Avaya Solution & Interoperability Test Lab

Application Notes for configuring NICE Interaction Management R4.1 with Avaya Proactive Contact R5.0.1, Avaya Aura® Communication Manager R6.2 and Avaya Aura® Application Enablement Services R6.2 using Service Observe for recording – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning NICE Interaction Management R4.1 with Avaya Proactive Contact R5.0.1 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.

1. Introduction

These Application Notes outline the steps necessary to configure Interaction Management R4.1 from NICE to successfully interoperate with Avaya Proactive Contact R5.0.1 and Avaya Aura® Application Enablement Services R6.2 to record voice calls handled by Avaya Aura® Communication Manager endpoints. NICE Interaction Management is a software-only solution for voice call recording that offers various recording, playback and archiving features and options.

These Application Notes focus on using Service Observe in order to record the RTP from each deskphone on an Avaya Proactive Contact or ACD call. NICE Interaction Management records calls triggered by events received via Avaya Proactive Contact Event Services. When a call is to be recorded, NICE Interaction Manager uses TSAPI provided by Avaya Aura® Application Enablement Services to Service Observe a defined agent endpoint on Avaya Aura® Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Interaction Management to record voice using Service Observe by way of events captured by its TSAPI interface with Application Enablement Services (AES) and Agent API interface with Proactive Contact. The feature test cases are performed both automatically and manually. Outbound calls are automatically placed by Proactive Contact, and inbound calls are 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 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 agents configured for Agent Blend for outbound calling when the inbound calling activity decreases. The dialer releases the Agent Blend agents to inbound calling when the inbound calling activity increases. The automated movement of agents between inbound and outbound work maximises agent productivity and contributes to keeping 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 and verified for the following scenarios.

- Proactive Contact Agent Events –Login, Logout, Leave Job, Join Job, Release Line, Finish Work etc
- Proactive Contact Call Events - Hold, Retrieve, Call transfer, Conference, Agent drop, Customer drop, Release line/Hang-up, and Finish work
- TSAPI Events – Events showing Service Observe and triggers to record inbound calls under PAB scenario
- Recordings of Calls– Test call recording for agent calls on each job type, and under various call scenarios
- Failover testing - The behaviour of Interaction Management under different simulated LAN failure conditions
- Verification of accurate call data including time stamp, call parties, business data and call duration
- Verification of recording quality

2.2. Test Results

All compliance test cases passed successfully with the following observations:

- An extra 0 second duration call is seen in the scenario where agent1 in a blend job forwards work to agent2 in an inbound job either unattended or supervised. No call recording is lost.

2.3. Support

Support from Avaya is available at http://support.avaya.com and support from NICE can be obtained as shown below.

NICE International Corporate Headquarters, Israel
Tel: +972 9 775 3800
Email: support@nice.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 G450 Gateway controlled by Communication Manager running on an S8800 Server. NICE Interaction Management obtains events from Avaya Proactive Contact and using Application Enablement Services it records the RTP using the Service Observe method.

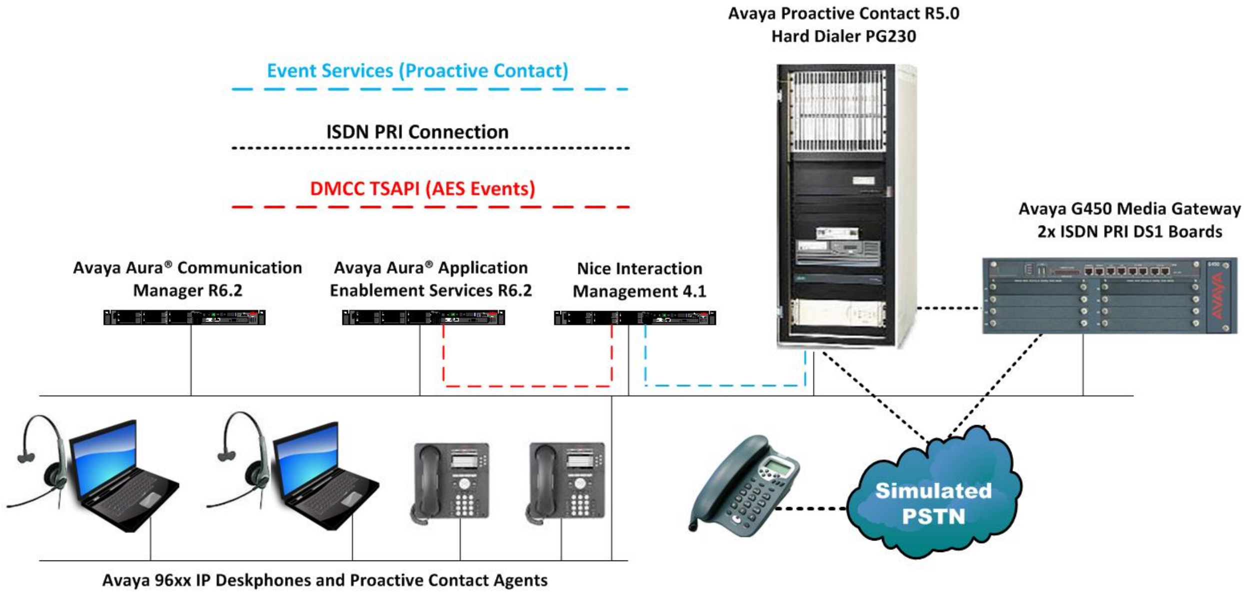

Avaya Proactive Contact R5.0
Hard Dialer PG230
Event Services (Proactive Contact)
ISDN PRI Connection
DMCC TSAPI (AES Events)
Avaya G450 Media Gateway
2x ISDN PRI DS1 Boards
Avaya Aura® Communication Manager R6.2
Avaya Aura® Application Enablement Services R6.2
Nice Interaction Management 4.1
Simulated PSTN
Avaya 96xx IP Deskphones and Proactive Contact Agents

Figure 1: NICE Interaction Management R4.1 interoperability with Avaya Proactive Contact R5.0, Avaya Aura® Communication Manager R6.2 and Avaya Aura® Application Enablement Services R6.2

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP3 R016x.02.0.823.0-20001
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.2
G450 Media Gateway MM710AP Media Module	31.22.0 HW5 FW022
Avaya Proactive Contact running on Avaya S8730 Server	R5.0.1 with patch 301, 302, 307, 309, 323, 328
Avaya 9630 H323 IP Telephone	R3.104S
Avaya PG230 Digital Switch	Generic Version 15.3.1
NICE Interaction Management	4.1

5. Configure Avaya Aura® Communication Manager

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

The following sections describe the configuration of a CTI link and adding of virtual stations required for Service Observe, as well as configuration of the service observe feature access code.

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: 5899
     Type: ADJ-IP
                                                                        COR: 1
     Name: aesserver62
```

Enter the **change node-names ip** command. In the compliance-tested configuration, the **procr** IP address was utilized for registering H.323 and connectivity to the Application Enablement Services server. Note also the AES server name and IP address added, **aesserver62** and **10.10.16.96**.

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
procr                   10.10.16.142
CM521                   10.10.16.23
Gateway                 10.10.16.1
IPbuffer                10.10.16.184
Intuition               10.10.16.51
MedPro                  10.10.16.32
Presence                10.10.16.83
RDTT                    10.10.16.185
SESMNGR                 10.10.16.44
SM1                     10.10.16.43
SM61                    10.10.16.201
default                 0.0.0.0
aesserver62             10.10.16.96
```

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 **procr** that was noted 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   4

                                    IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port

AESVCS        y          procr           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   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aesserver62       Avayapassword1         y        in use
```

5.2. Configure Virtual Stations for Service Observe

Add virtual stations to allow Interaction Management to record calls using Single Service Observe. Type **add station x** where x is the extension number of the station to be configured 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**. Note also the **COR** for the stations.

```
add station 6500                                     Page   1 of   6
                                     STATION

Extension: 6500                         Lock Messages? n              BCC: 0
     Type: 4624                         Security Code: 1234            TN: 1
     Port: IP                         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: 6500
            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 be enabled in order for Service Observe to work for recording.

```
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: none
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? n
     Restriction Override: none        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            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? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

5.3. Configure Service Observe Feature Access Code

Interaction Management uses the service observe feature access code in order to record the call of a defined endpoint. Interaction Management uses the AES to instigate the service observing of the defined endpoint. Enter the command **change feature-access-codes**, on **Page 5** enter a suitable code next to **Service Observing No Talk Access Code**.

```
change feature-access-codes                                Page   5 of  10
                               FEATURE ACCESS CODE (FAC)

