Avaya Solution & Interoperability Test Lab

Application Notes for Pindrop Fraud Detection System with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Pindrop Fraud Detection System solution to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3.

Pindrop Fraud Detection System is designed to monitor Avaya Aura® Communication Manager R6.3 via Avaya Aura® Application Enablement Services Device for detecting fraudulent calls.

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

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

1. Introduction

Pindrop Fraud Detection System (FDS) is designed to monitor Avaya Aura® Communication Manager via Avaya Aura® Application Enablement Service (AES) in a passive manner at the ingress point.

FDS needs to get certain information of calls being processed at Avaya Aura® Communication Manager, to know which audio streams to monitor in bidirectional conversations and to ascertain the moment at which call center agents are in communication with the calling party. To perform this, Pindrop has created the Avaya agent integration, which is a stand-alone component that registers with AES and monitors entities within the Avaya infrastructure to extract this information.

2. General Test Approach and Test Results

The compliance testing evaluated the ability of FDS to integrate correctly with AES and Communication Manager using a TSAPI link on AES to monitor Stations, Vector Directory Numbers (VDN) and Hunt Groups.

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

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing different call scenarios and verifying TSAPI events are received by FDS. The tests included:

- Agent Login
- Agent State Change
- Inbound calls
- Call features such as hold, transfers and conferencing
- Call termination
- TSAPI Link State Change

Additionally, serviceability testing was performed to confirm the ability for FDS to recover from common outages such as network outages and server reboots.

2.2. Test Results

All test cases passed with one exception mentioned below.

- In a scenario where the TSAPI link between Communication Manager and AES is busied out and released using "busyout cti-link" and "release cti-link" commands, FDS loses the monitoring capabilities of Stations, VDNs and Hunt Groups. FDS needs to be manually restarted in order for monitoring to recover. Pindrop may provide a fix for this in a future release.

2.3. Support

Technical support on Pindrop FDS can be obtained through the following:

- **Phone:** 1-404-692-2757
- **Web:** www.pindropsecurity.com
- **Email:** support@pindropsecurity.com

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager R6.3
- Avaya Aura® Application Enablement Services R6.3
- Various IP, Digital, and analog endpoints
- Pindrop Fraud Detection version 2.4.

