



Application Notes for Configuring CyberTech Pro with Avaya Communication Manager – Issue 1.2

Abstract

These Application Notes describe the compliance testing of the CyberTech Pro voice recording system with Avaya Communication Manager. These Application Notes contain an extensive description of the configurations for both CyberTech Pro and Avaya 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.

Table of Contents

1. Introduction.....	3
2. Equipment and Software Validated	4
3. Configuration	5
3.1. Configure Avaya Communication Manager	5
3.1.1. Verify system-parameters customer-options	6
3.1.2. Configure system-parameters features	9
3.1.3. Configure Feature Access Codes.....	10
3.1.4. Configure Node Names	11
3.1.5. Configure Telephone Stations.....	11
3.1.6. Configure CTI Telephone Stations	13
3.1.7. Configure Pickup Group	15
3.1.8. Configure Agents.....	15
3.1.8.1 Configure Agent VDN	15
3.1.8.2 Configure Agent Login	17
3.1.8.3 Configure Agent Hunt Group	19
3.1.8.4 Configure Agent Queue Vector	20
3.1.9. Configure Interface to Avaya AES.....	21
3.2. Configure Avaya AES	23
3.2.1. Create Switch Connection	25
3.2.2. Create TSAPI Link	28
3.2.3. Create Avaya AES User	30
3.3. Configure CyberTech CTI Server	31
3.3.1. Install TSAPI Client on CTI Server	31
3.3.2. Install the SSL Certificate for the AES Connection	35
3.4. Configure the CyberTech Pro Voice Recorder	41
4. Interoperability Compliance Testing	50
4.1. General Test Approach	50
4.2. Test Results	51
5. Verification Steps	51
6. Support.....	51
7. Conclusion	51
8. Additional References.....	52

1. Introduction

The purpose of this document is to describe the compliance testing done with CyberTech Pro and Avaya Communication Manager, including a description of the configuration of each, 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. 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 Avaya Application Enablement Services (AES) server was used by CyberTech Pro to receive call status information. CyberTech Pro then used the Avaya Communication Manager “service observe” facility to collect voice data streams of endpoints which were selected to be monitored.

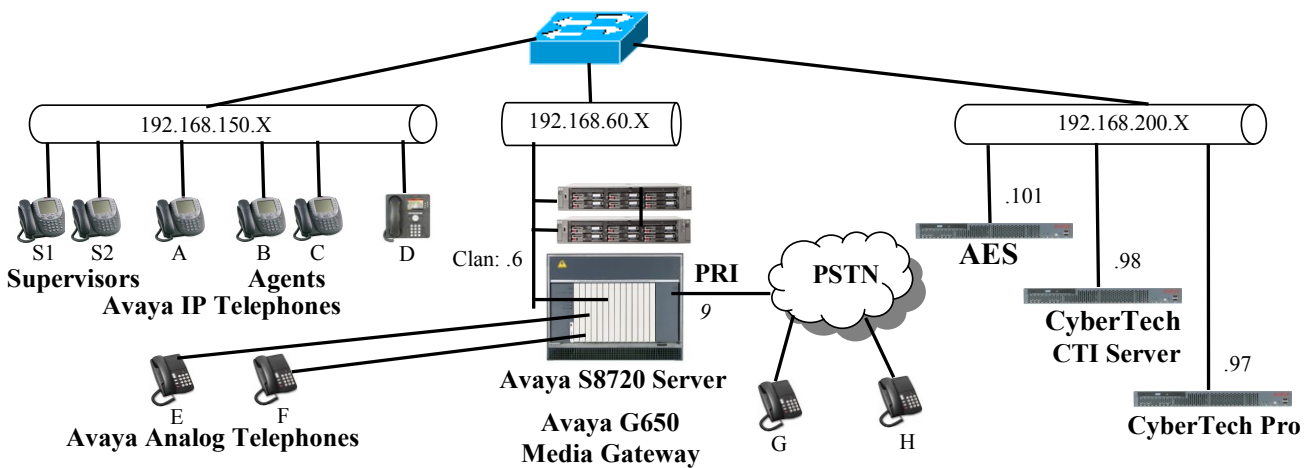


Figure 1: CyberTech Pro Test Configuration

2. Equipment and Software Validated

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

Equipment	Software Version
Avaya S8720 Servers Avaya Communication Manager	4.0.1 .731.2-14300
Avaya Application Enablement Services Server	4.0.1
Avaya TN2312BP IPSI interface.	HW01, FW40
Avaya TN799DP Control LAN	HW01, FW24
Avaya TN793CP DS1 Interface	HW01, FW19
Avaya TN2464CP Analog Line	HW07, FW09
Avaya 4600 series Telephones	2.8 (H.323)
Avaya 9640 Telephone	1.5 (H.323)
CyberTech Pro	MynaVoice 3.0 FP2.0 SP1
CyberTech CTI Server	CallController 1.0.6.0 AvayaLinkController 1.0.8.0

Table 1: Version Numbers of Equipment and Software

3. Configuration

Table 2 contains the extensions that are used for testing. The capital letter designations correspond to the telephones shown in **Figure 1**.

Extension	Type	Designation	PSTN
60131	4620	S1	069 9073 9887 60131
60123	4621	S2	069 9073 9887 60123
60113	4610	A	069 9073 9887 60113
60116	4610	B	069 9073 9887 60116
60093	9610	C	069 9073 9887 60093
60081	9640	D	069 9073 9887 60081
60201	2500	E	069 9073 9887 60201
60202	2500	F	069 9073 9887 60202
61001	VDN		069 9073 9887 61001
61401-5	Virtual CTI ext.		
61601	agent	Agent B	
61602	agent	Agent C	
61301		Agent HG	069 9073 9887 61301
	PSTN	G	069 7505 6176
	PSTN	H	069 7505 6645

Table 2: Extensions Used for Testing

3.1. Configure Avaya Communication Manager

The configuration and verification operations illustrated in this section were all performed using the Avaya Communication Manager System Administration Terminal (SAT) via SSH port 5022.

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

The configuration operations describe 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 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
- Allocate a 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.

3.1.1. Verify system-parameters customer-options

Use the **display system-parameters customer-options** command to verify that Avaya Communication Manager is licensed to meet the minimum requirements to interoperate with the CyberTech Pro server. Those items shown in bold 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.

display system-parameters customer-options		Page 2 of 10
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks: 30		5
Maximum Concurrently Registered IP Stations: 10		3
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: 0		0
Maximum Video Capable H.323 Stations: 0		0
Maximum Video Capable IP Softphones: 0		0
Maximum Administered SIP Trunks: 10		3
Maximum Number of DS1 Boards with Echo Cancellation: 0		0
Maximum TN2501 VAL Boards: 0		0
Maximum Media Gateway VAL Sources: 0		0
Maximum TN2602 Boards with 80 VoIP Channels: 0		0
Maximum TN2602 Boards with 320 VoIP Channels: 0		0
Maximum Number of Expanded Meet-me Conference Ports: 0		0

Figure 2: System-Parameters Customers-Options Form, Page 2

Verify that the parameters on page 3 are set as shown in the following table:

Parameter	Usage
Computer Telephony Adjunct Links?	This parameter must be set to “y”.

Table 3: System-Parameters Customer-Options Parameters, Page 4

```

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

```

Figure 3: System-Parameters Customers-Options Form, Page 4

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 10
                                OPTIONAL FEATURES

Emergency Access to Attendant? y          IP Stations? y
Enable 'dadmin' Login? y
Enhanced Conferencing? n
Enhanced EC500? y
Enterprise Survivable Server? n
Enterprise Wide Licensing? n
ESS Administration? n
Extended Cvg/Fwd Admin? n
External Device Alarm Admin? n
Five Port Networks Max Per MCC? n
Flexible Billing? n
Forced Entry of Account Codes? n
Global Call Classification? n
Hospitality (Basic)? y
Hospitality (G3V3 Enhancements)? n
IP Trunks? y
IP Attendant Consoles? n

ISDN Feature Plus? n
ISDN Network Call Redirection? n
ISDN-BRI Trunks? y
ISDN-PRI? y
Local Survivable Processor? n
Malicious Call Trace? n
Media Encryption Over IP? n
Mode Code for Centralized Voice Mail? n
Multifrequency Signaling? y
Multimedia Call Handling (Basic)? n
Multimedia Call Handling (Enhanced)? n

```

Figure 4: System-Parameters Customers-Options Form, Page 4

On page 6: the “EAS-PHD” parameter must be set to “y” so that skill levels greater than 3 can be selected.

```
display system-parameters customer-options                               Page 6 of 11
CALL CENTER OPTIONAL FEATURES

Call Center Release: 3.0

ACD? y                               Reason Codes? n
BCMS (Basic)? n                     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)? n
Business Advocate? n                Service Observing (VDNs)? n
Call Work Codes? n                  Timed ACW? n
DTMF Feedback Signals For VRU? n     Vectoring (Basic)? y
Dynamic Advocate? n                 Vectoring (Prompting)? 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
```

Figure 5: System-Parameters Customers-Options Form, Page 6

On page 9: the “CTI Stations” parameter must be set to “y”.

```
display system-parameters customer-options                               Page 9 of 11
ASAI ENHANCED FEATURES

CTI Stations? y
Increased Adjunct Route Capacity? n
Phantom Calls? y

ASAI PROPRIETARY FEATURES

Agent States? n
```

Figure 6: System-Parameters Customers-Options Form, Page 9

On page 10: the “IP_API_A” capacity must be sufficient to handle the number endpoints which are to be recorded (one for each endpoint).

```
display system-parameters customer-options
```

Page 10 of 11

MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID	Rel. Limit	Used
IP_API_A	: 1000	0
IP_API_B	: 1000	0
IP_API_C	: 1000	0
IP_Agent	: 1000	0
IP_IR_A	: 1000	0
IP_Phone	: 12000	12
IP_ROMax	: 12000	0
IP_Soft	: 1000	0
IP_eCons	: 128	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0

Figure 7: System-Parameters Customers-Options Form, Page 10

3.1.2. Configure system-parameters features

Use the **change system-parameters features** command to set the “Call Pickup Alerting?” and “Directed Call Pickup?” parameters to “y”.

