



Application Notes for XTEND Communications XpressDesk with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring XTEND Communications XpressDesk to control Avaya IP and Digital Telephones on Avaya Communication Manager. XpressDesk 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.

XpressDesk 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 XpressDesk applications.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* 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) server, various Avaya Digital and IP Telephones, and XTEND Communications XpressDesk. XpressDesk is a Windows-based application that 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. The XpressDesk uses the Device, Media, and Call Control application (CMAPI) 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 XTEND Communications solution. The configuration consists of an Avaya S8700 Media Server with an Avaya G650 Media Gateway, an Avaya AES server, Avaya IP Telephones, an Avaya Digital Telephone, and a PC with XpressDesk installed and running. Avaya Communication Manager runs on the S8700 Media Server, though the solution described herein is also extensible to other Avaya Media Servers and Media Gateways.

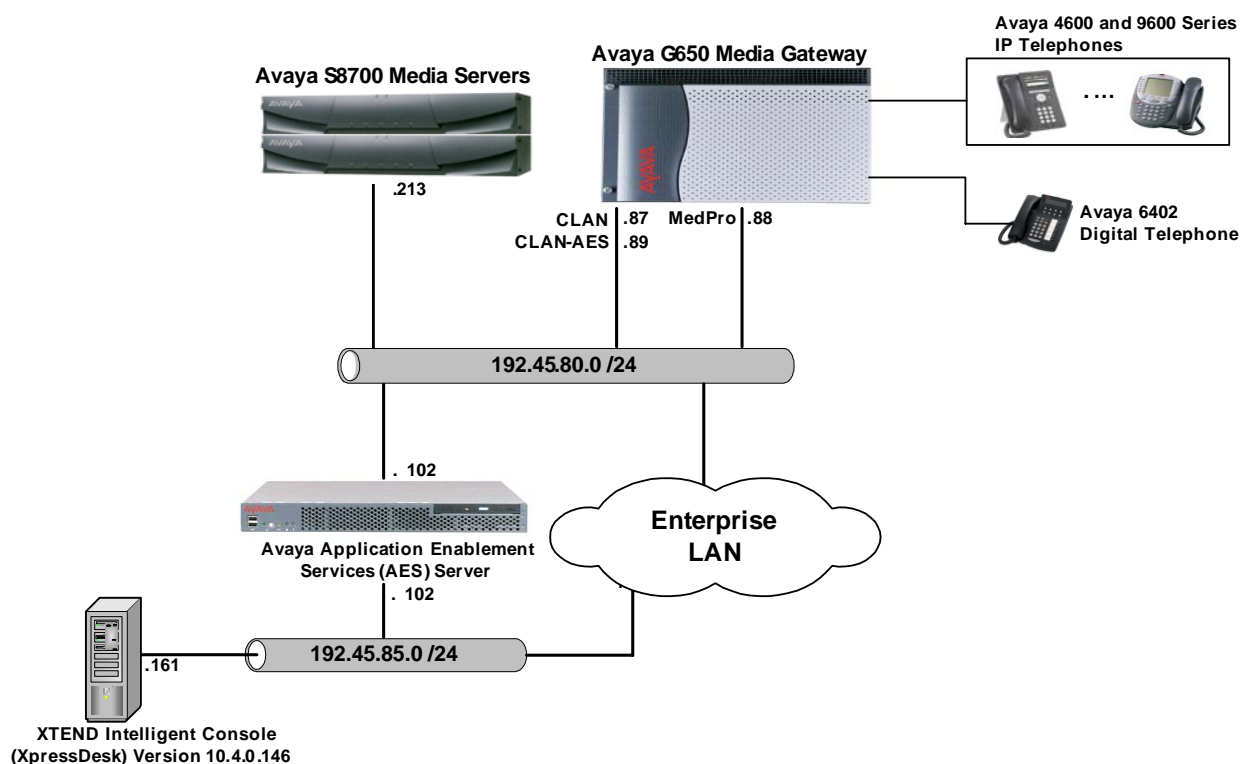


Figure 1: Test Configuration of XTEND XpressDesk with CMAPI

2. Equipment and Software Validated

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

Equipment		Software
Avaya S8700 Media Server		Avaya Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface	HW11 FW030
	TN799DP C-LAN Interface	HW20 FW017
	TN2302AP IP Media Processor	HW01 FW108
	TN2602AP IP Media Processor	HW02 FW007
Avaya Application Enablement Services (AES)		3.1 (r3-1-0-build-33-1-0)
Avaya 4600 Series IP Telephones		
	4620	2.6
	4625	2.5
Avaya 9630 Series IP Telephones		1.1
Avaya 6402 Digital Telephone		-
XTEND XpressDesk		10.4.0.146

