Avaya Solution & Interoperability Test Lab

Application Notes for Amcom Software MediCall with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Amcom Software MediCall to control Avaya IP and Digital Telephones on Avaya Communication Manager. MediCall is a software application that allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface.

MediCall uses the Device, Media, and Call Control application to share control of a physical telephone and receive the same terminal and first party call control information received by the physical telephone. During compliance testing, calls were successfully placed to and from Avaya IP and Digital Telephones that were in shared control mode with MediCall applications.

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 Manager, Avaya Application Enablement Services (AES), various Avaya IP Telephones, and Amcom Software MediCall. MediCall is a Windows-based attendant console application for the Healthcare industry, and MediCall allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI) on their desktop/laptop computer. MediCall uses the Device, Media, and Call Control application (DMCC) from the Avaya Application Enablement Services (AES) server to share control of a physical telephone and receive terminal and first party call control information.

Figure 1 illustrates the network configuration used to verify the Amcom Software solution. The configuration consists of Avaya S8720 Servers with an Avaya G650 Media Gateway, an Avaya AES Server, Avaya IP Telephones, an Avaya Digital Telephone, and PCs with MediCall installed and running. Avaya Communication Manager runs on the S8720 Servers, though 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.

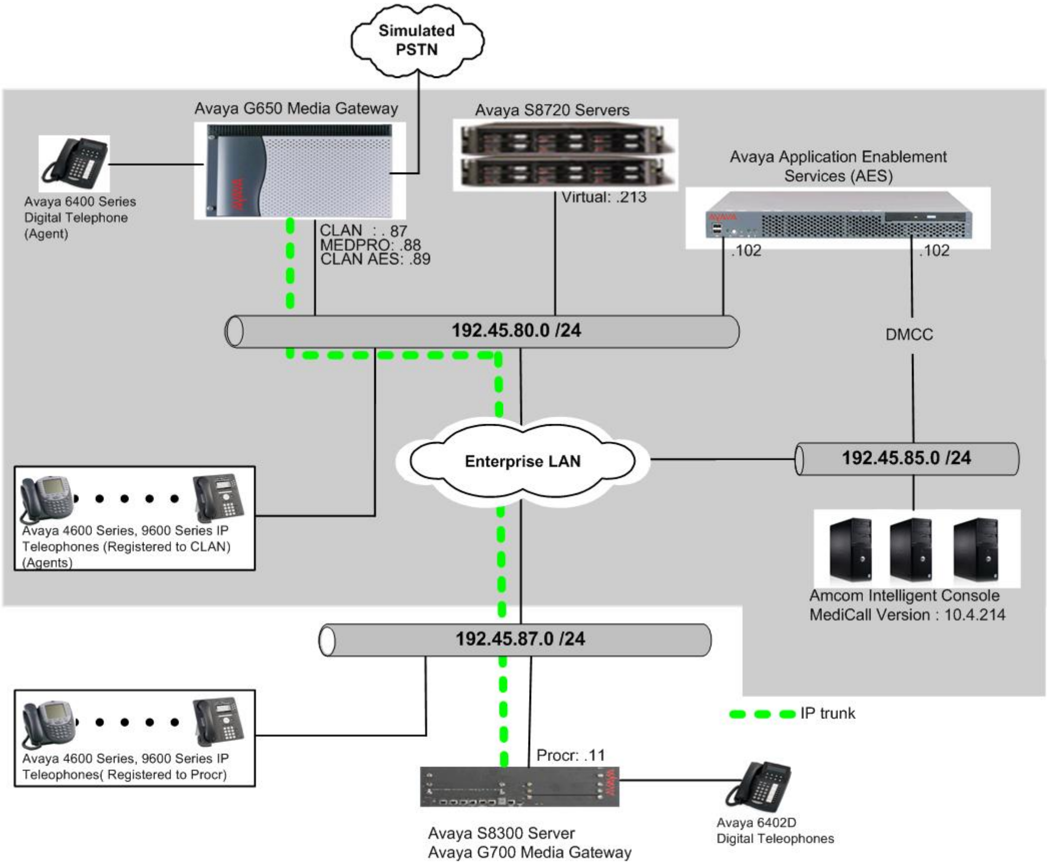

Simulated PSTN
Avaya G650 Media Gateway
Avaya S8720 Servers
Avaya Application Enablement Services (AES)
Avaya 6400 Series Digital Telephone (Agent)
Virtual: .213
CLAN : . 87
MEDPRO: .88
CLAN AES: .89
.102
.102
192.45.80.0 /24
DMCC
Enterprise LAN
192.45.85.0 /24
Avaya 4600 Series, 9600 Series IP Teleophones (Registered to CLAN) (Agents)
Amcom Intelligent Console MediCall Version : 10.4.214
192.45.87.0 /24
IP trunk
Avaya 4600 Series, 9600 Series IP Teleophones(Registered to Procr)
Procr: .11
Avaya S8300 Server
Avaya G700 Media Gateway
Avaya 6402D Digital Teleophones

Figure 1: Test Configuration of Amcom Software MediCall

2. Equipment and Software Validated

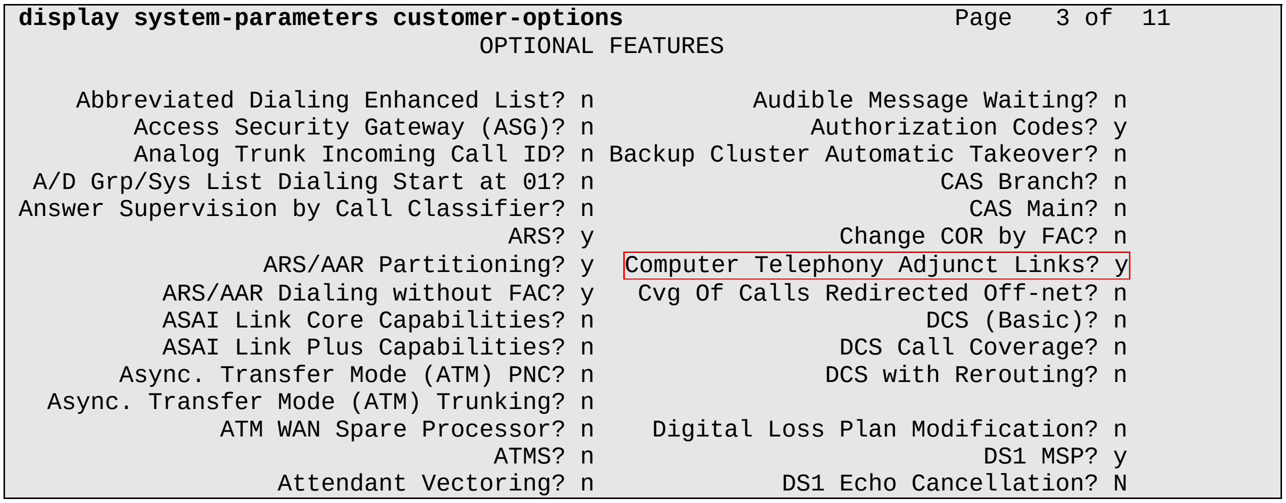
The following equipment and software were used for the sample configuration provided:

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 TN799DP C-LAN Interface TN2302AP IP Media Processor	HW11 FW044 HW01 FW028 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) 4625SW (H.323)	2.8 2.8
Avaya 9600 Series IP Telephones	
9630 (H.323) 9650 (H.323)	1.5 1.5
Avaya 6408D+ Digital Telephone	-
Amcom Software MediCall on Microsoft Windows 2003 Server with Service Pack 2 Amcom Software MediCall on Microsoft Windows XP Professional with Service Pack 3 Phone Software MediCall	 1.0.0.18 10.4.214

3. Configure Avaya Communication Manager

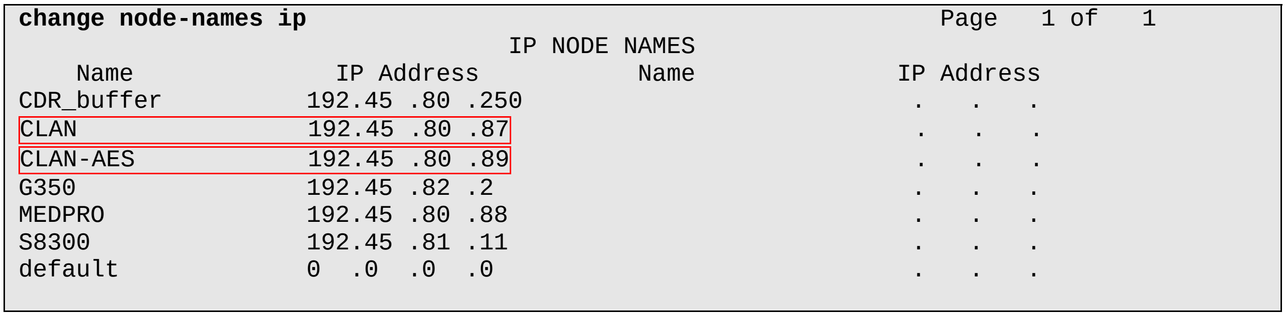
This section provides the procedures for configuring the system-parameters customer-options, a node-name and ip-services forms on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

Enter the **display system-parameters customer-options** command. On **Page 3**, verify that the Computer Telephony Adjunct Links field 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? y   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? y
                  Attendant Vectoring? n             DS1 Echo Cancellation? N
```

Enter the **change node-names ip** command. In the compliance tested configuration, the CLAN IP address was used 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   1
                                  IP NODE NAMES
    Name              IP Address          Name              IP Address
CDR_buffer          192.45 .80 .250                             .   .   .
CLAN                192.45 .80 .87                              .   .   .
CLAN-AES            192.45 .80 .89                              .   .   .
G350                192.45 .82 .2                               .   .   .
MEDPRO              192.45 .80 .88                              .   .   .
S8300               192.45 .81 .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 used 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 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        Password          Enabled    Status
                   Server
      1:       server1           xxxxxxxxxxxxxxxx       y         idle
      2:
      3:
      4:
      5:
```

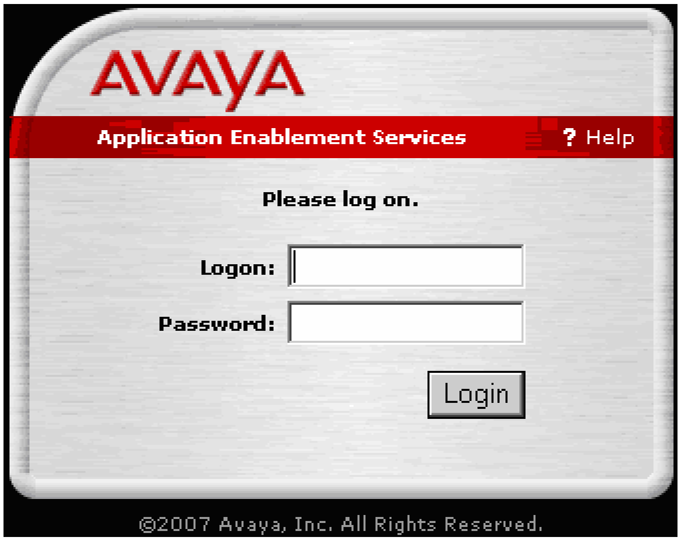
4. Configuring the DMCC application

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.

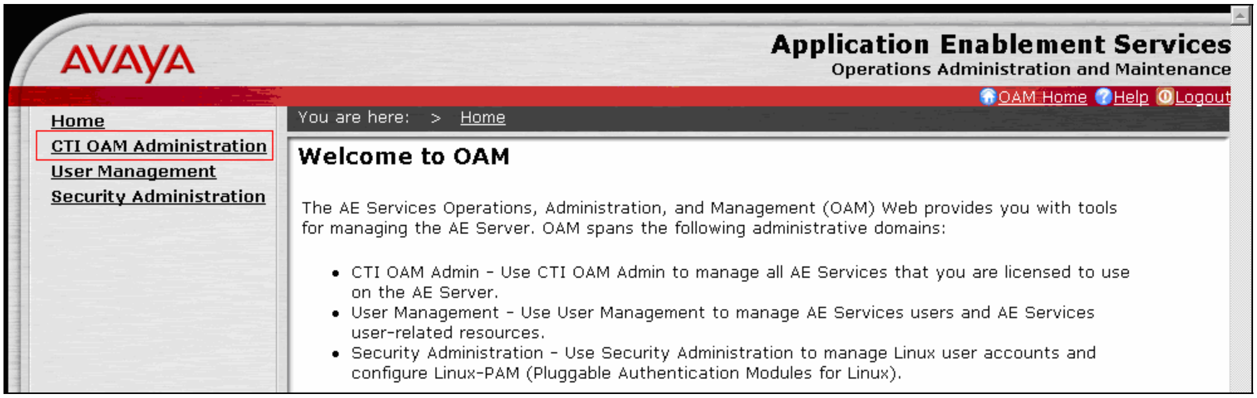
This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a DMCC Server port, and creating a CTI link for TSAPI.

