

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Enterasys Wireless Access Point 3000 (RBT3K-AG) to Support Avaya IP Office, Avaya IP Wireless Telephones and Avaya Phone Manager Pro - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Enterasys Wireless Access Point 3000 (RBT3K-AG) to support Avaya IP Office, Avaya IP Wireless Telephones and Avaya Phone Manager Pro.

1. Introduction

These Application Notes describe the steps necessary to configure Enterasys Wireless Access Point 3000 (RBT3K-AG) to support Avaya IP Office, Avaya Wireless Telephones and Avaya Phone Manager Pro. The network infrastructure used for verification is shown in **Figure 1**. These Application Notes cover the following areas:

- System IP and Wireless 802.11a/b/g radio configurations.
- Wired Equivalent Privacy (WEP) encryption
- 802.1x RADIUS authentication with WPA encryption.

These Application Notes do not cover the configuration for Avaya IP Wireless Telephones, Avaya Phone Manager Pro, Odyssey RADIUS Server and Clients. For detailed configuration on these devices, refer to the Application Notes listed in Section 7.

In the release tested, the Enterasys AP 3000 RBT 3K-AG did not support Spectralink Voice Priority (SVP), which is required for ensuring over the air Quality of Service (QoS).



Figure 1: Network Configuration

Device	VLAN	IP Address/Mask	Gateway
Avaya IP406 Office	VLAN 1	50.1.1.10 /24	50.1.1.1
Avaya Voice Priority Processor	VLAN 1	50.1.1.9/24	50.1.1.1
Avaya C360 Stackable Switch	VLAN20	20.1.1.2/24	20.1.1.1
Enterasys Wireless Access Point	VLAN 20	20.1.1.10/24	20.1.1.1
3000 (RBT3K-AG)			
Extreme Alpine 3804 Switch	VLAN1	50.1.1.1/24	
	VLAN20	20.1.1.1/24	
Avaya 3626 Wireless Telephone		20.1.1.100	20.1.1.1
Avaya 3616 Wireless Telephone		20.1.1.101	20.1.1.1
Avaya Phone Manager Pro		20.1.1.126	20.1.1.1
Odyssey RADIUS Server	VLAN 1	50.1.1.50/24	50.1.1.1

Table 1 lists the IP addresses and subnet masks for the tested devices.

2. Equipment and Software Validated

Table 2 lists the equipment and software version used for the configuration.

Equipment	Software
Avaya IP406 Office	IP Office 2.1(29)
Avaya Phone Manager Pro	V2.1.6
Avaya 4620SW/4610SW IP Telephones	R2.01
Avaya 3616/3626 Wireless IP Telephone	96.024
Avaya Voice Priority Processor	R168.112
Avaya C360 Stackable Switch	R4.3.12
Enterasys Wireless Access Point 3000 (RBT3K-AG)	V2.1.2
Extreme Alpine 3804 Switch	V7.2.0b25
Dell Laptop with	
 Windows XP 2000 	5.00.2195
 Enterasys RoamAbout 802.11 a/b/g Wireless Card 	V 3.0.0.111
Odyssey RADIUS Server	V2.01.00.653
Odyssey Client	V3.03.0.1194

Table 2: Equipment and Software Validated

3. Configure Enterasys AP 3000 (RBT3K-AG)

The configuration can be done using a web-based interface. Assume that the IP address 20.1.1.10 has been pre-configured on the Enterasys Wireless Access Point 3000. The following sessions display the related configuration using web-based interface.

3.1. Basic System and Wired Equivalent Privacy (WEP) Configuration

This section presents the steps of basic system wireless and WEP configuration. The Enterasys Wireless Access Point 3000 (RBT3K-AG) has both 802.11a and 802.11g radio interfaces. The 802.11g radio interface supports both 802.11b and 802.11g clients. In these Application Notes, the 802.11g radio is configured to accept both 802.11b and 802.11g clients to support the Avaya IP 3616 and 3626 IP wireless Telephones. Note that the Avaya 3626/3616 series wireless Telephones currently only operate in 802.11b mode. The 802.1x authentication is applied to the Avaya Phone Manager Pro using Odyssey Client.



• After				
DisalClick(OptiVerif	blogging in, click ble DHCP Clien (a Enable for HT (a block Enab (b) the IP address (b)	TCP/IP Sett t since static II IP Server and ole for HTTPS and Subnet Ma	ings from the left pane P address is used. I leave HTTP Port 80 S Server and leaver po ask are correct.	el. as default. ort 443 as default.
🖉 RoamAbo	ut Access Point - Microsoft In	ternet Explorer		_ _ X
<u> </u>	View Favorites Tools He	p		19 (B)
← Back →	🔿 - 🙆 😰 🚮 😡 Searc	h 💽 Favorites 🎯 Histo	ory 원· 🗿 🔟 📃	
Address (https://20.1.1.10/ip.htm			✓ @Go Links ‴
	ENTERASYS NETWORKS.		Roam	About
	RoamAbout	TCP/IP Se	ttinas	
	Roambout Identification TCP/IP Settings RADIUS PPPoE Settings Authentication Filter Control QoS SNMP Administration System Log 802.11a Interface Radio Settings Security 802.11b/g Interface Radio Settings Security Status AP Status Stations Status Event Logs	DHCP DHCP Client: Web Servers HTTP Server: HTTP Port: HTTPS Server: HTTPS Port: IP Address IP Address IP Address Subnet Mask: Default Gateway: Primary DNS: Secondary DNS:	© Disable © Enable © Disable © Enable 80 © Disable © Enable 443 20.1.1.10 255.255.255.0 20.1.1.1 0.0.0 0.0.0	
				Apply Cancel Help
				📄 📄 💓 Internet 👘

		Description
	• Click OK to lo	ogin to AP again.
<	🚰 RoamAbout Access Point -	- Microsoft Internet Explorer
	<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	s Tools Help
	🖕 Back 🔹 🤿 👻 👔	🟦 🔯 Search 📾 Favorites 🖉 History 🛛 🖏 🖬 🗐
	Address 🛃 https://20.1.1.10/	chtcpip 🔽 🖉 Go 🛛 Links »
	ENTERASYS	RoamAbout
	Logout Roam4bout	
	Identification TCP/IP Settings RADIUS PPPoE Settings Authentication Filter Control QoS SNMP Administration System Log 802.11a Interface Radio Settings	Configuration has been saved. Please login with new settings!
	Security 802.11b/g Interface	
		•

