Avaya Solution & Interoperability Test Lab

Application Notes for Grandsys LOG8000 with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Grandsys LOG8000 to monitor and record calls placed to and from Avaya IP telephones and agents on Avaya Aura™ Communication Manager. Grandsys LOG8000 uses the Device, Media and Call Control (DMCC) API of the Avaya Aura™ Application Enablement Services to monitor stations to obtain call information and to register DMCC softphones that Grandsys LOG8000 uses as recording ports.

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 a compliance-tested configuration comprised of an Avaya Aura™ Communication Manager, an Avaya Aura™ Application Enablement Services and Grandsys LOG8000.

Grandsys LOG8000 is a recording solution made for the customers of the call center market. Grandsys LOG8000 communicates with Application Enablement Services using the Device, Media and Call Control (DMCC) API to monitor stations to obtain call information and to register DMCC softphones that Grandsys LOG8000 uses as recording ports. When a call starts on an extension to be recorded, Communication Manager will send the audio stream to Grandsys LOG8000 which will then record the call and save the recording to the database. Detailed call information obtained using DMCC is also stored for each call along with the recording.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of Grandsys LOG8000 to monitor and record calls placed to and from stations and agents. The serviceability testing introduced failure scenarios to see if Grandsys LOG8000 can resume recording after failure recovery.

1.2. Support

For technical support on Grandsys LOG8000, contact Grandsys at:

- Phone: +886-2-87682715
- Email: service@grandsys.com

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8500 Server, an Avaya G650 Media Gateway, an Application Enablement Services Server, Avaya IP Telephones and a Windows 2003 Server running Grandsys LOG8000. The Grandsys LOG8000 Server monitors the agent extensions using the DMCC Service to record the call and obtain call related information. The DMCC Service is provided by the Application Enablement Services Server.

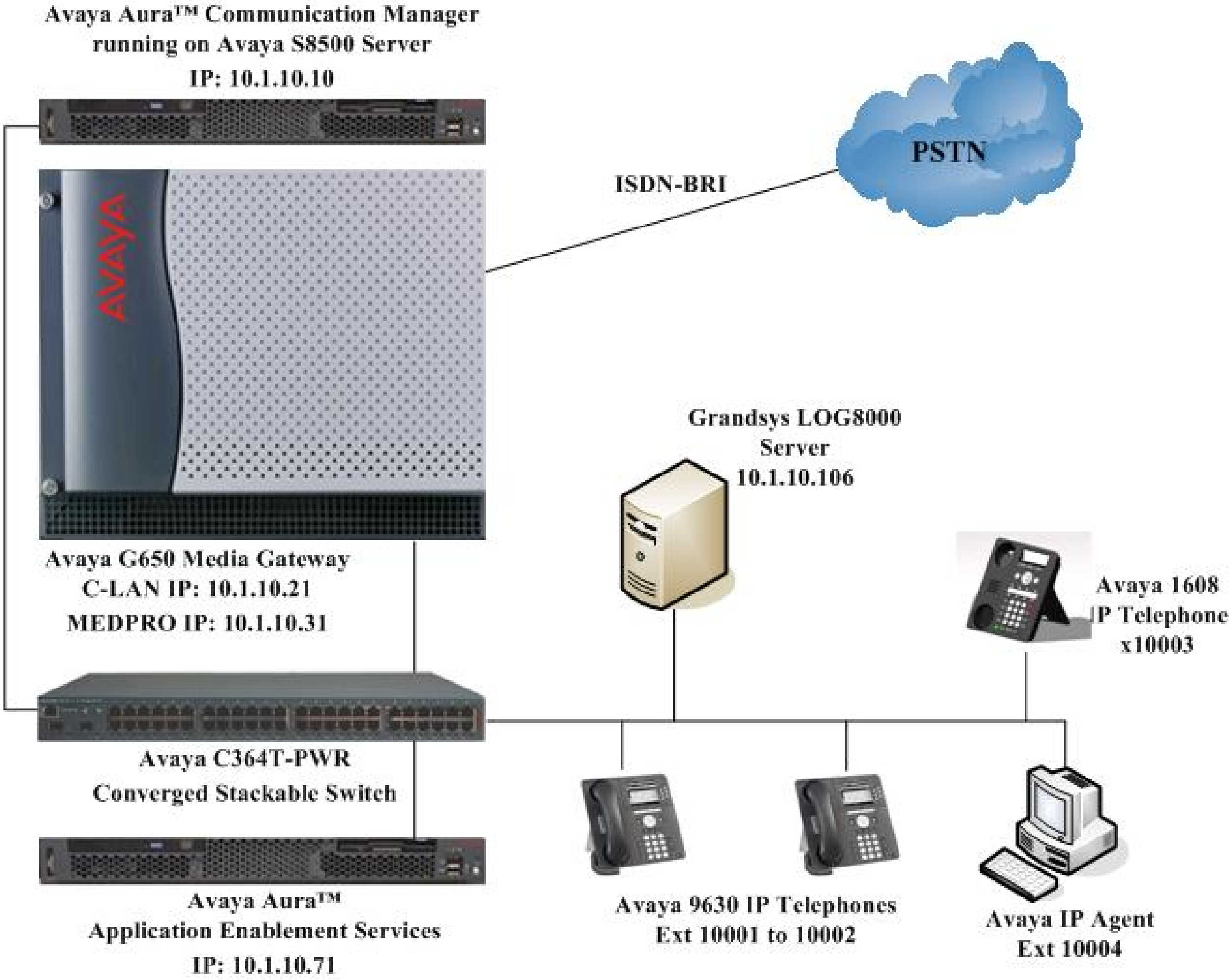


Figure 1: Test Configuration

3. Equipment and Software Validated

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

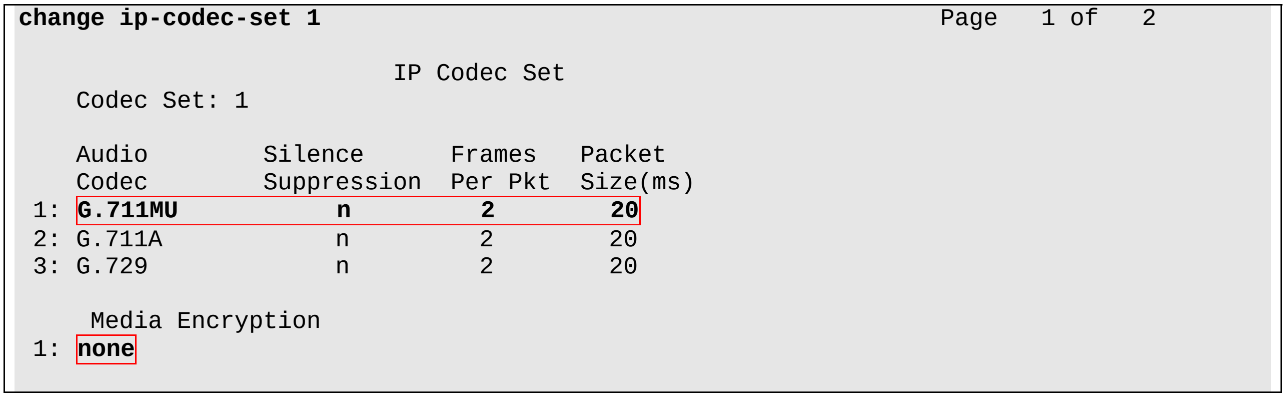
Equipment	Version
Avaya S8500 Server	Communication Manager 5.2 (Service Pack 02.0.947.3-17250)
Avaya G650 Media Gateway	-
- TN2312BP IP Server Interface	HW07, FW046
- TN799DP C-LAN Interface	HW01, FW032
- TN2602AP IP Media Processor	HW02, FW048
- TN2464BP DS1 Interface	HW05, FW022
Application Enablement Services	4.2.1 with Patch 2
Avaya 9630 IP Telephones	3.0 (H.323)
Avaya 1608 IP Telephone	1.1.0.0 (H.323)
Avaya IP Agent	7.0.32.198
Avaya C364T-PWR Converged Stackable Switch	4.5.18
Grandsys LOG8000	2.2.2

4. Configure Communication Manager

This section provides the procedures for configuring an ip-codec-set and ip-network region, a switch connection and Computer Telephony Integration (CTI) links and recorded/monitored stations on Communication Manager. All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

4.1. Codec Configuration

Enter the **change ip-codec-set n** command, where **n** is a number between 1 and 7, inclusive. Ensure that the supported codecs for DMCC are used. In this compliance testing, the **G.711MU** codec and no media encryption are 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: G.711A            n          2        20
 3: G.729             n          2        20

     Media Encryption
 1: none
```

4.2. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. The Avaya IP Telephones and IP Softphones used by Grandsys LOG8000 registered with the C-LAN board and were thus also assigned to IP network region 1. As a result, the RTP traffic between them is governed by the codec set defined by the **Codec Set** field. In this configuration, IP codec set **1** is used as defined in **Section 4.1**.

```
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? n
   UDP Port Max: 3929
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: 46
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
```

4.3. Configure AES and CTI Links

Grandsys LOG8000 uses the DMCC API to communicate with Application Enablement Services and to obtain call information, which requires the Telephony Services Application Programming Interface (TSAPI) CTI link to be configured on Communication Manager. Application Enablement Services communicates with Communication Manager over an AES link. Within the AES link, a CTI link is configured to provide the required TSAPI service to Grandsys LOG8000. The following steps demonstrate the configuration of the Communication Manager side of the AES and CTI links. See **Section 5** for the details of configuring the Application Enablement Services side of the AES and TSAPI CTI links.

Step **Description**

1. Enter the **display system-parameters customer-options** command. On Page 3, verify that **Computer Telephony Adjunct Links** is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.

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

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

2. Enter the **add cti-link n** command, where **n** is a number between 1 and 64, inclusive. Enter a valid **Extension** under the provisioned dial plan in Communication Manager, set the **Type** field to **ADJ-IP**, and assign a descriptive **Name** to the CTI link.