                                 Call Center Features
  AGENT WORK MODES
                    After Call Work Access Code: *36
                             Assist Access Code:
                            Auto-In Access Code: *38
                           Aux Work Access Code: *39
                              Login Access Code: *40
                             Logout Access Code: *41
                          Manual-in Access Code: *42
  SERVICE OBSERVING
             Service Observing Listen Only Access Code: *43
             Service Observing Listen/Talk Access Code:
                 Service Observing No Talk Access Code: *06
   Service Observing Next Call Listen Only Access Code:
 Service Observing by Location Listen Only Access Code:
 Service Observing by Location Listen/Talk Access Code:
```

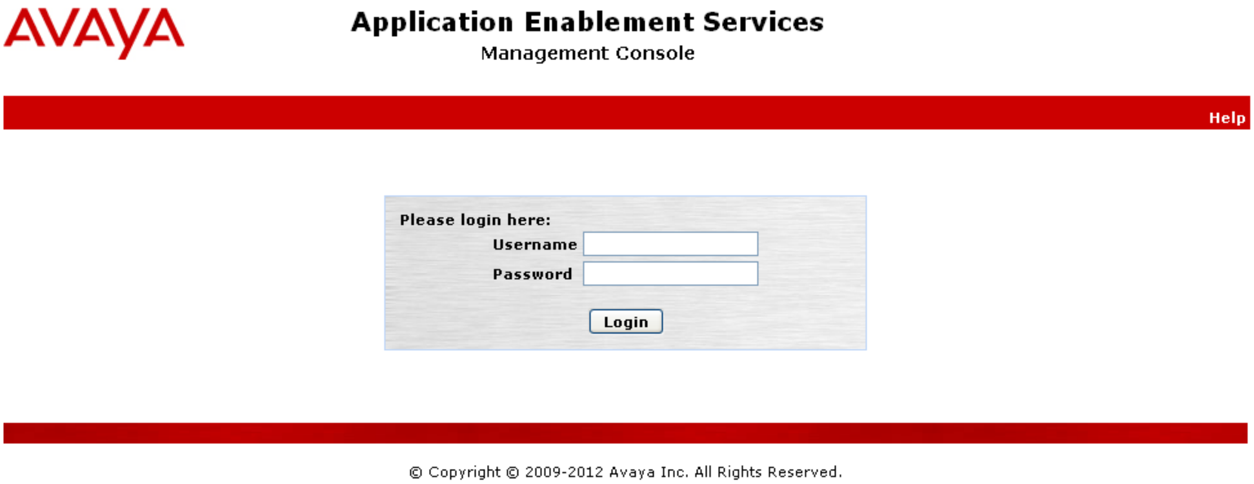
6. Configure Avaya Aura® Application Enablement Services

Application Enablement Services enable 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.

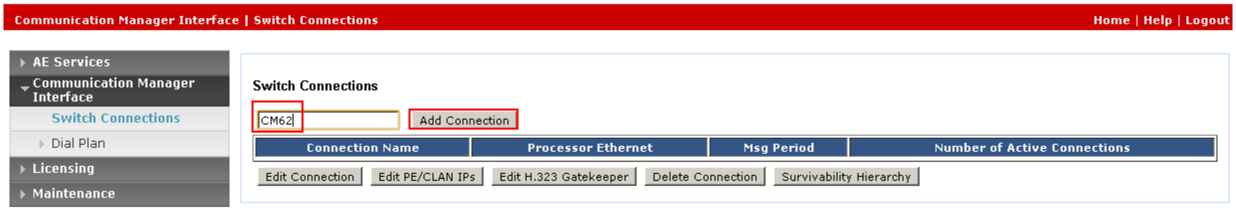
This section assumes that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, creating a CTI link for TSAPI, and a CTI user. For further information on Application Enablement Services please refer to **Section 11** of these Application Notes.

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.


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Password
Login
© Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

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**.

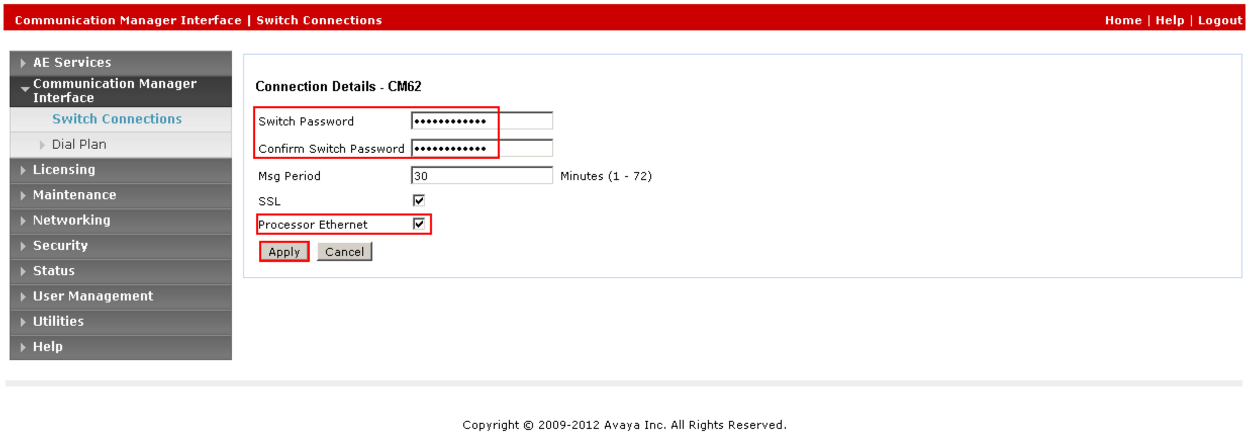


Switch Connections

CM62

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

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**.

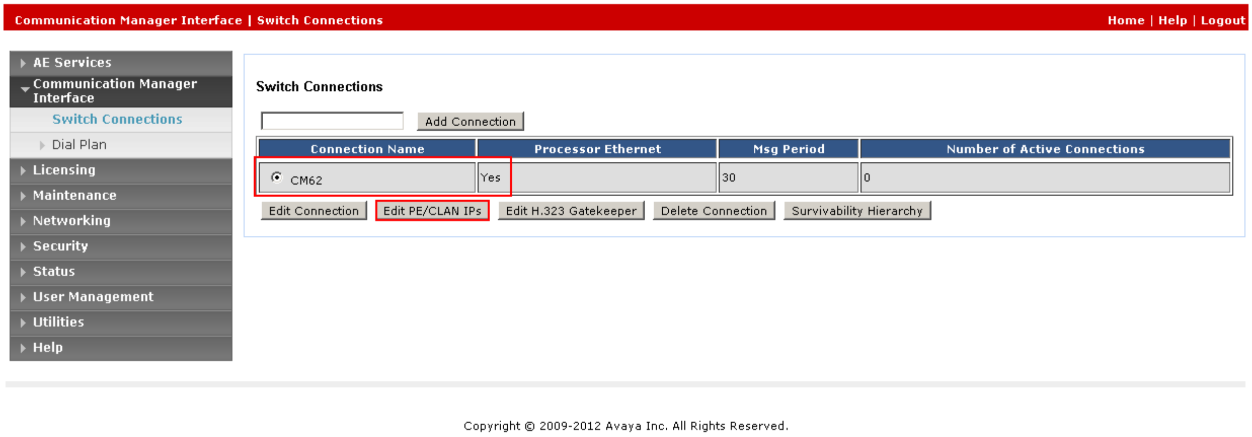


Connection Details - CM62

Switch Password ••••••••••••
Confirm Switch Password ••••••••••••
Msg Period 30 Minutes (1 - 72)
SSL ☑
Processor Ethernet ☑

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

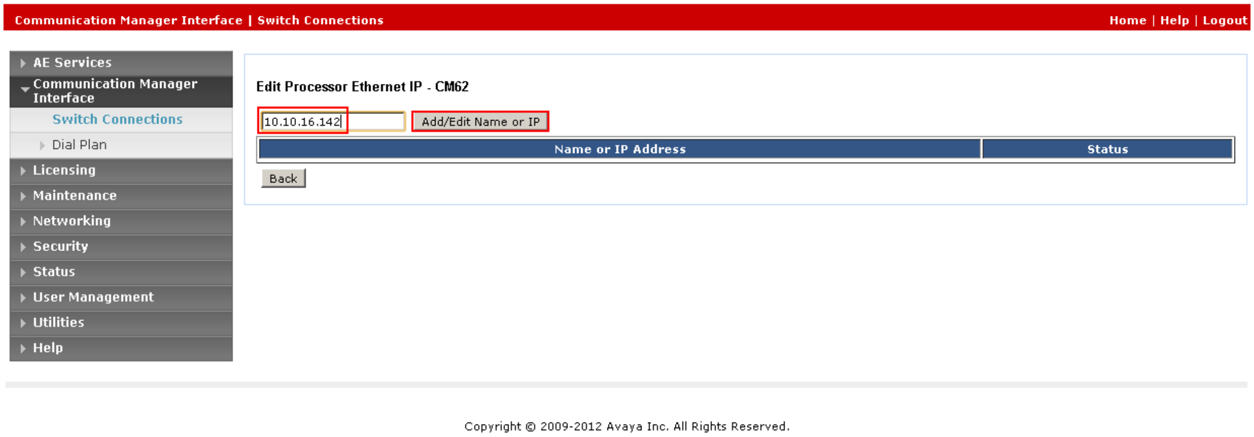
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit PE/CLAN IPs**.



Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● CM62	Yes	30	0

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

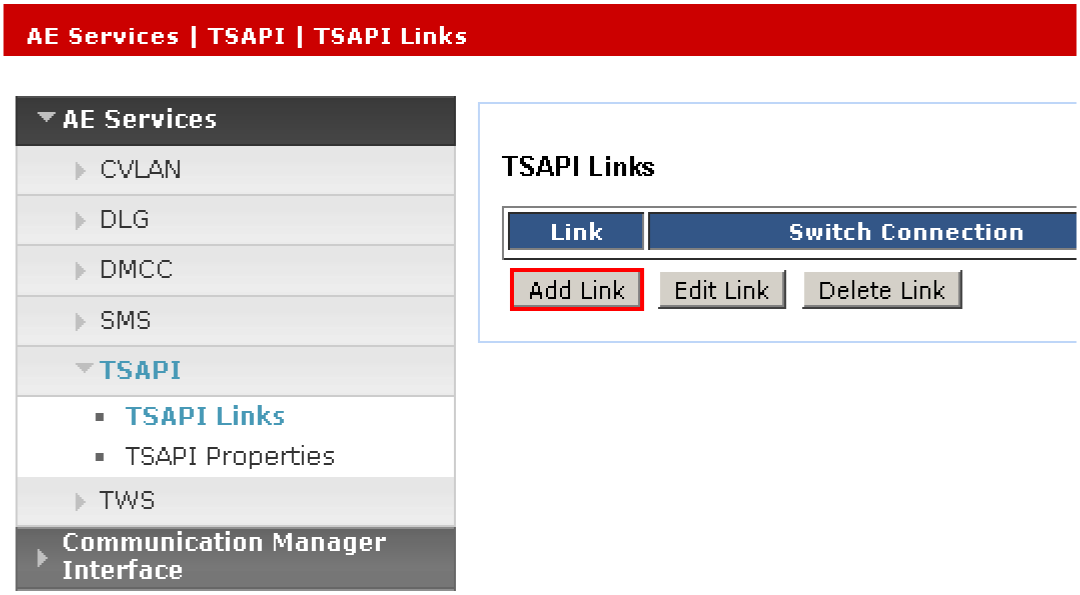


Edit Processor Ethernet IP - CM62

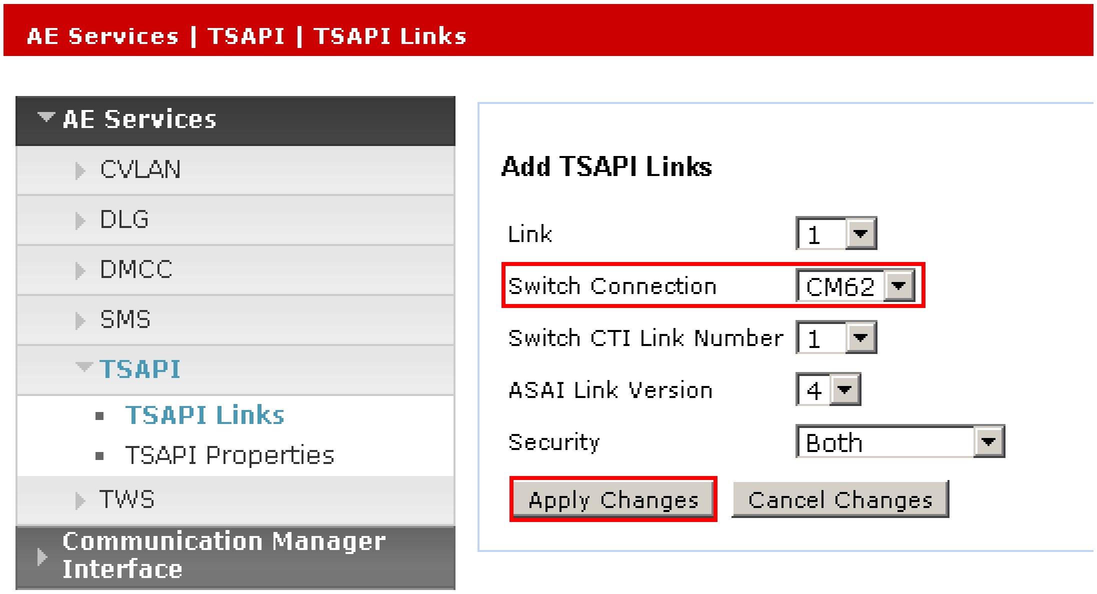
10.10.16.142

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**.



Add TSAPI Links

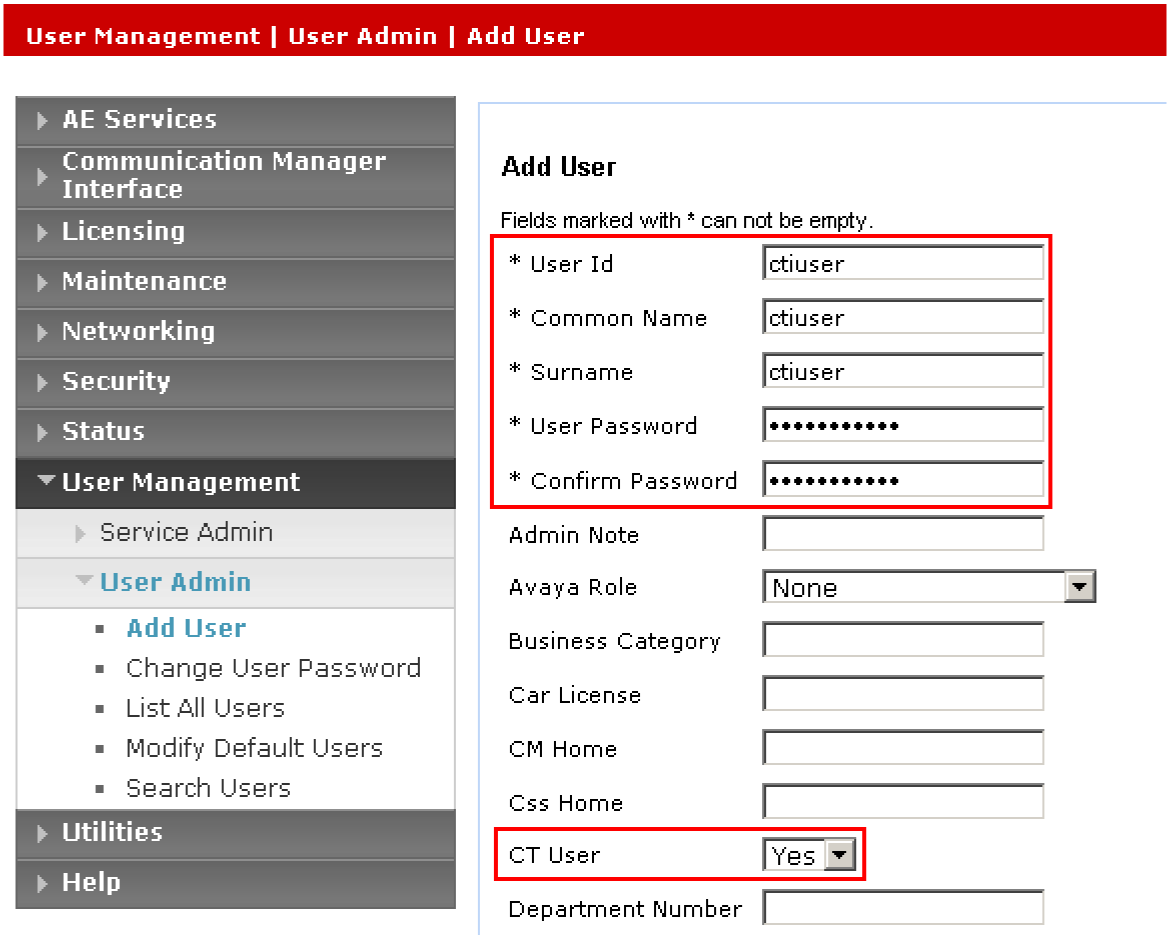
Link	1
Switch Connection	CM62
Switch CTI Link Number	1
ASAI Link Version	4
Security	Both

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.

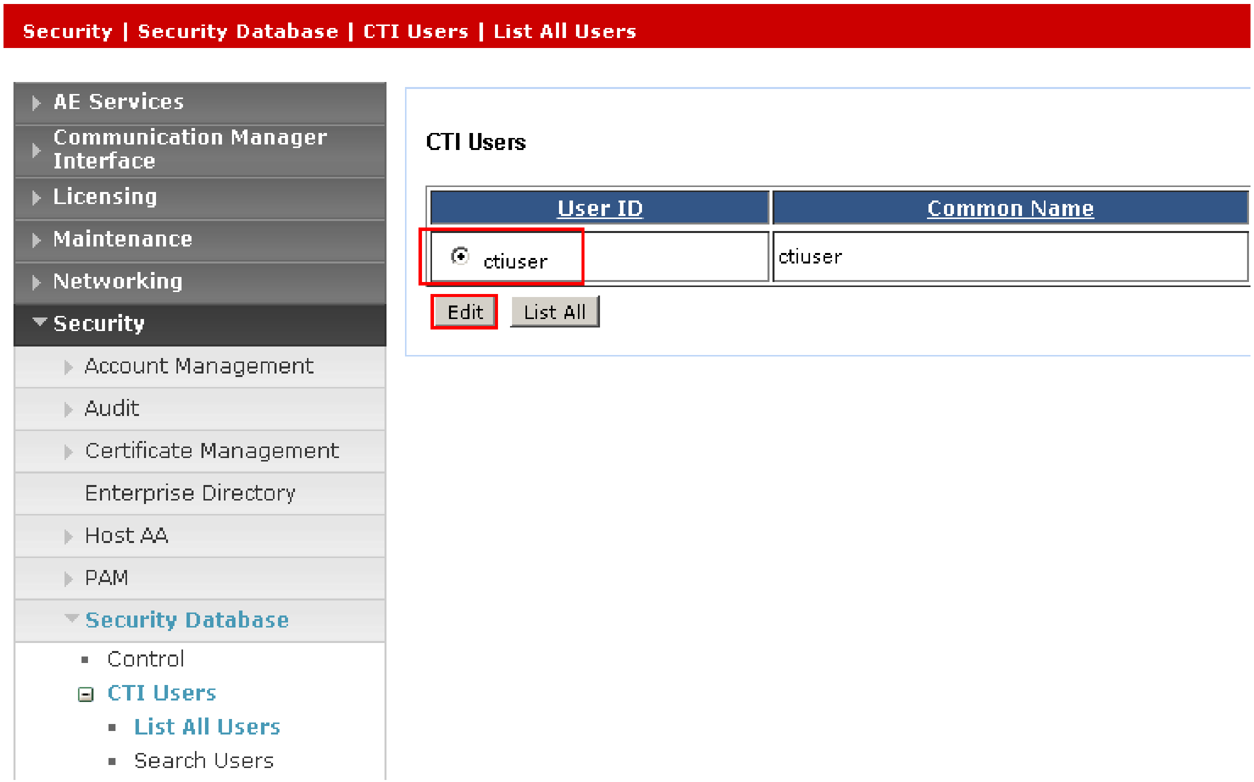


Add User

Fields marked with * can not be empty.

* User Id	ctiuser
* Common Name	ctiuser
* Surname	ctiuser
* User Password	••••••••••••
* Confirm Password	••••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	

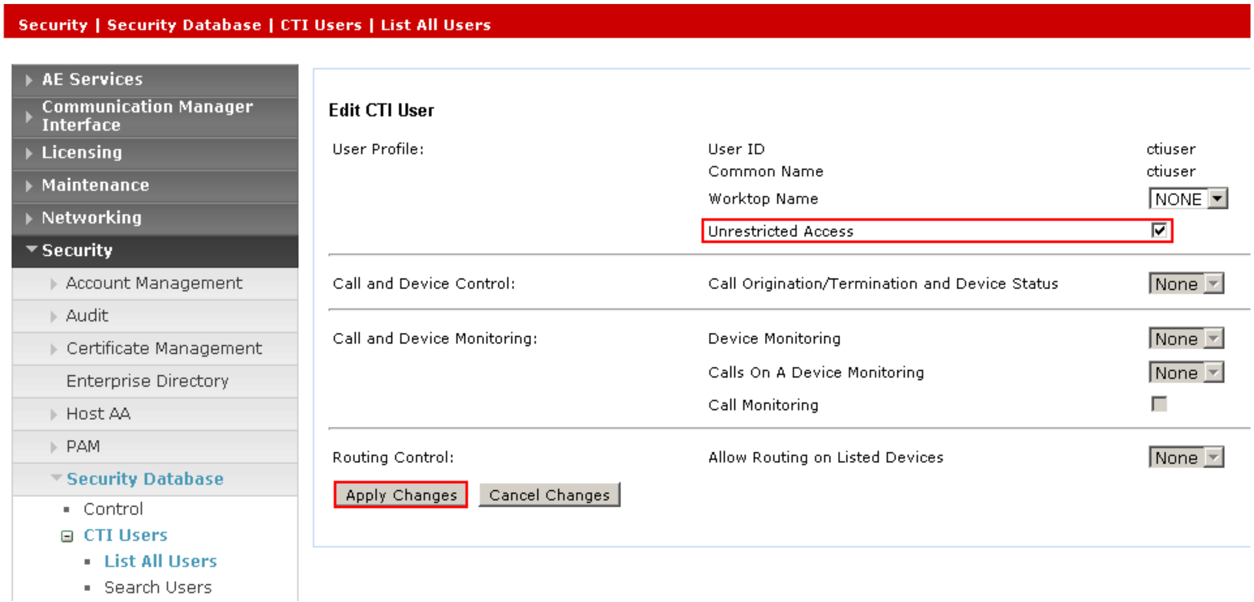
Once the user is created, navigate to the **Security → Security Database → CTI Users → List All Users** page. Select the **User ID** created previously, and click the **Edit** button to set the permission of the user.



CTI Users

User ID	Common Name
● ctiuser	ctiuser