		Description		
The following sections display the 802.11b/g interface configuration.				
• Click the Radio Settings under 802.11b/g Interface from the left panel.				
• Enter 1 for Native VLAN ID.				
	• Enter a unique	Network Name (e.g. RAbg) as its	SSID.	
	• Click Enable f	for Secure Access.		
	• Click Enable f	For Auto Channel Select.		
	• Click b & g m	ixed for Working Mode to accept	both b and g clients.	
	• Leave other set	ttings as defaults.		
	• Click Apply.			
	3 p al l a p -:			
	File Edit View Eavor	nt - Microsoft Internet Explorer		
		1 🖉 🖓 Search 📾 Eavorites 🖓 History 🛛 🕀		
	Address Chitros: (120 1 1	10/radio2.htm	Go Links ≫	
	ENTERASYS		Room About	
	NETWORKS		RoamAbout	
	Logout			
	RoamAbout	802.11b/g Interface		
	Identification			
	TCP/IP Settings RADIUS	Radio Settings	⊂Disable ®Enable	
	PPPoE Settings	Description	PoemAbout AP2000 - 902 11b/g	
	Authentication Filter Control			
	QoS	Native ¥LAN ID:		
	Administration	Network Name (SSID):	RAbg	
	System Log	Secure Access:	O Disable 💿 Enable	
	802.11a Interface	Radio Channel:		
	Radio Settings	Auto Channel Select:	O Disable 💿 Enable	
	Security	Working Mode:	● b & g mixed O g only O b only	
	802.11b/g Interface	Transmit Power:	100% -	
	Radio Settings	Maximum Tx Data Rate:	11Mbps 🔽	
	Security	Multicast Data Rate:	1Mbps 💌	
	Status	Beacon Interval (20-1000)	100 ms	
	AP Status	Data Beacon Rate(DTIM) (1-25	5) 2 Beacons	
	Stations Status Event Logs	Fragment Length (256-2346)	2346 Bytes	
		RTS Threshold (0-2347)	2347 Bytes	
		Maximum Associations (0-250)	100 Clients	
			Apply Cancel Help	
			Арріх сапсеі пер	
	🗳 Done		📔 🥙 Internet 🛛 🎼	

Step		Description			
4.	This section presents the WEP configuration. Because the Avaya 3626 and 3616 wireless				
	Telephones do not support 802.1x, the 802.1x authentication needs to be disabled on AP.				
	• Click Authentication from left panel and click Disable for 802.1x authentication as				
	shown below.				
	• Click Apply whe	en done.			
	🖉 RoamAbout Access Point	- Microsoft Internet Explorer			
	<u> </u>	es Iools Help			
	_ ← Back - → - 🙆 👔	🖄 🕅 Search 🔝 Favorites 👹 History 🖏 🚽 🚍			
	Address 🖉 https://20.1.1.10)/auth.htm			
	ENTERASYS				
	NETWORKS.	RoamAbout			
	Logout				
	RoamAbout	Authentication			
	Identification				
	TCP/IP Settings	MAC Authentication: Disable			
	PPPoE Settings				
	Authentication	802.1x Setup:			
	QoS	• Disable 802.1x authentications not allowed			
	SNMP Administration	O Supported Clients may or may not use 802.1x			
	System Log	C Required Client must use 802.1x			
	802.11a Interface	If 802.1x supported or required is selected, then RADIUS setup must be completed.			
	Radio Settings Security	Broadcast Key Refresh Rate 100 minutes (0 = Disabled)			
	802.11b/g Interface	Session Key Refresh Rate 100 minutes (0 = Disabled)			
	Radio Settings	802.1x Session Timeout 600 minutes (0 = Disabled)			
	Security	802.1x Supplicant:			
	Status	802.1x Supplicant 🔿 Disable 🖲 Epable			
	AP Status				
	Stations Status				
	Evenceogs				
		Local MAC Authentication:			
		System Default O Deny 💿 Allow			
		MAC Authentication Settings:			
		C Deny · Allow C Delete Update			
		MAC Authentication Table:			
		Number MAC Address Permission			
		Apply Cancel Help			
	Done				
	e pone				

Step	Description
5.	WEP configuration is shown on the next page.
5.	 Click Security under 802.11b/g Interface from the left panel. Select Shared Key for Authentication Type Setup. This will only allow users who have the correct key to access AP. Click Enable for Data Encryption Setup. Click 100 Data Encryption Setup. Click 128 Bit for Shared Key Setup (Note that Avaya IP 3626/3616 IP Telephones support both 40 and 128 bit key). Click Hexadecimal for Key Type. Enter 26 digits key string in Key1 field. Make sure this key matches the key entered in the IP Wireless Telephone. Click Apply.

	Description
RoamAbout Access Poin	nt - Microsoft Internet Explorer
<u>File Edit View Favori</u>	ites Tools Help
← Back ← → ~ 🙆 😰	🖓 🍳 Search 📷 Favorites 🔇 History 🖏 🖉 🧾
Address 🔄 https://20.1.1.1	10/security2.htm
RoamAbout	802.11b/g Interface
Identification TCP/IP Settings RADIUS	Security Settings
PPPoE Settings	Authentication Type Setup
Authentication Filter Control	O Open System Allow everyone to access
QoS	Shared Key Allow users with a correct key to access
Administration	Data Encryption Setup
System Log	O Disable O Enable
802.11a Interface	
Dedie Cettings	WPA Clients
Security	⊙ Supported ○ Required ○ Not Supported
802.11b/g Interface	WPA Key Management
Padia Sattinas	WPA authentication over 802.1x
Security	O WPA Pre-shared Key
Status	Multicast Cipher Mode
AP Status	• WEP Use WEP as WPA Multicast cipher mode
Stations Status	C TKIP Use TKIP as WPA Multicast cipher mode
Event Logs	C AES Use AES as WPA Multicast cipher mode
	WPA Pre-Shared Key Type
	C Hexadecimal Enter 64 digits
	Alphanumeric Enter between 8 and 63 characters
	WPA Pre-Shared Key
	Shared Key Setup
	C 64 Bit 📀 128 Bit C 152 Bit
	Кеу Туре
	Hexadecimal For 64 Bit enter 10 digits, for 128 Bit enter 26 digits for 152 Bit enter 32 digits
	C Alphanumeric 13 characters, for 152 Bit enter 16 characters
	Key Number Transmit Key Select Key
	Key 1 (C) 3000000000000000000000000000000000000
	Кеу 2 О
	Кеу З С
	Кеу 4 О
	Apply Cancel Help
(📄 📄 🔮 Internet