```
add cti-link 1                                               Page   1 of   2
                                    CTI LINK
 CTI Link: 1
Extension: 19951
     Type: ADJ-IP
                                                                    COR: 1
     Name: TSAPI Svcs
```

3. Enter the **change node-names ip** command. In the compliance-tested configuration, the **CLAN-01A02** IP address was utilized for registering H.323 endpoints (Avaya IP Telephones) and for connectivity to Application Enablement Services.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
CLAN-01A02              10.1.10.21
MEDPRO-01A13            10.1.10.31
VAL-01A04               10.1.10.41
default                 0.0.0.0
procr                   10.1.10.10
```

Step	Description
4.	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-01A02** board that was configured previously in **Step 3**. During the compliance test, the default port was utilized for the **Local Port** field.

```
change ip-services                                              Page   1 of    3

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      CLAN-01A02       8765
```

On Page 3, enter the hostname of the Application Enablement Services server for the **AE Services Server** field. The server name may be obtained by logging in to the Application Enablement Services server using Secure Shell (SSH), and running the **uname –a** command. Enter an alphanumeric password for the **Password** field and set the **Enabled** field to **y**. The same password will be configured on the Application Enablement Services server in **Section 5.1**.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes1              xxxxxxxxxxxxxxxx      y
      2:
      3:
```

4.4. Recorded (Monitored) Stations

Step	Description
1.	Enter the **change station n** command, where **n** is the extension of the agent station that is required to be recorded. On **Page 1** of the STATION form, set the **IP Softphone** field is to **y** and specify the **Security Code**. For the compliance test, the agent stations from 10001 to 10004 were modified.

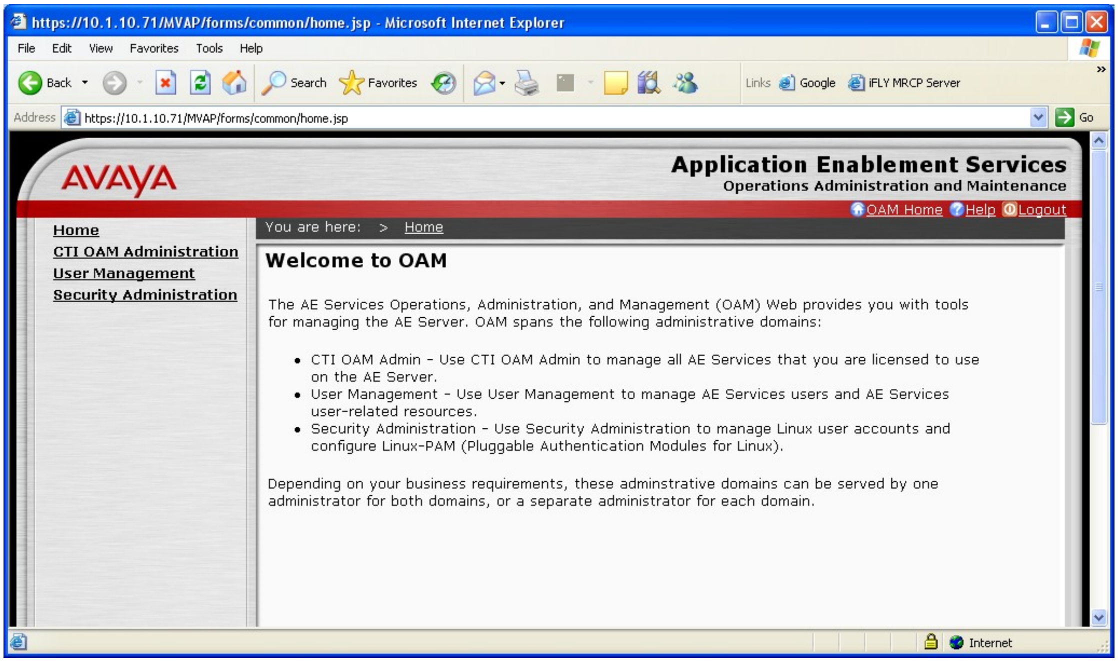
```
change station 10001                                            Page   1 of   5
                                     STATION

Extension: 10001                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: 000000           TN: 1
     Port: S00002                      Coverage Path 1:                 COR: 1
     Name: Alice                       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: 10001
            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? y

