Avaya Solution & Interoperability Test Lab

Application Notes for Applied Network Intelligence Trunk Dashboard with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Applied Network Intelligence (ANI) Trunk Dashboard to interoperate with Avaya Communication Manager and Avaya Application Enablement Services.

ANI Trunk Dashboard is a monitoring tool that uses Avaya Application Enablement Services to monitor up to 16 Avaya Communication Managers for any indication of a problem with Trunks. The Trunk Group monitoring is based on both snapshots of trunk group data and on 10-minute averages of trunk group usage information. The Dashboard also monitors for Major Alarms, Minor Alarms, DS1 Alarms, and CDR Link Alarms.

The overall objective of this testing is to verify the ANI Trunk Dashboard can interoperate with Avaya Application Enablement Services and Avaya Communication Manager.

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

1. Introduction

These Application Notes describe the configuration steps required for Applied Network Intelligence (ANI) Trunk Dashboard to interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES). ANI Trunk Dashboard is a monitoring tool that uses Avaya AES to monitor up to 16 Avaya Communication Managers for any indication of a problem with Trunks. The Trunk Group monitoring is based on both snapshots of trunk group data and on 10-minute averages of trunk group usage information. The Dashboard also monitors for Major Alarms, Minor Alarms, DS1 Alarms, and CDR Link Alarms.

The overall objective of this testing is to verify the ANI Trunk Dashboard can interoperate with Avaya AES and Avaya Communication Manager.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary.

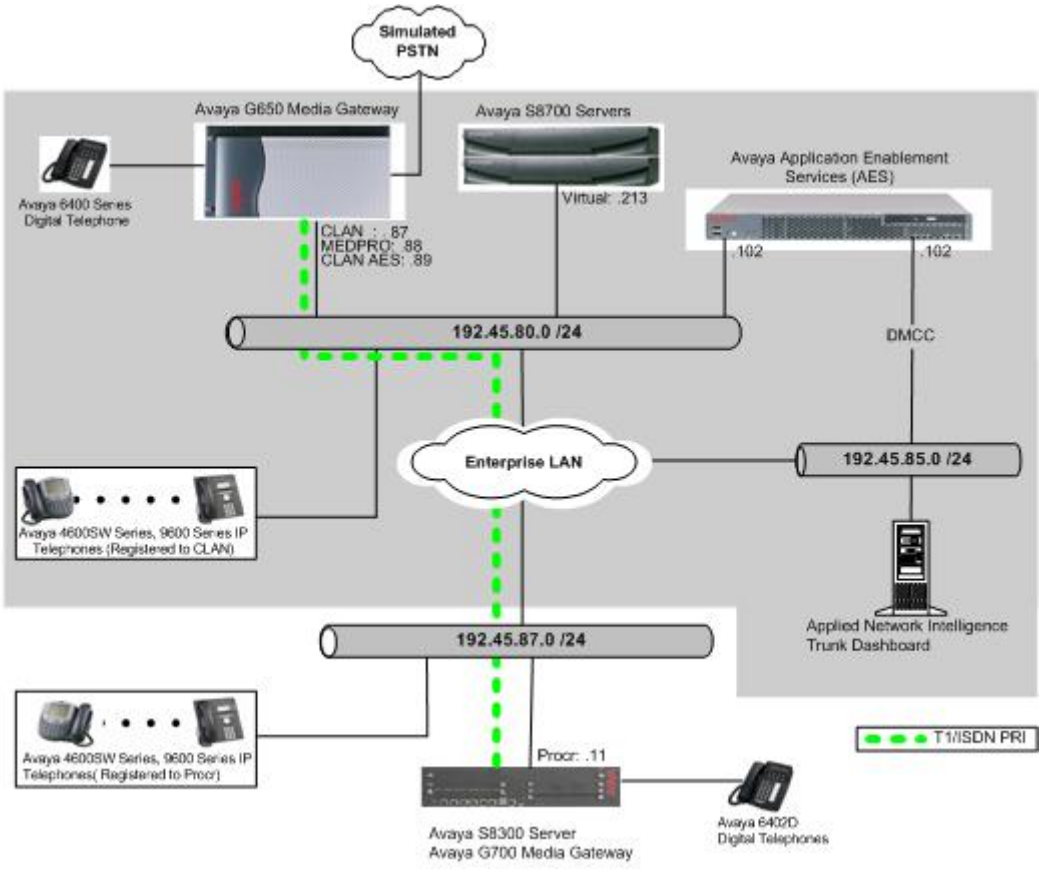


Figure 1: ANI Trunk Dashboard with Avaya Communication Manager and Avaya AES

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)
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)
Avaya G700 Media Gateway		25.28.0
Avaya Application Enablement Services		4.0 w/ Bundled Offer Build 47.3
Avaya 4600 Series IP Telephones		
	4620SW(H.323) 4625SW (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		-
Applied Network Intelligence Trunk Dashboard		1.0

3. Configure Avaya Communication Manager

This section provides the procedures for configuring a T1 trunk, trunk group, and signal group on Avaya Communication Manager. The highlights in the following screens indicate the values used during the compliance test.