3.2. 802.1x Authentication Configuration

This section presents the 802.1x authentication configuration. This configuration verifies that the Avaya Phone Manager Pro with Odyssey Client can pass 802.1x authentication from the Odyssey RADIUS Server through the AP. Note this configuration does not apply to the Avaya 3626/3616 Wireless Telephones since those telephones do not support 802.1x.

tep		Description	
1.	Configure 802.11a Interf	ace.	
	• Click the Radio S	Settings under 802.11a Interf	face from the left panel.
	• Enter 1 for Nativ	e VLAN ID.	-
	• Enter a unique No	etwork Name (e.g. RAa) as it	ts SSID.
	Click Enable for	Secure Access	
	Leave other settir	og as defaults as shown below	X 7
	Click Apply	igs as defaults as shown below	· · ·
	• Click Apply.		
	🖉 Doamábout áccass Boint - Microso	it Internet Funlorer	
	File Edit View Favorites Tools	Help	
	← Back ← → → ② ③ ④ 🖓	earch 📓 Favorites 🎯 History 🛛 🛃 🖬 📑	
	Address 🛃 https://20.1.1.10/radio1.htm		▼ 🖗 Go 🗍 Links ≫
		c	
		S G.	RoamAbout
	Logout		
	Roam4hout	902 11a Interface	
		802.11a Internace	
	Identification TCP/IP Settings	Radio Settings	○ Disable . ⓒ Enable
	RADIUS PPPoE Settings		
	Authentication	Description:	RoamAbout AP3000 - 802.11a
	Filter Control QoS	Native ¥LAN ID:	1
	SNMP Administration	Network Name (SSID):	RAa
	System Log	Secure Access:	O Disable 💿 Enable
	802.11a Interface	Turbo Mode:	Disable C Enable
	Radio Settings	Radio Channel:	44 ch, 5.220 GHz 💌
	Security	Auto Channel Select:	O Disable © Enable
	802.11b/g Interfa	e Transmit Power:	
	Radio Settings	Maximum Tx Data Rate:	54Mbps 🔽
	Security	Multicast Data Rate:	bMbps
	Status	Beacon Interval (20-1000)	IUU ms
	AP Status Stations Status	Data Beacon Rate(DTIM) (1-255	5) 2 Beacons
	Event Logs	Fragment Length (256-2346)	2346 Bytes
		RTS Threshold (0-2347)	2347 Bytes
		Maximum Associations (0-250)	100 Clients
			Apply Cancel Help
	¢		🔒 😻 Internet 🥢

