AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring CallCopy cc: Discover R4.5 with Avaya Proactive Contact R5.0, Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Application Enablement Services R6.1 using Multi Registration for Call Recording – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning CallCopy cc: Discover with Avaya Proactive Contact R5.0 to record calls handled by Avaya Proactive Contact 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.

PG; Reviewed:
SPOC 5/7/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
1 of 32
ccDisc_PC5_MR

1. Introduction

These Application Notes outline the steps necessary to configure cc: Discover R4.5 from CallCopy to successfully interoperate with Avaya Proactive Contact R5.0, Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Application Enablement Services R6.1 to record voice calls. CallCopy cc: Discover (cc: Discover) is a software-only solution for voice call recording that offers various recording, playback and archiving features and options. These Application Notes focus on recording of calls using multiple registrations on Avaya Aura® Communication Manager in order to record Real-time Transport Protocol (RTP) stream from each deskphone on an Avaya Proactive Contact call. cc: Discover's internal scheduling algorithm makes the determination on which calls should be recorded based on the events received via Avaya Proactive Contact Event Services. cc: Discover uses Multi Registration to register as an IP Softphone in order to mimic the registration of the deskphone to be recorded.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of cc: Discover to record voice by Multi Registration using events captured by its TSAPI and Agent API interface with Proactive Contact. The feature test cases were performed both automatically and manually. Outbound calls were automatically placed by Proactive Contact, and inbound calls were manually placed and delivered via a simulated PSTN connection on Communication Manager. Agents log into different Proactive Contact Jobs to verify proper generation and handling of events from Proactive Contact Agent Event Services. All test cases were executed.

The compliance testing incorporated both Intelligent Call Blending (ICB) and Proactive Agent Blending (PAB) on Proactive Contact. ICB distributes a blend of inbound and outbound calls to Proactive Contact agents. With ICB, agents handle outbound calls until there are more inbound calls than available inbound agents. ICB passes the excess inbound calls to the blend agents. When the inbound call volume decreases, Proactive Contact returns to passing outbound calls to the blend agent.

Proactive Agent Blending integrates outbound calling activities on Avaya Proactive Contact with inbound calling activities on Communication Manager. Agent Blending monitors the activity on the ACD to determine when to move agents between inbound and outbound calling activities. The dialer acquires the pooled agents for outbound calling when the inbound calling activity decreases. The dialer releases the pooled agents to inbound calling when the inbound calling activity increases. The movement between inbound and outbound calling keeps the ACD blend agents busy and the ACD service level within configured prescribed limits.

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.

2.1. Interoperability Compliance Testing

Compliance Testing focuses on verifying events from Proactive Contact Event Services and verifying recordings for all calls associated with the following jobs on Proactive Contact.
- Outbound
- Preview/Managed
- Inbound
- Intelligent Call Blend
- Proactive Agent Blend

Events and recordings were observed for the following scenarios.
- Proactive Contact Agent Events –Login, Logout, Leave Job, Join Job, Release Line, Finish Work
- Proactive Contact Call Events - Hold, Retrieve, Call transfer, Conference, Manual call, Agent drop, Customer drop, Release line/Hang-up, and Finish work
- TSAPI/DMCC Events – Events showing Multi Registration and ACD calls
- Recordings of Calls– Test call recording for agent calls on each job type
- Failover testing - The behaviour of cc Discover under different simulated LAN failure conditions

2.2. Test Results

All compliance test cases passed successfully. There were no errors observed on the Avaya Solution as a result of the addition of CallCopy cc: Discover.

2.3. Support

Support from Avaya is available by visiting the website http://support..avaya.com and a list of product documentation can be found in **Section 11** of these Application Notes. Support from CallCopy is available at http://www.callcopy.com or from the information shown here.

     CallCopy Inc
     530 W Spring St, Columbus, OH 43215, USA.
     Tel: +1 614 340 3346
     Email: support@callcopy.com

3. Reference Configuration

The diagram below, **Figure 1**, shows the compliance tested configuration which includes Proactive Contact R5.0 using PG230 Hard Dialer connected to an ISDN PRI DS1 Board in a G650 Gateway. CallCopy cc: Discover obtains events from Avaya Proactive Contact and using Application Enablement Services it records the RTP using Multi Registration.
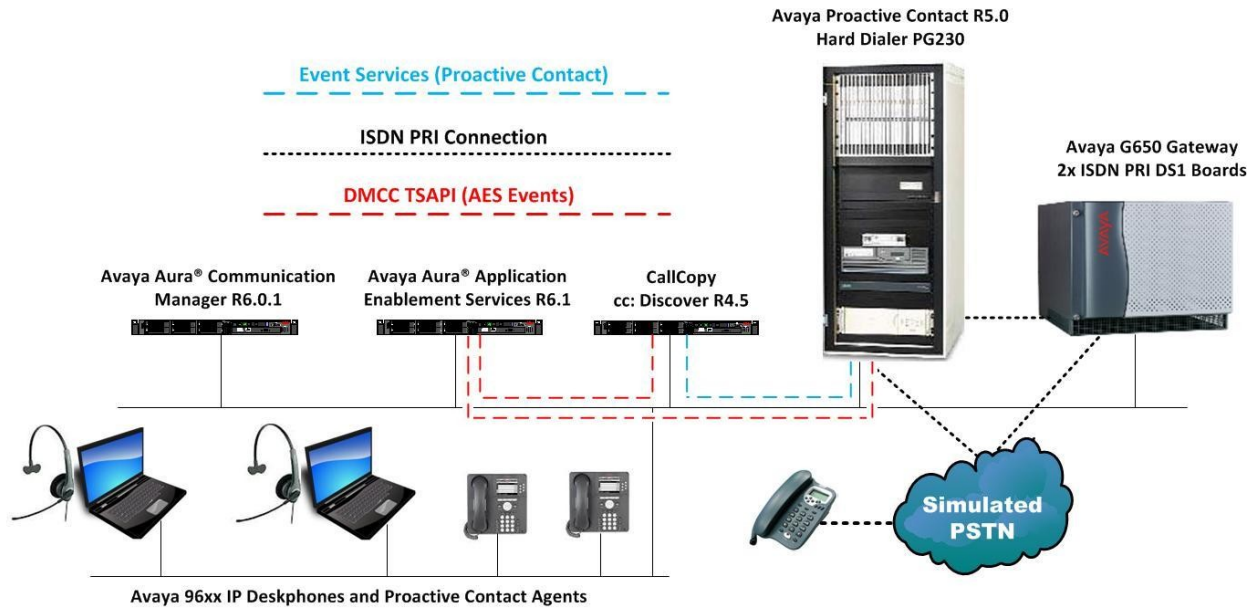