```
change system-parameters features
```

Page 4 of 17

FEATURE-RELATED SYSTEM PARAMETERS

Reserved Slots for Attendant Priority Queue: 5

Time before Off-hook Alert: 10

Emergency Access Redirection Extension:

Number of Emergency Calls Allowed in Attendant Queue: 5

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

Deluxe Paging and Call Park Timeout to Originator? n

Controlled Outward Restriction Intercept Treatment: tone

Controlled Termination Restriction (Do Not Disturb): tone

Controlled Station to Station Restriction: tone

AUTHORIZATION CODE PARAMETERS Authorization Codes Enabled? n

Controlled Toll Restriction Replaces: none

Figure 8: System-Parameters Features Form, Page 4

3.1.3. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure all of the access codes shown in **Table 4**.

Parameter	Usage
Call Pickup Access Code	This is used by telephone users to initiate a call-pickup operation.
Auto-in	This is used by the agent 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.

Table 4: Feature Access Codes

change feature-access-codes	Page 1 of 6
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: 00	Access Code 2: 9
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: *76	
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:

Figure 9: Feature Access Codes, Page 1

```

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

                                Automatic Call Distribution Features

                                After Call Work Access Code:
                                Assist Access Code:
                                Auto-In Access Code: *71
                                Aux Work Access Code: *72
                                Login Access Code: *73
                                Logout Access Code: *74
                                Manual-in Access Code: *75
                                Service Observing Listen Only Access Code: #91
                                Service Observing Listen/Talk Access Code: #92
                                Service Observing No Talk Access Code: #93
                                Add Agent Skill Access Code:
                                Remove Agent Skill Access Code:
                                Remote Logout of Agent Access Code:

```

Figure 10: Feature Access Codes, Page 5

3.1.4. Configure Node Names

Use the **change node-names ip** command to configure the IP address of the clan interface of the Avaya S8720 server.

```

change node-names ip                                         Page 1 of 2
                                IP NODE NAMES

                                Name          IP Address
                                default       0.0.0.0
                                CyberTech Pro 192.168.200.97
                                CTI-server    192.168.200.98
                                clan         192.168.60.6

```

Figure 11: Node-Names IP Form

3.1.5. Configure Telephone Stations

Use the **add station** command to configure all of the telephones shown in **Table 5**.

Parameter	Usage
Type	Enter the type of station that is to be configured.
Security Code	Enter a numeric security code.
Name	Enter a descriptive name for the user of the station.
Buttons	See the following table.

Table 5: Station Parameters

The Avaya IP telephone stations used for testing were each allocated control buttons as shown in the following table:

Station	Button Allocation
S1	3 x call-appr, serv-obsrv
S2	3 x call-appr, serv-obsrv
A	3 x call-appr, auto-cback
B	3 x call-appr, auto-cback, call-pkup
C	3 x call-appr, brdg-appr D
D	3 x call-appr

Table 6: Telephone Station Button Allocation

```

add station 60131                                     Page 1 of 5
                                     STATION
Extension: 60131                                     Lock Messages? n          BCC: 0
  Type: 4621                                         Security Code: 13106      TN: 1
  Port: S00006                                     Coverage Path 1:         COR: 1
  Name: extn 60131                                Coverage Path 2:         COS: 1
                                     Hunt-to Station:
STATION OPTIONS
    Loss Group: 19                                Time of Day Lock Table:
    Speakerphone: 2-way                          Personalized Ringing Pattern: 1
    Display Language: english                     Message Lamp Ext: 300-0136
Survivable GK Node Name:                        Mute Button Enabled? y
    Survivable COR: internal                      Expansion Module? n
    Survivable Trunk Dest? y                     Media Complex Ext:
                                               IP SoftPhone? n
                                               Customizable Labels? y

```

Figure 12: Add Station Form, Page 1

add station 60131

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: **serv-obsrv**

8:

Figure 13: Add Station Form, Page 4

3.1.6. Configure CTI Telephone Stations

Use the **add station** command to configure a station for each of the virtual endpoints shown in **Table 7**.

Parameter	Usage
Type	Enter a station type of “4620”.
Security Code	Enter a numeric security code.
Name	Enter a descriptive name for the station.
Button Assignments	Create a “serv-obsrv” button to be used to initiate a service observe operation from the CTI server.

Table 7: CTI Telephone Station Parameters

add station 61401		Page 1 of 5
STATION		
Extension: 61401	Lock Messages? n	BCC: 0
Type: 4620	Security Code: 10461	TN: 1
Port: S00104	Coverage Path 1:	COR: 1
Name: CTI 61401	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 61401	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Customizable Labels? y	

Figure 14: Add Station Form, Page 1

change station 61401		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: serv-obsrv	8:	

Figure 15: Add Station Form, Page 4

3.1.7. 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 allocated to endpoint B, as shown in **Table 6**.

add pickup-group 1		Page 1 of 4
PICKUP GROUP		
Group Number: 1		
Group Name:		
GROUP MEMBER ASSIGNMENTS		
Extension	Name	
1: 60113		
2: 60116		
3: 60093		
4: 60081		
5:		
6:		
7:		
8:		
9:		
10:		
11:		
12:		
13:		

Figure 16: Add Pickup-Group Form, Page 1

3.1.8. Configure Agents

3.1.8.1 Configure Agent VDN

Use the **add vdn** command to create a Vector Director Number extension which can be used to reference the Operator queue vector.

Parameter	Usage
Name	Use any name that is suitable to identify this item.
Vector Number	Enter the number of the vector to be activated for the Operator queue, as defined in Figure 19 .
Observe on Agent Answer?	Enter “y” to initiate service observe operation after the agent has answered the call.

Table 8: Configuration Operator VDN

add vdn 61001	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 61001	
Name*: AGENT	
Vector Number: 8	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
* Follows VDN Override Rules	

Figure 17: Add VDN Form, Page 1

add vdn 61001	Page 2 of 3
VECTOR DIRECTORY NUMBER	
AUDIX Name:	
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	
* Follows VDN Override Rules	

Figure 178: Add VDN Form, Page 2

3.1.8.2 Configure Agent Login

Use the **add agent-loginID** create agent logins for agents at stations B and C in the table shown in **Table 8**.

Parameter	Usage
Name	Use any name that is suitable to identify the agent.
Password	Specify a string up to 9 digits long to be used as the agent password.
Password (enter again)	Repeat the above parameter.
SN	The Skill Number should be the same as that configured for the Vector Number in Figure .
SL	Enter the Skill Level of the agent, as configured in Figure 18 .

Table 9: Agent LoginID Parameters

```
add agent-loginID 61601                                     Page 1 of 2
                                AGENT LOGINID

Login ID: 61601                                           AAS? n
Name: AGENT A                                           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 Display? n
Password: 10616
Password (enter again): 10616
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

WARNING: Agent must log in again before changes take effect
```

Figure 19: Agent-LoginID Form, Page 1

add agent-loginID 61601				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: 8	8	16:		31:		46:	
2:		17:		32:		47:	
3:		18:		33:		48:	
4:		19:		34:		49:	
5:		20:		35:		50:	
6:		21:		36:		51:	
7:		22:		37:		52:	
8:		23:		38:		53:	
9:		24:		39:		54:	
10:		25:		40:		55:	
11:		26:		41:		56:	
12:		27:		42:		57:	
13:		28:		43:		58:	
14:		29:		44:		59:	
15:		30:		45:		60:	

Figure 180: Agent-LoginID Form, Page 2

3.1.8.3 Configure Agent Hunt Group

Use the **add hunt-group** command to create a hunt group which is used to test the ability of CyberTech Pro to monitor hunt groups. Assign an unused extension to the hunt group.

Parameter	Usage
Group Name	Any alphanumeric string can be used as a Group Name.
Group Extension	Use an unused extension which is compatible with the dial plan.
Group Type	Enter “ucd-mia” to specify that system hunts for the “most idle agent”.
ACD?	Enter “y” to enable automatic call distribution
Queue?	Enter “y” to enable queuing.
Vector?	Enter “y” to enable vectoring.
Skill?	Enter “y” to specify that this is a “skilled” hunt group.

Table 10: Configuration Supervisor Hunt Group

add hunt-group 8	HUNT GROUP	Page 1 of 3
Group Number: 8	ACD? y	
Group Name: AGEMT HG	Queue? y	
Group Extension: 61301	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:		

Figure 21: Configuration Supervisor Hunt Group, Page 1

add hunt-group 8	HUNT GROUP	Page 2 of 3
Skill? y		
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		

Figure 22: Configuration Supervisor Hunt Group, Page 2

3.1.8.4 Configure Agent Queue Vector

Use the **change vector** command to define the steps to be performed for calls which are queued to this vector.

Parameter	Usage
Name	Use any name that is suitable to identify this item.
Vector Number	This must be the same as is configured for the VDN defined in Figure .
Step 01	Wait for 2 seconds on an incoming call.
Step 02	Queue the call to skill 8, as configured for the agents in Figure 18.

Table 11: Agent Vector Parameters

change vector 8		Page 1 of 3	
CALL VECTOR			
Number: 8		Name: AGENT	
Basic? y		Meet-me Conf? n	
EAS? y		Lock? n	
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 8 pri h		03	
		04	
		05	

Figure 193: Agent Vector Form

3.1.9. Configure Interface to Avaya AES

The Avaya Application Services server TSAPI interface provides CyberTech Pro with a means of communicating with Avaya Communication Manager to perform telephony operations. Avaya 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 1

                                IP INTERFACES

                                Type: C-LAN
                                Slot: 01A02
                                Code/Suffix: TN799 D
                                Node Name: clan
                                IP Address: 192.168.60.6
                                Subnet Mask: 255.255.255.0
                                Gateway Address: 192.168.60.254
                                Enable Ethernet Port? y
                                Network Region: 1
                                VLAN: n
                                Link:
                                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
```

Figure 24: Add Ip-Interface Form

Use the **change ip-services** command to set the parameters for **AESVCS** service as shown below for the C-LAN which was defined above to serve as the interface to the Avaya AES server.

```
change ip-services                                         Page 1 of 3

                                IP SERVICES
Service   Enabled   Local   Local   Remote   Remote
Type      Type      Node    Port    Node     Port
AESVCS    y         clan    8765
```

Figure 25: Change Ip-Services Form, page 1

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 was assigned to the switch connection, as shown in **Section 3.2.1** of this document.

change ip-services					Page 3 of 3
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	aes-server1	xxxxxxx	y	idle	

Figure 2620: Change Ip-Services Form, page 2

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 3.2.2** 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 4		Page 1 of 3
CTI LINK		
CTI Link: 4		
Extension: 699-9996		
Type: ADJ-IP		
Name: AES-devcon223-tsapi		COR: 1

Figure 2721: Add Cti-Link Form

Use the **add data-module <x>** command, where <x> is an unassigned extension, to allocate an extension to be used as the data interface for the clan module. The value used as “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 6000000		Page 1 of 1
DATA MODULE		
Data Extension: 6000000	Name: clan	
Type: ethernet		
Port: 01A0217		
Link: 1		
Network uses 1's for Broadcast Addresses? Y		

Figure 28: Add Data-Module Form

3.2. Configure Avaya AES

The information provided in this section describes the configuration of Avaya Application Enablement Services for this solution.