Provide the user with unrestricted access privileges by checking the **Unrestricted Access** check box. Click the **Apply Changes** button.

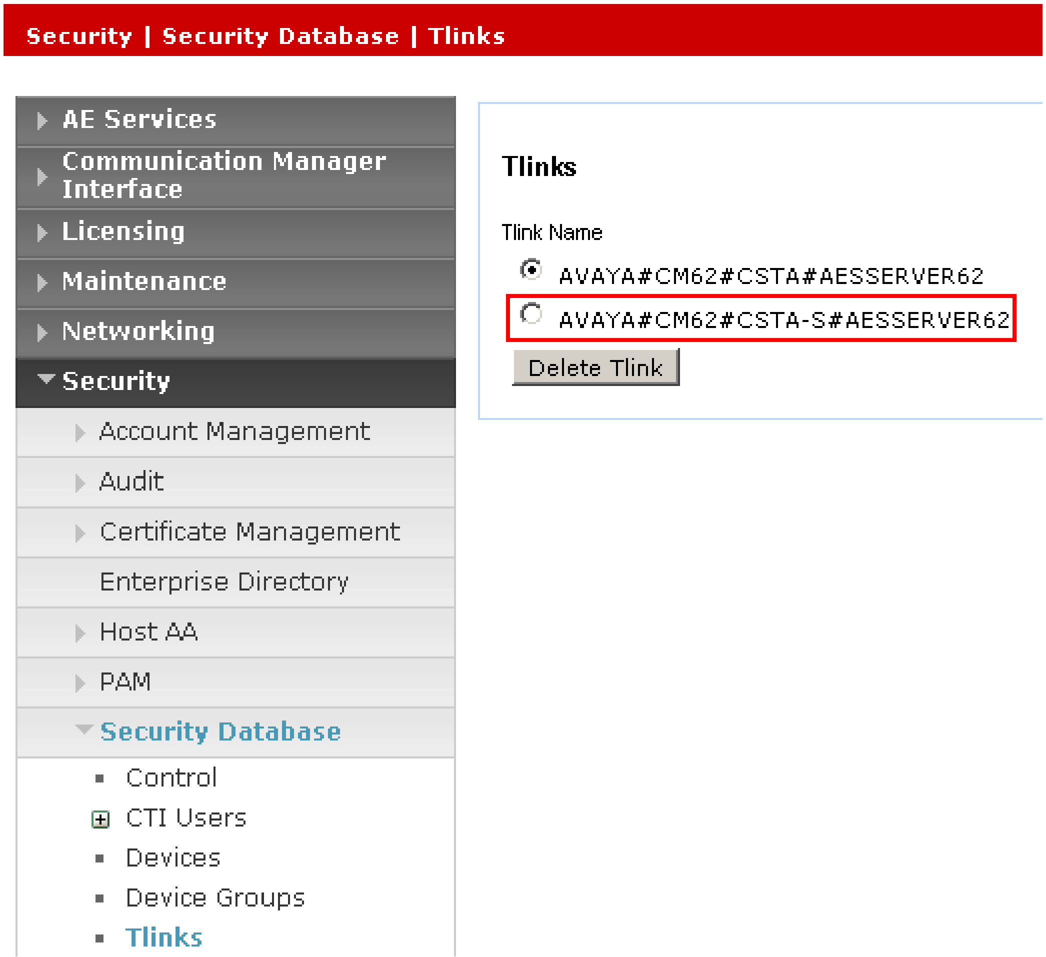


Edit CTI User

User Profile:	User ID	ctiuser
	Common Name	ctiuser
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	☐
Routing Control:	Allow Routing on Listed Devices	None

6.4. Obtain TLink Name

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



Tlinks

Tlink Name

● AVAYA#CM62#CSTA#AESSERVER62

○ AVAYA#CM62#CSTA-S#AESSERVER62

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. In this instance the IP address of the Proactive Contact server is 10.10.16.95 with a hostname of devconhd501.

Proactive Contact is installed with a preconfigured user client1 which was used by Interaction Management to log in and receive events from Event Services.

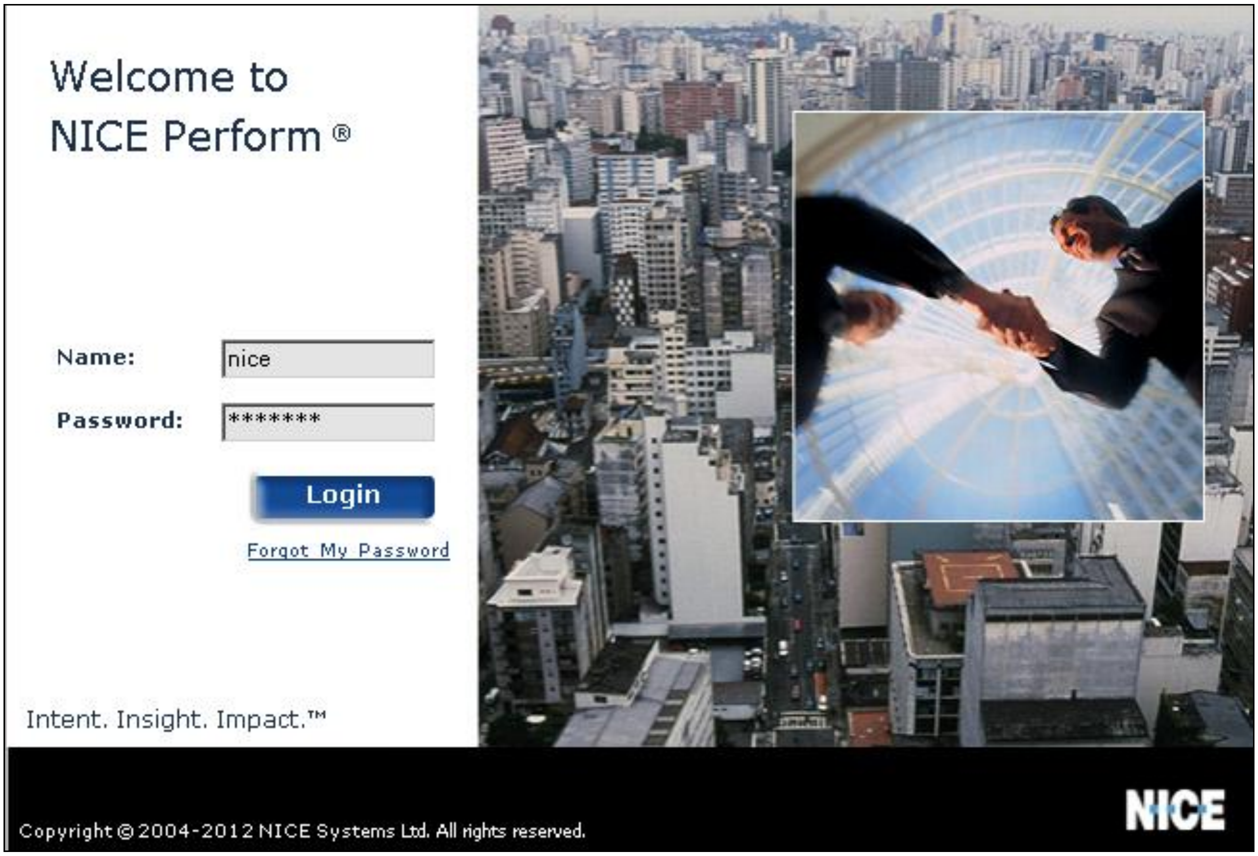
8. Configure Interaction Management

This section outlines the steps necessary to configure Interaction Management to successfully connect to the Avaya Solution outlined in **Section 3** of these Application Notes in order to record voice calls. Interaction Management logs into AES in order to send/receive CTI messages to/from Communication Manager to record voice calls using Service Observe. The Event Services API on Interaction Management allows a configured user 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 show:

- Configuration of Interaction Management to connect to AES for Service Observe based recording
- Configuration of Interaction Management to receive Proactive Contact Events
- Configuration of Interaction Management to drop “Long Call”

8.1. Configuration of Interaction Management to connect to AES for Service Observe

Open a web browser, navigate to:
http://NIM_IP_Addr/NiceApplications/Desktop/WebPage/DeskTopWebForm.aspx.
Enter the appropriate credentials and click **Login**.



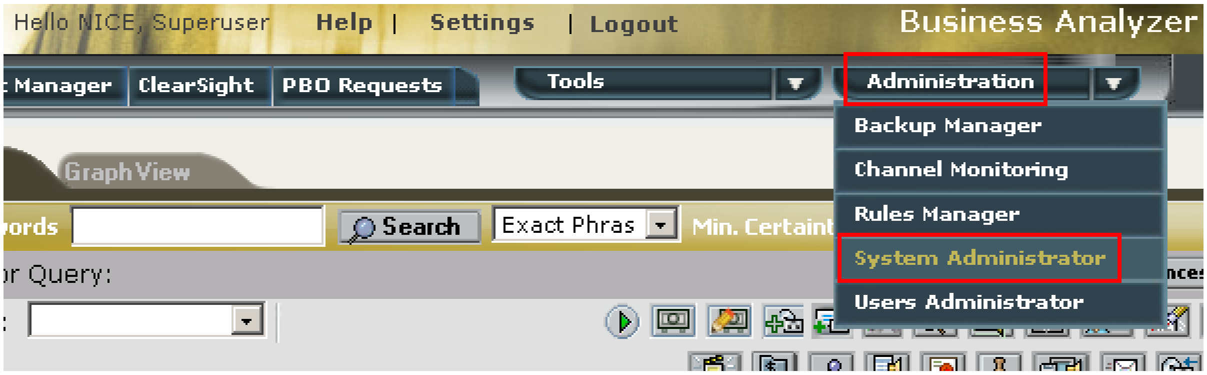
Welcome to NICE Perform ®

Name: nice

Password: *******

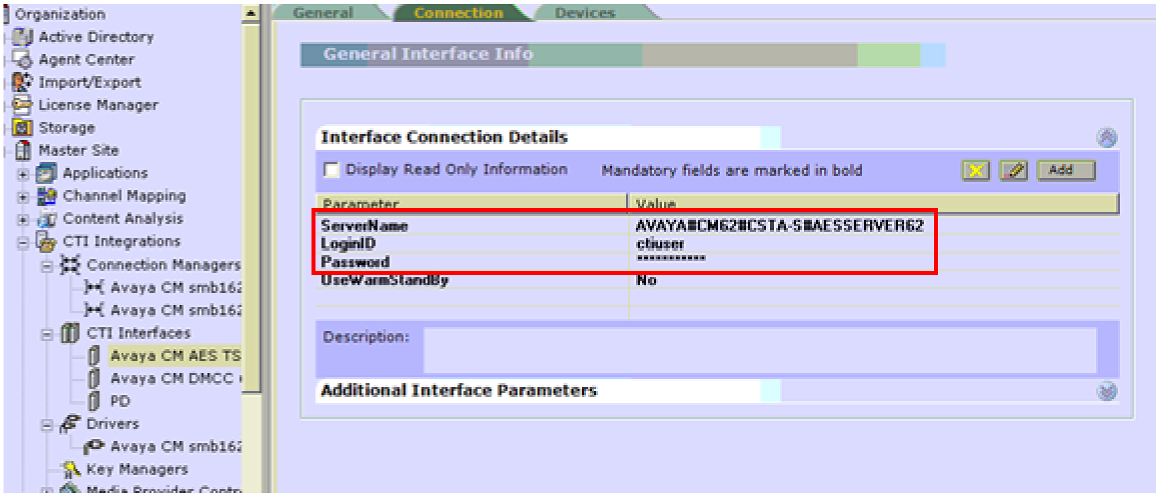
Login
Forgot My Password
Intent. Insight. Impact.™
Copyright © 2004-2012 NICE Systems Ltd. All rights reserved.
NICE

Click on **Administration → System Administration**.



Expand **Master Site → CTI Integrations → CTI Interfaces** –> **Avaya CM AES TSAPI**, click on the **Connection** tab and enter connection details as follows:

- **ServerName** – enter the TLink information from **Section 6.2**
- **LoginID** and **Password** – enter the CTI user credentials configured in **Section 6.3**

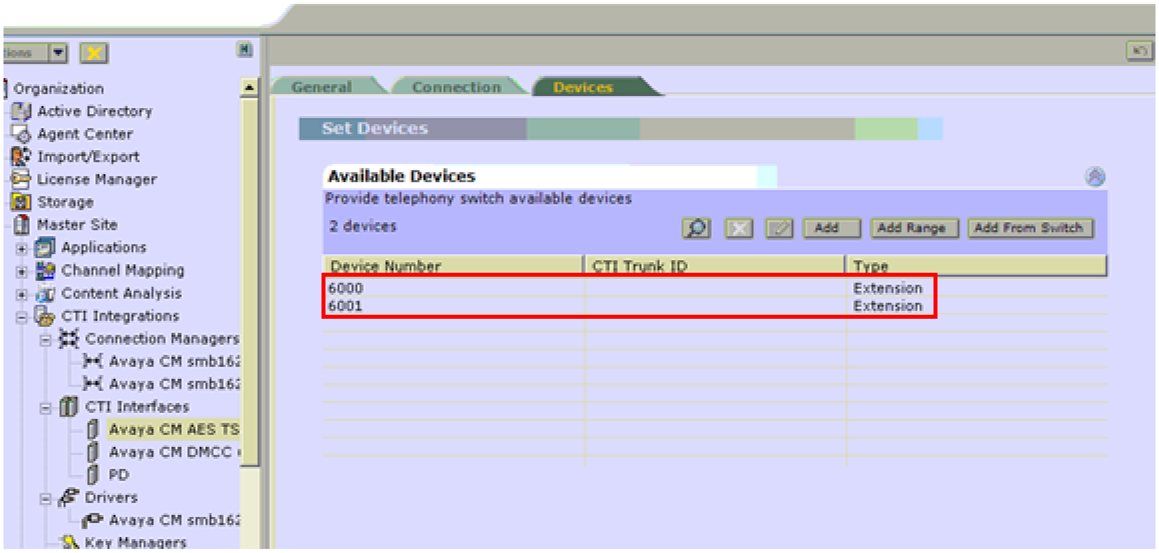


☐ Display Read Only Information Mandatory fields are marked in bold

Parameter	Value
ServerName	AVAYA#CM62#CSTA-S#AESSERVER62
LoginID	ctiuser
Password	************
UseWarmStandBy	No

Description:

Click the **Devices** tab and add the Communication Manager endpoints which are to be recorded, in this case 6000 and 6001.



Set Devices

Available Devices

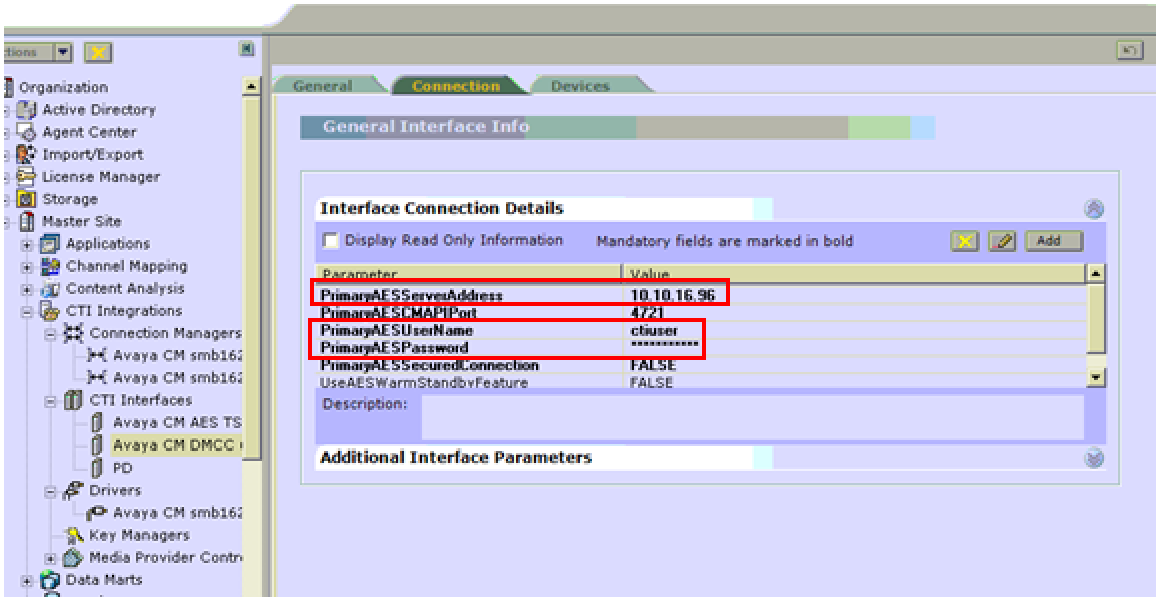
Provide telephony switch available devices

2 devices

Device Number	CTI Trunk ID	Type
6000		Extension
6001		Extension

Click on **Avaya CM DMCC** in the left pane and click on the **Connection** tab in the right pane. Enter the information as follows:

- **Primary AESServerAddress** – enter the IP address of the AES server
