ADSP Access Point Test How-To Guide

Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. The Symbol logo is a registered trademark of Symbol Technologies, Inc., a Zebra Technologies company. © 2016 Symbol Technologies, Inc.

Table of Contents

1	Introduction	5
2	System Diagram	5
3	Licensing AP Test	7
4	Configuring AP Test	8
	4.1 Scheduled AP Tests	9
	4.2 Managing APT Profiles	10
	4.2.1 Creating APT Profiles	10
	4.2.2 Deleting APT Profiles	19
	4.2.3 Scheduling AP Tests	19
	4.3 On-Demand AP Tests	21
	4.3.1 Initiating AP Tests	22
	4.3.2 Analyzing Test Results	23
	4.3.3 Saving APT Configuration	26
	4.4 Configuring AP Test in Action Manager	26
5	Interpreting AP Test Alarms	29
6	Supported Devices	

Table of Figures

Figure 1: ADSP System Architecture	6
Figure 2: No AP Test License Error	8
Figure 3: Launching Scheduled AP Test	9
Figure 4: Schedule AP Tests	10
Figure 5: Manage AP Test Profiles Window	10
Figure 6: Adding and Removing APT Profiles	11
Figure 7: Connectivity Profile Window	12
Figure 8: APT - Station Tab Configuration	14
Figure 9: APT – Captive Portal Configuration	15
Figure 10: APT - Network Tab Configuration	17
Figure 11: APT - Throughput Tab Configuration	18
Figure 12: Deleting APT Profiles	19
Figure 13: Scheduling an AP Test	20
Figure 14: Adding Scheduled AP Test	20
Figure 15: Launching On-demand AP Test	22
Figure 16: On-Demand AP Test Window	22
Figure 17: AP Test Results Window	24
Figure 18: Packet Capture during AP Test	25
Figure 19: Saving APT Profile	26
Figure 20: Action Manager Main Window	27
Figure 21: Creating AP Test Action Rule	27
Figure 22: Selecting AP Test Action	28
Figure 23: Selecting Scope and Alarms for AP Test Action	28
Figure 24: Expert Help on AP Test Alarms	29

Document Conventions

The following graphical alerts are used in this document to indicate notable situations:

- √
 - **NOTE** This symbol indicates something of special interest or importance to the reader. Failure to read the note will not result in physical harm to the reader, equipment or data.



CAUTION This symbol indicates that if this information is ignored, the possibility of data or material damage may occur.



WARNING! This symbol indicates that if this information is ignored the possibility that serious personal injury may occur.

1 Introduction

Access Point (AP) Test is part of the advanced troubleshooting module of the AirDefense Services Platform (ADSP.) AP Test is a tool that helps you (as an IT administrator) to track network failures using an automated or manual AP connectivity test. You can create test profiles to verify the availability of different network components and application servers right from Layer-2 to Layer-4.

AP Test generates alarms to indicate a failure of one or more of the test conditions in the test profile. These alarms indicate high priority events that may be preventing the wireless applications from operating properly. An Action can be set up for each alarm; for example, to send an e-mail notification to appropriate the network administrator so that corrective action can be taken.

2 System Diagram

The following figure depicts system components involved in an AP Test. In order to use AP Test functionality, the deployment should have an AirDefense appliance with one or more Sensors, or radio share enabled Access Points.

Sensors or radio share enabled AP collect frames transmitted by 802.11a-b-g-n compliant devices, and sends that data to a central ADSP server for analysis and correlation.

ADSP provides the most advanced wireless LAN troubleshooting with a distributed architecture of remote Sensors or radio share enabled AP that communicate with a centralized server.



Figure 1: ADSP System Architecture

The AP Test is accomplished by using a deployed Sensor as a wireless station to connect to an AP and validating appropriate network resources (layer-2 to layer-4) that can be reached.

AP Testing allows validation of wireless authentication, encryption, DHCP, ACL and firewall testing, general network connectivity, and application availability testing. These connectivity tests can be run automatically or manually providing proactive notification that the network resources may be unavailable.

3 Licensing AP Test

AP Test is part of the Advanced Troubleshooting Module and requires a license for unlocking this functionality in the ADSP appliance.

AP Test requires a license for each device, where the device can be a Sensor or a radio share enabled AP. Note that, the Sensor can be a dedicated Sensor device or a dual-radio AP where one radio is configured for a Sensor and other for WLAN mode.