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

`https://<Avaya AES server address>:8443/MVAP/`

Once the login screen appears, enter either the OAM Admin login ID/password to perform administrative activities on the AE Server or the User Management ID/password to manage AE Services users and AE Services user-related resources. AE Server administrative activities have been partitioned into two administrative domains to enable each to be administered by separate administrators, should business requirements so dictate. To change from one of these domains to the other, first log out and then log in again with the user name/password which corresponds to the domain to be accessed (do not forget the “s” on “https”, or the login will not succeed).

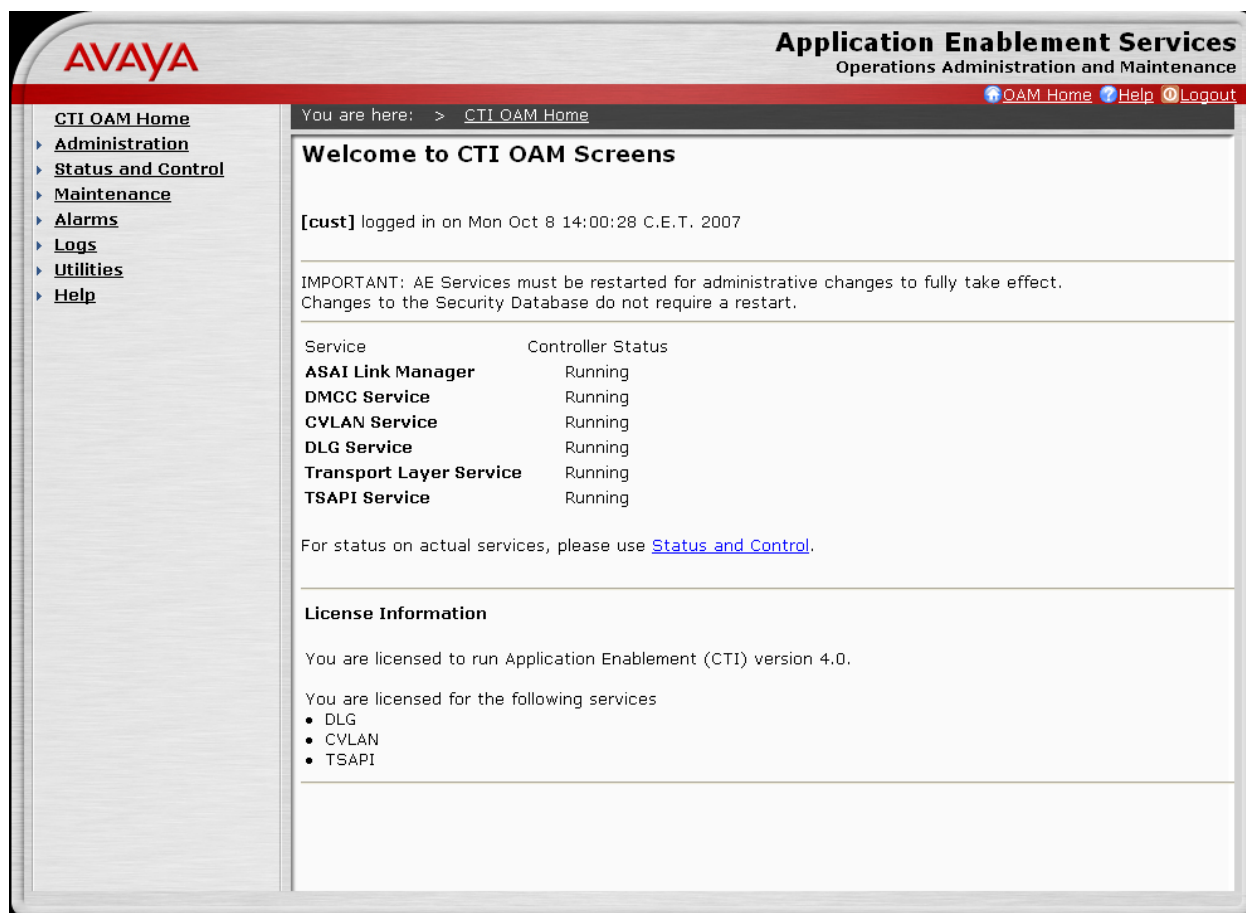


Figure 29: AES OAM Introductory Screen

After logging in with the OAM Admin user ID/password, select “CTI OAM Home” which displays the following screen. Verify Avaya AES server installation has a TSAPI service license. If this is not the case, please contact an Avaya representative regarding licensing.

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

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

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

Welcome to CTI OAM Screens

[cust] logged in on Mon Oct 8 14:00:28 C.E.T. 2007

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Controller Status
ASAI Link Manager	Running
DMCC Service	Running
CVLAN Service	Running
DLG Service	Running
Transport Layer Service	Running
TSAPI Service	Running

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

License Information

You are licensed to run Application Enablement (CTI) version 4.0.

You are licensed for the following services

- DLG
- CVLAN
- TSAPI

Figure 30: AES OAM Home Screen

3.2.1. 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.

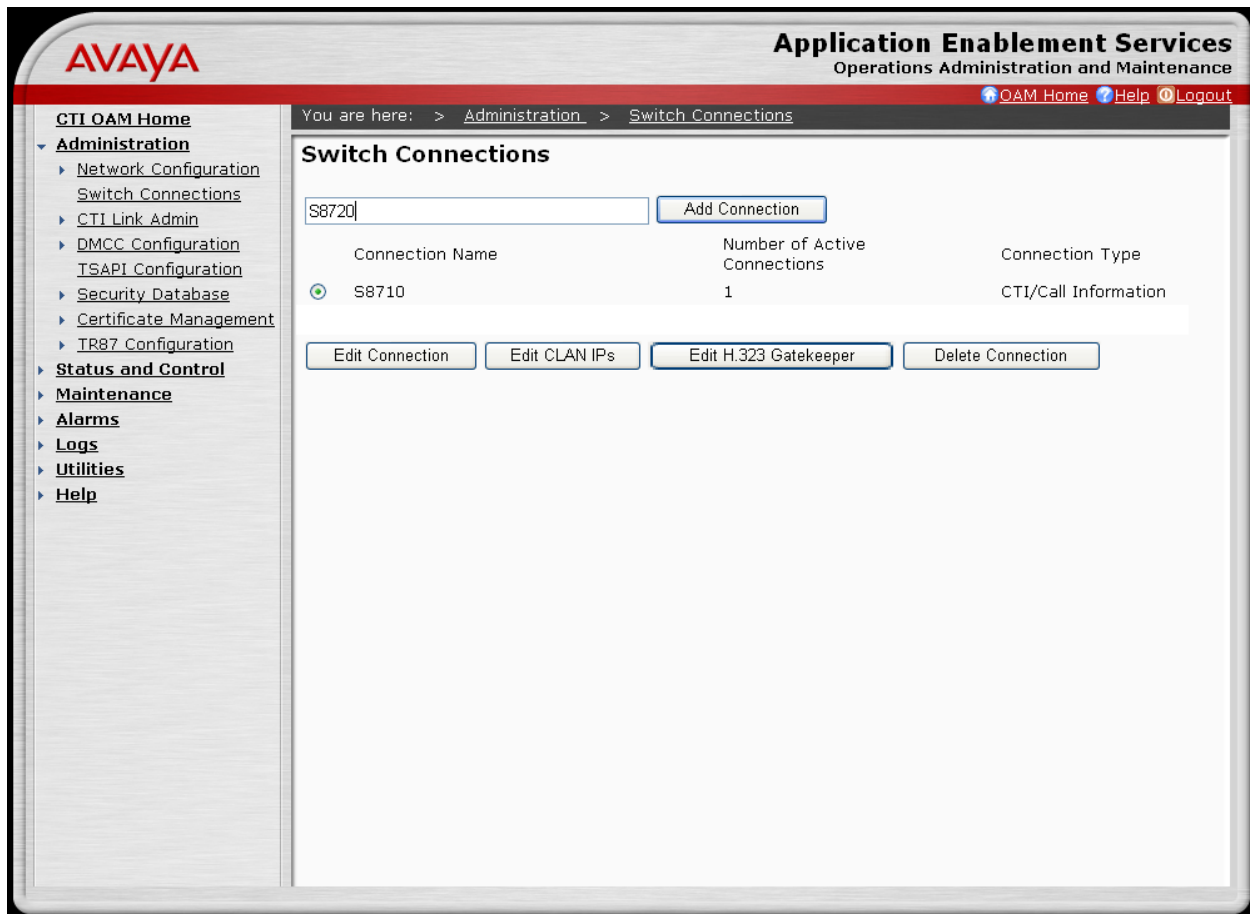


Figure 31: AES Switch Connections Screen

The AES Set Switch Connection Password screen is displayed. Enter the screen fields as described in the following table, and click the “Apply” button.

Parameter	Usage
Switch Connection Type	Specify a type of CTI/Call Information.
Switch Password	The Switch Password must be the same as was entered into the Avaya Communication Manager AE Services Administration form via the “change ip-services” command, described in Section 3.1.9 . Passwords must consist of 12 to 16 alphanumeric characters.
SSL	SSL (Secure Socket Layer) is enabled by default. Keep the default setting unless you are adding a Switch Connection for a DEFINITY Server CSI.

Table 12: Configuration of Switch Password

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

Set Password - S8720

Please note the following:
 * A password is not required for a H323 Gatekeeper Connection.
 * Changing the password affects only new connections, not open connections.

Switch Connection Type: CTI/Call Information

Switch Password: [Masked]

Confirm Switch Password: [Masked]

SSL: ☒

[Apply] [Cancel]

Figure 32: AES Set Switch Connection Password Screen

From the **Administration**→**Switch Connections** screen, click the “Edit CLAN IPs” button to display the screen shown below. Enter the IP address of the CLAN with which Avaya AES is to use for communication with Avaya Communication Manager as defined in **Section 3.1.9**. Click the “Add Name or IP” button.

The screenshot displays the Avaya AES web interface. The top header includes the Avaya logo and the text 'Application Enablement Services Operations Administration and Maintenance'. A breadcrumb trail shows 'You are here: > Administration > Switch Connections'. The left sidebar contains a tree view with categories like 'Administration', 'Network Configuration', 'CTI Link Admin', 'DMCC Configuration', 'TSAPI Configuration', 'Security Database', 'Certificate Management', 'TR87 Configuration', 'Status and Control', 'Maintenance', 'Alarms', 'Logs', 'Utilities', and 'Help'. The main content area is titled 'Edit CLAN IPs - S8720'. It features a table with two columns: 'Name or IP Address' and 'Status'. A text input field in the 'Name or IP Address' column contains the IP address '192.168.60.6'. To the right of this field is a button labeled 'Add Name or IP'. Below the input field is a button labeled 'Delete IP'.

