



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Multiple Registrations on 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 using the Multiple Registrations recording method on CyberTech Pro with 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. In this compliance test, it uses Communication Manager's Multiple Registrations 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 API associated with the AES server monitors the digital and VoIP extensions. The application uses the AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device and records the call.

## 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, Communication Manager and Application Enablement Services. The recording method used by CyberTech for the purpose of this compliance test is Multiple Registrations. Testing covered 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
- Testing of the secure RTP
- Use of both G.711 and G.729 codecs for call recording

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

## 1.2. Support

Technical support from CyberTech can be obtained through the following:

CyberTech Support Desk

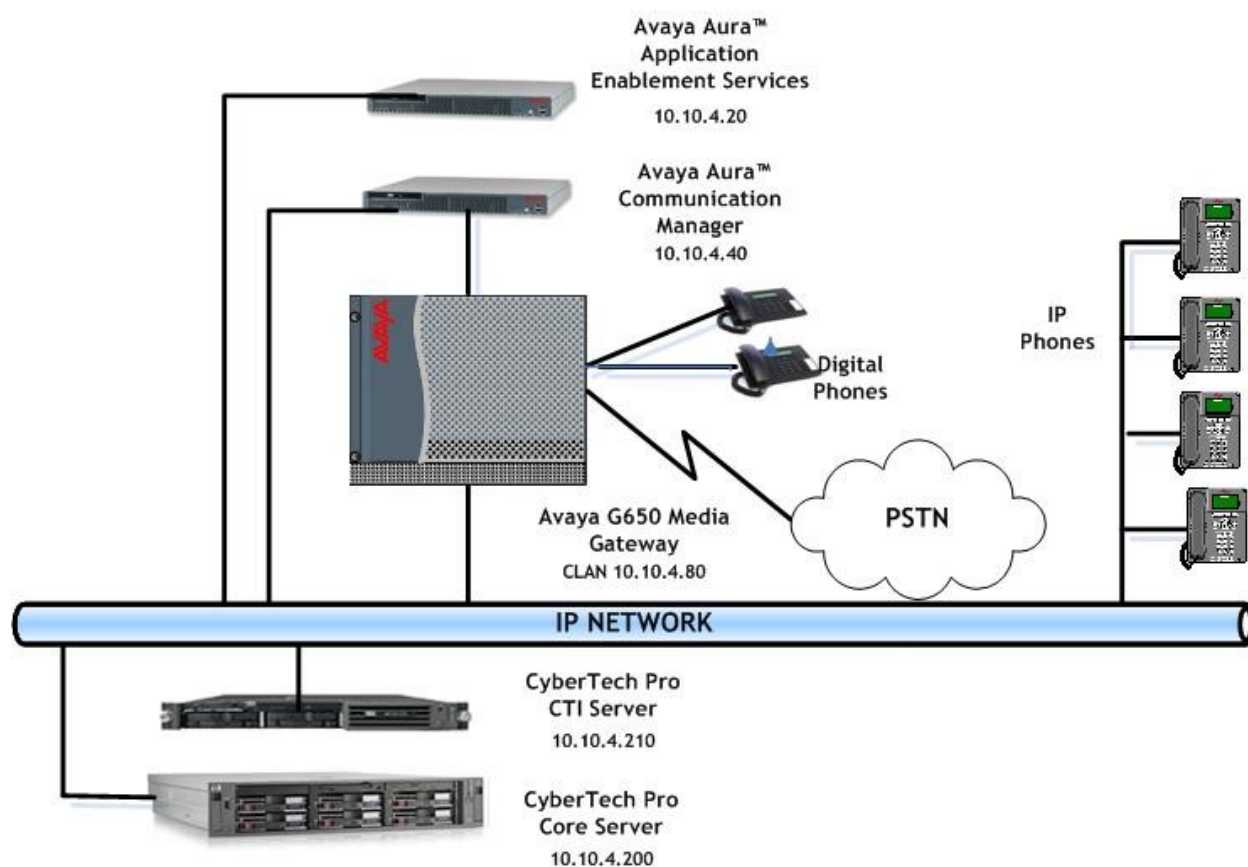
Email: [supportdesk@CyberTech-int.com](mailto:supportdesk@CyberTech-int.com)

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 the Communication Manager “Multiple Registration” feature 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 4.2.2
Avaya G650 Media Gateway IPSI TN2312BP CLAN TN799DP IP Media Processor TN2602AP DS1 Interface TN246CP Digital Line TN2214CP	HW15, FM46 HW01, FM32 HW02, FM49 HW02, FM024 HW08, FM015
Avaya 96xx and Series IP Telephones (H.323) 9620 9630 9640 9670G	3.0 3.0 3.0 3.0
Digital Telephone 2420	R5
CyberTech Core server	5.3.0.107
CyberTech CTI Server	Avaya_DMCC_Active_IP_6.8.0 Callcontroller - 1.8.4.686 AvayaLinkController - 1.6.12.436 Service Monitor 1.1.8.61 Cti_receiver V3 3.2.1.15

**Table 1: Hardware and Software Version Numbers**

## 4. Test Configuration

Table 2 contains the extensions that were used in the test.

Type of Phone	Phone Extension	Station	Button Allocation	Comments
IP9620	3000	S1	3 x call-appr, serv-obsrv, brgd-appr to D	
IP9630	3001	S2	3 x call-appr, serv-obsrv	
Digital-2420	3002	A	3 x call-appr, auto-cback	
Digital-2420	3003	B	3 x call-appr, auto-cback, call-pkup	*Agent logged in
IP9640	3004	C	3 x call-appr, brdg-appr D, call-pkup, auto-cback	*Agent logged in
IP9670G	3005	D	3 x call-appr	
Digital	3006	E	3 x call-appr	
IP	3007	S	3 x call-appr, exclusion	
External CM	2501	G		
External CM	2502	H		

**Table 2: Station Extensions and Details Used for Testing**

## 5. Configure Avaya Aura™ 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
- Allocate a call pickup group
- Allocate agent resources
- Configure Codecs and Media Encryption on CM
- 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	
<b>Maximum Concurrently Registered IP Stations: 18000</b>	<b>0</b>	
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 parameter is set as follows:

- **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	<b>Computer Telephony Adjunct Links? y</b>	
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. Ensure that the Communication Manager has a license for media encryption by checking that **Media Encryption Over IP** is set to **y**.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y		<b>IP Stations? y</b>
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	<b>Media Encryption Over IP? y</b>	
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. **Service Observing (Basic)** is also defaulted to **y**.

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	<b>Service Observing (Basic)? y</b>	
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	
<b>EAS-PHD? y</b>	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      Call Pickup Alerting? y
    Temporary Bridged Appearance on Call Pickup? y      Directed 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
    VECTORING
        Converse First Data Delay: 0          Second Data Delay: 2
        Converse Signaling Tone (msec): 100      Pause (msec): 70
        Prompting Timeout (secs): 10
    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

### 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	This is used by telephone users to initiate a call-pickup operation.
Auto-in	This is used by agents to indicate availability to take a call.
Login	Agent login.
Logout	Agent logout.
Service Observing No Talk	This is used by the voice recorder to receive the voice stream without sending voice data. The value used is a free choice, but 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. These are free choices.

<b>change feature-access-codes</b>	<b>Page 1 of 8</b>
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:	*56
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code:	
Auto Route Selection (ARS) - Access Code 1:	9
Automatic Callback Activation:	Access Code 2:
Call Forwarding Activation Busy/DA:	All: Deactivation:
Call Forwarding Enhanced Status:	Act: Deactivation:
Call Park Access Code:	
<b>Call Pickup Access Code: #4</b>	
CAS Remote Hold/Answer Hold-Unhold Access Code:	
CDR Account Code Access Code:	
Change COR Access Code:	
Change Coverage Access Code:	
Conditional Call Extend Activation:	Deactivation:
Contact Closure Open Code:	Close Code:

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

<b>change feature-access-codes</b>	Page 5 of 8
FEATURE ACCESS CODE (FAC)	
Automatic Call Distribution Features	
After Call Work Access Code:	
Assist Access Code:	
<b>Auto-In Access Code: #2</b>	
Aux Work Access Code:	
<b>Login Access Code: #6</b>	
<b>Logout Access Code: #5</b>	
Manual-in Access Code:	
Service Observing Listen Only Access Code:	
Service Observing Listen/Talk Access Code:	
<b>Service Observing No Talk Access Code: #3</b>	
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 used for connectivity to Application Enablement Services.

<b>change node-names ip</b>	Page 1 of 2
IP NODE NAMES	
Name	IP Address
<b>CLAN</b>	<b>10.10.4.80</b>
CM2	10.1.0.10
Gateway001	10.10.4.1
MEDPRO	10.10.4.90
announce	10.10.4.85
default	0.0.0.0
procr	10.255.255.100
quebust	10.10.4.25

## 5.5. Configure Recording Stations

Use the **add station** command to configure a station for each of the target stations shown in **Table 2, Section 4**. Enter in a descriptive **Name** and **Security Code** for each one. Set the **IP Softphone?** to **y**. The **Security Code** will be referenced by CyberTech solution when setting up the Multiple Registration extensions in **Section 7.3**.

<b>add station 3003</b>	Page 1 of 5	
STATION		
Extension: 3003	Lock Messages? n	BCC: 0
Type: 2420	<b>Security Code: 3003</b>	TN: 1
Port: 01A0601	Coverage Path 1:	COR: 1
<b>Name: PhoneB</b>	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: 3003	
Display Language: english	Mute Button Enabled? y	
	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Customizable Labels? y	

On **Page 2**, ensure that the **Multimedia Mode** is set to **enhanced**.

