Avaya Solution & Interoperability Test Lab

Application Notes for eLoyalty Behavioral Analytics™ with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for eLoyalty Behavioral Analytics™ to interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES).

eLoyalty Behavioral Analytics is an analytical tool that transforms the unstructured conversations of customer interactions into structured, actionable data that drives informed decision making and business actions. The Call Capture Service is a part of eLoyalty Behavioral Analytics that performs the recording solution.

The Call Capture Service utilizes the Device, Media and Call Control (DMCC) service of Avaya AES to register DMCC softphones that the Call Capture Service uses as recording ports. When recording of audio is desired, the Call Capture Service issues a Single Step Conference request through Avaya AES to bridge a DMCC softphone onto the call.

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

eLoyalty Behavioral Analytics is an analytical tool that transforms the unstructured conversations of customer interactions into structured, actionable data that drives informed decision making and business actions. The Call Capture Service is a part of eLoyalty Behavioral Analytics that performs the recording solution.

The Call Capture Service utilizes the Device, Media and Call Control (DMCC) service of Avaya AES to register DMCC softphones that the Call Capture Service uses as recording ports. When recording of audio is desired, the Call Capture Service issues a Single Step Conference request through Avaya AES to bridge a DMCC softphone onto the call.

The overall objective of this testing was to verify the Call Capture Service can interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES). Serviceability and performance testing were also conducted to assess the reliability of the solution.

Figure 1 provides the test configuration used for the compliance testing.

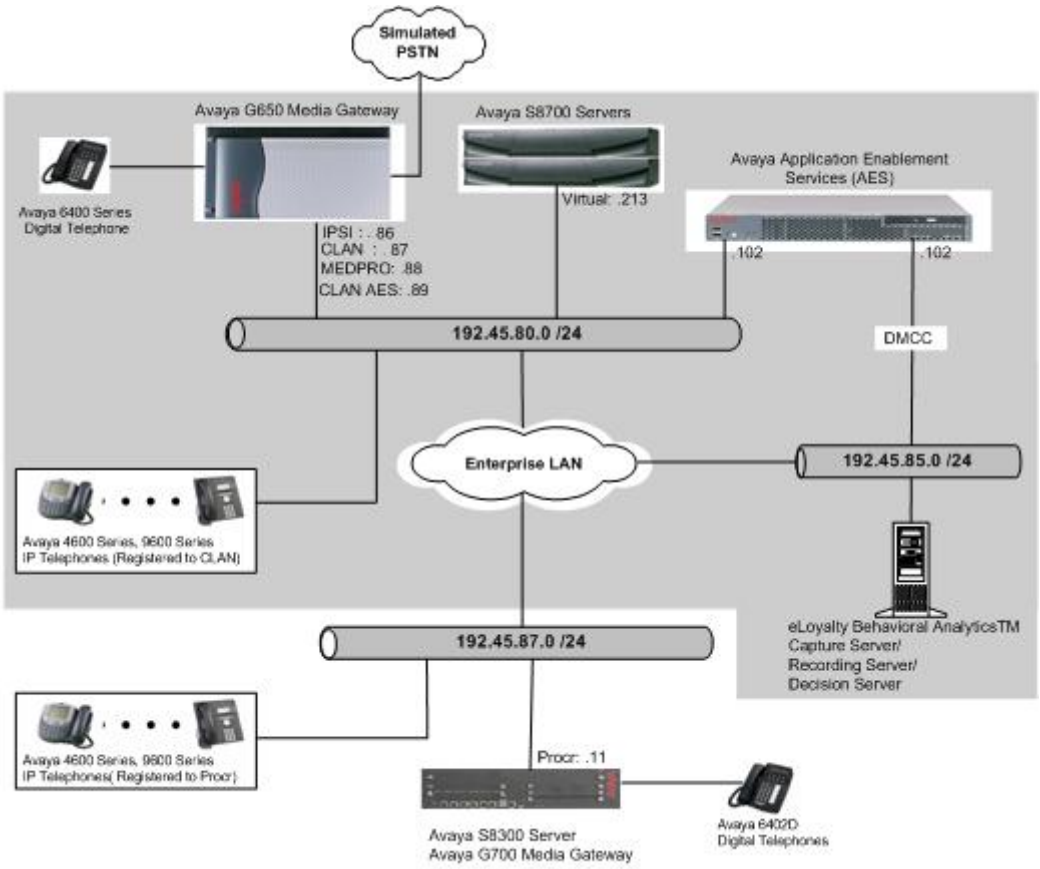


Figure 1: Test Configuration for eLoyalty Behavioral Analytics™ with Avaya Communication Manager and Avaya AES

2. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8700 Servers		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2 with patch 14300)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface TN799DP CLAN Interface TN2302AP IP Media Processor	HW11 FW030 HW01 FW017 HW20 FW108
Avaya S8300 Server		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2 with patch 14300)
Avaya G700 Media Gateway		25.28.0
Avaya Application Enablement Services		4.0 w/ Bundled Offer Build 47.3
Avaya 4600 Series IP Telephones		
	4620 (H.323) 4625 (H.323)	2.8 2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323) 9650 (H.323)	1.5 1.5
Avaya 6400D Series Digital Telephones		-
eLoyalty Behavioral Analytics™		2.1.0.4

3. Configure Avaya Communication Manager

This section provides the procedures for configuring the recording ports and recording stations, recorded stations, an IP codec set, IP network region, and IP Services on Avaya Communication Manager. All the configuration steps are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance testing. For the compliance testing, the following devices were used.

Device Type	Device Number/Extension
Recorded stations (IP Telephones)	IP Telephones: 22001, 22002, 22003 DCP Telephone: 22007 IP Agent: 22009
Recording stations (DMCC stations)	23001 - 23023

3.1. Recording Ports

The recording ports in this configuration are Avaya AES DMCC stations that appear as IP Softphones to Avaya Communication Manager. Each DMCC station requires an IP_API_A license. In the DMCC environment, the IP_API_A license is required for both the recorded and the recording stations.

Enter the **display system-parameters customer-options** command and verify that there are sufficient **IP_API_A** licenses. If not, contact an authorized Avaya account representative to obtain these licenses.

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

Product ID  Rel. Limit          Used
IP_API_A       : 200            0
IP_API_B       : 0              0
IP_API_C       : 0              0
IP_Agent       : 50             0
IP_IR_A        : 0              0
IP_Phone       : 12000          3
IP_ROMax       : 12000          0
IP_Soft        : 2              0
IP_eCons       : 0              0
               : 0              0
               : 0              0

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

Enter the **add station <s>** command, where <**s**> is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, set the Port field to **ip**, enter a descriptive Name, specify a Security Code, and set the IP SoftPhone field to **y**.

Repeat this step as necessary, with the same Security Code, to configure additional DMCC stations.

```
add station 23001                                             Page   1 of   5
                                    STATION

Extension: 23001                        Lock Messages? n              BCC: 0
     Type: 4620                         Security Code: 1234            TN: 1
     Port: ip                      Coverage Path 1:                   COR: 1
     Name: DMCC-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: 23001
           Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english               Expansion Module? n
 Survivable GK Node Name:
         Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? y

                                         IP Video Softphone? n

                                        Customizable Labels? y
```

3.2. Recorded Stations

The stations that were recorded during the compliance testing include an Avaya Digital Telephone, Avaya IP Telephones (Avaya 4600 and 9600 Series), and an Avaya IP Agent. The extensions used were in the range 22001-22009.

Enter the **add station <s>** command, where <**s**> is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to the appropriate IP telephone set type (if the station is an Avaya IP telephone), set the Port field to **ip**, enter a descriptive Name, specify a Security Code, and set the IP SoftPhone field to **y**.

```
add station 22001                                          Page   1 of   5
                                    STATION

Extension: 22001                       Lock Messages? n               BCC: 0
     Type: 4620                        Security Code: 1234             TN: 1
     Port: ip                        Coverage Path 1:                 COR: 1
     Name: 22001                     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: 22001
           Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english               Expansion Module? n
 Survivable GK Node Name:
         Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? y

                                              IP Video Softphone? n


                                         Customizable Labels? y
```

3.3. Codec Configuration

Enter the **change ip-codec-set <t>** command, where **<t>** is a number between 1 and 7, inclusive, and represents an unused IP codec set. Enter a list of audio codecs to be used, and their related parameters. For the compliance testing, G.711MU was used.

```
change ip-codec-set 1                                      Page   1 of   2

                         IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2:
 3:
 4:
     Media Encryption
 1: none
 2:
```

3.4. IP Network Regions

This section describes the steps for administering an IP network region in Avaya Communication Manager. Enter the **change ip-network-region <n>** command, where <**n**> is a number between **1** and **250** inclusive, and represents an available IP network region. For Codec Set, enter the IP codec set number provisioned in **Section 3.3**.