Figure 33: AES Edit Switch Connection CLAN IP Address Screen

3.2.2. Create TSAPI Link

In the left pane of the screen, navigate to **Administration**→**CTI Link Admin**→**TSAPI Links**. The following screen is displayed. Click the “Add Link” button.

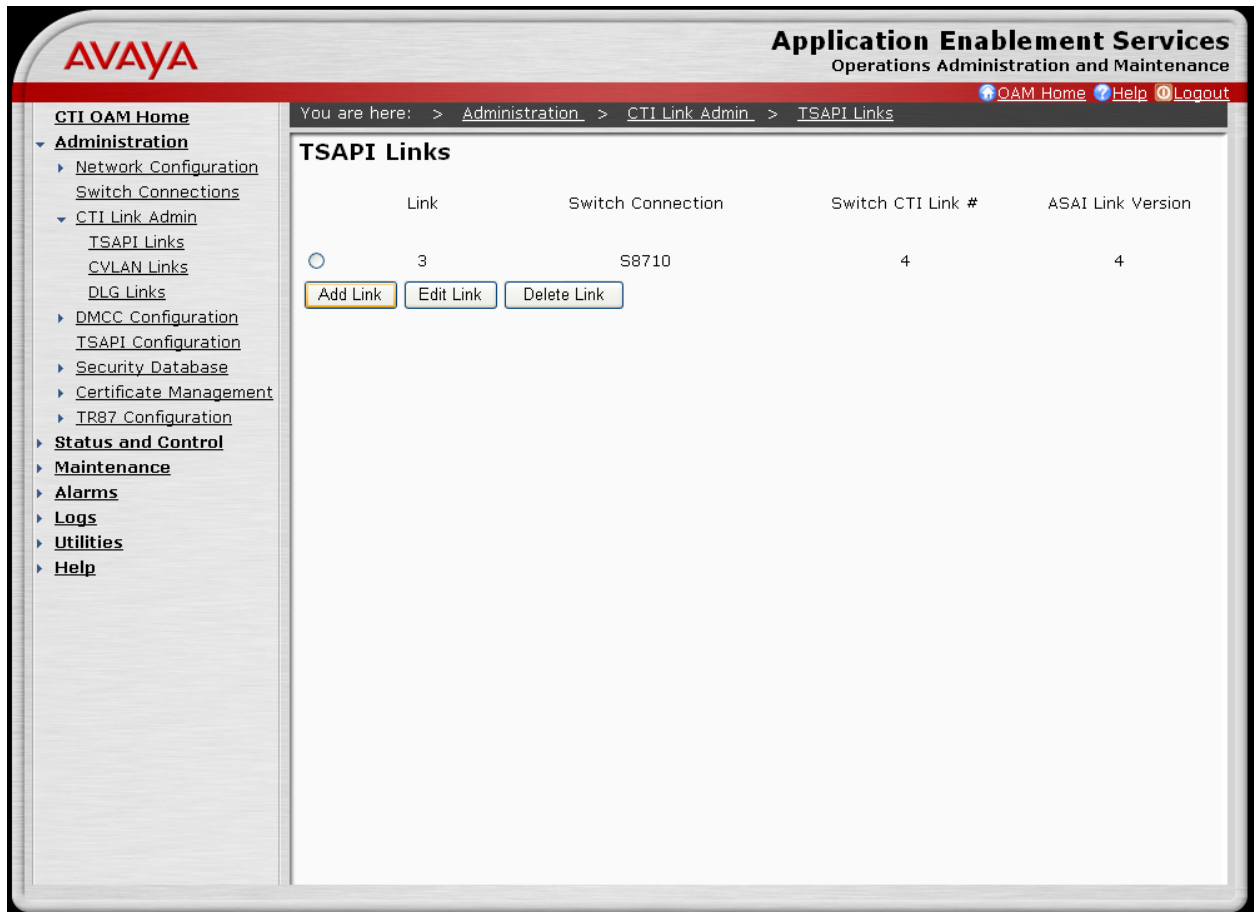


Figure 34: AES TSAPI Links Screen

Fill in the parameters for the link to be added. The “Link” parameter must be a value between 1 and 16 which is not assigned to another link. The “Switch Connection” parameter should be the name of the Avaya Media Server which is to be controlled by this link. The value for the TSAPI “Switch CTI Link Number” must be a value between 1 and 64, and must be the same as was used in the Avaya Communication Manager “add cti-link” configuration command in **Section 3.1.9**. Click the “Apply Changes” button.

The screenshot displays the AVAYA Application Enablement Services (AES) interface. The top header features the AVAYA logo and the text "Application Enablement Services Operations Administration and Maintenance". A navigation bar includes links for "OAM Home", "Help", and "Logout". The left sidebar contains a tree view with categories: "Administration" (sub-items: Network Configuration, Switch Connections), "CTI Link Admin" (sub-items: TSAPI Links, CVLAN Links, DLG Links), "DMCC Configuration", "TSAPI Configuration", "Security Database", "Certificate Management", "TR87 Configuration", "Status and Control", "Maintenance", "Alarms", "Logs", "Utilities", and "Help". The main content area is titled "Add / Edit TSAPI Links" and shows the following configuration fields:

- Link: 1
- Switch Connection: S8720
- Switch CTI Link Number: 4

At the bottom of the form are two buttons: "Apply Changes" and "Cancel Changes".

Figure 35: AES Add/Edit TSAPI Links Screen

3.2.3. Create Avaya AES User

Log out and log in again with the user administration ID/password, which will cause the “OAM Welcome” screen to be displayed just as after the previous login.

Navigate to “User Management→Add User”.

The “CT User” field for this user must be set to “Yes”. In this case, the Avaya AES user is CyberTech Pro, which uses Avaya AES to monitor stations and initiate switching operations. The values chosen for the “User Id” and “User Password” fields must be the same as those defined in **Figure** . Upon completion, click “Apply” button.

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

You are here: > User Management > Add User

Add User

Fields marked with * can not be empty.

* User Id: avaya

* Common Name: avaya

* Surname: avaya

* User Password: *****

* Confirm Password: *****

Admin Note:

Avaya Role: None

Business Category:

Car License:

CM Home:

Css Home:

CT User: Yes

Department Number:

Display Name:

Employee Number:

Employee Type:

Enterprise Handle:

Given Name:

Home Phone:

Home Postal Address:

Initials:

Labeled URI:

Mail:

MM Home:

Mobile:

Organization:

Pager:

Preferred Language: English

Room Number:

Telephone Number:

Apply Cancel

Figure 22: AES Add User Screen

3.3. Configure CyberTech CTI Server

The Cybrtech Pro CTI server is largely preconfigured for the customer by Cybertec prior to delivery. This section shows those configuration steps which need be made after delivery.

3.3.1. Install TSAPI Client on CTI Server

The Avaya TSAPI Client must be installed on the CTI Server, as shown by the following steps. First, execute the installation program and click “Next”.

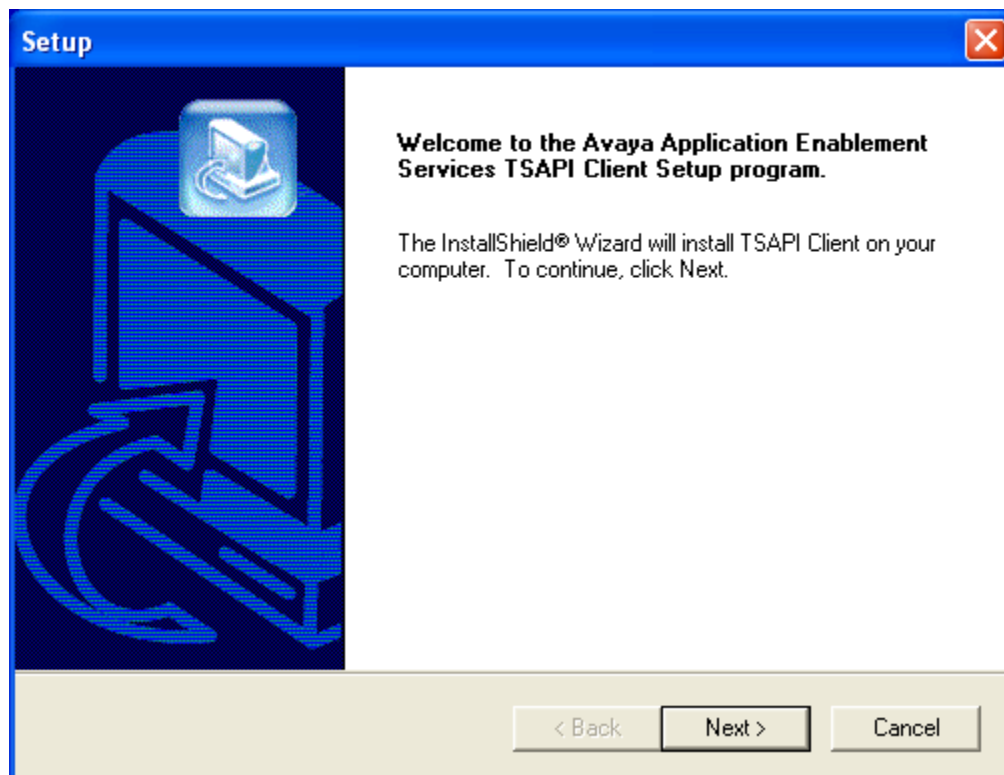


Figure 37: Avaya TSAPI Client Installation Introductory Screen

Retain the default installation folder and click “Next”.