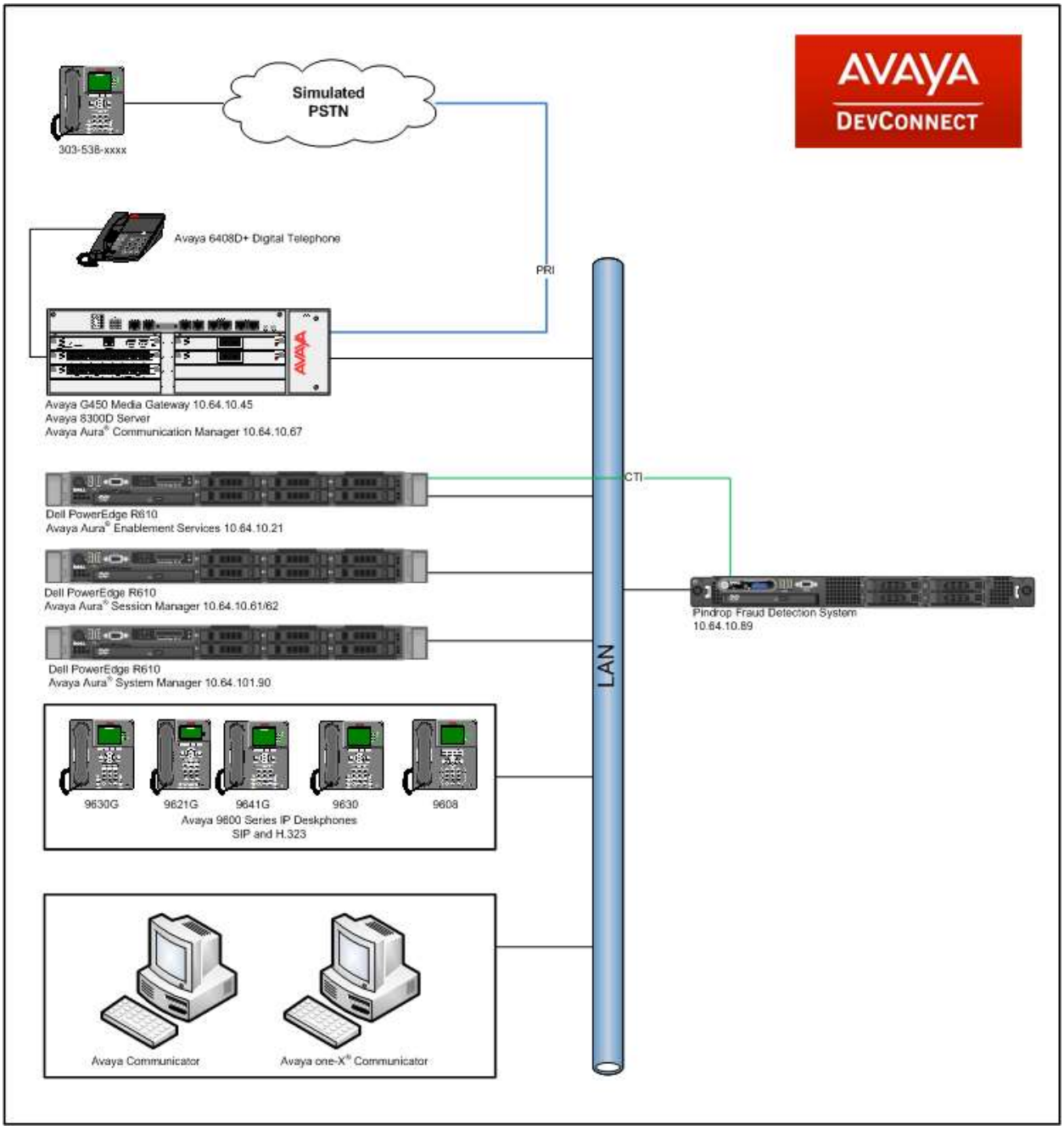


Figure 1 – Pindrop FDS Compliance Test Configuration

4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

Equipment/Software	Version
Avaya S8300D Server running Avaya Aura® Communication Manager	6.3 SP10
HP Proliant DL360 G7 Server running Avaya Aura® Session Manager	6.3.12
Dell R610 Server running Avaya Aura® System Manager	6.3.12
Avaya G450 Media Gateway • MGP • MM710AP (DS1) • MM712AP (DCP) • MM711AP (ANA)	 HW 1 FW 31.20.0 HW 04 FW 018 HW 07, FW 011 HW 27, FW 073
Dell R610 Server running Avaya Aura® Application Enablement Services	6.3.3
Avaya 9600 Series IP Telephone • 9640 (H.323)	6.3
Avaya 96x1 Series IP Telephone • 9641 (H.323)	6.3
Desktop PC running Avaya One-X® Communicator	6.4
Pindrop Fraud Detection System	2.4.0

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure Pindrop FDS successfully with Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

5.1. Verify Feature and License

Enter the **display system-parameters customer-options** command and ensure that the following features are enabled.

One Page 3, verify **Computer Telephone Adjunct Links** is set to **y.**

```
display system-parameters customer-options                    Page   3 of  11
                              OPTIONAL FEATURES

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

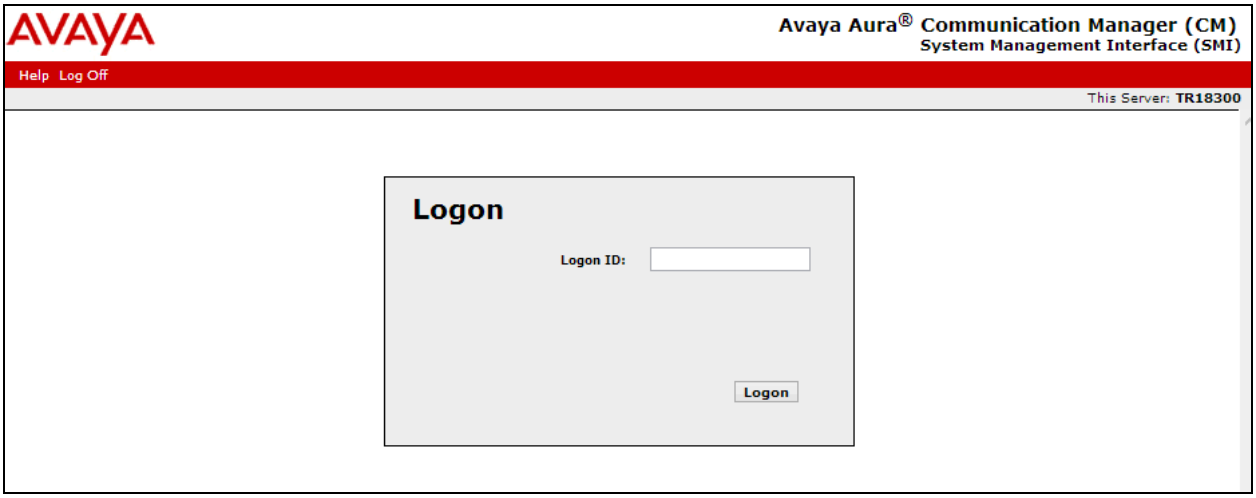
On Page 4, verify **ISDN Feature Plus, ISDN-PRI, IP Trunks** and **Multimedia IP SIP Trunking** are set to **y.**