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3028
DIFFSERV/TOS PARAMETERS                RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

3.5. Configure IP-Services

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

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
MEDPRO                 192.45.80.88
S8300G700              192.45.87.11
default                0.0.0.0
CLAN                   192.45.80.87
CLAN-AES               192.45.80.89
```

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form. 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       CLAN-AES        8765
```

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

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:        server1          xxxxxxxxxxxxxxxx      y        idle
      2:
      3:
```

4. Configure Avaya Application Enablement Services

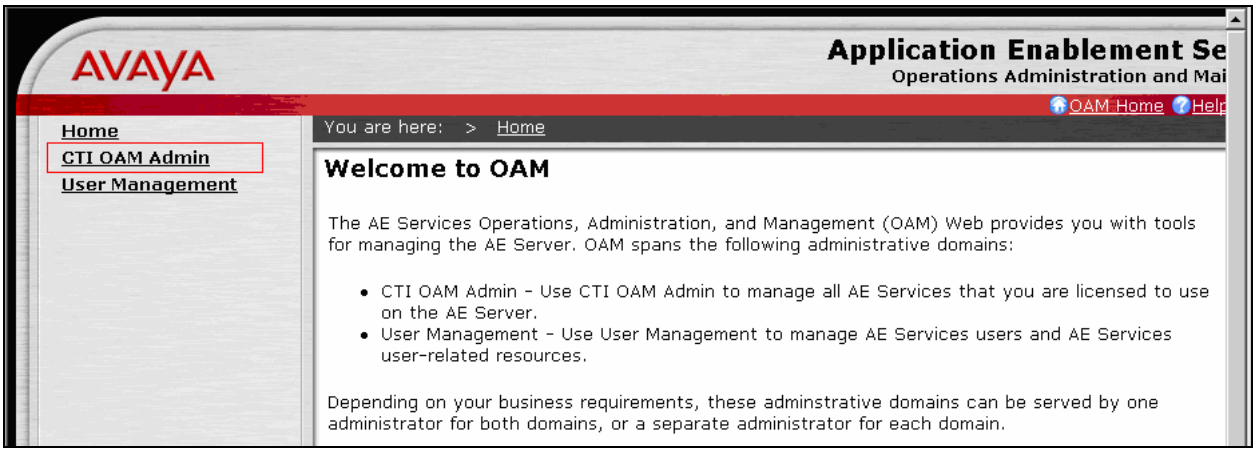
Avaya AES enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. Avaya AES receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, Avaya AES receives responses and events from Avaya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