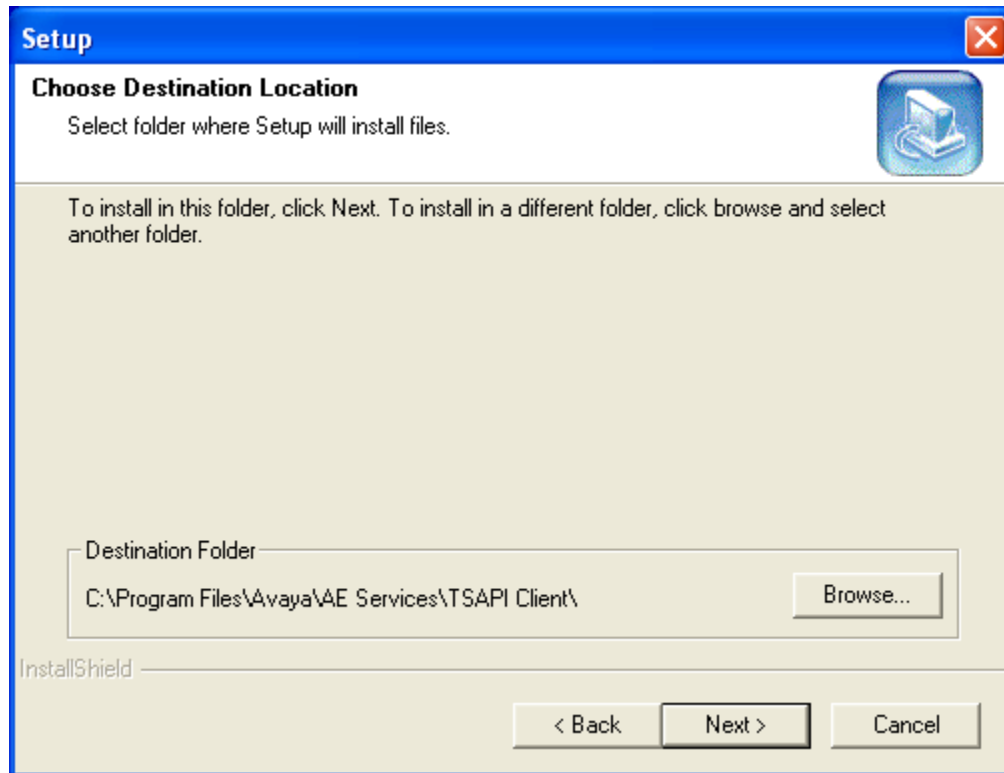
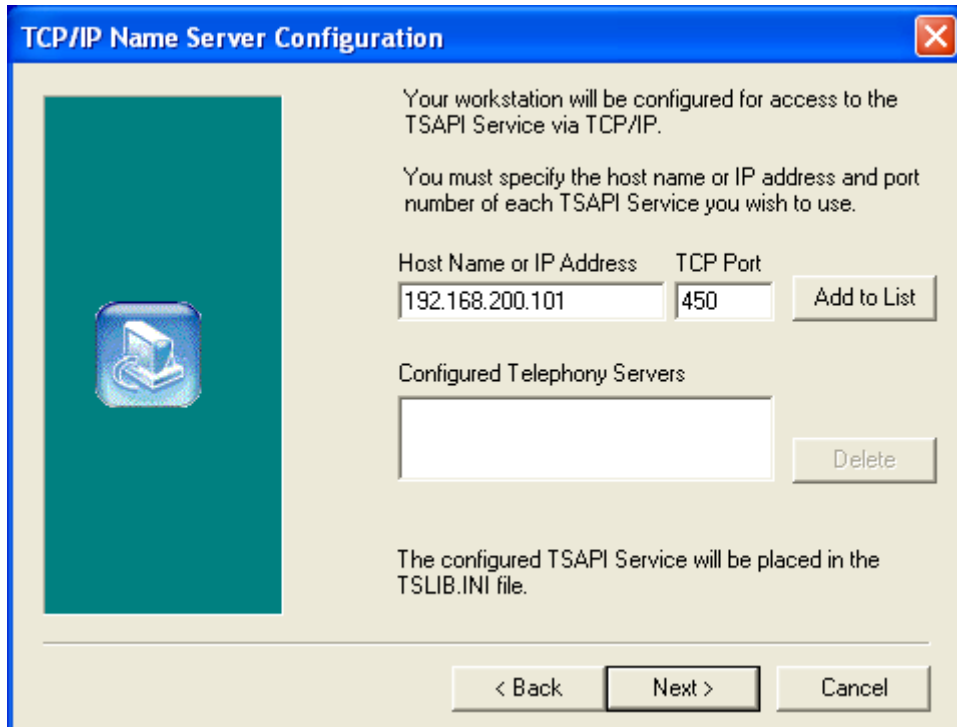


Figure 38: Avaya TSAPI Client Installation Destination Selection Screen

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 image shows a Windows-style dialog box titled "TCP/IP Name Server Configuration". On the left is a teal vertical bar with a small icon of a computer and a telephone. The main area has a light beige background. It contains 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 is a table with two columns: "Host Name or IP Address" and "TCP Port". The first row has the values "192.168.200.101" and "450" respectively. To the right of the table is an "Add to List" button. Below the table 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".

Host Name or IP Address	TCP Port
192.168.200.101	450

Configured Telephony Servers

< Back Next > Cancel

Figure 39: Avaya TSAPI Client Address Selection Screen

Click “Finish” after the installation completes.

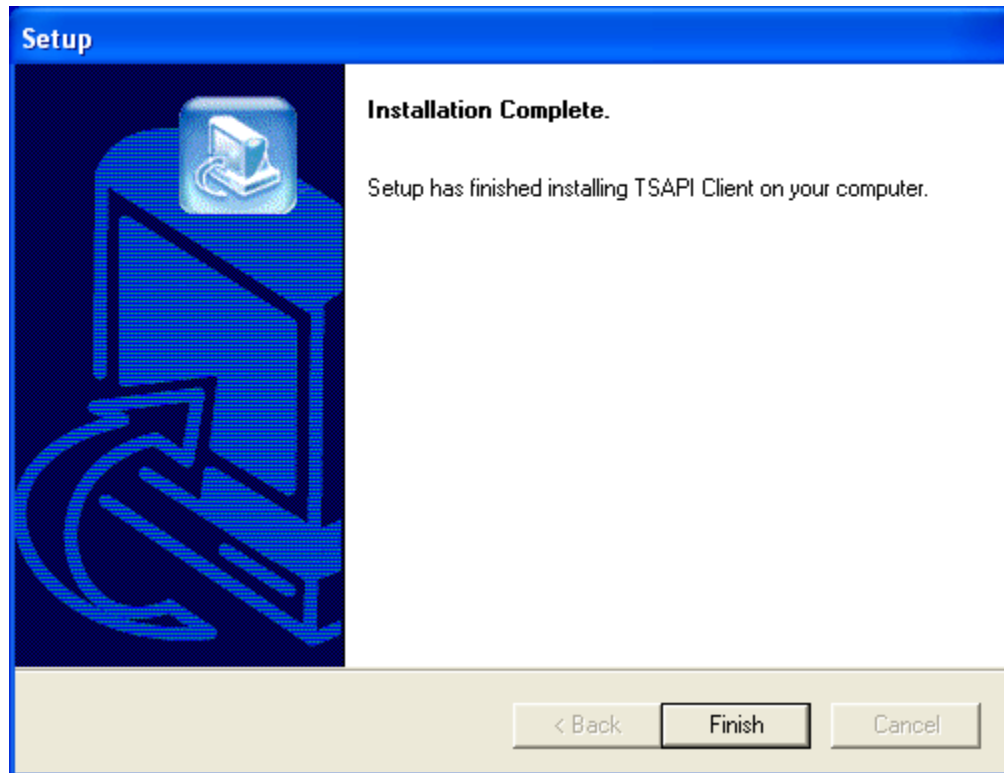


Figure 230: Avaya TSAPI Client Installation Completion Screen

3.3.2. Install the SSL Certificate for the AES Connection

The CyberTech CTI server requires a certificate to communicate with the Avaya AES Server. Double click on the 'avaya' certificate contained within the directory containing the distribution files.

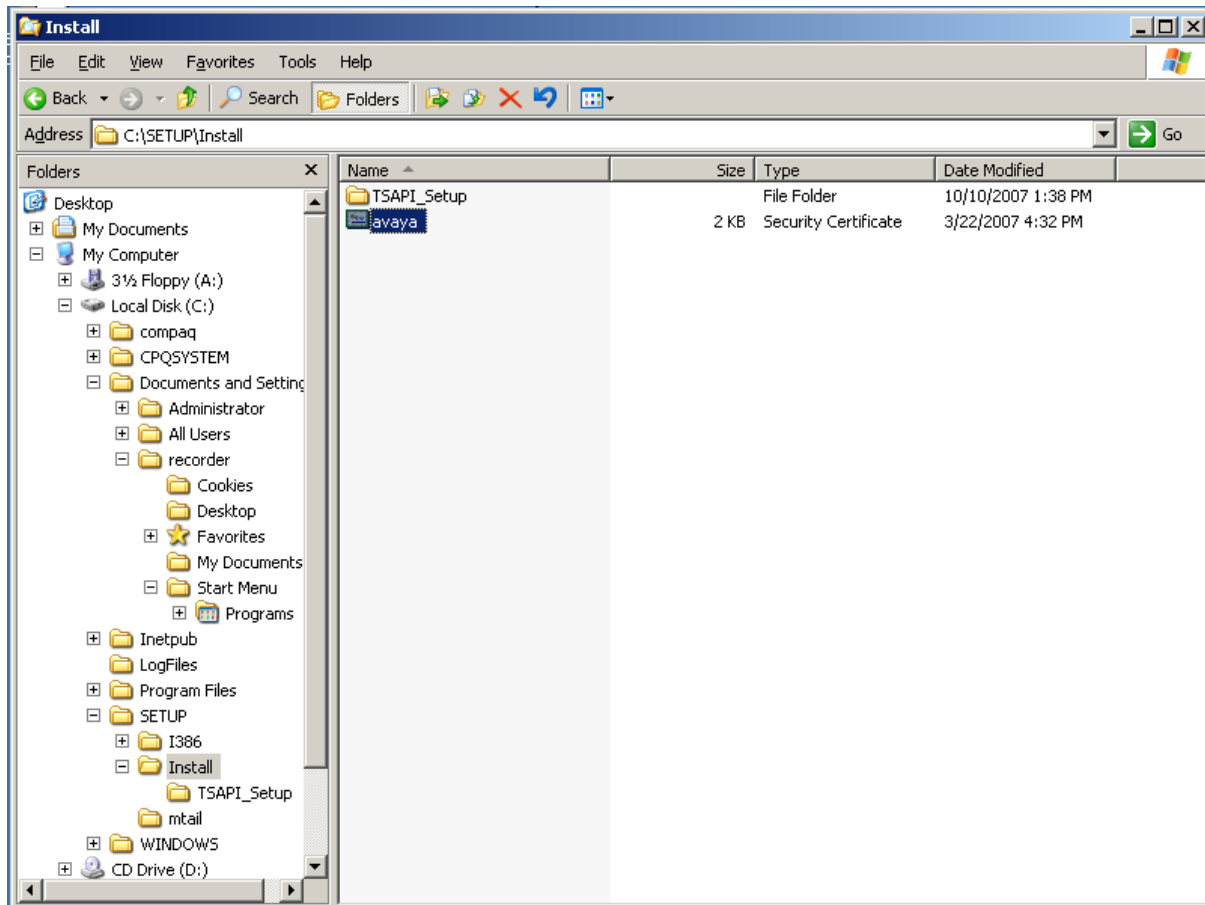


Figure 41: Avaya AES Certificate Directory

Click “Install Certificate”.