```
display system-parameters customer-options                      Page   4 of  11
                               OPTIONAL FEATURES

   Emergency Access to Attendant? y                               IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                     ISDN Feature Plus? y
                  Enhanced EC500? y       ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                ISDN-PRI? y
              ESS Administration? y              Local Survivable Processor? n
         Extended Cvg/Fwd Admin? y                   Malicious Call Trace? y
     External Device Alarm Admin? y                Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
               Flexible Billing? n
   Forced Entry of Account Codes? y                Multifrequency Signaling? y
      Global Call Classification? y        Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y              Multimedia IP SIP Trunking? y
                       IP Trunks? y
```

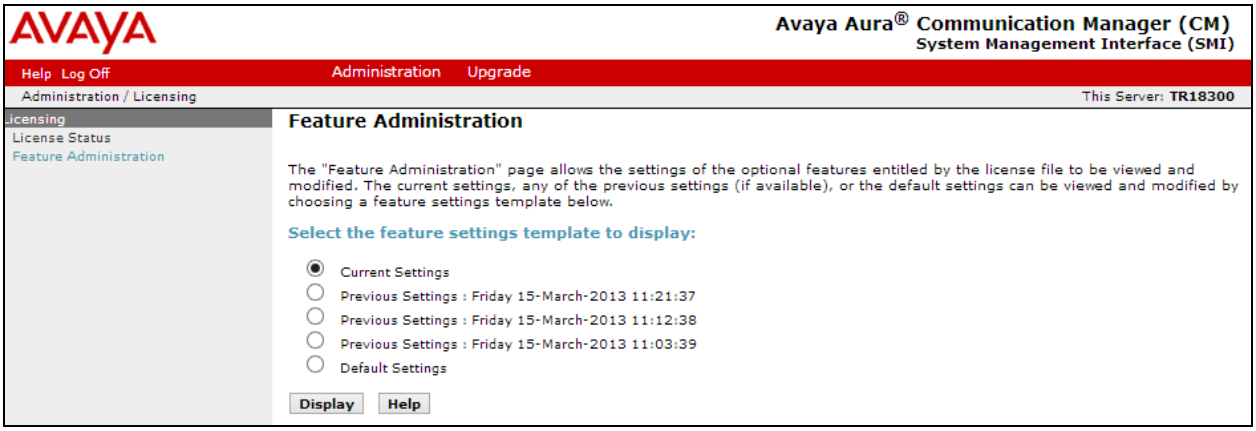
On Page 10, verify **IP_API_A** has a sufficient limit.

```
display system-parameters customer-options                      Page  10 of  11
                    MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
AgentSC     *  : 2400           0
IP_API_A    *  : 2400           6
IP_Agent    *  : 2400           0
IP_NonAgt   *  : 2400           0
IP_Phone    *  : 2400           1
IP_ROMax    *  : 2400           0
IP_Soft     *  : 2400           0
IP_Supv     *  : 2400           0
IP_eCons    *  : 68             0
oneX_Comm   *  : 2400           0
               : 0              0
           IP Attendant Consoles? y
```

From a web browser, use the http://<ip-address>, where ip-address is the ip address of Communication Manager URL to access System Management Interface for Communication Manager. Log in using appropriate credentials.



Navigate to **Administration → Licensing → Feature Administration**. Select **Current Settings** and click **Display**.



Verify **ASAI Link Core Capabilities** and **ASAI Link Plus Capabilities** are available and turned on.

8	ON OFF	ASAI Link Core Capabilities?	FEAT_ASAI	Notes
9	ON OFF	ASAI Link Plus Capabilities?	FEAT_ASAIPLUS	Notes

Verify **Vectoring** features are available and turned on as shown in the screen capture below.

72	ON OFF	Vectoring (3.0 Enhanced)?	FEAT_3EVEC	Notes
73	ON OFF	Vectoring (Best Service Routing)?	FEAT_BSR	Notes
74	ON OFF	Vectoring (Variables)?	FEAT_VAR	Notes

5.2. Configure Stations – Call Center

Add station for Call Center agents to answer calls. Use **add station *n*** command to add a station, where ***n*** is an available station extension. Configure the station as follows, on Page 1:

- In **Name** field, enter a descriptive name
- Set **Type** to the type of the telephones
- Enter a **Security Code**

```
Add station 25001                                          Page   1 of   5
                                    STATION