4.1. Configure Switch Connection

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


AVAYA
Application Enablement Services
? Help
Please log on.
Logon:
Password:
Login
©2007 Avaya, Inc. All Rights Reserved.

Select the **CTI OAM Administration** link from the left pane of the screen.

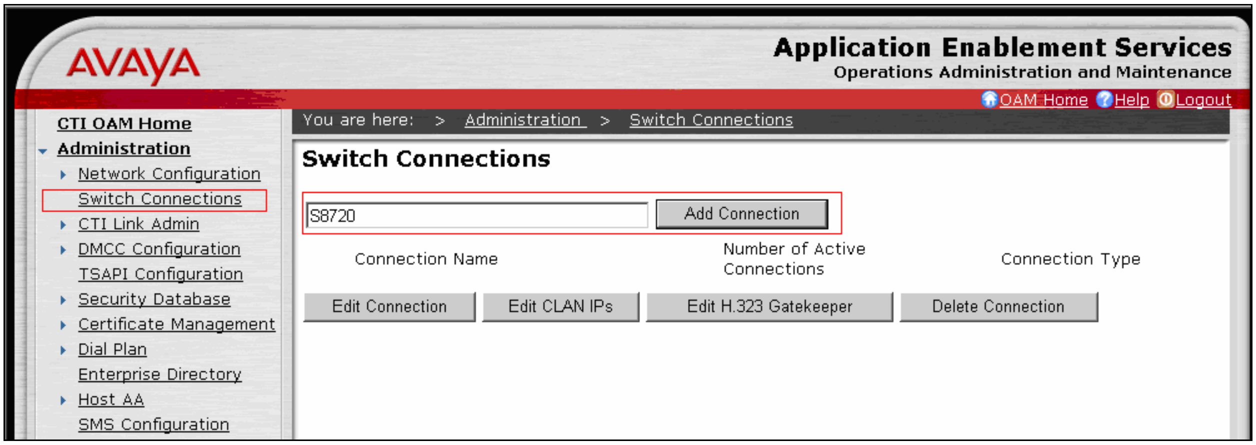


Welcome to OAM

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).

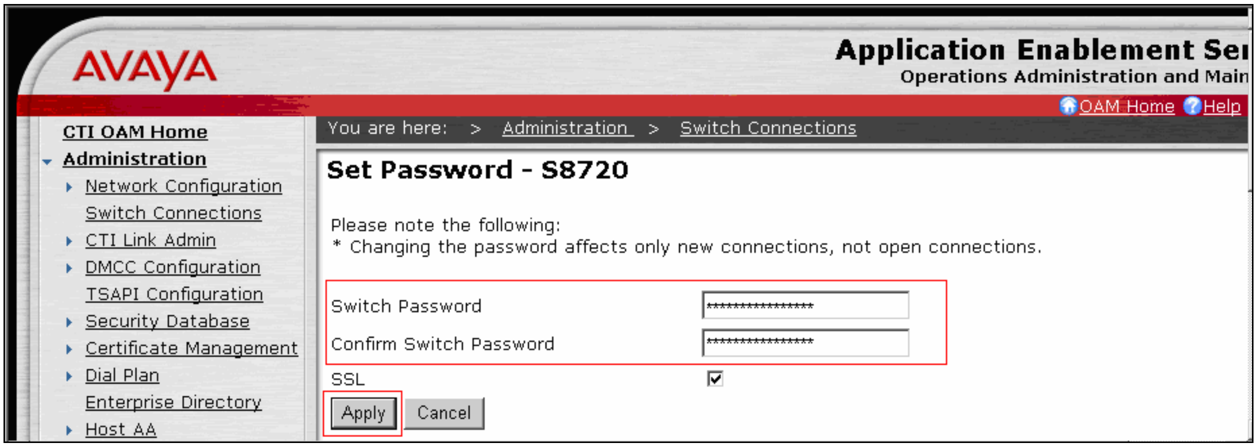
Click on **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



Switch Connections

S8720

The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 3**. Default values may be used in the remaining fields. Click on **Apply**.

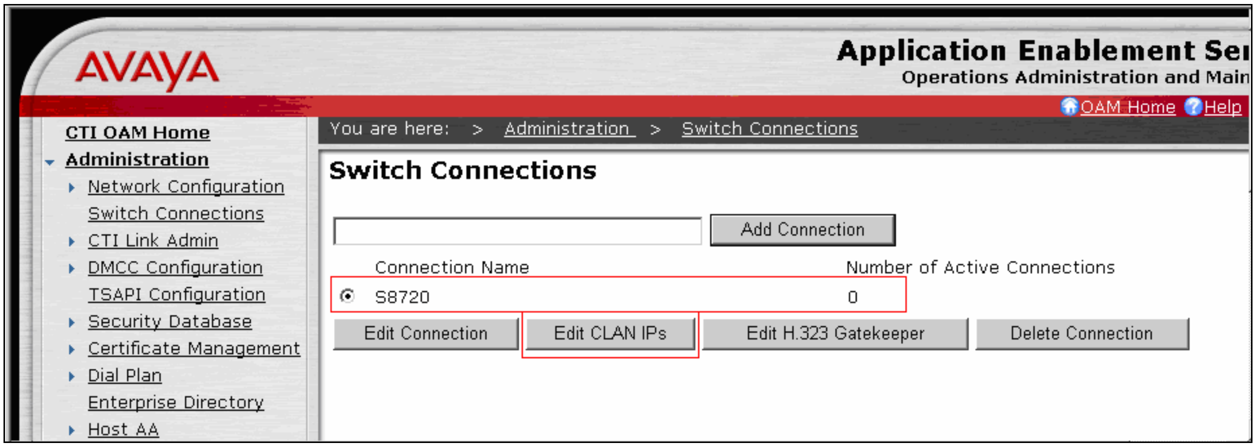


Set Password - S8720

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

Switch Password	*****************
Confirm Switch Password	*****************
SSL	☑