This section presents the RADIUS Server configuration. Click Radius from left panel to enter the radius server information as shown bel Enter IP address 50.1.1.50 for primary RADIUS Server. Leave port number 1812 as default settings. Since only one RADIUS server is used in this configuration, leave IP address 0.1 in the field for the Secondary RADIUS Server. Enter shared key, 1234567890 is used in this case, in Key field. This Key is share between the Wireless Access Point and the Radius Server while authenticating t supplicant (Note the Key entered here must match the key entered in the RADIU Server.). Click Apply. Cognet RADIUS Primary RADIUS Server Setup RADIUS Primary RADIUS Server Setup Retransmit attempts: 3		Descri	ption		
 Click Radius from left panel to enter the radius server information as shown bel Enter IP address 50.1.1.50 for primary RADIUS Server. Leave port number 1812 as default settings. Since only one RADIUS server is used in this configuration, leave IP address 0.1 in the field for the Secondary RADIUS Server. Enter shared key, 1234567890 is used in this case, in Key field. This Key is sharbetween the Wireless Access Point and the Radius Server while authenticating t supplicant (Note the Key entered here must match the key entered in the RADIU Server.). Click Apply. Promabout Access Point-Microsoft Internet Explorer Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Prove Payorites Tools Help Image: Click Apply. Primary RADIUS Server Setup Prover Number: Illi2 Redio Settings Security Beatures Security Port Number: Illi2 Radio Settings Securi	section presents the	e RADIUS Server confi	iguration.		
 Enter IP address 50.1.1.50 for primary RADIUS Server. Leave port number 1812 as default settings. Since only one RADIUS server is used in this configuration, leave IP address 0.1 in the field for the Secondary RADIUS Server. Enter shared key, 1234567890 is used in this case, in Key field. This Key is sharbetween the Wireless Access Point and the Radius Server while authenticating t supplicant (Note the Key entered here must match the key entered in the RADIU Server.). Click Apply. RoamAbout Access Point - Microsoft Internet Explorer Be Edit Vew Favorites Tools Heb Were Favorites Tools Heb Baddress: P	Click Radius fro	om left panel to enter the	e radius server information as	shown below	
 Leave port number 1812 as default settings. Since only one RADIUS server is used in this configuration, leave IP address 0.1 in the field for the Secondary RADIUS Server. Enter shared key, 1234567890 is used in this case, in Key field. This Key is shall between the Wireless Access Point and the Radius Server while authenticating t supplicant (Note the Key entered here must match the key entered in the RADIU Server.). Click Apply. RoamAbout Access Point - Microsoft Internet Explorer Be Edit Yew Favorites Tools Help Back - → - ②	• Enter IP address 50.1.1.50 for primary RADIUS Server.				
 Since only one RADIUS server is used in this configuration, leave IP address 0.1 in the field for the Secondary RADIUS Server. Enter shared key, 1234567890 is used in this case, in Key field. This Key is shall between the Wireless Access Point and the Radius Server while authenticating t supplicant (Note the Key entered here must match the key entered in the RADIU Server.). Click Apply. Click Apply. Click Apply. CoamAbout Access Point - Microsoft Internet Explorer Ele Ede Vew Paventes Tools thep Head	Leave port numb	er 1812 as default settin	igs.		
Enter shared key, 1234567890 is used in this case, in Key field. This Key is shall between the Wireless Access Point and the Radius Server while authenticating t supplicant (Note the Key entered here must match the key entered in the RADIU Server.). Click Apply. RoamAbout Access Point - Microsoft Internet Explorer Ide Edit Yow Favorites Tools Help Headterss Interstition This Server Setup RoamAbout RADIUS Identification TCP/IP Settings RADIUS Primary RADIUS Server Setup Robust Control Qos Sittings Authentication System Log Bill 2 Address: 50.1.1.50 Primary RADIUS Server Setup Robust Settings Retransmit attempts: 3 Secondary RADIUS Server Setup B02.111/g Interface Radio Settings Secondary RADIUS Server Setup B02.111/g Interface Radio Settings Secondary RADIUS Server Setup B02.111/g Interface Radio Settings Secondary RADIUS Server Setup B02.111/g Interface IP Address: 0.0.0.0 Port Number: 1812 Key: 0.0.0 Radio Settings Secondary RADIUS Server Setup B02.111/g Interface Retransmit attempts: 3 Secondary RADIUS Server Setup B02.112/g Interface Retransmit attempts: 3 Secondary RADIUS Server Setup B02.113/g Interface Retransmit attempts: 3 Secondary RADIUS Server Setup B02.113/g Interface Retransmit attempts: 3 Secondary RADIUS Server Setup B02.113/g Interface Retransmit attempts: 3 Secondary RADIUS Server Setup B02.113/g Interface Retransmit attempts: 3 Secondary RADIUS Server Setup B02.113/g Interface Retransmit attempts: 3 Secondary RADIUS Server Setup B02.113/g Interface Retransmit attempts: 3 Secondary RADI	in the field for the	ADIUS server is used in Secondary RADIUS	Server	address 0.0.0	
Inter ontact Key, FLO FOR DA Local in this class, Server while authenticating t between the Wireless Access Point and the Radiu, Server while authenticating t supplicant (Note the Key entered here must match the key entered in the RADIU Server.). • Click Apply. Ple Edit Yew Favorites Tools Help Image: Secondary Radius Server Setup Address Identification TCP/IP Settings Address: Identification TCP/IP Settings Address: 50.1.1.50 Primary RADIUS Server Setup Port Number: 1812 Robits Key: Address: 50.1.1.50 Primary RADIUS Server Setup Robits Recondary RADIUS Server Setup Robits Recondary RADIUS Server Setup Robits Key: Madress: 50.1.1.50 Primary RADIUS Server Setup Boot Exercise Seture Robits Secondary RADIUS Server Setup Robits Secondary RADIUS Server Setup Boot Port Number: 1812 Radio Settings Secondary RADIUS Server Setup Boot P	Enter shared key	1234567890 is used in	this case in Key field This	Key is shared	
supplicant (Note the Key entered here must match the key entered in the RADIU Server.). • Click Apply. • Cli	between the Wir	eless Access Point and t	the Radius Server while author	enticating the	
Server.). • Click Apply. • C	supplicant (Note	the Key entered here m	ust match the key entered in	the RADIUS	
 Click Apply. RoamAbout Access Point - Microsoft Internet Explorer Be Edit View Favorites Tools Help Back +	Server.).				