Extension: 25001                        Lock Messages? n               BCC: 0
     Type: 9630                         Security Code: 123456           TN: 1
     Port: IP                         Coverage Path 1: 1                COR: 1
     Name: IP Station 1               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: 25001
           Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

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

One Page 4, under **BUTTON ASSIGNMENTS**, add **call-disp, auto-in, after-call, manual-in** and **logout,** as shown below:

```
add station 25001                                          Page   4 of   5
                                    STATION
 SITE DATA
       Room: D4-H30                                      Headset? n
       Jack:                                             Speaker? y
      Cable:                                            Mounting: d
      Floor: 4                                       Cord Length: 0
   Building: D                                         Set Color:

ABBREVIATED DIALING
     List1:                     List2:                     List3:

BUTTON ASSIGNMENTS
 1: call-appr                          5: auto-in              Grp:
 2: call-appr                          6: aux-work    RC:      Grp:
 3: call-appr                          7: after-call           Grp:
 4: call-disp                          8: manual-in            Grp:

                                            Customizable Labels? y
```

5.3. Configure Hunt Group

Use **add hunt-group *n*** command to add a hunt group, where ***n*** is an available hunt group. On Page 1:

- In the **Group Name** filed, enter a descriptive name.
- Set **ACD, Queue, Vector** to **y.**
- Enter an available **Group Extension**

```
add hunt-group 10                                              Page   1 of   4
                                HUNT GROUP

            Group Number: 10                                 ACD? y
              Group Name: Skill 1                          Queue? y
         Group Extension: 11010                           Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                       MM Early Answer? n
           Security Code:                   Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

5.4. Configure Agents

User **add agent-loginID *n*** to add an agent, where ***n*** is an available agent id. On Page 1:

- In the **Name** field, type in a descriptive name
- Enter a **Security Code**

```
add agent-loginID 2501                                         Page   1 of   2
                                AGENT LOGINID

               Login ID: 2501                                    AAS? n
                   Name: IP Agent 1                            AUDIX? n
                     TN: 1                               LWC Reception: spe
                    COR: 1                       LWC Log External Calls? n
          Coverage Path:                       AUDIX Name for Messaging:
          Security Code: 1234
                                       LoginID for ISDN/SIP Display? n
                                                           Password: 123456
                                             Password (enter again): 123456
                                                         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 skill number and skill level in **SN** and **SL** fields. Skill number is the hunt group that was added in previous section.

```
add  agent-loginID 2501                                        Page   2 of   2
                                  AGENT LOGINID
      Direct Agent Skill: 1                            Service Objective? n
Call Handling Preference: skill-level                Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 10       1       16:
 2: 11       1       17:
 3:                  18:
 4:                  19:
 5:                  20:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
```

5.5. Configure Vectors

Use **change vector *n*** to configure a Vector, where ***n*** is an available Vector number. Configure a simple vector to queue the call as follows:

```
change vector 11                                                Page   1 of   6
                                  CALL VECTOR

    Number: 11               Name: Email
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing music
02 queue-to     skill 10   pri m
03
```

5.6. Configure VDN

Use **add vdn *n*** to add a vdn, where ***n*** is an available vdn extension**.** On Page 1:

- In the **Name** field, enter a descriptive name
- In the **Destination** field, set **Vector Number** to the vector configured earlier in this document. i.e., Vector Number 11.

```
change vdn 10010                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10010
                                 Name*: Pindrop VDN
                           Destination: Vector Number        11
                     Attendant Vectoring? n
                    Meet-me Conferencing? n
                      Allow VDN Override? n
                                    COR: 1
                                    TN*: 1
                               Measured: both
          Acceptable Service Level (sec): 20

          VDN of Origin Annc. Extension*:
                              1st Skill*:
                              2nd Skill*:
                              3rd Skill*:
```

Note: During compliance test 2 different VDNs were created to test a various mix of calls.

5.7. Configure AES connection

Use **change ip-services** command to add an entry for AES. On Page 1,

- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.

```
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 4 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the name obtained from the Application Enablement Services server.
- In the **Password** field, type a password to be administered on the Application Enablement Services server.
- In the **Enabled** field, type **y**.