3.1. Configure T1/ISDN-PRI trunk

This section describes the steps for configuring the T1/ISDN-PRI trunk on Avaya Communication Manager. Enter the **list configuration all** command and note the Board Number for the DS1 circuit pack to be configured.

```
list configuration all                                          Page   3

                              SYSTEM CONFIGURATION

Board                                                    Assigned Ports
Number    Board Type              Code     Vintage    u=unassigned t=tti p=psa

01A10     DS1 INTERFACE            TN464F  000018      01 02 03 04 05 06 07 08
                                                       09 10 11 12 13 14 15 16
                                                       17 18 19 20 21 22 23 24
                                                       u  u  u  u  u  u  u  u
```

Enter the **add ds1 x** command, where **x** is the board number of the DS1 circuit pack noted previously. Enter a descriptive Name and set the other highlighted fields below to the values indicated.

```
add ds1 1a10                                                  Page   1 of   2
                              DS1 CIRCUIT PACK

            Location: 01A10                          Name: ANI-test
            Bit Rate: 1.544                    Line Coding: b8zs
   Line Compensation: 1                        Framing Mode: esf
      Signaling Mode: isdn-pri
             Connect: pbx                          Interface: user
   TN-C7 Long Timers? n                  Country Protocol: 1
Interworking Message: PROGress           Protocol Version: a
Interface Companding: mulaw                          CRC? n
           Idle Code: 11111111
                                DCP/Analog Bearer Capability: 3.1kHz

                                          T303 Timer(sec): 4
```

3.2. Configure Signaling Group

Enter the **add signaling-group s** command, where **s** is an unused signaling group number. Set the highlighted fields below to the values indicated. Note that the value for the Primary D-Channel field is set to channel 24 on the DS1 circuit pack for a T1.

```
add signaling-group 10                                        Page   1 of   1
                              SIGNALING GROUP

 Group Number: 10              Group Type: isdn-pri
                     Associated Signaling? y          Max number of NCA TSC: 10
                        Primary D-Channel: 01A1024     Max number of CA TSC: 10
                                                    Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:
          Supplementary Service Protocol: a
```

After the completion of the trunk group configuration in **Section 3.3**, enter the **change signaling-group s** command, where **s** is the number of the signaling group configured previously. Set the Trunk Group for Channel Selection field value to the trunk group number configured in **Section 3.3**.

```
change signaling-group 10                                     Page   1 of   1
                              SIGNALING GROUP

 Group Number: 10              Group Type: isdn-pri
                     Associated Signaling? y          Max number of NCA TSC: 10
                        Primary D-Channel: 01A1024     Max number of CA TSC: 10
                                                    Trunk Group for NCA TSC: 10
       Trunk Group for Channel Selection: 10
          Supplementary Service Protocol: a
```

3.3. Configure Trunk Group

Enter the **add trunk-group t** command, where **t** is an unused trunk group number. On **Page 1** of the TRUNK GROUP form, enter a descriptive Group Name and enter a TAC that is valid under

the provisioned dial plan in Avaya Communication Manager. Set the other highlighted fields below to the values indicated.

```
add trunk-group 10                                          Page   1 of  21
                             TRUNK GROUP

Group Number: 10                   Group Type: isdn          CDR Reports: y
  Group Name: trunk-ANI                 COR: 1        TN: 1        TAC: 111
   Direction: two-way        Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? n                Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n             TestCall ITC: rest
                        Far End Test Line No:
TestCall BCC: 4
```

On **Page 3**, set the highlighted fields below to the values indicated.

```
add trunk-group 10                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: internal
                                 Internal Alert? n        Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                     Send Name: y      Send Calling Number: y
            Used for DCS? n                           Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: public
                                        UUI IE Treatment: service-provider

                                           Replace Restricted Numbers? n
                                         Replace Unavailable Numbers? n
                                               Send Connected Number: n
                                          Hold/Unhold Notifications? n
             Send UUI IE? y                Modify Tandem Calling Number? n
               Send UCID? n
 Send Codeset 6/7 LAI IE? y
```

On **Page 5** of the trunk-group form, add trunk members by entering:

- **xxxxxzz** for Port, where **xxxxx** is the board number of the DS1 circuit pack configured in the SYSTEM CONFIGURATION form in **Section 3.1**, and **zz** is a channel in the T1/ISDN-PRI.
- The signaling group number configured in **Section 3.2** for the Sig Grp field.

