



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Cybertech Pro with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the compliance testing of the Cybertech Pro voice recording system with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. The document contains an extensive description of the configurations for both Cybertech Pro and Avaya Aura™ Communication Manager.

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

1. Introduction

The purpose of this document is to describe the compliance testing carried out with Cybertech Pro, Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. It includes a description of the configuration of both the Avaya and the Cybertech solutions, a description of the tests that were performed and a summary of the results of those tests.

Cybertech Pro is a voice recording system which can be used to record the voice stream of Avaya telephone endpoints. It uses Communication Manager's 'Service Observe' feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording.

The Device, Media and Call Control (DMCC) API associated with the AES server allows the creation of "Virtual" IP phones to monitor analogue, digital or VoIP extensions. A group of virtual IP phones is created in Communication Manager to be used by the CyberTech recorder application. These virtual phones are used to monitor the status of the target to be recorded. Recording can be activated using 'Service Observe' or 'Single Step Conference'. The method used is selected on the Cybertech recorder.

1.1. Interoperability Compliance Testing

The interoperability compliance tests included feature functionality and serviceability testing. The focus was on testing scenarios that involve interaction between the Cybertech Pro server, Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services, with various sequences involving the following:

- Verification of connectivity
- Verification of correct recording of basic internal and external calls
- Verification of correct recording for transfer, hold, and conference operations for internal and external calls
- Verification of call-back and bridged appearance operations
- Verification that agent information is included when monitoring calls to logged-in agents
- Verification of correct recovery after disconnection of various inter-device connections

The serviceability testing focused on verifying the Cybertech Pro's ability to recover from adverse conditions, such as disconnect from Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services.

1.2. Support

Technical support from Cybertech can be obtained through the following:

Cybertech Support Desk
Email: supportdesk@Cybertech-int.com
Telephone: +31 72 567 31 79

2. Reference Configuration

Cybertech Pro is a voice recording system which can be used to record the voice stream of Avaya telephone endpoints. The voice traffic of selected endpoints can be monitored and recorded to a voice data archive, with the time and call participants recorded with each call segment file.

The Avaya IP Telephony configuration used to verify these Application Notes is shown in **Figure 1**. The Application Enablement Services (AES) server was used by Cybertech Pro to receive call status information. Cybertech Pro then used Communication Manager “Service Observe” facility and “Single Step Conference” to collect voice data streams of endpoints which were selected to be monitored.

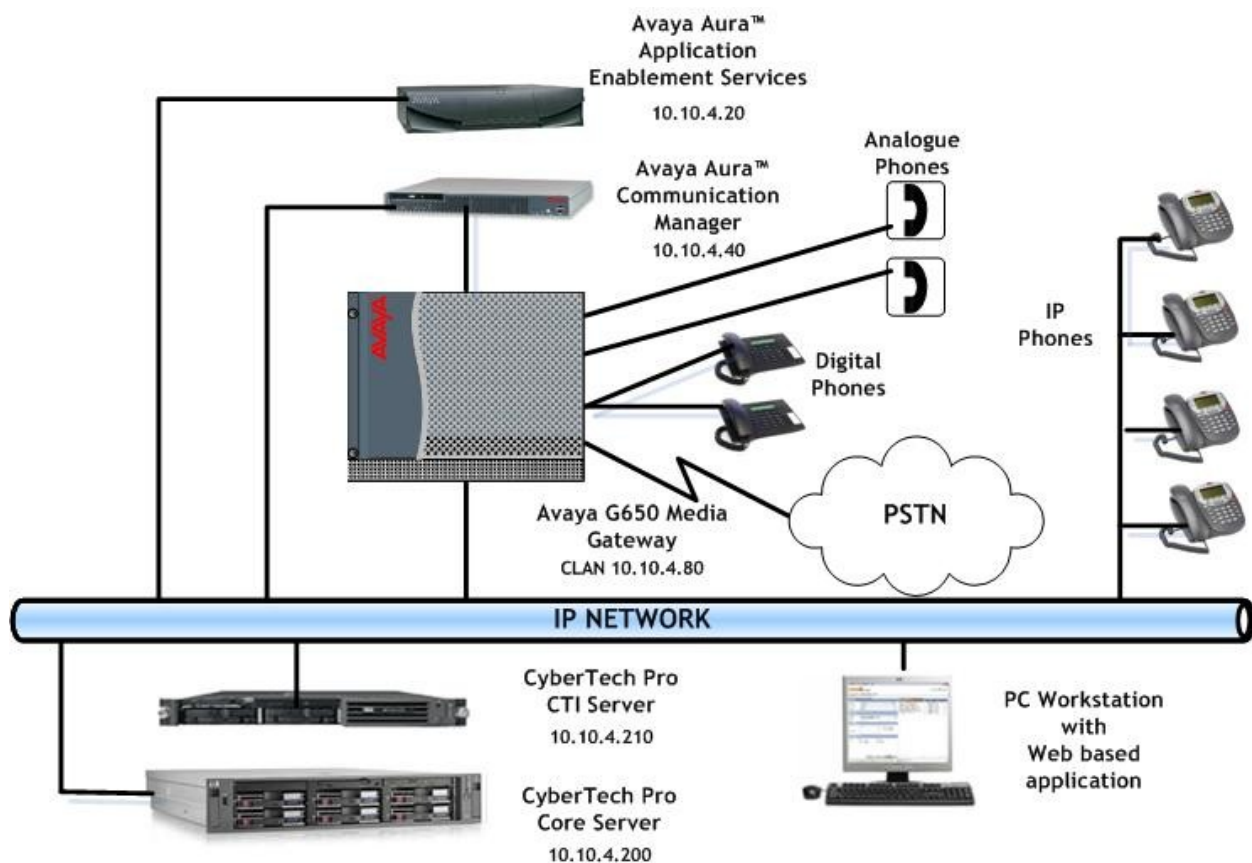


Figure 1: Cybertech Pro Test Configuration

3. Equipment and Software Validated

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

Equipment	Software Version
Avaya S8500B Server	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya S8500B Server	Avaya Aura™ Application Enablement Services 4.2.1
Avaya G650 Media Gateway IPSI TN2312BP CLAN TN799DP IP Media Processor TN2602AP Analog Card TN793CP DS1 Interface TN246CP Digital Line TN2214CP	HW15, FM45 HW01, FM31 HW02, FM47 HW09, FM010 HW02, FM022 HW08, FM015
Avaya 96xx and Series IP Telephones (H.323) 9640 9620 9630 9670G 2420 Analog Telephones – POTS	3.0 3.0 3.0 3.0 R5 N/A
Cybertech Recording server	Version 5.2.0.75
Cybertech CTI Server	Avaya_DMCC_Active_IP_5.8.0 Call Controller – 1.4.18.492 Avaya Link Controller - 1.2.14.271 Service Monitor 1.1.8.61

Table 1: Hardware and Software Version Numbers

4. Test Configuration

Table 2 contains the extensions that were used in the test. The capital letter designations correspond to the telephones shown in **Figure 1**. The virtual phones are softphones which were added to act as recording extensions.

Type of Phone	Phone Extension	Station	Button Allocation	Comments	IP Address
IP9630	3002	S1	3 x call-appr, serv-obsrv, brdg-appr D		10.10.4.52
IP9670G	3005	S2	3 x call-appr, serv-obsrv		10.10.4.54
Digital-2420	3009	A	3 x call-appr, auto-cback		
Digital-2420	3006	B	3 x call-appr, auto-cback, call-pkup	*Agent logged in	
IP9640	3000	C	3 x call-appr, brdg-appr D, call-pkup, auto-cback	*Agent logged in	
IP9620	3001	D	3 x call-appr		
POTS		E			
POTS		F			
IP Softphone	3012	Virtual 1	3 x call-appr, serv-obsrv	*Recording extension not visible	
IP Softphone	3013	Virtual 2	3 x call-appr, serv-obsrv	*Recording extension – not visible	
External CM	2502	G			
External CM	2501	H			

Table 2: Station Extensions and Details Used for Testing

5. Configuration of Communication Manager

The configuration and verification operations illustrated in this section were all performed using Avaya Aura™ Communication Manager System Administration Terminal (SAT).

The information provided in this section describes the configuration of Avaya Aura™ Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in reference [1].

The configuration operations described in this section can be summarized as follows:

- Verify that the licenses allocated to the system are sufficient to support the required configuration
- Configure system parameters and system features
- Allocate Feature Access Codes
- Configure IP node names
- Configure the telephone stations that are to be used for testing
- Configure virtual CTI telephone stations
- Configure Class of Restriction for recording devices
- Allocate a call pickup group
- Allocate agent resources
- Configure the interface to AES

The configuration of the PRI interface to the PSTN is outside the scope of these application notes.

5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Communication Manager is licensed to meet the minimum requirements to interoperate with the Cybertech Pro server. Those items shown in bold in the screen below indicate required values or minimum capacity requirements. If these are not met in the configuration, please contact an Avaya representative for further assistance.

On **Page 2**, the value configured for **Maximum Concurrently Registered IP Stations** must be sufficient to support the total number of IP stations used. For Voice Recording, the Maximum Concurrently Registered IP stations needs to be at least two times the number of targets.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks: 100	0	
Maximum Concurrently Registered IP Stations: 2400	0	
Maximum Administered Remote Office Trunks: 0	0	
Maximum Concurrently Registered Remote Office Stations: 0	0	
Maximum Concurrently Registered IP eCons: 0	0	
Max Concur Registered Unauthenticated H.323 Stations: 10	0	
Maximum Video Capable H.323 Stations: 10	0	
Maximum Video Capable IP Softphones: 10	0	
Maximum Administered SIP Trunks: 10	0	
Maximum Administered Ad-hoc Video Conferencing Ports: 10	0	
Maximum Number of DS1 Boards with Echo Cancellation: 0	0	
Maximum TN2501 VAL Boards: 10	0	
Maximum Media Gateway VAL Sources: 0	0	
Maximum TN2602 Boards with 80 VoIP Channels: 128	0	
Maximum TN2602 Boards with 320 VoIP Channels: 128	1	
Maximum Number of Expanded Meet-me Conference Ports: 0	0	

Verify with the Avaya account team that the required licenses are installed. In this test the following parameters were used though not all may be required for the solution. On **Page 3** the parameters are set as follows:

- **Answer Supervision by Call Classifier?** to y
- **Computer Telephony Adjunct Links?** to y

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

On **Page 4**, the **IP Stations** parameter must be set to **y** so that IP stations can be configured.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	IP Stations? y	
Enable 'dadmin' Login? y		
Enhanced Conferencing? n	ISDN Feature Plus? n	
Enhanced EC500? n	ISDN/SIP Network Call Redirection? n	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	ISDN-PRI? y	
ESS Administration? n	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? n	Malicious Call Trace? n	
External Device Alarm Admin? n	Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? n	Multifrequency Signaling? y	

On **Page 6**, the **EAS-PHD** parameter must be set to **y** so that skill levels greater than 3 can be selected. This is not mandatory for recording but was used in testing.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 5.0		
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)? y	
Call Work Codes? n	Timed ACW? n	
DTMF Feedback Signals For VRU? n	Vectoring (Basic)? y	
Dynamic Advocate? n	Vectoring (Prompting)? y	
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y	
EAS-PHD? y	Vectoring (3.0 Enhanced)? y	
Forced ACD Calls? n	Vectoring (ANI/II-Digits Routing)? y	
Least Occupied Agent? n	Vectoring (G3V4 Advanced Routing)? y	
Lookahead Interflow (LAI)? n	Vectoring (CINFO)? y	
Multiple Call Handling (On Request)? n	Vectoring (Best Service Routing)? y	
Multiple Call Handling (Forced)? n	Vectoring (Holidays)? y	
PASTE (Display PBX Data on Phone)? n	Vectoring (Variables)? y	

5.2. Configure System Parameters Features

Use the **change system-parameters features** command to set the **Call Pickup Alerting?** and **Directed Call Pickup?** parameters to **y**. These features were used in testing but are not mandatory for recording.

display system-parameters features		Page 18 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
IP PARAMETERS		
	Direct IP-IP Audio Connections?	y
	IP Audio Hairpinning?	n
	SDP Capability Negotiation for SRTP?	n
CALL PICKUP		
	Maximum Number of Digits for Directed Group Call Pickup:	4
	Call Pickup on Intercom Calls?	y
	Temporary Bridged Appearance on Call Pickup?	y
	Extended Group Call Pickup:	none
	Enhanced Call Pickup Alerting?	n
	Display Information With Bridged Call?	n
	Keep Bridged Information on Multiline Displays During Calls?	n
	PIN Checking for Private Calls?	N

On **Page 11** ensure the features were set as follows to allow service observing.