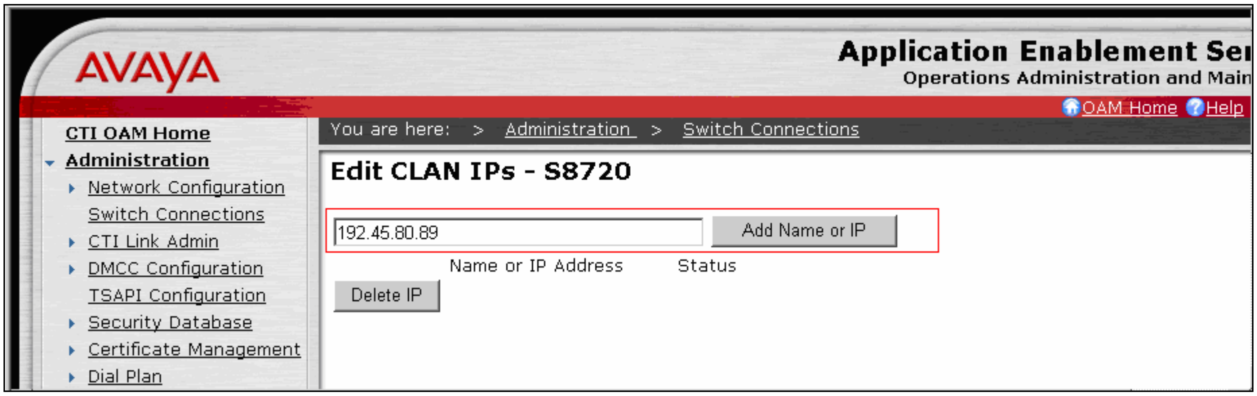
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.



Switch Connections

	Connection Name	Number of Active Connections
●	S8720	0

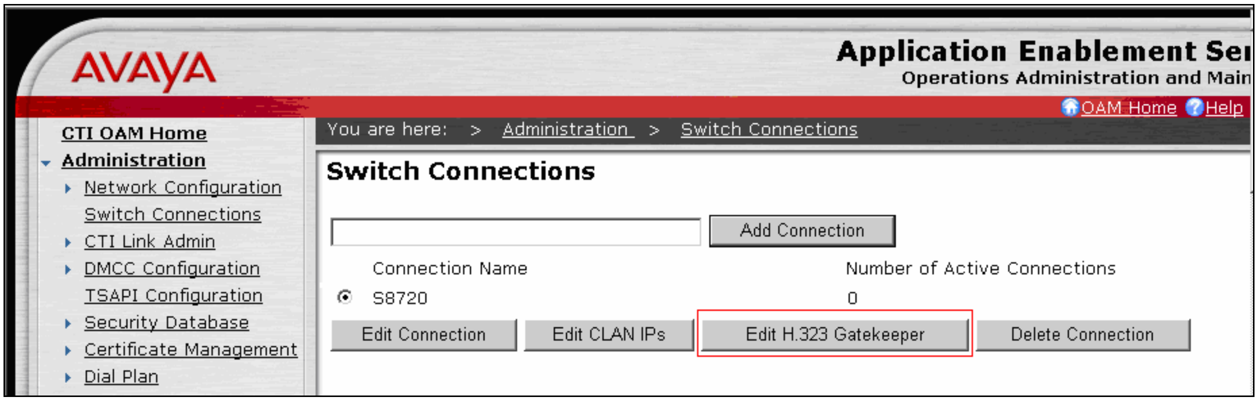
Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 3**, and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



Edit CLAN IPs - S8720

192.45.80.89

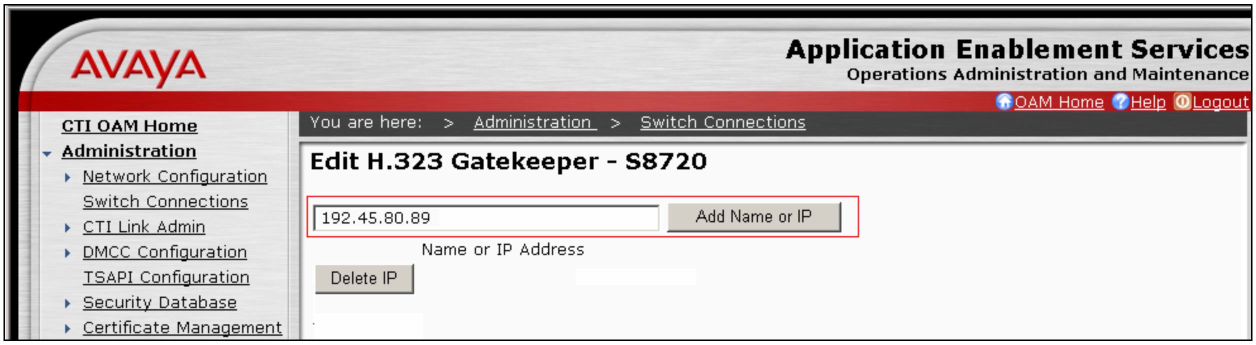
After the completion, navigate back to **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. Click on **Edit H.323 Gatekeeper** for DMCC call control and monitor.



Switch Connections

	Connection Name	Number of Active Connections
●	S8720	0

On the **Edit H.323 Gatekeeper – S8720** page, enter the C-LAN IP address which will be used for the DMCC service. During the compliance test, CLAN-AES was used for the DMCC service. Click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