For the compliance test, channels 1 – 15 and 16 – 23 (not shown) of the T1/ISDN-PRI were added. Channel 24, the Primary D-Channel configured in **Section 3.2**, was excluded.

```
add trunk-group 10                                          Page   5 of  21
                                TRUNK GROUP
                                     Administered Members (min/max):   0/0
GROUP MEMBER ASSIGNMENTS                 Total Administered Members:   0

       Port    Code Sfx Name        Night           Sig Grp
  1: 01A1001  TN464  F                               10
  2: 01A1002  TN464  F                               10
  3: 01A1003  TN464  F                               10
  4: 01A1004  TN464  F                               10
  5: 01A1005  TN464  F                               10
  6: 01A1006  TN464  F                               10
  7: 01A1007  TN464  F                               10
  8: 01A1008  TN464  F                               10
  9: 01A1009  TN464  F                               10
 10: 01A1010  TN464  F                               10
 11: 01A1011  TN464  F                               10
 12: 01A1012  TN464  F                               10
 13: 01A1013  TN464  F                               10
 14: 01A1014  TN464  F                               10
 15: 01A1015  TN464  F                               10
```

3.4. Configure Uniform Dialplan

Enter the **change uniform-dialplan d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial extension for the Matching Pattern field. Enter the length of the extension for the Len field. Set the Del field set to **0**, and the Net field to **aar**.

```
change uniform-dialplan 4                                    Page   1 of   2
                      UNIFORM DIAL PLAN TABLE
                                                           Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len Del       Digits      Net Conv Num
7                5   0                    aar  n
                                                n
                                                n
```

3.5. Configure AAR

Enter the **change aar analysis d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial extension for the Dialed String field. Enter the number of an unused route pattern for the Route Pattern field. The route pattern will be defined in **Section 3.6**. The Call Type field is set to **aar**.

```
change aar analysis 444                                      Page   1 of   2
                          AAR DIGIT ANALYSIS TABLE
                                                      Percent Full:    2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    7                     5    5     79        aar          n
```

3.6. Configure Route Pattern

Enter the **change route-pattern r** command, where **r** is the number of the route pattern specified in **Section 3.5**. Enter the number of the trunk group configured in **Section 3.3** for the Grp No field. Assign a Facility Restriction Level to this routing preference for the FRL field. The FRL value is set to **0**, which is the least restrictive.

```
change route-pattern 79                                      Page   1 of   3
                    Pattern Number: 79   Pattern Name: Lyrix
                                SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                                  Dgts                              Intw
 1: 10    0                                                         n   user
 2:                                                                 n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 3 4 W     Request                                  Dgts Format
                                                          Subaddress
 1: y y y y y n  n            rest                                      none
 2: y y y y y n  n            rest                                      none
```

3.7. Configure IP Services

Enter the **change node-names ip** command. Define node names for two CLANs. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoints, and 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
CLAN                   192.45.80.87
CLAN-AES               192.45.80.89
MEDPRO                 192.45.80.88
S8300G700              192.45.87.11
default                0.0.0.0
```

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