                                               IP Video Softphone? n


                                              Customizable Labels? y
```

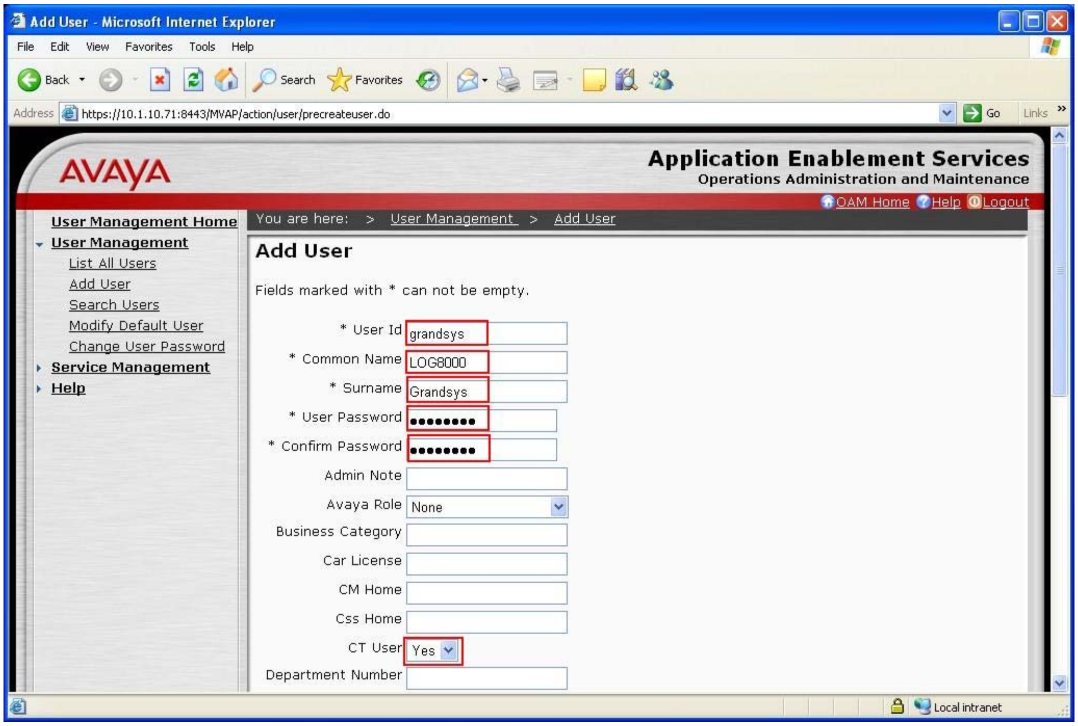
5. Configure Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

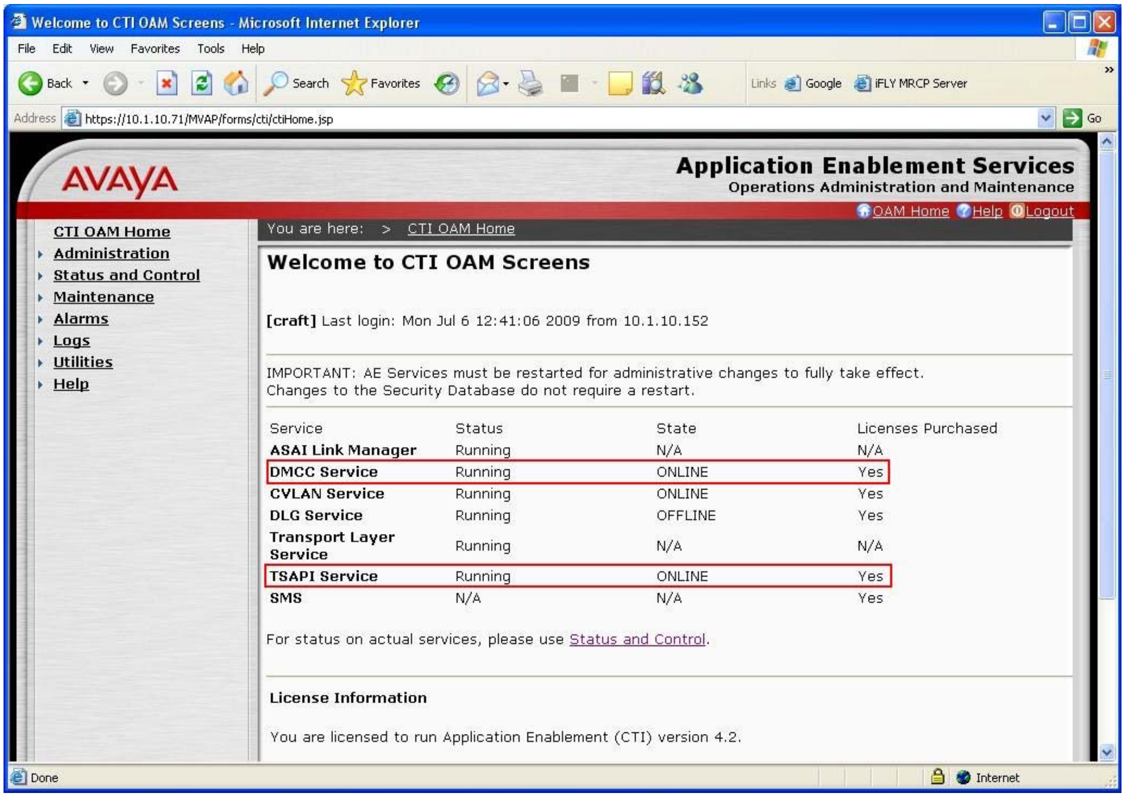
- Administer CTI User
- Verify Application Enablement Services License
- Administer Switch Connection
- Administer TSAPI link
- Administer Ports
- Administer CTI user permission

5.1. Administer CTI User

Step	Description
1.	Launch a web browser and enter **https://<IP address of AES server>/MVAP/** to access the Application Enablement Services OAM web based interface. Log in to OAM using an administrative login and password (not shown), and the Welcome To OAM screen will be displayed.  https://10.1.10.71/MVAP/forms/common/home.jsp - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Links Google iFLY MRCP Server Address https://10.1.10.71/MVAP/forms/common/home.jsp Go AVAYA Application Enablement Services Operations Administration and Maintenance OAM Home Help Logout Home CTI OAM Administration User Management Security Administration You are here: > Home Internet **Welcome to OAM** The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains: • CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server. • User Management - Use User Management to manage AE Services users and AE Services user-related resources. • Security Administration - Use Security Administration to manage Linux user accounts and configure Linux-PAM (Pluggable Authentication Modules for Linux). Depending on your business requirements, these adminstrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

Step	Description
2.	Click **User Management**, then **User Management > Add User** in the left pane. Specify a value for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set **CT User** to **Yes**. Use the values for **User Id** and **User Password** to configure Grandsys LOG8000 in **Section 6.1 Step 1** to access the DMCC Services on the Application Enablement Services. Scroll down to the bottom of the page and click **Apply** (not shown).  Add User - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://10.1.10.71:8443/MVAP/action/user/precreateuser.do Go Links AVAYA Application Enablement Services Operations Administration and Maintenance OAM Home Help Logout User Management Home User Management List All Users Add User Search Users Modify Default User Change User Password Service Management Help You are here: > User Management > Add User Local intranet Add User Fields marked with * can not be empty. * User Id: grandsys * Common Name: LOG8000 * Surname: Grandsys * User Password: ●●●●●●●●● * Confirm Password: ●●●●●●●●● Admin Note: Avaya Role: None Business Category: Car License: CM Home: Css Home: CT User: Yes Department Number:

5.2. Verify Avaya Application Enablement Services License

Step	Description
1.	Select **OAM Home**, then click on **CTI OAM Administration** from the left menu (not shown). From the Welcome to CTI OAM screen, verify that the Avaya Application Enablement Services license has proper permissions for the features illustrated in these Application Notes by ensuring both the **DMCC Service** and **TSAPI Service** are licensed. If they are not licensed, then contact the Avaya sales team or business partner for a proper license file. 

Welcome to CTI OAM Screens - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Links Google iFLY MRCP Server
Address https://10.1.10.71/MVAP/forms/cti/ctiHome.jsp
Go
AVAYA
OAM Home Help Logout
CTI OAM Home
Administration
Status and Control
Maintenance
Alarms
Logs
Utilities
Help
Done
Internet

Application Enablement Services
Operations Administration and Maintenance

You are here: > CTI OAM Home

Welcome to CTI OAM Screens

[craft] Last login: Mon Jul 6 12:41:06 2009 from 10.1.10.152

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

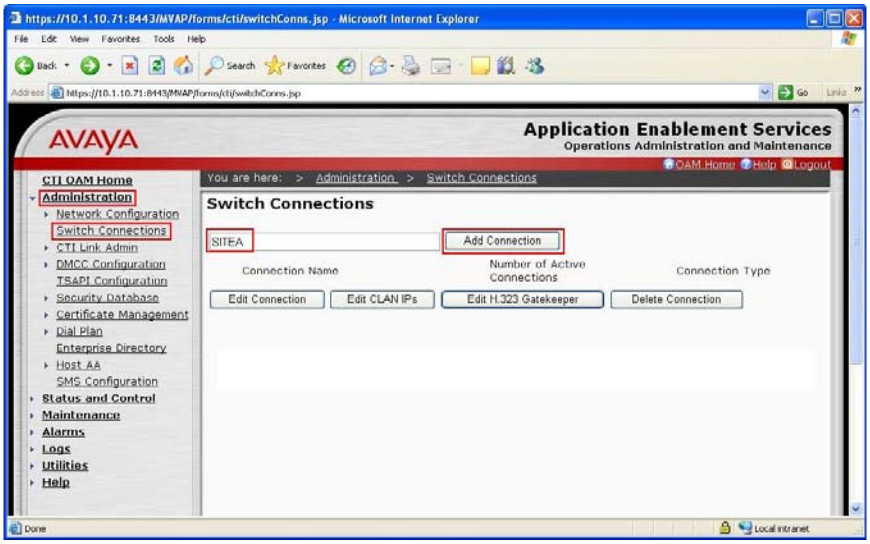