- **PrimaryAESUserName** and **PrimaryAESPassword** - the CTI user credentials configured in **Section 6.3**



General Interface Info

Interface Connection Details

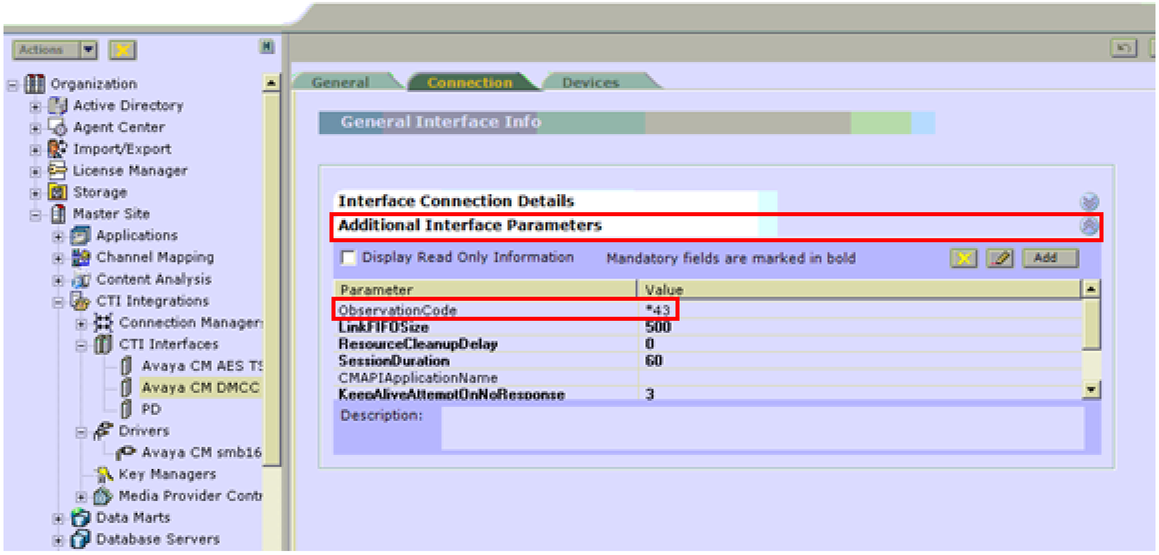
☐ Display Read Only Information   Mandatory fields are marked in bold

Parameter	Value
PrimaryAESServerAddress	10.10.16.96
PrimaryAESCMAPIPort	4721
PrimaryAESUserName	ctiuser
PrimaryAESPassword	************
PrimaryAESSecuredConnection	FALSE
UseAESWarmStandbyFeature	FALSE

Description:

Additional Interface Parameters

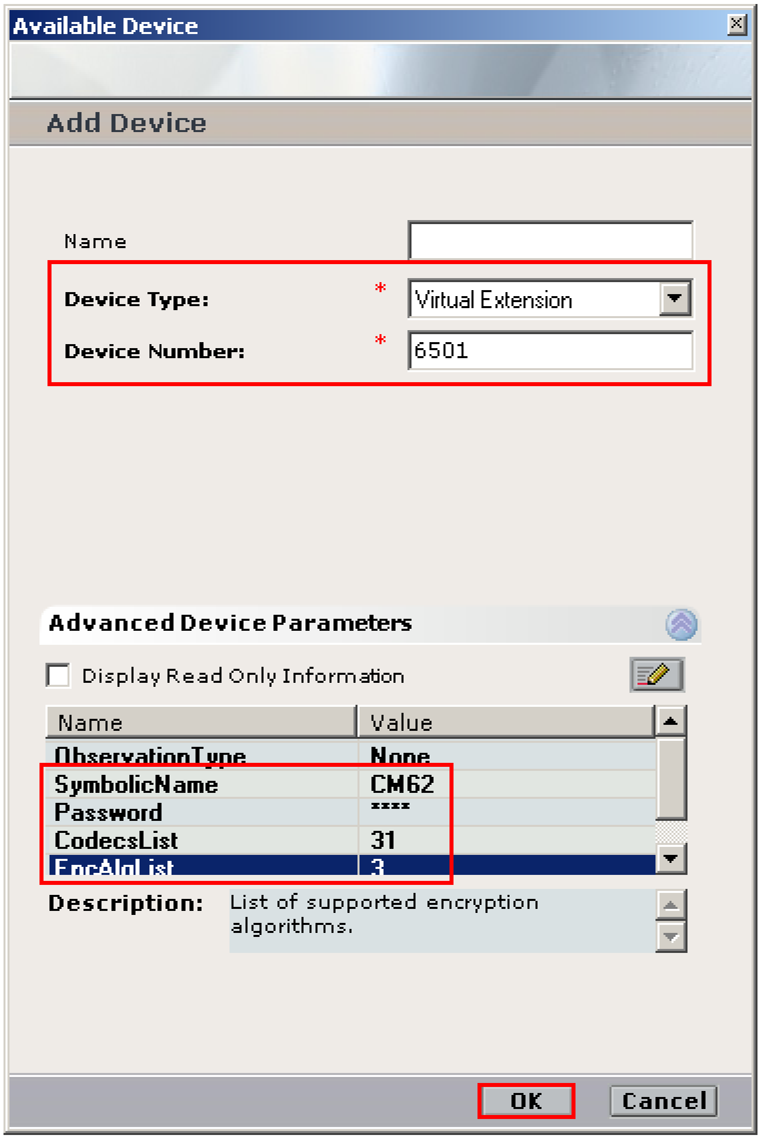
Click on **Additional Interface Parameters** and enter the **Service Observing No Talk Access Code** from **Section 5.3** next to **Observation Code**.



Parameter	Value
ObservationCode	*43
LinkFIFOSize	**500**
ResourceCleanupDelay	**0**
SessionDuration	**60**
CMAPIApplicationName	
KeepAliveAttemptOnNoResponse	**3**

Click the **Devices** tab and add the Communication Manager virtual stations which are to act as recorders as configured in **Section 5.2**, in this case 6500 and 6501 as follows:

- **Device Type** – select **Virtual Extension** from the drop down list
- **Device Number** – enter a recorder extension number from **Section 5.2**
- **Symbolic Name** – enter the Switch Connection Name from **Section 6.1**
- **Password** – enter the password assigned to the recorder extension
- **CodecsList** and **EncAlgList** – double click on each of these and place a tick in every box shown, this will populate the value field with figure shown.



Name

Device Type: * Virtual Extension

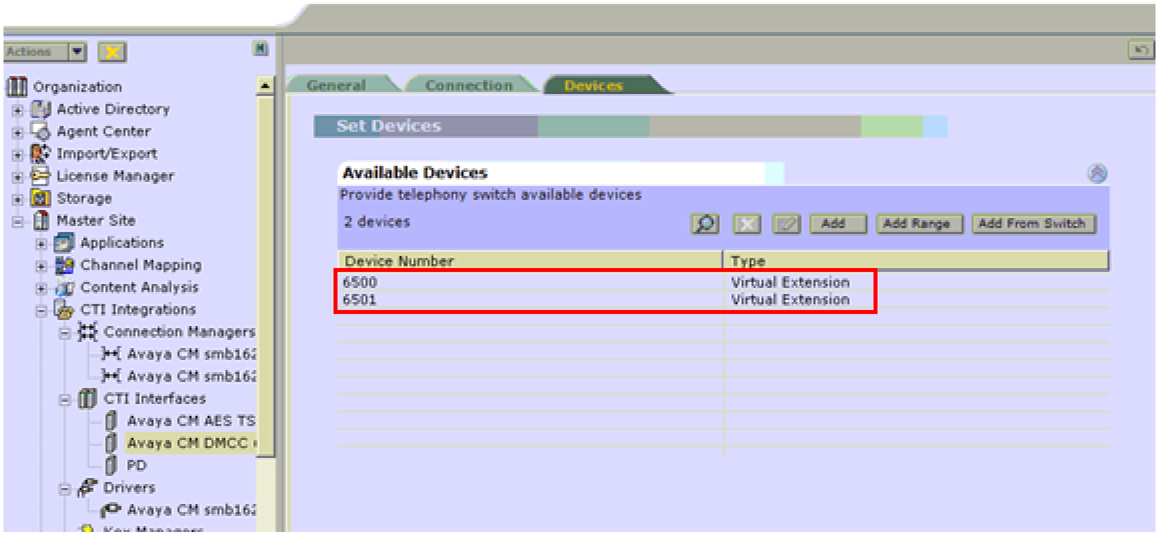
Device Number: * 6501

☐ Display Read Only Information

Name	Value
ObservationType	None
SymbolicName	CM62
Password	****
CodecsList	31
EncAlgList	3

Description: List of supported encryption algorithms.

Newly added recorder devices.



Available Devices

Provide telephony switch available devices

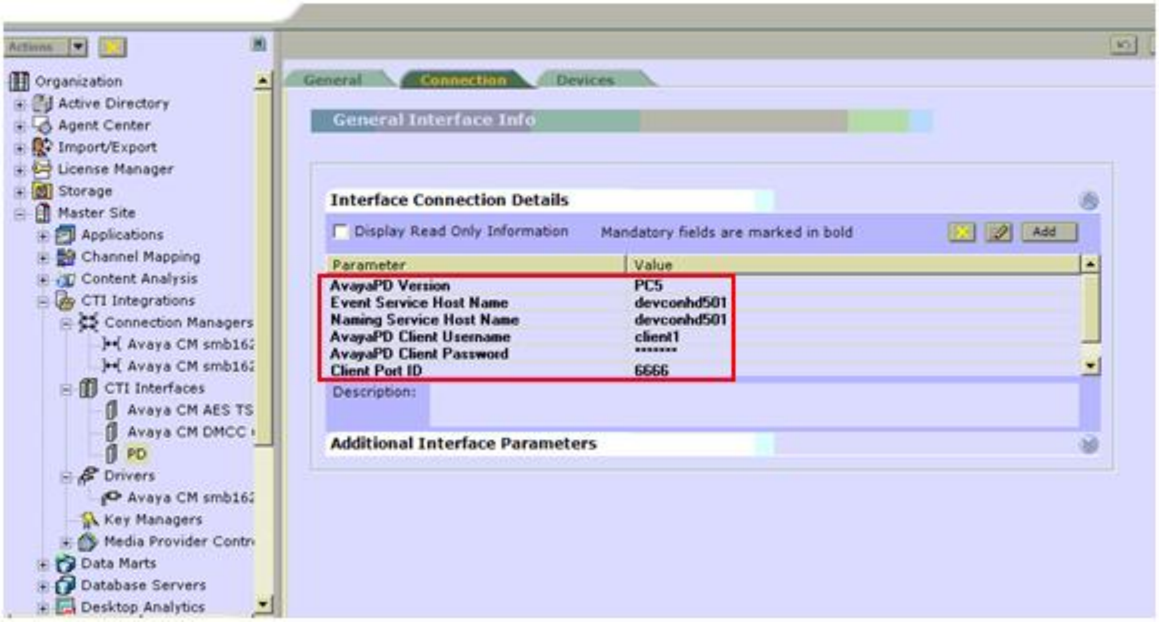
2 devices

Device Number	Type
6500	Virtual Extension
6501	Virtual Extension

8.2. Configuration of Interaction Manager to receive Proactive Contact Events

Expand **Master Site → CTI Integrations → CTI Interfaces –> PD**, click on the **Connection** tab and enter connection details as follows:

- **AvayaPD Version** – set to **PC5**
- **Event Service Host Name** and **Naming Service Host Name** – configure as the Proactive Contact hostname, in this case **devconhd501**
- **AvayaPD Client Username** and **AvayaPD Client Password** – configure as the default user of **client1** and **client1** respectively
- **Client Port ID** – set to **6666**



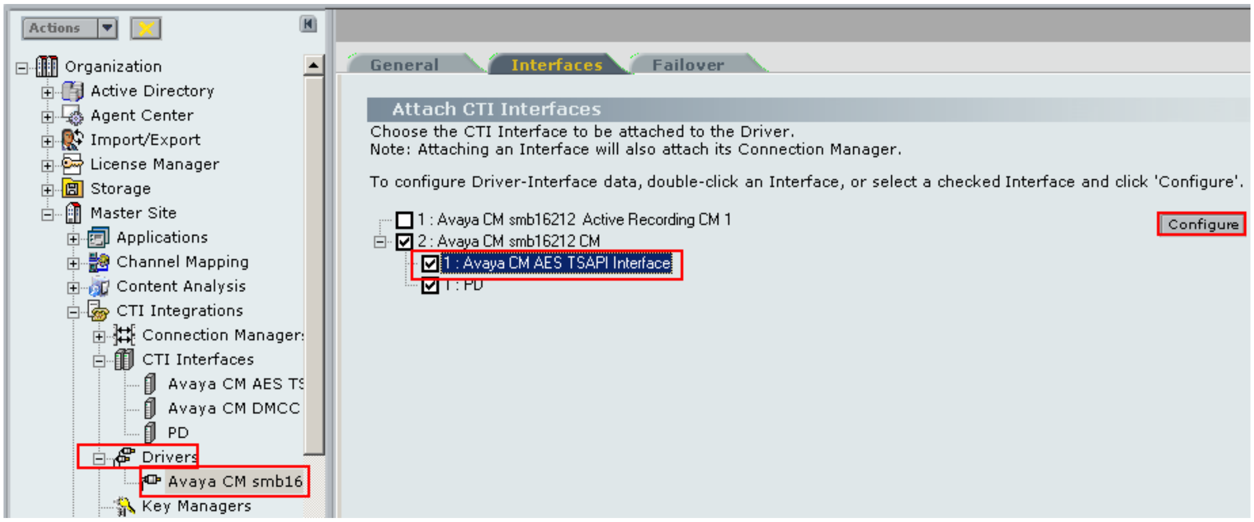
☐ Display Read Only Information   Mandatory fields are marked in bold

Parameter	Value
AvayaPD Version	PC5
Event Service Host Name	devconhd501
Naming Service Host Name	devconhd501
AvayaPD Client Username	client1
AvayaPD Client Password	*******
Client Port ID	6666

Description:

8.3. Configuration of Interaction Management to drop “Long Call”