```
change ip-services                                              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 AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and run **uname –a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 4.1**.

```
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

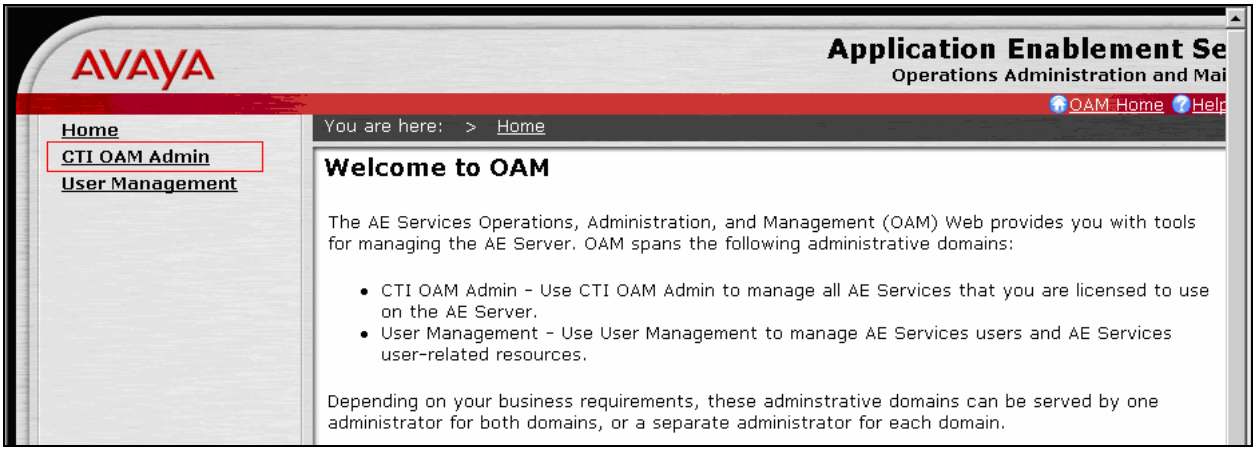
Avaya AES enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. Avaya AES receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, Avaya AES receives responses and events from Avaya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

This section assumes that installation and basic administration of Avaya AES has been performed. The steps in this section describe configuring of a Switch Connection and creating a CTI user.

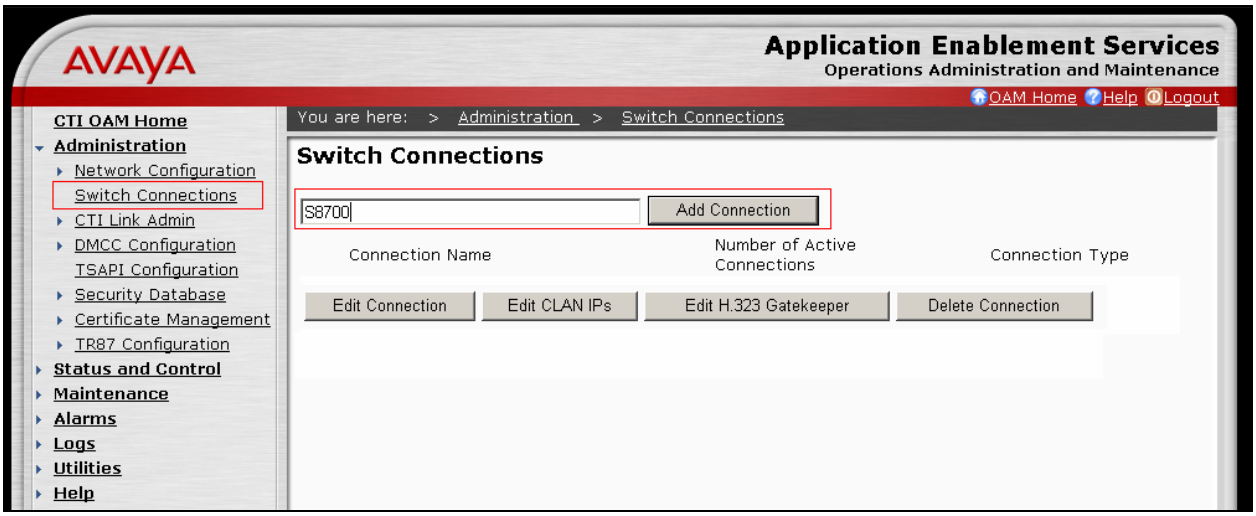
4.1. Configure Switch Connection

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.