RoamAbout Access Point - Microsoft Internet Explorer Image: Control Status	Click Apply.				
Image: Secondary RADIUS Server Setup Radio Settings System Log B02.11b/g Interface Radio Settings Secondary RADIUS Server Setup B02.11b/g Interface IP Address: 0.0.0.0 Radio Settings Security Security Status <	Doom@bout @ccess Doin	- Microsoft Internet Evplorer			
Hadress Address Reading Reading Security Box Address Status Status <th><u>File Edit View Favorit</u></th> <td>es <u>T</u>ools <u>H</u>elp</td> <td></td> <td></td>	<u>File Edit View Favorit</u>	es <u>T</u> ools <u>H</u> elp			
Address https://20.1.1.10/radius.htm ENTERASYS NETWORKS Logout RoamAbout Logout RoamAbout Identification TCP/IP Settings RADIUS PPPoE Settings Authentication Filter Control Qos SNMP Administration System Log 802.116 Interface Radio Settings Security 802.11b/g Interface Radio Settings Security Status Status <t< td=""><th>🗢 Back 🔹 🔿 👻 😰</th><td>🖓 😡 Search 👔 Favorites 🔇</td><td>History 🛛 🛃 🚽 🗐</td><td></td></t<>	🗢 Back 🔹 🔿 👻 😰	🖓 😡 Search 👔 Favorites 🔇	History 🛛 🛃 🚽 🗐		
ENTERASYS RoamAbout Logout RoamAbout RoamAbout RADIUS Identification TCP/IP Settings RADIUS Primary RADIUS Server Setup PPPOE Settings IP Address: Authentication Filter Control QoS SMMP Authentication Port Number: Filter Control QoS SMMP Retransmit attempts: Addresse Secondary RADIUS Server Setup B02.11b/g Interface IP Address: Radio Settings Secondary RADIUS Server Setup B02.11b/g Interface IP Address: Radio Settings Secontry Security Security Status IP Address: AP Status Timeout (seconds): Status Security	Address 🙋 https://20.1.1.10)/radius.htm		🖌 🧬 Go 🗍 Links 🏻	
Instruction ReamAbout Lagout Radination RoamAbout RADIUS Identification TCP/IP Settings RADIUS Primary RADIUS Server Setup Primary RADIUS Server Setup IP Address: Sump Sump Administration System Log B02.111a Interface Retransmit attempts: Radio Settings Security B02.11b/g Interface IP Address: Radio Settings Security B02.11b/g Interface IP Address: Radio Settings Security B02.11b/g Interface IP Address: Radio Settings Security Security Security B02.11b/g Interface IP Address: Radio Settings Security Security Security AP Status Key: Status Timeout (seconds): Status Security	ENTERASVS			▲ 	
Logout RoamAbout RADIUS Identification TCP/IP Settings RADIUS Primary RADIUS Server Setup PPDoE Settings IP Address: Authentication Filter Control Qo8 IP Address: SIMP Retransmit attempts: Administration Secondary RADIUS Server Setup 802.11a Interface Retransmit attempts: Radio Settings Secondary RADIUS Server Setup 802.11b/g Interface IP Address: Radio Settings Secondary RADIUS Server Setup 802.11b/g Interface IP Address: Radio Settings Secondary RADIUS Server Setup Status IP Address: 0.0.0.0 Port Number: 1812 Key: Image: Status Image: Image: AP Status Key: Image: Stations Status Event Logs 5 Stations Status Security: Security:	ENTERASYS NETWORKS. RoamAbout				
RoamAbout RADIUS Identification TCP/IP Settings RADIUS Primary RADIUS Server Setup PPPoE Settings IP Address: 50.1.1.50 Authentication Filter Control Port Number: 1812 QoS Key: wwww Administration System Log Key: wwww 802.11a Interface Retransmit attempts: 3 Radio Settings Security Security Security 802.11b/g Interface IP Address: 0.0.0.0 Radio Settings Port Number: 1812 Security IP Address: 0.0.0.0 Port Number: 1812 Key: Address: 0.0.0.0 Port Number: 1812 Status Key: wwww Key: Key: Key: Status Status Timeout (seconds): 5 Status	Logout				
Identification TCP/IP Settings AdDIUSPrimary RADIUS Server SetupPPPoE Settings Authentication Filter Control QoS SNMP Administration System LogIP Address:50.1.1.50B02.11a InterfacePort Number:1812Radio Settings SecurityKey:wwwwB02.11b/g InterfaceRetransmit attempts:3B02.11b/g InterfaceIP Address:0.0.0.0Radio Settings SecurityPort Number:1812B02.11b/g InterfaceIP Address:0.0.0.0Radio Settings SecurityPort Number:1812Key:wwww1812Key:Imeout (seconds):5StatusFort Number:1812StatusKey:wwwwStatusStatus5StatusTimeout (seconds):5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus5StatusStatus3<	RoamAbout RADIUS				
PPPoE Settings Authentication Filter Control QoS SNMP Administration System LogIP Address:50.1.1.50Port Number:1812B02.11a Interface Radio Settings SecurityRetransmit attempts:3B02.11b/g Interface Radio Settings SecurityPort Number:1812B02.11b/g Interface Radio Settings SecurityIP Address:0.0.0.0B02.11b/g Interface Retransmit attempts:IS12Control Control Con	Identification TCP/IP Settings RADIUS	Primary RADIUS Server :	Setup		
Filter Control QoS SNMPPort Number:1812Administration System LogKey:wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww	PPPoE Settings Authentication	IP Address:	50.1.1.50		
SNMP Administration System LogKey:Image: Constant of the second s	Filter Control	Port Number:	1812		
Administration System LogTimeout (seconds):5802.11a InterfaceRetransmit attempts:3Radio Settings SecuritySecondary RADIUS Server Setup802.11b/g InterfaceIP Address:0.0.0.0Radio Settings SecurityPort Number:1812StatusKey:MercenceAP Status Status Event LogsTimeout (seconds):5Retransmit attempts:3	SNMP	Key:	Yolololok		
802.11a InterfaceRetransmit attempts: 3Radio Settings SecuritySecondary RADIUS Server Setup802.11b/g InterfaceIP Address:0.0.0.0Radio Settings SecurityPort Number:1812StatusKey:*******AP Status Stations Status Event LogsTimeout (seconds):5Retransmit attempts:3	Administration System Log	Timeout (seconds):	5		
Radio Settings SecuritySecondary RADIUS Server Setup802.11b/g Interface Radio Settings SecurityIP Address:0.0.0.0Radio Settings SecurityPort Number:1812StatusKey:*********************************	302.11a Interface	Retransmit attempts:	3		
802.11b/g Interface IP Address: 0.0.0.0 Radio Settings Security Port Number: 1812 Status Key: ************************************	Radio Settings Security	Secondary RADIUS Serve	er Setup		
Radio Settings Security IP Address: 0.0.0.0 Port Number: 1812 Status Key: ************************************	B02.11b/g Interface				
Security Port Number: 1812 Status Key: Number: AP Status Timeout (seconds): 5 Stations Status Retransmit attempts: 3	Radio Settings	IP Address:	0.0.0		
Status Key: December AP Status Timeout (seconds): 5 Stations Status Retransmit attempts: 3	Security	Port Number:	[1812 [
AP Status Timeout (seconds): 5 Stations Status Retransmit attempts: 3	Status	Key:			
Event Logs	AP Status	Timeout (seconds):	5		
	stations Status Event Logs	Retransmit attempts:	3		
Applu Concel Help			Apple - C	ancel Help -	
Appiy Cancel Help			<u>арріу Са</u>		
	1			•	