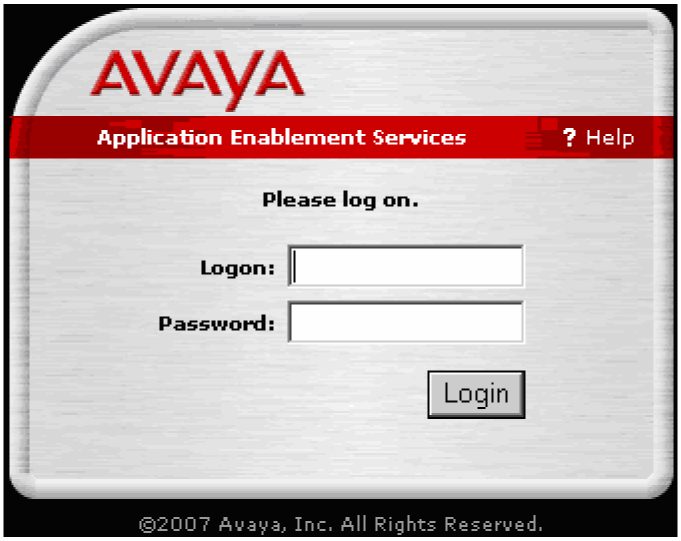
Edit H.323 Gatekeeper - S8720

192.45.80.89

Name or IP Address

4.2. Configure DMCC User

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



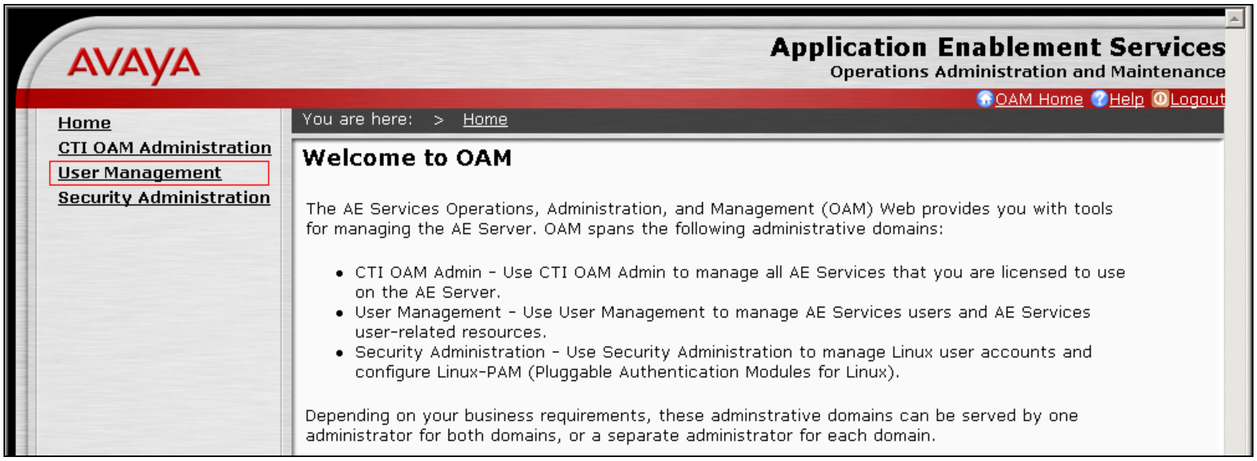
Please log on.

Logon:

Password:

©2007 Avaya, Inc. All Rights Reserved.

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



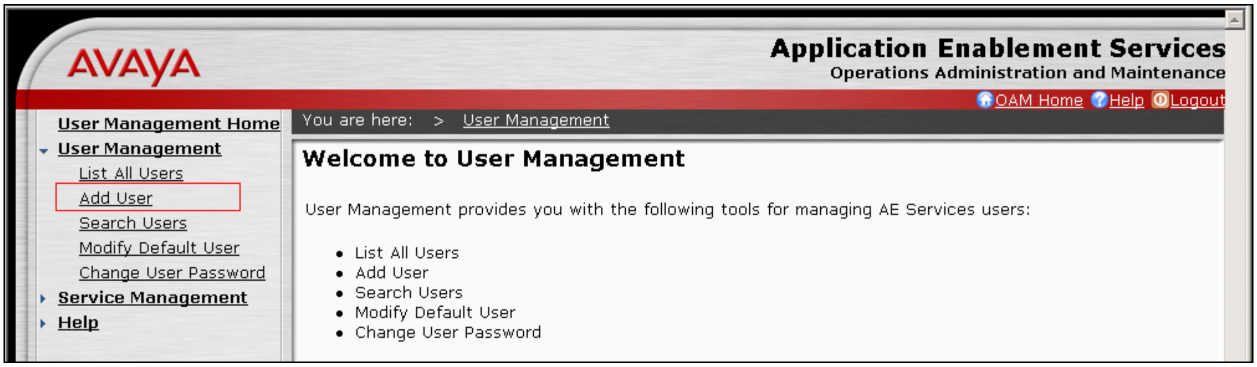
Welcome to OAM

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.

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



Welcome to User Management

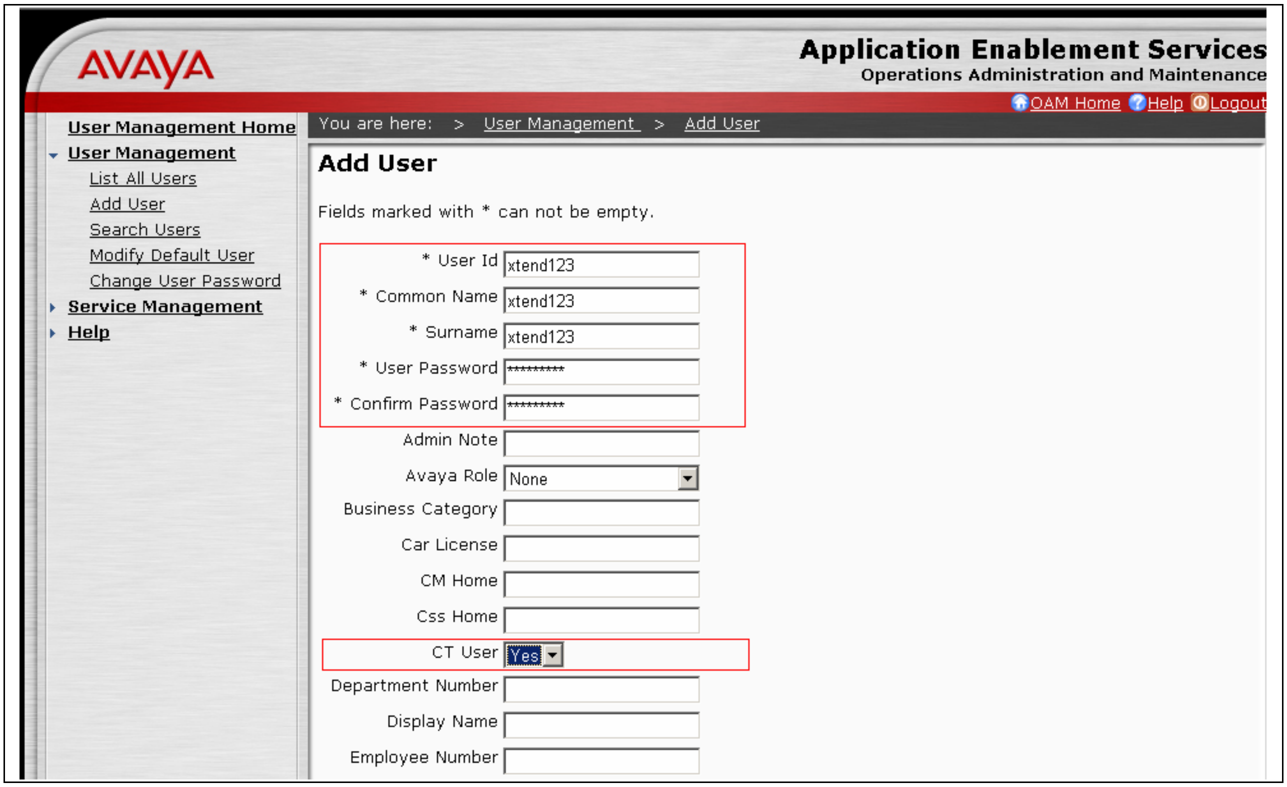
User Management provides you with the following tools for managing AE Services users:

- List All Users
- Add User
- Search Users
- Modify Default User
- Change User Password

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 MediCall 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.