<b>add station 3003</b>	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? n
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: enabled
<b>Multimedia Mode: enhanced</b>	
MWI Served User Type:	Display Client Redirection? n
AUDIX Name:	Select Last Used Appearance? n
	Coverage After Forwarding? s
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y
Emergency Location Ext: 3003	Always Use? n IP Audio Hairpinning? N

## 5.6. Configure Codecs and Media Encryption on CM

The G.711MU codec was used for the compliance testing. However, G.729 is also supported by CyberTech and was used in part of the testing. Use the command **change ip-codec-set x**. The **Audio Codecs** added are **G.711MU** and **G.729**. The CyberTech system needs to be set to expect the codec in the RTP stream as in **Section 7.3**. The **Media Encryption** is set to either **none** or **aes** depending on whether encryption is being used for the compliance test.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711MU	n	2	20
2: G.729	n	2	20
3:			
4:			
5:			
6:			
7:			

Media Encryption

1: none

2:

3:

## 5.7. Configure a Hunt Group, Vector, VDN, and 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	3090/1	Hunt Group 1
Agent Login	6001	AgentB
	6002	AgentC

**Table 4: Call Center Agent Details**

### 5.7.1. 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 3
HUNT GROUP		
Group Number: 1	ACD? y	
Group Name: Hunt Group 1	Queue? y	
Group Extension: 3090	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 3
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		

### 5.7.2. Configure Agent Queue Vector

Enter the **add vector n** command to set the vector **Number** to **1**. Enter the vector steps to queue to the skill 1/Hunt Group 1 as shown below.

```
add vector 1                                     Page 1 of 6
                                           CALL VECTOR

      Number: 1                Name: Vector1
                                Lock? n
      Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
      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
```

### 5.7.3. Configure Agent VDN

Use the **add vdn n** command to create a Vector Directory Number extension which can be used to reference the Agent queue vector. Set the values **Name\*** and **Vector Number** by referencing **Table 4, Section 5.7** above.

```
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*:
```

### 5.7.4. 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 **Login ID** chosen is **6001**. Enter a descriptive name for the agent in the **Name** field and set **Password** to **6001**.

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 **SN** (Skill Number) to **1**. The **SL** (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	SN	SL	SN	SL
1: 1	1	16:		31:		46:	
2:		17:		32:		47:	

## 5.8. Configure Pickup Group

Create a pickup group which contains several station extensions. This is used in conjunction with the “call-pkup” button which is allocated to one endpoint B, as shown in **Section 4, Table 2**. Use the command; **add pickup-group 1** to add this group. Assign a **Group Name** and add extensions. Note that a call pick-up group was used for compliance testing but is not mandatory for the CyberTech solution.

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

                                PICKUP GROUP

      Group Number: 1
      Group Name: CallPickUP
GROUP MEMBER ASSIGNMENTS

      Extension      Name
1: 3002             PhoneA
2: 3003             PhoneB
3: 3004             PhoneC
4: 3005             PhoneD
5:
```

## 5.9 Configure Interface to 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. The **Ethernet Interface** is set to y and the **Network Region** is set to 1.

```
display ip-interface 01a02                             Page 1 of 3

                                IP INTERFACES

      Type: C-LAN
      Slot: 01A02      Target socket load and Warning level: 400
      Code/Suffix: TN799 D      Receive Buffer TCP Window Size: 8320
      Enable Interface? y      Allow H.323 Endpoints? y
      VLAN: n      Allow H.248 Gateways? y
      Network Region: 1      Gatekeeper Priority: 5

                                IPV4 PARAMETERS

      Node Name: CLAN
      Subnet Mask: /24
      Gateway Node Name: Gateway001

      Ethernet Link: 1
      Network uses 1's for Broadcast Addresses? 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 be 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	xxxxxxxxxxx	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				
		COR: 1		
Name: PresAES				
y				

## 6. Configure Avaya Aura™ AES

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

- Verify AES License
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable CTI User
- Configure DMCC Port

## 6.1. Verify AES Licensing

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

<https://< 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 both the TSAPI and DMCC services are **Running** on the **Welcome to CTI OAM Screens**.

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

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

**CTI OAM Home**  
Administration  
Status and Control  
Maintenance  
Alarms  
Logs  
Utilities  
Help

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
<b>DMCC Service</b>	Running	ONLINE	Yes
CVLAN Service	Running	ONLINE	No
DLG Service	Running	OFFLINE	Yes
Transport Layer Service	Running	N/A	N/A
<b>TSAPI Service</b>	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.

AVAYA Application Enablement Services  
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

### Switch Connections

Connection Name	Number of Active Connections
CMCyber	1

After clicking **Add Connection**, the **Set 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

AVAYA Application Enablement Services  
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

### Set Password - New

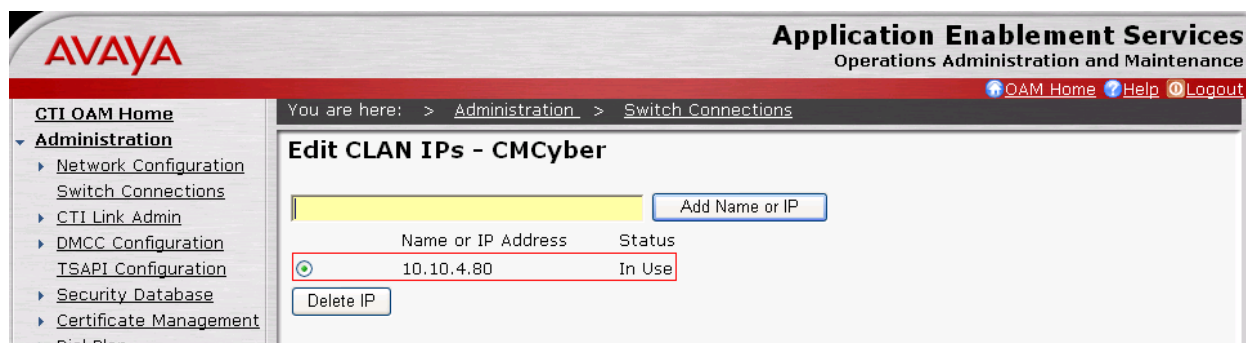
Please note the following:  
\* Changing the password affects only new connections, not open connections.

Switch Password

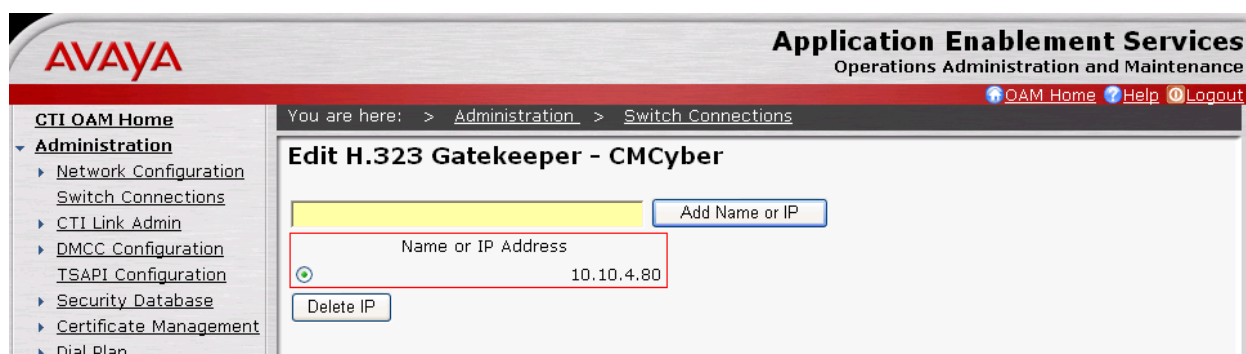
Confirm Switch Password

SSL ☒

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 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 in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Use the corresponding CTI link number configured in **Section 5.11** which is **10**.
- **ASAI Link Version:** **4** is the number chosen here.
- **Security:** **Encrypted** is the option chosen here. The customer can choose Encrypted\Unencrypted\Both.

Once completed, select **Apply Changes**.

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

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

You are here: > [Administration](#) > [CTI Link Admin](#) > [TSAPI Links](#)

### Add / Edit TSAPI Links

Link: 1

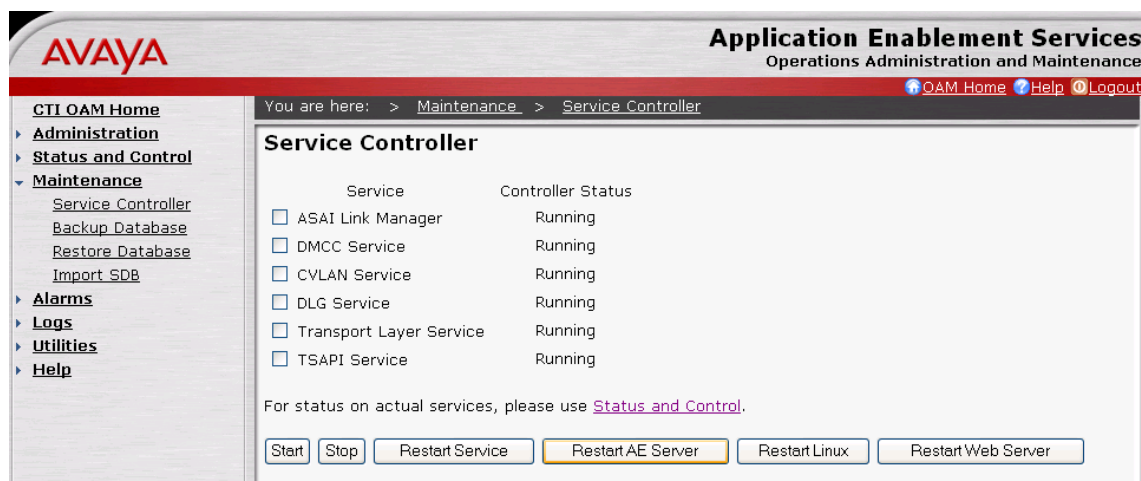
Switch Connection: CMCyber

Switch CTI Link Number: 10

ASAI Link Version: 4

Security: Encrypted

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**.