Select the **CTI OAM Admin** link from the left pane of the page.

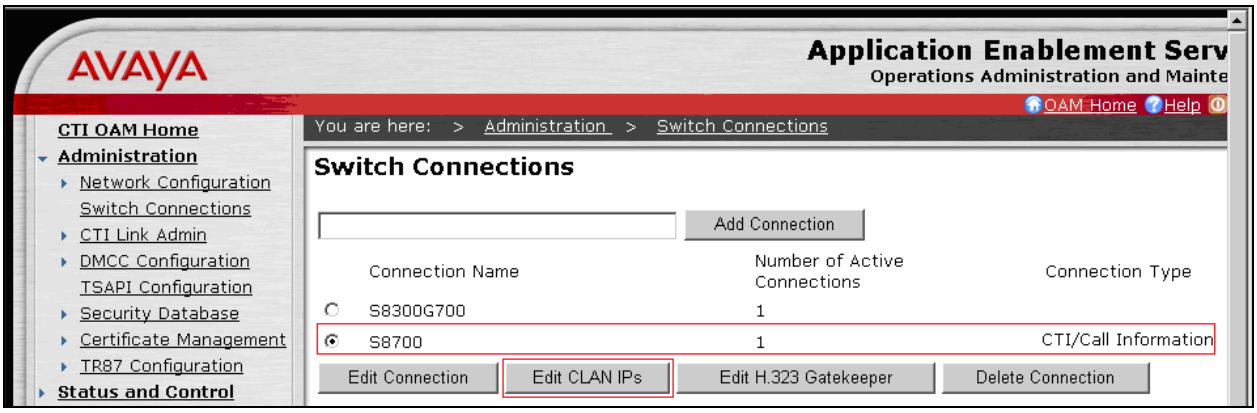


Click on **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

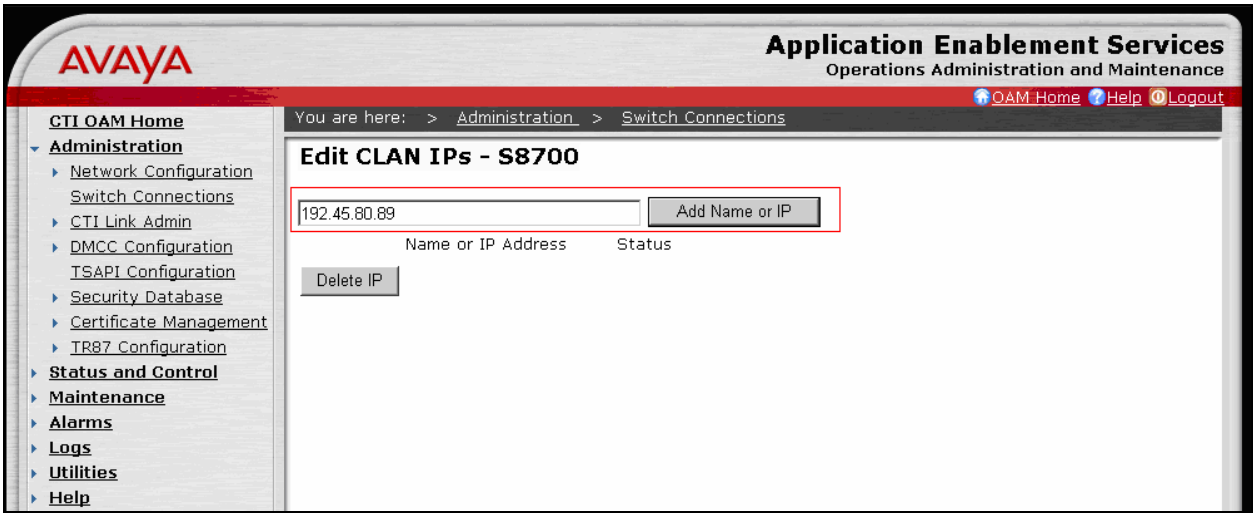


The next window that appears prompts for the switch connection password. Select **CTI/Call Information** using the drop down menu on the Switch Connection Type field. Enter the same password that was administered on Avaya Communication Manager in **Section 3.7**. Default values may be used in the remaining fields. Click on **Apply**.

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

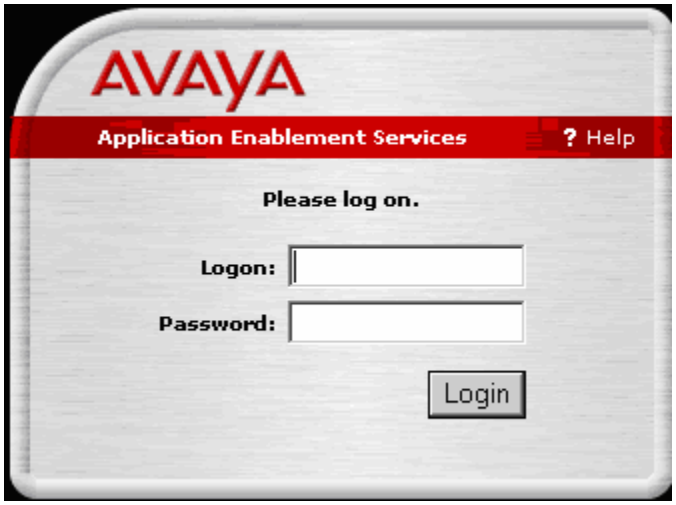


Enter the IP address of the CLAN used for AES connectivity from **Section 3.7**, and click on **Add Name or IP**.

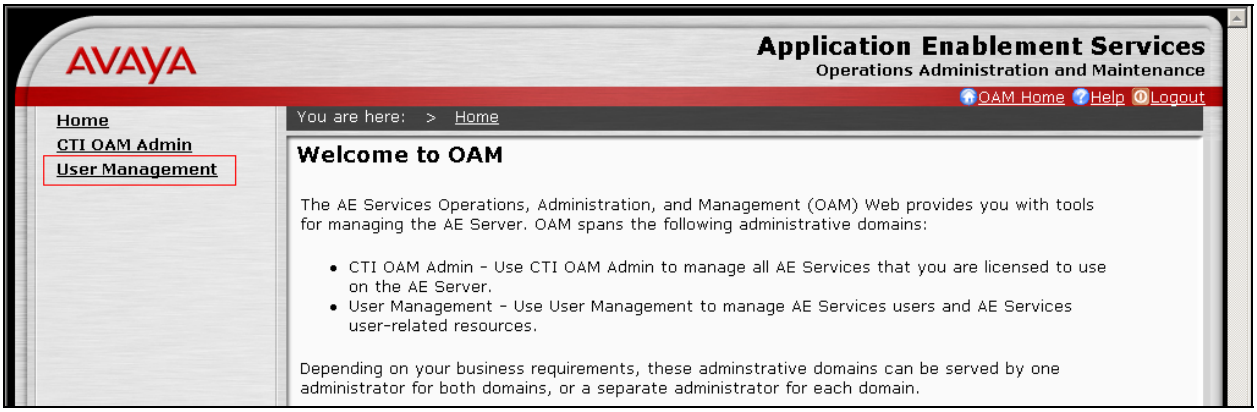


4.2. Configure CTI User

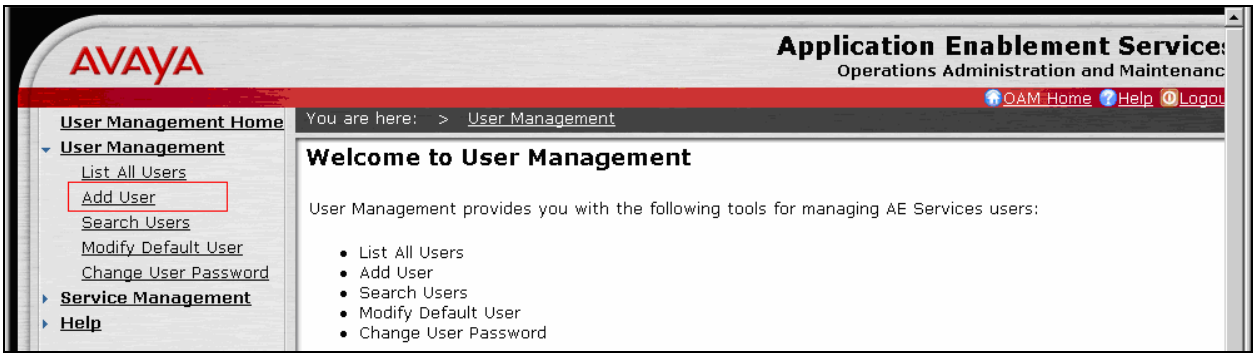