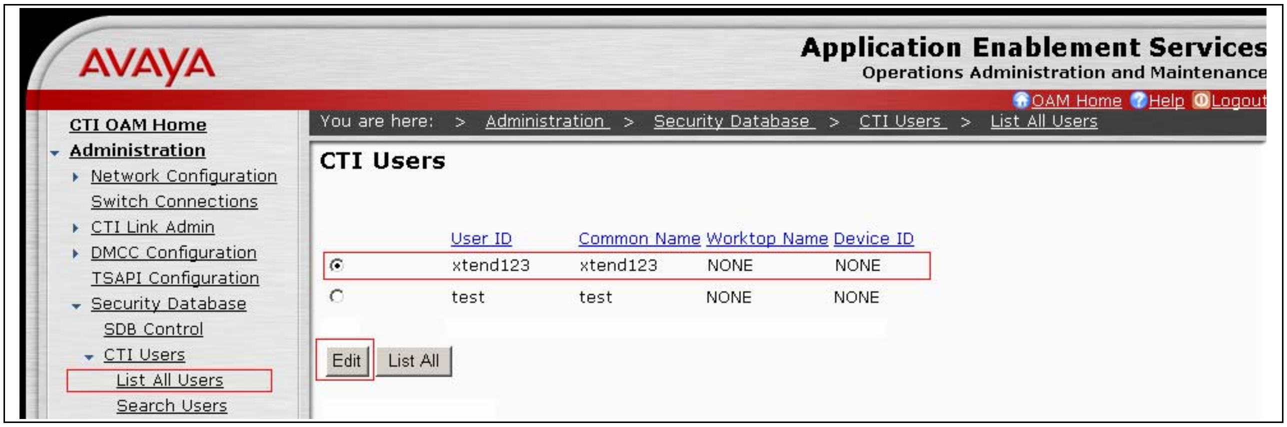


Add User

Fields marked with * can not be empty.

* User Id	xtend123
* Common Name	xtend123
* Surname	xtend123
* User Password	*********
* Confirm Password	*********
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	

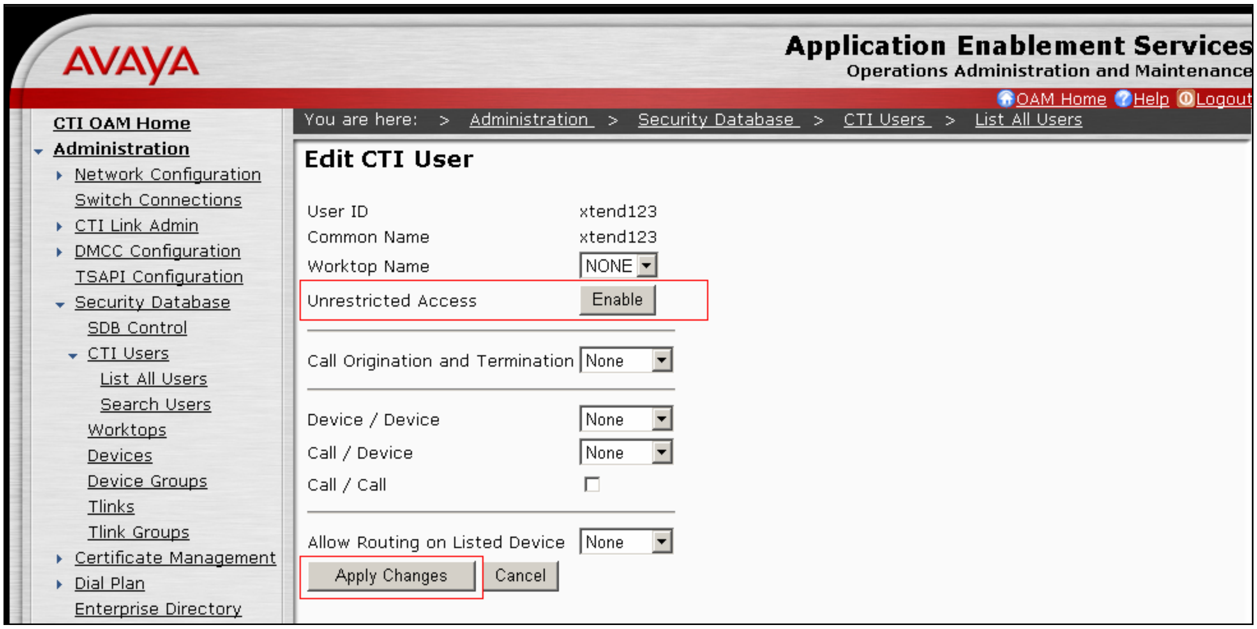
Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Administration → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.



CTI Users

	User ID	Common Name	Worktop Name	Device ID
●	xtend123	xtend123	NONE	NONE
○	test	test	NONE	NONE