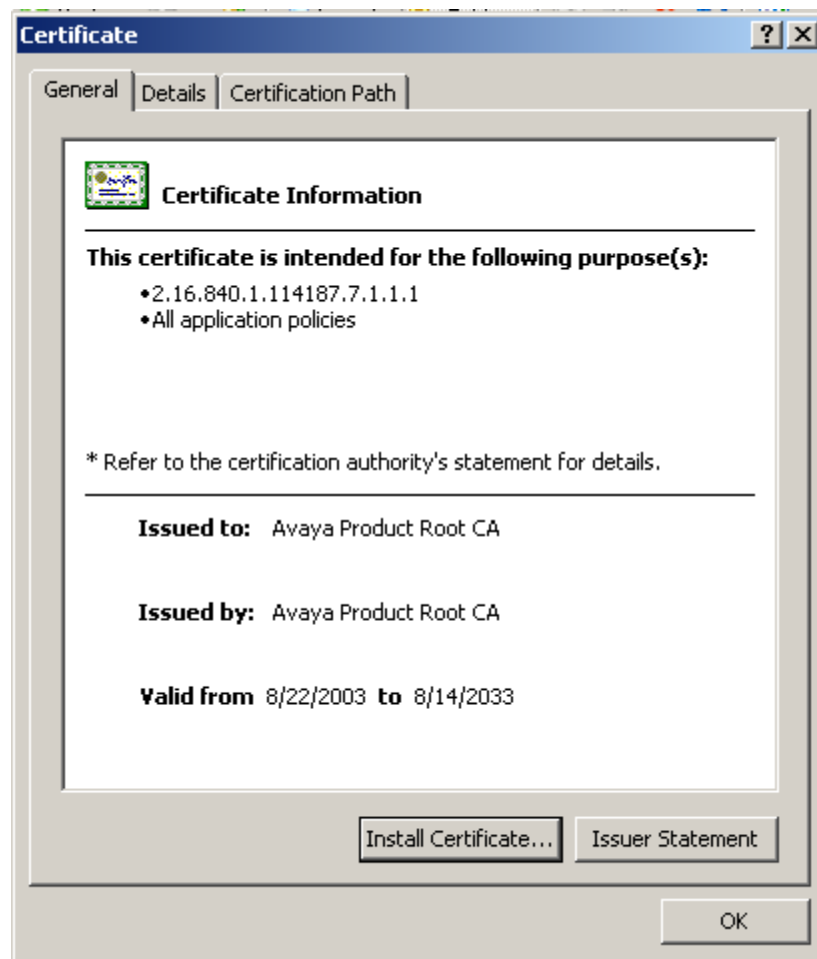


Figure 242: Avaya AES Certificate Installation Introduction Screen

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



Figure 253: Avaya AES Certificate Import Wizard Screen

Click “Browse” to select the certificate destination.

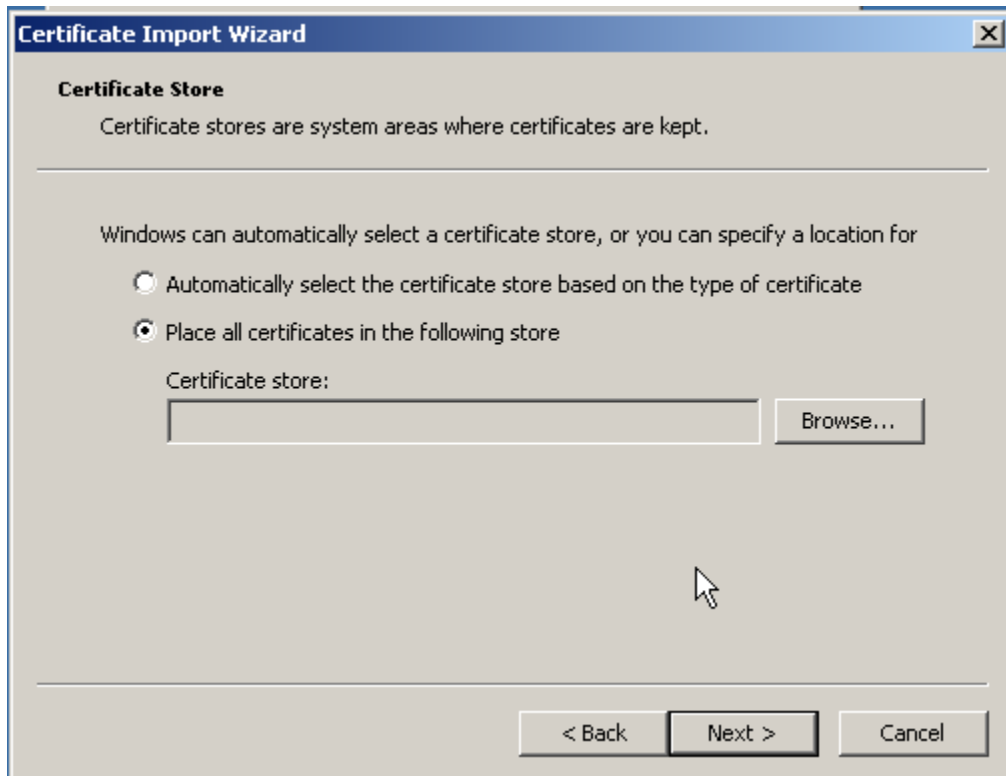


Figure 264: Avaya AES Certificate Destination Selection Screen

Select the “Local Computer”, as shown.



Figure 275: Avaya AES Certificate Path Selection Screen

Click “Next” after confirming the destination.

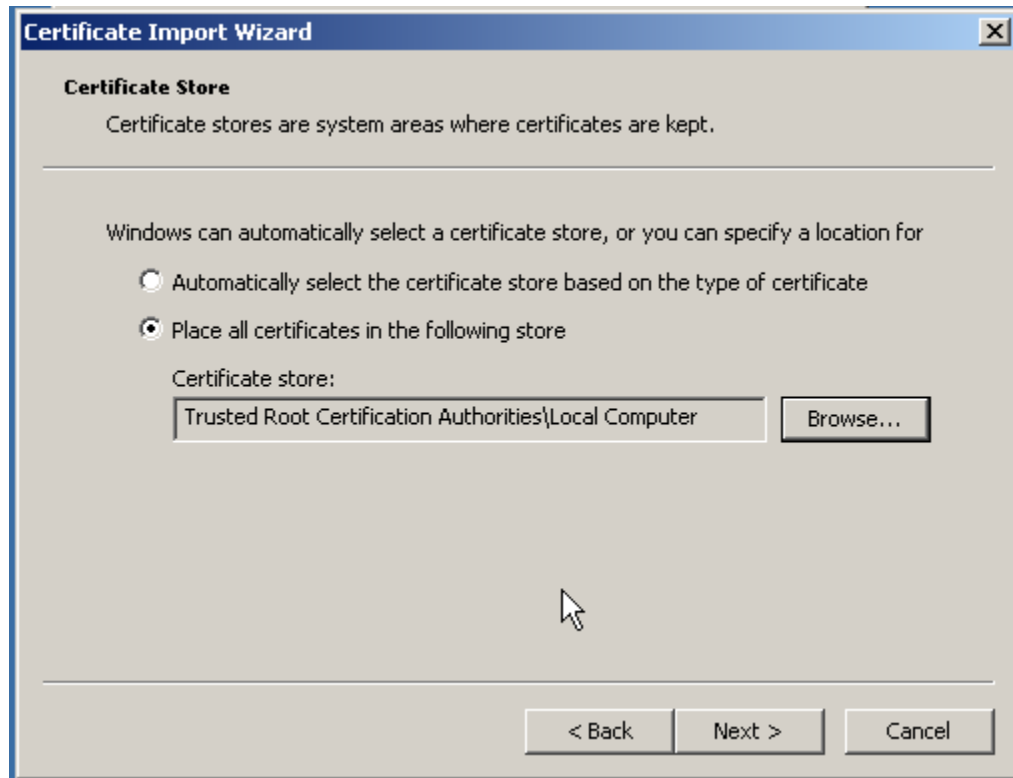


Figure 286: Avaya AES Certificate Destination Confirmation Screen

Click “Finish” after the certificate installation is complete.



Figure 47: Avaya AES Certificate Installation Completion Screen

3.4. Configure the CyberTech Pro Voice Recorder

Enter the URL of the CyberTech Voice Recorder in the web browser, and enter the login ID and password and click on the “>” button:

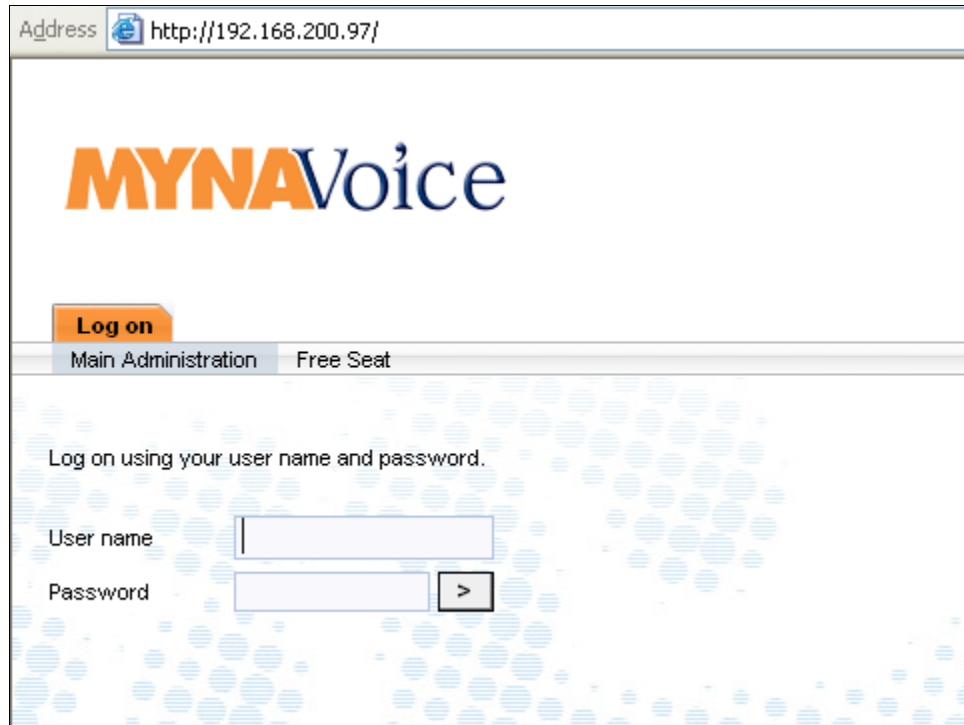


Figure 48: Cybertec Pro Logon Screen

After Logon, select the “cti integration” tab which initially displays the “devices” secondary tab. Click on the Pencil symbol in the upper right portion of the screen.