- **Service Observing: Warning Tone?** to **y**. It is not mandatory for recording but was used in testing.
- **Allow Two Observers in Same Call?** to **y**

display 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:	
	Direct Agent Announcement Extension:	Delay:
	Message Waiting Lamp Indicates Status For:	station
VECTORIZING		
	Converse First Data Delay:	0
	Converse Signaling Tone (msec):	100
	Prompting Timeout (secs):	10
	Second Data Delay:	2
	Pause (msec):	70
	Reverse Star/Pound Digit For Collect Step?	n
	Available Agent Adjustments for BSR?	n
	BSR Tie Strategy:	1st-found
	Store VDN Name in Station's Local Call Log?	n
SERVICE OBSERVING		
	Service Observing: Warning Tone?	y or Conference Tone? n
	Service Observing Allowed with Exclusion?	n
	Allow Two Observers in Same Call?	y

Universal Call ID is used to uniquely identify calls. **On Page 5** of the system-parameters features form, set **Create Universal Call ID (UCID)?** to **y** and **UCID Network Node ID** to an unassigned node ID.

display system-parameters features		Page 5 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
SYSTEM PRINTER PARAMETERS		
Endpoint:	Lines Per Page: 60	
SYSTEM-WIDE PARAMETERS		
	Switch Name:	
	Emergency Extension Forwarding (min): 10	
	Enable Inter-Gateway Alternate Routing? n	
	Enable Dial Plan Transparency in Survivable Mode? n	
	COR to Use for DPT: station	
MALICIOUS CALL TRACE PARAMETERS		
	Apply MCT Warning Tone? n	MCT Voice Recorder Trunk Group:
SEND ALL CALLS OPTIONS		
	Send All Calls Applies to: station	Auto Inspect on Send All Calls? n
UNIVERSAL CALL ID		
	Create Universal Call ID (UCID)? y	UCID Network Node ID: 1

On Page 13, set **Send UCID to ASAI?** to **y**.

display system-parameters features		Page 13 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
CALL CENTER MISCELLANEOUS		
	Clear Callr-info: next-call	
	Allow Ringer-off with Auto-Answer? n	
	Reporting for PC Non-Predictive Calls? n	
ASAI		
	Copy ASAI UUI During Conference/Transfer? n	
	Call Classification After Answer Supervision? y	
	Send UCID to ASAI? y	

On Page 16, set **Automatic Exclusion by COS?** to **y**.

display system-parameters features		Page 16 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
AUTOMATIC EXCLUSION PARAMETERS		
	Automatic Exclusion by COS? y	
	Automatic Exclusion Coverage/Hold? n	
	Automatic Exclusion with Whisper Page? n	
	Recall Rotary Digit: 2	
	Duration of Call Timer Display (seconds): 3	
WIRELESS PARAMETERS		
	Radio Controllers with Download Server Permission (enter board location)	
1:	2:	3: 4: 5:

5.3. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure all of the access codes shown in the table below.

Parameter	Usage
Call Pickup Access Code	This is used by telephone users to initiate a call-pickup operation.
Auto-in	This is used by agents to indicate readiness.
Login	Agent login.
Logout	Agent logout.
Service Observing No Talk	This is used by the voice recorder to receive the voice stream without send voice data. Value used below (#3) is a free choice, the value chosen must match the Cybertech configuration settings.

Table 3: Feature Access Codes

The values set for each option can be seen highlighted on **Page 1** and **Page 5** in the figures below.

change feature-access-codes	Page 1 of 8
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code:	
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code:	
Auto Route Selection (ARS) - Access Code 1:	Access Code 2:
Automatic Callback Activation:	Deactivation:
Call Forwarding Activation Busy/DA: All:	Deactivation:
Call Forwarding Enhanced Status: Act:	Deactivation:
Call Park Access Code:	
Call Pickup Access Code: #4	
CAS Remote Hold/Answer Hold-Unhold Access Code:	
CDR Account Code Access Code:	
Change COR Access Code:	
Change Coverage Access Code:	
Contact Closure Open Code:	Close Code:

The feature access codes set below are referenced in **Table 3**.

change feature-access-codes	Page 5 of 8
FEATURE ACCESS CODE (FAC)	
Automatic Call Distribution Features	
After Call Work Access Code:	
Assist Access Code:	
Auto-In Access Code: #2	
Aux Work Access Code:	
Login Access Code: #6	
Logout Access Code: #5	
Manual-in Access Code:	
Service Observing Listen Only Access Code:	
Service Observing Listen/Talk Access Code:	
Service Observing No Talk Access Code: #3	
Add Agent Skill Access Code:	
Remove Agent Skill Access Code:	
Remote Logout of Agent Access Code:	

5.4. Configure Node Names

Ensure that the CLAN IP address is in the node-names form. 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 'PresAES' IP address was used for connectivity to Avaya AES.

change node-names ip	Page 1 of 2
IP NODE NAMES	
Name	IP Address
CLAN	10.10.4.80
MEDPRO	10.10.4.90
PresAES	10.10.4.40
default	0.0.0.0
procr	10.255.255.100

5.5. Configure Telephone Stations

Use the **add station** command to configure all of the telephones shown in **Section 4, Table 2**. Refer to this table when allocating names and button assignments for each test phone.

On **Page 1, Phone A, Extension 3009**, is a digital phone therefore a **Type** of **2420** is chosen.

add station 3009		Page 1 of 5
STATION		
Extension: 3009	Lock Messages? n	BCC: 0
Type: 2420	Security Code:	TN: 1
Port: 01A0607	Coverage Path 1:	COR: 1
Name: Phone A	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 2	Time of Day Lock Table:	
Data Option: none	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 3009	
Display Language: english	Mute Button Enabled? y	
	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
Customizable Labels? Y		

Add the appropriate button assignments as shown in the screen on **Page 4** below.

add station 3009		Page 4 of 5
STATION		
SITE DATA		
Room:	Headset? n	
Jack:	Speaker? n	
Cable:	Mounting: d	
Floor:	Cord Length: 0	
Building:	Set Color:	
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3: call-appr	7:	
4: auto-cback	8:	
voice-mail Number:		

Repeat this process to add stations for telephones B, C, D, S1 and S2 as displayed in **Table 2, Section 4**.

To use the exclusion functionality on an extension set a restriction on a station as shown below.
 Use the **change station x**, command where **x** is the station chosen for exclusion.
 On **Page 1**, set **COS** to **1**. This value will be configured in **Section 5.8**.

change station 3005		Page 1 of 5
STATION		
Extension: 3005	Lock Messages? n	BCC: 0
Type: 4620	Security Code: 3005	TN: 1
Port: S00007	Coverage Path 1:	COR: 1
Name: S2	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: 3005	
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	

On **Page 2**, set the **Data Restriction** to **y**.

change station 3005		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? y	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: disabled	
Multimedia Mode: enhanced		
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 3005	Always Use? n IP Audio Hairpinning? N	

5.6. Configure CTI Telephone Stations

Use the **add station** command to configure a station for each of the virtual endpoints shown in **Table 2, Section 4**. Each of the virtual stations has a **Type** of **4620**. Enter in a descriptive **Name** and **Security Code** for each one. Set the **IP Softphone?** to **y**.

change station 3012		Page 1 of 5
STATION		
Extension: 3012	Lock Messages? n	BCC: 0
Type: 4620	Security Code: 3012	TN: 1
Port: S00013	Coverage Path 1:	COR: 1
Name: Virtual 1	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: 3012	
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? y	
	IP Video Softphone? n	
	Customizable Labels? Y	

Allocate the button assignments as shown in the screen below. Create a **serv-obsrv** button to initiate a service observe from the CTI server.

change station 3012		Page 4 of 5
STATION		
SITE DATA		
Room: [B		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3: call-appr	7:	
4: serv-obsrv	8:	

5.7. Configure COR

Set the class of restriction so that the stations can all be service observed by a recording device.

Set the values in the following screen as follows:

- **Can Be Service Observed?** as y
- **Can Be A Service Observer?** as y

change cor 1	Page 1 of 23
CLASS OF RESTRICTION	
COR Number: 1	
COR Description:	
FRL: 0	APLT? y
Can Be Service Observed? y	Calling Party Restriction: none
Can Be A Service Observer? y	Called Party Restriction: none
Partitioned Group Number: 1	Forced Entry of Account Codes? n
Priority Queuing? n	Direct Agent Calling? y
Restriction Override: none	Facility Access Trunk Test? n
Restricted Call List? n	Can Change Coverage? n
Access to MCT? y	Fully Restricted Service? n
Group II Category For MFC: 7	Add/Remove Agent Skills? y
Send ANI for MFE? n	Automatic Charge Display? n
MF ANI Prefix:	PASTE (Display PBX Data on Phone)? n
Hear System Music on Hold? y	Can Be Picked Up By Directed Call Pickup? y
	Can Use Directed Call Pickup? y
	Group Controlled Restriction: inactive

On Page 2 set the value **Service Observing by Recording Device?** to y.

change cor 1	Page 2 of 23
CLASS OF RESTRICTION	
MF Incoming Call Trace? n	
Brazil Collect Call Blocking? n	
Block Transfer Display? n	
Block Enhanced Conference/Transfer Displays? y	
Remote Logout of Agent? n	
Station Lock COR: 1 TODSL Release Interval (hours):	
Outgoing Trunk Disconnect Timer (minutes):	
Station-Button Display of UI IE Data? n	
Service Observing by Recording Device? y	
ERASE 24XX USER DATA UPON	
Dissociate or unmerge this phone: none	
EMU login or logoff at this phone: none	
Mask CPN/NAME for Internal Calls? n	

5.8. Configure COS

Set a Class of Service (COS) to facilitate data privacy and exclusion by stations.

On **Page 1**, set **Data Privacy** to **y** and **Automatic Exclusion** to **y** for the **COS 1**. This is the COS of the station to be excluded as identified in **Section 5.5**.

change cos																Page	1	of	2
CLASS OF SERVICE																			
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15			
Auto Callback	n	y	y	n	y	n	y	n	y	n	y	n	y	n	y	n			
Call Fwd-All Calls	n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y			
Data Privacy	y	y	n	n	n	y	y	y	y	n	n	n	n	n	y	y			
Priority Calling	n	y	n	n	n	n	n	n	n	y	y	y	y	y	y	y			
Console Permissions	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Off-hook Alert	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Client Room	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Restrict Call Fwd-Off Net	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y			
Call Forwarding Busy/DA	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Personal Station Access (PSA)	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Extended Forwarding All	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Extended Forwarding B/DA	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Trk-to-Trk Transfer Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n			
Automatic Exclusion	y	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n			

5.9. Configure Agents

A hunt group, Vector Directory Number (VDN), vector and two agent logins were created as in the following table. These were created for testing purposes only.

	Value	Name
VDN	1800	VDN1800
Vector	1	Vector1
Skill Ext\Hunt Groups	35001/1	Agent HG1
Agent Login	6001 6002	AgentB AgentC

Table 4: Call Center Agent Details

5.9.1. Configure Agent Hunt Group

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 **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to yes (**y**) as shown below.