3. Configure Avaya Communication Manager

This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. Refer to [2] for further guidance. 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 of the “system-parameters customer-options” form, verify that the ASAI Link Core Capabilities 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? n	
ARS/AAR Dialing without FAC? y	Cvg Of Calls Redirected Off-net? n	
ASAI Link Core Capabilities? y	DCS (Basic)? n	
ASAI Link Plus Capabilities? y	DCS Call Coverage? n	
Async. Transfer Mode (ATM) PNC? n	DCS with Rerouting? n	
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? n	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? n	DS1 Echo Cancellation? N	
Attendant Vectoring? n		

Enter the **change node-names ip** command. The C-LAN board (**CLAN-AES**) was enabled with Application Enablement Services to serve the AES link.

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	.	.
MEDPRO2	192.45 .80 .161	.	.
S8300	192.45 .81 .11	.	.
default	0 .0 .0 .0	.	.

Enter the **change ip-services** command. On Page 1 of the IP SERVICES form, configure entries for the C-LAN board that is dedicated for the AES link:

- Service Type – set to **AESVCS**
- Enabled – set to **y**.
- Local Node – **CLAN-AES** [Set to the node name of the C-LAN that serves the AES link]
- Local Port – set to **8765**.

change ip-services		Page 1 of 4	
		IP SERVICES	
Service Type	Enabled	Local Node	Local Port
AESVCS	y	CLAN-AES	8765

On Page 4 of the IP SERVICES form, enter the hostname of the AES server (ssh into the AES server and run “uname -a” to get the hostname) for the AE Services Server field and 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
1:	server1	xxxxxxxxxxxxxxxx	y
2:			
3:			
4:			
5:			

4. Configuring the CMAPI application

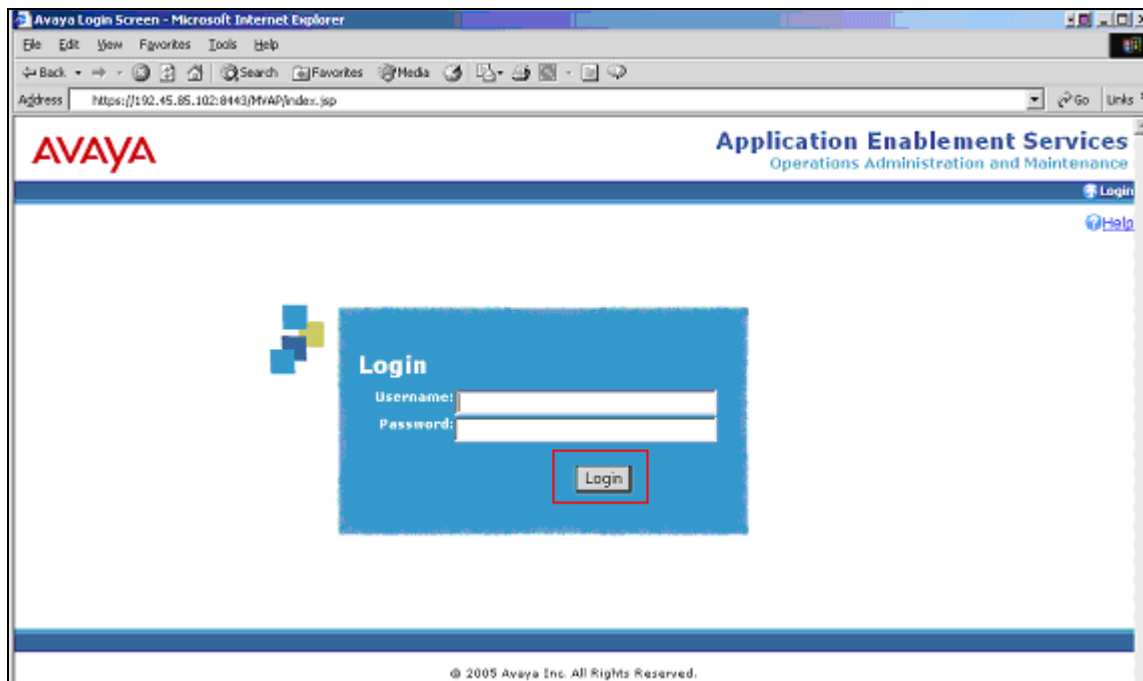
Avaya Application Enablement Services (AES) server enables Computer Telephony Integration (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to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

In this section, the following steps will be discussed:

- Configuring a Switch Connection
- Configuring an AES (CMAPI) user and a CMAPI port.