```
change ip-services                                          Page   4 of   4
                          AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aes6_tr1          devconnect123         y        in use
      2:       AES_21_46         Interop123456         y        in use
      3:
      4:
      5:
      6:
      7:
      8:
      9:
     10:
     11:
     12:
     13:
     14:
     15:
     16:
```

5.8. Configure CTI Link

Use **add cti-link *n*** command, where ***n*** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
change cti-link 1                                              Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 6201
     Type: ADJ-IP
                                                                      COR: 1
     Name: TSAPI
```

6. Configure Avaya Aura® Application Enablement Services

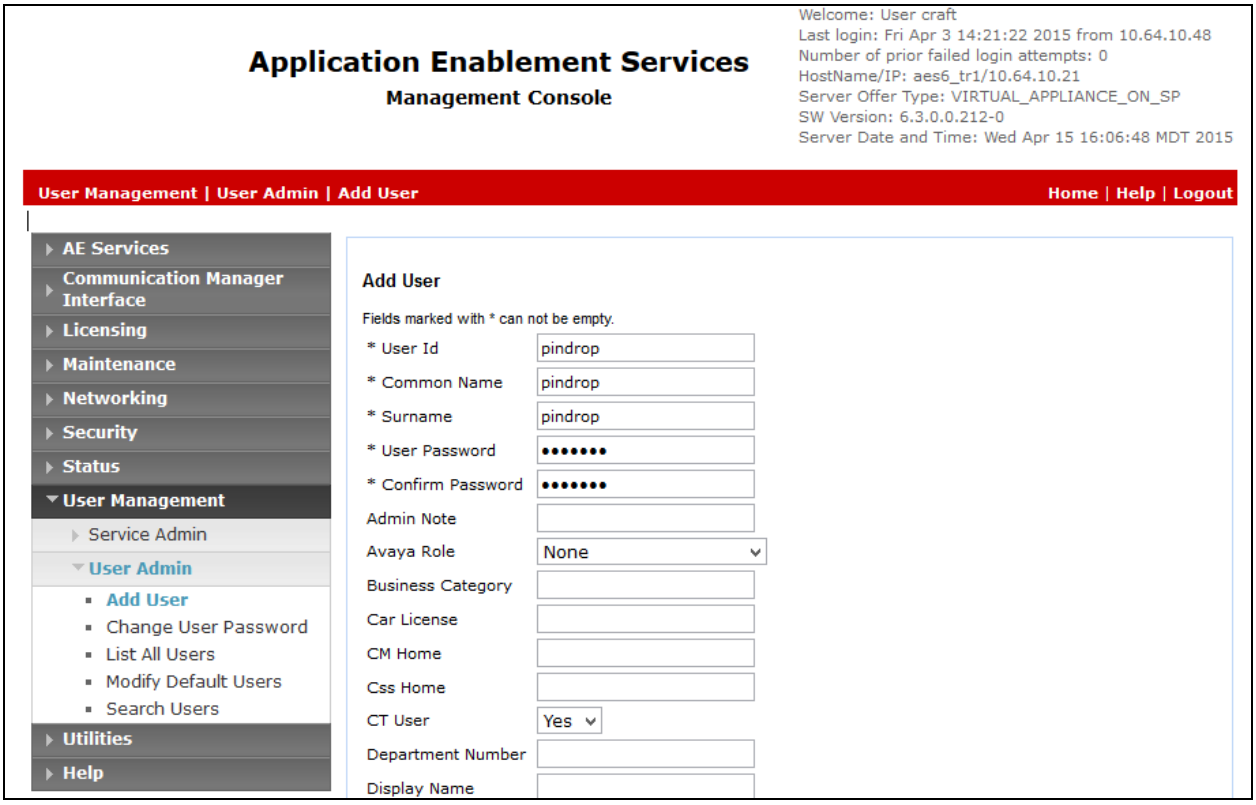
Configuration of Avaya Aura® Application Enablement Services requires a user account be configured for Pindrop FDS.

6.1. Configure User

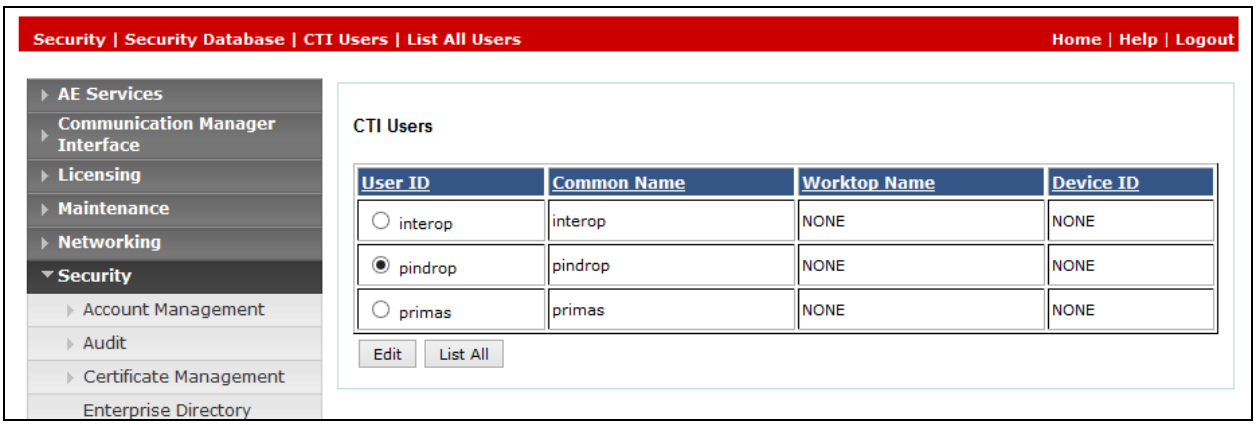
All administration is performed by web browser, https://<aes-ip-address>/