When a Proactive Contact agent logs into Proactive Contact, an ISDN channel is dedicated and permanently active for the entire duration that the agent is logged in. This results in one constant or “long call”. In order to prevent recording this “long call” click **Master Site → CTI Integrations → Drivers.** Select the Avaya CM Driver configured, in this case Avaya CM smb16212 Driver, and click the **Interfaces** tab. Select the **Avaya CM AES TSAPI Interface** and click **Configure**.



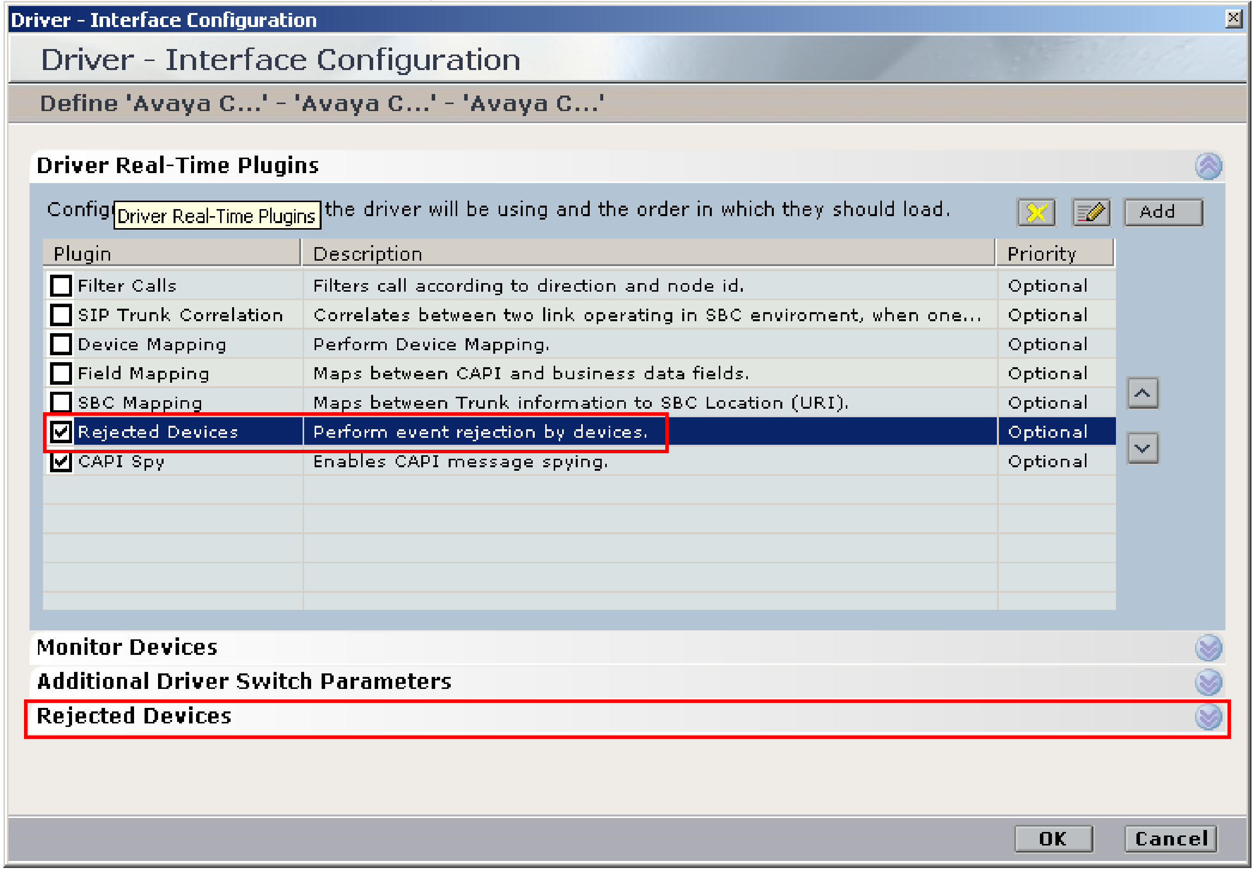
Attach CTI Interfaces

Choose the CTI Interface to be attached to the Driver.
Note: Attaching an Interface will also attach its Connection Manager.

To configure Driver-Interface data, double-click an Interface, or select a checked Interface and click 'Configure'.

- ☐ 1 : Avaya CM smb16212 Active Recording CM 1
- ☑ 2 : Avaya CM smb16212 CM
  - ☑ 1 : Avaya CM AES TSAPI Interface
  - ☑ 1 : PD

Place a tick in the box next to **Rejected Devices**.


Driver - Interface Configuration
Driver - Interface Configuration
Add
OK
Cancel

Define 'Avaya C...' - 'Avaya C...' - 'Avaya C...'

Driver Real-Time Plugins

Config Driver Real-Time Plugins the driver will be using and the order in which they should load.

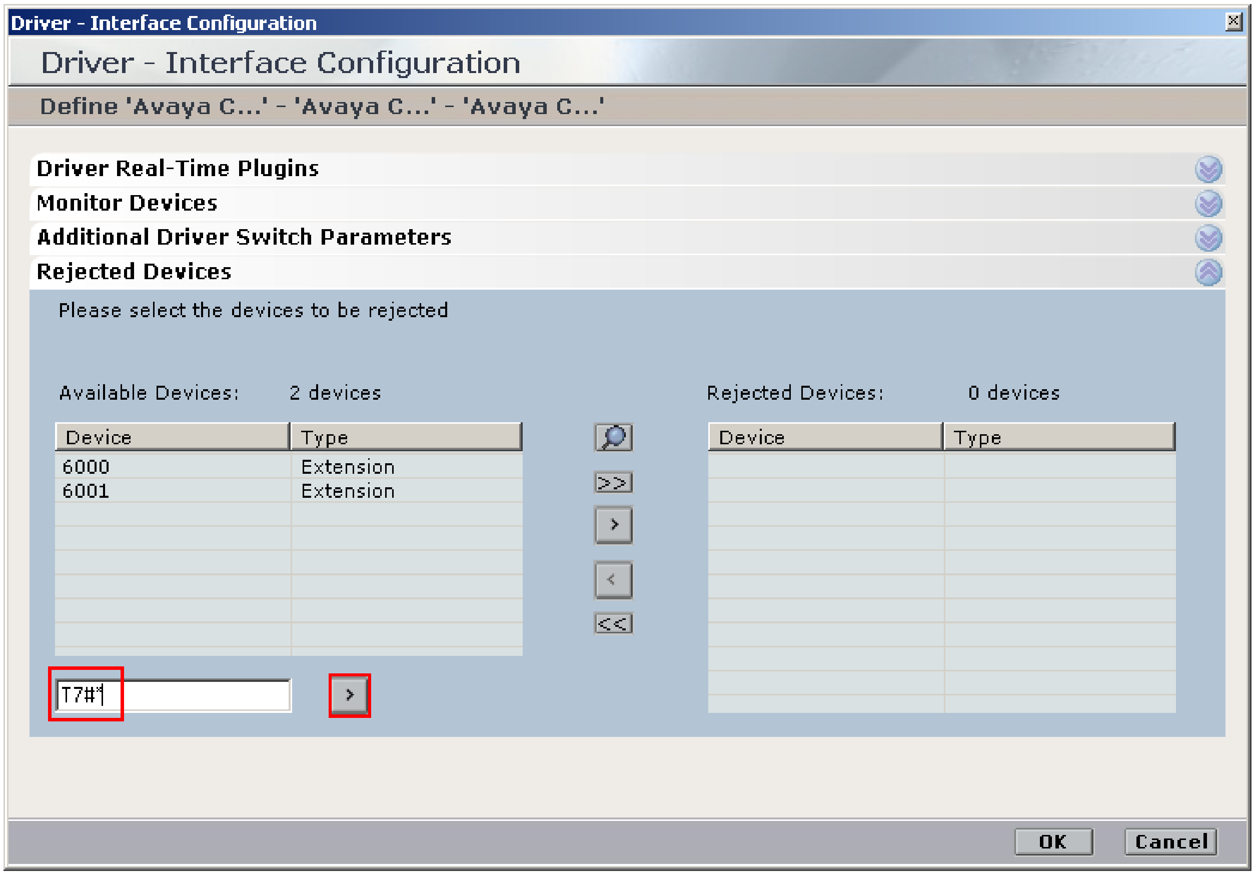
Plugin	Description	Priority
☐ Filter Calls	Filters call according to direction and node id.	Optional
☐ SIP Trunk Correlation	Correlates between two link operating in SBC enviroment, when one...	Optional
☐ Device Mapping	Perform Device Mapping.	Optional
☐ Field Mapping	Maps between CAPI and business data fields.	Optional
☐ SBC Mapping	Maps between Trunk information to SBC Location (URI).	Optional
☑ Rejected Devices	Perform event rejection by devices.	Optional
☑ CAPI Spy	Enables CAPI message spying.	Optional

Monitor Devices

Additional Driver Switch Parameters

Rejected Devices

Click **Rejected Devices** at the bottom of the screen shown above. For the purpose of the compliance test, Communication Manager was configured with trunk 7 as the Proactive Contact headset trunk group, in the field at the bottom left of the screen enter **T7#*** and click >.



Driver - Interface Configuration
Driver - Interface Configuration
Define 'Avaya C...' - 'Avaya C...' - 'Avaya C...'
Driver Real-Time Plugins
Monitor Devices
Additional Driver Switch Parameters
Rejected Devices
Please select the devices to be rejected
>>
>
<
<<
>
OK
Cancel

Available Devices: 2 devices

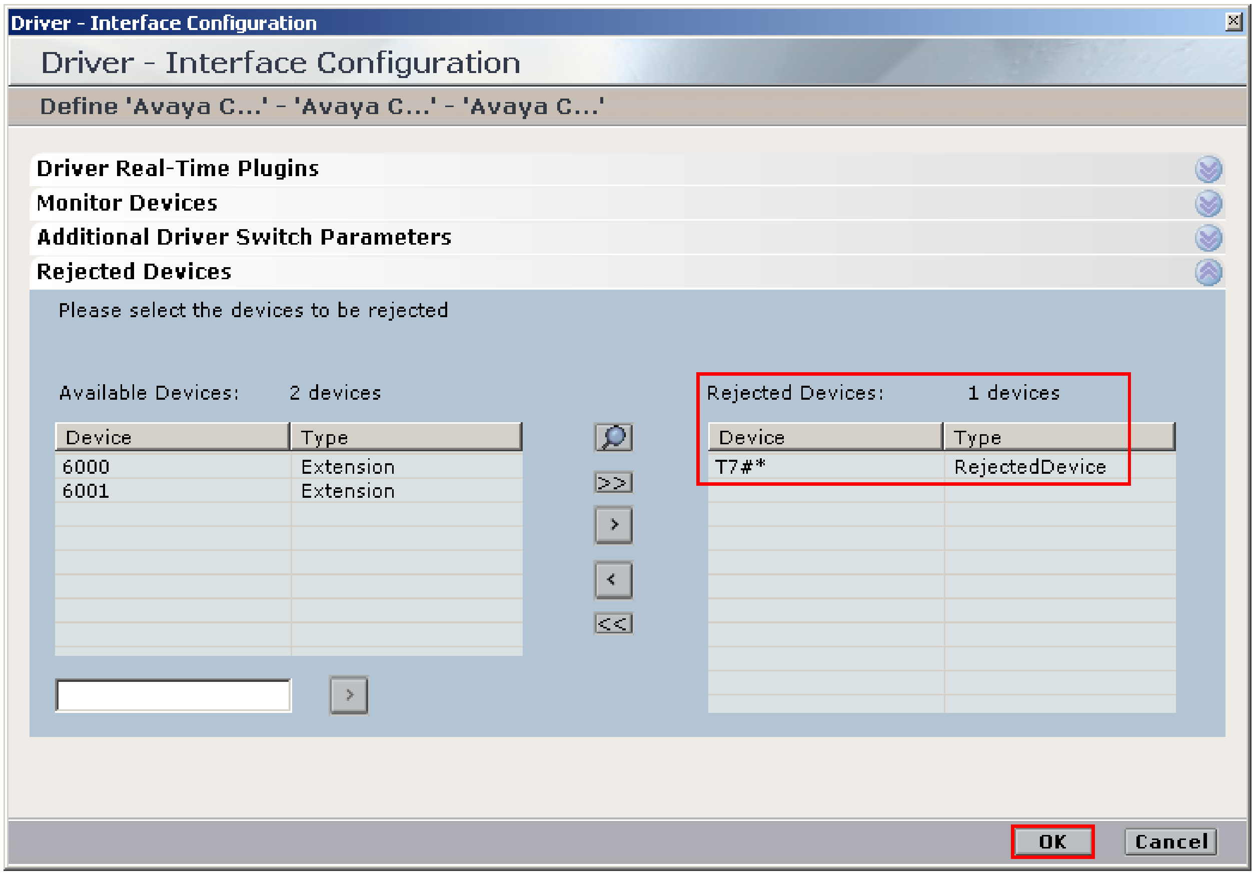
Device	Type
6000	Extension
6001	Extension

Rejected Devices: 0 devices

Device	Type

T7#*

The following screen will appear showing **T7#*** in the rejected devices area on the right of the screen. Click **OK** when done.



Driver - Interface Configuration

Define 'Avaya C...' - 'Avaya C...' - 'Avaya C...'

Driver Real-Time Plugins

Monitor Devices

Additional Driver Switch Parameters

Rejected Devices

Please select the devices to be rejected

Available Devices: 2 devices

Device	Type
6000	Extension
6001	Extension

Rejected Devices: 1 devices

Device	Type
T7#*	RejectedDevice

9. Verification Steps

The following steps can be taken to ensure that connections between Communication Manager, AES, Proactive Contact and Interaction Management are configured correctly.

9.1. Verify Avaya Aura® Communication Manager CTI link

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     4        no    aesserver62      established   18       18
```