Figure 1: CallCopy cc: DiscoverR4.5 interoperability with Avaya Proactive Contact R5.0 and Avaya Aura® Application Enablement Services R6.1

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.0.1 SP6
Avaya G650 Gateway 2 x ISDN DS1 Boards	N/A
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.1
Avaya Proactive Contact	R5.0
Avaya Proactive Contact Hard Dialer PG230	R5.0
Avaya 96xx Series Deskphone	96xx H.323 Release 3.1 SP2
Avaya 2400 Series Deskphone	N/A
CallCopy cc: Discover running on Windows 2008 Server	R4.5 SP1

PG; Reviewed:
SPOC 5/7/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

5 of 32
ccDisc_PC5_MR

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing and an ISDN connection setup to Avaya Proactive Contact. It is also assumed that Vectors and Skill Groups are configured for inbound and acquire calls. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes.

The following sections go through the configuration of a CTI link and adding of virtual stations for use in Multi Registration.

5.1. Configure TSAPI CTI Link

Enter the **add cti-link x** command, where **x** is a number between 1 and 64, inclusive. Enter a valid **Extension** under the provisioned dial plan. Set the **Type** field to **ADJ-IP** and assign a descriptive **Name** to the CTI link. Default values may be used in the remaining fields.

```
add cti-link 1                                              Page   1 of   3
                                 CTI LINK
 CTI Link: 1
Extension: 4999
     Type: ADJ-IP
                                                                    COR: 1

     Name: devconaes61
```

Enter the **change node-names ip** command. In the compliance-tested configuration, the **procr** IP address was utilized for registering H.323 endpoints (Avaya IP Telephones, Avaya IP Agents, and Avaya AES DMCC stations). The **clancm601** IP address was used for connectivity to the Application Enablement Services server. Note also the AES server name and IP address added, **devconaes611** and **10.10.16.29**.

```
change node-names ip                                       Page   1 of   2
                               IP NODE NAMES
    Name              IP Address
aammstd           10.10.16.122
clancm601         10.10.16.31
default           0.0.0.0
devconaes611      10.10.16.29
medprocm601       10.10.16.32
netscreen         10.10.16.1
procr             10.10.16.47
procr6            ::
sesmgr-sm100      10.10.16.201
tn2302medproa10   10.10.16.33
```

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 **clancm601** that was configured previously in the node-name ip form. During the compliance test, the default port was utilized for the **Local Port** field.

```
change ip-services                                             Page    1 of    3

                              IP SERVICES
  Service      Enabled      Local       Local       Remote       Remote
   Type                     Node        Port        Node         Port
AESVCS          y        clancm601      8765
```

On **Page 3**, enter the hostname of the AES server for the AE Services Server field. Enter an alphanumeric password for the **Password** field. Set the **Enabled** field to **y**. The same password will be configured on the Application Enablement Services in **Section 6.1**.

```
change ip-services                                             Page    3 of    3
                         AE Services Administration

   Server ID     AE Services      Password         Enabled    Status
                   Server
       1:       devconaes611    Avayapassword1        y        in use
       2:
       3:
       4:
       5:
```

5.2. Configure IP Softphone for Multi Registration

Change the stations that are to be monitored by cc: Discover in order to record calls. IP SoftPone 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 8.1.** Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**. Take note of the **COR** number displayed below.

```
change station x                                              Page   1 of   6
                                  STATION

Extension: x                         Lock Messages? n              BCC: 0
     Type: 9630                      Security Code: 1234           TN: 1
     Port: S00101                    Coverage Path 1:              COR: 1
     Name: Recorder                  Coverage Path 2:              COS: 1
                                     Hunt-to Station:
STATION OPTIONS
                                     Time of Day Lock Table:
            Loss Group: 19        Personalized Ringing Pattern: 1
                                        Message Lamp Ext: 1591
         Speakerphone: 2-way          Mute Button Enabled? y
     Display Language: english
 Survivable GK Node Name:
         Survivable COR: internal      Media Complex Ext:
   Survivable Trunk Dest? y           IP SoftPhone? y

                                     IP Video Softphone? n
                        Short/Prefixed Registration Allowed: default
```

Type **display cor x**, where x is the COR number in the screen above, to check the existing Class of Restriction. Ensure that **Can be Service Observed** is set to **y**. If not type **change cor 1** to make a change to Class or Restriction (cor) 1. This needs to enabled for Multi registration to work properly.

```
display cor 1                                                  Page 1 of 23
                            CLASS OF RESTRICTION

                    COR Number: 1
              COR Description:

                         FRL: 0                             APLT? y
    Can Be Service Observed? y         Calling Party Restriction: all-toll
    Can Be A Service Observer? y        Called Party Restriction: none
            Time of Day Chart: 1     Forced Entry of Account Codes? n
            Priority Queuing? n             Direct Agent Calling? y
        Restriction Override: all     Facility Access Trunk Test? n
        Restricted Call List? n             Can Change Coverage? n
      Unrestricted Call List: 1
               Access to MCT? y           Fully Restricted Service? n
   Group II Category For MFC: 7       Hear VDN of Origin Annc.? n
            Send ANI for MFE? n           Add/Remove Agent Skills? n
                MF ANI Prefix:           Automatic Charge Display? n
   Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? y
                                   Can Use Directed Call Pickup? y
                                   Group Controlled Restriction: inactive
```