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 TSAPI and DMCC services are **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.
- **User 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 shows "You are here: > User Management > Add User". The left sidebar contains a menu with "User Management Home", "User Management" (expanded), "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 contains a form with 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 dots), "\* Confirm Password" (password box with 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). A note above the form states "Fields marked with \* can not be empty."

## 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. A second screen appears. Click the **Apply** button. The CTIUser is now enabled for unrestricted access.

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 contains several form fields. The 'Unrestricted Access' field has a red box around it, and the 'Enable' button is highlighted. Other fields include User ID, Common Name, Worktop Name, Call Origination and Termination, Device / Device, Call / Device, Call / Call, and Allow Routing on Listed Device. At the bottom are 'Apply Changes' and 'Cancel' buttons.

## 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, and its 'Enabled' radio button is selected. The other rows have their 'Disabled' radio buttons selected.

DMCC Server Ports	Enabled	Disabled
Unencrypted Port 4721	<input type="radio"/>	<input checked="" 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 System

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. It is assumed that the CyberTech system has been pre-configured to release 5.3 at this point.

The subsequent configuration includes the following areas:

- **Install components on Core Server**
  - Install the `cti_receiver.exe`
  - Upgrade the CyberTech database to set Multiple Registrations as a recording option
- **Install components on CTI Server**
  - Install of the SSL Certificate
  - Install of the Avaya Link Controller, Call Controller and the TSAPI Client
- **Configure the CyberTech Pro Voice Recorder**

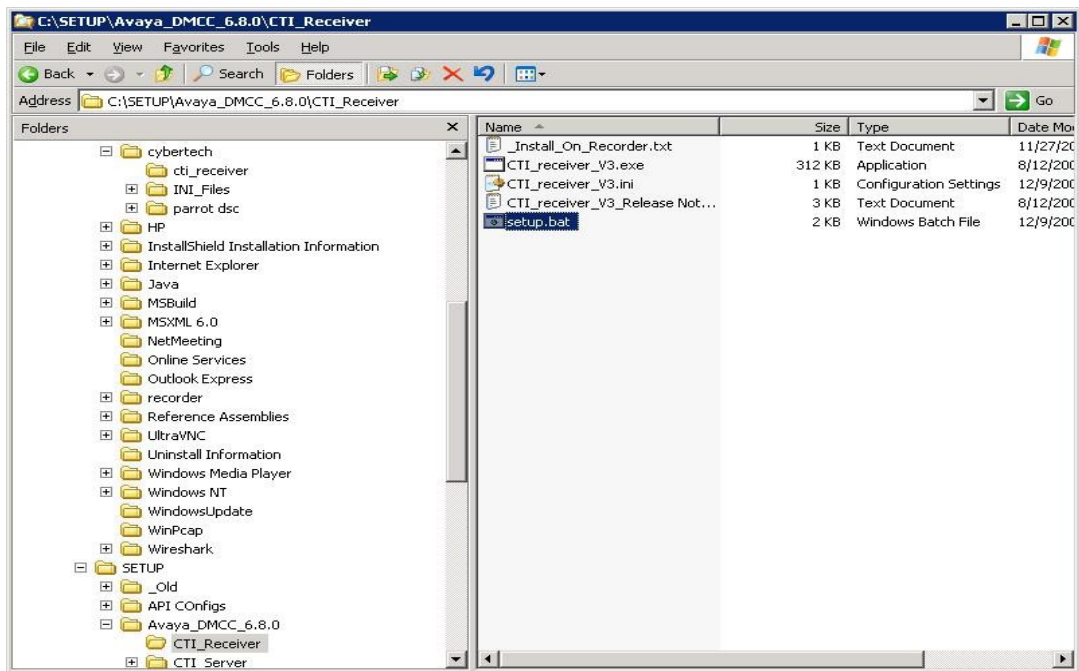
### 7.1 Install Components on the Core Server

A `cti_receiver` file needs to be installed on the CyberTech server and the database needs to be upgraded to set Multiple Registrations as a recording option.

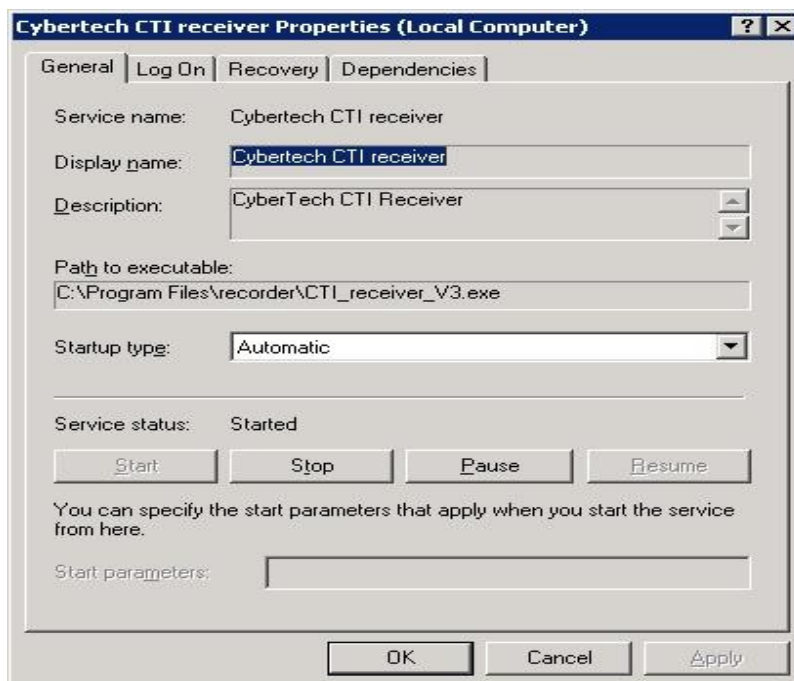
#### 7.1.2 Cti Receiver

The `cti_receiver3.exe` needs to be installed. The original version must be removed from the system where it is located at `\\Program Files\\CyberTech\\cti_receiver`. The new version will be located at `\\Program Files\\Recorder`.

To remove the old version and install the new one, run the **C:\SETUP\Avaya\_DMCC\_6.8.0\CTI\_Receiver\setup.bat** which is located in the CTI\_Receiver directory as shown in the following screen.

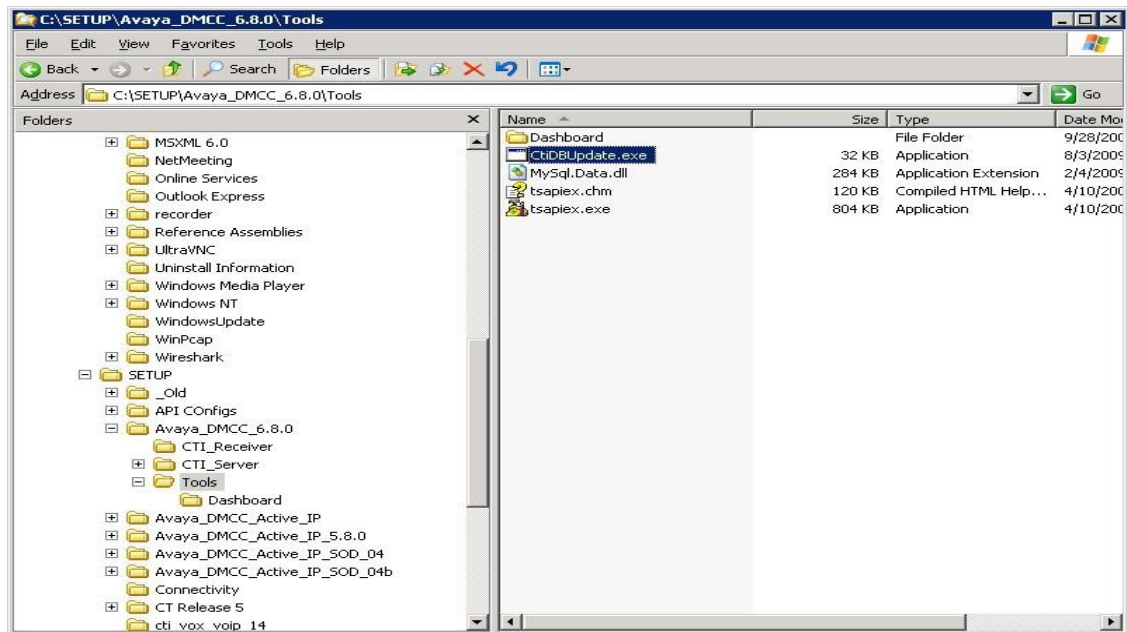


Two command line screens follow in quick succession to indicate that the setup has started and later that the install has been successful. If the installation was successful it can be verified by checking the Microsoft Services as shown below.



### 7.1.3 Upgrade the Recorder Database

An entry needs to be added to the Recorder Database to allow the Multiple Registrations method of recording. This is carried out by running the file **C:\SETUP\Avaya\_DMCC\_6.8.0\Tools\CtiDBUpdate.exe** which is located in the Tools directory as shown in the screen below.



The following screen **Setup CTI Fields** is displayed. Choose the **Test Connection** button to connect to the database. Choose the **Avaya Targets** button to display default values. Next choose **Write Back** and a record with default values is written to the database.

Database is open!  
DB Connection open!