- **ACD?** to **y**
- **Queue?** to **y**
- **Vector?** to **y**
- **Group Type** to **ucd-mia** to specify that the system hunts for the “most idle agent”.

add hunt-group 1		Page 1 of 61	
HUNT GROUP			
Group Number: 1		ACD? y	
Group Name: Agent HG1		Queue? y	
Group Extension: 35000		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 **Skill?** to **y** to indicate that this is a skilled hunt group.

add hunt-group 1		Page 2 of 61	
HUNT GROUP			
Skill? y		Expected Call Handling Time (sec): 180	
AAS? n			
Measured: none			
Supervisor Extension:			
Controlling Adjunct: none			
Redirect on No Answer (rings):			
Redirect to VDN:			
Forced Entry of Stroke Counts or Call Work Codes? N			
Redirect on No Answer (rings):			
Redirect to VDN:			
Forced Entry of Stroke Counts or Call Work Codes? n			

5.9.2. Configure Agent Queue Vector

Enter the **add vector n** command; where **n** is associated to hunt group 1. The **Vector number** is set to **1**. Enter the vector steps to queue to the 1st skill on the VDN as shown below.

```
add vector 1                                     Page 1 of 6
                                           CALL VECTOR
Number: 1                                     Name: Vector1
Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   Lock? n
Prompting? y   LAI? n   G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
Variables? y   3.0 Enhanced? y
01 wait-time   2 secs hearing ringback
02 queue-to    skill 1   pri m
03
```

5.9.3. Configure Agent VDN

Use the **add vdn n** command to create a Vector Directory Number extension which can be used to reference the Operator queue vector. Set the values **Name** and **Vector Number 1** by referencing **Table 3, Section 5.8** above. The **1st Skill** is set to **1**.

```
add vdn 1800                                     Page 1 of 3
                                           VECTOR DIRECTORY NUMBER
Extension: 1800
Name*: VDN1800
Vector Number: 1
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none
1st Skill*: 1
2nd Skill*:
3rd Skill*:
```

Set **Observe on Agent Answer?** to **y** on **Page 2**. This will initiate service observe after the agent has answered the call.

```
add vdn 1800                                     Page 2 of 3
                                           VECTOR DIRECTORY NUMBER
AUDIX Name:
BSR Available Agent Strategy*: 1st-found
BSR Tie Strategy*: system
Observe on Agent Answer? y
Display VDN for Route-To DAC*? n
VDN Override for ISDN Trunk ASAI Messages*? n
Reporting for PC Predictive Calls? N
```

5.9.4. Configure Agent Login

Use the **add agent-loginID n** command; where **n** is a valid extension under the provisioned dialplan. Two agents are created at stations B and C as in **Table 2, Section 4**. The agent loginID chosen is **6001**. Enter a descriptive name for the agent in the **Name** field and set **Password**.

add agent-loginID 6001		Page 1 of 2	
AGENT LOGINID			
Login ID: 6001		AAS? n	
Name: AgentB		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: 6001	
		Password (enter again): 6001	
		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: :			

Specify the list of skills assigned to the login and the skill level for each of them in the **SN/SL** field as shown below. Set the **Skill Number** to **1**, it should be the same as that configured for the associated vector number. The **Skill Level** is set to **1**.

add agent-loginID 6001		Page 2 of 2	
AGENT LOGINID			
Direct Agent Skill:			
Call Handling Preference: skill-level		Local Call Preference? n	
SN	SL	SN	SL
1: 1	1	16:	
2:		17:	
		31:	
		32:	
		46:	
		47:	

5.10. Configure Pickup Group

Create a pickup group which contains stations A, B, C, D. This is used in conjunction with the “call-pkup” button which is allocated to endpoint B, as shown in **Section 4, Table 2**. Use the command; **add pickup-group 1** to add this group as shown below. Assign a name and add extensions.

```
add pickup-group 1                                     Page 1 of 4

                                PICKUP GROUP

        Group Number: 1
        Group Name: CallPickUP
GROUP MEMBER ASSIGNMENTS

    Extension      Name
1: 3009
2: 3006
3: 3000
4: 3001
5:
6:
```

5.11 Configure Interface to Avaya AES

The Application Enablement Services server has a TSAPI interface which provides Cybertech Pro with a means of communicating with Communication Manager to perform telephony operations. Communication Manager requires the configuration parameters shown in this section.

Use the **add ip-interface** command to allocate a call control interface. The slot value specified should be the CLAN interface. The value used as **Node Name** must be one of the names from the list defined by the **change node-names ip** command. The **Subnet Mask** and **Gateway Address** should be assigned to the values used by the Ethernet network to which the CLAN is attached.

```
add ip-interface 01a02                                Page 1 of 2

                                IP INTERFACES

        Type: C-LAN
        Slot: 01A02
    Code/Suffix: TN799 D
        Node Name: CLAN
        IP Address: 10 .10 .4 .80
        Subnet Mask: 255.255.255.0                               Link: 1
        Gateway Address: 10 .10 .4 .1
    Enable Ethernet Port? y
        Network Region: 1
        VLAN: n
        Allow H.323 Endpoints? y
        Allow H.248 Gateways? y
        Gatekeeper Priority: 5

    Target socket load and Warning level: 400
    Receive Buffer TCP Window Size: 8320
                                ETHERNET OPTIONS
        Auto? y
```

Use the **change ip-services** command to set the parameters for **AESVCS** service for the CLAN as shown below. This was defined above to serve as the interface to the Avaya AES server. On **Page 1** add **CLAN** as the **Local Node** and accept default of **8765** as **Local Port**.

change ip-services					Page	1 of	3
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	CLAN	8765				

On **Page 3** an entry for the Avaya AES server must be made in the list in the screen shown below. The name assigned to the Avaya AES server when it was installed must be entered in the **AE Services Server** field for that entry. The **Password** entry must the same as that assigned to the switch connection, as shown in **Section 6.2** of this document.

change ip-services				Page 3 of 3
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	~~~~~	xxxxxxxxxxx	n	idle
2:	PresAES	xxxxxxxxxxxxx	y	in use
3:				

Use the **add cti-link** command to add a CTI link for use by TSAPI. The link number can be any value between 1 and 64 which is not currently assigned to another link. The link number specified must be the same value that is used in the **Add / Edit TSAPI Links** configuration screen shown in **Section 6.3** of this document. Use an unused extension as the value for the **Extension** parameter. The value chosen for the **Name** parameter is a matter of personal preference. Specify a **Type** of **ADJ-IP**, as required for a TSAPI link.

add cti-link 10		Page 1 of 3
CTI LINK		
CTI Link: 10		
Extension: 5002		
Type: ADJ-IP		
Name: PresAES		COR: 1

Use the **add data-module n** command; where **n** is an unassigned extension, to allocate an extension to be used as the data interface for the clan module. The value used as **Data Extension** can be any free extension. The **Name** value is only used for identification purposes. The **Type** field must be **ethernet**. The **Port** should be assigned to port 17 of the CLAN interface. The **Link** number should be assigned a value between 1 and 99.

add data-module 3400	
DATA MODULE	
Data Extension: 3400	Name: CLAN
Type: ethernet	
Port: 01A0217	
Link: 1	
Network uses 1's for Broadcast Addresses? y	

6. Configuration of Avaya AES

The information provided in this section describes the configuration of Application Enablement Services for this solution. The configuration includes the following areas:

- Verify Application Enablement Services License
- Create Switch Connection
- Administer TSAPI link
- Add CTI User
- Enable CTI Link User
- Set DMCC Port

6.1. Verify Avaya AES Licensing

The Avaya AES server is configured via a web browser by accessing the following URL:

<https://<Avaya AES server address>/>

Once the login screen appears, enter the OAM Admin login ID/password to perform administrative activities on the AE Server. Verify that Communication Manager/AES is licensed for DMCC by consulting with your Avaya account manager or Business Partner to acquire the proper license for your solution.

From the OAM Home screen select **CTI OAM Admin** (not shown) to bring up the CTI OAM Home menu. Verify that the TSAPI service is licensed at the Welcome to CTI OAM Screens screen by ensuring that **TSAPI Service** and **DMCC Service** are in the list of services in the License Information section.

AVAYA **Application Enablement Services**
Operations Administration and Maintenance

[OAM Home](#) [Help](#) [Logout](#)

You are here: > [CTI OAM Home](#)

Welcome to CTI OAM Screens

[craft] Last login: Mon Feb 23 19:05:58 2009 from 135.64.21.180

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	No
DLG Service	Running	OFFLINE	Yes
Transport Layer Service	Running	N/A	N/A
TSAPI Service	Running	ONLINE	Yes
SMS	N/A	N/A	No

For status on actual services, please use [Status and Control](#).

License Information

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

6.2. Create Switch Connection

Navigate to **Administration → Switch Connections**. Enter the name of the Switch Connection to be added and click on the **Add Connection** button. The screen below displays the active switch connection once it has been added.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top navigation bar includes the Avaya logo and the title 'Application Enablement Services - Operations Administration and Maintenance'. A breadcrumb trail indicates the current location: 'You are here: > Administration > Switch Connections'. The left sidebar contains a menu with 'Administration' expanded, showing options like 'Network Configuration', 'Switch Connections', 'CTI Link Admin', 'DMCC Configuration', 'TSAPI Configuration', 'Security Database', 'Certificate Management', 'Dial Plan', and 'Enterprise Directory'. The main content area is titled 'Switch Connections' and features a table with the following data:

Connection Name	Number of Active Connections
CMCyber	1

Below the table are buttons for 'Edit Connection', 'Edit CLAN IPs', 'Edit H.323 Gatekeeper', and 'Delete Connection'. An 'Add Connection' button is located at the top right of the table area.

Following the addition of the switch connection the AES Set Switch Connection Password screen is displayed. Enter the screen fields as described below and click the **Apply** button.

- **Switch Password:** The Switch Password must be the same as that entered into Communication Manager AE Services screen via the **change ip-services** command, described in **Section 5.11**.
- **SSL:** This is enabled

The screenshot shows the 'Set Password - New' screen in the Avaya Application Enablement Services (AES) interface. The top navigation bar and breadcrumb trail are the same as in the previous screenshot. The left sidebar menu is also the same. The main content area is titled 'Set Password - New' and includes the following information:

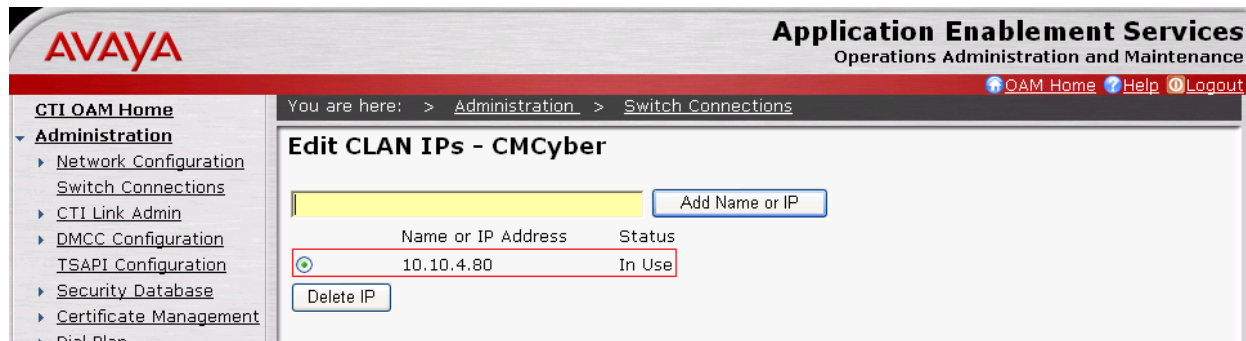
Please note the following:
* Changing the password affects only new connections, not open connections.

Fields for input:

- Switch Password: [Redacted]
- Confirm Switch Password: [Redacted]
- SSL: ☒

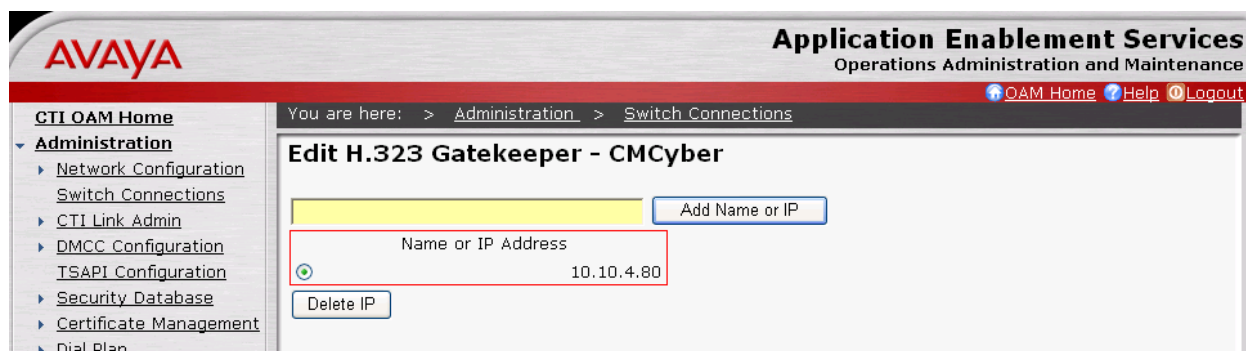
Buttons for 'Apply' and 'Cancel' are located at the bottom of the form.

The CLAN IP address must then be set on the AES. From the **Administration → Switch Connections** screen (not shown), click the **Edit CLAN IPs** button. Enter the IP address of the CLAN which the Avaya AES is to use for communication with Communication Manager as defined in **Section 5.11**. Click the **Add Name or IP** button (not shown). The following screen displays the added CLAN IP address.