A user needs to be created for Pindrop FDS to communicate with AES. Navigate to **User Management → User Admin → Add User**.

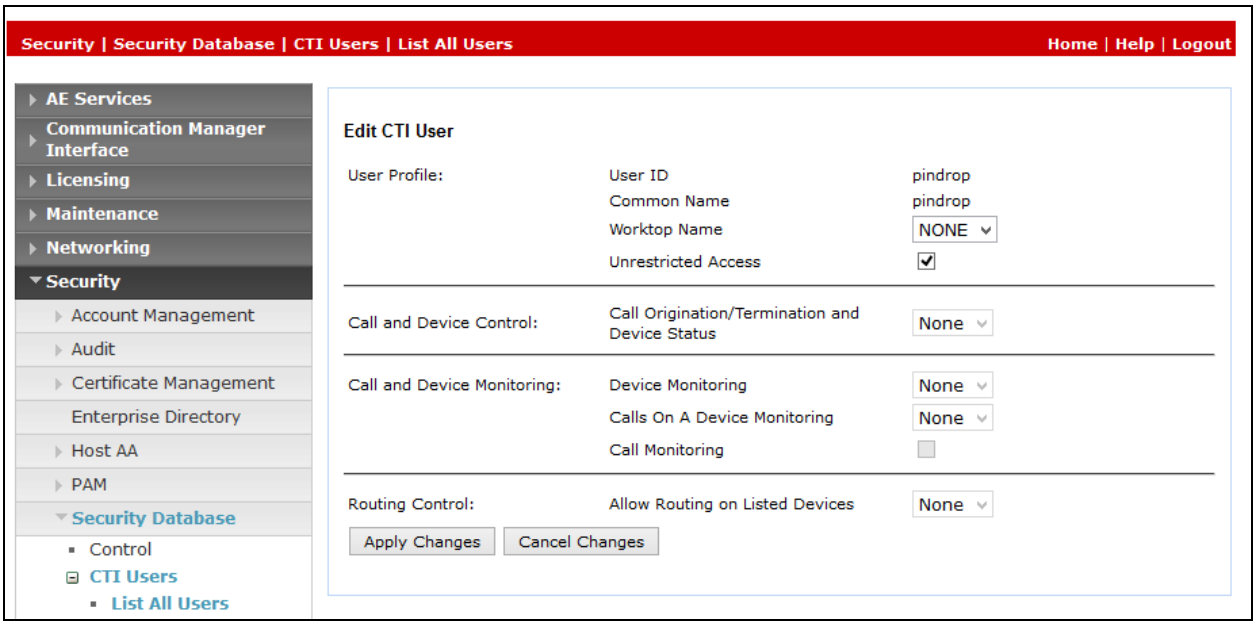
Fill in **User Id, Common Name, Surname, User Password** and **Confirm Password**. Set the **CT User** to **Yes,** and **Apply**.



Navigate to **Security → Security Database → CTI Users → List All Users**.

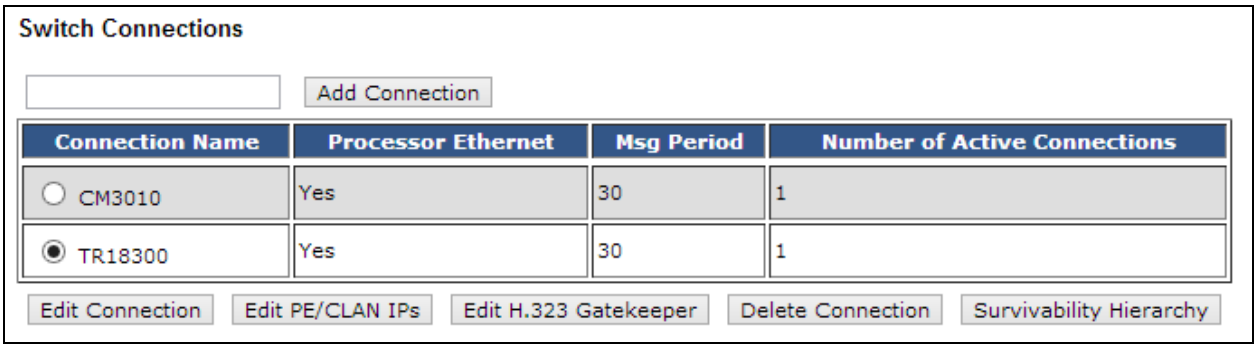


Select the recently added user and click **Edit**. Check the box for **Unrestricted Access** and click **Apply Changes**.