4.1. Configure Switch Connection

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



Click on **CTI OAM Home** → **Administration** → **Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the AES server 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

QAM Home
CTI OAM Home
Administration
Local IP
Ports
Switch Connections
CTI Link Admin
CMAPI Configuration
TSAPI Configuration
Security Database
Status and Control
Maintenance
Alarms
Logs
Utilities
Help

You are here: > Administration > Switch Connections

Switch Connections

S8700TOP Add Connection

Connection Name Number of Active Connections Connection Type

Edit Connection Edit CLAN IPs Edit H.323 Gatekeeper Delete Connection

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

AVAYA Application Enablement Services
Operations Administration and Maintenance

QAM Home
CTI OAM Home
Administration
Local IP
Ports
Switch Connections
CTI Link Admin
CMAPI Configuration
TSAPI Configuration
Security Database
Status and Control
Maintenance
Alarms
Logs
Utilities
Help

You are here: > Administration > Switch Connections

Set Password - S8700TOP

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

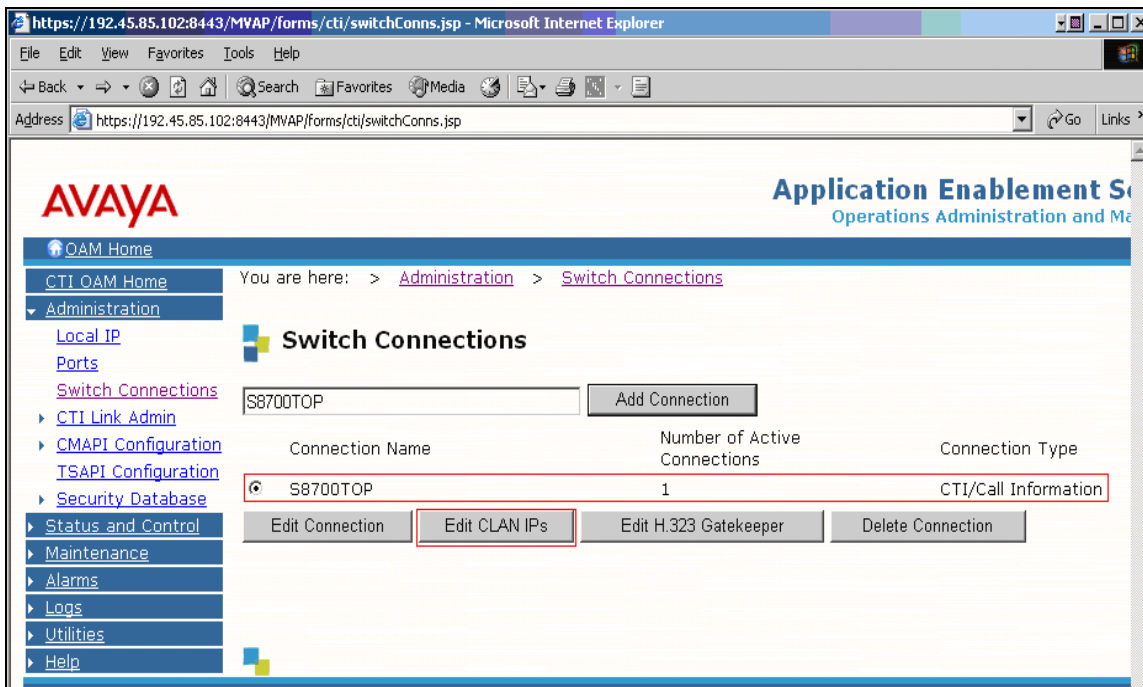
Switch Password

Confirm Switch Password

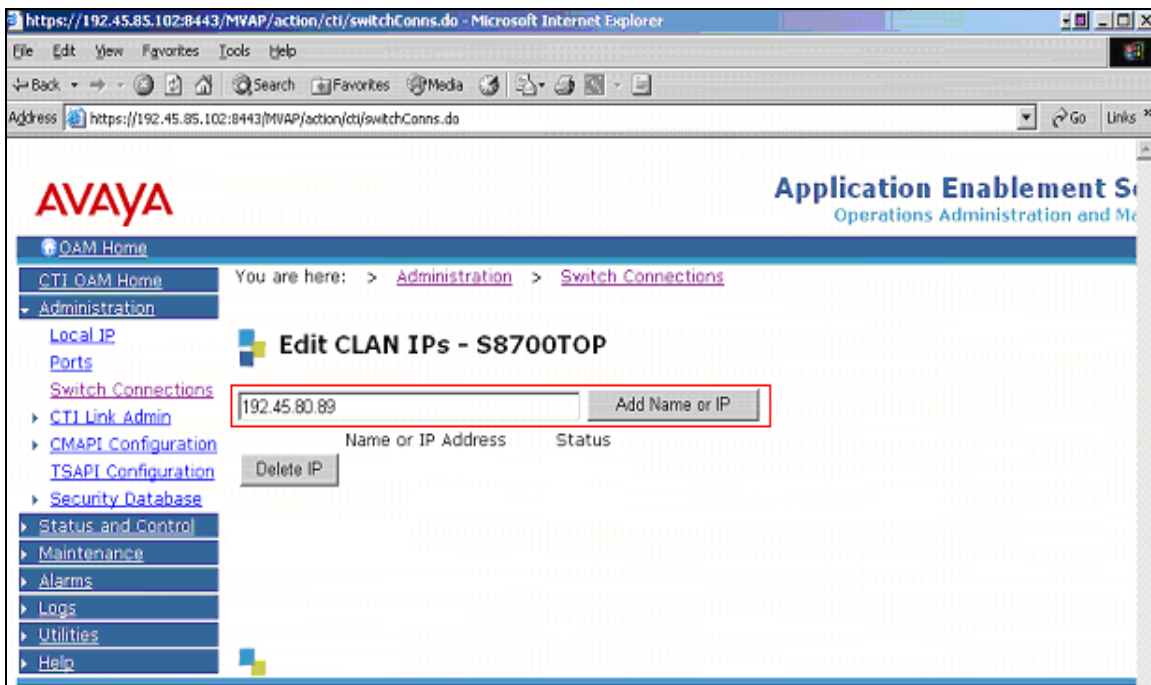
SSL ☒

Apply Cancel

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

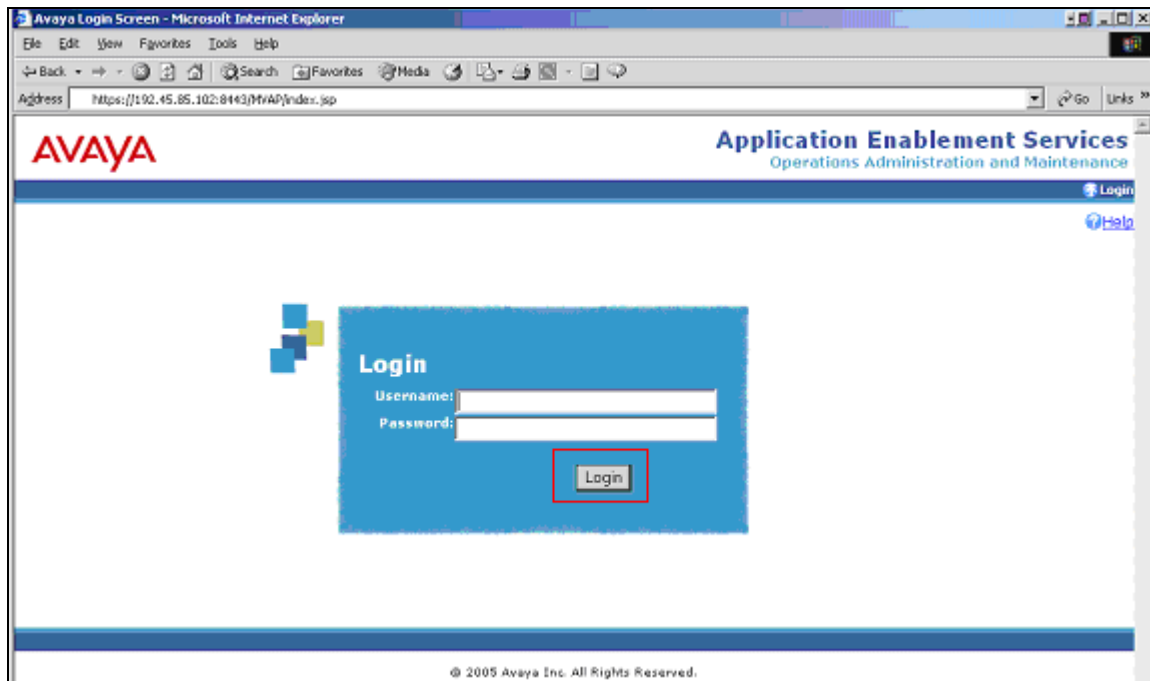


Enter the IP address of a C-LAN board enabled with Application Enablement Services (see Section 3) and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



4.2. Configure CMAPI User

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



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



On the “Add User” page, provide the following information:

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

Select **Yes** using the drop down menu on the CT User field. This enables the user as a CT user. Click the **Apply** button (not shown) to at the bottom of the screen to complete the process.