The H.323 Gatekeeper should be set up to point to the Communication Manager where the virtual extensions are registered. Enter the CLAN IP address which will be used for the DMCC service.

Navigate to **CTI OAM Home → Administration → Switch Connection → Edit H323 Gatekeeper**. Enter the IP Address and click **Add Name or IP** button. The screen below shows the added IP address.



6.3. Administer TSAPI Link

From the CTI OAM Home menu, select **Administration** → **CTI Link Admin** → **TSAPI Links**. On the TSAPI Links screen (not shown), select **Add Link**. On the **Add/Edit TSAPI Links** screen, enter the following values:

- **Link:** Select an unused link number. The link number chosen is **1**.
- **Switch Connection:** The “Switch Connection” parameter should be the name of the Avaya Media Server which is to be controlled by this link. Choose the switch connection **CMCyber**, which has already been configured from the drop-down list.
- **Switch CTI Link Number:** Use the corresponding CTI link number configured in **Section 5.11** which is **10**.
- **Security:** **Both** is the option chosen here. The customer can choose Secure\UnSecure\Both.

Once completed, select **Apply Changes**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > CTI Link Admin > TSAPI Links

Add / Edit TSAPI Links

Link: 1
Switch Connection: CMCyber
Switch CTI Link Number: 10
ASAI Link Version: 4
Security: Both

Apply Changes Cancel Changes

The AES must be restarted to affect the changes made in this section. From the CTI OAM Home menu, select **Maintenance** → **Service Controller**. On the Service Controller screen, select **Restart AE Server**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Maintenance > Service Controller

Service Controller

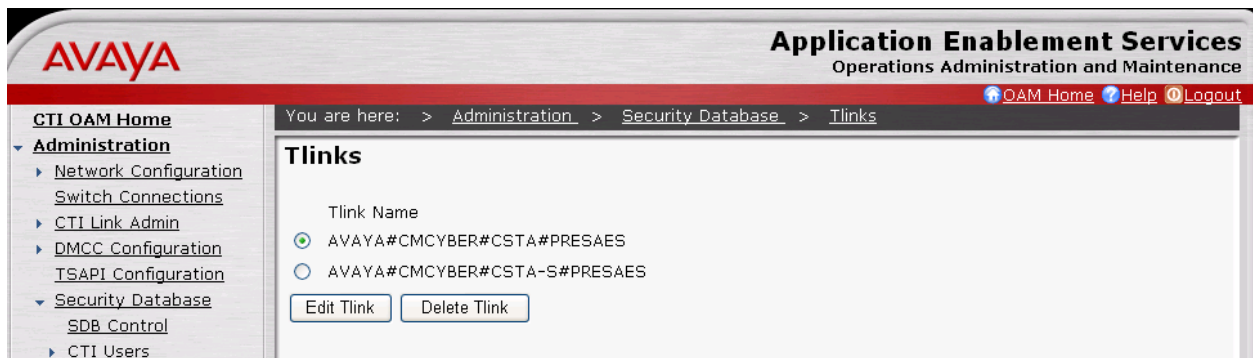
Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#).

Start Stop Restart Service **Restart AE Server** Restart Linux Restart Web Server

Restart AE Server screen (not shown), select **Restart**. Wait at least 10 minutes and select **Maintenance → Service Controller**. On the Service Controller screen, verify that all services show **Running** in the **Controller Status** column (not shown).

Navigate to the Tlinks screen by selecting **Administration → Security Database → Tlinks**. Note the value of the **Tlink Name**, as this will be needed for configuring the Cybertech server in **Section 7.3**. The **Tlink Name** shown below is automatically created by the AES server.



6.4. Create Avaya CTI User

A User ID and password needs to be configured for the Cybertech Pro server to communicate as a TSAPI Client with the AES server to monitor stations and initiate switching operations. Click on **OAM Home** → **User Management** and log into the **User Management** page. Click on **User Management** and then **Add User**.

In the **Add User** screen shown below, enter the following values:

- **User ID** – This will be used by the Cybertech server in **Section 7.3**.
- **Common Name and Surname** – A descriptive name needs to be entered.
- **New Password and Confirm Password** – This will be used with the User Id in **Section 7.3**.
- **CT User** – Select **Yes** from the drop-down menu

Complete the process by choosing **Apply** (not shown) at the bottom of the screen.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top header includes the Avaya logo and the text "Application Enablement Services Operations Administration and Maintenance". A navigation bar contains links for "OAM Home", "Help", and "Logout". The left sidebar shows a menu with "User Management Home" and a list of options: "List All Users", "Add User", "Search Users", "Modify Default User", "Change User Password", "Service Management", and "Help". The main content area is titled "Add User" and includes a breadcrumb trail: "You are here: > User Management > Add User". Below the title, a note states "Fields marked with * can not be empty." The form contains the following fields: "* User Id" (text box with "CTIUser"), "* Common Name" (text box with "CTIUser"), "* Surname" (text box with "CTIUser"), "* User Password" (password box with 10 dots), "* Confirm Password" (password box with 10 dots), "Admin Note" (text box), "Avaya Role" (dropdown menu with "None" selected), "Business Category" (text box), "Car License" (text box), "CM Home" (text box), "Css Home" (text box), "CT User" (dropdown menu with "Yes" selected), "Department Number" (text box), and "Display Name" (text box).

6.5. Enable CTI User

Navigate to the CTI Users by selecting **Administration** → **Security Database** → **CTI Users** → **List All Users**. Select the **CTIUser** user that was set up in **Section 6.4** and select the **Edit** option. For the **Unrestricted Access** option, select the **Enable** button and **Apply Changes** at the bottom of the screen.

The screenshot shows the Avaya Application Enablement Services interface. The left sidebar contains a navigation menu with options like 'Administration', 'Security Database', and 'CTI Users'. The main content area is titled 'Edit CTI User' and displays various configuration fields for the 'CTIUser'. The 'Unrestricted Access' field has an 'Enable' button highlighted with a red box. At the bottom, the 'Apply Changes' button is also highlighted with a red box.

6.6. Configure DMCC Ports

Navigate to **CTI OAM Home** → **Administration** → **Network Configuration** → **Ports** to set the DMCC server port. During the compliance test, the **Encrypted Port** was enabled as shown in the following screen. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

The screenshot shows the 'DMCC Server Ports' configuration screen. It has a table with three rows: 'Unencrypted Port', 'Encrypted Port', and 'TR/87 Port'. Each row has a text input field for the port number and two radio buttons labeled 'Enabled' and 'Disabled'. The 'Encrypted Port' row is highlighted with a red box, showing the port number 4722 and the 'Enabled' radio button selected.

DMCC Server Ports	Enabled	Disabled
Unencrypted Port 4721	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port 4722	<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port 4723	<input type="radio"/>	<input checked="" type="radio"/>

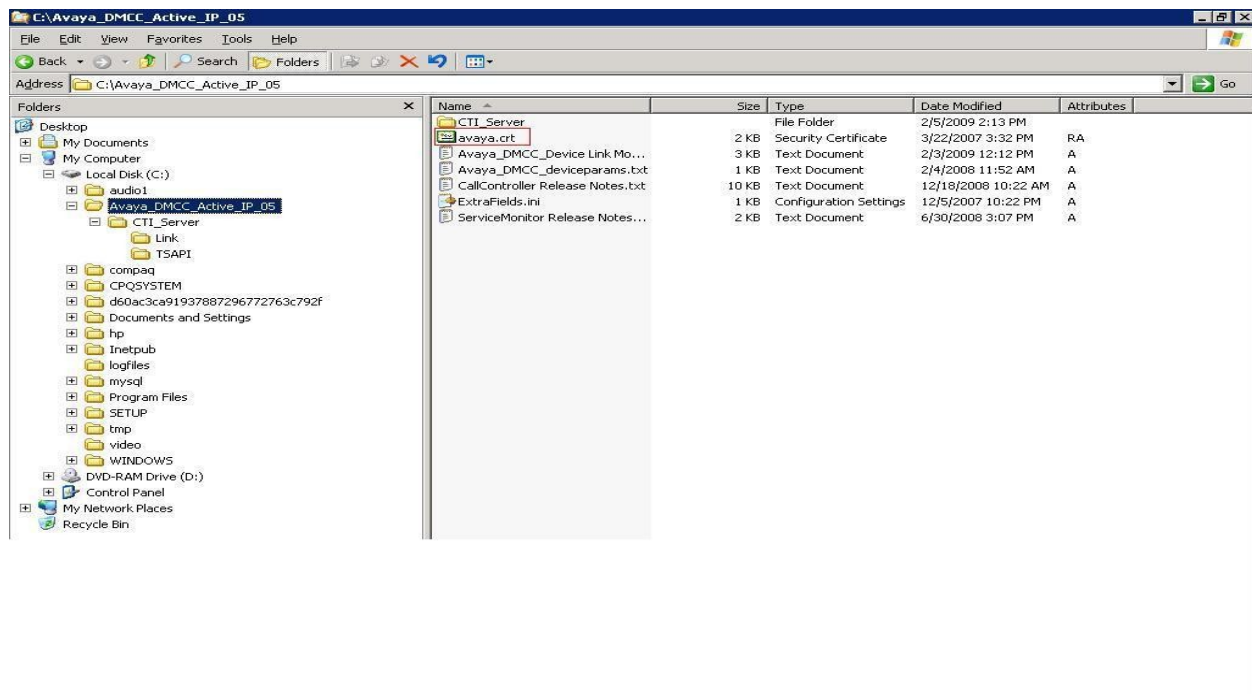
7. Configure Cybertech CTI Server

The Cybertech Pro CTI server is largely pre-configured for the customer by Cybertech prior to delivery. This section shows those configuration steps which need to be made after delivery. The configuration includes the following areas:

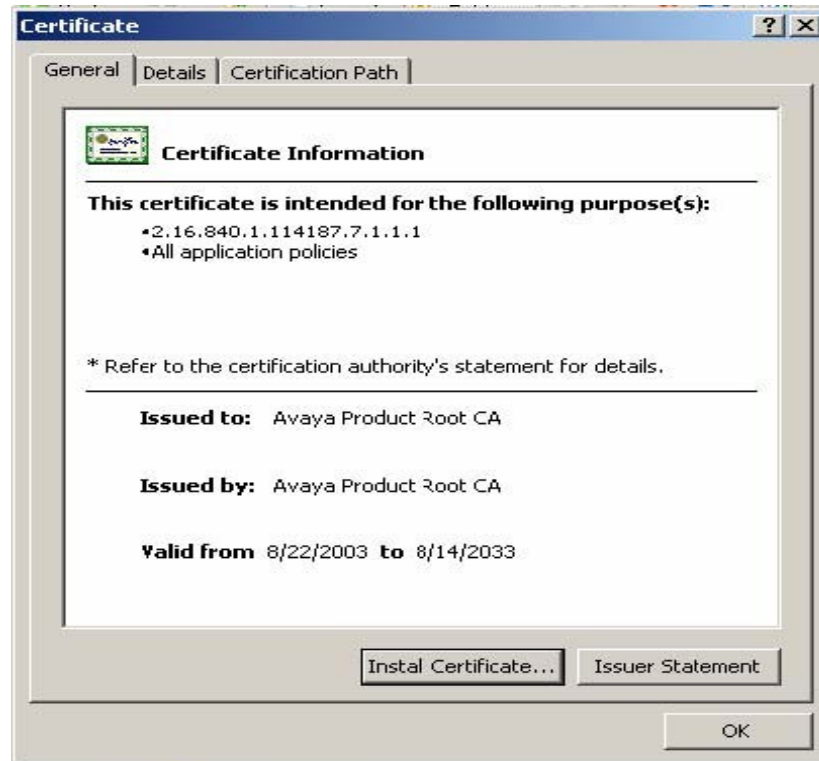
- Install of the SSL Certificate
- Install of the Avaya Link Controller, Call Controller and the TSAPI Client
- Configure the Cybertech Pro Voice Recorder

7.1. Install the SSL Certificate for the AES Connection

The Cybertech CTI server requires a certificate to communicate with the Avaya AES Server. After installation the following files are present on the CTI server. Double click on the 'avaya' certificate in the directory containing the distribution files. Please check CyberTech Connectivity Manual for latest details.



Click **Install Certificate** on the subsequent screen.



The Certificate Import Wizard is displayed. Click **Next** to begin the import.



