy Server           State         Sent Rcvd
2              no    server1          restarting 15 15
4     4        no    server1          established 15 15
```

7.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services by selecting `Status and Control → Services Summary` from the left pane.

8. Support

Technical support for Cacti FocusRecord Enterprise can be obtained by contacting via the support link at [http://support@cacticom.com](http://support@cacticom.com) or by calling the support telephone number at 1-(866) 34cacti.

9. Conclusion

These Application Notes illustrate the procedures for configuring Cacti FocusRecord Enterprise call recording solution to monitor and record calls placed to and from stations and VDNs on an
Avaya Communication Manager system. In the configuration described in these Application Notes, Cacti FocusRecord Enterprise employs DMCC API virtual stations as recording ports. During compliance testing, Cacti FocusRecord Enterprise successfully monitored events and recorded calls placed to and from stations, as well as calls placed to a VDN and then queued to an agent hunt/skill group. Cacti FocusRecord Enterprise was also able to record calls under continuous call volumes over extended periods of time.

10. Additional References

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

The following Avaya product documentation can be found at [http://support.avaya.com](http://support.avaya.com).


The following Cacti product documentation was provided by Cacti

©2008 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.