AVAYA Application Enablement Services
Operations Administration and Maintenance

QAM Home You are here: > [User Management](#) > [Add User](#) Logout Help

User Management Home
User Management
Add User
List All Users
Search Users
Modify Default User
Change User Password
Service Management
Help

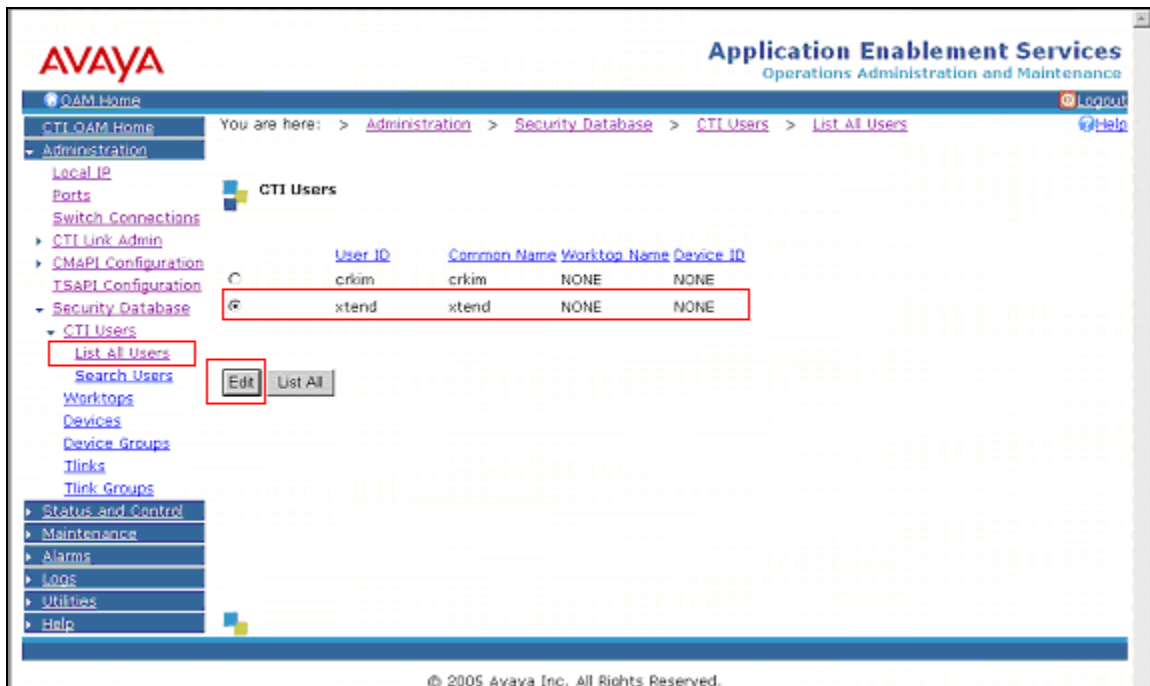
Add User

Fields marked with * can not be empty.