Steps in this section describe configuring a Switch Connection and creating a CTI user. This section assumes that installation and basic administration of Avaya AES has been performed. See reference [2] for further details.

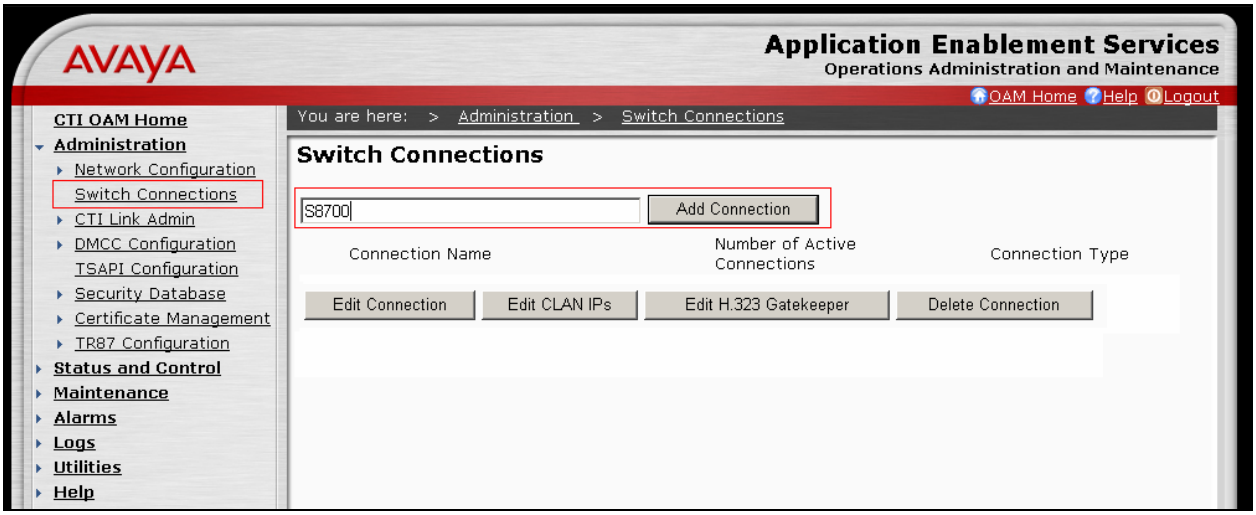
4.1. Configure Switch Connection

Launch a Web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

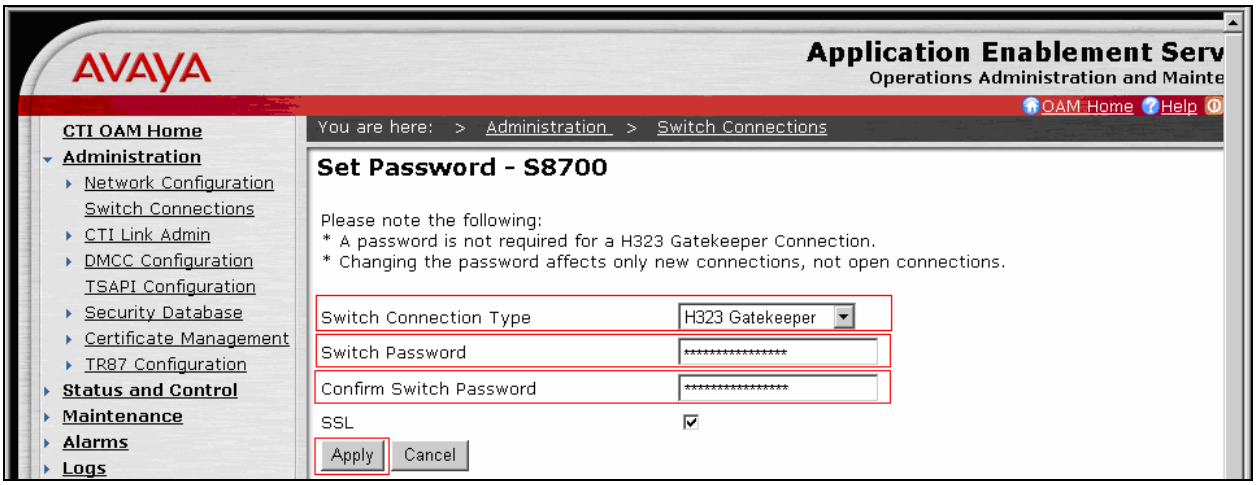
At the Welcome to OAM screen, select the **CTI OAM Admin** link from the left pane of the screen.



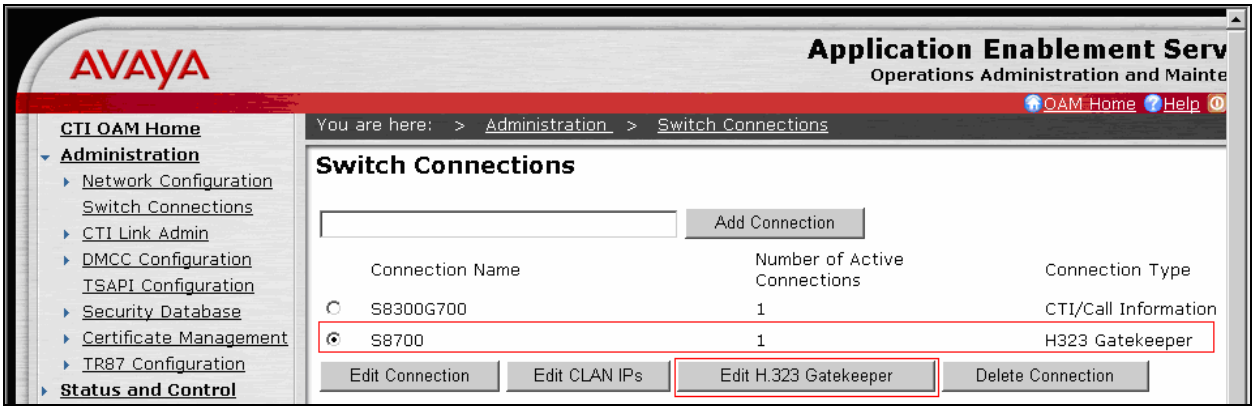
Click on **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



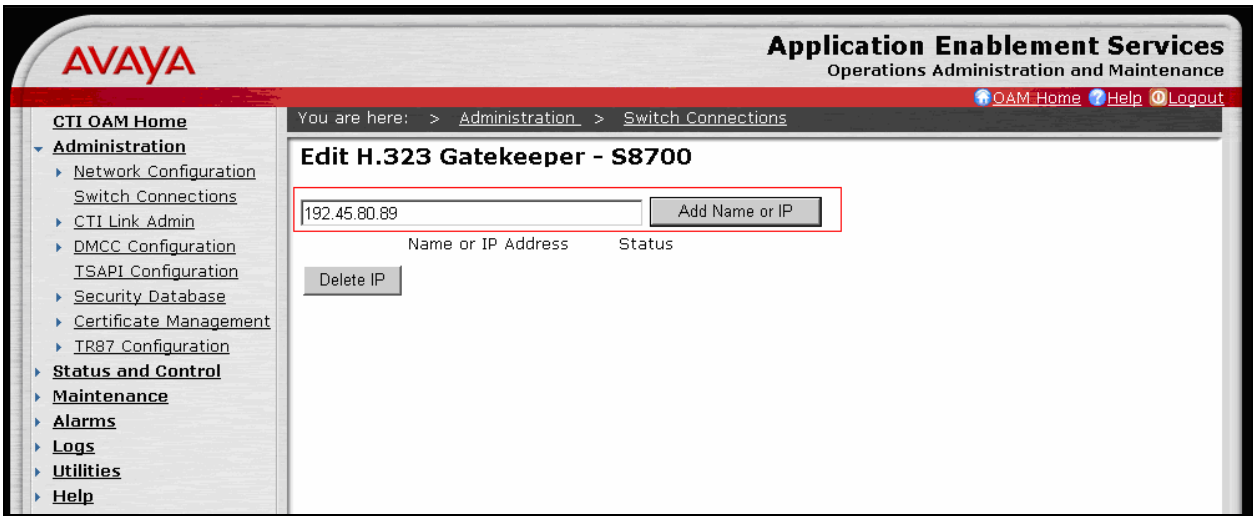
The next window that appears prompts for the switch connection password. Select **H323 Gatekeeper** using the drop down menu on the Switch Connection Type field. Enter into the Switch Password and Confirm Switch Password fields the same password that was administered in Avaya Communication Manager in **Section 3.5**. Default values may be used in the remaining fields. Click **Apply**.



After returning to the Switch Connections page, select the radio button corresponding to the switch connection added above, and click **Edit H.323 Gatekeeper**.



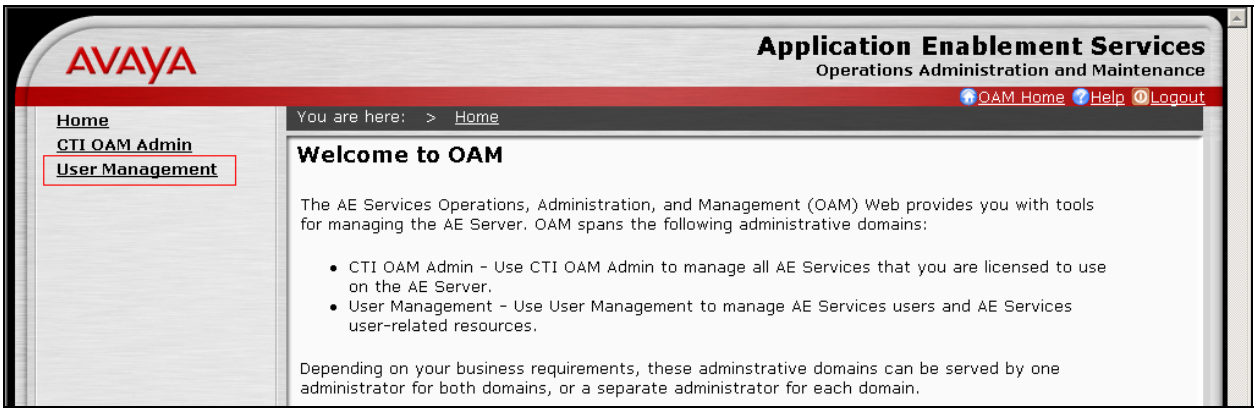
Enter the IP address of the CLAN used for AES connectivity from **Section 3.5**, and click **Add Name or IP**.