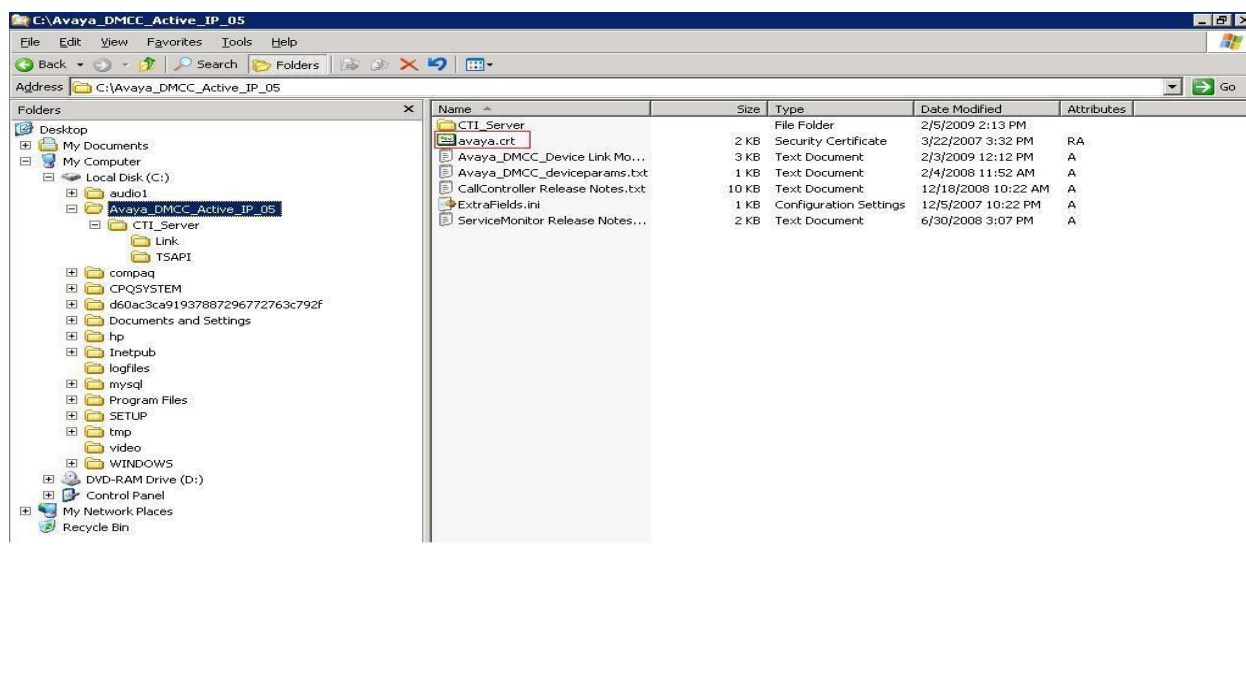
No message is received that the database is updated successfully. Verify by checking on the web interface if the 'Multiple Registration Extension' has been added as a recording type (as shown in **Section 7.3**).

## 7.2 Install Components on the CTI Server

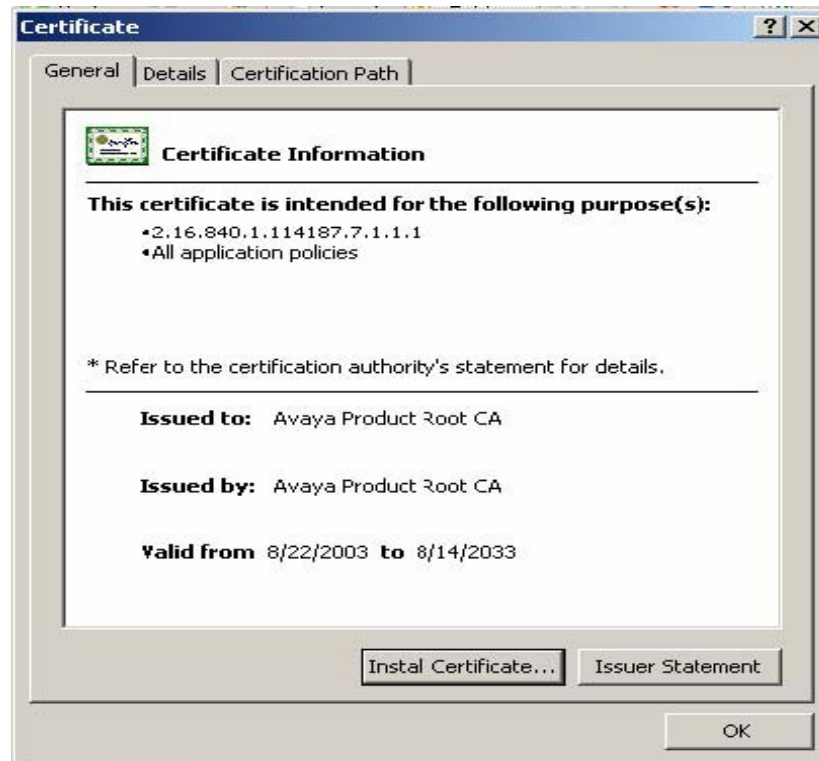
The SSL certificate, Avaya Link Controller, Call Controller, MS Visual C++ and TSAPI Client components need to be installed on the CTI Server.

## 7.2.1 Install the SSL Certificate for the AES Connection

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



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



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



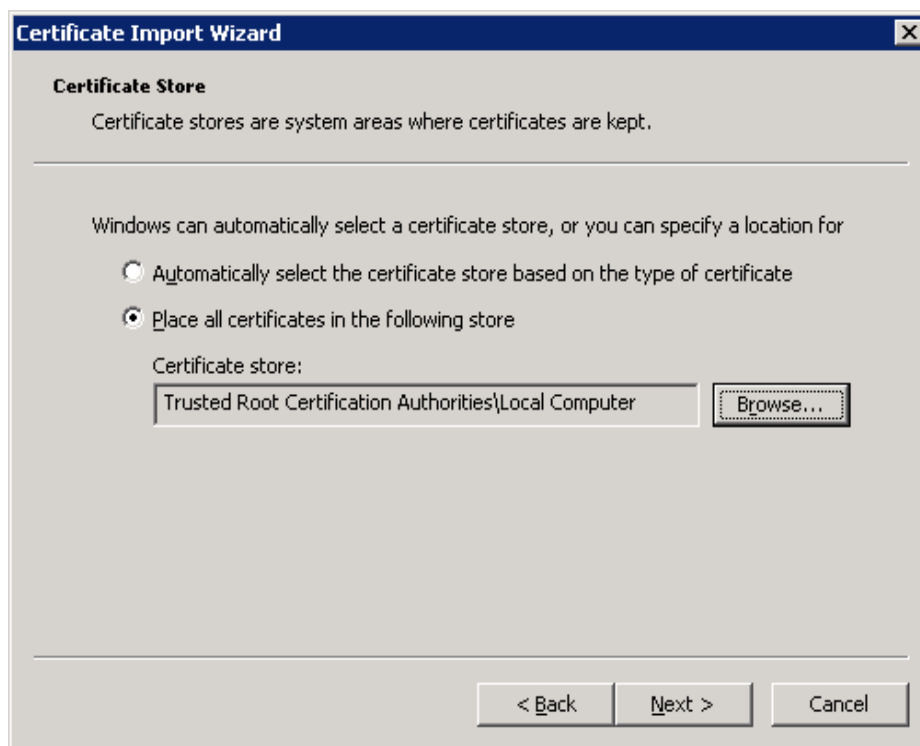
Click **Browse** to select the certificate destination.



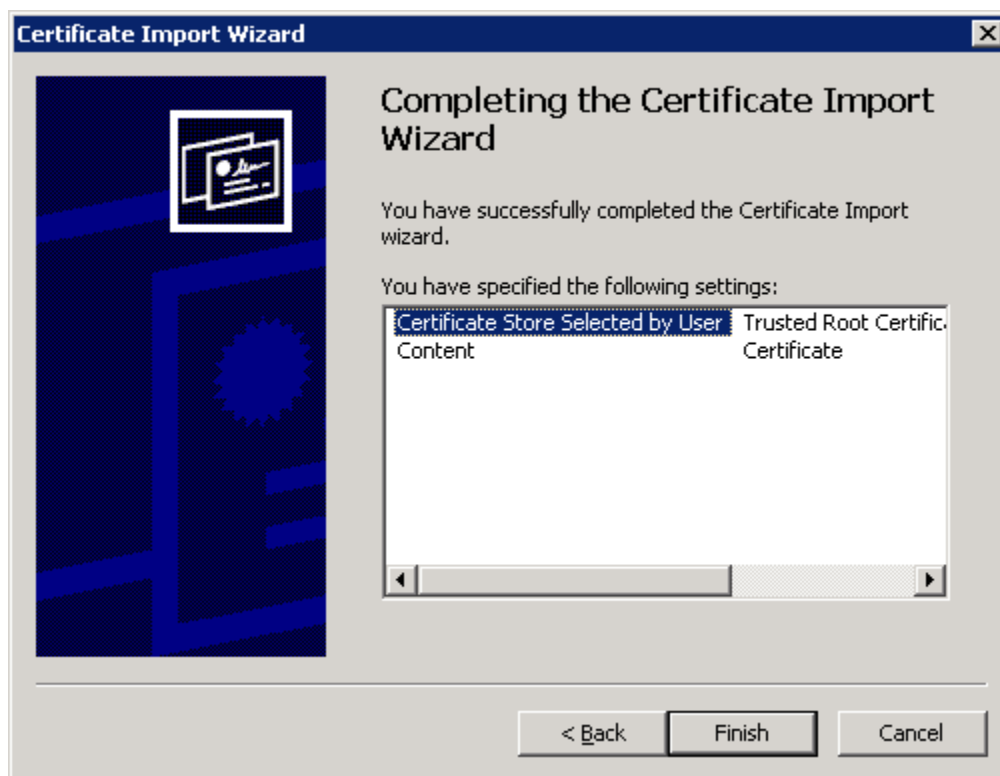
Select the **Local Computer**, as shown.



Click **Next** after confirming the destination.