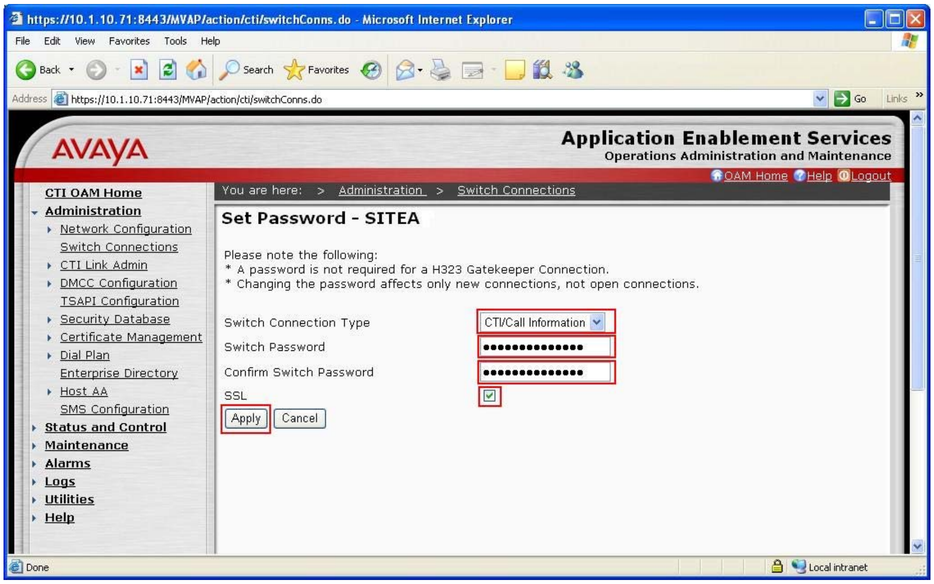
Service	Status	State	Licenses Purchased
ASAI Link Manager	Running	N/A	N/A
DMCC Service	Running	ONLINE	Yes
CVLAN Service	Running	ONLINE	Yes
DLG Service	Running	OFFLINE	Yes
Transport Layer Service	Running	N/A	N/A
TSAPI Service	Running	ONLINE	Yes
SMS	N/A	N/A	Yes

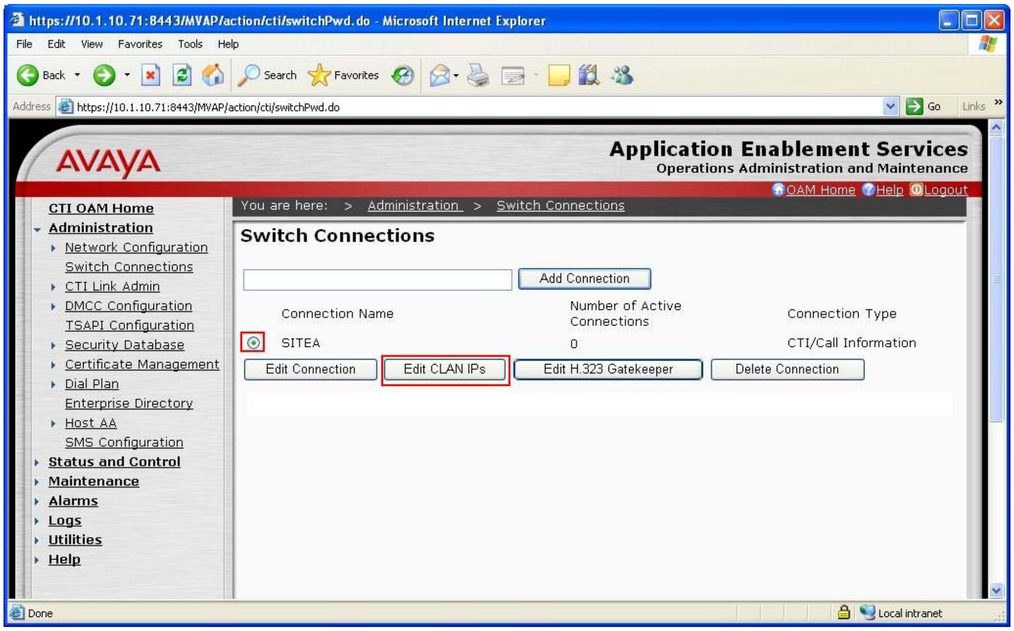
For status on actual services, please use Status and Control.

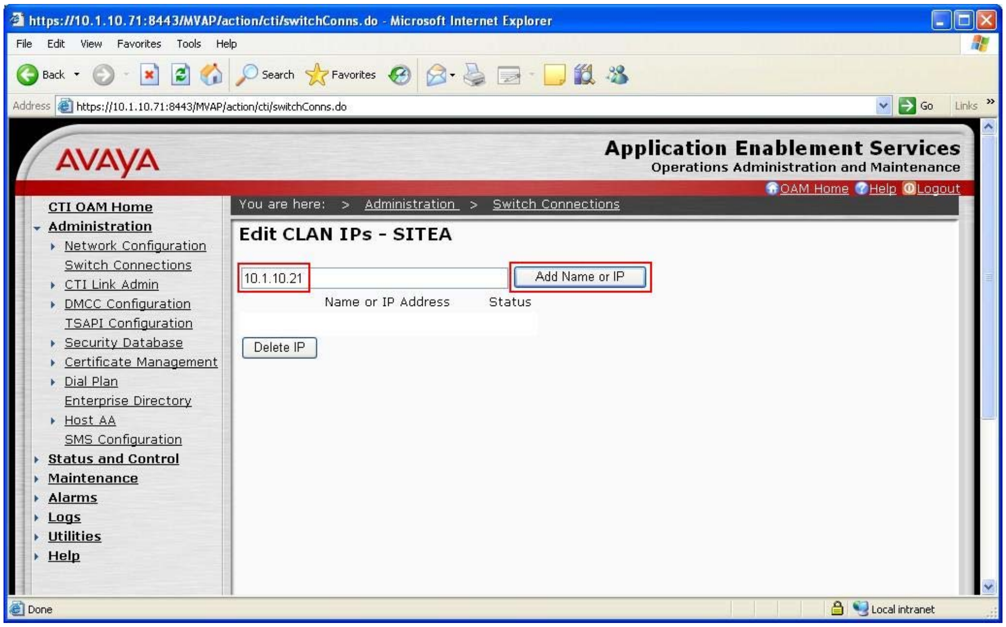
License Information

You are licensed to run Application Enablement (CTI) version 4.2.

5.3. Administer Switch Connection

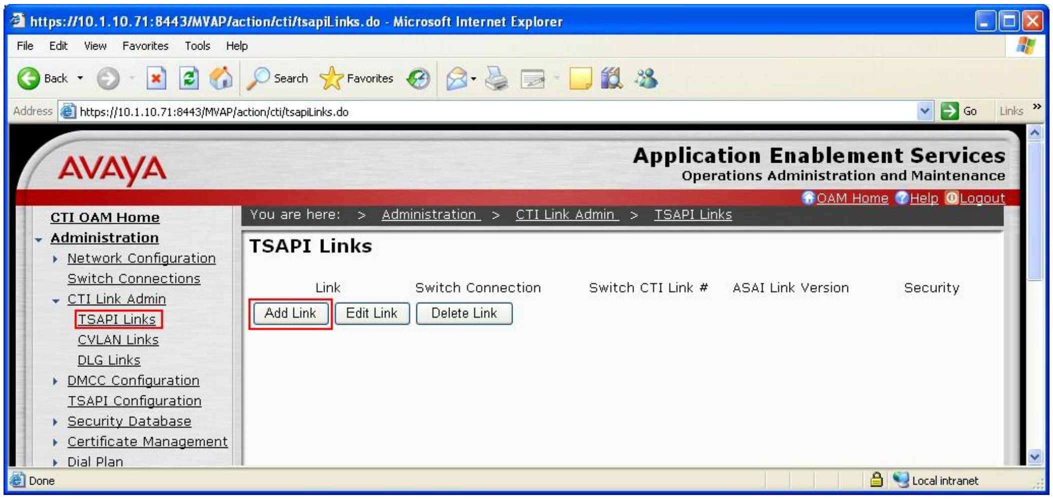
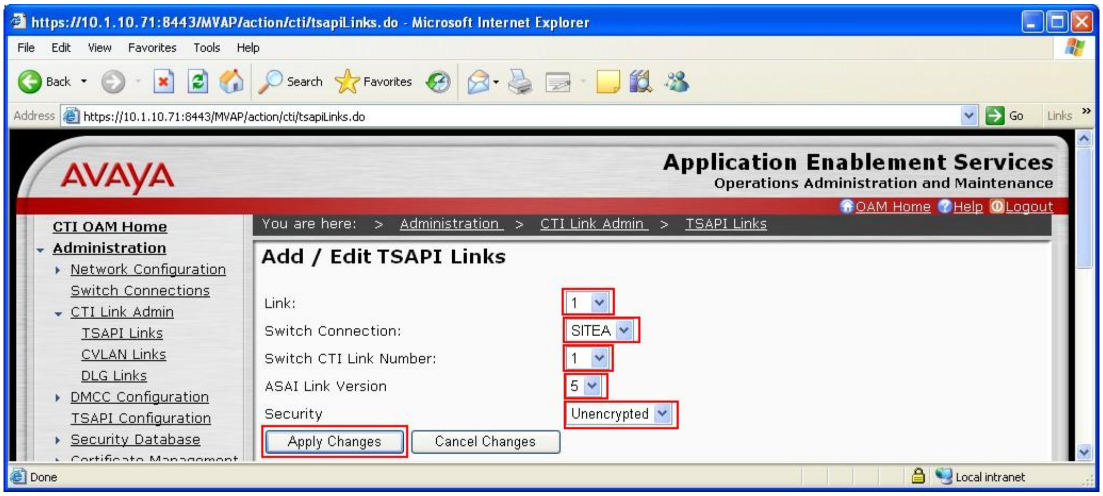
Step	Description
1.	From the CTI OAM Home menu, select **Administration > Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this case, **SITEA** is used.  https://10.1.10.71:8443/MVAP/forms/cti/switchConns.jsp - Microsoft Internet Explorer You are here: > Administration > Switch Connections Switch Connections SITEA File Edit View Favorites Tools Help Back Search Favorites Address https://10.1.10.71:8443/MVAP/forms/cti/switchConns.jsp Go Links AVAYA Application Enablement Services Operations Administration and Maintenance OAM Home Help Logout CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database Certificate Management Dial Plan Enterprise Directory Host AA SMS Configuration Status and Control Maintenance Alarms Logs Utilities Help Add Connection Connection Name Number of Active Connections Connection Type Edit Connection Edit CLAN IPs Edit H.323 Gatekeeper Delete Connection Done Local intranet
2.	The Set Password screen is displayed. Select **CTI/Call Information** for **Switch Connection Type**. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Communication Manager using the IP Services form in **Section 4.3 Step 4**. The **SSL** field needs to be checked for the S8500 Server. Click **Apply**.  https://10.1.10.71:8443/MVAP/action/cti/switchConns.do - Microsoft Internet Explorer You are here: > Administration > Switch Connections Set Password - SITEA Please note the following: * A password is not required for a H323 Gatekeeper Connection. * Changing the password affects only new connections, not open connections. Switch Connection Type: CTI/Call Information Switch Password: •••••••••••••• Confirm Switch Password: •••••••••••••• SSL: ☑ File Edit View Favorites Tools Help Back Search Favorites Address https://10.1.10.71:8443/MVAP/action/cti/switchConns.do Go Links AVAYA Application Enablement Services Operations Administration and Maintenance OAM Home Help Logout CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database Certificate Management Dial Plan Enterprise Directory Host AA SMS Configuration Status and Control Maintenance Alarms Logs Utilities Help Apply Cancel Done Local intranet

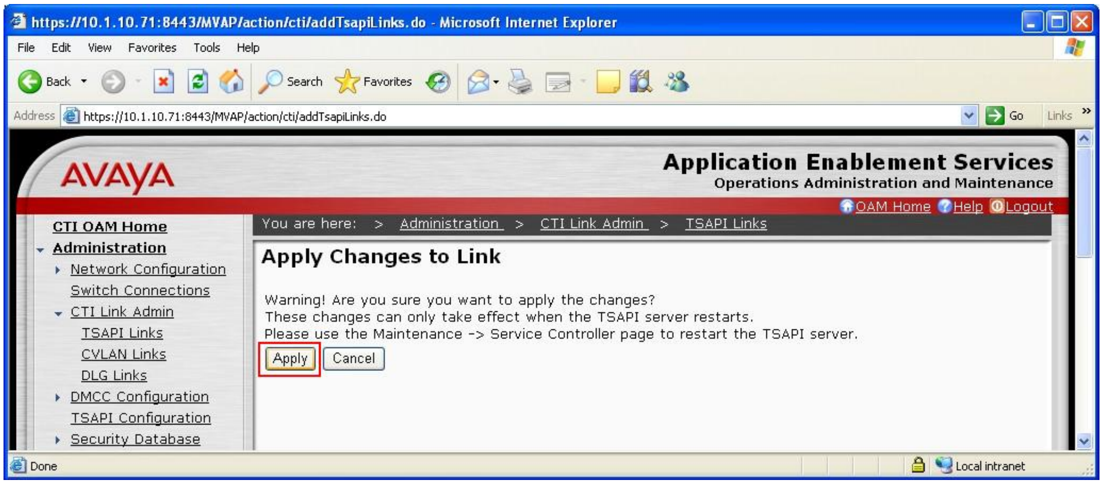
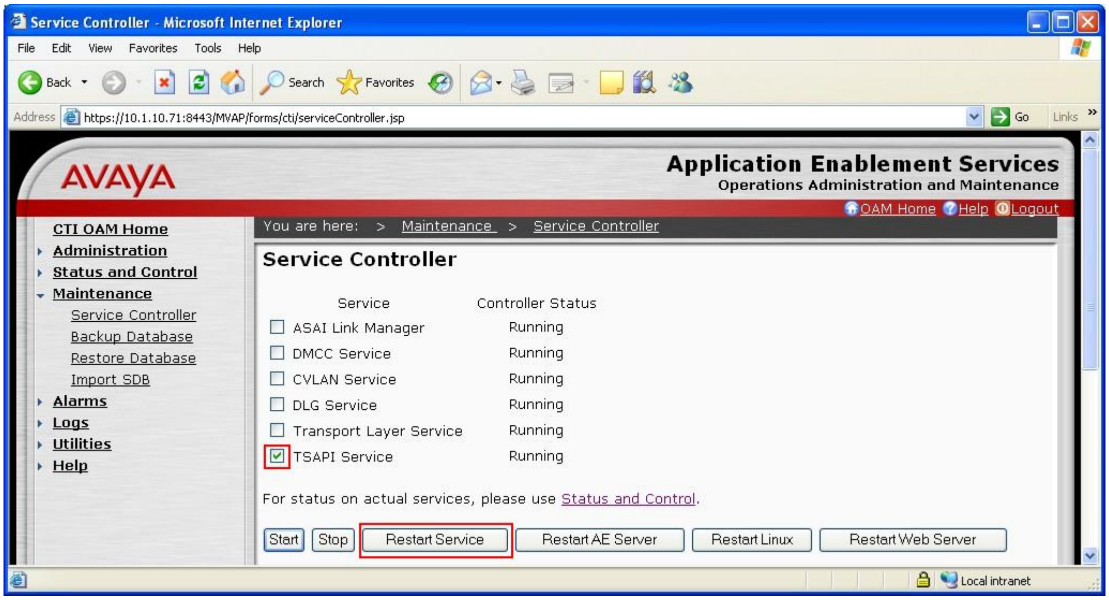
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>The Switch Connections screen is displayed. Select the newly added switch connection name and click **Edit CLAN IPs**.


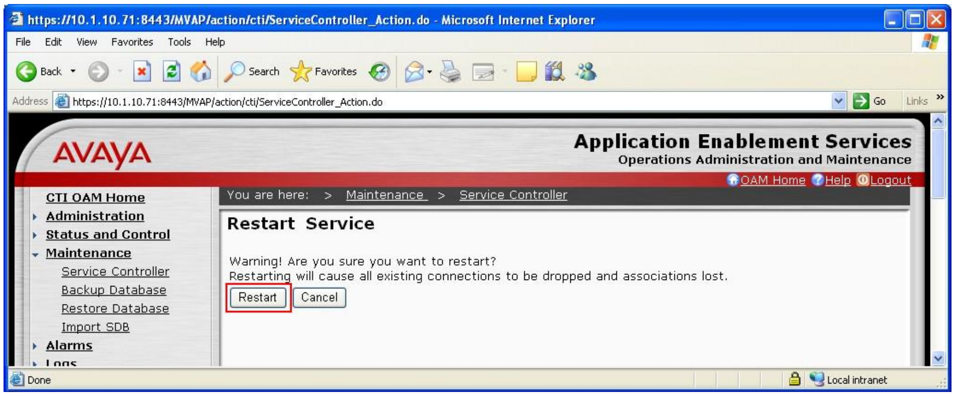
Connection Name: ● SITEA
Number of Active Connections: 0
Connection Type: CTI/Call Information
</td></tr>
<tr><td>4.</td><td>In the Edit CLAN IPs screen, enter the host name or IP address of the C-LAN used for Application Enablement Services connectivity. In this case, **10.1.10.21** is used, which corresponds to the IP address of the C-LAN administered on Communication Manager in **Section 4.3 Step 3**. Click **Add Name or IP**.


10.1.10.21
</td></tr>
</table>

5.4. Administer TSAPI Link

Step	Description
1.	To administer a TSAPI link on AES, select **Administration > CTI Link Admin > TSAPI Links** from the CTI OAM Home menu. Click **Add Link**.  https://10.1.10.71:8443/MVAP/action/cti/tsapiLinks.do - Microsoft Internet Explorer AVAYA Application Enablement Services Operations Administration and Maintenance You are here: > Administration > CTI Link Admin > TSAPI Links TSAPI Links Link Switch Connection Switch CTI Link # ASAI Link Version Security Add Link Edit Link Delete Link