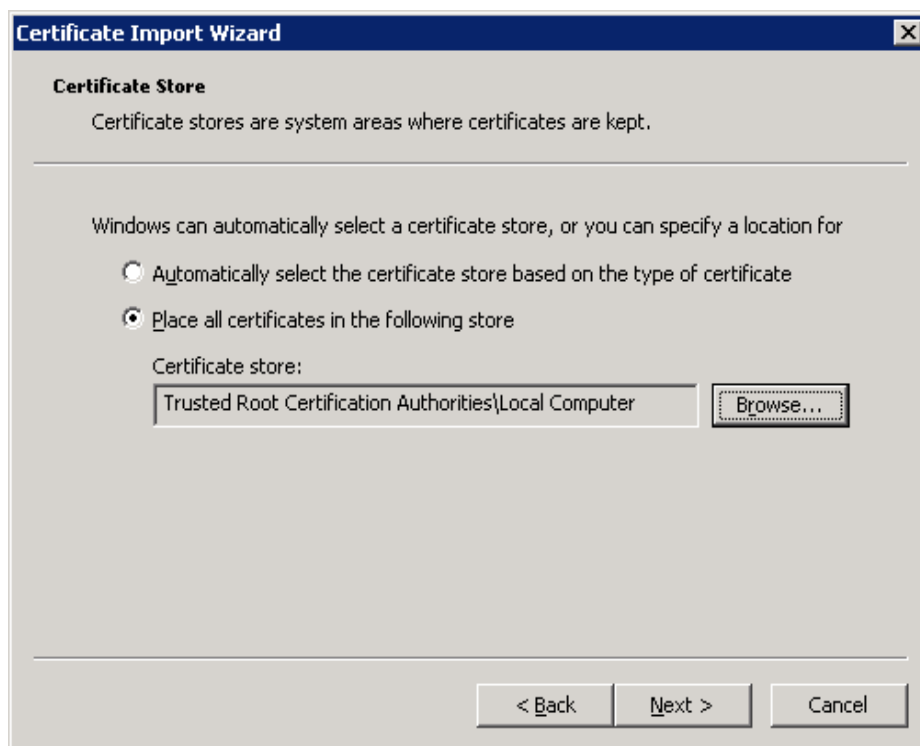
Click **Browse** to select the certificate destination.



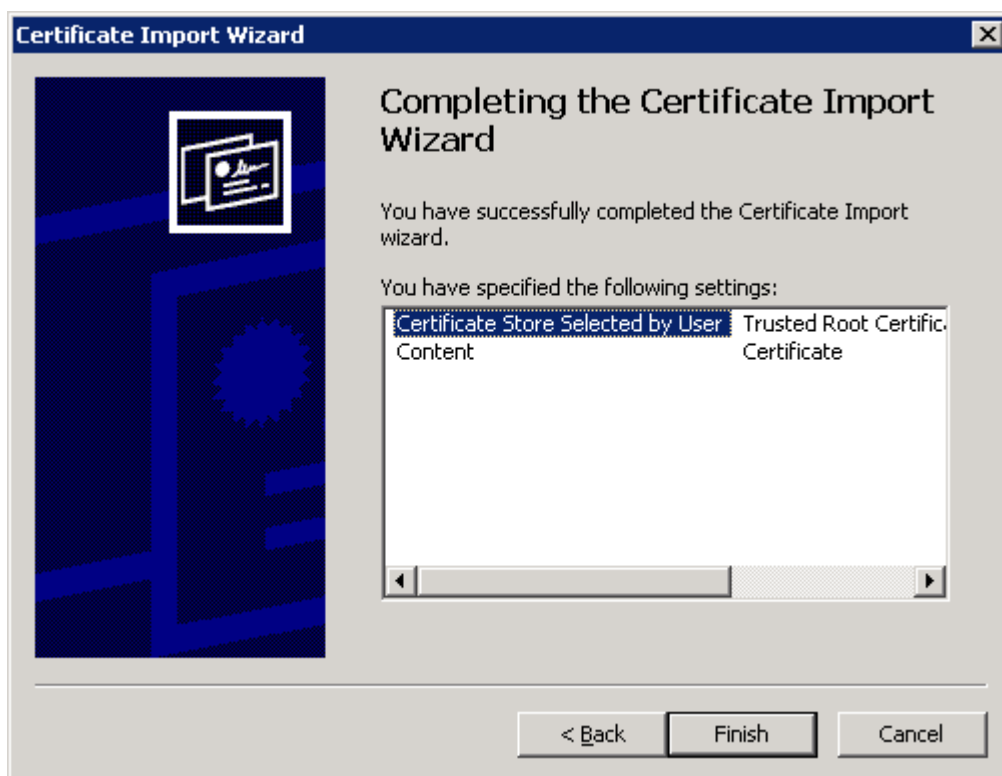
Select the **Local Computer**, as shown.



Click **Next** after confirming the destination.

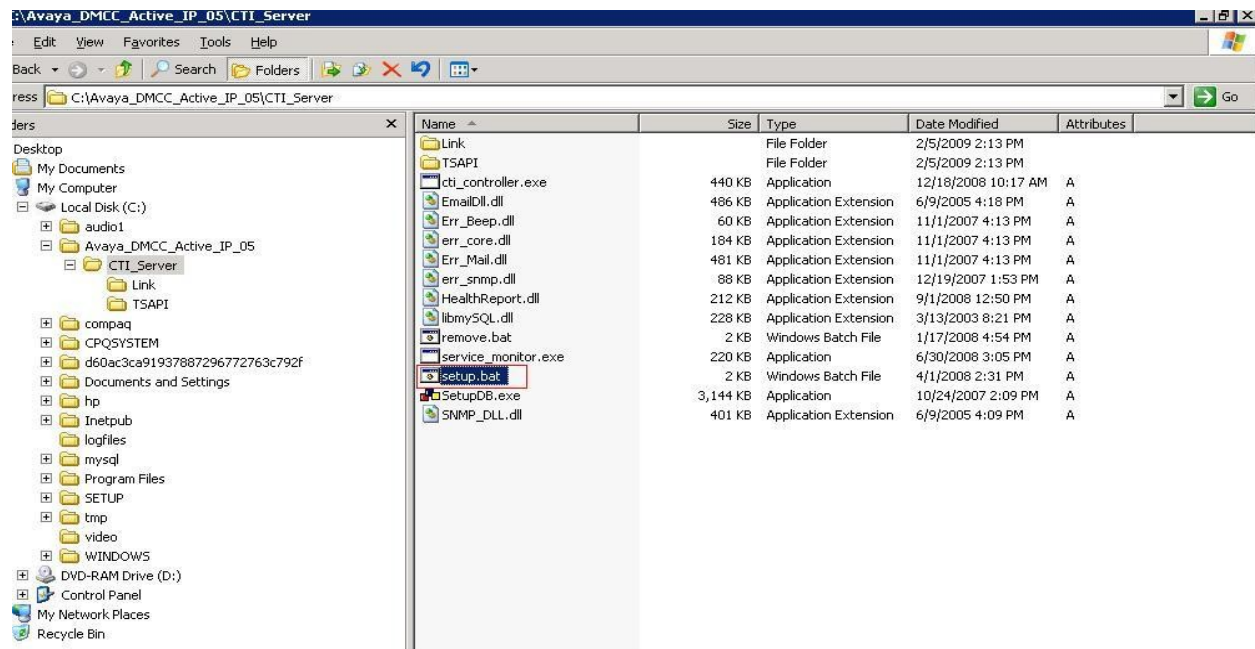


Click **Finish** after the certificate installation is complete.

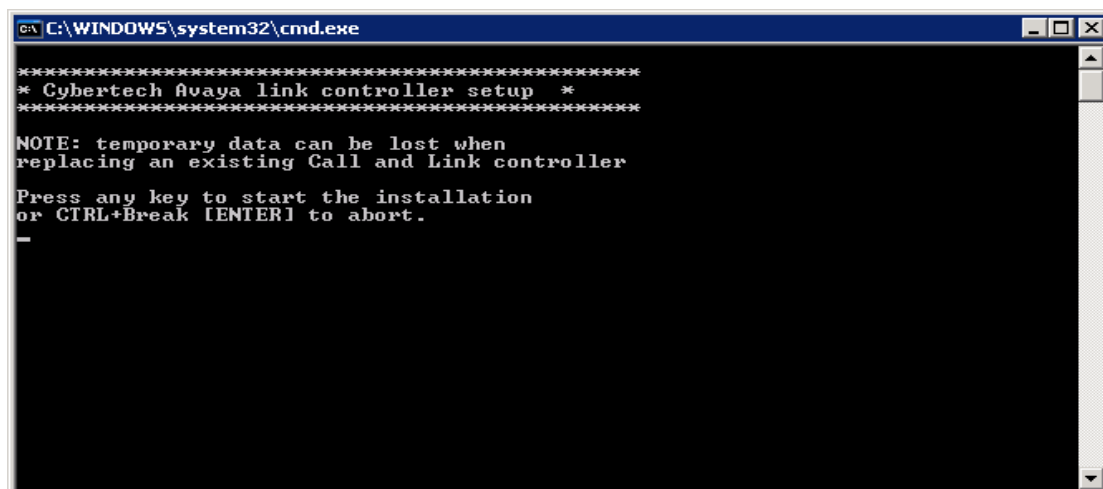


7.2. Install Avaya Link Controller, Call Controller and the TSAPI Client on CTI Server

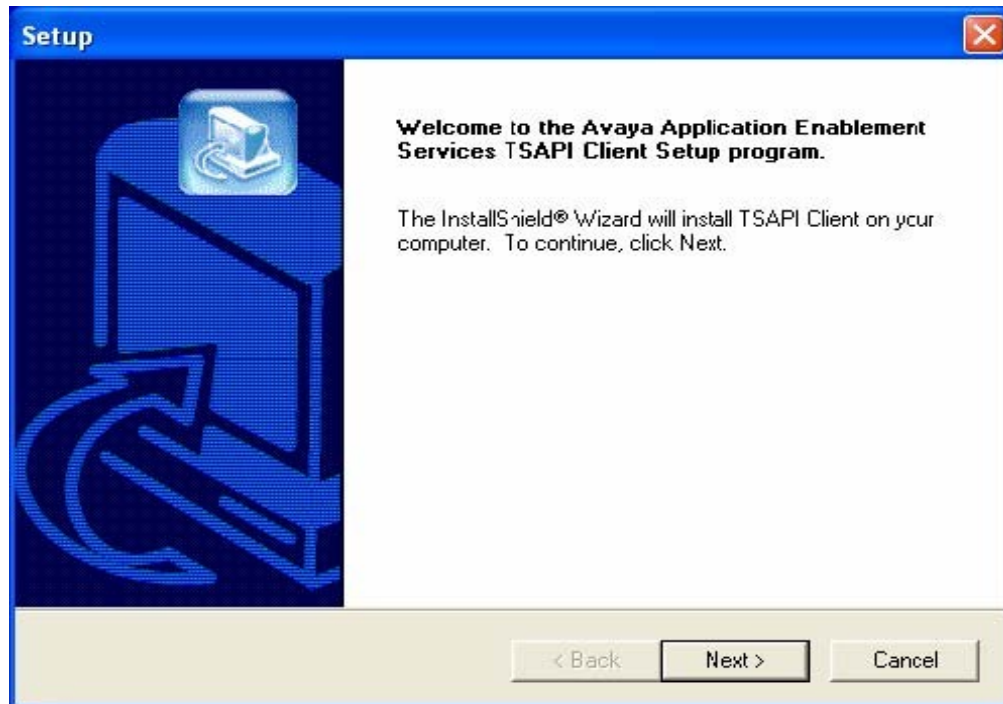
The Avaya Link Controller, Call Controller and the TSAPI Client must be installed on the CTI Server, as shown by the following steps. First, execute the 'setup.bat' file as shown in the default directory in the following screen. Make sure you run this batch file on the CTI server.