Radio Share AP Test license can be used in environments where there are no dedicated Sensors. Customers with the existing WLAN infrastructure can benefit from radio share license to gain access to Advanced Troubleshooting tools and maximize the return on their WLAN investment.

Part Number	Description
AD-APSN-P-1	AirDefense AP Test license for one (1) Sensor.
	NOTE Must add a first-year maintenance/service program to this
	product SKU.
AD-APRS-P-1	AirDefense Radio Share AP Test license for one (1) AP.
	NOTE Must add a first-year maintenance/service program to this
	product SKU.
ADB-NARS-P-1	AirDefense Radio Share license, Network Assurance bundle for
	one (1) AP. Includes: AP Test, Adv. Forensics, Connectivity
	Troubleshooting, LiveRF and Spectrum Analysis.
	NOTE Must add a first-year maintenance/service program to this
	product SKU.

The following table provides different licensing options for the AP Test module.

Table 1: License Options for AP Test

The license can be applied on an ADSP appliance. In ADSP version 9.x, you can apply the above licenses from **Configuration** > **Appliance Platform** > **Appliance Licensing** in the ADSP User Interface.

Note that, if you run an AP Test on a BSS, where there is no licensed Sensor or Radio Share enabled AP available, you will see the following error.

AP Test- AirDefense Shelter	
Scope: 🦣 Motorola:86:2c:75 [b,g,n]	
↓	Save Profile
Security Station Network Throughput	
SSID: DevMgmt_106	
Authentication: Open	
Key Generation: None 🗸	
Unicast Encryption: None	
Multicast Encryption: None	
Error	
There is no licensed sensor able to test this BSS.	
ОК	
Run Te	st Cancel

Figure 2: No AP Test License Error

Please refer to Section 6 for details on the supported firmware versions for different Access Point and Sensor models for using AP Test.

4 Configuring AP Test

AP Test can be run in two ways:

• The **Scheduled AP Test** is an automatic test that can be scheduled to run at any specific time in a day or a week. This provides proactive notification to the IT staff about any issues regarding the availability of wireless and wired network resources and application servers.

• The **On-Demand AP Test** is a manual test.

4.1 Scheduled AP Tests

To access the **Scheduled AP Test** window, you must select **Menu** > **Scheduled AP Test**, as shown below.



Figure 3: Launching Scheduled AP Test

The following window is displayed where you can schedule an AP Test. Please refer to next section for details on creating APT profiles.

🗷 So	hedule AP	Tests - ADSP					
🔶 Ad	id 📄 Edit 🗶	Delete 🛛 🥝 Cance	l Test 📳 View Res	ults 🛃 Manage Pr	rofiles		69
	Name	Profile	Scope	Last Test	Next Test	Test Duration	Last Result
							Close

Figure 4: Schedule AP Tests

4.2 Managing APT Profiles

Profiles make it easy to apply the same settings to different AP Tests. You can create different APT profiles to test networks with different SSIDs and authentication/encryption settings, or different resources on the network. These profiles can be modified or deleted if the network configuration or setup changes.

4.2.1 Creating APT Profiles

To create an APT profile, press the **Manage Profiles** button in the **Schedule AP Tests** window, as shown below.

Schedule AP Tests- ADSP								
🕂 Add 📄 Edit 🕽	🕻 Delete 🛛 🖉 Canc	el Test 💼 View Re	sult. 🚱 Manage P	rofiles		4		
Name	Profile	Scope	Last Test	Next Test	Test Duration	Last Result		
						Close		
L								

Figure 5: Manage AP Test Profiles Window

The following window displays. From here you can create and delete the profiles for AP Test.



Figure 6: Adding and Removing APT Profiles

Press the **Add** button to create an APT profile. This brings up the **Connectivity Profiles** window as shown below.

Connectivity Profiles		×
🕂 Add 💢 Remove	Profile Name: Temporary Profile Name	
Temporary Profile Name	Security Station Captive Portal Network Throughput	
	SSID: O2wirelessF61BA1	
	Authentication: Open 🗸	
	Key Generation: None 🗸	
	Unicast Encryption: None	
	Multicast Encryption: None	
	ОК	Cancel

Figure 7: Connectivity Profile Window

Enter a profile name and configure the following sections in the APT profile.

- Security— configures the SSID and authentication settings
- Station—configures MAC address, and IP/DHCP settings used for STA to connect to AP
- Captive Portal—configures input parameters for validation of captive portal service
- Network—configures Layer-3 tests
- Throughput—configures downlink throughput test.