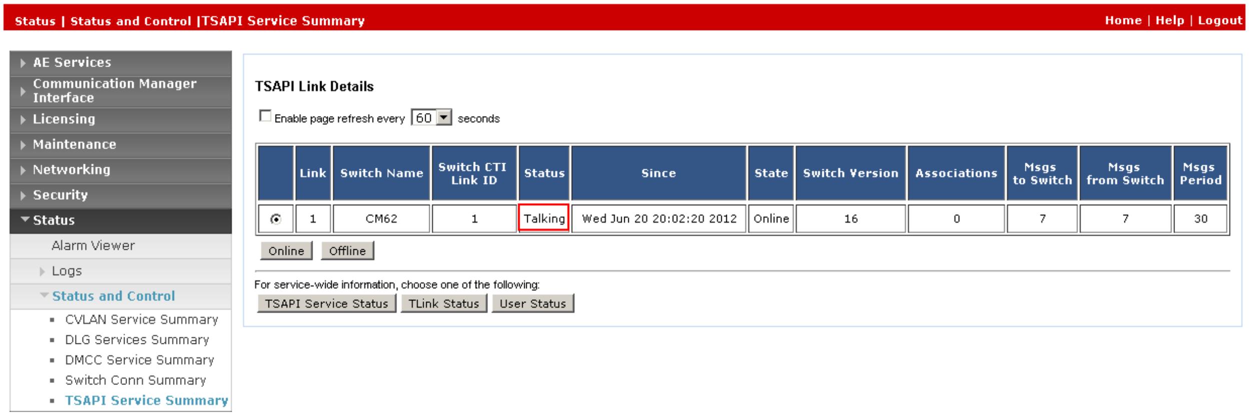
9.2. Verify Avaya Aura® Communication Manager Trunks

