



Avaya Solution & Interoperability Test Lab

Application Notes for HigherGround Praetorian with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring HigherGround Praetorian to monitor and record calls through a trunk. Recording calls were accomplished by tapping a trunk. In the configuration discussed in these Application Notes, HigherGround Praetorian employs Telephony Services Application Programming Interface (TSAPI) for monitoring call events. During the compliance test, HigherGround Praetorian successfully recorded calls placed to and from stations via an IP trunk, as well as calls placed to a VDN and then queued to an agent hunt/skill group.

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 Avaya Communication Managers, an Avaya Application Enablement Services (AES) and HigherGround Praetorian. HigherGround Praetorian can record a trunk and/or stations. Recording calls were accomplished by tabbing a trunk. In the configuration discussed in these Application Notes, HigherGround Praetorian employs TSAPI for monitoring and call events. During compliance testing, HigherGround Praetorian successfully recorded calls placed to and from stations, as well as calls placed to a VDN and then queued to an agent hunt/skill group.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide an IP trunk between two Avaya Communication Manager Systems.

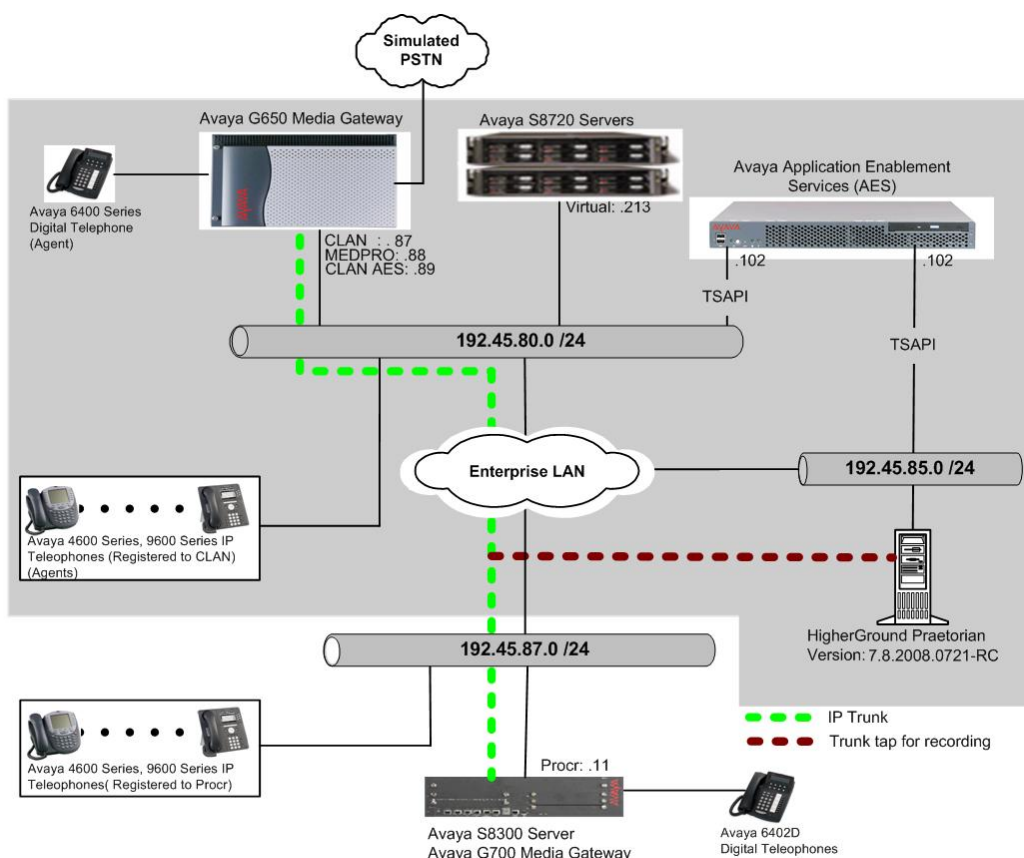


Figure 1: Sample Test Configuration for the HigherGround Praetorian Solution

2. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Server		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface	HW11 FW044
	TN799DP C-LAN Interface	HW01 FW028
	TN2302AP IP Media Processor	HW20 FW118
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya Application Enablement Services Server		4.2 (R4.2.0.19.4)
Avaya 4600 Series IP Telephones		
	4620SW (H.323)	2.8.3
	4625SW (H.323)	2.8.3
Avaya 9600 Series IP Telephones		
	9630 (H.323)	1.5
	9650 (H.323)	1.5
Avaya 6408D+ Digital Telephone		-
Analog Telephones		-
HigherGround Praetorian on Windows Microsoft 2003 Server with Service Pack 2		7.8.2008.0721-RC

3. Configure Avaya Communication Manager

This section provides the procedures for configuring a TSAPI Computer Telephony Integration (CTI) link, hunt/skill groups, vectors, Vector Directory Numbers (VDN), agents, agent login/logoff codes, and recording ports on Avaya Communication Manager. All the configuration changes in Avaya 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.

3.1. Configure TSAPI CTI Link between Avaya Communication Manager and Avaya Application Enablement Services Server

The Avaya AES server forwards CTI requests, responses, and events between HigherGround Praetorian and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as HigherGround Praetorian. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI links. See **Section 4** for the details of configuring the AES side of the AES and CTI links.

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

add cti-link 4		Page 1 of 2
CTI LINK		
CTI Link: 4		
Extension: 20006		
Type: ADJ-IP		
Name: TSAPI		COR: 1

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoint (Avaya IP Telephones and IP Agent) 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	
procr	192.45.80.214	

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 Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 running the command **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 Server	Password	Enabled	Status	
1:	server1	xxxxxxxxxxxxxxxxxx	y		
2:					
3:					

3.2. Configure Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the **display system-parameters customer-options** command. On **Page 6**, verify that the ACD, Expert Agent Selection (EAS) and Vectoring (Basic) fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 3.0		
ACD? y	Reason Codes? n	
BCMS (Basic)? y	Service Level Maximizer? n	
BCMS/VuStats Service Level? n	Service Observing (Basic)? y	
BSR Local Treatment for IP & ISDN? n	Service Observing (Remote/By FAC)? y	
Business Advocate? n	Service Observing (VDNs)? n	
Call Work Codes? n	Timed ACW? N	
DTMF Feedback Signals For VRU? n	Vectoring (Basic)? y	
Dynamic Advocate? n	Vectoring (Prompting)? n	
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? n	
EAS-PHD? n	Vectoring (3.0 Enhanced)? n	
Forced ACD Calls? n	Vectoring (ANI/II-Digits Routing)? n	
Least Occupied Agent? n	Vectoring (G3V4 Advanced Routing)? n	
Lookahead Interflow (LAI)? n	Vectoring (CINFO)? n	
Multiple Call Handling (On Request)? n	Vectoring (Best Service Routing)? n	
Multiple Call Handling (Forced)? n	Vectoring (Holidays)? n	
PASTE (Display PBX Data on Phone)? n	Vectoring (Variables)? n	
(NOTE: You must logoff & login to effect the permission changes.)		