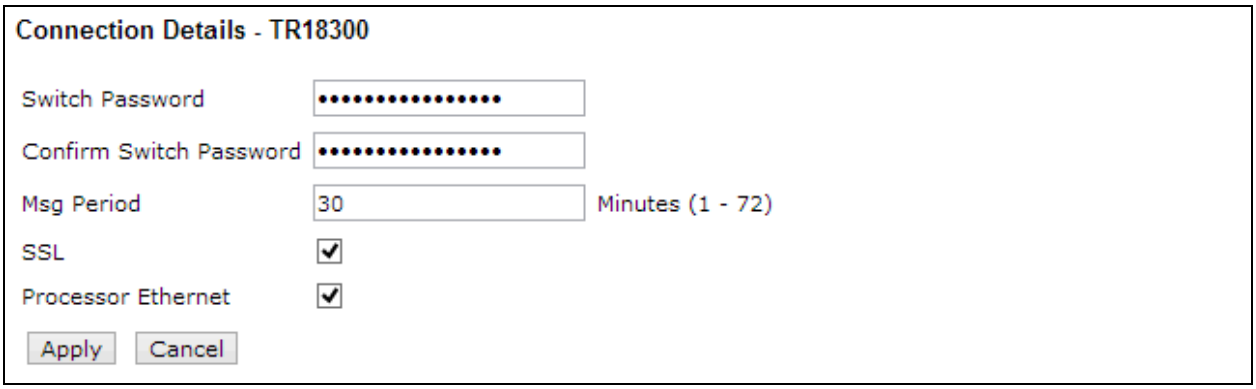


6.2. Configure Communication Manager Switch Connections

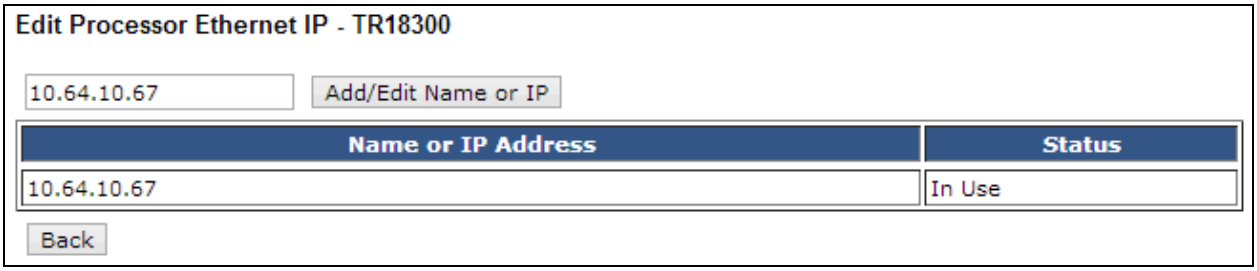
To add links to the Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as **TR18300** for this test environment:



Use the **Edit Connection** button shown above to configure the connection. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below. This must match the password configured when adding AESVCS connection in Communication Manager as seen in **Section 5.7**.



Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address.



Use the **Edit H.323 Gatekeeper** button (shown in this section's first screen capture above) to configure the **procr** or **CLAN** IP Address(es).

6.3. Configure TSAPI Link

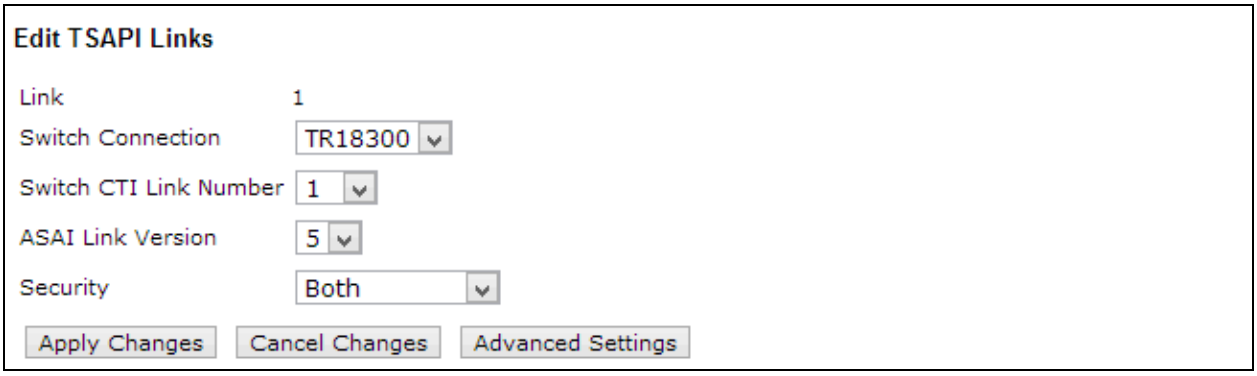
Navigate to the **AE Services → TSAPI → TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link** (not shown).