Verify the status of the ISDN trunks between Communication Manager and Proactive Contact. In this example, the command **status trunk-group 7** is used. Verify each channel is either **in-service/idle** or **in-service/active** in the case when an agent is logged in to Proactive Contact using a Communication Manager endpoint.

```
status trunk 7

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0007/001 001V801  in-service/idle    no
0007/002 001V802  in-service/active  no   S00006
0007/003 001V803  in-service/idle    no
0007/004 001V804  in-service/idle    no
0007/005 001V805  in-service/idle    no
```

9.3. Verify Avaya Aura® Application Enablement Services TSAPI link

From the Application Enablement Services Management Console web pages click **Status** → **Status and Control** → **TSAPI Service Summary** and verify the TSAPI Link Status is **Talking**.



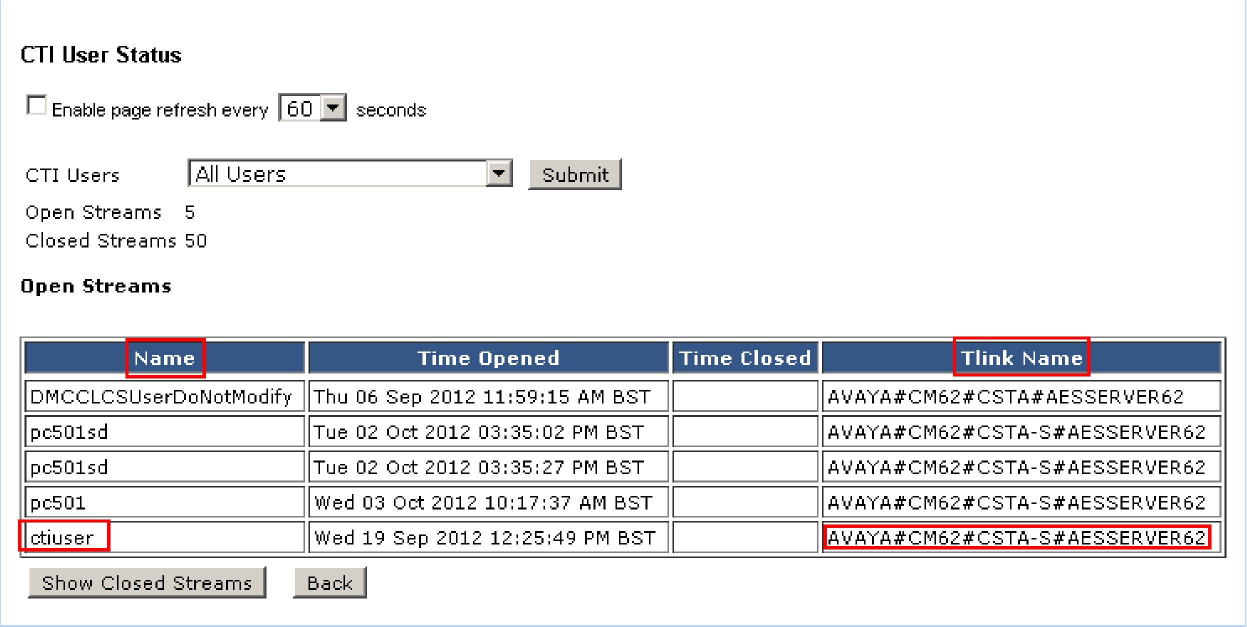
TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	CM62	1	Talking	Wed Jun 20 20:02:20 2012	Online	16	0	7	7	30

For service-wide information, choose one of the following:

Click **User Status** and verify that the configured CTI user **Name** has an active stream using the configured **Tlink Name**.



Open Streams 5
Closed Streams 50

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Thu 06 Sep 2012 11:59:15 AM BST		AVAYA#CM62#CSTA#AESSERVER62
pc501sd	Tue 02 Oct 2012 03:35:02 PM BST		AVAYA#CM62#CSTA-S#AESSERVER62
pc501sd	Tue 02 Oct 2012 03:35:27 PM BST		AVAYA#CM62#CSTA-S#AESSERVER62
pc501	Wed 03 Oct 2012 10:17:37 AM BST		AVAYA#CM62#CSTA-S#AESSERVER62
ctiuser	Wed 19 Sep 2012 12:25:49 PM BST		AVAYA#CM62#CSTA-S#AESSERVER62

9.4. 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.