Once the Expert Agent Selection (EAS) field is set to **y**, from the previous step, enter the **change system-parameters features** command. On **Page 11**, verify that the Expert Agent Selection (EAS) Enabled field is set to **y**. To enable the EAS feature, the Expert Agent Selection field in both the system-parameters customer-options form and the system-parameters features form should be set to **y**.

change system-parameters features		Page 11 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
CALL CENTER SYSTEM PARAMETERS		
EAS		
Expert Agent Selection (EAS) Enabled? y		
Minimum Agent-LoginID Password Length:		Delay:
Direct Agent Announcement Extension:		
Message Waiting Lamp Indicates Status For: station		
VECTORIZING		
Converse First Data Delay: 0		Second Data Delay: 2
Converse Signaling Tone (msec): 100		Pause (msec): 30
Prompting Timeout (secs): 10		
Reverse Star/Pound Digit For Collect Step? n		
Store VDN Name in Station's Local Call Log? y		
SERVICE OBSERVING		
Service Observing: Warning Tone? y		or Conference Tone? n
Service Observing Allowed with Exclusion? n		
Allow Two Observers in Same Call? y		

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the HUNT GROUP form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan. Set the ACD, Queue, and Vector fields to **y**. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.

add hunt-group 1		Page 1 of 3	
HUNT GROUP			
Group Number: 1		ACD? y	
Group Name: test		Queue? y	
Group Extension: 50011		Vector? y	
Group Type: ucd-mia			
TN: 1			
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display:			
Queue Limit: unlimited			
Calls Warning Threshold:	Port:		
Time Warning Threshold:	Port:		

On **Page 2**, set the Skill field to **y**, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

add hunt-group 1		Page 2 of 3	
HUNT GROUP			
Skill? y			
AAS? n			
Measured: internal			
Supervisor Extension:			
Controlling Adjunct: none			
VuStats Objective:			
Redirect on No Answer (rings):			
Redirect to VDN:			
Forced Entry of Stroke Counts or Call Work Codes? n			

Enter the **add agent-loginID p** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1** of the AGENT LOGINID form, enter a descriptive Name and valid Password.

add agent-loginID 50021		Page 1 of 2	
AGENT LOGINID			
Login ID: 50021	AAS? n		
Name: Agent-1	AUDIX? n		
TN: 1	LWC Reception: spe		
COR: 1	LWC Log External Calls? n		
Coverage Path:	AUDIX Name for Messaging:		
Security Code:	LoginID for ISDN/SIP Display? n		
	Password:		
	Password (enter again):		
	Auto Answer: station		
	MIA Across Skills: system		
	ACW Agent Considered Idle: system		
	Aux Work Reason Code Type: system		
	Logout Reason Code Type: system		
	Maximum time agent in ACW before logout (sec): system		
	Forced Agent Logout Time: :		
WARNING: Agent must log in again before changes take effect			

On Page 2, set the SN (Skill Number) field to the hunt group number previously created. The SL (Skill Level) field may be set according to customer requirements. Repeat this step as necessary to configure additional agent extensions.

add agent-loginID 50021		Page 2 of 2	
AGENT LOGINID			
Direct Agent Skill:		Local Call Preference? n	
Call Handling Preference: skill-level			
SN	SL	SN	SL
1: 1	1	16:	
2:		17:	
3:		18:	
		31:	
		32:	
		33:	
		46:	
		47:	
		48:	

Enter the **change vector q** command, where **q** is an unused vector number. Enter a descriptive Name for the vector, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

change vector 1		Page 1 of 3	
CALL VECTOR			
Number: 1	Name: Queue to skill1		
	Meet-me Conf? n		
	Lock? n		
Basic? y	EAS? y	G3V4 Enhanced? n	ANI/II-Digits? n
Prompting? n	LAI? n	G3V4 Adv Route? n	ASAI Routing? y
Variables? n	3.0 Enhanced? n	CINFO? n	BSR? n
			Holidays? n
01 wait-time	2	secs	hearing ringback
02 queue-to	skill 1	pri	m

Enter the **add vdn r** command, where **r** is an unused extension valid in the provisioned dial plan. Specify a descriptive Name for the VDN and the **Vector Number** configured in the previous step. In the example below, incoming calls to the extension 50000 will be routed to **testVDN50000**, which in turn will invoke the actions specified in vector 1.

```

add vdn 50000                                     Page 1 of 2
                                         VECTOR DIRECTORY NUMBER

                                         Extension: 50000
                                         Name*: testVDN50000
                                         Vector Number: 1

Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none

1st Skill*:
2nd Skill*:
3rd Skill*:

```

Enter the **change feature-access-codes** command. Define the Auto-In Access Code, **Aux Work Access Code**, Login Access Code, and Logout Access Code.

```

change feature-access-codes                       Page 5 of 6
                                         FEATURE ACCESS CODE (FAC)

                                         Automatic Call Distribution Features

                                         After Call Work Access Code: 120
                                         Assist Access Code: 121
                                         Auto-In Access Code: 122
                                         Aux Work Access Code: 123
                                         Login Access Code: 124
                                         Logout Access Code: 125
                                         Manual-in Access Code: 126
                                         Service Observing Listen Only Access Code: 127
                                         Service Observing Listen/Talk Access Code: 128
                                         Add Agent Skill Access Code: 130
                                         Remove Agent Skill Access Code: 131
                                         Remote Logout of Agent Access Code: 132

```

Enter the **add abbreviated-dialing group g** command, where **g** is the number of an available abbreviated dialing group. In the DIAL CODE list, enter the Feature Access Codes, created previously, for ACD Login and Logout.

```

add abbreviated-dialing group 1                 Page 1 of 1
                                         ABBREVIATED DIALING LIST

                                         Group List: 1           Group Name: Call Center
                                         Size (multiple of 5): 5   Program Ext:           Privileged? n
DIAL CODE
11: 124
12: 125

```


3.3. Configure Monitored Stations

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, enter a descriptive Name, and specify the Security Code. For the compliance test, recorded stations from 22001 to 22009 were created. For the performance test, stations from 21101 to 21123 were created. These stations were configured as analog (2500 Series) telephones, and auto answer and auto termination were set.

add station 22001		Page 1 of 4	
STATION			
Extension: 22001	Lock Messages? n	BCC: 0	
Type: 4621	Security Code: *	TN: 1	
Port: S00142	Coverage Path 1:	COR: 1	
Name: 72001	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 19	Time of Day Lock Table:		
	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? n		
Customizable Labels? y			

On **Page 3** of the STATION form, for ABBREVIATED DIALING List2, enter the abbreviated dialing group configured in **Section 3.2**. Configure the following BUTTON ASSIGNMENTS in addition to the call-appr (call appearance) buttons:

- auto-in
- aux-work
- abrv-dial – for Login
- abrv-dial – for Logout.

add station 22001		Page 3 of 4	
STATION			
SITE DATA			
Room:	Headset? n		
Jack:	Speaker? n		
Cable:	Mounting: d		
Floor:	Cord Length: 0		
Building:	Set Color:		
ABBREVIATED DIALING			
List1: personal 1	List2: group 1	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	5: auto-in	Grp:	
2: call-appr	6: aux-work	RC:	Grp:

3: call-app
4:

7: abrv-dial List: 2 DC: 11
8: abrv-dial List: 2 DC: 12

4. Configure Avaya Application Enablement Services

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

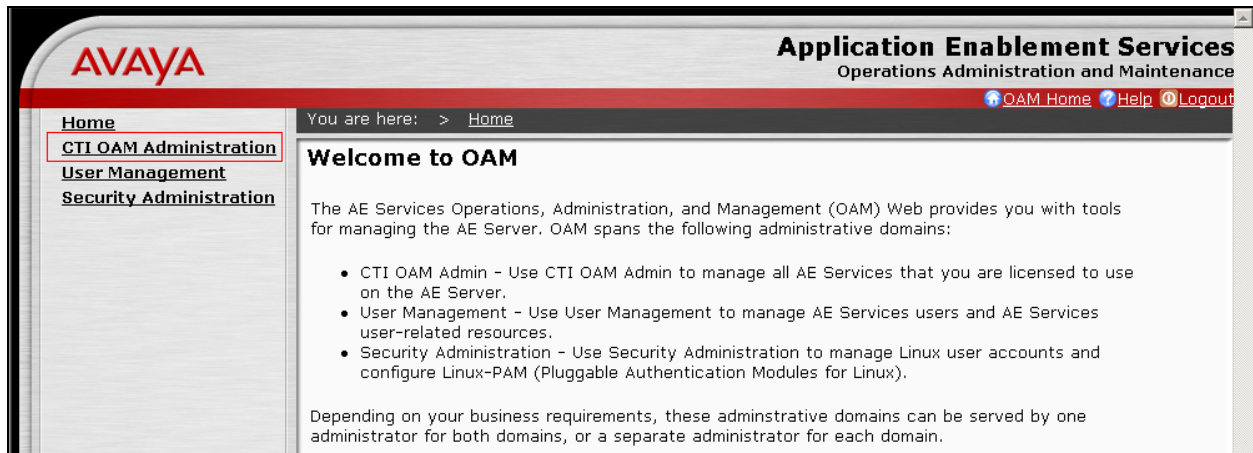
This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a CMAPI port, and creating a CTI link for TSAPI.

4.1. Configure Switch Connection

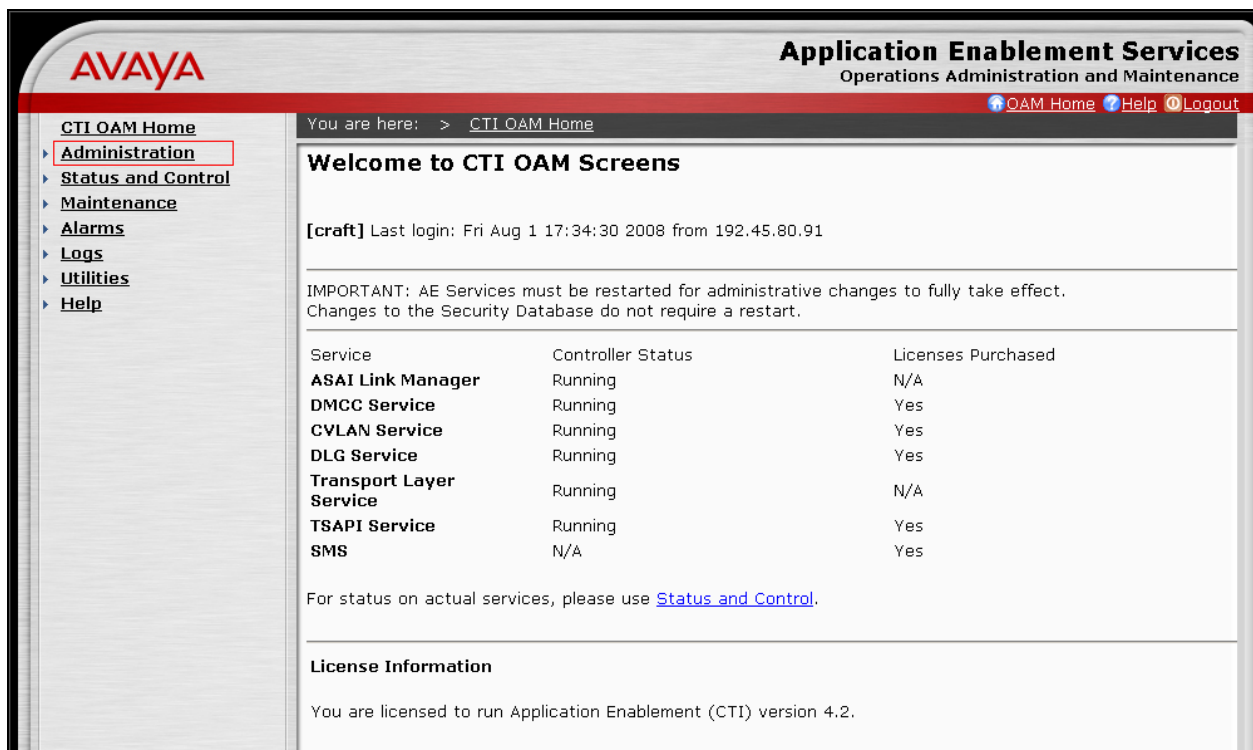
Launch a web browser, enter <https://<IP address of AES server>:8443/MVAP> in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.



Select the **CTI OAM Administration** 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**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

Switch Connections

Connection Name Number of Active Connections

The next window that appears prompts for the Switch Password. Enter the same password that was administered in Avaya Communication Manager in **Section 3.1**. Default values may be used in the remaining fields. Click on **Apply**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

Set Password - S8720

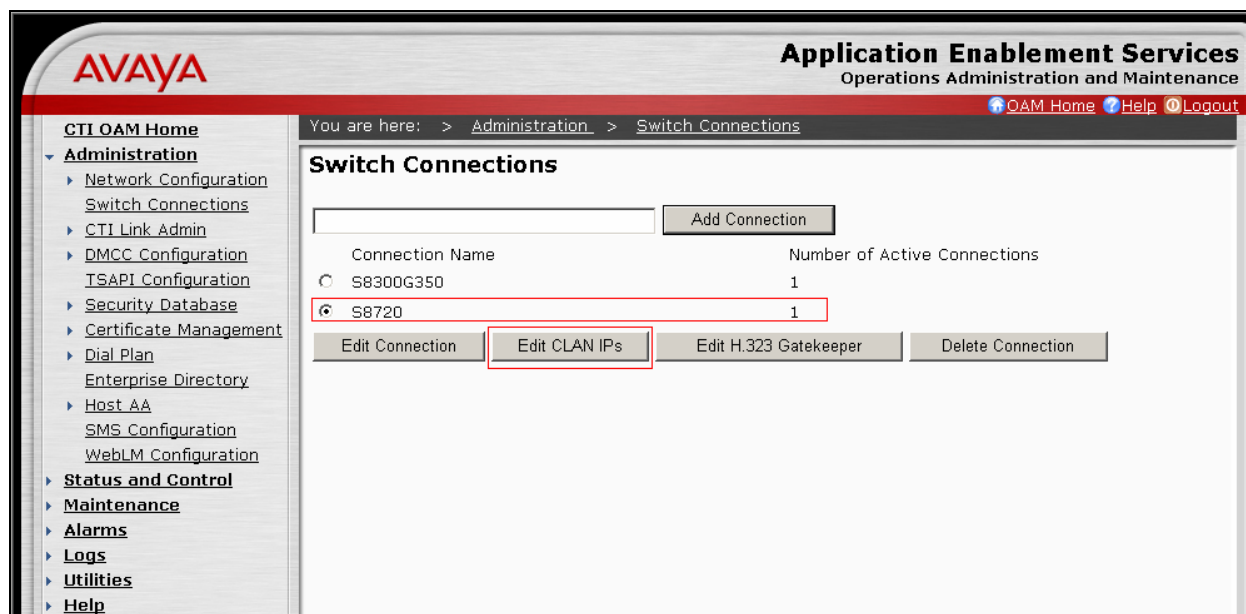
Please note the following:
* Changing the password affects only new connections, not open connections.