2.	In the Add / Edit TSAPI Links screen, select the following values: • **Link:** Select an available Link number from 1 to 16. • **Switch Connection:** Administered switch connection in **Section 5.3 Step 1**. • **Switch CTI Link Number:** Corresponding CTI link number in **Section 4.3 Step 2**. • **ASAI Link Version:** Set to **5**. • **Security:** **Unencrypted** TSAPI Links are used. Note that the actual values may vary. Click **Apply Changes**.  Add / Edit TSAPI Links Link: 1 Switch Connection: SITEA Switch CTI Link Number: 1 ASAI Link Version 5 Security Unencrypted

Step	Description
	Click **Apply** to confirm the changes.  https://10.1.10.71:8443/MVAP/action/cti/addTsapiLinks.do - Microsoft Internet Explorer Application Enablement Services Operations Administration and Maintenance You are here: > Administration > CTI Link Admin > TSAPI Links Apply Cancel Apply Changes to Link Warning! Are you sure you want to apply the changes? These changes can only take effect when the TSAPI server restarts. Please use the Maintenance -> Service Controller page to restart the TSAPI server.
3.	To restart the TSAPI Service, select **Maintenance > Service Controller** from the CTI OAM Home menu. Check the **TSAPI Service** checkbox and click **Restart Service**.  Service Controller - Microsoft Internet Explorer Application Enablement Services Operations Administration and Maintenance You are here: > Maintenance > Service Controller Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server Service Controller Service Controller Status ☐ ASAI Link Manager Running ☐ DMCC Service Running ☐ CVLAN Service Running ☐ DLG Service Running ☐ Transport Layer Service Running ☑ TSAPI Service Running For status on actual services, please use Status and Control.

Step	Description
	Click **Restart** to confirm the restart. 

https://10.1.10.71:8443/MVAP/action/cti/ServiceController_Action.do - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.1.10.71:8443/MVAP/action/cti/ServiceController_Action.do
AVAYA
OAM Home Help Logout
CTI OAM Home
Administration
Status and Control
Maintenance
Service Controller
Backup Database
Restore Database
Import SDB
Alarms
Logs
Done
Local intranet

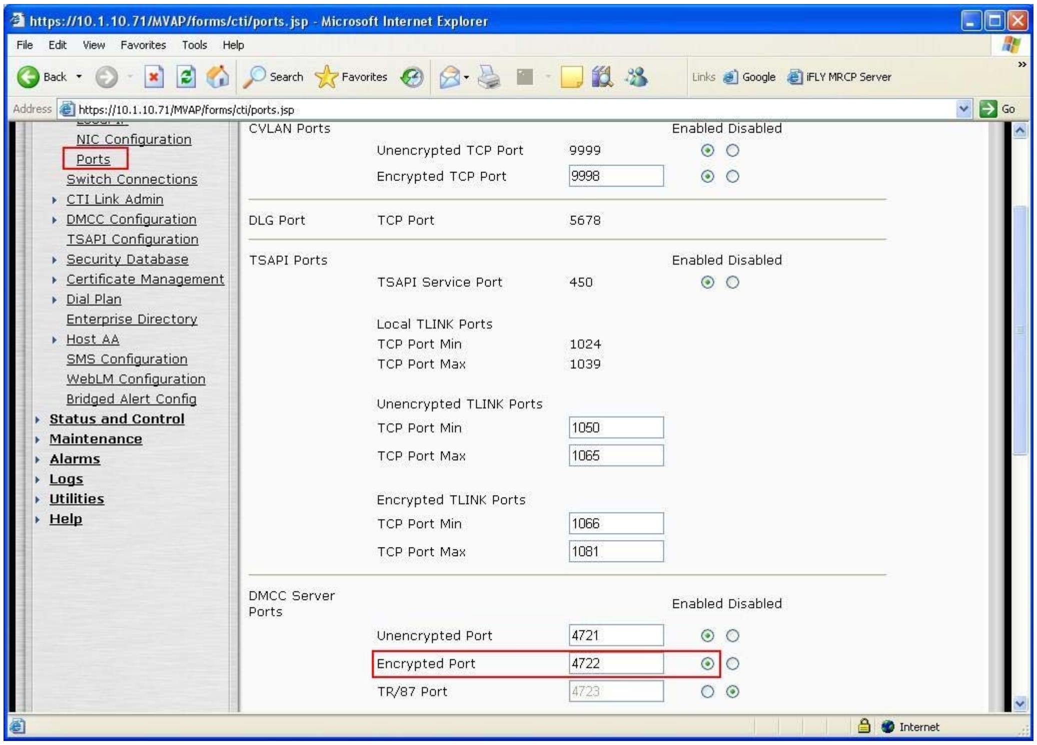
Application Enablement Services
Operations Administration and Maintenance

You are here: > Maintenance > Service Controller

Restart Service

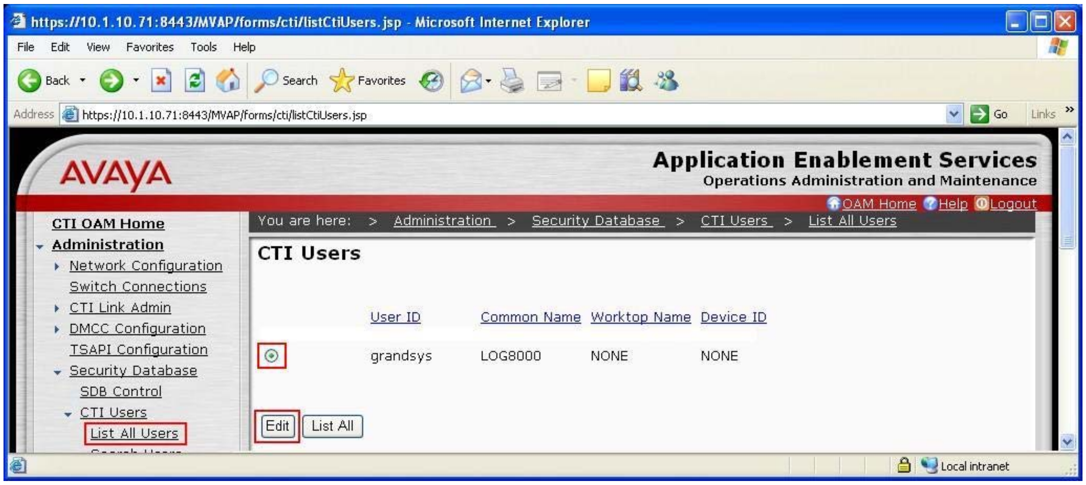
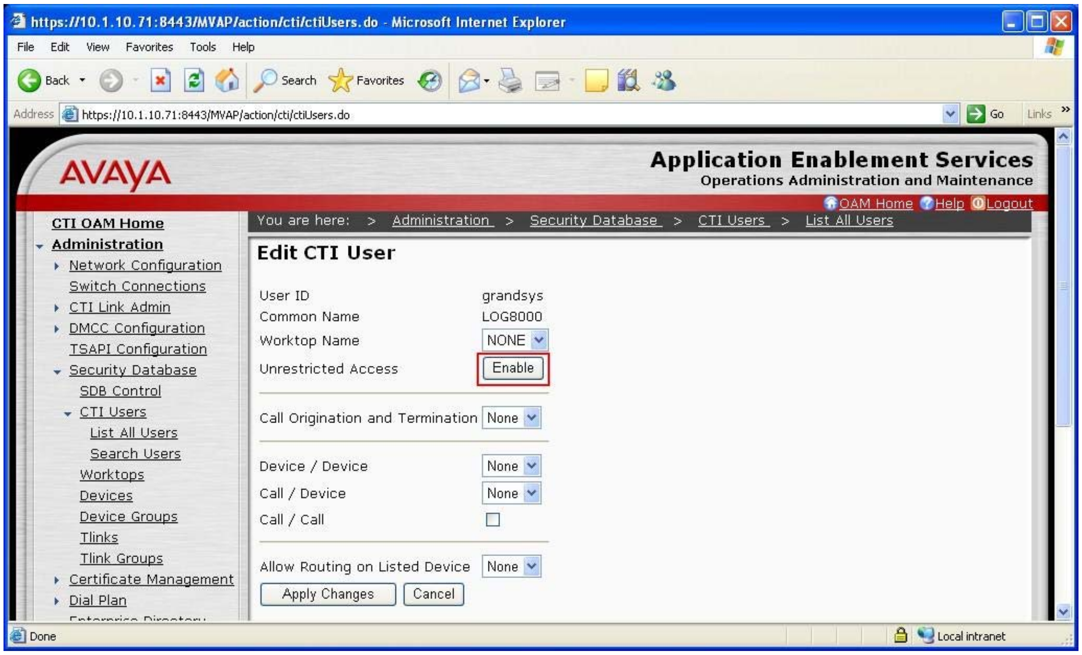
Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

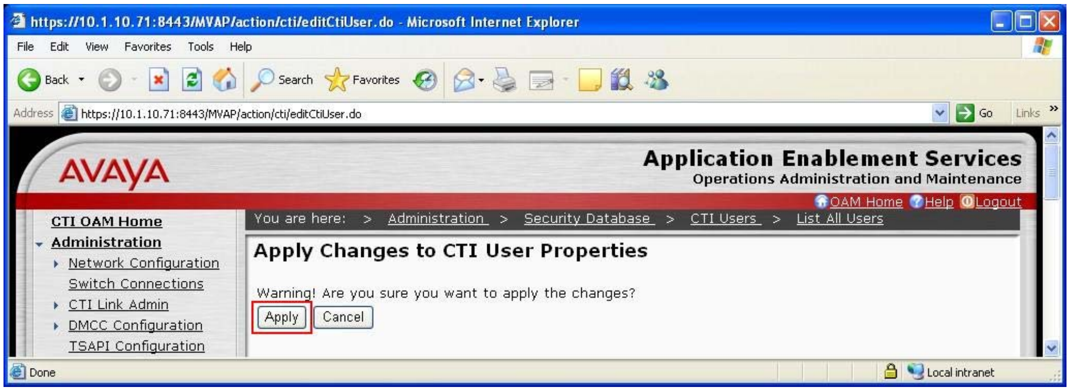
5.5. Administer Ports

Step	Description
1.	Navigate to the **CTI OAM Home > Administration > Network Configuration > Ports** page to set the DMCC Server Ports. During the compliance test, the default port values were utilized as shown below. Since the encrypted port was utilized during the compliance test, set the **Encrypted Port** field to **Enabled**. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process. 

			Enabled	Disabled
CVLAN Ports	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●

5.6. Administer CTI User Permission

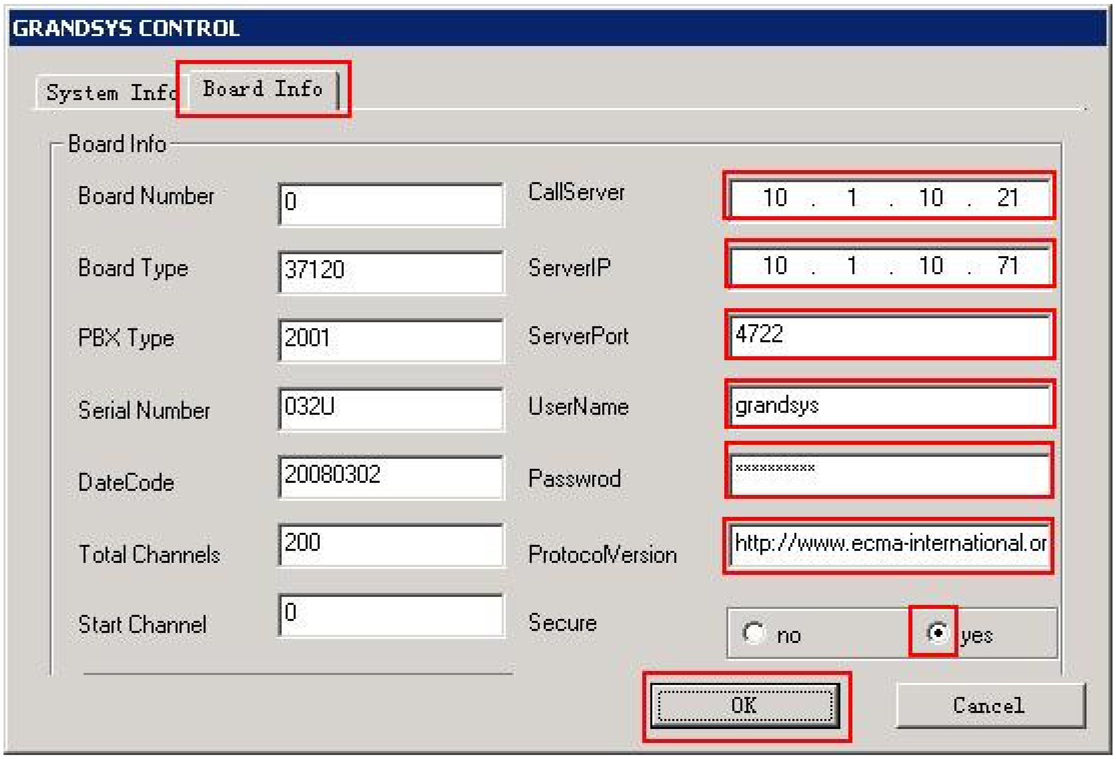
Step	Description
1.	Select **Administration > Security Database > CTI Users > List All Users** from the CTI OAM Home menu. Select the **User ID** created in **Section 5.1 Step 2** and click **Edit**.  https://10.1.10.71:8443/MVAP/forms/cti/listCtiUsers.jsp - Microsoft Internet Explorer Address https://10.1.10.71:8443/MVAP/forms/cti/listCtiUsers.jsp AVAYA Application Enablement Services Operations Administration and Maintenance OAM Home Help Logout You are here: > Administration > Security Database > CTI Users > List All Users CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database SDB Control CTI Users List All Users Local intranet CTI Users User ID | Common Name | Worktop Name | Device ID ◉ grandsys | LOG8000 | NONE | NONE Edit List All