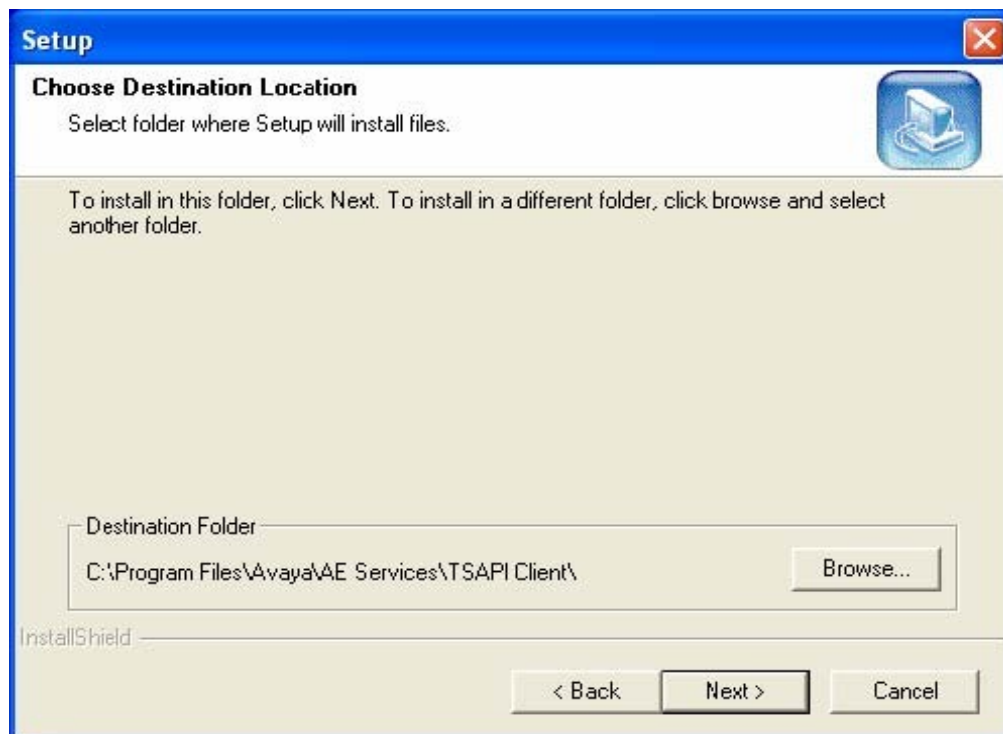
This will open a dialog box as follows. Press any key to automatically install the Avaya Link controller and the Call controller to the CTI server.



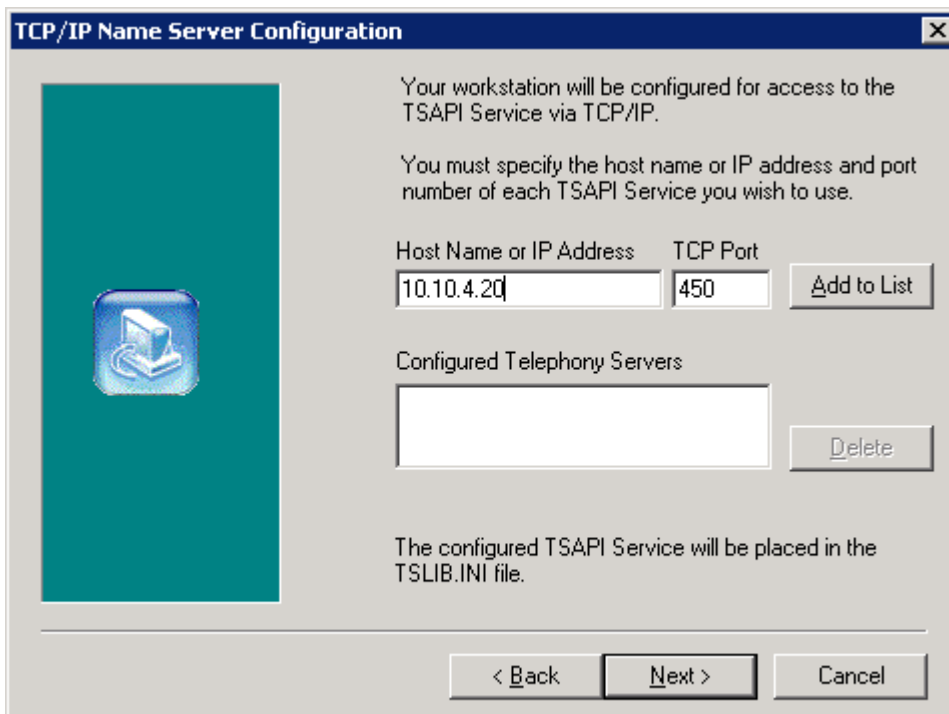
After these steps the TSAPI installer will start.



Retain the default installation folder and click **Next**.



Enter the IP address of the Avaya AES server in the **Host Name or IP Address** field, retaining the default port of **450**. Click **Add to List** and then **Next**.



The dialog box is titled "TCP/IP Name Server Configuration". It contains a teal sidebar on the left with a computer icon. The main area has instructional text: "Your workstation will be configured for access to the TSAPI Service via TCP/IP." and "You must specify the host name or IP address and port number of each TSAPI Service you wish to use." Below this are two input fields: "Host Name or IP Address" with the value "10.10.4.20" and "TCP Port" with the value "450". To the right of these fields is an "Add to List" button. Below the input fields is a section titled "Configured Telephony Servers" with an empty list box and a "Delete" button. At the bottom, there is a note: "The configured TSAPI Service will be placed in the TSLIB.INI file." and three buttons: "< Back", "Next >", and "Cancel".

TCP/IP Name Server Configuration

Your workstation will be configured for access to the TSAPI Service via TCP/IP.

You must specify the host name or IP address and port number of each TSAPI Service you wish to use.

Host Name or IP Address TCP Port

10.10.4.20 450 Add to List

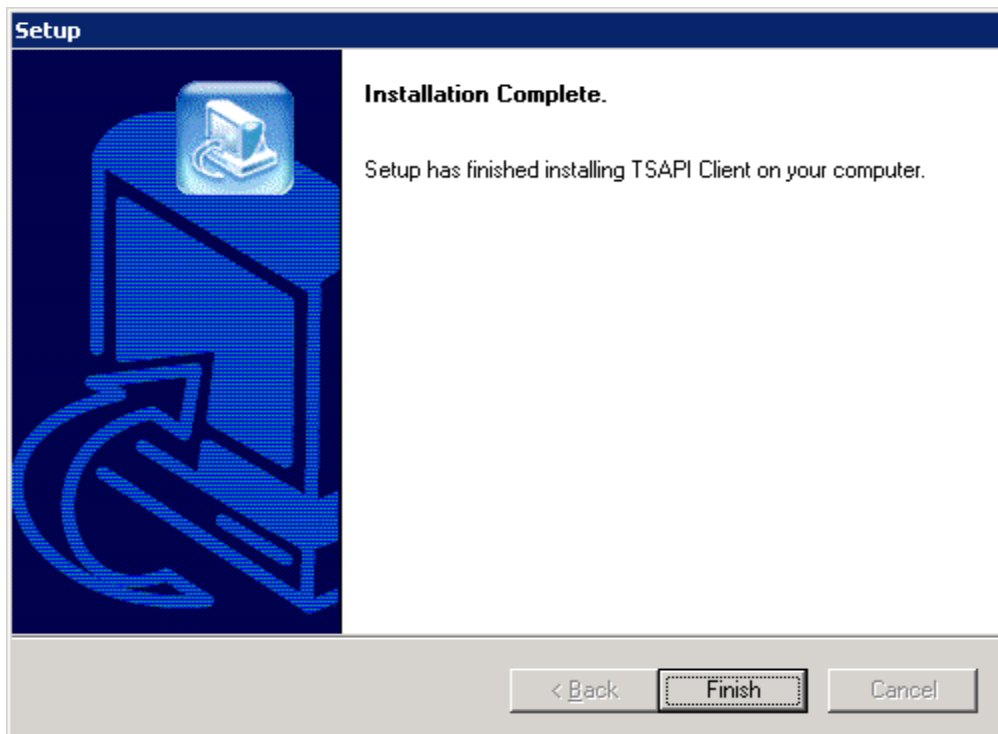
Configured Telephony Servers

Delete

The configured TSAPI Service will be placed in the TSLIB.INI file.

< Back Next > Cancel

Click **Finish** after the installation completes.



The dialog box is titled "Setup". It features a large blue graphic on the left showing a computer monitor with a curved arrow pointing to it. The main area displays the text "Installation Complete." followed by "Setup has finished installing TSAPI Client on your computer." At the bottom, there are three buttons: "< Back", "Finish", and "Cancel".

Setup

Installation Complete.

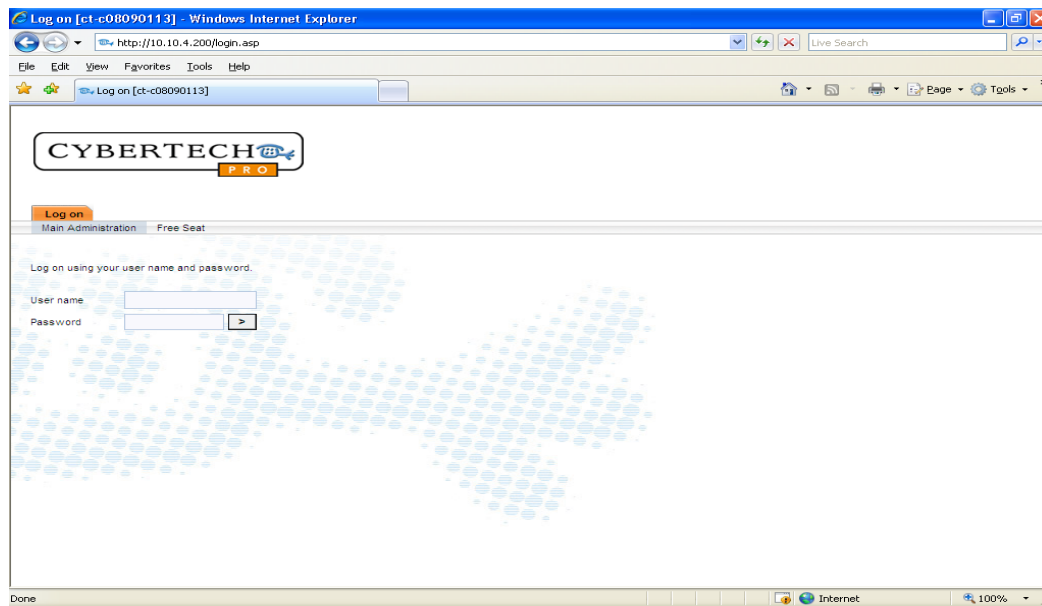
Setup has finished installing TSAPI Client on your computer.

< Back Finish Cancel

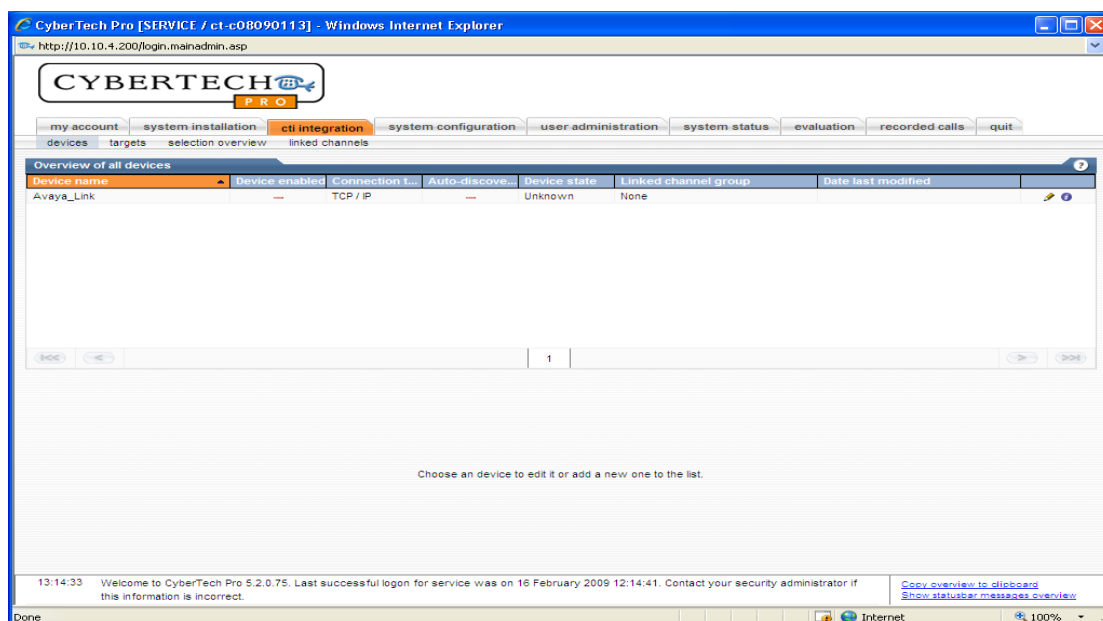
7.3. Configure the Cybertech Pro Voice Recorder

The Cybertech Pro Voice Recorder is configured for each of “Service Observe” and “Single Step Conference” modes in this section.