Switch Password

Confirm Switch Password

SSL ☒

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 CLAN-AES IP address which was configured for AES connectivity in **Section 3.1** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

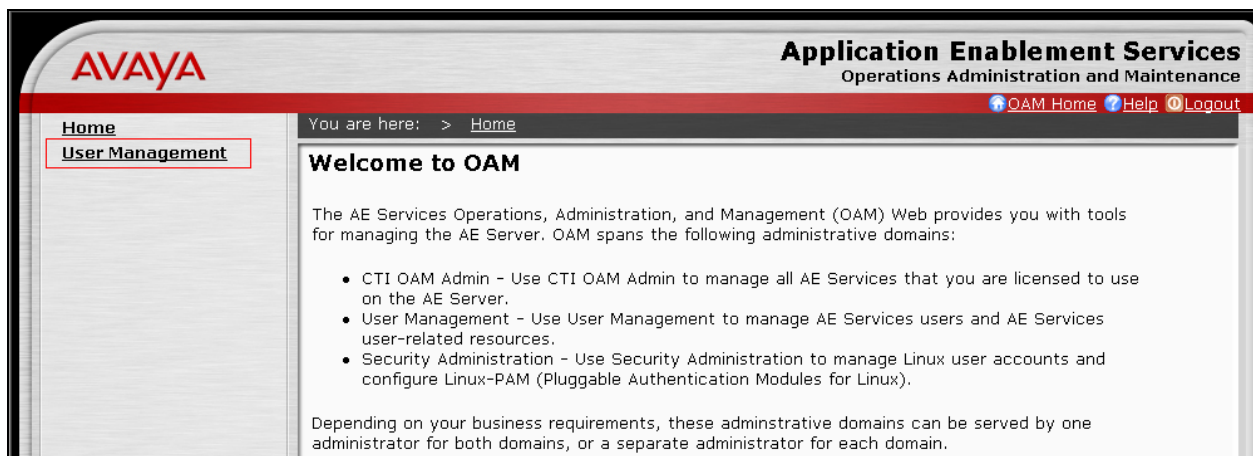


4.2. Configure the CTI Users

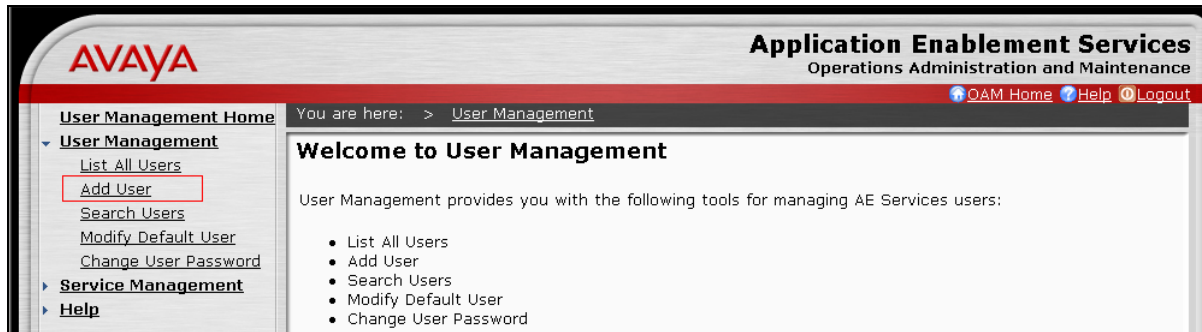
The steps in this section describe the configuration of a CTI user. Launch a web browser, enter <https://<IP address of AES server>:8443/MVAP> in the URL, and log in with the appropriate credentials to access the relevant administration pages.



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.

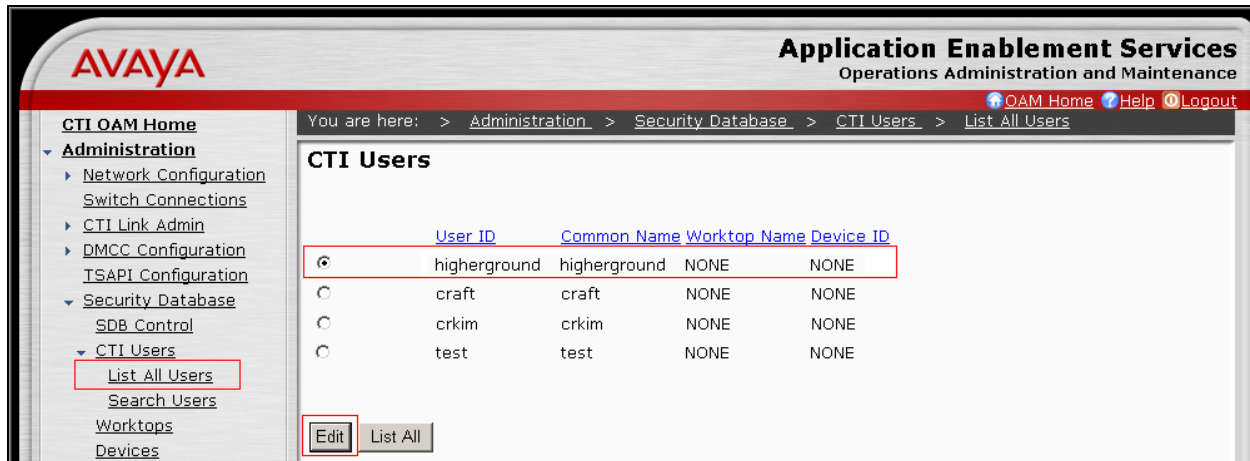


On the Add User page, provide the following information:

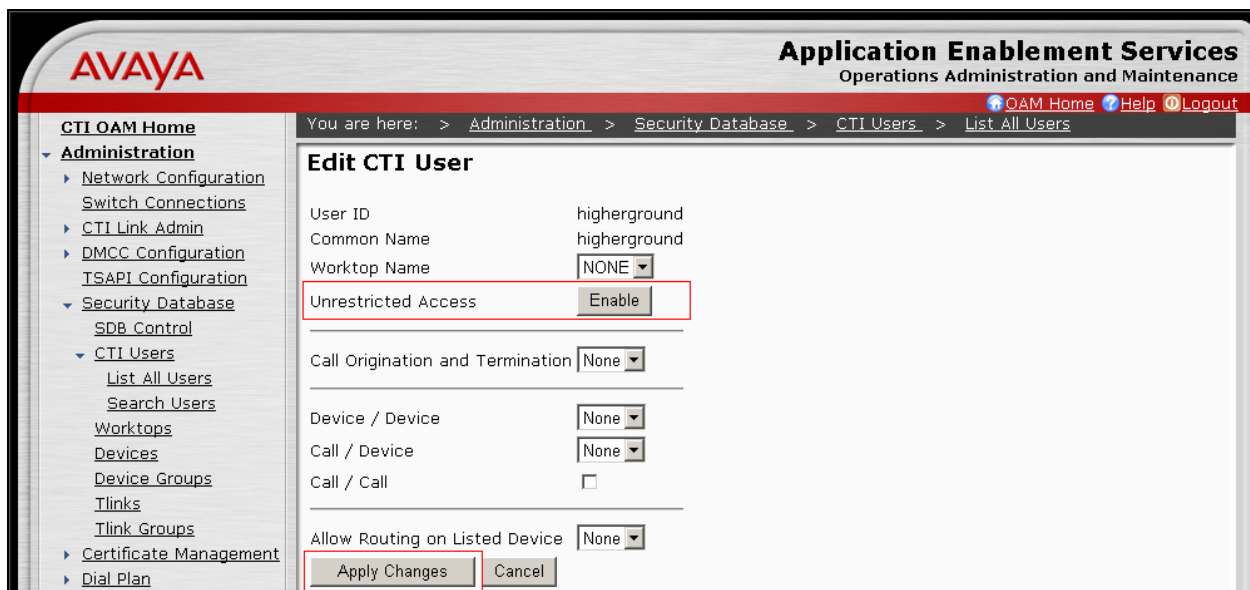
- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the HigherGround Server Configuration page 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 and navigate to the **CTI OAM Home Administration → 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.

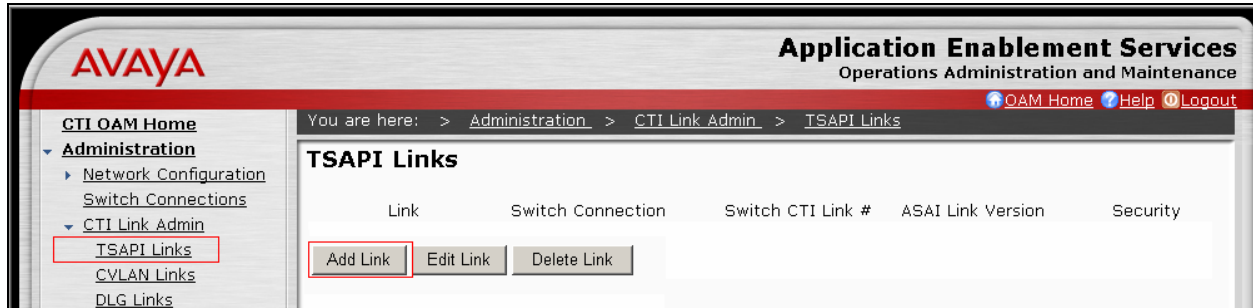


Provide the user with unrestricted access privileges by clicking the **Enable** button on the **Unrestricted Access** field. Click the **Apply Changes** button.

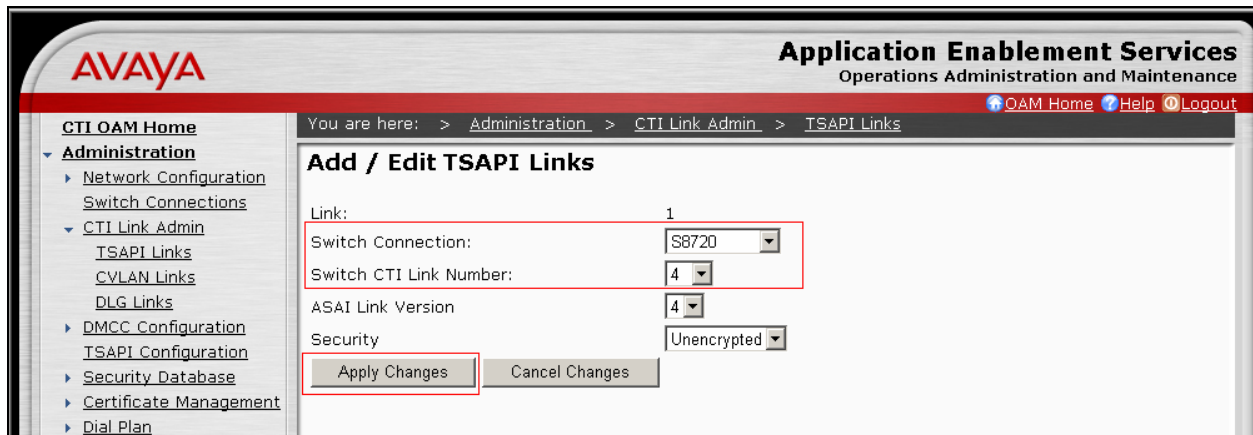


4.3. Configure the TSAPI CTI Link

Navigate to the **Administration → CTI Link Admin → TSAPI Links** page from the CTI OAM HOME Administration page, to set the TSAPI CTI Link. Click on **Add Link**.



Select a Switch Connection using the drop-down menu. The Switch Connection is configured in **Section 4.1**. Select the Switch CTI Link Number using the drop-down menu. Switch CTI Link Number should match with the number configured in the cti-link form in **Section 3.1**. Click the **Apply Changes** button. Default values may be used in the remaining fields.



5. Configure HigherGround Praetorian

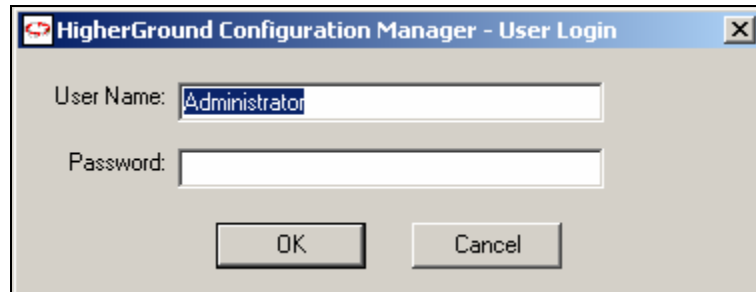
This section only describes the interface configuration for the Praetorian application to communicate with Avaya AES and Avaya Communication Manager. Refer to [3] and [4] for configuring the HigherGround Praetorian application. The following configuration steps will be included:

- TSAPI configuration
- Station configuration

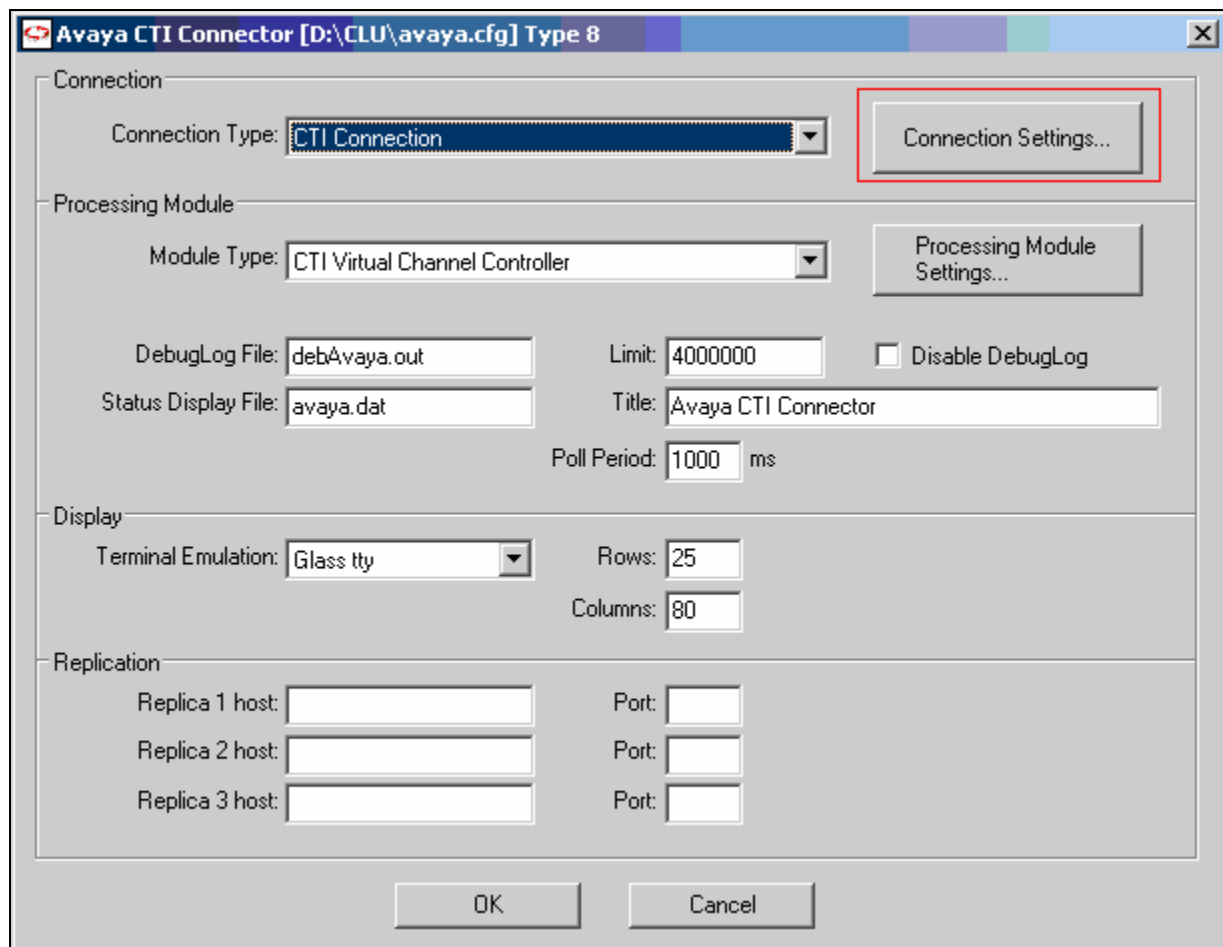
5.1. Configure TSAPI

This section describes how to configure the TSAPI interface that will communicate with Avaya AES. The HigherGround Praetorian application was installed into the D:\CLU directory, as a

default. All executions were performed in the D:\CLU directory. To start the TSAPI link configuration, run **cadcfg avayacfg** in the D:\CLU directory. On the HigherGround Configuration Manager – User Login window, provide appropriate credentials, and click on **OK**



Select the **Connection Settings** at the **Avaya CTI Connector** window.



In the CTI /QM Connection Settings window, provide the following information:

- CTI Type – Select **CSTA STD** using the drop-down menu.
- CTI Sub Type – Select **Avaya** using the drop-down menu.
- Server Name – In this field, enter the Tlink name. The Tlink name can be obtained by navigating to **CTI OAM Home → Administration → Security Database → Tlinks** in Avaya AES.
- User Name – Enter the User Id created in **Section 4.2**.
- Password – Enter the User Password created in **Section 4.2**.
- Check the **Produce “CTI Event” records** box.
- Check the **Produce “CTI State” records** box.
- Click on **OK**.

CTI/QM Connection Settings

Connection Type

CTI Type: CSTA STD

CTI Sub Type: Avaya

Server Name: AVAYA#S8720#C

Logical ID:

User Name: higherground

Password: Higherground123&

☒ Produce "CTI Event" records

☒ Produce "CTI State" records

OK Cancel

Select the **Processing Module Setting** button on **Avaya CTI Connector** window.

Avaya CTI Connector [D:\CLU\avaya.cfg] Type 8

Connection

Connection Type: CTI Connection

Connection Settings...

Processing Module

Module Type: CTI Virtual Channel Controller

Processing Module Settings...

DebugLog File: debAvaya.out

Limit: 4000000

☐ Disable DebugLog

Status Display File: avaya.dat

Title: Avaya CTI Connector

Poll Period: 1000 ms

Display

Terminal Emulation: Glass tty

Rows: 25

Columns: 80

Replication

Replica 1 host:

Port:

Replica 2 host:

Port:

Replica 3 host:

Port:

OK Cancel

In the CTI Virtual Channel Controller Module Settings windows, provide the following information:

- CTIVCH Type – Select **CSTA STD** using the drop-down menu.
- Subtype – Select **Generic** using the drop-down menu.
- Trigger Type – Select **API** using the drop-down menu.
- Click OK.

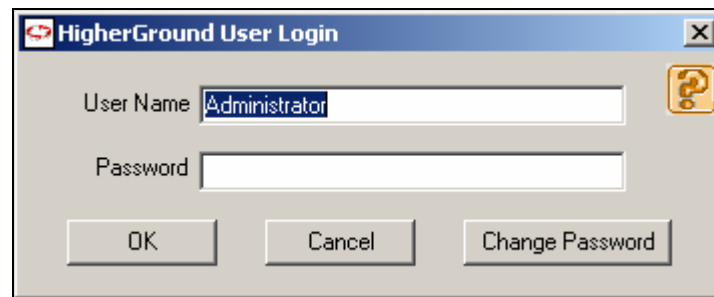
The screenshot shows the 'CTI Virtual Channel Controller Module Settings' dialog box. It has two main sections: 'Virtual Channel Controller' and 'Output'. In the 'Virtual Channel Controller' section, there are three dropdown menus: 'CTIVCH Type' is set to 'CSTA STD', 'Subtype' is set to 'Generic', and 'Trigger Type' is set to 'API'. In the 'Output' section, there are four text boxes: 'SMDR Output File' contains 'smdr.log', 'Record Prefix' is empty, 'Raw Data Capture File' contains 'csta.log', and 'Poll Character' is empty. At the bottom, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red rectangular box.