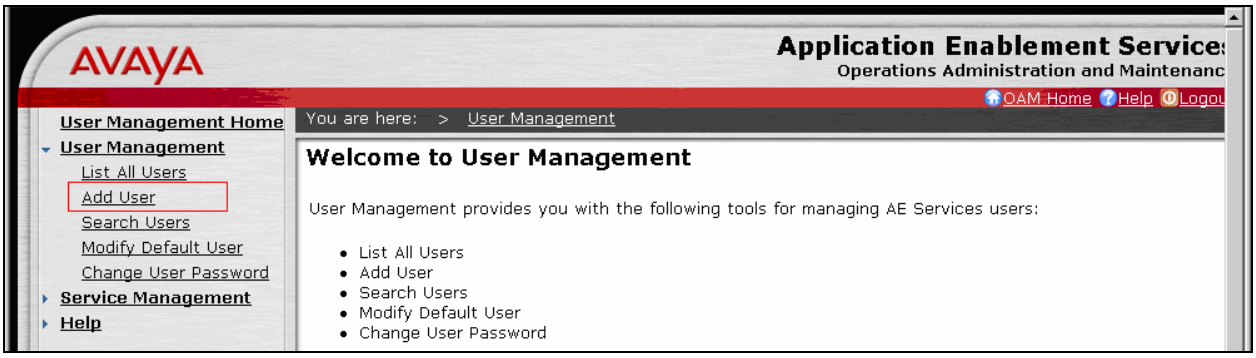
4.2. Configure CTI User

The steps in this section describe the configuration of a CTI user. Launch a Web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the OAM Home page.

The Welcome to OAM screen is displayed next. Select **User Management** from the left pane. NOTE: A second login screen will be presented greater access permissions are required.



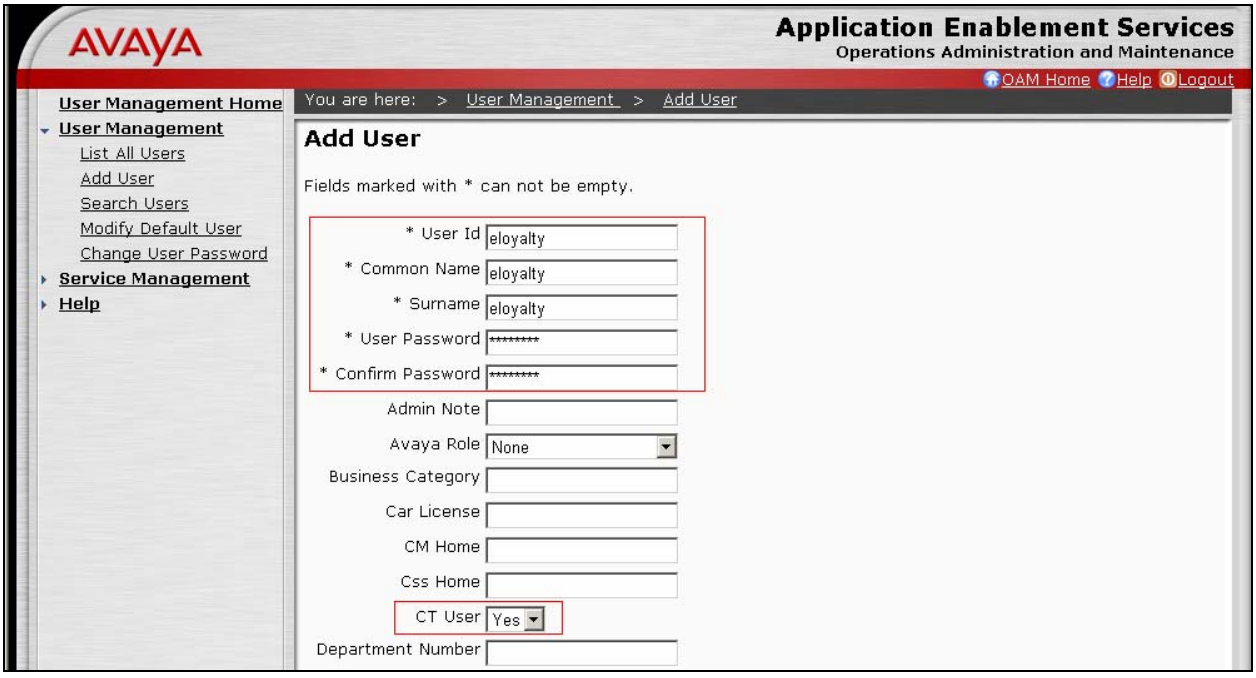
From the Welcome to the User Management Home page, navigate to the **User Management → Add User** page to add a CTI user.



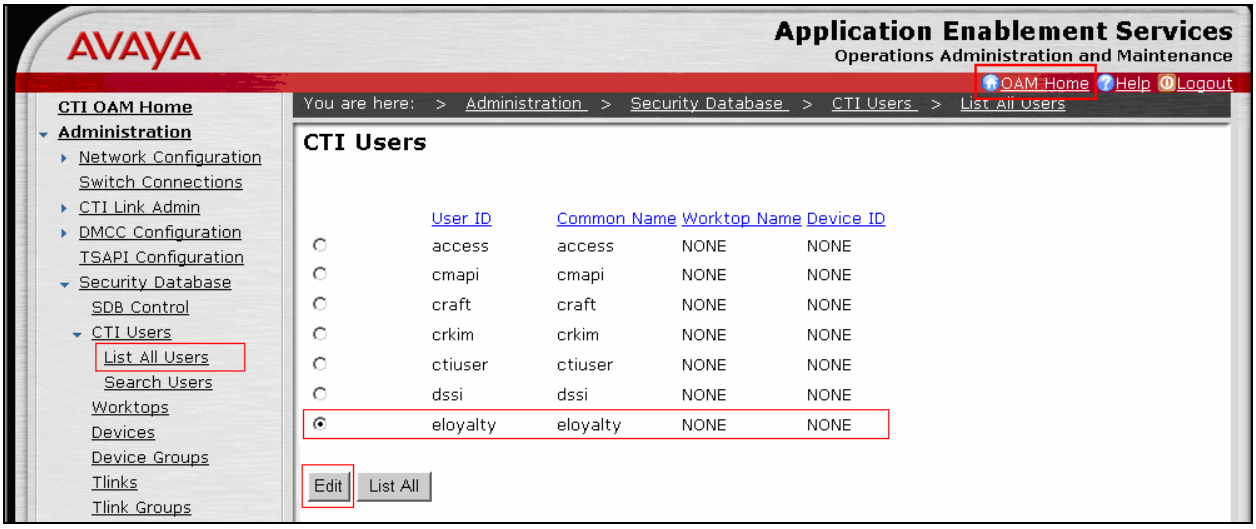
On the Add User page, provide the following information:

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

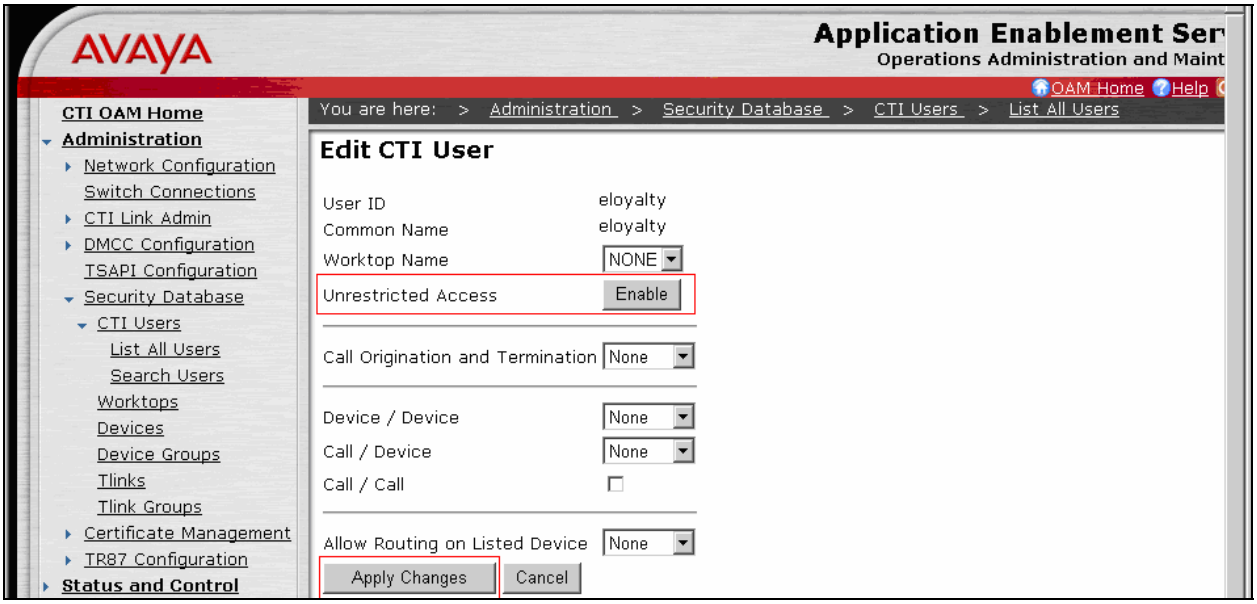
Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Default values may be used in the remaining fields. Click the **Apply** button (not shown here) at the bottom of the screen to complete the process.



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



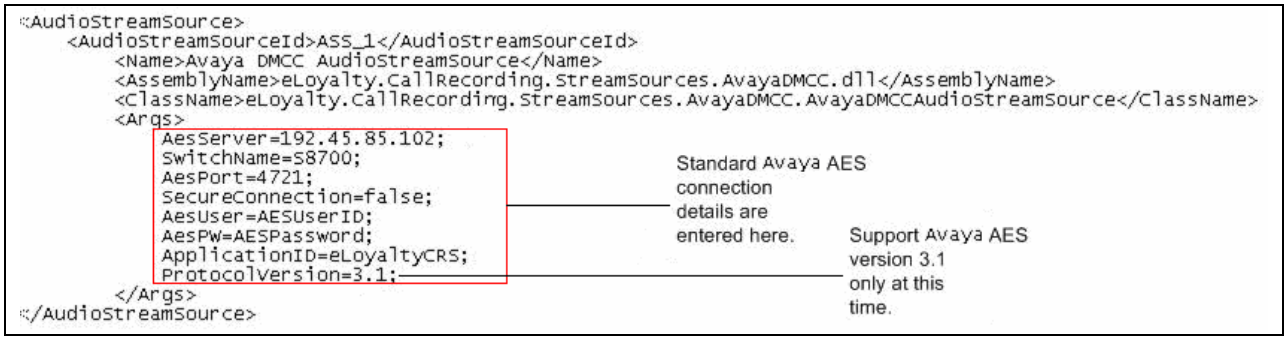
Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.



5. Configure eLoyalty Behavioral Analytics