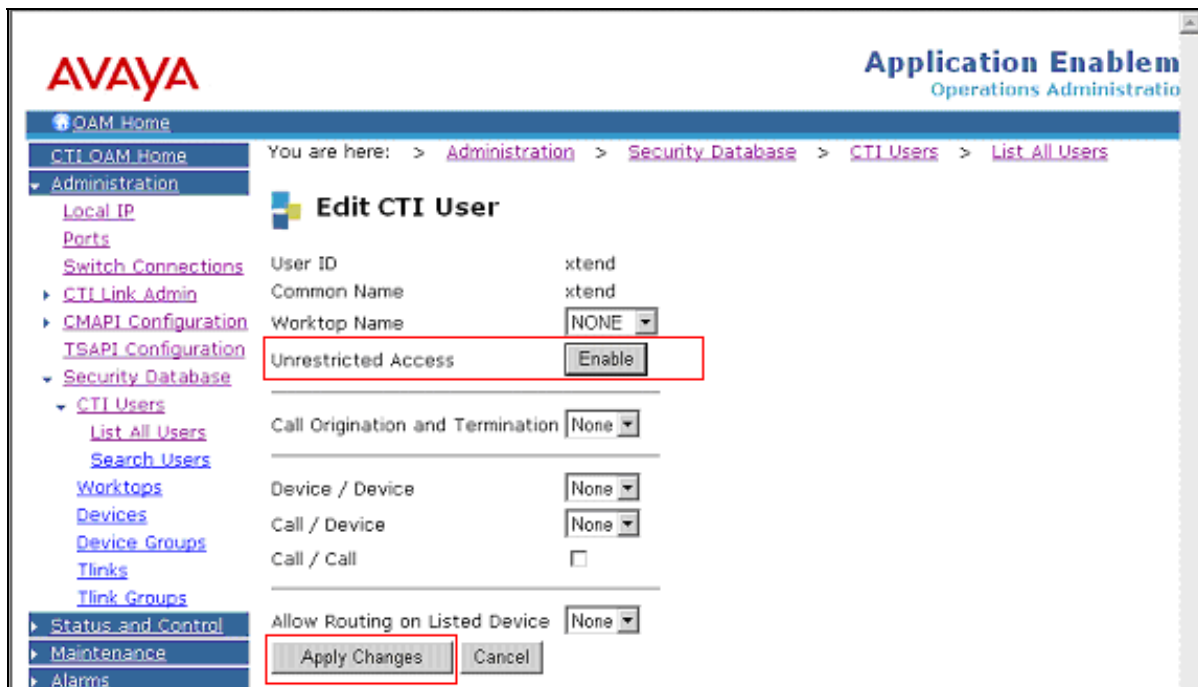
* User Id
* Common Name
* Surname
* User Password
* Confirm Password

Admin Note
Avaya Role
Business Category
Car License
CM Home
Ciss Home
CT User
Department Number
Display Name
Employee Number
Employee Type
Enterprise Handle
Given Name
Home Phone
Home Postal Address
Initials

Once the user is created, navigate to the **OAM Home** → **CTI OAM Admin** → **Administration** → **Security Database** → **CTI Users** → **List All Users** page. Select an appropriate Used ID, 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.



Navigate to the **OAM Home** → **CTI OAM Admin** → **Administration** → **Ports** page to set the CMAPI server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. If CMAPI Server Ports are changed, then, click the **Apply Changes** button to submit new values.

AVAYA Application Enablement Services
Operations Administration and Maintenance

[OAM Home](#) You are here: > [Administration](#) > [Ports](#) [Logout](#) [Help](#)

Ports

CVLAN Port	TCP Port	9999
DLG Port	TCP Port	5678
TSAPI Port	TCP Port	450

CSTA Tlinks Port

TCP Port Min	1050
TCP Port Max	1065

CMAPI Server Ports

	Enabled	Disabled
Unencrypted Port	<input type="radio"/> 4721	<input type="radio"/>
Encrypted Port	<input type="radio"/> 4722	<input type="radio"/>