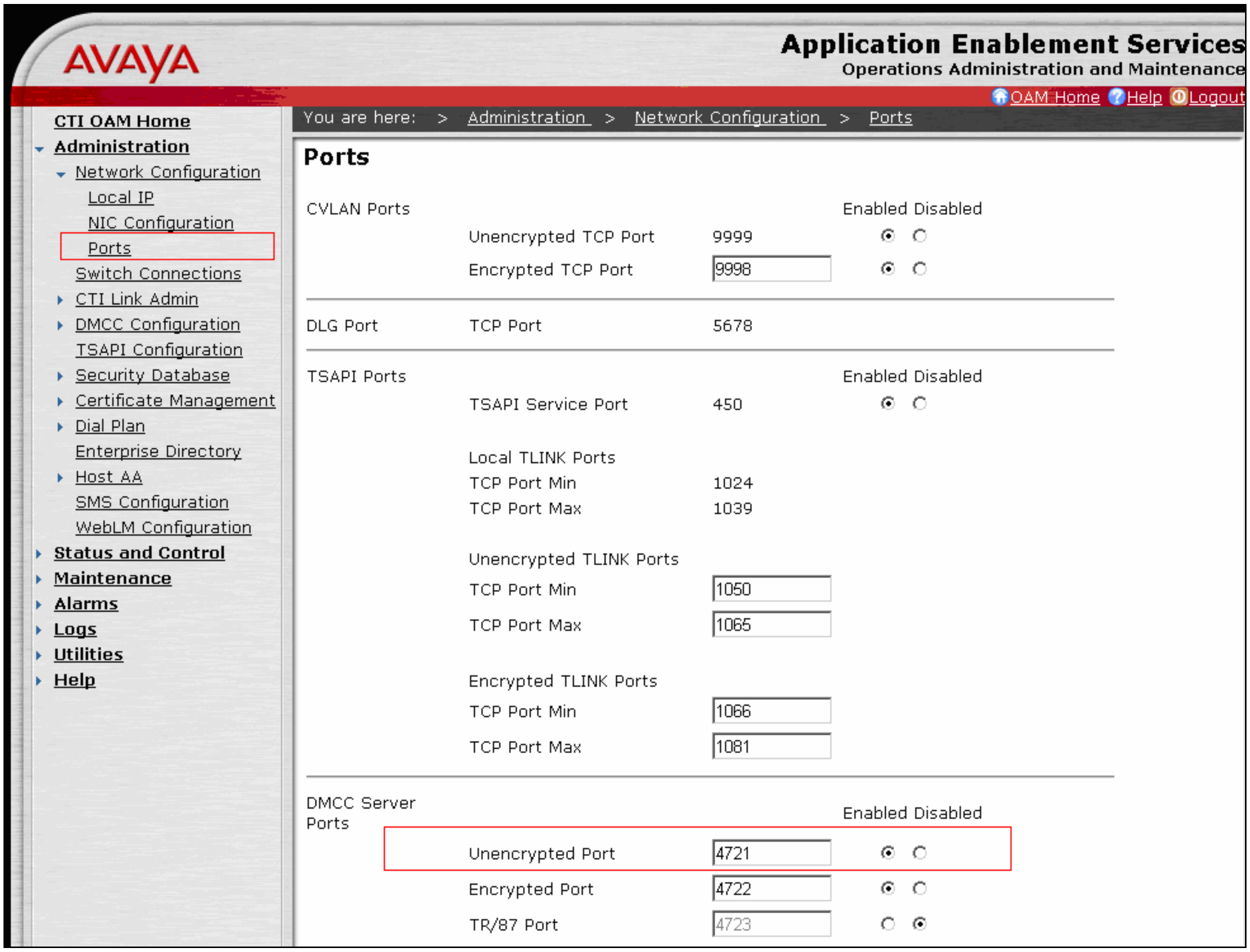
Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.



Edit CTI User

User ID	xtend123
Common Name	xtend123
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

Navigate to the **CTI OAM Home → Administration → Ports** page to set the DMCC server port. During the compliance test, the default port values were used. The following screen displays the default port values. Since the unencrypted port was used during the compliance test, set the Unencrypted Port field to **Enabled**. Default values may be used in the remaining fields. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



You are here: > Administration > Network Configuration > Ports

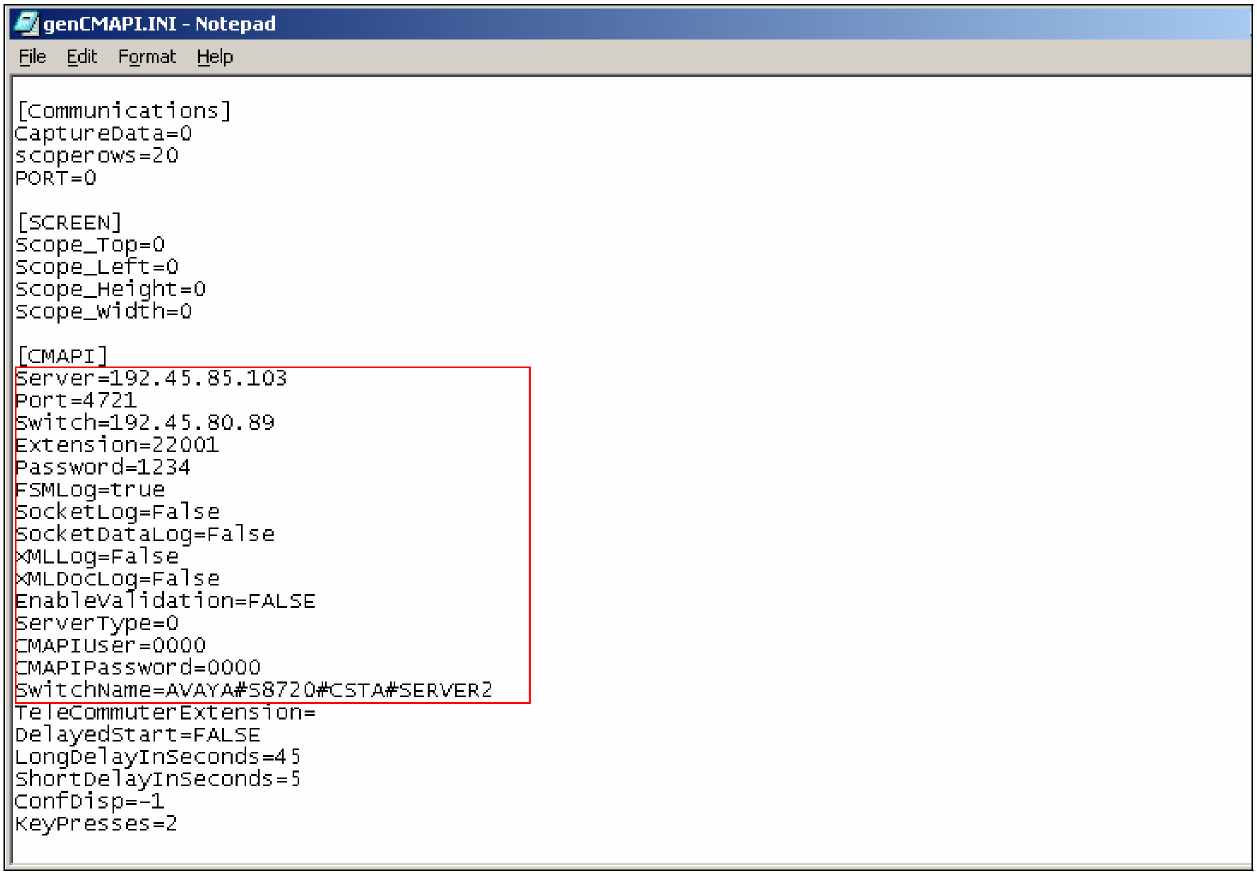
Ports

			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. Configure Amcom Software MediCall

Amcom Software installs and customizes MediCall for their end customers. Therefore, the only configuration that is relevant to the compliance test is “genCMAPI.ini” file, which specifies the DMCC configuration. Refer to [3] for further guidance.