Security Tab

The **Security** tab provides fields for configuration of security parameters like authentication, key generation, encryption, and passphrase for the BSS to be tested. The following table describes the various fields, which are dependent on the type of BSS being tested.

SSID	Service Set Identifier (SSID) of the Access Point.
Authentication	Type of authentication used to authenticate users on a local or remote (LDAP or RADIUS) server. Choices are Open , Shared Key , or NetworkEAP .

Key Generation	Method used to generate the keys that are necessary to encrypt data. Choices are None , 802.1x , PSK , or EAP .
Unicast Encryption	Encryption method used during unicast transmissions.
Multicast Encryption	Encryption method used during multicast transmissions.
WPA Protocol	(Wi-Fi Protected Access (WPA) method used to secure the connection to the wireless network. Choices are WPA or WPA2.
PSK Key	Pre-shared key (shared secret) used to authenticate user access to the AP.
Key Size	Key size used for a WEP key. Choices are 64 bits 10 hex digits or 128 bits 26 hex digits.
WEP Key	Wireless Equivalent Privacy (WEP) key used to authenticate user access to the AP.
Key Index	Index number used to identify a WEP key.
EAP Method	Extensible Authentication Protocol (EAP) method used in LAN authentication. Choices are LEAP, EAP/Fast Auto, EAP/Fast Manual, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, or PEAP- TLS. All methods except LEAP and EAP/FAST Auto, when selected, allow you to use certificates.
EAP Username	EAP username used in LAN authentication.
EAP Password	EAP password used in LAN authentication.

Station Tab

AP Test uses a Sensor as a virtual STA for its AP connectivity test. The **Station** tab allows you to configure the virtual station used during the AP test.

AC Address:	00:e0:d4:5b:6b:b0	Rando	m Address	Vendor Address
🔽 Obtain IP a	address using DHCP			
	IP Address:			
	Subnet Mask:			
	Default Gateway:			
🗸 Obtain DN	5 server address automa	tically		
Obtain DN:	5 server address automa Primary DNS:	tically		
Cbtain DN	S server address automa Primary DNS:	tically		

Figure 8: APT - Station Tab Configuration

The following fields are part of this tab.

MAC Address	Since AP Test uses a virtual station for its test, an artificial MAC address must be specified for the test station. The MAC address field is initialized to the most recently used test station MAC address. If no previous address is found, a random MAC address is used. You may change the MAC address by typing one in the field or click the Random Access button to generate one. You may also generate a MAC address by clicking the Vendor Address button and selecting a vendor from a list of vendors.
Obtain IP address using DHCP	You can obtain an IP address using DHCP or specify a static IP address. If you want to specify a static IP address, you must also specify the subnet mask and default gateway. The default is to obtain IP address using DHCP. Uncheck the checkbox to activate the fields and to specify a static IP address, subnet mask, and default gateway.
Obtain DNS server address automatically	You can obtain DNS server information automatically or specify the information yourself. The default is to obtain the information automatically. If you want to specify the information, uncheck the checkbox to activate the fields and then specify the primary DNS, secondary DNS, and domain name.

Captive Portal Tab

The **Captive Portal** tab allows you to configure AP Test for testing captive portal service running on the infrastructure device and validate whether the service is running correctly or not.

NOTE The upload throughput test is available from ADSP 9.0.3 release.

Capti	ve Portal			
Enable Captive Porta	Test			
Captive Portal Plugin:	Def •	import Export	Revert	
Response Timeout:	20 -	e test prome		
Walled Garden URLs:				+
User's Target URL: Verification text:				
Agreement / Login URL:				
Porm Name:		_		
Required Valuation.	Name	Туре	Value	-
Validation check URL:				
Welcome URL:				
Logout URL:				
			Run Test	Cancel

Figure 9: APT – Captive Portal Configuration

The following fields are part of this tab:

Enable Captive	Enable/disable captive portal testing in AP Test.
Portal Test	

Captive Portal Plug-in	Specifies captive portal plug-in containing information about the captive portal. The dropdown menu contains a list of plug-ins. You can import plug-ins with the Import button. You can export plug-ins with the Export button. The Revert button resets all fields to their previous stats. Some fields may be hidden because the information is contained in the plug-in. Selecting Show complete test profile reveals the hidden fields.
Response Timeout	Sets the response timeout for the initial redirected login page or post login page. The default response timeout is 20 seconds.
Walled Garden URLs	If the captive portal being tested supports the Walled Garden feature with a list of white list URLs, AP Test will verify that the system allows access to the white list. AP Test can verify a maximum of 5 URLs. This field is optional.
User's Target URL	Specifies an IP address or URL that will be checked by AP Test to ensure that it can't be accessed before captive portal log-in. The same URL will also be checked by AP Test to see whether captive portal grants access to it, after successful log-in.
Verification text	Specifies some text that appears on the target website as specified in User's Target URL.
Agreement / Login URL	Specifies the agreement web page or the login web page where a user has to accept the use policy or authenticate with a username and password.
Form Name	The form name used to submit acceptance of the use policy or authentication credentials.
Required validation	Provides a list of names that require validation. The name must be specified by type (dynamic or static) and value.
Validation check URL	Specifies the web page used to validate names in the Required validation field.

Welcome URL	Specifies a welcome page the user accesses once he/she has accepted the use policy or authenticated with a username and password. This field is optional.
Logout URL	Specifies a logout page after the user has terminated from the target URL.

Network Tab

The **Network** tab allows you to configure tests related to Layer-3 and above. You can include appropriate tests by enabling or disabling corresponding check boxes.

	Network			
Perform tra	ceroute to host googles.com			
Perform DN	S lookup on host name oodles.com			
	○ Resolve to any address ④ Re	solve to address	43.21.12.56	
Ping Hosts	Host	Expected Stat	us	÷
	Default Gateway	Pingable		-
	zomglols.com	Pingable		_
C Curr Durba		Deat		
Scan Ports	Host	PORC		~
	theinternets.com		80	-

Figure 10: APT - Network Tab Configuration

The following fields are part of this tab.

Perform trace route to host	Used to determine the route taken by packets across the network to the specified host.
Perform DNS lookup on host name	Used to determine DNS information of the AP on the specified host. You can resolve to any address or to a specific address.
Ping Hosts	Used to test the ability of the AP to communicate with the specified host by pinging the host.

Scan Ports	Used to conduct a port scan on the specified host.

Throughput Tab

The **Throughput** tab allows you to specify FTP server details to download or upload a test file during an AP Test and provide the acceptable downlink or uplink bandwidth speed. You can enable or disable throughput test by selecting or deselecting **Enable Download Test** or **Enable Upload Test** checkbox in the **Throughput** tab.

	Throughput	
C Enable Download	Test	
FTP Server Address:	10.59.39.107	
Path:	/upload/test.bd	(include file name)
Port:	21	
User:	admin	
Password:	•••••	
	Minimum acceptible bandwidth throughput	
	10 💠 bytes/s 👻 per second	

Figure 11: APT - Throughput Tab Configuration

The following fields are part of this tab.

FTP Server	Address IP address of your ftp server that you want to test.
Path	Full path of the file that you want to use in your test.
Port	Port number to your FTP server. (Usually 21 for FTP servers.)
User	User name used to log into the FTP server.
Password	Password of the user specified in the User field.
Minimum acceptable bandwidth throughput	Minimum bandwidth throughput that is acceptable to download (or upload) the test file. If bandwidth throughput is less than the specified value, an error occurs and is displayed in the Results.

18

Once you configure all the sections, Press **OK** in the **Connectivity Profiles** window to save the profile that was created.

✓ **NOTE** The upload throughput test is available from ADSP 9.0.2 release.

4.2.2 Deleting APT Profiles

To delete an APT profile, select the profile and press the **Remove** button in the **Connectivity Profiles** windows, as shown below.

Connectivity Profiles	
And X Remove Profile Name: APT-	Suest-Network
APT-Corporate Network Security Station	Network Throughput
SSID:	Guest-Network
Authentication	Open 👻
Key Generation:	None
Unicast Encryption:	None
Multicast Encryption:	None 👻
	OK Cancel

Figure 12: Deleting APT Profiles

4.2.3 Scheduling AP Tests

To schedule an AP Test, press the **Add** button in the **Schedule AP Tests** window as shown below.



Figure 13: Scheduling an AP Test

You will see the following **Add Scheduled AP Test** window, where you can select the APT profile, configure various parameters related to the scheduled AP Test, and enable the test.