Step	Description
4.	This section presents the WPA (WiFi Protected Access) configuration associated with the 802.1x . WPA includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. The combination of these two mechanisms provides dynamic key encryption and mutual authentication. The configuration screen is shown on the next page.
	 Click Security under 802.11a Interface from left panel. Click Open System as Authentication Type Setup. Click Enable for Data Encryption Setup. Click Supported for WPA Clients. Click WPA authentication over 802.1x under WPA Key Management.
	 Click TKIP (Temporal Key Integrity Protocol) under Multicast Cipher Mode for key encryption. (Note: Since the TKIP can provide dynamic key and encryption, the manual key entry is not required for client authentication. Leave both the WPA Pre-Shared Key and Shared Key fields blank.) Click Apply when done.
SZ; Rev	riewed: Solution & Interoperability Test Lab Application Notes 14 of 27
GAK 4/	22/2005 ©2005 Avaya Inc. All Rights Reserved. Enterasys-IPO.doc

		Description
🍯 Roar	mAbout Access Point - Micr	osoft Internet Explorer
	Edit View Favorites To	
]	ick ▼ ⇒ ▼ 🐸 🙆 🙆	Q Search 承 Favorites 《영 History 타고 + 글에 도 드
Addres	s 🙋 https://20.1.1.10/securi	y1.htm
	RoamAbout	802.11a Interface
	Identification	
	TCP/IP Settings	Security Settings
	PPPoE Settings	Authentication Type Setun
	Authentication	Open System Allow everyone to access
	QoS	© Shared Key Allow users with a correct key to access
	SNMP	
	System Log	Data Encryption Setup
	802.11a Interface	
	Radio Settings	WPA Clients
	Security	• Supported C Required C Not Supported
	802.11b/g Interface	WPA Key Management
	Radio Settinos	WPA authentication over 802.1x
	Security	O WPA Pre-shared Key
	Status	Multicast Cipher Mode
	AP Status	C WEP Use WEP as WPA Multicast cipher mode
	Stations Status	• TKIP Use TKIP as WPA Multicast cipher mode
	Event Logs	C AES Use AES as WPA Multicast cipher mode
		WPA Pre-Shared Key Type
		C Hexadecimal Enter 64 digits
		Alphanumeric Enter between 8 and 63 characters
		WPA Pre-Shared Key
		Shared Key Setup
		C 64 Bit ⊙ 128 Bit C 152 Bit
		Key Type Ear 64 Bit enter 10 digits for 128 Bit enter 26
		C Hexadecimal digits, for 152 Bit enter 32 digits
		Alphanumeric A
		Key Number Transmit Key Select Key
		Key 1 (0
		Key 2 O
		Key 3 O
		Key 4 O
		<u>Apply</u> <u>Cancel</u> <u>Help</u>
@		🔒 💓 Internet

For detailed Avaya Voice Priority Processor, Odyssey Server and Client configuration, refer to the Application Notes listed in Section 7 and other documents from Funk Software web site at http://www.funk.com.

4. Configure Avaya IP406 Office

This section describes the steps necessary to configure the Avaya IP406 Office. IP406 Office is configured using the IP Office Manager application. Assume that a proper license has been installed on the Avaya IP406 Office.

Step	Description
1.	 <i>Configuring interface LAN1.</i> Using the IP Office Manager, browse the configuration tree and select System Configuration and click on the LAN1 tab. Set IP Address to 50.1.1.10 and IP Mask to 255.255.255.0. For the DHCP Mode, select Disabled. Click OK.
	Manager [50.1.1.10] (C:\Program Files\\Manager\) 00E007004990.cfg File Edit View Tools Window Help
	System Configuration : 00E007004990
	IP Address 50.1.1.10 Number Of DHCP IP Addresses 200
	IP Mask 255.255.255.0 DHCP Mode © Server © Disabled © Dialin © Client
	RIP Mode None Listen Only (Passive) RIP 1 RIP 2 Broadcast (RIP 1 Compatibility) RIP 2 Multicast
	OK <u>C</u> ancel <u>H</u> elp

Step	Description				
2.	Adding Avaya Voice	Priority Processo	or (AVPP) IP	Address.	
	Using the IP Office N and click on the Syste	fanager, browse the m tab.	he configurati	on tree and select	System Configuration
	 Enter 50.1.1.9 Enter manage IP Address fit 	into AVPP IP A ment PC's IP add elds. This is the P	ddress field. ress 20.1.1.12 C that runnin	2 into TFTP Serv g IP Office Manag	ver and License Server ger Application.
	Leave other fiClick OK.	elds as default.			
	Manager [50.1.1.10] (C:\Prog Eile Edit View Tools Window	ram Files\\Manager\) 00E00 <u>H</u> elp	7004990.cfg		
	Configuration Tree		007004990		
	Derator (3) System 00E007004990 E.Line (2)	System LAN1 DNS Voice	mail Telephony Gatekee	eper LDAP SNMP	
	E Control Unit (1) Extension (7)	Name	00E 007004990	Locale	enu
		Monitor Password		Confirm Monitor Password	
	B			Licence Server IP Address	20.1.1.122
	WAN Port (1) Directory (0) Time Profile (0)	Time Offset (hours) TFTP Server IP Address	20.1.1.122		50119
	Firewall Profile (1) Firewall Profile (2)	Time Server IP Address		AVEF IF Address	30.1.1.3
	Ecast Cost Houte (0)	File Writer IP Address			DSS Status Beep on listen
		Conferencing Center IP Address			Hide auto recording
	🛟 E911 System(0)		Favour RIP Routes, o	ver static routes	
				ОК	<u>Cancel</u> <u>H</u> elp
		-9			

Step	Description
3.	 Configuring the default gateway. Browse the configuration tree and select IP Route. Leave the IP Address and IP Mask fields blank. This sets the default gateway. Enter 50.1.1.1 as gateway IP address Select LAN1 as gateway interface. Enter 1 in Metric field. Click OK.
	Imanager [S0.1.1.10] (C\Program Files\\Manager\) 00E007004990.cfg Ele Edt Wew Tools Window Help Image: Solution of the second secon

Step	Description	
4.	Configuring a User.	
	In the IP Office, ever example shows how	ry extension created requires a user associated with it. The following to configure a user for a PhoneManager Pro using extension 50004.
	Using the IP Office N in the fields as shown	Manager, browse the configuration tree and select User. Enter information n below
	Manager [50.1.1.10] (C:\	Program Files\\Manager\) 00E007004990.cfg
		now Gah
	大User Extn50004	
	User Voicemail DND	ShortCodes SourceNumbers Telephony Forwarding Dial In VoiceRecording ButtonProgramming Coverage
	Name	Extr50004
	Password	
	Confirm Password	
	Full Name	PhoneManager 50004
	Extension	50004
	Locale	
	Priority	
	Restrictions	
	•	
		li.