The following screen displays the “genCMAPI.ini” file. Under the CMAPI section, the parameters have to match with the DMCC settings in the Avaya AES server.



```
[Communications]
CaptureData=0
scoperows=20
PORT=0

[SCREEN]
Scope_Top=0
Scope_Left=0
Scope_Height=0
Scope_Width=0

[CMAPI]
Server=192.45.85.103
Port=4721
Switch=192.45.80.89
Extension=22001
Password=1234
FSMLog=true
SocketLog=False
SocketDataLog=False
XMLLog=False
XMLDocLog=False
EnableValidation=FALSE
ServerType=0
CMAPIUser=0000
CMAPIPassword=0000
SwitchName=AVAYA#S8720#CSTA#SERVER2
TeleCommuterExtension=
DelayedStart=FALSE
LongDelayInSeconds=45
ShortDelayInSeconds=5
ConfDisp=-1
KeyPresses=2
```

6. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of MediCall to operate Avaya IP and Digital telephones and view their display and first party call information. The serviceability test introduced failure scenarios to see if MediCall can resume operation after failure recovery.

6.1. General Test Approach

The general approach was to exercise basic telephone and call operations on Avaya IP and Digital telephones using MediCall. The main objectives were to verify that:

- The user may successfully perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, and conference operations on the physical telephone from the MediCall console.
- Manual operations performed on the physical telephones are correctly reflected in the MediCall console.
- MediCall and manual telephone operations may be used interchangeably, i.e. go off hook using MediCall and manually dial digits.
- Display and call information provided on the MediCall console are consistent with the actual display and call information on the physical telephones.
- Call states are consistent between MediCall and the physical telephones.

For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, conference calls, and Automatic Call Distribution (ACD) calls. For serviceability testing, cable disconnects and reconnects, application restarts, and device resets were applied.

6.2. Test Results

Calls were successfully placed to and from telephones using manual methods, MediCall, and both. Other telephone operations such as off-hook, on-hook, hold, retrieve, transfer, and conference were successfully performed from the MediCall console. Manual telephone operation, display and call information, and call states were also correctly reflected in the MediCall console.

For serviceability testing, MediCall was able to resume control of Avaya IP and Digital telephones after restarts of the MediCall application and the computer on which it runs, and resets of the physical telephone, the Avaya AES server, and Avaya S8720 Server.

7. Verification Steps

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

7.1. Verify Avaya Communication Manager

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

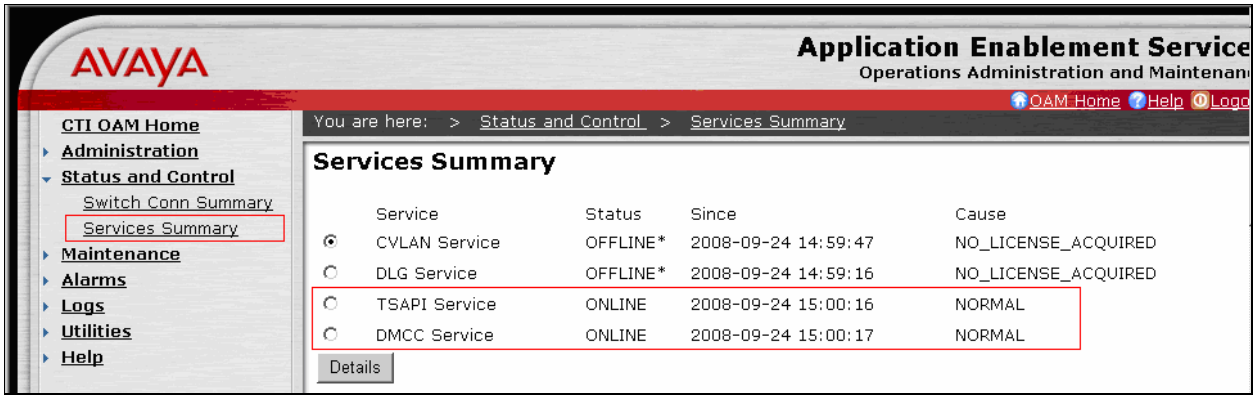
```
status aesvcs link

                            AE SERVICES LINK STATUS

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

01/01  server2         192. 45. 80.103  60336   CLAN-AES        208     197
```

Verify the Service State field of the administered TSAPI CTI link is in **established** state, by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

4     4        no    server2          established   15       15
```

7.2. Verify Avaya Application Enablement Services

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



Services Summary

	Service	Status	Since	Cause
●	CVLAN Service	OFFLINE*	2008-09-24 14:59:47	NO_LICENSE_ACQUIRED
○	DLG Service	OFFLINE*	2008-09-24 14:59:16	NO_LICENSE_ACQUIRED
○	TSAPI Service	ONLINE	2008-09-24 15:00:16	NORMAL
○	DMCC Service	ONLINE	2008-09-24 15:00:17	NORMAL

8. Support

For technical support on Amcom Software products, call Amcom Software at (212) 951-7670 or send email to xtendsupport@amcomsoft.com.

9. Conclusion

These Application Notes illustrate the procedures for configuring Amcom Software MediCall applications to operate Avaya IP and Digital telephones and view the physical telephones' display and call information from MediCall graphical user interfaces.

MediCall uses the DMCC service from Avaya AES server to control a physical telephone and receive the same terminal and first party call control information received by the physical telephone. During compliance testing, calls were successfully placed to and from Avaya IP and Digital Telephones that were in shared control mode with MediCall applications.

10. References

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

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

[1] *Feature Description and Implementation For Avaya Communication Manager*, Release 5.1, Issue 6, January 2008, Document Number 555-245-205.

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

The following document is provided by Amcom Software. For additional product and company information, visit http://www.amcomsoft.com.

[3] *User's Guide for Intelligent Console* , Version 1, December 2008

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 the 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.