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form for Communication Manager as seen in **Section 5.8**.

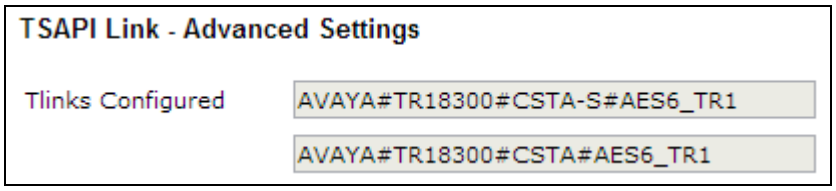
If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box.

Click **Apply Changes**.

Configuration shown below was previously configured.



Select **Advanced Settings** and note the Tlinks Configured, it will be used when configuring Pindrop FDS Application Gateway.



7. Configure Pindrop Fraud Detection System

Log on to Pindrop FDS via a SSH Client. Edit the configuration file located at /etc/pindrop/fds/avaya_agent.conf

Please note that log_level was set to full loging (0) for test but should be set to (2) for normal production.

Edit and modify the fields in bolded values in the configuration file as per the configuration in **Section 5** and **Section 6**.

```
; configuration for the Avaya Agent for TSAPI integration with
FDS

[filters]
; This setting is mutually exclusive with hunt_groups/numbers.
; extension_list=7000001,7000002-7000008
extension_list=25001, 25002, 25551, 25552, 25101, 25151
; This should always have a value.
vdn_list=10010, 10011

[hunt_groups]
; This setting is mutually exclusive with filters/extension_list
numbers=1,49000
; Hunt group events outside this range are ignored.

extension_ranges=11001-11002

; At start time, the service queries for a list of currently
logged-in agents.
; Afterwards, it monitors login/logout events to keep the list
up to date. There
; is a concern that some of these login/logout events could be
missed. To
; address this concern, the service will periodically re-query
the full list
; of logged-in agents.

requery_all_logged_in_agents_seconds=3600

[agent]
idle_sleep_microseconds=100000
; 0-trace, 1-debug, 2-info, 3-warning, 4-error, 5-fatal
log_level=2
aes_username=pindrop
aes_password=pindrop
aes_servicename=AVAYA#TR18300#CSTA#AES6_TR1
```

```
[broker]
; The URL of the pcap_broker which will receive TSAPI events
zmqurl=tcp://192.168.0.197:7004/

[watchdog]
; default values are fine here
heartbeat_url=
poll_interval_sec=
deadtime_sec=
queue_full_ratio=<%= @avaya_agent['queue_full_ratio_percent']

[event]
reopen_interval_seconds=60

[heartbeat]
heartbeat_url=ipc:///tmp/avaya_agent_heartbeat.ipc
poll_interval_sec=5
deadtime_sec=3600
queue_full_ratio=95
ipc_socket_timeout_ms=5000
```

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that the interface on Communication Manager to AES is enabled and in **listening** status (use the **status aesvcs interface** command on the Communication Manager SAT).
- Verify that the link between Communication Manager and Application Enablement Services is transmitting and receiving messages (use the **status aesvcs link** command on the SAT).
- Verify that the **con state** of the Switch Connection is **talking** (on Application Enablement Services web page, navigate to **Status → Status and Control → Switch Conn Summary**).
- Verify that the **service state** of the CTI link is **established** (use the **status aesvcs cti-link** command on the SAT).
- Verify the Pindrop FDS has successfully monitored the agent stations using TSAPI (use the **list monitored-stations** command on the SAT).

9. Conclusion

These Application Notes describe the procedures for configuring Pindrop FDS to monitor Stations, VDNs and Hunt Groups on Avaya Aura® Communication Manager. In the configuration described in these Application Notes, Pindrop FDS uses the TSAPI link to Avaya Aura® Application Enablement Services to perform monitoring.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 10, June 2014, Document Number 03-300509.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014

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.