2.	Assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, **Unrestricted Access** was enabled during compliance testing. If **Unrestricted Access** is not desired, then consult [1] for guidance on configuring the call/device privileges as well as devices and device groups. Click **Enable**.  https://10.1.10.71:8443/MVAP/action/cti/ctiUsers.do - Microsoft Internet Explorer Address https://10.1.10.71:8443/MVAP/action/cti/ctiUsers.do AVAYA Application Enablement Services Operations Administration and Maintenance OAM Home Help Logout You are here: > Administration > Security Database > CTI Users > List All Users CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database SDB Control CTI Users List All Users Search Users Worktops Devices Device Groups Tlinks Tlink Groups Certificate Management Dial Plan Done Local intranet Edit CTI User User ID grandsys Common Name LOG8000 Worktop Name NONE Unrestricted Access Enable Call Origination and Termination None Device / Device None Call / Device None Call / Call ☐ Allow Routing on Listed Device None Apply Changes Cancel

Step	Description
	Click **Apply** to apply the changes.  https://10.1.10.71:8443/MVAP/action/cti/editCtiUser.do - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://10.1.10.71:8443/MVAP/action/cti/editCtiUser.do Go Links AVAYA Application Enablement Services Operations Administration and Maintenance OAM Home Help Logout CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration You are here: > Administration > Security Database > CTI Users > List All Users Apply Cancel Done Local intranet **Apply Changes to CTI User Properties** Warning! Are you sure you want to apply the changes?

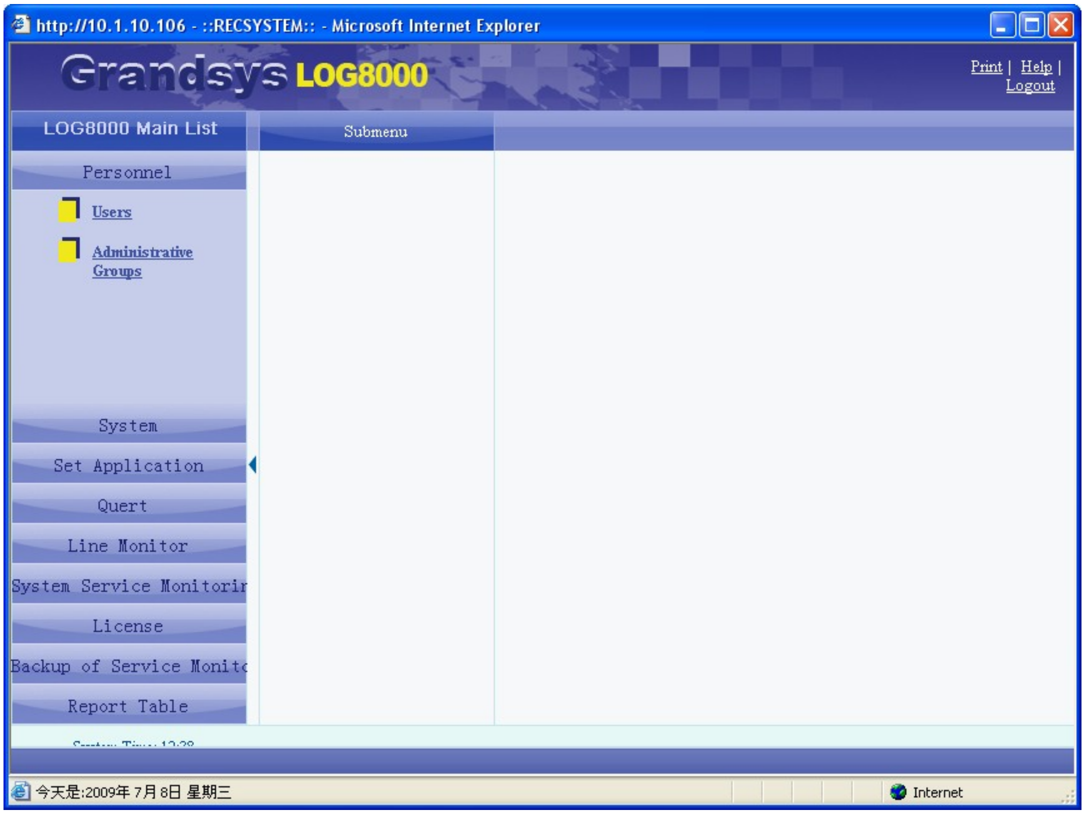
6. Configure Grandsys LOG8000

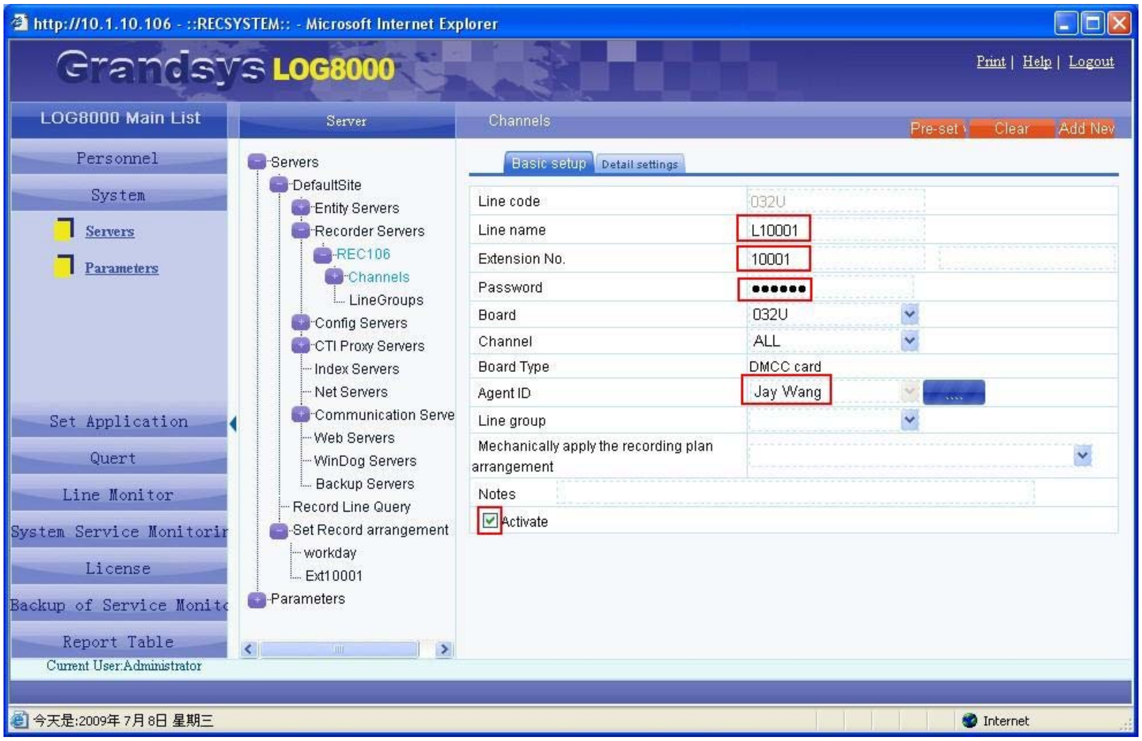
Grandsys installs, configures, and customizes the Grandsys LOG8000 application for their end customers. This section only describes the interface configuration for the Grandsys LOG8000 application to communicate with Application Enablement Services and Communication Manager. Refer to [3] and [4] for configuring the Grandsys LOG8000 application.

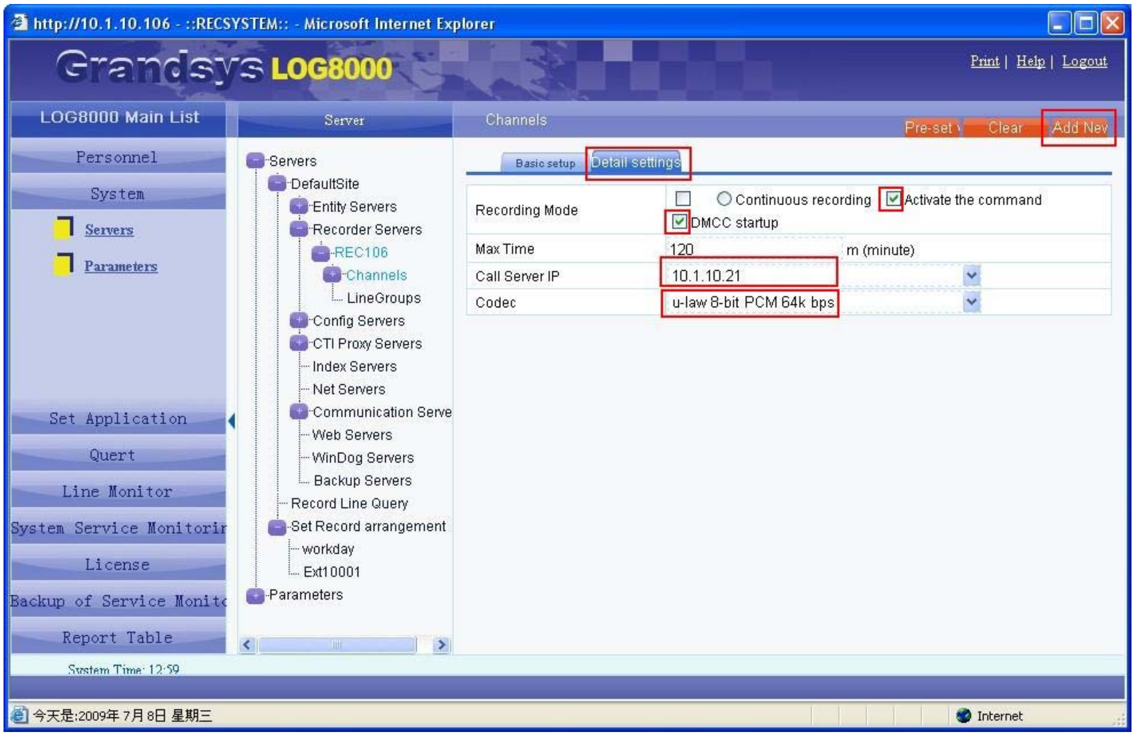
6.1. Configure DMCC Settings

Step	Description
1.	On the Grandsys LOG8000 Server, execute **C:\Program Files\Grandsys Software\Record System\Record Service\Grandsys_Contral.exe** to configure the DMCC settings. Click on the **Board Info** tab and configure the following: • **CallServer**: Set to the C-LAN IP address in **Section 4.3 Step 3** for the registration of the DMCC stations. • **ServerIP**: Set to the IP address of the Application Enablement Services. • **ServerPort**: Set to the encrypted DMCC Server Port in **Section 5.5**. • **UserName**: Set to the **User Id** field in **Section 5.1 Step 2**. • **Password**: Set to the **User Password** field in Section **5.1 Step 2**. • **ProtocolVersion**: Set to the value **http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv3**. • **Secure**: Set to **yes** since encryption is used.  GRANDSYS CONTROL Board Info Board Number: 0 Board Type: 37120 PBX Type: 2001 Serial Number: 032U DateCode: 20080302 Total Channels: 200 Start Channel: 0 CallServer: 10 . 1 . 10 . 21 ServerIP: 10 . 1 . 10 . 71 ServerPort: 4722 UserName: grandsys Passwrod: ********** ProtocolVersion: http://www.ecma-international.or Secure: ○ no ● yes

6.2. Configure Recording Stations

Step	Description
1.	Launch a web browser and enter **http://<IP address of Grandsys LOG8000 Server>/record/** to access the Grandsys LOG8000 web based interface. Log in using an administrative login and password (not shown) and the following screen will be displayed.  http://10.1.10.106 - ::RECSYSTEM:: - Microsoft Internet Explorer Grandsys LOG8000 Print | Help | Logout LOG8000 Main List Submenu Personnel Users Administrative Groups System Set Application Quert Line Monitor System Service Monitorir License Backup of Service Monitc Report Table 今天是:2009年 7月 8日 星期三 Internet