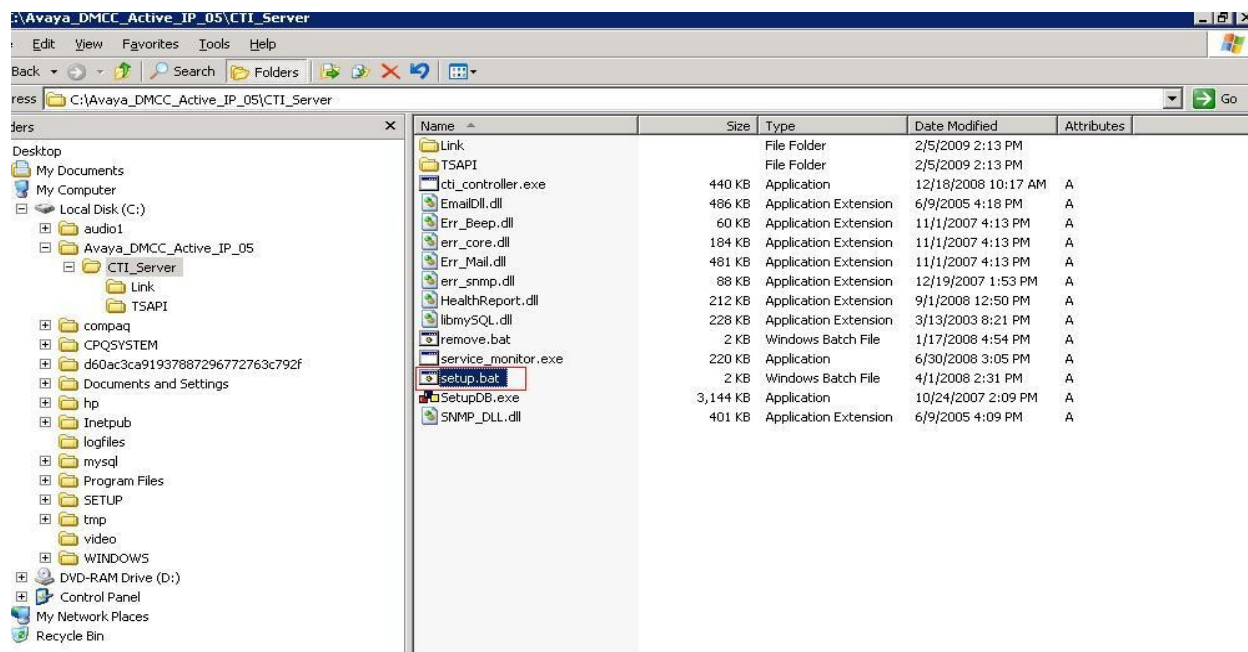


Click **Finish** after the certificate installation is complete.

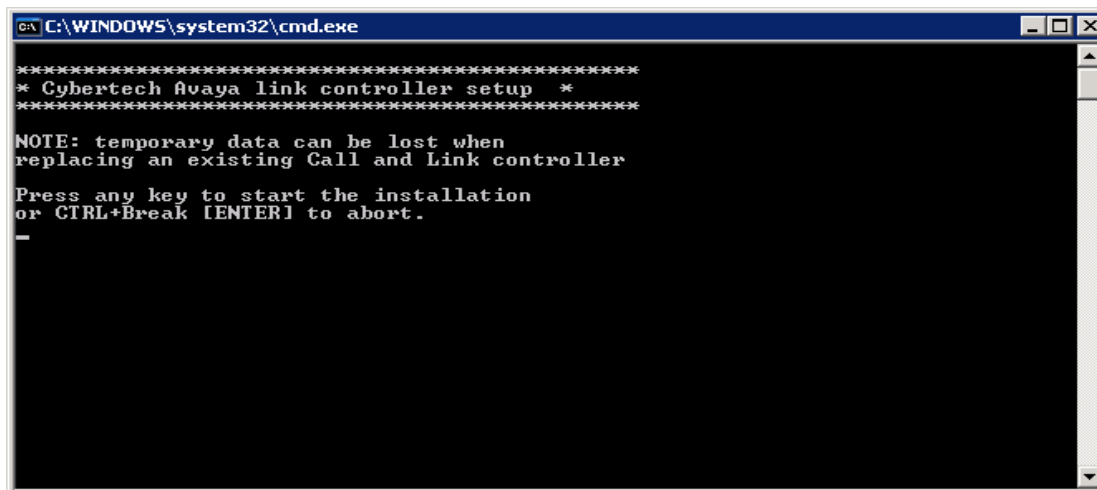


## 7.2.2 Install Avaya Link Controller, Call Controller and the TSAPI Client on CTI Server

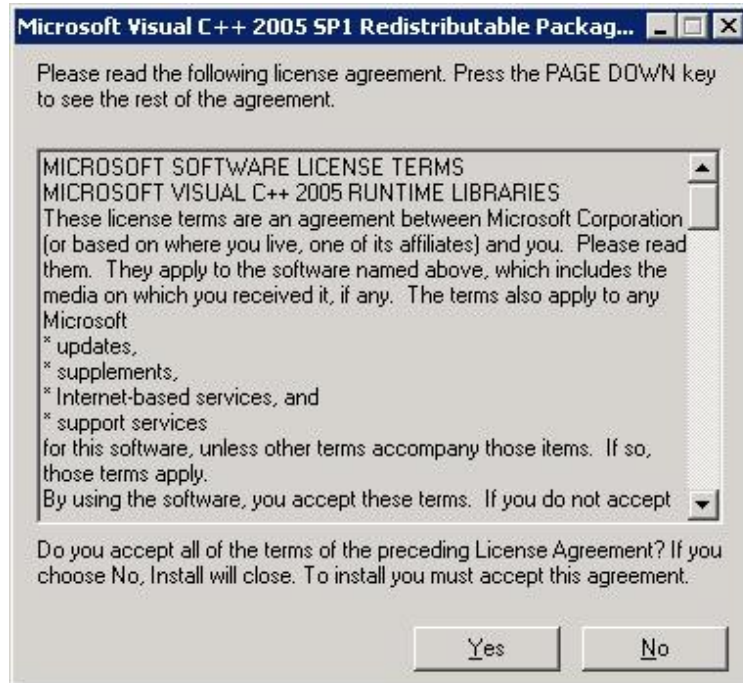
The Avaya Link Controller, Call Controller and the TSAPI Client must be installed on the CTI Server, as shown by the following steps. First, execute the 'setup.bat' file as shown in the default directory **C:\Avaya\_DMCC\_Active\_IP\_05\CTI\_Server** in the following screen. Make sure you run this batch file on the CTI server.



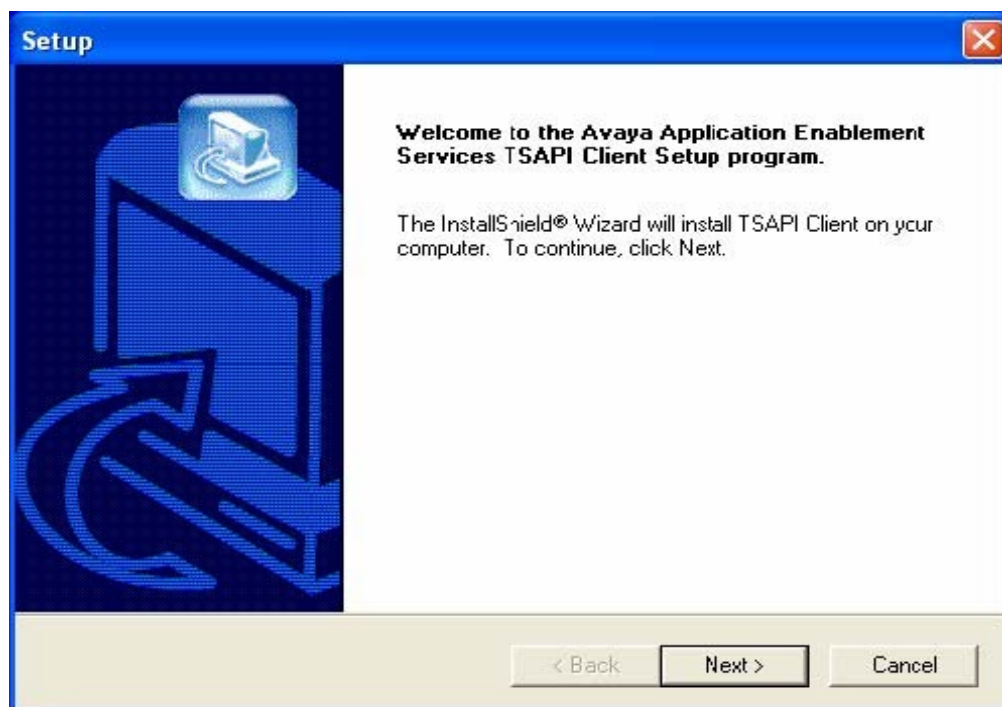
This will open a dialog box as follows. Press any key to automatically install the Avaya Link Controller and the Call Controller on the CTI server.



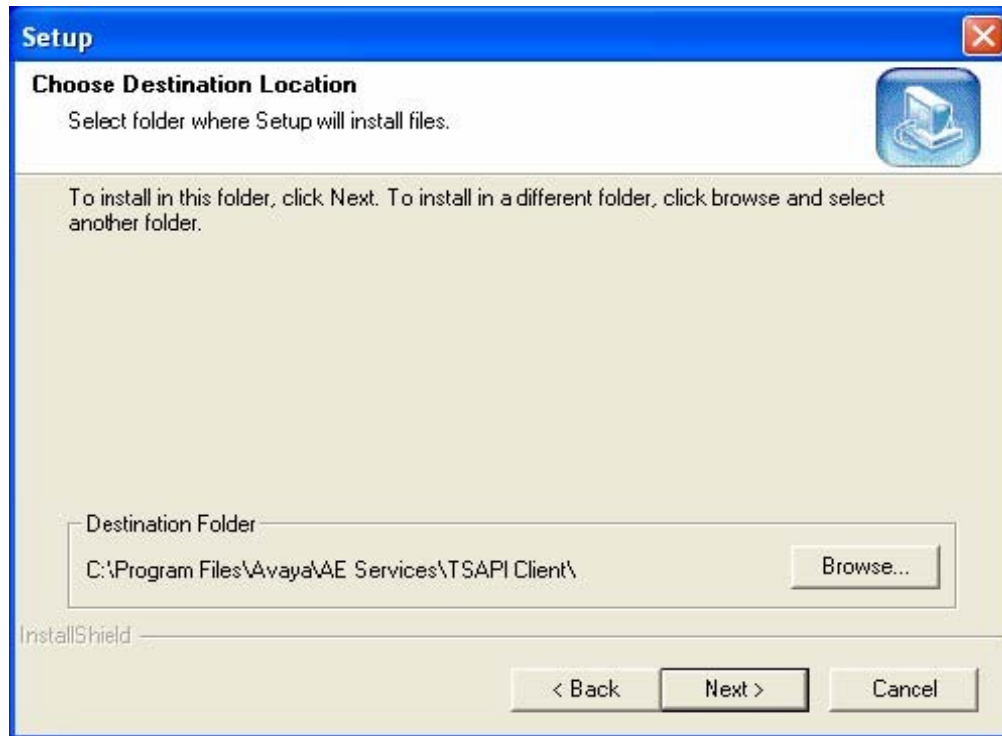
Next MS Visual C++ 2005 SP1 is installed as shown in the following screen.