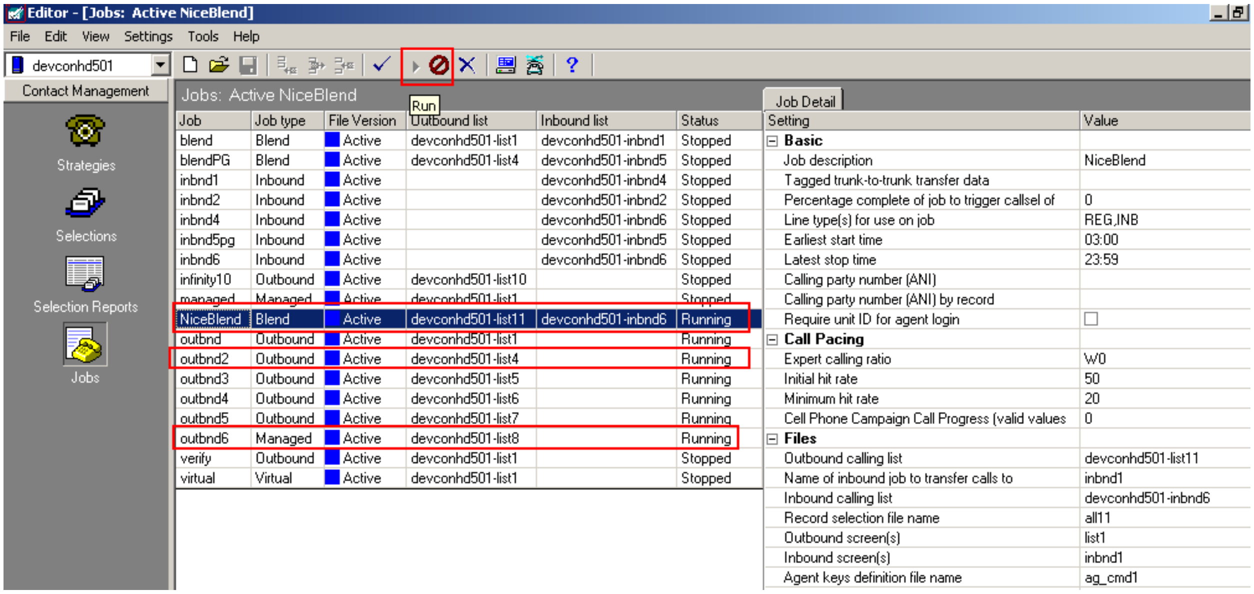
```
PC 5.0.1.328.0101 - Proactive_Contact_PATCH_328.PATCH_328 installed on 2012/09/19 at
11:03:00

========================================================================================
#  ID           Sev       Short Text                        Enabled   First Instance
Last Instance      Count  State
 ---------------------------------------------------------------------------------------
-------------------------------------------
    3  QPC000D0001  Info      Services started  - PDS           Yes       2012-10-03
10:22:20  2012-10-03 10:22:20    1  ACTIVE
    4  QPC000D0002  Info      Services started  - MTS           Yes       2012-09-19
11:04:45  2012-09-19 11:04:45    1  ACTIVE
    5  QPC000D0003  Info      Services started  - DB            Yes       2012-09-19
11:03:28  2012-09-19 11:03:28    1  ACTIVE
   15  QPC000D0013  Info      Dyanamic logging log-level modif  Yes       2012-09-04
10:53:28  2012-09-04 11:02:28    6  ACTIVE
   25  QPC000D0023  Warning   Illegal agent logoff              Yes       2011-05-24
18:48:20  2012-10-04 15:38:02  443  ACTIVE

========================================================================================
==========================================
  Found '5' ACTIVE or RETIRED alarms.

DEVCONHD501(admin)@/opt/avaya/pds [1000]
$ check_pds
```

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

```
root     24733     1  0 Oct03 ?        00:00:00 agentcount
root     25194     1  0 Oct03 ?        00:00:00 agent -d
admin    25204     1  0 Oct03 ?        00:00:00 ao_recall
admin    25200     1  0 Oct03 ?        00:00:00 recall_rmp
admin    25190     1  0 Oct03 ?        00:00:00 listserver
admin    24864     1  0 Oct03 ?        00:00:00 opmon
root     24888     1  0 Oct03 ?        00:00:00 evmon
root     24827 24814  0 Oct03 ?        00:00:03 /opt/avaya/pds/bin/enforcer -ORB
root     24786     1  0 Oct03 ?        00:00:00 bridgeSmEnf -ORBSvcConf /opt/ava
admin    24781     1  0 Oct03 ?        00:00:00 switcher
admin    24748     1  0 Oct03 ?        00:00:00 job_strter
root     24733     1  0 Oct03 ?        00:00:00 agentcount
root     24718     1  0 Oct03 ?        00:11:07 enserver -ORBSvcConf /opt/avaya/
root     25228     1  1 Oct03 ?        02:01:48 dccserver -ORBSvcConf /opt/avaya
admin    24725     1  0 Oct03 ?        00:00:54 datamgr
admin    24704     1  0 Oct03 ?        00:00:00 soe_routed
admin    24706 24704  0 Oct03 ?        00:00:00 soe_routed
root     24741     1  0 Oct03 ?        00:00:00 signalit
admin    24709     1  0 Oct03 ?        00:00:00 conn_mgr
root     25234     1  0 Oct03 ?        00:02:38 hdsc -ORBSvcConf /opt/avaya/pds/

>>> All processes running!

DEVCONHD501(admin)@/opt/avaya/pds [1001]
$
```

9.5. Verify Proactive Contact jobs are running

Before an agent is logged into a job verify that the appropriate 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 can be started and stopped using the icons highlighted in the screen shot below.

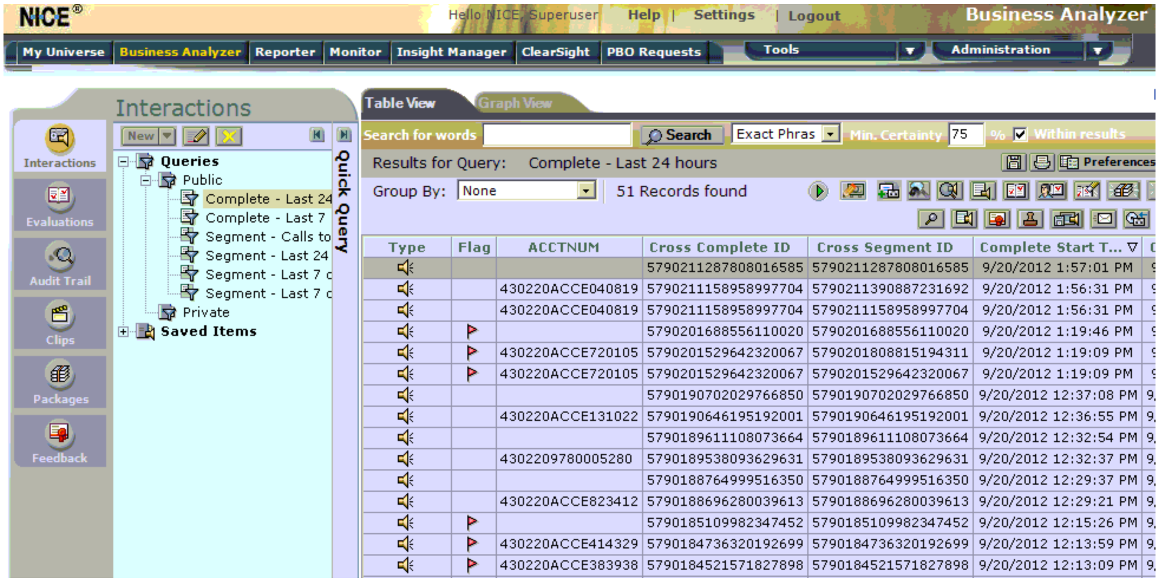


Job	Job type	File Version	Outbound list	Inbound list	Status
blend	Blend	🟦 Active	devconhd501-list1	devconhd501-inbnd1	Stopped
blendPG	Blend	🟦 Active	devconhd501-list4	devconhd501-inbnd5	Stopped
inbnd1	Inbound	🟦 Active		devconhd501-inbnd4	Stopped
inbnd2	Inbound	🟦 Active		devconhd501-inbnd2	Stopped
inbnd4	Inbound	🟦 Active		devconhd501-inbnd6	Stopped
inbnd5pg	Inbound	🟦 Active		devconhd501-inbnd5	Stopped
inbnd6	Inbound	🟦 Active		devconhd501-inbnd6	Stopped
infinity10	Outbound	🟦 Active	devconhd501-list10		Stopped
managed	Managed	🟦 Active	devconhd501-list1		Stopped
NiceBlend	Blend	🟦 Active	devconhd501-list11	devconhd501-inbnd6	Running
outbnd	Outbound	🟦 Active	devconhd501-list1		Running
outbnd2	Outbound	🟦 Active	devconhd501-list4		Running
outbnd3	Outbound	🟦 Active	devconhd501-list5		Running
outbnd4	Outbound	🟦 Active	devconhd501-list6		Running
outbnd5	Outbound	🟦 Active	devconhd501-list7		Running
outbnd6	Managed	🟦 Active	devconhd501-list8		Running
verify	Outbound	🟦 Active	devconhd501-list1		Stopped
virtual	Virtual	🟦 Active	devconhd501-list1		Stopped

Setting	Value
⊟ **Basic**	
Job description	NiceBlend
Tagged trunk-to-trunk transfer data	
Percentage complete of job to trigger callsel of	0
Line type(s) for use on job	REG,INB
Earliest start time	03:00
Latest stop time	23:59
Calling party number (ANI)	
Calling party number (ANI) by record	
Require unit ID for agent login	☐
⊟ **Call Pacing**	
Expert calling ratio	W0
Initial hit rate	50
Minimum hit rate	20
Cell Phone Campaign Call Progress (valid values	0
⊟ **Files**	
Outbound calling list	devconhd501-list11
Name of inbound job to transfer calls to	inbnd1
Inbound calling list	devconhd501-inbnd6
Record selection file name	all11
Outbound screen(s)	list1
Inbound screen(s)	inbnd1
Agent keys definition file name	ag_cmd1

9.6. Verify Interaction Management is Recording Calls

Log into the Interaction Manager web interface. Click **Business Analyser → Queries → Public → Complete – Last 24 hours** and verify recordings have been captured. Right click on the file to be listened to and use the intuitive onscreen application to playback the recording and verify audio quality. Verify associated call details accurately represents the handled call.



Results for Query: Complete - Last 24 hours

Group By: None

51 Records found

Type	Flag	ACCTNUM	Cross Complete ID	Cross Segment ID	Complete Start T...
🔈			5790211287808016585	5790211287808016585	9/20/2012 1:57:01 PM
🔈		430220ACCE040819	5790211158958997704	5790211390887231692	9/20/2012 1:56:31 PM
🔈		430220ACCE040819	5790211158958997704	5790211158958997704	9/20/2012 1:56:31 PM
🔈	⚑		5790201688556110020	5790201688556110020	9/20/2012 1:19:46 PM
🔈	⚑	430220ACCE720105	5790201529642320067	5790201808815194311	9/20/2012 1:19:09 PM
🔈	⚑	430220ACCE720105	5790201529642320067	5790201529642320067	9/20/2012 1:19:09 PM
🔈			5790190702029766850	5790190702029766850	9/20/2012 12:37:08 PM
🔈		430220ACCE131022	5790190646195192001	5790190646195192001	9/20/2012 12:36:55 PM
🔈			5790189611108073664	5790189611108073664	9/20/2012 12:32:54 PM
🔈		4302209780005280	5790189538093629631	5790189538093629631	9/20/2012 12:32:37 PM
🔈			5790188764999516350	5790188764999516350	9/20/2012 12:29:37 PM
🔈		430220ACCE823412	5790188696280039613	5790188696280039613	9/20/2012 12:29:21 PM
🔈	⚑		5790185109982347452	5790185109982347452	9/20/2012 12:15:26 PM
🔈	⚑	430220ACCE414329	5790184736320192699	5790184736320192699	9/20/2012 12:13:59 PM
🔈	⚑	430220ACCE383938	5790184521571827898	5790184521571827898	9/20/2012 12:13:09 PM

10. Conclusion

These Application Notes describe the configuration steps required for NICE Interaction Management to successfully interoperate with Avaya Proactive Contact, Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager using Service Observe. 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, Release 6.2, Issue 7.0, July 2012 Document ID 03-300509*

[2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 6.2 Issue 1, July 2012*

[3] *Implementing Avaya Proactive Contact 5.0*

All information on product installation and configuration for NICE Interaction Management can be obtained by visiting http://www.nice.com

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.