Step	Description
2.	Click **System > Servers** on the left-most pane. To configure the recording stations, expand **Servers > DefaultSite > Recorder Servers > REC106** in the center pane and click on **Channels**. Note: “REC106” is the name defined for this compliance test and will vary. On the right-most pane, enter the following values in the **Basic Setup** tab: • **Line Name**: Enter a descriptive name. • **Extension No.**: Phone extension to be recorded. • **Password**: Enter the Phone **Security Code** configured in **Section 4.4, Step 1**. • **Agent ID**: Select from the list a user configured in Grandsys LOG8000. • **Activate**: Check.  Line code 032U Line name L10001 Extension No. 10001 Password •••••• Board 032U Channel ALL Board Type DMCC card Agent ID Jay Wang Line group Mechanically apply the recording plan arrangement Notes ☑ Activate http://10.1.10.106 - ::RECSYSTEM:: - Microsoft Internet Explorer Grandsys LOG8000 Print | Help | Logout LOG8000 Main List Personnel System Servers Parameters Set Application Quert Line Monitor System Service Monitorir License Backup of Service Monito Report Table Current User:Administrator Server Servers DefaultSite Entity Servers Recorder Servers REC106 Channels LineGroups Config Servers CTI Proxy Servers Index Servers Net Servers Communication Serve Web Servers WinDog Servers Backup Servers Record Line Query Set Record arrangement workday Ext10001 Parameters Channels Pre-set Clear Add New Basic setup Detail settings 今天是:2009年 7月 8日 星期三 Internet

Step	Description
3.	Click the **Detail Settings** tab and configure the following: - **Activate the command**: Check. - **DMCC Startup**: Check. - **Call Server IP**: Select the IP Address of the C-LAN configured in **Section 6.1 Step 1**. - **Codec**: Select the codec to match the one configured on Communication Manager in **Section 4.1**. Click **Add New** to save the settings. Repeat this step for all the agent stations to be recorded. In this configuration, the agent stations 10001 to 10004 are configured.  http://10.1.10.106 - ::RECSYSTEM:: - Microsoft Internet Explorer Grandsys LOG8000 Print | Help | Logout LOG8000 Main List Personnel System Servers Parameters Set Application Quert Line Monitor System Service Monitorir License Backup of Service Monitc Report Table System Time: 12:59 Server Servers DefaultSite Entity Servers Recorder Servers REC106 Channels LineGroups Config Servers CTI Proxy Servers Index Servers Net Servers Communication Serve Web Servers WinDog Servers Backup Servers Record Line Query Set Record arrangement workday Ext10001 Parameters Channels Pre-set Clear Add New Basic setup Detail settings 今天是:2009年 7月 8日 星期三 Internet Recording Mode: ☐ ○ Continuous recording ☑ Activate the command ☑ DMCC startup Max Time: 120 m (minute) Call Server IP: 10.1.10.21 Codec: u-law 8-bit PCM 64k bps

7. General Test Approach and Test Results

The general approach was to place various types of calls to and from stations, agents, and Vector Directory Numbers (VDNs), monitor and record the calls using Grandsys LOG8000, and verify the recordings. For feature testing, the types of calls included internal calls, inbound and outbound trunk calls, transferred calls, and conferenced calls. For serviceability testing, failures such as disconnecting the LAN cable to the Grandsys LOG8000 Server and Application Enablement Services, and resetting the Grandsys LOG8000 Server and Communication Manager were applied.

All test cases were executed and passed.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services and Grandsys LOG8000.

8.1. Verify Communication Manager

Verify the status of the administered AE Services Link by using the **status aesvcs link** command. The following shows that the link between the Application Enablement Services and the Communication Manager C-LAN is up.

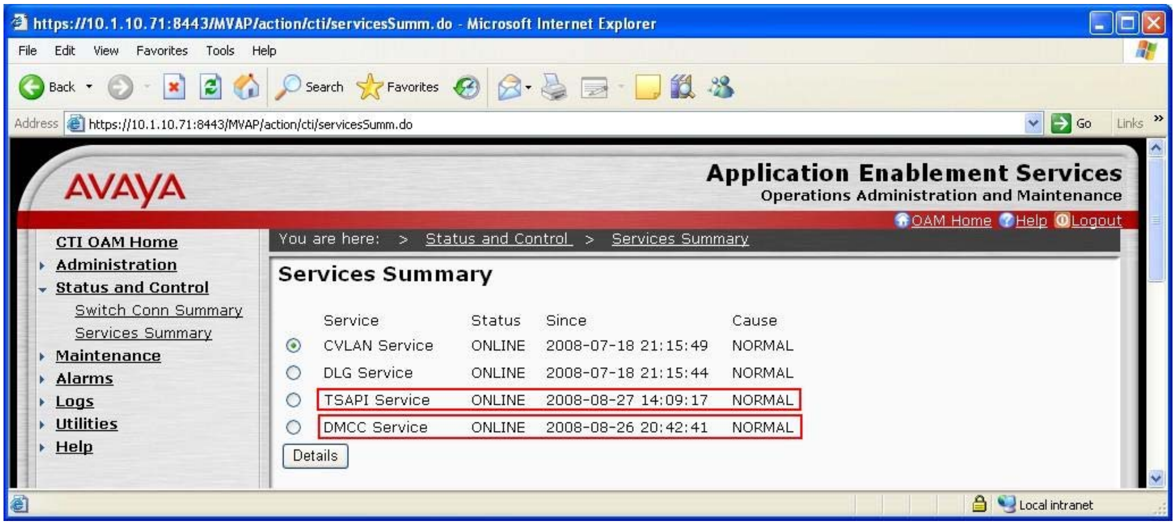
```
status aesvcs link