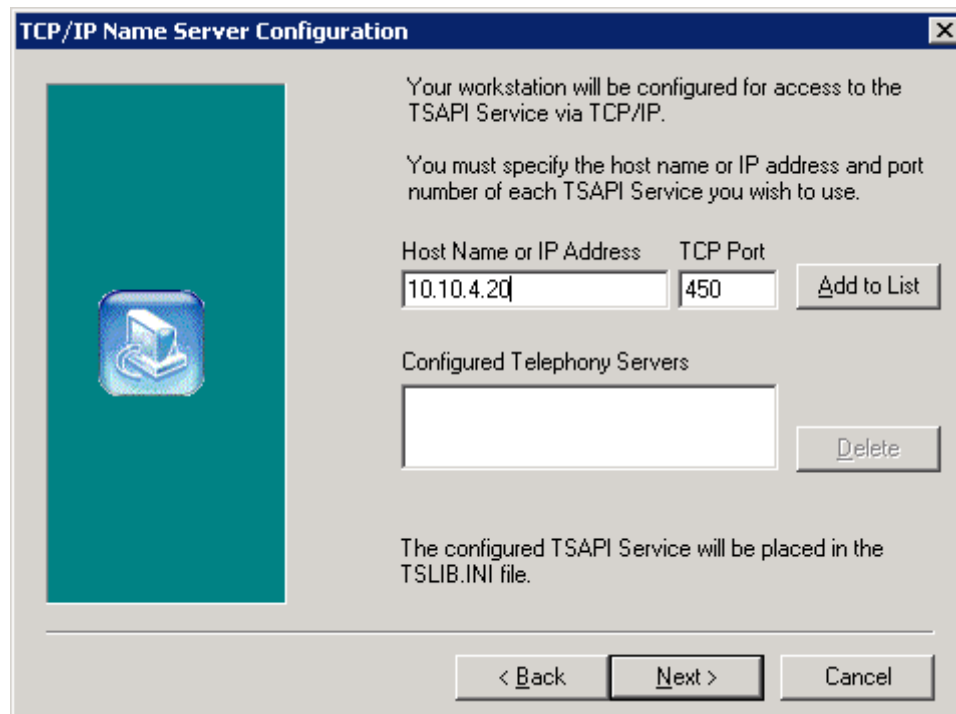
After these steps the TSAPI installer will start.



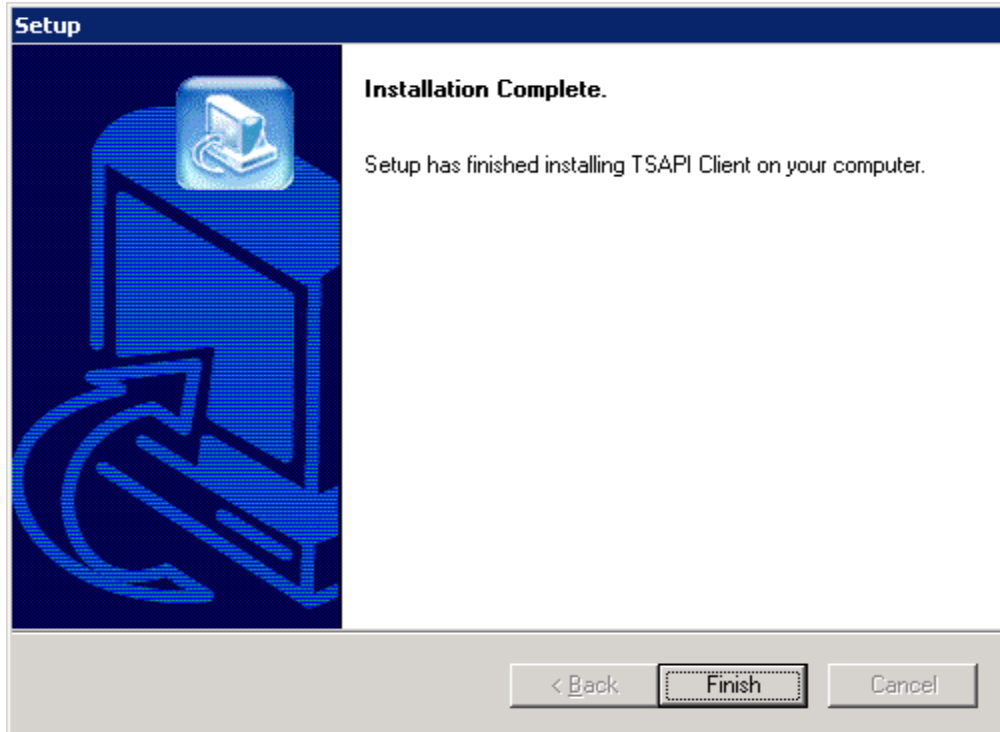
Retain the default installation folder and click **Next**.



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



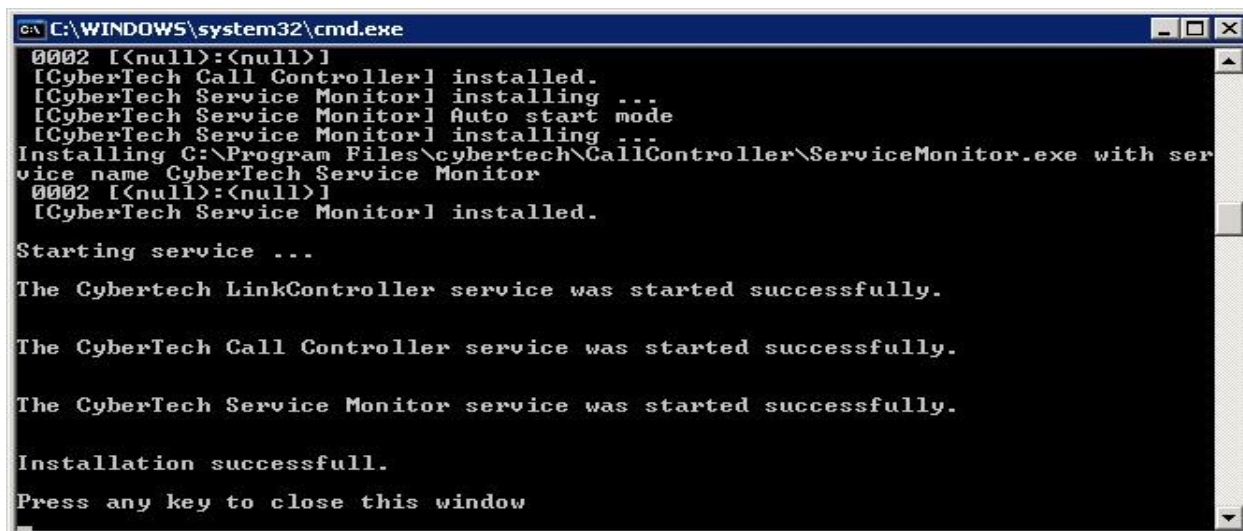
Click **Finish** after the installation completes.



Once the TSAPI installation is complete the **SetupDB** screen appears with most of the fields populated as follows. The **Database HostName** field is populated with the IP address of the Recorder Server. The **Recorder ID** field is also populated. The value given must be 0 or 1. The value 0 represents the stand-alone CTI Server while 1 represents the all-in-one box solution. In this case the value **0** is entered. For the all-in-one box solution, the Database HostName given must be 'localhost' and the Recorder ID value '1'. Press enter to continue to next screen.

A screenshot of the 'SetupDB' configuration window. The title bar says 'SetupDB'. It contains several text input fields and two buttons. The fields are: 'Database HostName' (value: 10.10.4.200), 'Database Name' (value: recorder), 'Database Username' (value: recorder), 'Database Password' (value: masked with dots), 'Recorder ID' (value: 0), 'Log File Location' (value: c:\LogFiles), and 'Log File retention (Days)' (value: 14). The 'Recorder ID' field is highlighted with a red rectangle. To the right of the 'Recorder ID' field is a button labeled 'Read from registry'. To the right of the 'Log File retention (Days)' field is a button labeled 'Write to registry'. At the bottom is a text area labeled 'Red settings on Start-up'.