 Click the Telephony tab. Select VoIP in the Phone Manager Type field. Leave the other parameters as default. Click OK when done. Winnager [Sol.1.10] (C)Program Files\\Manager\) 00E007004990.cfg Select Year Solution File Edit Year Tools Window Help Were ExtraSol04 Were ExtraSol04 Prove Notice Rest Solution Default Ring Click OK when does Worder ExtraSol04 Prove Rest Solution Default Ring Click Value Click Ring Pattern DefaultRing Clink Value Click Ring Pattern DefaultRing Clink Value Click Station Click Ring Pattern DefaultRing Clink Value Click Ring Pattern DefaultRing Click Chained Click Ring Pattern DefaultRing Click Ring Pattern DefaultRing Click Ring Pattern DefaultRing Click Ring Pattern DefaultRing Click Ring Pattern Click Ring Pattern<!--</th--><th>Γ</th><th>Description</th><th></th>	Γ	Description	
Ele Edit Yew Tools Window Help Image: Your Tools Window Help<		 Click the Telephony Select VoIP in the F Leave the other para Click OK when don 	y tab. Phone Manager Type field. imeters as default. ie.
		Eile Edit View Iools Window Help	nies \ (Manager () 00c007004590.crg
User Voicemail DND ShortCodes SourceNumbers Telephony Forwarding Dial In VoiceRecording ButtonProgramming Coverage Outside Ring Pattern DefaultRing Call Waiting Busy On Held Ring Back Pattern DefaultRing Outward Restricted Allocated Answer Interval (secs) Cannot be Intrude Wrap-up Time (secs) Cannot be Intruded Transfer return Time (secs) Core Account Code Login Code Force Login Login Idle Period (secs) System Phone Monitor Group Phone Manager Type VolP Book a Power Conference in Phone Manager Monitor Group Image Book a Power Conference in Phone Manager Monitor Group Monit		t User Extn50004	
Outside Ring Pattern DefaultRing Call Waiting On Inside Ring Pattern DefaultRing Busy On Held Ring Back Pattern DefaultRing Outward Restricted Allocated Answer Interval (secs) Can Intrude Wrap-up Time (secs) Can Intrude Transfer return Time (secs) Directory Exclude Force Login Login Code Login Idle Period (secs) System Phone Monitor Group VolP Phone Manager Type VolP OK Cancel Help VolP		User Voicemail DND ShortCode	s SourceNumbers Telephony Forwarding Dial In VoiceRecording ButtonProgramming Coverage
Inside Ring Pattern DefaultRing ✓ Busy On Held Ring Back Pattern DefaultRing ✓ Outward Restricted Allocated Answer Interval (secs) ✓ Offhook Station Can Intrude ✓ Can Intrude Wrap-up Time (secs) 2 ✓ Cannot be Intruded Transfer return Time (secs) □ Directory Exclude Login Code □ Force Login Login Idle Period (secs) ✓ System Phone Monitor Group ✓ ■ Phone Manager Type VolP ✓ Book a Power Conference in Phone Manager		Outside Ring Pattern	DefaultRing Call Waiting On
Ring Back Pattern DefaultRing Outward Restricted Allocated Answer Interval (secs) Can Intrude Wrap-up Time (secs) Cannot be Intruded Transfer return Time (secs) Directory Exclude Force Login Force Login Login Idle Period (secs) System Phone Monitor Group Image: Cancel Help (Cancel (Cancel Help (Cancel (Cancel (Cancel (Cancel		Inside Ring Pattern	
Allocated Answer Interval (secs) Image: Cannot be Intrude Wrap-up Time (secs) Image: Cannot be Intrude Transfer return Time (secs) Image: Cannot be Intrude Login Code Image: Cannot be Intrude Login Code Image: Cannot be Intrude Login Idle Period (secs) Image: Cannot be Intrude Monitor Group Image: Cannot be Intrude Phone Manager Type VolP Image: Cannot be Intrude Image: Cannot be Intrude Image: Code Image: Cannot be Intrude <th></th> <th>Bing Back Pattern</th> <th>✓ Busy On Held</th>		Bing Back Pattern	✓ Busy On Held
Allocated Answer Interval (secs) Can Intrude Wrap-up Time (secs) Transfer return Time (secs) Login Code Login Code Login Idle Period (secs) Monitor Group Phone Manager Type VoIP K Cancel Help K Help K		Thing Back Fakon	Outward Restricted Offbook Station
Wrap-up Time (secs) 2 Cannot be Intruded Transfer return Time (secs) Directory Exclude Force Login Force Login Login Code Force Account Code Login Idle Period (secs) System Phone Monitor Group Image: Conference in Phone Manager Phone Manager Type VolP Image: Conference in Phone Manager Image: Conference in Phone Manager Image: Conference in Phone Manager Image: Conference in Phone Manager		Allocated Answer Interval (secs)	
Transfer return Time (secs) Login Code Login Idle Period (secs) Monitor Group Phone Manager Type VolP OK Cancel Help		Wrap-up Time (secs)	2 Cannot be Intruded
Login Code Login Idle Period (secs) Monitor Group Phone Manager Type VolP Book a Power Conference in Phone Manager OK Cancel Help		Transfer return Time (secs)	Directory Exclude
Login Code Login Idle Period (secs) Monitor Group Phone Manager Type VolP OK Cancel Help			Force Login
Login Idle Period (secs) Monitor Group Phone Manager Type VolP OK Cancel Help		Login Code	Force Account Code
Monitor Group Phone Manager Type VolP OK Cancel Help Image: Content of the second secon		Login Idle Period (secs)	J System Phone
Phone Manager Type		Monitor Group	
OK <u>C</u> ancel <u>H</u> elp		Phone Manager Type	VoIP Book a Power Conference in Phone Manager
			OK <u>C</u> ancel <u>H</u> elp

Step	Description	
5.	Configuring an extension.	
	Using the IP Office Manager Pro, b	prowse the configuration tree and select Extension.
	 Right click Extension and s Extension ID "8007" is ass Enter 50004 in the Extension Leave other parameters as c Click OK. 	select Add . signed by the Avaya IP Office. Leave it unchanged. on field. lefault.
	Manager [50.1.1.10] (C:\Program Fil	es\\Manager\) 00E007004990.cfg
	File Edit View Tools Window Help	
	IP Extension 50004	
	Extn VoIP	
	Extension ID	8007
	Extension	50004
	Caller Display Type	On 💌
	C Quiet Headset	
	C Paging Speaker	Minimum Width 2 - Clinit - 10ms
	 Standard Telephone 	Maximum Width 50 🚔 Unit - 10ms
	O IVB Port	Message Waiting Lamp Indication Turce
		None
		Beset Volume After Calls
	Hook Persistency Units - 1ms 100	

Step	Description
	 Select the VoIP tab. Select G.711 ULAW 64K codec for Compression Mode. Check Out Of Band DTMF. Check Allow Direct Media Path. Click OK when done.
	Manager [50.1.1.10] (C:\Program Files\\Manager\) 00E007004990.cfg File Edit View Tools Window Help
	IP Extension 50004
	IP Address Silence Suppression Voice Pkt. Size 160 Compression Mode G.711 ULAW 64K Compression Mode G.711 ULAW 64K Cocal Tones Enable RSVP Voit Of Band DTMF MAC Address Allow Direct Media Path
	OK <u>C</u> ancel <u>H</u> elp
	Follow Steps 4 and 5 to create extensions for Avaya 3616 and 3626 wireless IP Telephones.