6. Configure Avaya Aura® Application Enablement Services

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

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

6.1. Configure Switch Connection

Launch a web browser, enter https://<IP address of AES server> in the URL, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console page.
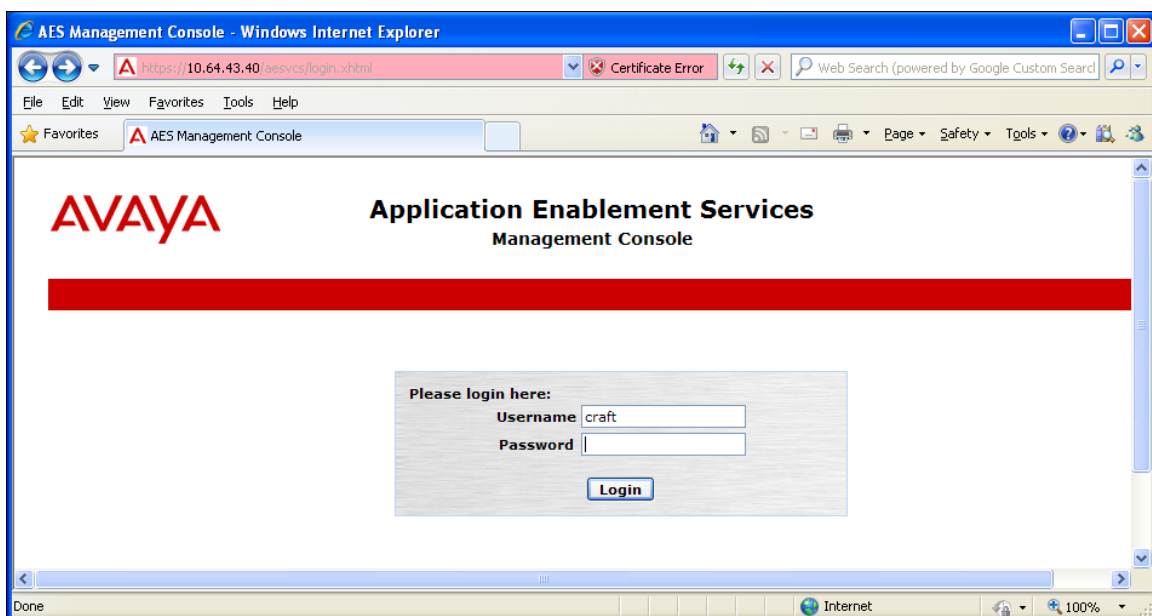
Click on **Communication Manager Interface→ Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

The next window that appears prompts for the Switch Password. Enter the same password that was administered on Communication Manager in **Section 5.1**. 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 PE/CLAN IPs**.

Enter the IP address of clan used for Application Enablement Services connectivity from **Section 5.1**, and click on **Add Name or IP**.

6.2. Configure TSAPI CTI Link

Navigate to **AE Services → TSAPI → TSAPI Links** to configure the TSAPI CTI link. Click the **Add Link** button to start configuring the TSAPI link.

Select the switch connection using the drop-down menu. Select the switch connection configured in **Section 6.1**. 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 in **Section 5.1**. Click **Apply Changes**.

PG; Reviewed:
SPOC 5/7/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
12 of 32
ccDisc_PC5_MR

6.3. Configure CTI User

Navigate to **User Management → Add User**. On the Add User page, provide the following information.

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

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 here) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

Once the user is created, navigate to the **Security → 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 checking the **Unrestricted Access** check box. Click the **Apply Changes** button.

Navigate to the **Security → Security Database → Tlinks** page and verify the Tlink name. The following screen shows the Tlink used during the compliance test.

PG; Reviewed:
SPOC 5/7/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

15 of 32
ccDisc_PC5_MR

7. Configure Avaya Proactive Contact

It is assumed that a fully operational Proactive Contact is in place and the connection is made to Communication Manager in order to acquire agents. Documentation on the Installation and Configuration of Proactive Contact may be found in **Section 11** of these Application Notes.

7.1. Obtain Proactive Contact Certificates

cc: Discover is required to register certificates from Avaya Proactive Contact and these certificates can be obtained as follows:

1. On the Proactive Contact server, go to **/opt/avaya/pds/openssl**
2. Copy the following files
   /private/**corbaServer_key.pem**
   /certificate/**corbaServer_cert.pem**
   /cacertificate/**ProactiveContactCA.pem**
3. Paste the above three files into the **C:\Certificates** folder on cc: Discover.

7.2. Check Proactive Contact Agent cc: Discover user details

Proactive Contact is installed with 10 pre-configured agents Agent 01-10 with corresponding passwords. In the compliance test Agent 10 was used by cc: Discover to log in and receive events from Event Services.