                            AE SERVICES LINK STATUS

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

01/01  aes1             10.  1. 10. 71  32856   s8500-clan1     226     211
```

Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command. The **Service State** field should display **established**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     5        no    aes1             established   33       45
```

8.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services by selecting **Status and Control > Services Summary** from the left pane. The **Status** field for both **TSAPI Service** and **DMCC Service** should display **ONLINE**.


https://10.1.10.71:8443/MVAP/action/cti/servicesSumm.do - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address https://10.1.10.71:8443/MVAP/action/cti/servicesSumm.do
Go
Links
AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home
Help
Logout
CTI OAM Home
Administration
Status and Control
Switch Conn Summary
Services Summary
Maintenance
Alarms
Logs
Utilities
Help
You are here: > Status and Control > Services Summary
Details
Local intranet

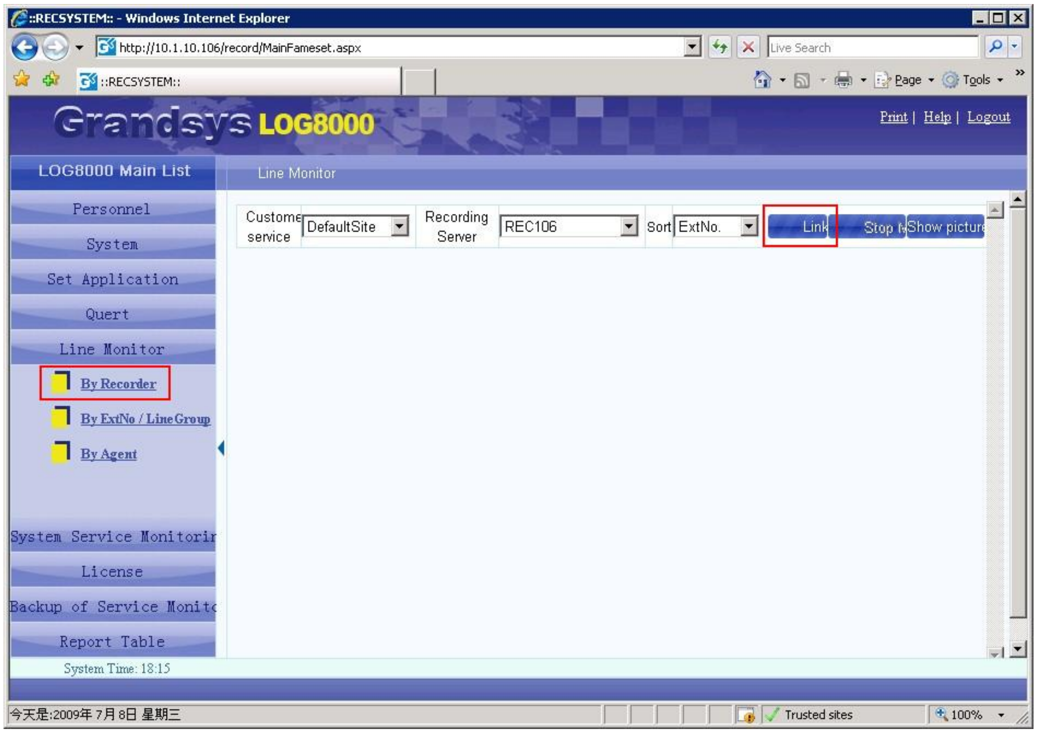
Services Summary

	Service	Status	Since	Cause
●	CVLAN Service	ONLINE	2008-07-18 21:15:49	NORMAL
○	DLG Service	ONLINE	2008-07-18 21:15:44	NORMAL
○	TSAPI Service	ONLINE	2008-08-27 14:09:17	NORMAL
○	DMCC Service	ONLINE	2008-08-26 20:42:41	NORMAL

8.3. Verify Grandsys LOG8000

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

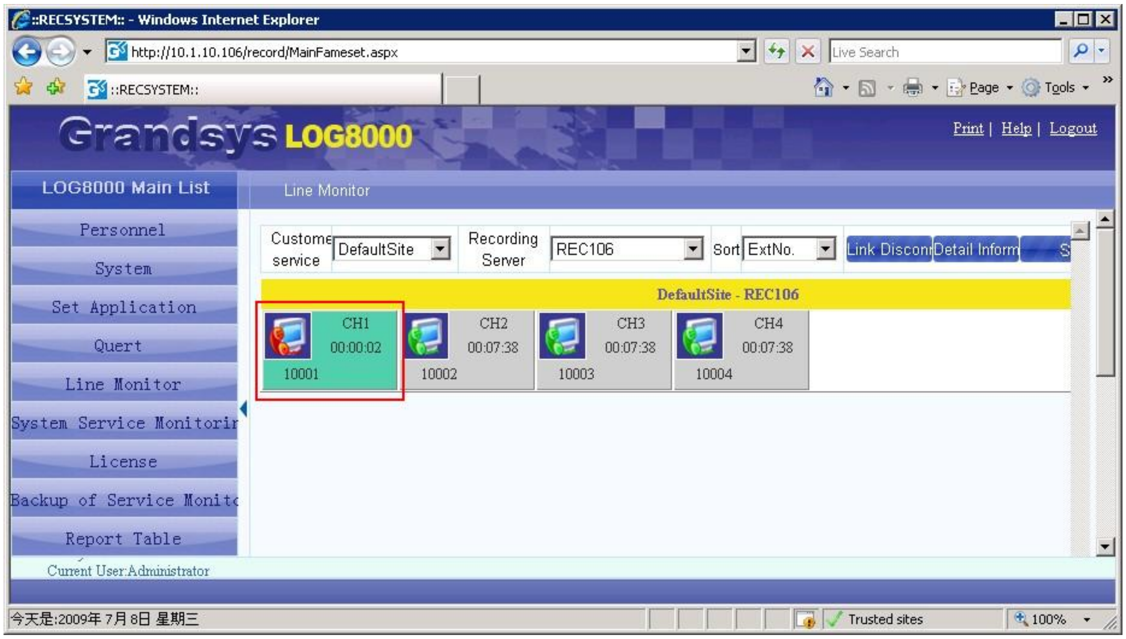
From the Grandsys LOG8000 Server, launch a web browser and log in to the Grandsys LOG8000 web based interface. Select **Line Monitoring > By Recorder** on the left pane and click **Link Connect** on the right pane.



Customer service: DefaultSite
Recording Server: REC106
Sort: ExtNo.

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>Place a test call to an extension being recorded and verify that one of the recording stations on Grandsys LOG8000 becomes active as it records the call.



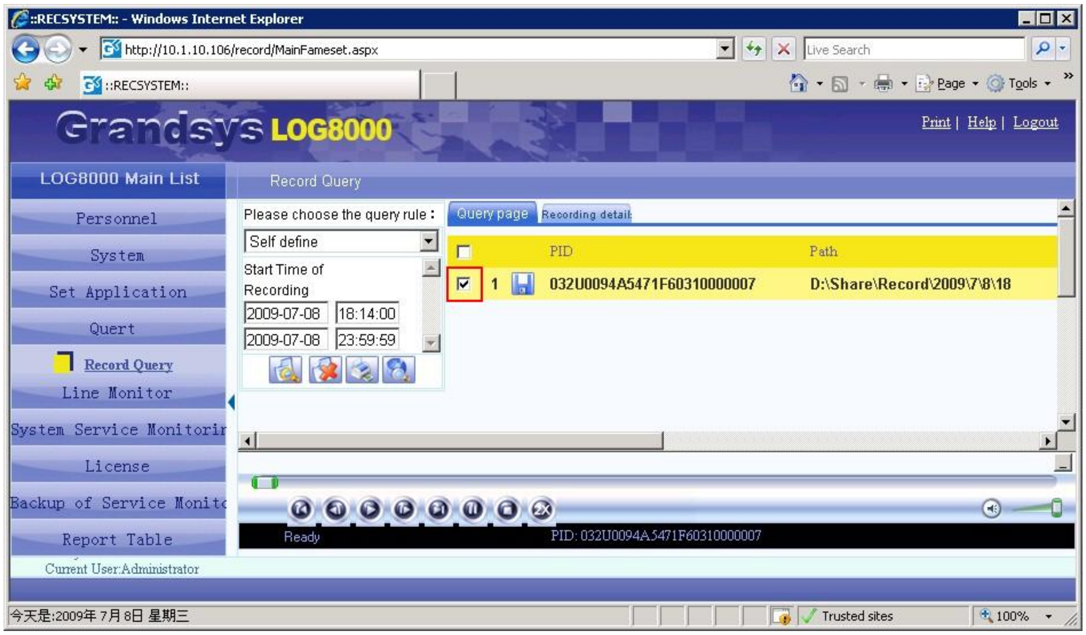
Customer service: DefaultSite
Recording Server: REC106
Sort: ExtNo.

DefaultSite - REC106

CH1 00:00:02 10001
CH2 00:07:38 10002
CH3 00:07:38 10003
CH4 00:07:38 10004

Current User:Administrator

今天是:2009年 7月 8日 星期三</td></tr>
<tr><td>3.</td><td>Query for the recording of the test call. Verify that the recording can be played back correctly.



Please choose the query rule : Self define
Start Time of Recording
2009-07-08 18:14:00
2009-07-08 23:59:59

☐			PID	Path
☑	1		032U0094A5471F60310000007	D:\Share\Record\2009\7\8\18

Ready
PID: 032U0094A5471F60310000007

Current User:Administrator

今天是:2009年 7月 8日 星期三</td></tr>
</table>

9. Conclusion

These Application Notes illustrate the procedures for configuring Grandsys LOG8000 to monitor and record calls placed to and from stations and VDNs on Avaya Aura™ Communication Manager. In the configuration described in these Application Notes, Grandsys LOG8000 uses the DMCC Service of Avaya Aura™ Application Enablement Services to perform recording. All test cases were completed successfully.

10. Additional References

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

The following Avaya product documentation can be found at http://support.avaya.com .
[1] *Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide*, Release 4.2, Document ID 02-300357, Issue 10, May 2008.
[2] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Issue 7, May 2009, Document Number 555-245-205.

The following product documentation are available from Grandsys.
[3] *Grandsys LOG8000 System Installation Manual*, Version 2.2.2, May 2009.
[4] *Grandsys LOG8000 System Operation Manual*, Version 2.2.2, May 2009.

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.