The steps in this section describe the configuration of a CTI user. Launch a web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the OAM Home page.



The Welcome to OAM page is displayed next. Select **User Management** from the left pane.



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

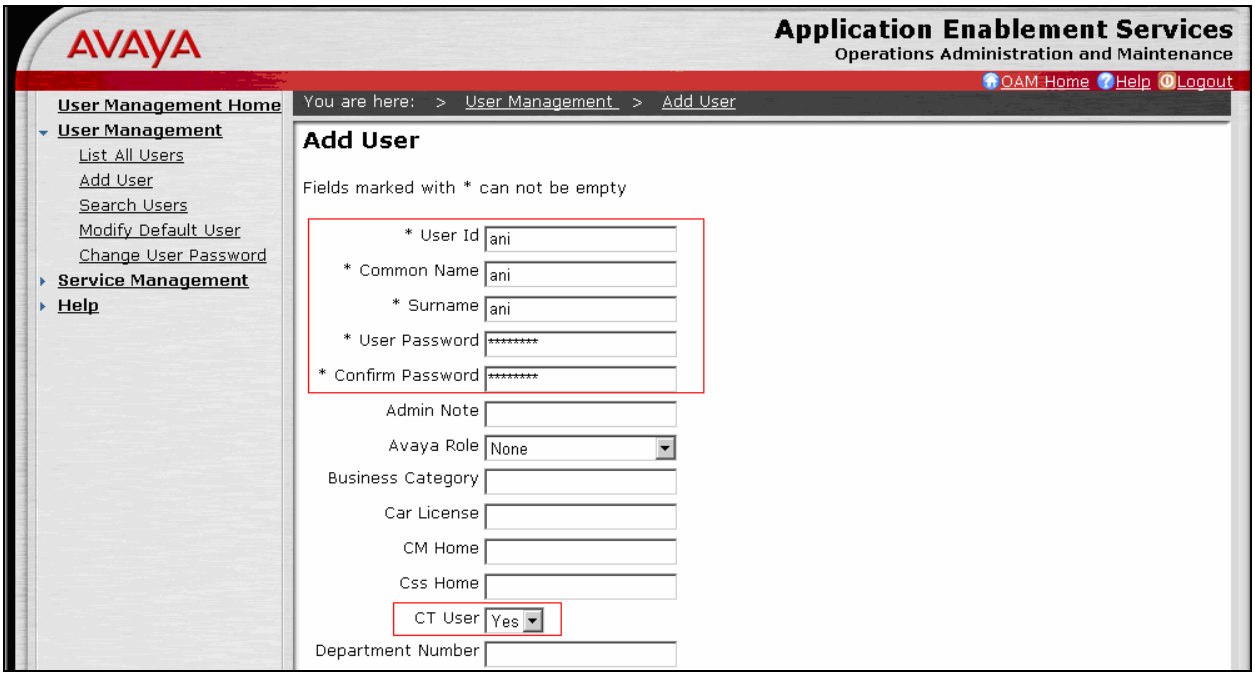


On the Add User page, provide the following information:

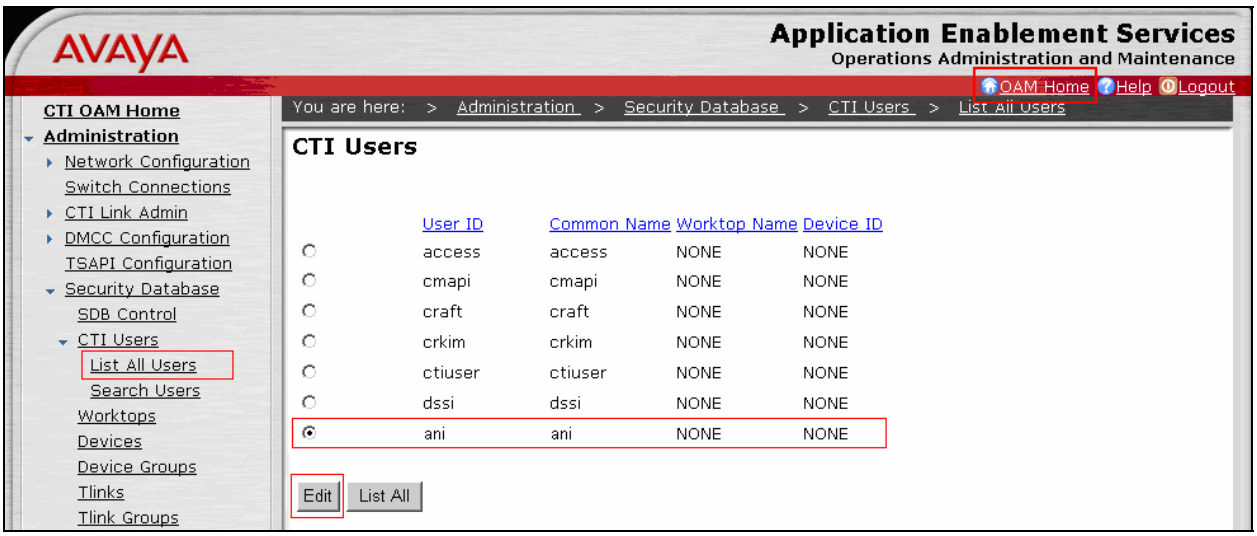
- User Id
- Common Name
- Surname
- User Password
- Confirm Password

Note: User ID and User Password must match with information configured in the **cmapi.properties** file in **Section 5**.

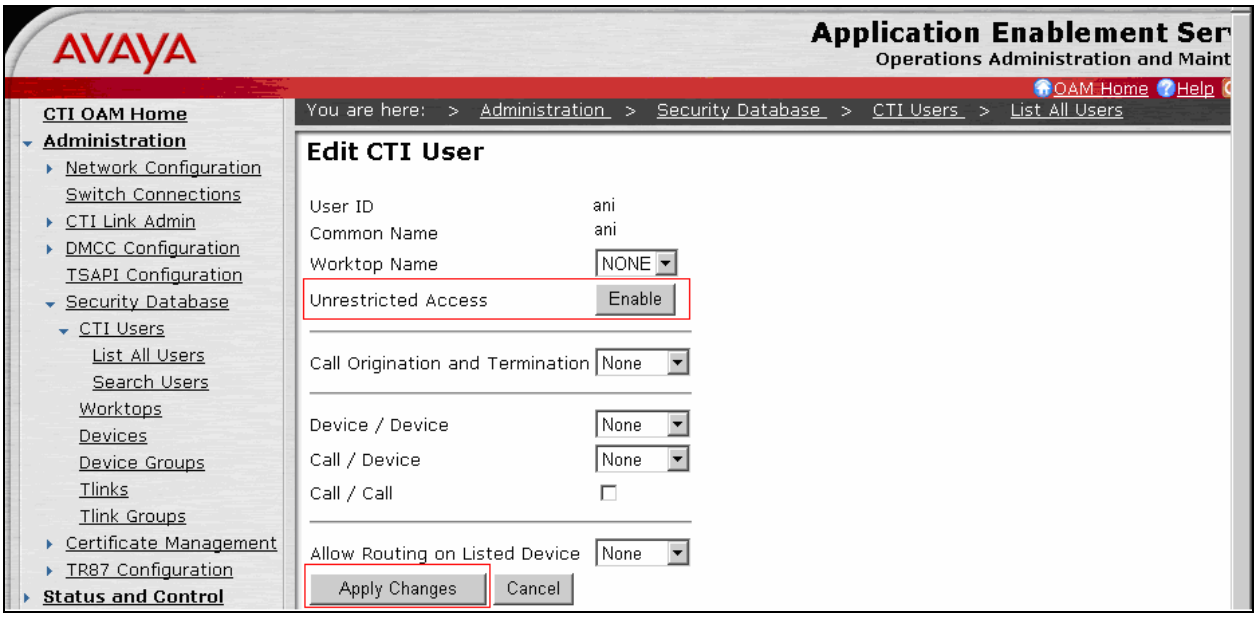
Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Click the **Apply** button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields



Once the user is created, select **OAM Home** in upper right of the page 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 ANI Trunk Dashboard

ANI installs, configures, and customizes the Trunk Dashboard application for their end customers. For installation and configuration of the Trunk Dashboard, contact ANI technical support.

This section only illustrates the interface configuration of the Trunk Dashboard to communicate with Avaya AES utilizing DMCC service. The following shows the contents of the **cmapi.properties** file located in the **c:\Program Files\starfish\datacollector\config** directory.

- cmapi1.server_ip – Enter the Client Connectivity IP address of AES.
- cmapi1.username – Enter the CTI username configured in **Section 4.2**.
- cmapi1.password – Enter the CTI password configured in **Section 4.2**.
- cmapi1.server_port – Enter the unencrypted DMCC server port. The default port, **4721**, was used during the compliance test.
- cmapi1.secure – Since the unencrypted port was used, this field was set to **false**.