PG; Reviewed:
SPOC 5/7/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
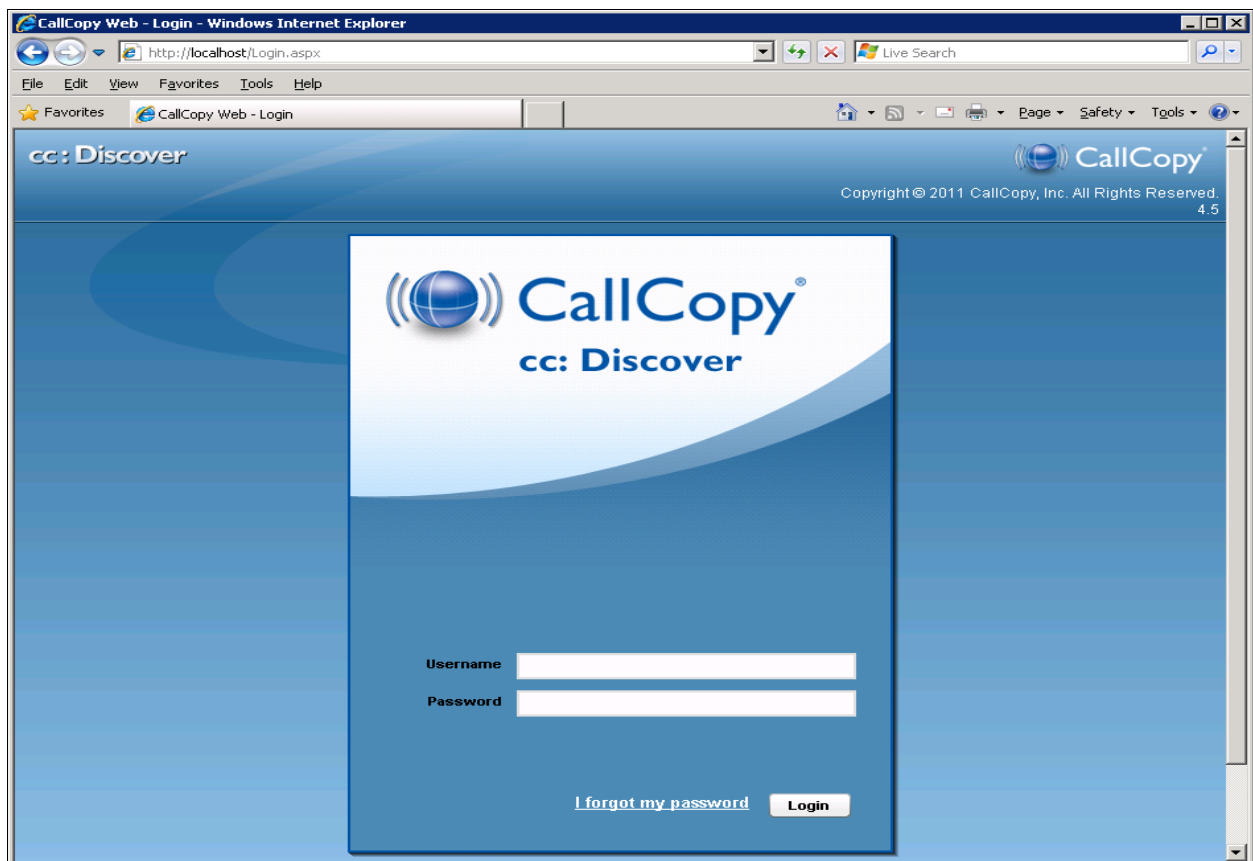16 of 32
ccDisc_PC5_MR

8. Configure CallCopy cc: Discover

This section outlines the steps necessary to configure cc: Discover to successfully connect to the Avaya Solution outlined in **Section 3** of these Application Notes in order to record voice calls. cc: Discover logs into AES in order to send/receive CTI messages to/from Communication Manager in order to utilise Multi-Registration to record voice calls. The Agent API on cc: Discover allows a configured agent to log into Proactive Contact and receive events from Proactive Contact Event Services in order to stop and start the call recording. The following sections will show:

- Configuration of cc: Discover to connect to AES for Multi Registration
- Configuration of cc: Discover to receive Proactive Contact Events

8.1. Configure CallCopy cc: Discover to connect to AES for Multi Registration

Open a web browser, navigate to **http://<cc: Discover machine name>** or **http://<cc: Discover IP Address>** . Enter the appropriate credentials and click **Login**.

PG; Reviewed:
SPOC 5/7/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

17 of 32
ccDisc_PC5_MR

Click on the **Administration** tab on the top of the page and under **Settings** in the left column click on **Voice Boards**. Click on **Add Board** to configure a new board.
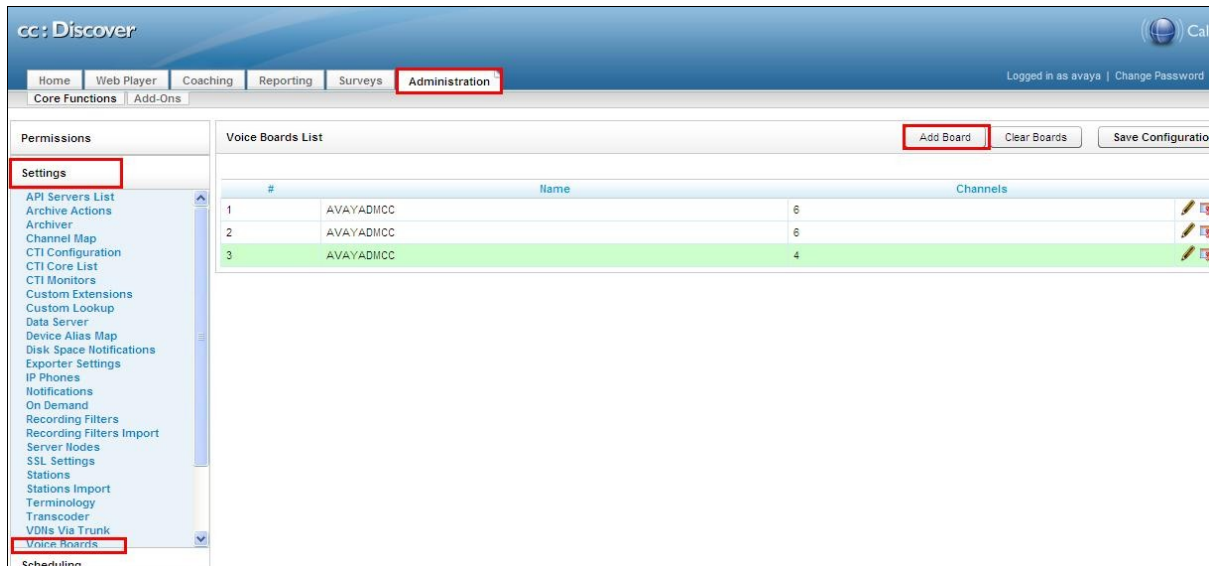
The following two screens show the configuration required for the Voice Board for Single Step Conference and Service Observe. Enter the following details as shown below.