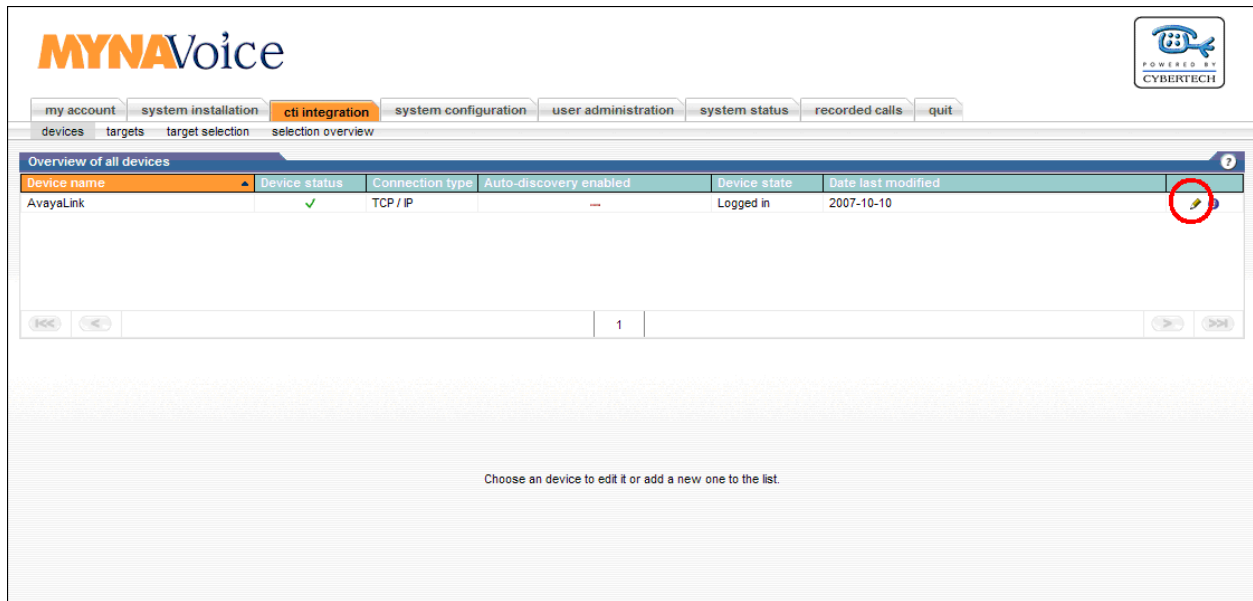


Figure 49: Cybertec Pro “Cti Integration / Devices” Screen

In the “General device settings” form, select “Active” from the “Device Status” drop-down box. Configure the “Device parameters” as follows:

```
SwitchName=S8720
ObserveCode=#93
TSAPIServerName=AVAYA#S8720#CSTA#AES-SERVER1
ConnectionUseSSL=Yes
ConnectionProtocol=4.0
```

Figure 50: Cybertec Pro Device Settings Values

Configure the “Connections settings” parameters as shown in the following table:

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 Figure 22 .
Connection password	Enter the “User Password” which was defined in Figure 22 .

Table 13: Cybertec Pro Connection Settings

Click “Save changes” upon completion.

Figure 51: Cybertec Pro “Cti Integration / Devices” Settings Screen

Select the “Targets” secondary tab and click the “+” symbol for each target to be added.

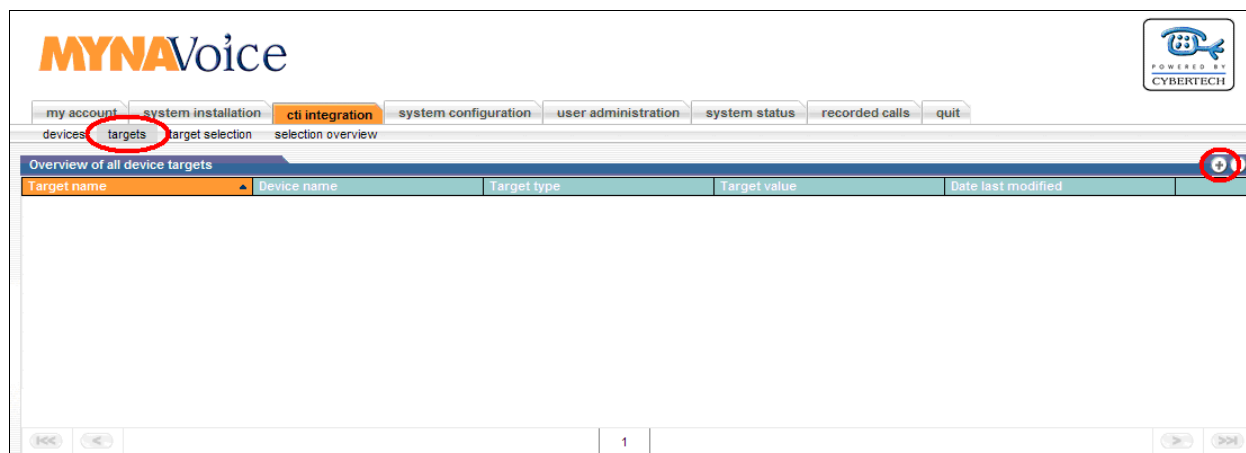
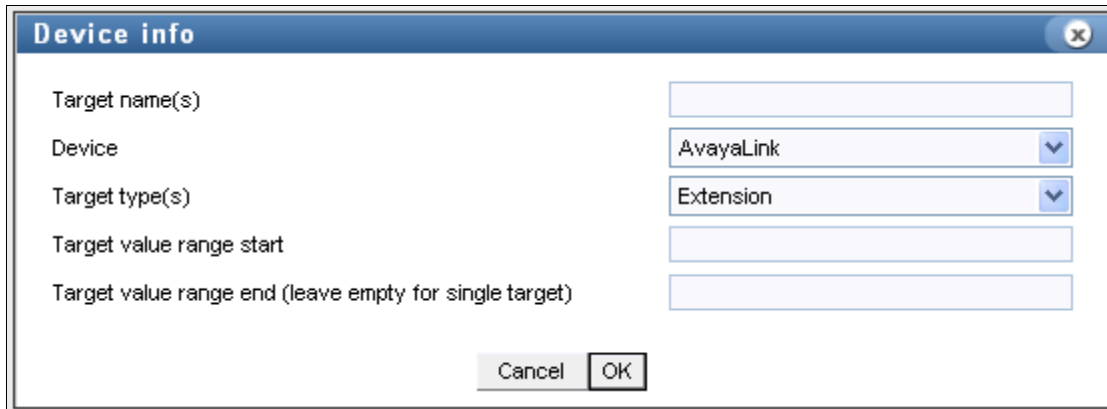


Figure 52: Cybertec Pro “Cti Integration / Targets” Screen

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

Name	Device	Type	Range Start
10461	AvayaLink	Active Extension	61401
20416	AvayaLink	Active Extension	61402
30416	AvayaLink	Active Extension	61403
40416	AvayaLink	Active Extension	61404
50416	AvayaLink	Active Extension	61405
Agent1	AvayaLink	Recorded Extension	60131
Agent2	AvayaLink	Recorded Extension	60123
Huntgroup	AvayaLink	Extension	60301
Target_B	AvayaLink	Recorded Extension	60116
Target_C	AvayaLink	Recorded Extension	60093

Table 14: Cybertec Pro Target Device Info Parameters



Device info

Target name(s)

Device

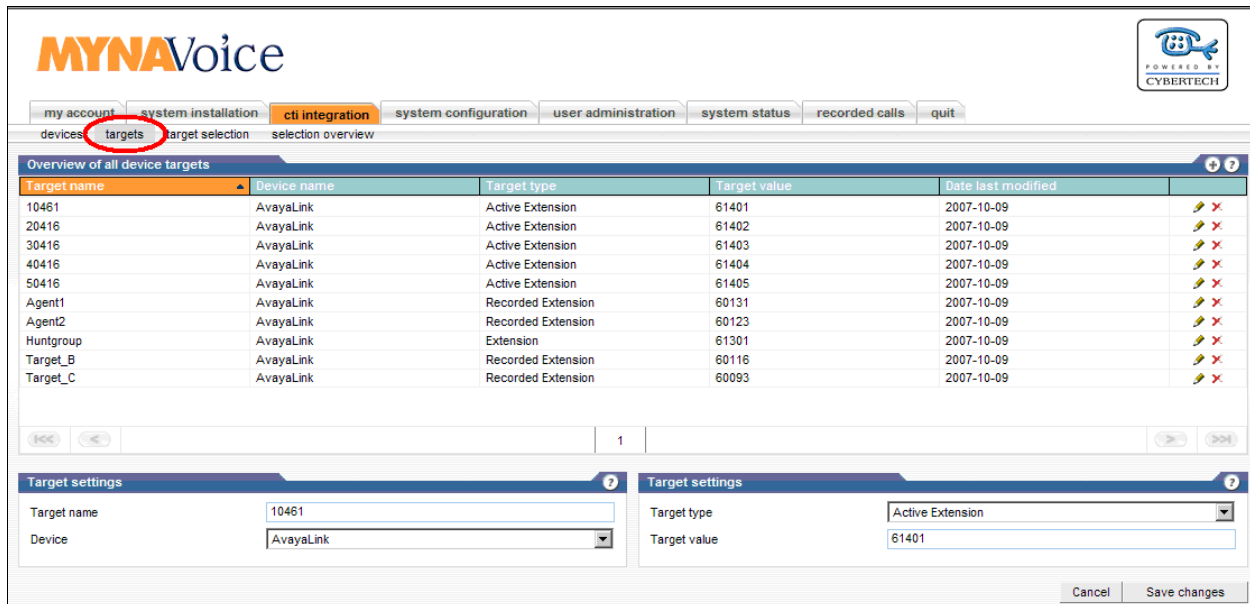
Target type(s)


Target value range start

Target value range end (leave empty for single target)

Figure 53: Cybertec Pro “Cti Integration / Targets” Device Info Entry Control

After the targets have been entered, the “targets” secondary tab should contain the following information:



MYNAVoice 

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

devices | **targets** | target selection | selection overview

Overview of all device targets

Target name	Device name	Target type	Target value	Date last modified	
10461	AvayaLink	Active Extension	61401	2007-10-09	
20416	AvayaLink	Active Extension	61402	2007-10-09	
30416	AvayaLink	Active Extension	61403	2007-10-09	
40416	AvayaLink	Active Extension	61404	2007-10-09	
50416	AvayaLink	Active Extension	61405	2007-10-09	
Agent1	AvayaLink	Recorded Extension	60131	2007-10-09	
Agent2	AvayaLink	Recorded Extension	60123	2007-10-09	
Huntgroup	AvayaLink	Extension	61301	2007-10-09	
Target_B	AvayaLink	Recorded Extension	60116	2007-10-09	
Target_C	AvayaLink	Recorded Extension	60093	2007-10-09	

Target settings

Target name

Device

Target type

Target value

Figure 54: Cybertec Pro “Cti Integration / Targets” Entered Screen

Select the “target selection” secondary tab and elect the pencil symbol the AvayaLink to display the list of targets which can be selected.