```
# CMAPI specific data.
cmapi1.server_ip=192.45.85.102
cmapi1.username=ani
cmapi1.password=ani
cmapi1.server_port=4721
# Legal values for cmapi1.secure are true and false.
cmapi1.secure=false
#cmapi.trust_store_location=C:\\Program Files\\starfish\\datacollector\\config\\avaya.jks


#Button specific data.
majorbutton=263
minorbutton=264
cdr1button=266
cdr2button=267
ds1button=265
nextbutton=285

# 3.1 to 4.0 transition related changes!
exitbutton=0
shared=false
waitfordisplayrefresh=0
restartcount=3
restartenable=false
```

6. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of ANI Trunk Dashboard to monitor and collect statistics of calls placed thru the trunk. The serviceability testing introduced failure scenarios to see if ANI Trunk Dashboard can resume recording after failure recovery.

6.1. General Test Approach

All test cases were performed manually. The general approach was to place trunk calls to and from stations. These trunk calls were monitored using ANI Trunk Dashboard, and trunk usage

statistics were verified. Alarms were manually created and verified using ANI Trunk Dashboard. For serviceability testing, failures such as cable pulls, busyouts and releases of the DS1 trunk group, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

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

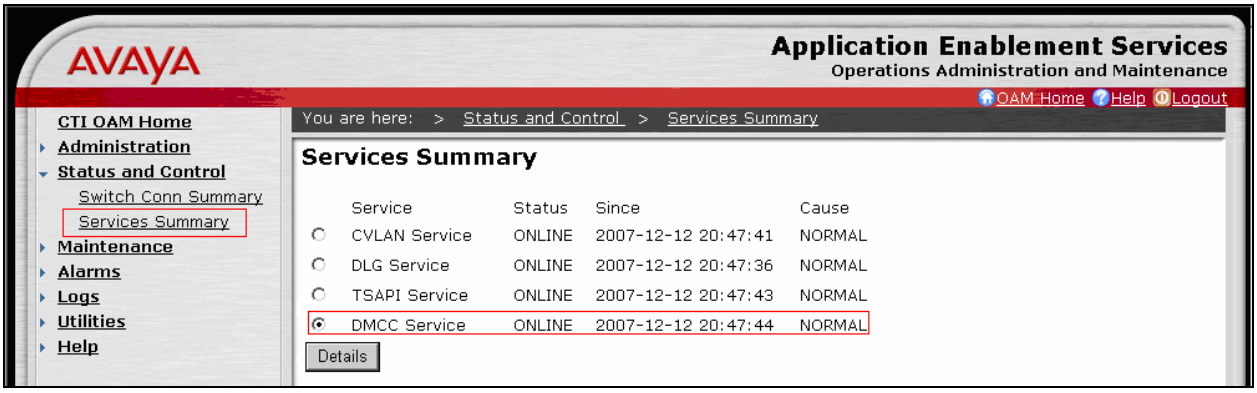
7.1. Verify Avaya Communication Manager

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

```
status aesvcs link

                              AE SERVICES LINK STATUS

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 the status of the DMCC Service by selecting **Status and Control → Services Summary** from the left pane.



8. Support

Technical support on ANI Trunk Dashboard can be obtained through the following:

- **Phone:** (908) 203-4660 or (800) 771-6943
- **Email:** info@starfishdevelopment.com
- **Web:** https://www.starfishdevelopment.com

9. Conclusion

These Application Notes describe the configuration steps required for ANI Trunk Dashboard 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 ANI 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] *Telecom Dashboard, Real-Time Monitoring of Trunk Performance*

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.