- **AES/DMCC Host**   IP Address of the AES Server
- **DMCC User**   Username as configured in **Section 6.3**
- **DMCC Password**   Password as configured in **Section 6.3**
- **Avaya Call Manager Host** CLAN IP address of Communication Manger
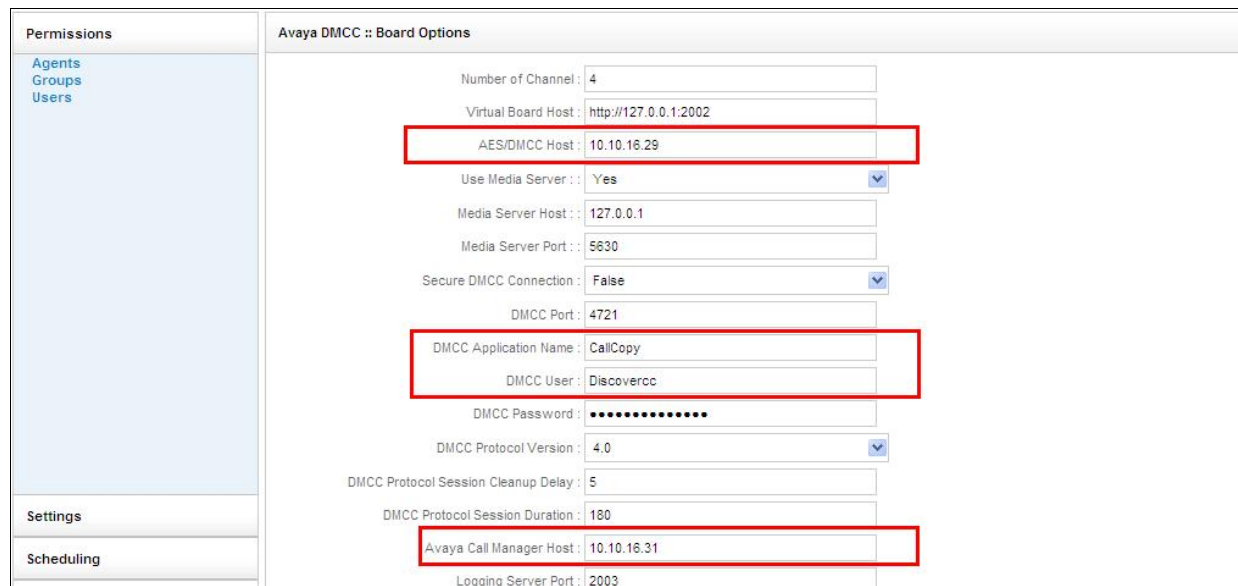
Further down on the same page, enter the following details as shown below.

- **DMCC Station Endpoint Host**   IP Address of the cc: Discover Server
- **RTP Listening Interface (NIC)**   Unique identifier of eth cc: Discover NIC Card

Under **Channel Configuration** enter the station numbers to be monitored. Any station that needs to be recorded is included here and each will be configured on Communication Manager as outlined in **Section 5.2.** Enter the station passwords obtained as shown in **Section 5.2**. Ensure that **#Assign** is set to **Dedicated Record Voice Port**. Once the correct information is filled in click on **Save** at the top right corner (not shown).