HigherGround Praetorian utilizes DNS, instead of IP address, to resolve the machine name, like AES. Since the compliance test environment does not include the DNS server, the hosts file was used instead. The hosts file is located in the c:\WINDOWS\system32\drivers\etc directory

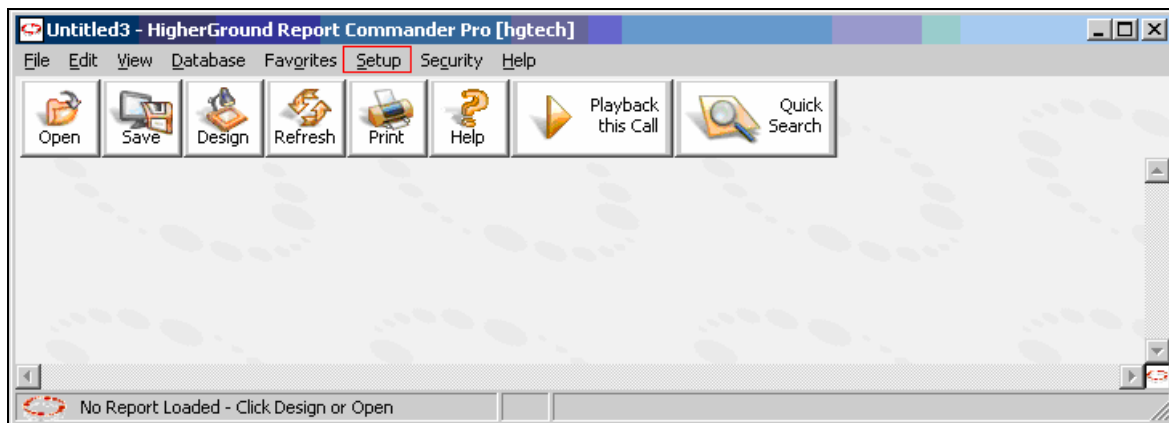
```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost
192.45.85.102 AES
```

5.2. Configure Stations

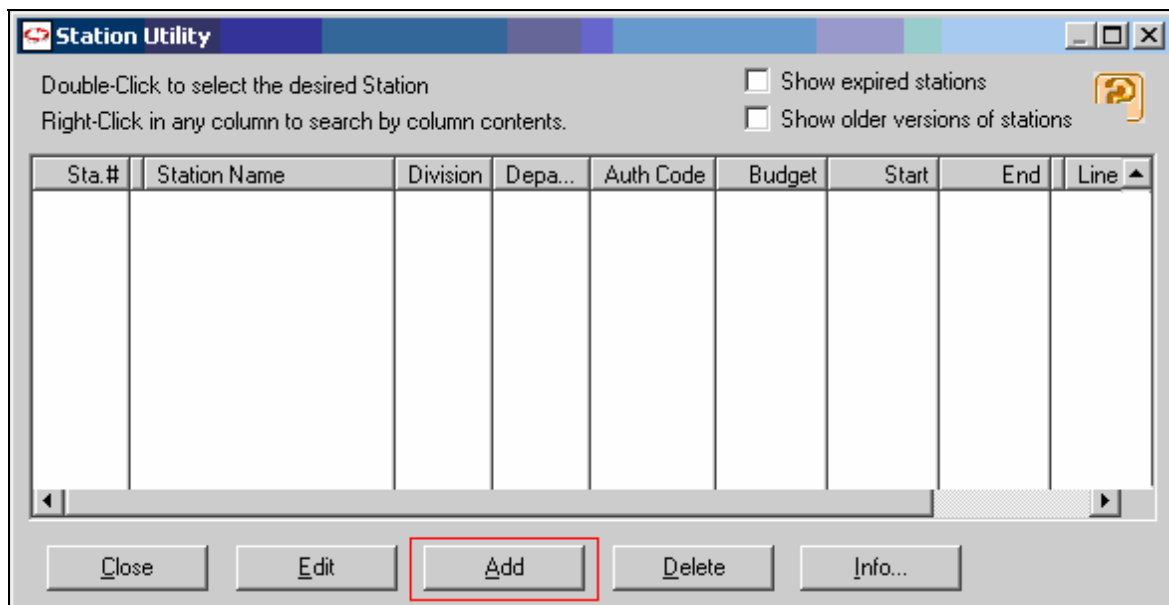
To configure the station, run **report** in the D:\CLU directory. Provide appropriate credentials on the HigherGround User Login screen.



In the HigherGround Report Commander Pro window, navigate to **Setup** → **Station Utility**.



From the Station Utility window, click on **Add** to add stations to be monitored.




On the Add New Station window, provide the following information:

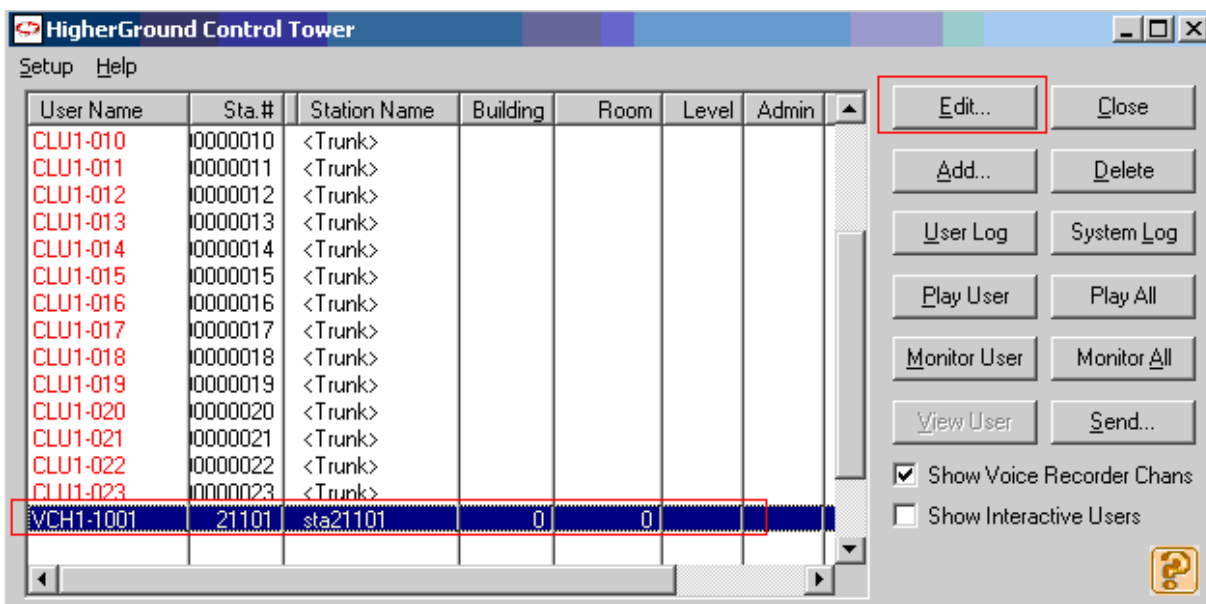
- Sta. # – Monitoring station's extension.
- Station Name – A descriptive name for the station.
- Check the **Request CTI Monitor on this Station** box.
- Click on **OK**.

Repeat this step as necessary to configure additional monitoring stations.