Step	Description
6.	Save changes to the IP Office.
	 Under the Manager File Menu item, select Save. At the Sending Config to dialog box, select the option to immediately reboot and press OK. If the IP Office Server IP address has been changed, update the IP address of the PC running IP Office Manager and edit the IP Office Manager "Preferences" setting under the File menu before reconnecting.

5. Verification Steps

The following verification steps were used in these Application Notes to verify correct system operation:

- Verify network connectivity by launching pings between the IP406 Office and the wireless laptop PC. Verify that all pings are successful.
- Enable WEP on both IP Wireless Telephones.
- Power up the Avaya 3616 and 3626 IP Wireless Telephones and verify that they can register with IP406 Office.
- Make a call between these two IP wireless Telephones and verify that the voice quality is good.
- Make a call from the 3626 IP Wireless Telephone to the 4620SW IP Telephone, and verify that the voice quality is good.
- While the call is up, make a conference call to the 4620SW IP Telephone. Verify that all three parties are in conference call and voice quality is good.
- Enable 802.1x on the Odyssey Client and verify that the RADIUS server can authenticate the client. The following screen capture shows the connection status. Note that, under the **Connection information**, the **Status** shows **open and authenticated**. The blue color on **Odyssey** icon shows the client is connected and authenticated. The blue color on the **Key** icon shows that data is encrypted using dynamic keys (TKIP).

💩 Odyssey Client A	Aanager 📃 🗖 🔀
<u>S</u> ettings <u>C</u> ommands	Web Help
	Connection Adapter: RoamAbout 802.11 a/b/g Client PC Card
Profiles	Adapter type: wireless
+++Networks	Connect to network: ++ <raa></raa>
Auto-Scan Lists	Connection information
Trusted Servers	Status: open and authenticated
Adapters	Network (SSID): RAa Access point: EnterpriseAP IP address: 20.1.1.126 Packets in/out: 174 / 139
	Reconnect Reauthenticate

• Click icon 🧟 to show the last authentication results.

🕹 Ody	S Odyssey Client Manager							
<u>S</u> ettings	<u>C</u> ommands	<u>W</u> eb <u>H</u> elp						
- C- C	Connection	Connection Adapter:	RoamAb	out 802.11 a/b/g Client	PC Ca	ard 🔻		
€ •	Profiles	Adapter type:	wireless					
*	letworks	Connect t	o network:	💠 <raa></raa>		•		
**	Auto-Scan Lists	Connection	information		50	ca <u>n</u>		
Г <mark>Б</mark> т	rusted Servers	Status: Elapsed time:		open and authenticate 00:11:54	ed	Last auth	entica	ation results
<i>S</i> •	Adapters	Network (S Access poi IP address: Packets in/	SID): nt: 'out:	RAa EnterpriseAP 20.1.1.126 424 / 250		Result: Type: Elapsed time Cipher suite: Access poir	e: : ntid:	Success EAP-PEAP/v1 [EAP-MS-CHAP-V2] 00:11:50 0016 (DHE-RSA,3DES-EDE-CBC,SHA) networkid=RAa,nasid=EnterpriseAP
		<u>R</u> ecor	nnect	Reauthenticate		بي		

• Click the **Key** icon to show the Key Encryption.

🕹 Odyssey Client A	🕹 Odyssey Client Manager							
<u>S</u> ettings <u>C</u> ommands <u>W</u> eb <u>H</u> elp								
	Connection Adapter: RoamAbout 802.11 a/b/g Client PC Card							
Profiles	Adapter type: wireless							
+++Networks	Connect to network: ++ <raa></raa>							
Auto-Scan Lists	Connection information							
Trusted Servers	Status: open and authenticated Elapsed time: 00:18:19							
Adapters	Network (SSID): RAa							
	Access point: EnterpriseAP Encryption							
	IP address: 20.1.1.126 Pairwise cipher: TKIP Packets in/out: 663 / 377 Group cipher: TKIP							
	Reauthenticate							

- Launch PhoneManager Pro and verify that the PhoneManager can register with IP406 Office.
- Make a call from the PhoneManager Pro to the 4610SW IP Telephone and verify that voice quality is good.

6. Conclusion

These Application Notes illustrate the procedures necessary for configuring the Enterasys Wireless Access Point 3000 (RBT3K-AG) to support Avaya IP406 Office, Avaya IP Wireless Telephones and Avaya Phone Manager Pro. The Enterasys Wireless Access Point 3000 (RBT3K-AG) is able to support 802.11a/b/g radio, WPA with 802.1x authentication as well as WEP encryption.

7. References

Use this URL <u>http://avaya.com/gcm/master-usa/en-us/pillars/iptelephony/index.htm</u> to access these Application Notes.

- Application Notes for Configuring 3Com Wireless LAN Access Point 8750 to Support Avaya Communication Manager, Avaya IP Wireless Telephone and Avaya IP Softphone - Issue 1.0
- [2] Configuring the Avaya 3606 Wireless Telephone with Compatible 802.11b Access Points from Avaya and Other Vendors Issue 1.0
- [3] Configuring the Funk Odyssey Software, Avaya Access Point 3 and Avaya 802.11a/b Wireless Client for User Authentication (802.1x) and Data Encryption Issue 1.0
- [4] Implementing Encrypted Conversations between Avaya Softphone Endpoints with Avaya IP Office 403 and Avaya S8300 Media Server Issue 1.0

Use this URL <u>http://www.funk.com</u> to access the configuration documentations for Odyssey products.

©2005 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by \mathbb{R} and TM 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 Developer*Connection* Program at devconnect@avaya.com.