The installation displays a screen indicating the successful completion.



```
C:\WINDOWS\system32\cmd.exe
0002 [<null>:<null>]
[CyberTech Call Controller] installed.
[CyberTech Service Monitor] installing ...
[CyberTech Service Monitor] Auto start mode
[CyberTech Service Monitor] installing ...
Installing C:\Program Files\cybertech\CallController\ServiceMonitor.exe with ser
vice name CyberTech Service Monitor
0002 [<null>:<null>]
[CyberTech Service Monitor] installed.

Starting service ...

The Cybertech LinkController service was started successfully.

The CyberTech Call Controller service was started successfully.

The CyberTech Service Monitor service was started successfully.

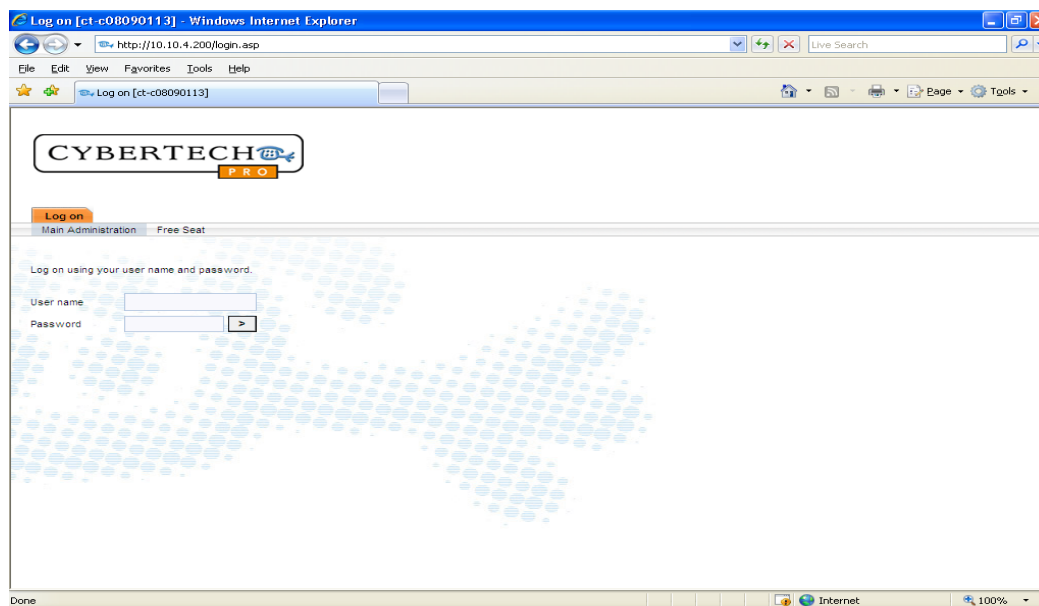
Installation successfull.

Press any key to close this window
```

### 7.3. Configure the CyberTech Pro Voice Recorder

The CyberTech Pro Voice Recorder is configured for the Multiple Registrations recording method 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 (not shown). Select the **Device name** to display details of device settings as shown below.

The screenshot shows the CyberTech Pro web interface. The top navigation bar includes tabs like 'my account', 'system installation', 'cti integration', 'system configuration', 'user administration', 'system status', 'evaluation', 'recorded calls', and 'quit'. The 'cti integration' tab is selected, showing a sub-tab 'devices'. Below this is a table titled 'Overview of all devices' with columns: Device name, Device enabled, Connection type, Auto-discovery en..., Device state, Linked channel group, and Date last modified. The table contains one entry: 'Avaya\_Link' with 'Device enabled' as 'Yes', 'Connection type' as 'TCP / IP', 'Auto-discovery en...' as 'No', 'Device state' as 'Logged in', and 'Linked channel group' as 'Avaya cert'. Below the table, there are two sections: 'General device settings' and 'Connection settings'. The 'General device settings' section shows 'Device name' as 'Avaya\_Link', 'Device enabled' as 'Yes', 'Auto-discovery enabled' as 'No', and 'Device parameters' as 'SwitchName=CMCYBER, ObserveCode=#3, TSAPIServerName=AVAYA#CMCYBER#CSTA#PRESAES, ConnectionUseSSL=Yes, ConnectionProtocol=4.2'. The 'Connection settings' section shows 'Connection host' as '10.10.4.20', 'IP port' as '4722', 'Connection user' as 'CTIUser', 'Connection password' as '\*\*\*\*\*', 'Password (retype)' as '\*\*\*\*\*', and 'Linked channel group' as 'Avaya cert'. At the bottom, there are 'Cancel' and 'Save changes' buttons. A status bar at the very bottom shows the time '14:13:33' and a message 'You are editing an existing record.'.

In the next screen below, in the **General device settings** form, ensure that the **Device Parameters** values in **Table 5** are entered. Then select **Device Enabled** as **Yes**. The **TSAPIServerName** value is shown in **Section 6.3**.

Parameter	Value
SwitchName	CMCyber
ObserveCode	#3
TSAPIServerName	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.

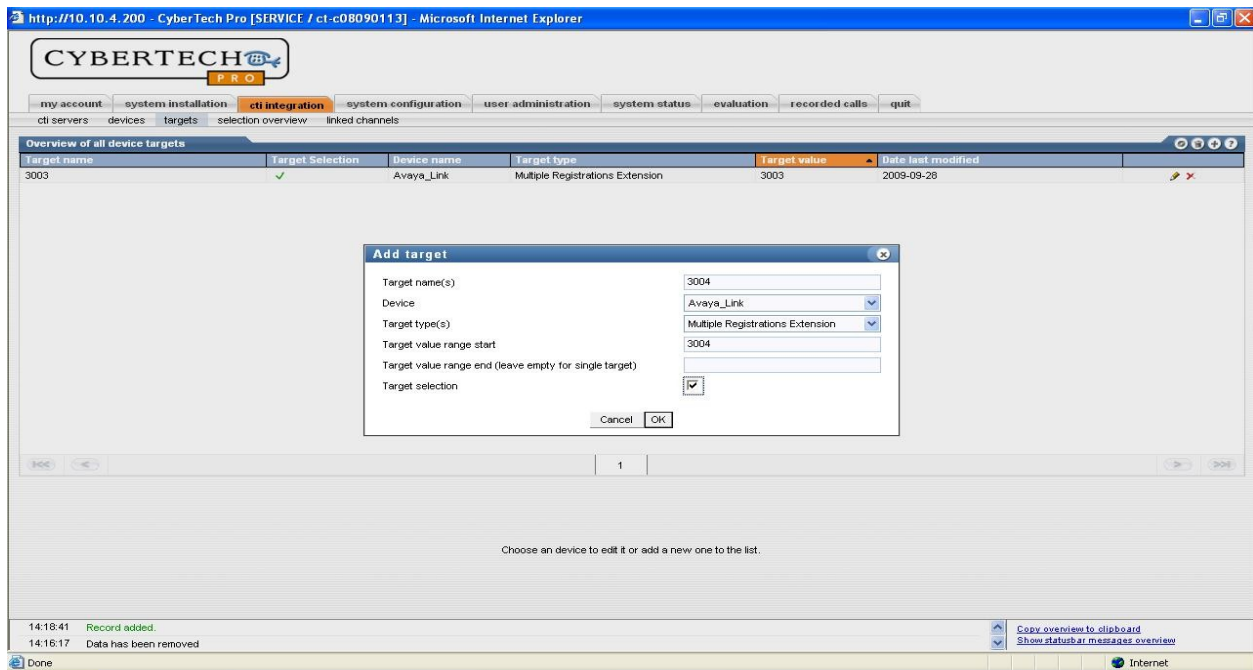
Parameter	Usage
Connection host	Enter the IP address of the Avaya AES Server.
IP port	Enter the default encrypted port of <b>4722</b> .
Connection user	Enter the user name which was defined in <b>Section 6.4</b> .
Connection password	Enter the “User Password” which was defined in <b>Section 6.4</b> .

**Table 6: CyberTech Pro Connection Settings**

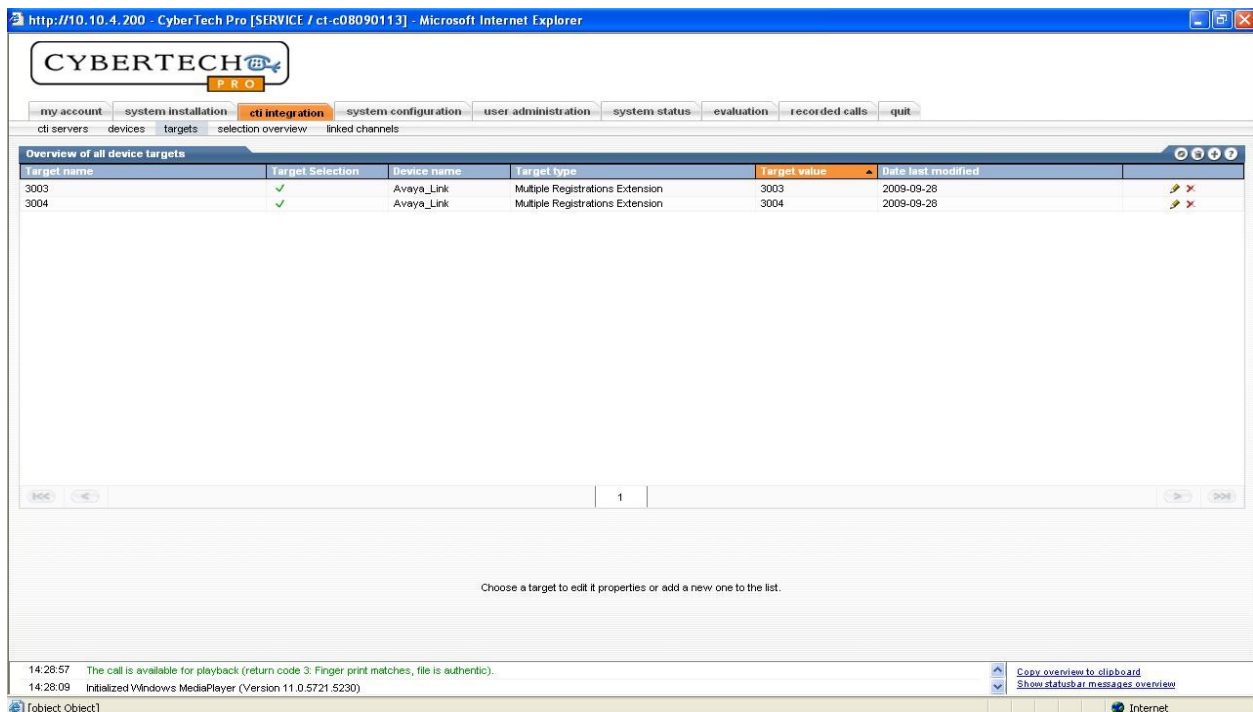
Click **Save changes** once the values have been added.