Add New Station

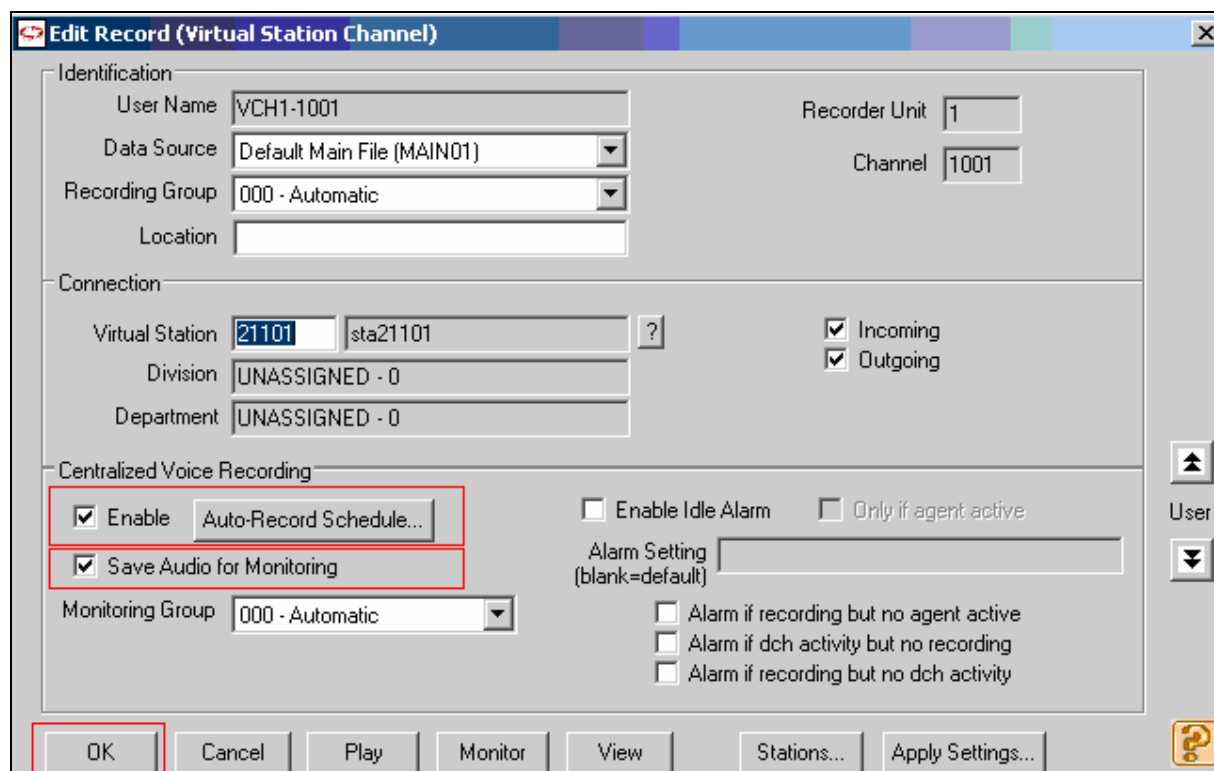
Sta.# ☐ Executive Station Privacy Start Date
Station Name End Date
Other Station #s
Auth Code Empl. No.
Division Select Division and Department...
Department Equipment...
Location
Equipment
Port No.
Cable No.
P/U Group
Hunt Group
Budget
Line Term Jack
Bus. Man. Chg.
Calling Card
Cell Phone
Acct Number
Level
Remarks
Accountg. Rem.
Remarks 1
Remarks 2
☐ Exclude from PM Load Wage Rate
☐ Pro-Rate Equip. Wage Group
☐ Disable Distributed Recording
☐ Disable Screen Capture
☒ Request CTI Monitor on this station
☐ Allow Automatic Channel Assignment
 

In the HigherGround Report Commander Pro window, navigate to **Security → Control Tower**. Double click on a virtual channel, or select the **Edit** button.



In the Edit Record window, provide the following information:

- Check the **Enable Auto Record Schedule** box.
- Check the **Save Audio for Monitoring** box.
- Click on **OK**.



6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability, and performance testing. The feature testing evaluated the ability of HigherGround Praetorian to monitor and record calls placed to and from stations and to a VDN. The serviceability testing introduced failure scenarios to see if HigherGround Praetorian can resume recording after failure recovery. The performance testing stressed HigherGround Praetorian 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 stations, agents, and VDNs, monitor and record them using HigherGround Praetorian, and verify the recordings. For feature testing, the types of calls included inbound and outbound trunk calls, transferred calls, bridged calls, and conferenced calls. Performance tests verified that HigherGround Praetorian could record calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, 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/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	server1	192. 45. 80.102	36538	CLAN-AES	17	18

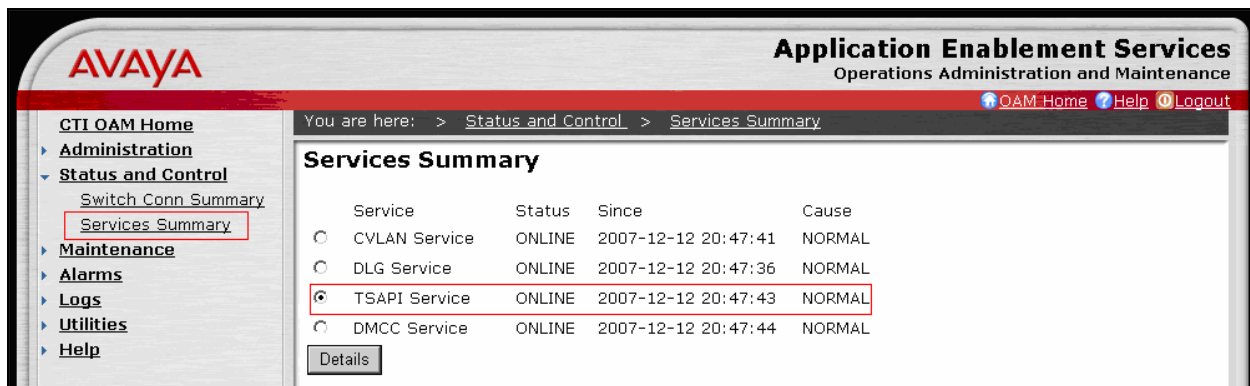
Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
2		no	server1	restarting	15	15
4	4	no	server1	established	15	15

7.2. Verify Avaya Application Enablement Services

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



8. Support

Technical support for HigherGround Praetorian can be obtained by contacting HigherGround via the support link at <http://www.highergroundinc.com/support.html>.

9. Conclusion

These Application Notes illustrate the procedures for configuring the HigherGround Praetorian call recording solution to monitor and record calls placed to and from stations via a trunk and to a VDN on an Avaya Communication Manager system. In the configuration described in these Application Notes, HigherGround Praetorian employs a trunk tabbing technique to record the trunk and/or station. During compliance testing, HigherGround Praetorian successfully monitored events and recorded calls placed to and from stations via a trunk, as well as calls placed to a VDN and then queued to an agent hunt/skill group. HigherGround Praetorian was also able to record calls under continuous call volumes over extended periods of time.

10. Additional References

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

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Administrator Guide for Avaya Communication Manager*, Issue 4, January 2008, Document Number 03-300509.

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 4.2, Issue 10, May 2008, Document Number 02-300357

The following documentation was provided by HigherGround

[3] *HIGHERGROUND WORKBOOK: Praetorian VOICE RECORDER*, 2007

[4] *HIGHERGROUND FUSION SERIES 7: INSTALLATION TRAINING WORKBOOK*, VERSION 7.7

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.