H.323 Port

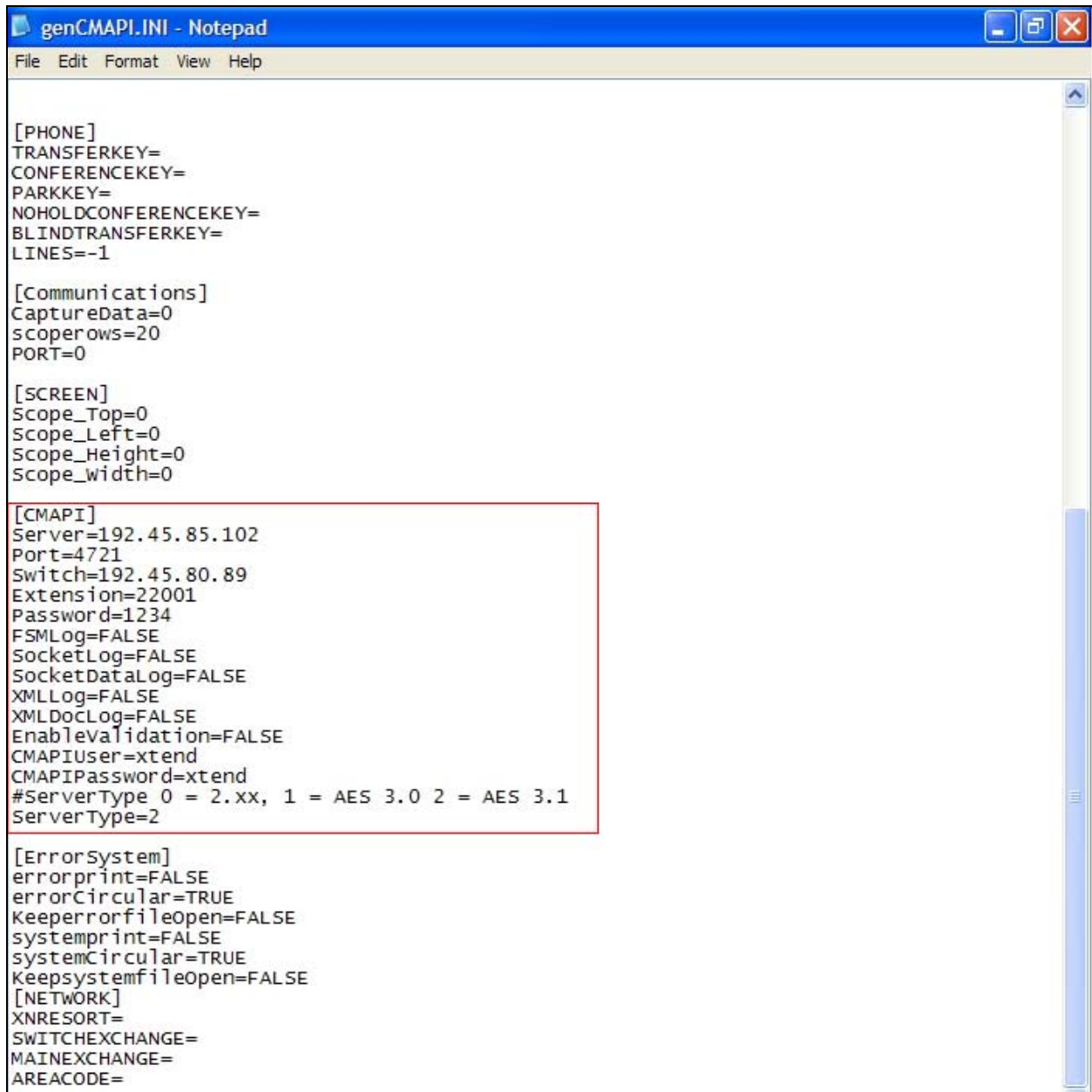
TCP Port Min	3000
TCP Port Max	4100
Local UDP Port Min	7000
Local UDP Port Max	8100
RTP Local UDP Port Min	5000
RTP Local UDP Port Max	5300

[Apply Changes](#) [Restore Defaults](#)