Enter the URL of the Cybertech Voice Recorder in the web browser and enter the **User name** and **Password** and click on the “>” button or press Enter.



Once logged in, select the **cti integration** tab which initially displays the **devices** on the secondary tab. Click on the Pencil symbol in the upper right portion of the screen.



In the next screen **General device parameters** form below ensure that the **Device Parameters** values in **Table 5** are entered. Then select **Device Enabled** as **Yes**. The **TSAPIServerName** value depends on whether the TSAPI link is set to Encrypted, Unencrypted or Both. Refer to **Section 6.3**.

Parameter	Value
SwitchName	CMCyber
ObserveCode	#3
TSAPIServerName	AVAYA#CMCYBER#CSTA#PRESAES <i>or</i> AVAYA#CMCYBER#CSTA-S#PRESAES
ConnectionUseSSL	Yes
ConnectionProtocol	4.2

Table 5: Cybertech Device Parameter Settings

Under the **Connections settings** parameters in the same form, configure the **Connection settings** as shown in **Table 6** below.

Parameter	Usage
Connection host	Enter the IP address of the Avaya AES Server.
IP port	Enter the default port address of “4722”.
Connection user	Enter the user name which was defined in Section 6.4 .
Connection password	Enter the “User Password” which was defined in Section 6.4 .

Table 6: Cybertech Pro Connection Settings

Click **Save changes** once the values have been added.

CyberTech Pro [SERVICE / ct-c08090113] - Windows Internet Explorer
http://10.10.4.200/login.mainadmin.asp

CYBERTECH PRO

my account | system installation | **cti integration** | system configuration | user administration | system status | evaluation | recorded calls | quit

devices | targets | selection overview | linked channels

Overview of all devices

device name	device enabled	Connection L...	Auto-discove...	Device state	Linked channel group	Date last modified
Avaya_Link	✓	TCP / IP	---	Logged in	Avaya cert	

1

General device settings

Device name: Avaya_Link

Device enabled: Yes

Auto-discovery enabled: ☐

Device parameters: SwitchName=CMCyber, ObserveCode=#3, TSAPIServerName=AVAYA#CMCYBER#CSTA#PRE, SAES, Connection=SSL, Yes

Connection settings

Connection host: 10.10.4.20

IP port: 4722

Connection user: CTIUser

Connection password:

Password (retype):

Linked channel group: Avaya cert

Cancel | **Save changes**

17:51:06 You are editing an existing record.
17:46:46 You are editing an existing record.

Copy overview to clipboard
Show statusbar messages overview

Select the **targets** secondary tab and click the “+” symbol for each target to be added. A target is any extension added either as active or a recording extension.

CyberTech Pro [SERVICE / ct-c08090113] - Windows Internet Explorer
http://10.10.4.200/login.mainadmin.asp

CYBERTECH PRO

my account | system installation | **cti integration** | system configuration | user administration | system status | evaluation | recorded calls | quit

devices | **targets** | selection overview | linked channels

Overview of all device targets

No records found in the database.

Choose a target to edit its properties or add a new one to the list.

13:34:14 You are editing an existing record.
13:33:07 You are editing an existing record.

Copy overview to clipboard
Show statusbar messages overview

The **Device info** control appears each time the “+” control is clicked. Enter information for each of the targets to be monitored, as shown in the following table.

Name	Device	Type	Range Start
3012	AvayaLink	Active Extension	3012
3013	AvayaLink	Active Extension	3013
3006	AvayaLink	Active Extension	3006
AgentB	AvayaLink	Extension	6001
AgentC	AvayaLink	Extension	6002
VDN	AvayaLink	Extension	1800
Huntgroup	AvayaLink	Extension	3090
Target_B	AvayaLink	Recorded Extension	3006
Target_C	AvayaLink	Recorded Extension	3000

Table 7: Cybertech Pro Target Device Info Parameters

An example of one target being added is shown in the following screen.

The screenshot shows the Cybertech Pro web interface in a Windows Internet Explorer browser. The address bar shows the URL <http://10.10.4.200/login.mainadmin.asp>. The page title is "CyberTech Pro [SERVICE / ct-c08090113]". The main navigation bar includes tabs for "my account", "system installation", "cti integration" (which is active), "system configuration", "user administration", "system status", "evaluation", "recorded calls", and "quit". Below this, there are sub-tabs for "devices", "targets", "selection overview", and "linked channels". The main content area is titled "Overview of all device targets". A dialog box titled "Add target" is open, showing the following fields: "Target name(s)" with the value "ExtDtg", "Device" with a dropdown menu showing "Avaya_Link", "Target type(s)" with a dropdown menu showing "Recorded Extension", "Target value range start" with the value "3006", "Target value range end (leave empty for single target)" which is empty, and "Target selection" with a checked checkbox. At the bottom of the dialog box are "Cancel" and "OK" buttons. A red box highlights the "Add target" button in the top right corner of the dialog box.

Service Observe mode

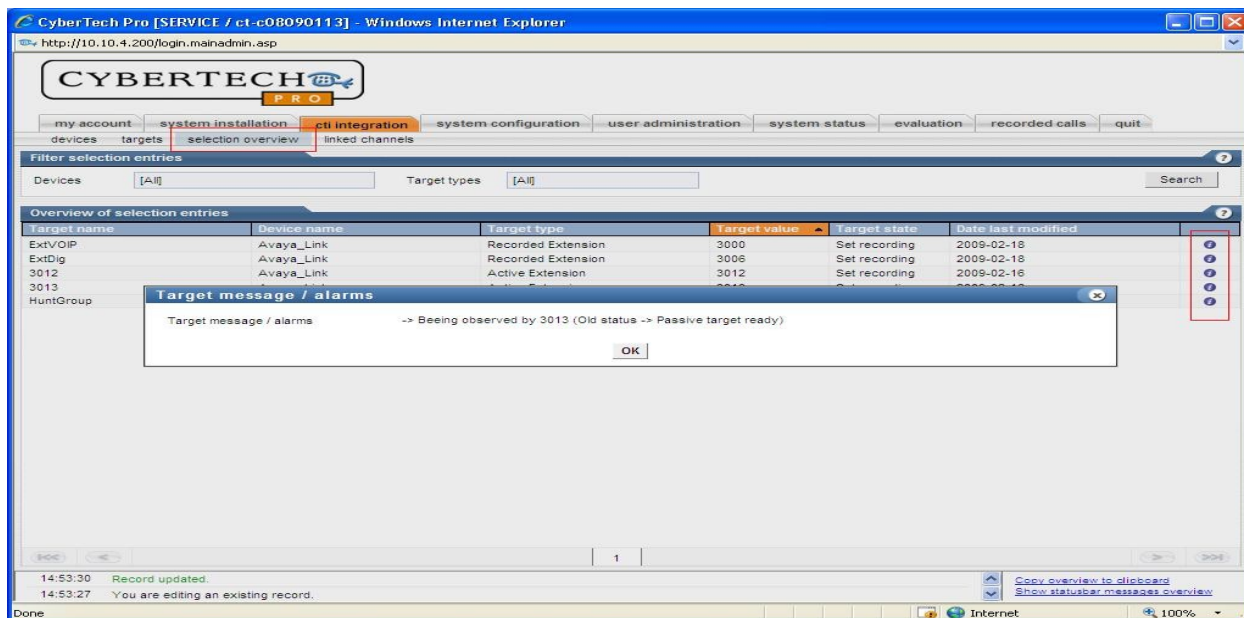
After the targets have been entered, it should contain the following information in the Service Observe mode.

Target name	Target Selection	Device name	Target type	Target value	Date last modified
VND	—	Avaya_Link	Extension	1800	2009-02-18
ExtVOIP	✓	Avaya_Link	Recorded Extension	3000	2009-02-18
ExtDig	✓	Avaya_Link	Recorded Extension	3006	2009-02-18
3012	✓	Avaya_Link	Active Extension	3012	2009-02-16
3013	✓	Avaya_Link	Active Extension	3013	2009-02-16
HuntGroup	✓	Avaya_Link	Extension	3090	2009-02-17
AgentB	—	Avaya_Link	Extension	6001	2009-02-17
AgentC	—	Avaya_Link	Extension	6002	2009-02-17

In the selection overview screen below, the selected extensions which will be monitored in the Service observe mode, are displayed. The selected VND is added as an extension.

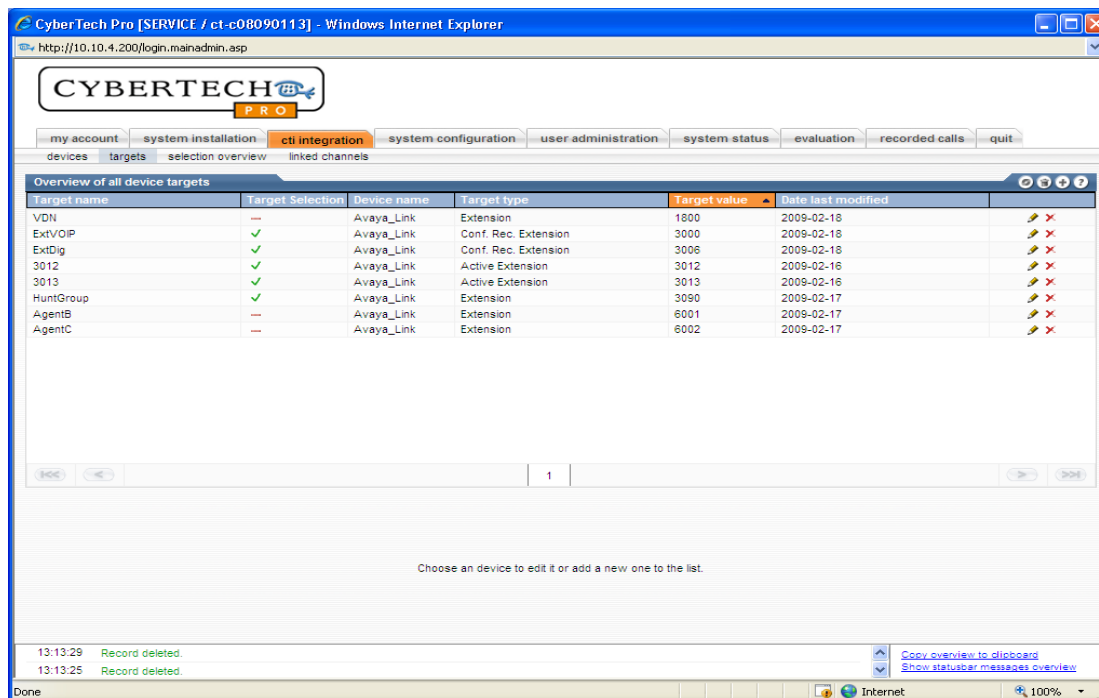
Target name	Device name	Target type	Target value	Target state	Date last modified
ExtVOIP	Avaya_Link	Recorded Extension	3000	Set recording	2009-02-18
ExtDig	Avaya_Link	Recorded Extension	3006	Set recording	2009-02-18
3012	Avaya_Link	Active Extension	3012	Set recording	2009-02-16
3013	Avaya_Link	Active Extension	3013	Set recording	2009-02-16
HuntGroup	Avaya_Link	Extension	3090	Selected	2009-02-17

Additional information for each of the targets is available via the **I** button. For example, this mechanism can be used to determine that endpoint C is being observed via virtual extension 3013.