In order to set up recording server for the Avaya AES recording solution, the following three files must be properly configured in eLoyalty Behavioral Analytics. These files are located in the **C:\Program f\Files\eLoyalty\eLoyalty Call Recording Service** directory.

- **configStations.csv** must contain the list of recorded stations.
- **configTDM.csv** must contain list of recording devices configured.
- **configMaster_DMCC.xml** must be updated to contain the Avaya AES connection information as shown below.



NOTE: The recording server is configured by eLoyalty personnel only and servers are always managed by eLoyalty.

6. Interoperability Compliance Testing

The interoperability compliance testing included feature, serviceability, and performance testing. The feature testing evaluated the ability of eLoyalty Behavioral Analytics to record calls placed to and from stations. The serviceability testing introduced failure conditions to verify that eLoyalty Behavioral Analytics can resume recording after failure recovery. The performance testing stressed eLoyalty Behavioral Analytics by continuously placing calls over extended periods of time.

6.1. General Test Approach

The general approach was to place various types of calls to and from both ACD stations (i.e. with EAS agents logged in) and non-ACD stations. These calls were recorded using the Call Capture Service, and the recordings verified. For feature testing, the types of calls included inbound and outbound trunk calls, transferred calls, and conferenced calls. Performance tests verified that the Call Capture Service could record calls during a sustained high volume of calls. The Call Capture Service is designed to record the first call appearance, and successfully recorded this appearance during transferring and conferencing testing. Serviceability failures were simulated by disconnecting cables and circuit packs as well as resetting the Avaya S8700 Server. The Call Capture Service required a restart, and reacted as expected during these failures. All test cases were performed manually.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

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

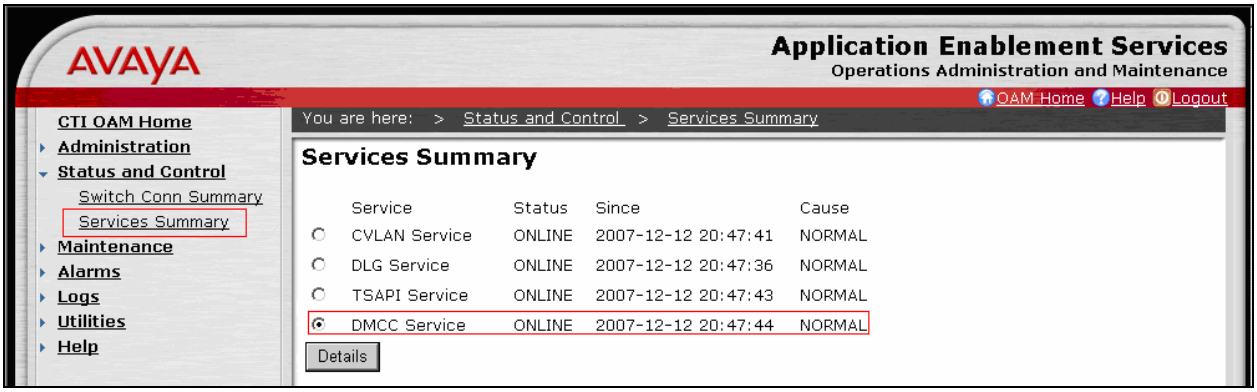
7.1. Verify Avaya Communication Manager

Verify the status of the administered link to Avaya AES by using the **status aesvcs link** command. The presence of an entry of the type shown below indicates that the link is up.

```
status aesvcs link

                          AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                          Port                    Sent    Rcvd

01/01  server1         192. 45. 80.102  36538   CLAN-AES        17      18
```

7.2. Verify Avaya Application Enablement Services

From the AES CTI OAM Admin web pages, verify that the status of the DMCC Service is ONLINE by selecting **Status and Control → Services Summary** from the left pane.



8. Support

Technical support on eLoyalty Behavioral Analytics can be obtained through the following:

- **Phone:** (877) 615-6925
- **Email:** BAServiceDesk@eLoyalty.com
- **Web:** https://servicedesk.eloyalty.net

9. Conclusion

These Application Notes describe the configuration steps required for eLoyalty Behavioral Analytics to interoperate with Avaya Communication Manager and Avaya Application Enablement Services. All feature and serviceability test cases were completed.

10. Additional References

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

[1] *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 3.1, February 2007

[2] *Application Enablement Services Installation and Upgrade Guide for a Bundled Server*, Issue 4.0, July 2007

[3] *eLoyalty Call Capture Service Test Plan, Avaya VoIP Integration*, November 2007.

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.