5. Configure XTEND XpressDesk

XTEND Communications installs and customizes XpressDesk for their end customers. Therefore, the only configuration that is relevant to the compliance test is “genCMAPI.ini” file, which specifies the CMAPI 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 CMAPI settings in the Avaya AES server in Section 4.1.



```
[PHONE]
TRANSFERKEY=
CONFERENCEKEY=
PARKKEY=
NOHOLDCONFERENCEKEY=
BLINDTRANSFERKEY=
LINES=-1

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

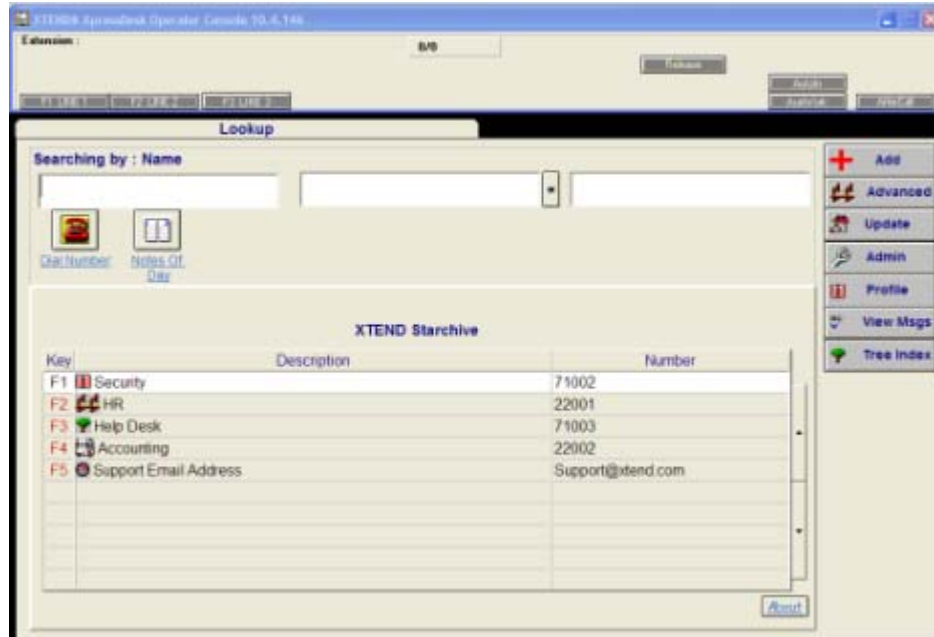
[SCREEN]
Scope_Top=0
Scope_Left=0
Scope_Height=0
Scope_Width=0

[CMAPI]
Server=192.45.85.102
Port=4721
Switch=192.45.80.89
Extension=22001
Password=1234
FSMLog=FALSE
SocketLog=FALSE
SocketDataLog=FALSE
XMLLog=FALSE
XMLDocLog=FALSE
EnableValidation=FALSE
CMAPIUser=xtend
CMAPIPassword=xtend
#ServerType 0 = 2.xx, 1 = AES 3.0 2 = AES 3.1
ServerType=2

[ErrorSystem]
errorprint=FALSE
errorCircular=TRUE
KeeperrorfileOpen=FALSE
systemprint=FALSE
systemCircular=TRUE
KeepsystemfileOpen=FALSE

[NETWORK]
XNRESORT=
SWITCHEXCHANGE=
MAINEXCHANGE=
AREACODE=
```

The following screen displays the XpressDesk Operator Console page.



6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability, and performance testing. The feature testing evaluated the ability of XpressDesk 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 XpressDesk can resume operation after failure recovery. The performance test stressed the XpressDesk application by continuously placing calls to a telephone controlled by XpressDesk over extended periods of time.

6.1. General Test Approach

The general approach was to exercise basic telephone and call operations on Avaya IP and Digital telephones using XpressDesk. 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 XpressDesk console.
- Manual operations performed on the physical telephones are correctly reflected in the XpressDesk console.
- XpressDesk and manual telephone operations may be used interchangeably, i.e. go offhook using XpressDesk and manually dial digits.
- Display and call information provided on the XpressDesk console are consistent with the actual display and call information on the physical telephones.
- Call states are consistent between XpressDesk 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.

For performance testing, a call generator continuously placed calls to a Vector Directory Number (VDN) that queues the calls in a hunt/skill group, which in turn delivers the calls to an agent logged into the hunt/skill group; the agent's physical telephone is controlled by XpressDesk.

6.2. Test Results

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

For serviceability testing, XpressDesk was able to resume control of Avaya IP and Digital telephones after restarts of the XpressDesk application and the computer on which it runs, and resets of the physical telephone, the Avaya AES server, and Avaya S8700 Media Server. For performance testing, XpressDesk successfully performed off-hook, on-hook, hold, retrieve, transfer, and conference call operations under a continuous call volume for extended periods of time.

7. Verification Steps

The following steps may be used to verify the configuration:

- From the PC or laptop on which XpressDesk runs, ping IP interfaces, in particular the CLAN and MedPro board(s) in the Avaya G650 Media Gateway, the Avaya AES server, and IP telephones, and verify connectivity.
- Go off-hook and on-hook on the controlled telephone manually and using XpressDesk, and verify consistency.
- Place and answer calls from the telephone manually and using XpressDesk, and verify consistency.

8. Support

For technical support on XTEND Communications products, call XTEND Communications at (212) 951-7670 or send email to support@xtend.com.

9. Conclusion

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

XpressDesk uses the CMAPI 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 XpressDesk applications.

10. References

This section references the Avaya and XTEND Communications 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 3.1, Issue 4, February 2006, Document Number 555-245-205.
- [2] *Application Enablement Services Administration and Maintenance Guide*, Release 3.1, Issue 2, February 2006, Document Number 02-300357

The following XTEND Communications product documentation is provided. For additional product and company information, visit <http://www.xtend.com>.

- [3] *Xtend MediCall/XpressDesk/AnswerPro Instructions for Operator Console*, 1/12/2007

©2007 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 the 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 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 Developer*Connection* Program at devconnect@avaya.com.