Click on the **Administration** tab on the top of the page and under **Settings** in the left column click on **CTICore List**. Click on **Add Core** to create a new Core.
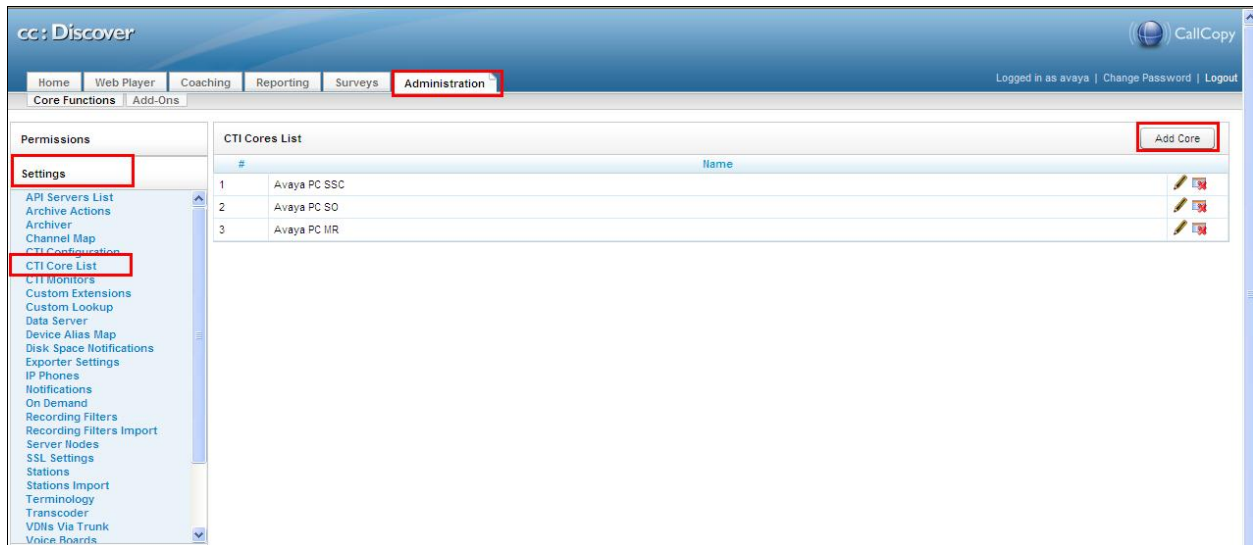
The following two screens show the CTI Settings screen for a Multi Registration recording solution. Enter the IP address of the cc: Discover Server under **Host** and choose **Passive** for the **Record Method**.
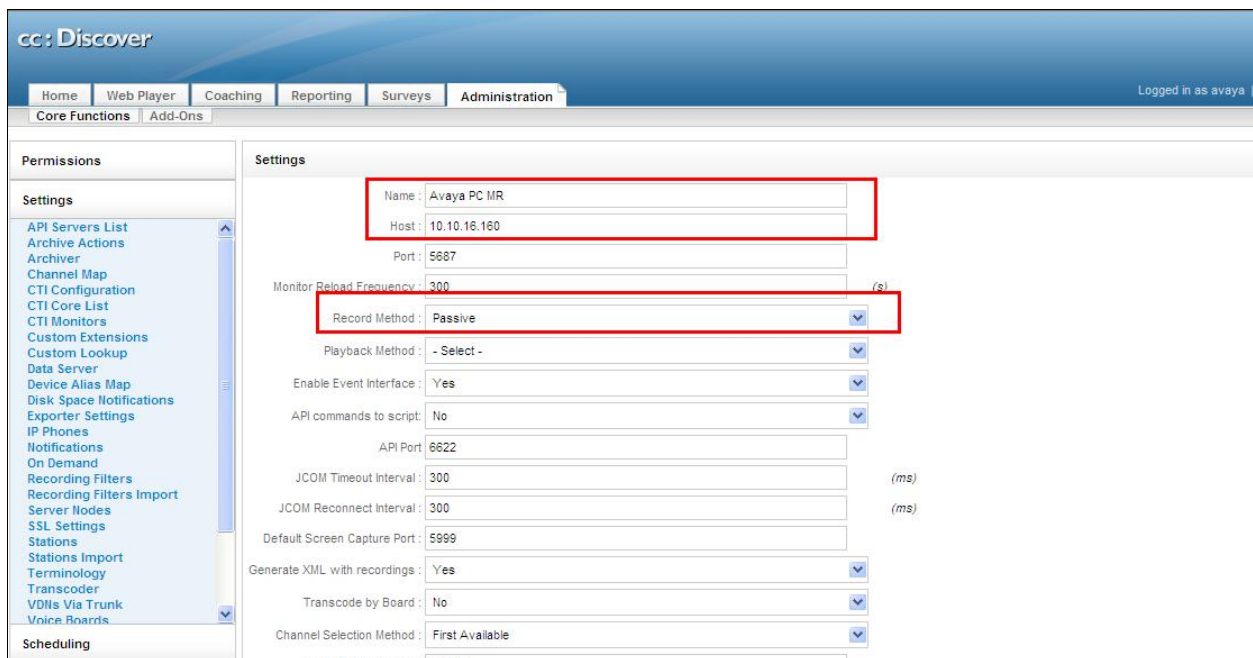
Under **Related Components** ensure that the board configured above is selected for **Related Boards** and click on the icon highlighted beside **cc_AvayaTSAPIFx** to edit.

Enter the AES Tlink string obtained in **Section 6.3** under **Server Name** and enter the administered CTI user under **Server Username** and **Server Password** for the AES server. Enter the device numbers to be monitored under **Monitor Values** and click on the + icon as highlighted below to add these devices. Click on **Save** highlighted below once the configuration has been inputted correctly.

8.2. Configuration of cc: Discover to receive Proactive Contact Events

Click on **Back** on the above screen in Section 8.1 this will bring up the screen shown below. Click on **Add CTI Module** to add second CTI Module for the connection to Avaya Proactive Contact.

Enter the Proactive Contact **Server** name and the **Username** and **Password** obtained in **Section 7.2.** Note also the **Certificate Directory** location where the certificates used for connecting to Proactive Contact is stored. These are the certificates obtained in **Section 7.1.** Click **Save** once the correct information is filled in.

9. Verification Steps

The following steps can be taken to ensure that connections between Communication Manager, AES, Proactive Contact and cc: Discover are up.

9.1. Verify Avaya Aura® Communication Manager

Verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify the Service State is **established** for the CTI link number administered in **Section 5.1**, as shown below.

```
status aesvcs cti-link

                    AE SERVICES CTI LINK STATUS

CTI     Version  Mnt   AE Services      Service       Msgs    Msgs
Link             Busy  Server           State         Sent    Rcvd

1                no                     down          0       0
4       4        no    aes              established   15      15
```

9.2. Verify Avaya Aura® Application Enablement Services

From the Application Enablement Services Management Console web pages, verify the state of the TSAPI Service is set to **ONLINE** by selecting **Status** from the left pane.

PG; Reviewed:
SPOC 5/7/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
23 of 32
ccDisc_PC5_MR

9.3. Verify Proactive Contact services are running correctly

Using putty open an SSH connection to Proactive Contact and **login** using the appropriate credentials as shown below.

```
login as: admin
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

                         ***  WARNING NOTICE  ***

This system is restricted solely to Avaya authorized users for legitimate
business purposes only. The actual or attempted unauthorized access, use,
or modification of this system is strictly prohibited by Avaya. Unauthorized
users are subject to Company disciplinary proceedings and/or criminal and
civil penalties under state, federal, or other applicable domestic and
foreign laws. The use of this system may be monitored and recorded for
administrative and security reasons. Anyone accessing this system expressly
consents to such monitoring and is advised that if monitoring reveals possible
evidence of criminal activity, Avaya may provide the evidence of such activity
to law enforcement officials. All users must comply with Avaya Security
Instructions regarding the protection of Avaya's information assets.


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Using keyboard-interactive authentication.
Password:
```