The screenshot shows the CyberTech Pro web interface in a Microsoft Internet Explorer browser window. The address bar displays 'http://10.10.4.200 - CyberTech Pro [SERVICE / ct-c08090113] - Microsoft Internet Explorer'. The interface features a navigation menu with tabs: 'my account', 'system installation', 'cti integration' (selected), 'system configuration', 'user administration', 'system status', 'evaluation', 'recorded calls', and 'quit'. Below this, there are sub-tabs: 'cti servers', 'devices', 'targets', 'selection overview', and 'linked channels'. The main content area is titled 'Overview of all devices' and contains a table with the following columns: 'Device name', 'Device enabled', 'Connection type', 'Auto-discovery en...', 'Device state', 'Linked channel group', and 'Date last modified'. The table lists one device, 'Avaya\_Link', which is enabled, has a connection type of 'TCP / IP', auto-discovery is disabled, its state is 'Unknown', it is linked to the 'Avaya cert' group, and was last modified on '2009-09-28'. Below the table, there are two panels: 'General device settings' and 'Connection settings'. The 'General device settings' panel shows 'Device name' as 'Avaya\_Link', 'Device enabled' as 'Yes', 'Auto-discovery enabled' as 'No', and 'Device parameters' as 'User record=0', 'TSAPServerName=AVAYA#CMCYBER#CSTA-S#PRESAES', 'ConnectionUseSSL=Yes', 'ConnectionProtocol=4.2', and 'UseSRTP=Yes'. The 'Connection settings' panel shows 'Connection host' as '10.10.4.200', 'IP port' as '4722', 'Connection user' as 'CTIUser', 'Connection password' as '\*\*\*\*\*', 'Password (retype)' as '\*\*\*\*\*', and 'Linked channel group' as 'Avaya cert'. At the bottom right of the configuration panels are 'Cancel' and 'Save changes' buttons. The status bar at the bottom shows '15:08:32 You are editing an existing record.', '15:08:29 Record updated.', and a 'Copy overview to clipboard' button. The bottom of the browser window shows '[Object Object]' and '10.10.4.200 - Remote Desktop'.

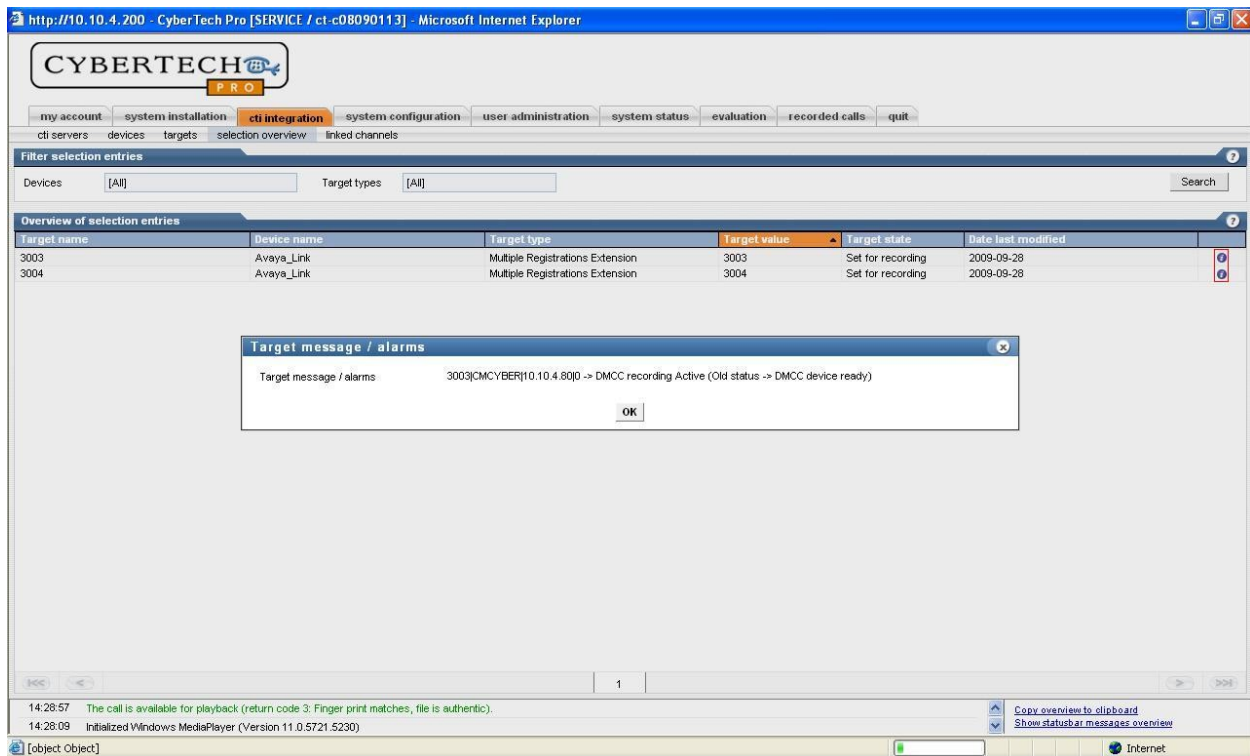
Select the **targets** secondary tab and click the “+” symbol for each target to be added. A target is any extension added as a Multiple Registration Extension (screen not shown). A target is added as shown in the following screen. Populate the fields as shown. The **Target name** is the station password of the station assigned with the **Target type** of **Multiple Registration Extension** as seen in the screen below..



After the targets have been entered, the targets extensions are shown as follows.



Additional information for each of the targets is available via the **I** button. This indicates whether the extensions to be recorded are actively monitored by the DMCC.



## 8. General Test Approach and Test Results

The test approach was to make calls using digital and VOIP phones as supported by Multiple Registrations. 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. 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 clear audio for each of G.711 and G.729 codec
- Confirmation of calling and called party CLI
- 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.

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

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

<b>status aesvcs interface</b>			
AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
<b>CLAN</b>	<b>yes</b>	<b>1</b>	<b>listening</b>

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

<b>status aesvcs link</b>						
AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
<b>02/01</b>	<b>PresAES</b>	<b>10. 10. 4. 20</b>	<b>32851</b>	<b>CLAN</b>	<b>244</b>	<b>255</b>

## 9.2. Verify 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.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top header displays the Avaya logo and the title "Application Enablement Services Operations Administration and Maintenance". The breadcrumb trail indicates the user is in "Status and Control > Switch Conn Summary". The left sidebar contains navigation links: CTI OAM Home, Administration, Status and Control (selected), Maintenance, Alarms, Logs, Utilities, and Help. The main content area is titled "Switch Connections Summary" and displays a table with the following data:

Switch Conn	Conn State	Since	Online/ Offline	Active CLANS/ Admin'd CLANS	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
CMCyber	Talking	2009-09-23 20:45:54.0	Online	1 / 1	2	287	280	30

Below the table, there are buttons for "Online", "Offline", "Message Period", and "Switch Connection Details". A link for "Per Service Switch Connections Details" is also present.

Verify the status of the TSAPI link by checking that the **Connection State** 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 displays the Avaya logo and the title "Application Enablement Services Operations Administration and Maintenance". The breadcrumb trail indicates the user is in "Status and Control > Services Summary". The left sidebar contains navigation links: CTI OAM Home, Administration, Status and Control (selected), Maintenance, Alarms, Logs, Utilities, and Help. The main content area is titled "DMCC Service Summary - Session Summary" and displays the following information:

**Session Summary** [Device Summary](#)  
Generated on Mon, Sep 28, 2009 06:08:50 PM IST

Service Uptime: 4 days, 21:22 hours  
Number of Active Sessions: 1  
Number of Sessions Created Since Service Boot: 6  
Number of Existing Devices: 2  
Number of Devices Created Since Service Boot: 17

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/> B50C530582E2AE30B 134E0C9C32C77C8-8	CTIUser	Avaya_Link	10.10.4.210	XML Encrypted	2

At the bottom, there are buttons for "Terminate Sessions" and "Show Terminated Sessions".

### 9.2.3. 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 user is at "Utilities > TSAPI Test". The left sidebar contains a navigation menu with options like "Administration", "Status and Control", "Maintenance", "Alarms", "Logs", "Utilities", and "Help". The "Utilities" section is expanded, showing "ASAI Test", "Ping Host", "TSAPI Test", and "TR/87 Test". The main content area is titled "TSAPI Test" and contains several input fields: "TLink" (a dropdown menu showing "AVAYA#CMCYBER#CSTA-S#PRESAES"), "User:" (a text box with "CTIUser"), "Password:" (a masked text box with "\*\*\*\*\*"), "From:" (a text box with "3002"), and "To:" (a text box with "3004"). There is also a "Dial" button.

The following message indicates a successful result.

The screenshot shows the AVAYA Application Enablement Services (AES) interface displaying the "TSAPI Test Result". The breadcrumb trail now shows "Utilities". The left sidebar is the same as in the previous screenshot. The main content area is titled "TSAPI Test Result" and displays a list of test results:

- TsTest
- (Using TLink AVAYA#CMCYBER#CSTA#PRESAES instead of AVAYA#CMCYBER#CSTA-S#PRESAES.)
- cstaMakeCall() succeeded!
- cstaClearConnection() succeeded!

### 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 hunt groups and agents and verify that correct call records are produced
- Ensure RTP packages are received successfully from the AES

## 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. *Administering Avaya Aura™ Communication Manager*, Document No 03-300509, May 2009
2. *Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide - Release 4.2*, Document No 02-300357, Issue 10, May 2008
3. *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 v5.5*
2. *CyberTech Parrot DSC - VOIP installation manual*
3. *CyberTech CT Recording Solutions R5 - CTI manual*
4. *CyberTech CTI Avaya Recording Installation 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](mailto:devconnect@avaya.com).