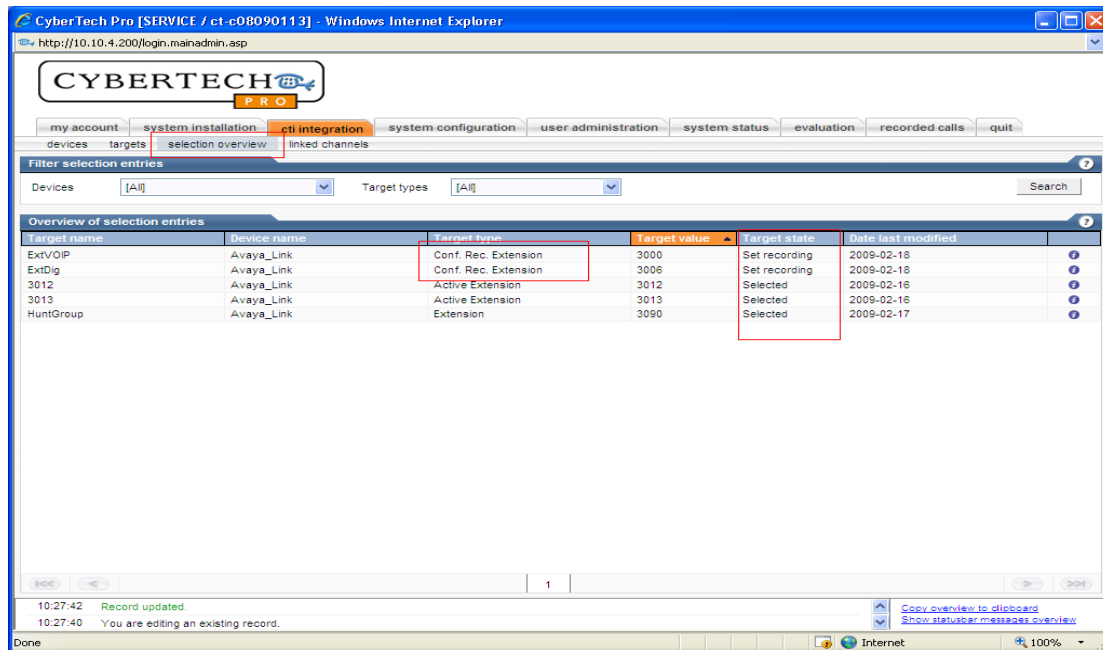


Single Step Conference mode

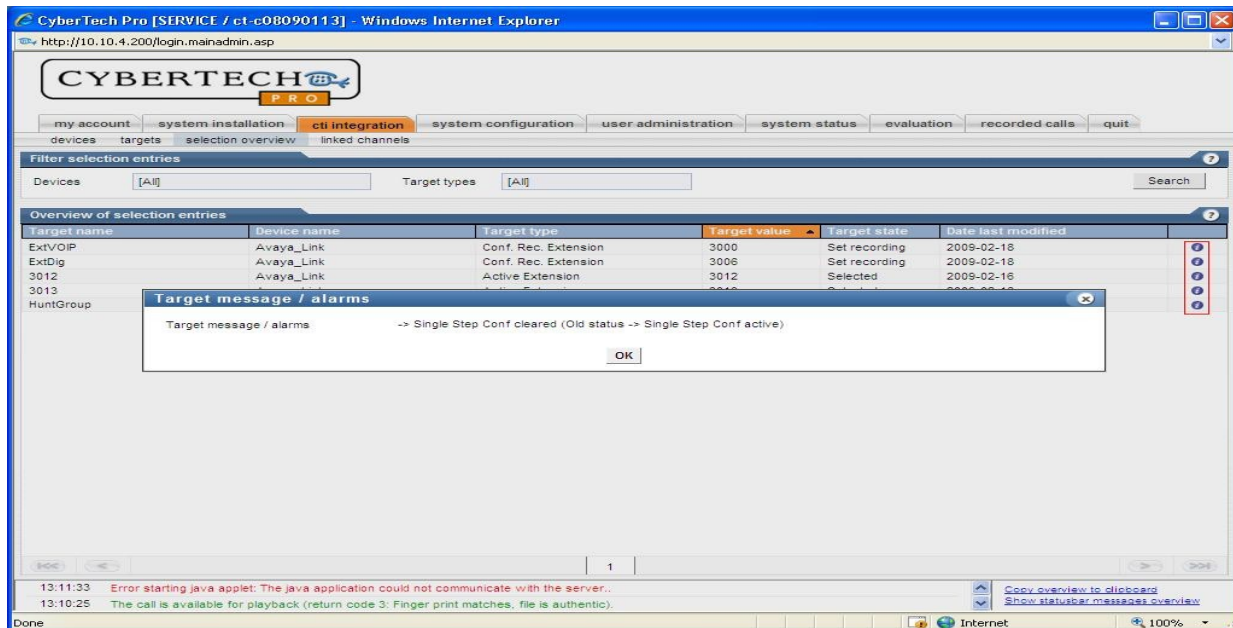
The Cybertech Pro Recorder is configured for Single Step Conferencing. Targets are added as in Service Observe mode. After the targets have been entered, it should contain the following information in Single Step Conference mode.



In the **selection overview** tab on the screen below, the selected extensions are displayed which will be monitored in Single Step Conference mode. The selected Hunt group is added as an extension.



Additional information for each of the targets is available via the **I** button. For example, this mechanism can be used to determine that endpoint C is being observed in Single Step Conference mode.



8. General Test Approach and Test Results

The test approach was to make calls using digital, VOIP and analogue phones. The tests were to verify that the calls were being placed correctly and accurate audio recordings were being generated and collected by the Cybertech solution. Testing was performed manually. The tests were all functional in nature and performance testing was not included.

All of the test cases were executed and overall the solution was successful. One area of failure was a missing Call Line Identification on three recorded calls. This is a known issue on the Cybertech recorder for call transfers.

The following results were obtained

- Confirmation of the ability of Cybertech Pro to correctly create voice recording files of various telephony operations
- Confirmation that the correct number of voice recording files is created for each operation performed
- Confirmation of voice content
- Confirmation of calling and called party
- Confirmation of start and stop times

9. Verification Steps

9.1. Verify Communication Manager Status

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly.

Verify that the service state of the TSAPI link is established. Check the TSAPI link status with AES by using the command below. The CTI Link is 10.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
10	4	no	PresAES	established	12	13

Verify that the status of AES interface is connected and listening.

status aescvs interface			
AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
CLAN	yes	1	listening

Verify that there is a link with the AES and messages are being sent and received.

status aescvs link							
AE SERVICES LINK STATUS							
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd	
02/01	PresAES	10. 10. 4. 20	51158	CLAN	25	25	

9.2. Verify Avaya AES Status

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly.

9.2.1. TSAPI Link

Verify the status of the TSAPI link by selecting **Status and Control** → **Services Summary**. Select **TSAPI Service** (not shown), followed by **Details**.

The **TSAPI Link Details** screen is displayed as shown below.

AVAYA

Application Enablement Services
Operations Administration and Maintenance

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

TSAPI Link Details

	Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
	1	CMCyber	10	Talking	2009-02-24 13:31:59.0	Online	15	0	15

Verify the status of the TSAPI link by checking that the **Connection Status** is **Talking** and the **Service State** is **Online**.

9.2.2. DMCC Service

Verify the status of the DMCC service by selecting **Status and Control** → **Services Summary**. Select **DMCC Service** (not shown), followed by **Details**. The **DMCC Services Summary** screen is displayed as shown below. It shows a connection to the Cybertech CTI Server, IP address '10.10.4.210'.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top header includes the Avaya logo and the title "Application Enablement Services" with the subtitle "Operations Administration and Maintenance". Navigation links for "OAM Home", "Help", and "Logout" are present. The breadcrumb trail indicates the current location: "You are here: > Status and Control > Services Summary".

The left sidebar contains a navigation menu with the following items:

- CTI OAM Home
- Administration
 - Network Configuration
 - Switch Connections
- Status and Control
 - Switch Conn Summary
 - Services Summary
- Maintenance
- Alarms
- Logs
- Utilities
- Help

The main content area is titled "DMCC Service Summary - Session Summary". It includes a sub-header "Session Summary" and "Device Summary". Below this, it states "Generated on Mon, Feb 16, 2009 04:22:33 PM GMT".

The service status is displayed as follows:

- Service Uptime: 0 days, 2:07 hours
- Number of Active Sessions: 1
- Number of Sessions Created Since Service Boot: 4
- Number of Existing Devices: 0
- Number of Devices Created Since Service Boot: 0

A table lists the active sessions:

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
226303EE7C00E9534 588430B048165B5-8	CTIUser	Avaya_Link	10.10.4.210	XML Encrypted	0

Below the table are two buttons: "Terminate Sessions" and "Show Terminated Sessions".

9.2.3. TLinks

Navigate to **Administration** → **Security Database** → **TLinks**. Verify the value of the Tlinks name. This will be needed to configure the Cybertech server.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top header includes the Avaya logo and the title "Application Enablement Services" with the subtitle "Operations Administration and Maintenance". Navigation links for "OAM Home", "Help", and "Logout" are present. The breadcrumb trail indicates the current location: "You are here: > Administration > Security Database > Tlinks".

The left sidebar contains a navigation menu with the following items:

- CTI OAM Home
- Administration
 - Network Configuration
 - Switch Connections
 - CTI Link Admin
 - DMCC Configuration
 - TSAPI Configuration
- Security Database
 - SDB Control
- CTI Users

The main content area is titled "Tlinks". It displays a list of Tlink names:

- ☒ AVAYA#CMCYBER#CSTA#PRESAES
- ☐ AVAYA#CMCYBER#CSTA-S#PRESAES

Below the list are two buttons: "Edit Tlink" and "Delete Tlink".

9.2.4. TSAPI Test

Make a call between two stations on Communication Manager using the TSAPI Link. Navigate to the screen **CTI OAM Home → Utilities → TSAPI Test**. Use the username and password set up as in **Section 6.4**.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top header includes the Avaya logo and the text "Application Enablement Services Operations Administration and Maintenance". A breadcrumb trail indicates the current location: "You are here: > Utilities > TSAPI Test". On the left, a navigation menu lists various sections: Administration, Status and Control, Maintenance, Alarms, Logs, Utilities, and Help. The Utilities section is expanded, showing links to ASAI Test, Ping Host, TSAPI Test, and TR/87 Test. The main content area is titled "TSAPI Test" and contains the following fields: TLink (a dropdown menu showing "AVAYA#CMCYBER#CSTA-S#PRESAES"), User (a text field with "CTIUser"), Password (a masked text field with "*****"), From (a text field with "2500"), and To (a text field with "2510"). A "Dial" button is located below the To field.

9.2.5. ASAI Test

Additional tests can be carried out by using the ASAI Test. Open this screen under **CTI OAM Home → Utilities → ASAI Test**. This verifies that the TSAPI Link set up in **Section 6.3** is communicating.

The screenshot shows the Avaya Application Enablement Services (AES) interface for the ASAI Test. The top header includes the Avaya logo and the text "Application Enablement Services Operations Administration and Maintenance". A breadcrumb trail indicates the current location: "You are here: > Utilities > ASAI Test". On the left, a navigation menu lists various sections: Administration, Status and Control, Maintenance, Alarms, Logs, Utilities, and Help. The Utilities section is expanded, showing links to ASAI Test, Ping Host, TSAPI Test, and TR/87 Test. The main content area is titled "ASAI Test" and contains the following elements: A heading "Check the link numbers you would like to run ASAI Test on:". Two columns of checkboxes are displayed: "CVLAN Link" and "TSAPI Link". The "TSAPI Link" column has a red box around the "link 1" checkbox, which is checked. Below the checkboxes are three buttons: "Select All", "Deselect All", and "Test".

Run the ASAI Test and check the TSAPI link number on which you would like to run the test. A successful test will display a result as in the following screen.



9.3. Verify Cybertech Configuration

The following steps can be performed to verify the basic operation of the system components:

- Make calls local and external to and from monitored stations to verify that the correct call records are produced
- Perform hold, transfer, blind transfer, and conferencing operations to verify that correct call records are produced
- Make calls to and from bridged appearances to verify that correct call records are produced
- Make calls from external telephones to a VDN to verify that correct call records are produced
- Make calls to agents and verify that correct call records are produced

10. Conclusion

These Application Notes describe the conformance testing of the Cybertech Pro with Communication Manager and Application Enablement Services. All functionality and serviceability test cases were completed successfully with the Cybertech Pro solution.

11. Additional References

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

Product documentation for Avaya products may be found at <http://support.avaya.com>

1. ***Administrator Guide for Avaya Communication Manager, Document No 03-300509, Issue 4, January 2008***
2. ***Change Description for Release 5.1 of Avaya Communication Manager, SIP Enablement Services, Avaya Servers, and Media Gateways, Document No 03-602958, Issue 1, June 2008***
3. ***Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide - Release 4.2, Document No 02-300357, Issue 10, May 2008***
4. ***Developing Client-side IP Recording Applications using Avaya Application Enablement Services, An Avaya DevConnect Application Note, October 2008***

The following documentation is available on request from Cybertech <http://www.cybertech-int.com>

1. ***Cybertech CT Recording Solutions R5 – Installation Manual v5.3***
2. ***Cybertech Parrot DSC - VOIP installation manual***
3. ***Cybertech CT Recording Solutions R5 - CTI manual***
4. ***Cybertech AVAYA DMCC connectivity manual***

©2009 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.