Once logged in correctly type **check_pds** as shown below.

```
================================================================================
=======================================
   # ID          Sev      Short Text                   Enabled   First
Instance      Last Instance      Count  State
 -----------------------------------------------------------------------------------
-------------------------------------------
   3 QPC000D0001  Info     Services started  - PDS        Yes      2012-03-01
16:06:48  2012-03-01 16:06:48   1  ACTIVE
   4 QPC000D0002  Info     Services started  - MTS        Yes      2012-02-29
16:31:39  2012-02-29 16:31:39   1  ACTIVE
   5 QPC000D0003  Info     Services started  - DB         Yes      2012-02-29
16:30:30  2012-02-29 16:30:30   1  ACTIVE
  25 QPC000D0023  Warning  Illegal agent logoff          Yes      2011-05-24
18:48:20  2012-03-01 16:25:58  431  ACTIVE


================================================================================
=======================================
  Found '4' ACTIVE or RETIRED alarms.

DEVCONHD(admin)@/opt/avaya/pds [992]
$ check_pds
```

The following screen should show **All processes running!**.

```
root     28532    1  0 Mar01 ?         00:00:00 agent -d
admin    28543    1  0 Mar01 ?         00:00:00 ao_recall
admin    28539    1  0 Mar01 ?         00:00:00 recall_rmp
admin    28529    1  0 Mar01 ?         00:00:00 listserver
admin    28216    1  0 Mar01 ?         00:00:00 opmon
root     28238    1  0 Mar01 ?         00:00:00 evmon
root     28125 28116  0 Mar01 ?        00:00:00 /opt/avaya/pds/bin/enforcer -ORB
root     28106    1  0 Mar01 ?         00:00:00 bridgeSmEnf -ORBSvcConf /opt/ava
admin    28101    1  0 Mar01 ?         00:00:00 switcher
admin    28069    1  0 Mar01 ?         00:00:00 job_strter
root     28054    1  0 Mar01 ?         00:00:00 agentcount
root     28037    1  0 Mar01 ?         00:04:00 enserver -ORBSvcConf /opt/avaya/
root     28565    1  0 Mar01 ?         00:01:20 dccserver -ORBSvcConf /opt/avaya
admin    28044    1  0 Mar01 ?         00:00:08 datamgr
admin    28025    1  0 Mar01 ?         00:00:00 soe_routed
admin    28027 28025  0 Mar01 ?        00:00:00 soe_routed
root     28062    1  0 Mar01 ?         00:00:00 signalit
admin    28030    1  0 Mar01 ?         00:00:00 conn_mgr
root     28571    1  0 Mar01 ?         00:01:08 hdsc -ORBSvcConf /opt/avaya/pds/

>>> All processes running!

DEVCONHD(admin)@/opt/avaya/pds [993]
$
```

Check the database is running correctly by typing **check_db** as shown. **All processes are running and the database is opened to the users!** should be returned.

```
DEVCONHD(admin)@/opt/avaya/pds [993]
$ check_db

Checking for required database processes...
Found:
oracle   29897    1  0 Feb29 ?         00:00:21 ora_smon_orastd
oracle   29893    1  0 Feb29 ?         00:00:54 ora_lgwr_orastd
oracle   29885    1  0 Feb29 ?         00:00:12 ora_pmon_orastd
oracle   29895    1  0 Feb29 ?         00:00:56 ora_ckpt_orastd
oracle   29891    1  0 Feb29 ?         00:00:11 ora_dbw0_orastd
oracle   29899    1  0 Feb29 ?         00:00:00 ora_reco_orastd
oracle   29913    1  0 Feb29 ?         00:00:00 ora_qmnc_orastd
oracle   29901    1  0 Feb29 ?         00:01:34 ora_cjq0_orastd
oracle   29907    1  0 Feb29 ?         00:00:00 ora_d000_orastd
oracle   29889    1  0 Feb29 ?         00:00:00 ora_mman_orastd
oracle   29909    1  0 Feb29 ?         00:00:00 ora_s000_orastd
oracle   29903    1  0 Feb29 ?         00:00:20 ora_mmon_orastd
oracle   29905    1  0 Feb29 ?         00:00:10 ora_mmnl_orastd
admin    29881    1  0 Feb29 ?         00:00:00 /opt/dbase/OraHome1/bin/tnslsnr

Verifying Database availability...

>>> All processes are running and the database is opened to the users!

DEVCONHD(admin)@/opt/avaya/pds [994]
$
```

Type **check_mts**, this should return **All processes are running** as shown.

```
================================================================================
======================================
   #  ID          Sev       Short Text                        Enabled   First
Instance       Last Instance      Count  State
 -------------------------------------------------------------------------------
-----------------------------------------------
   3  QPC000D0001  Info      Services started  - PDS           Yes       2012-03-01
16:06:48  2012-03-01 16:06:48   1   ACTIVE
   4  QPC000D0002  Info      Services started  - MTS           Yes       2012-02-29
16:31:39  2012-02-29 16:31:39   1   ACTIVE
   5  QPC000D0003  Info      Services started  - DB            Yes       2012-02-29
16:30:30  2012-02-29 16:30:30   1   ACTIVE
  25  QPC000D0023  Warning   Illegal agent logoff              Yes       2011-05-24
18:48:20  2012-03-01 16:25:58  431   ACTIVE


================================================================================
======================================
  Found '4' ACTIVE or RETIRED alarms.

DEVCONHD(admin)@/opt/avaya/pds [992]
$ check_mts

>>> All processes are running!
$
```

9.4. Verify Avaya Proactive Contact jobs are running

Before an agent is logged into a job verify that the correct jobs are running. Open Proactive Contact Editor (not shown) once logged in click on jobs as shown below and ensure that the correct jobs are up and running. **Jobs** cab be started and stopped using the icons highlighted in the screen shot below.

9.5. Verify CallCopy cc: Discover services are running

Log into cc: Discover as shown in **Section 8.1**. Under **Administration** tab select **Tools** on the left hand side and click on **Service Manager**. Under **Status** see which services are **Running**, an example of the correct services running is shown below.

9.6. Verify Call Events are being received by cc: Discover

Navigate to the /Program Files/CallCopy/Logs folder on the cc: Discover Server. Open a file called CC_CTICore1r.log. See an example of this file in the Appendix of these Application Notes.