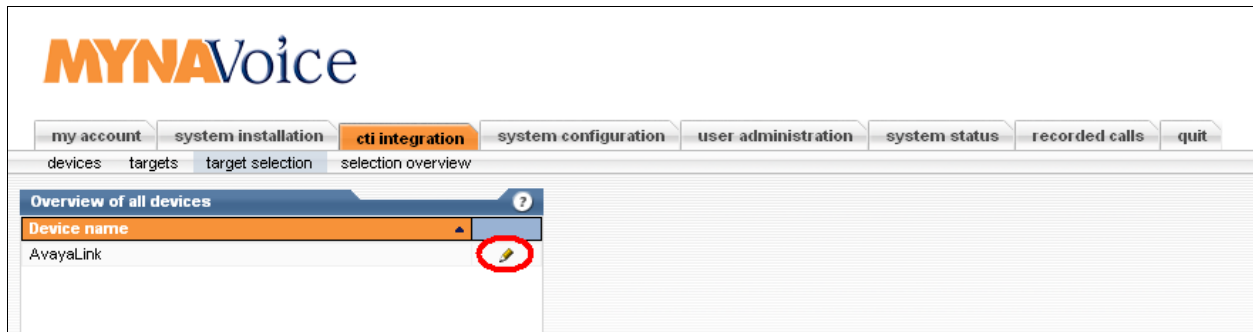


Figure 55: Cybertec Pro “Cti Integration / Target Selection” Screen

Select the “Target type Extension” entry from the list of targets.

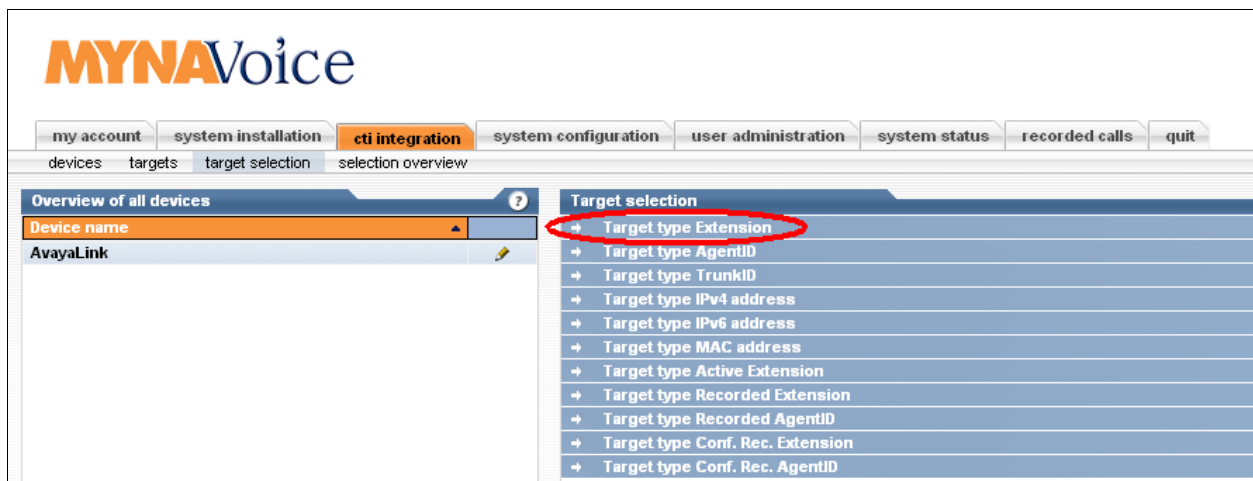


Figure 56: Cybertec Pro Extension Selection Screen

Enter the Agent Hunt Group number as target and click “Save changes”.

The screenshot displays the MYNAVoice web interface. At the top, the MYNAVoice logo is on the left, and the 'POWERED BY CYBERTECH' logo is on the right. Below the logos is a navigation bar with tabs: 'my account', 'system installation', 'cti integration' (which is highlighted), 'system configuration', 'user administration', and 'system status'. Under the 'cti integration' tab, there are sub-tabs: 'devices', 'targets', and 'target selection' (which is highlighted). The main content area is divided into two panels. The left panel, titled 'Overview of all devices', shows a table with the header 'Device name' and one entry, 'AvayaLink'. The right panel, titled 'Target selection', contains a form with the following fields: 'Description' (empty), 'Targets' (containing '61301'), and a list of target types with expandable arrows: 'Target type AgentID', 'Target type TrunkID', 'Target type IPv4 address', 'Target type IPv6 address', 'Target type MAC address', 'Target type Active Extension', 'Target type Recorded Extension', 'Target type Recorded AgentID', 'Target type Conf. Rec. Extension', and 'Target type Conf. Rec. AgentID'. At the bottom right of the 'Target selection' panel, there are two buttons: 'Cancel' and 'Save changes' (which is highlighted with a red circle).

Figure 57: Cybertec Pro Hunt Group Selection Screen

Select the “Target type Active Extension” entry from the list of targets, and enter the numbers of the extensions used as virtual extensions for service observe by Cyberlink Pro, as configured in **Figure 60**. Click “Save changes” when completion.

The screenshot shows the MYNAVoice web interface. The top navigation bar includes tabs for 'my account', 'system installation', 'cti integration' (selected), 'system configuration', 'user administration', and 'system status'. Below this, a sub-navigation bar shows 'devices', 'targets', 'target selection' (selected), and 'selection overview'. The main content area is divided into two panels. The left panel, titled 'Overview of all devices', shows a table with one entry: 'AvayaLink'. The right panel, titled 'Target selection', contains a list of target types: 'Target type Extension', 'Target type AgentID', 'Target type TrunkID', 'Target type IPv4 address', 'Target type IPv6 address', 'Target type MAC address', 'Target type Active Extension' (selected), 'Target type Recorded Extension', 'Target type Recorded AgentID', 'Target type Conf. Rec. Extension', and 'Target type Conf. Rec. AgentID'. Below the list, there are input fields for 'Description' and 'Targets'. The 'Targets' field contains the text '61401,61402'. At the bottom right of the 'Target selection' panel, there are two buttons: 'Cancel' and 'Save changes'.

Figure 58: Cybertec Pro Active Extension Selection Screen

Select the “Target type Recorded Extension” entry from the list of targets, and enter the numbers of the extensions for endpoints B and C. Click “Save changes” upon completion.

MYNAVoice POWERED BY CYBERTECH

my account | system installation | **cti integration** | system configuration | user administration | system status

devices | targets | target selection | selection overview

Overview of all devices

Device name: AvayaLink

Target selection

- Target type Extension
- Target type AgentID
- Target type TrunkID
- Target type IPv4 address
- Target type IPv6 address
- Target type MAC address
- Target type Active Extension
- Target type Recorded Extension**
- Target type Recorded AgentID
- Target type Conf. Rec. Extension
- Target type Conf. Rec. AgentID

Description:

Targets:

Cancel | **Save changes**

Figure 59: Cybertec Pro Recorded Extension Selection Screen

Select the “selection overview” in the secondary tab, and verify that the “Target state” of each of the targets is “Selected”.

MYNAVoice POWERED BY CYBERTECH

my account | system installation | **cti integration** | system configuration | user administration | system status

devices | targets | target selection | **selection overview**

Filter selection entries

Devices: [All] Target types: [All] Search

Overview of selection entries

Target name	Device name	Target ty...	Target value	Target state	Date last ...
Target_C	AvayaLink	Recorded	60093	Selected	2007-10-09
Target_B	AvayaLink	Recorded ...	60116	Selected	2007-10-09
Huntgroup	AvayaLink	Extension	61301	Selected	2007-10-09
20416	AvayaLink	Active Ext...	61402	Selected	2007-10-09
10461	AvayaLink	Active Ext...	61401	Selected	2007-10-09

Figure 60: Cybertec Pro “Cti Integration / Selection Overview” Screen

Additional information about 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 61401.

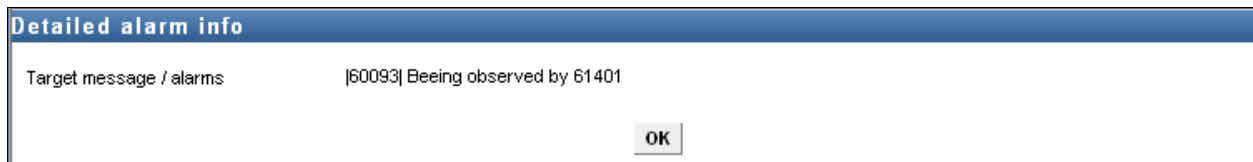


Figure 29: Cybertec Pro “Cti Integration / Detail Alarm Info” Screen

4. Interoperability Compliance Testing

The interoperability compliance tests included feature and serviceability testing.

The feature testing focused on testing scenarios that involve interaction between the CyberTech Pro server and Avaya products, including 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

4.1. General Test Approach

The test method employed can be described as follows:

- Confirmation 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 the voice content of each of the files is correct.
- Confirmation that the calling and called party for each of the files is correct.
- Confirmation that the start and stop times of each of the files is correct.

All testing was performed manually. The tests were all functional in nature, and no performance testing was done.

4.2. Test Results

The following was observed during testing:

- There was a problem when recording calls which were answered from a bridged appearance: the voice recording file contains silence.

All other test results were as expected.

5. Verification Steps

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

- Verify that Avaya Communication Manager and the CyberTech Pro server can ping each other. The “ping” command can be executed from the CyberTech Pro server by executing the “cmd” component via the run facility from the Windows “Start” control and entering “ping” followed by the IP address to which the ping message is to be sent. The “ping” command can be executed from Avaya Communication Manager via an SSH login session.
- Make calls local and external to and from monitored stations and verify that the correct call records are produced.
- Perform hold, transfer, blind transfer, and conferencing operations, and verify that correct call records are produced.
- Make calls to and from bridged appearances and verify that correct call records are produced.
- Make calls from external telephones to a VDN and verify that correct call records are produced.
- Make calls to agents and verify that correct call records are produced.

6. Support

Technical support from CyberTech can be obtained through the following:

CyberTech Support Desk
Email: supportdesk@CyberTech.nl
Telephone: +31 72 567 31 79

7. Conclusion

These Application Notes describe the conformance testing of the CyberTech Pro with Avaya Communication Manager and Avaya Application Enablement Services. The test configuration is described in detail, including the configuration of each of the components used in the test.

8. Additional References

- [1] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3, Document Number 03-300509
- [2] *Feature Description and Implementation for Avaya Communication Manager*, February 2007, Issue 5, Document Number 555-245-205
- [3] *CyberTech Pro 4.0 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.