9.7. Verify calls are begin recorded on cc: Discover

Recordings are stored on the cc: Discover server and can be replayed using Web Player as shown below. Click on the **Web Player** tab and click on **Call List** as shown below. Each call recorded is displayed and can be played by clicking on the required call. Confirm correct call information is displayed.

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

10. Conclusion

These Application Notes describe the configuration steps required for CallCopy cc: Discover to successfully interoperate with Avaya Proactive Contact Avaya Application Enablement Services and Avaya Aura® Communication Manager using Multi Registration. All test cases were completed successfully. Please refer to **Section 2.2** for test results and observations.

11. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com where the following documents can be obtained.

[1] *Administering Avaya Aura® Communication Manager,* Document ID 03-300509
[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205
[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 6.1 Issue 2
[4] *Application Notes for CallCopy cc:Discover with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference and Service Observing for Recordings*
[5] *Implementing Avaya Proactive Contact 5.0*

All information on the product installation and configuration cc: Discover can be found at http://www.callcopy.com

APPENDIX

Below is an extract from the CC_CTICore1r.log file. See highlighted **AGENT** and **CALL** events used to begin a recording for a Multi Registration Call.

2012-03-09 13:12:06.758	Info	0	Channel 0[4000] Type: CTI_EVENT_AVAYA_PC 8225(2005)

AGENTONCALL IP:

2012-03-09 13:12:06.759 Info 0 Channel 0[4000]
Msg==>timeReceived=13:12:06.742|dialerid=1|agentid=1106|TYPEOFCALL=OUTBOUNDCALL|CALLID=00100106913000 002|DEVICEID=1|EQUIPNUM=366|DNIS=92033333333|USERDATA=IDENT:ACCTNUM,5300292013187256<==

2012-03-09 13:12:06.914	Info	0	Channel 0[] Type: CTI_EVENT_AVAYA_PC 8225(1003)

CALLCONNECTED IP:

2012-03-09 13:12:06.916 Info 0 Channel 0[]
Msg==>timeReceived=13:12:06.910|dialerid=1|callid=00100106913000002|AGENTNAME=agent2|HEADSETEXTENSION=4 000|AGENTDEVICEID=2|AGENTEQUIPNUM=362|USERDATA=IDENT:ACCTNUM,5300292013187256|SWITCHID=1<= =

2012-03-09 13:12:06.916	Info	0	Sending callstart for callid and device 4000
2012-03-09 13:12:06.916	Info	0	Adding call 00100106913000002 to device 4000

2012-03-09 13:12:06.917 Debug 0 **CALL START** deviceid:4000 devicealias:agent2 group: gate: ani:4000
dnis:92033333333 callid: callinstance: user1: user2:outbnd2 user3: user4:dialer user5:00100106913000002 user6: user7: user8: user9: user10: user11: use12: user13:-1 user14: user15:, keepdays:-1, archiveaction:-1

2012-03-09 13:12:06.917	Debug	0	Looking for matching schedule.
2012-03-09 13:12:06.917	Info	0	Current state is ''
2012-03-09 13:12:06.918	Info	0	Current state '' was not found, using all associated schedules
2012-03-09 13:12:06.918	Info	0	Schedule ID: [1] Name: [Record All] matched.
2012-03-09 13:12:06.918	Debug	0	Schedule Record All matches at priority 50
2012-03-09 13:12:06.918	Info	0	Schedule ID: [0] Name: [DesktopOnly] failed to match condition [Expression Match]
2012-03-09 13:12:06.919	Debug	0	Schedule DesktopOnly doesn't match
2012-03-09 13:12:06.919	Info	0	Using schedule Record All.
2012-03-09 13:12:06.919	Debug	0	Selectting channel for recording.
2012-03-09 13:12:06.919	Debug	0	Setting board 3 channel 1 status to ReservedForRecording
2012-03-09 13:12:06.920	Debug	0	A channel was selected, it was not a stacked match. Recording will consume a concurrent recording slot.
2012-03-09 13:12:06.920	Debug	0	Selected board CallCopy.Recording.VoiceBoard channel Channel 1 - Assignment:DedicatedRecordDevice AssignmentValue:'4000' Name:'' Desc:'' for recording
2012-03-09 13:12:06.920	Debug	0	Setting board 3 channel 1 status to PreparingToRecord
2012-03-09 13:12:06.920	Debug	0	Setting board 3 channel 1 status to Recording
2012-03-09 13:12:06.921	Debug	0	CTIHost.RecordStart
2012-03-09 13:12:06.921	Debug	0	GetChannelByDeviceId - Using Existing Channel: Channel for deviceId[4000] localRtpPort:7000 remoteRtpPort:7001
2012-03-09 13:12:06.921	Debug	0	Opening file F:\Recordings\20120309\agent2\agent2-13-12-06.cca
2012-03-09 13:12:06.921	Debug	0	Writing .cca header to F:\Recordings\20120309\agent2\agent2-13-12-06.cca
2012-03-09 13:12:06.922	Info	0	Extension record begin: 4000 [F:\Recordings\20120309\agent2\agent2-13-12-06.cca]
2012-03-09 13:12:06.922	Debug	0	Record started [4000]
2012-03-09 13:12:06.922	Info	0	Notify stream detected from Avaya Dmcc device:4000 alias:agent2 record:5

```
setIp:0.0.0.0 setPort:7000
2012-03-09 13:12:06.922     Debug    0          Media server> Sending stream notification Detected

2012-03-09 13:12:06.923     Debug    0          10.10.16.160:5630BoardMaster SendJsonCommand():
```
{"command":"streamdetected","deviceid":"4000","devicealias":"agent2","recordid":"5","setip":"0.0.0.0","setport":"7000","gate":
"","group":"","ani":"4000","dnis":"92033333333","sys_username":"","requestId":1}
2012-03-09 13:12:06.923   Debug   0   CTIHost.RecordStart Complete

PG; Reviewed:
SPOC 5/7/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

32 of 32
ccDisc_PC5_MR