Add Scheduled A	P Test	-	X
Tests Enabled			
Name:	Profile: APT-Corporate-Network - Edit		
Scope		Schedule	
Test all APs in	ADSP 🔹	One Time Schedule 👻	
Test a single AP		Time: 14:00 -	
Advanced		Date: 07/08/12	
Test Preference:	Over the Air (with OTA retries & single cell test where available)		
	 Single Cell (where unavailable, use OTA testing) 		
OTA Retry Count:	2		
	Switch sensors when retrying test		
Schedule Conflicts:	Skip test if sensor is in use		
	O Wait to run test until sensor is available		
	Wait no more than: Minutes 👻		
SSID Filter:	 Filter APs by profile SSID 		
	No SSID Filter		
Signal Threshold:	-70 dBm		
	Ignore APs with signal strength below the threshold		
Last Seen Threshold:	24 Hours 👻		
	Ignore APs with last seen time older than the threshold		
Parallel Tests:	20 👻		
			OK Cancel

Figure 14: Adding Scheduled AP Test

The following fields are part of this window. Once you set all the options, click **OK** to schedule the AP Test.

Name	Name of this scheduled AP Test.

Profile	Choose the profile from the list of APT profiles created earlier.
Edit	Click this button to edit any APT profile.
Scope	The Scope section is where you can limit the scope of your AP Test.
-	You can test all of the APs in a specific network level. You can also
	search and select one AP as your scope.
Schedule	There are five options to schedule a test: One Time , Intra-Day , Daily ,
	Weekly, or Monthly Schedule.
	Once you have selected an option, you must select a time and date
	for the test.
Advanced	The Advanced section is where you can select specific criteria for the
	test.
	Over the Air—Select to perform over the air AP Test. Typically used
	for testing APs using Sensors.
	Single Cell—Select this button to carry out the AP Test on a BSS
	whose radio is collocated in same physical AP as that of Sensor, or for
	radio share enabled AP/BSS.
	Retry Count—Specify the number of times the test should be repeated
	if not completed. You can elect to switch Sensors on each retry.
	Schedule Conflicts—Select to skip a test if the Sensor or profile is
	already in use or select to wait until the Sensor or profile is available. If
	you select to wait, you can specify how long to wait in minutes or
	hours.
	SSID Filter—Select whether or not to filter APs using the SSID
	specified in the profile.
	Signal Threshold—Select a signal strength that the AP must have in
	order to conduct the test. Any AP below the threshold is ignored and
	will not be tested.
	Last Seen Threshold—Specify a threshold in minutes, days, or hours
	that an AP was last seen on the network. Any AP that has a last seen
	time older than the one specified will be ignored and will not be tested.
	Parallel Test – Specify how many AP Test can be run in parallel while
	testing APs in a given scope.

4.3 On-Demand AP Tests

You can run an AP Test at anytime by using an on-demand test. The test can be initiated on any selected BSS or at network level.

4.3.1 Initiating AP Tests

To initiate the test on a specific BSS, go to **Network** tab and select **BSS** in the **Show** list box for any desired scope in the network hierarchy. This lists all BSSs in that scope. Select the BSS to be tested, Right click on it, and choose **AP Test** option as shown below to launch the AP Test.

1	lenu	Dashboard Ne	twork Alarms Config	uration		
C	15	Show BSS	- for	AirDefense Shelter	> 🎾 US-GA 🔹	Actions + Search
Þ		Device		Severity	Scope	SSID
	96	Motorola:2e:8a:4) 🕤	Safe(0)	🜍 GA27 🕤	nearbuy-cp
	99	Motorola:2e:a0.m	1.0	Safe(0)	💱 GA27 💿	DevMgmt_101
	10	Motorola:2e:	Alarms		🜍 GA27 💿	DevMgmt_102
	24	Motorola:2e:	Rename		🜍 GA27 🕤	DevMgmt_103
	24	Motorola:2e:	Remove		🜍 GA27 💿	DevMgmt_104
	14	Motorola:2e:	Classification		🜍 GA27 🕞	DevMgmt_105
	24	Motorola:2e:	Action Details		🜍 GA27 💿	DevMgmt_106
	14	Motorola:2e:	Forensic Analysis		💱 GA27 💿	DevMgmt_107
	94	Motorola:2e:	Cenerate Tracker Files		🜍 GA27 💿	DevMgmt_WPA
	94	Motorola:2f:8	Live View		🜍 GA27 💿	automation-open
	24	Motorola:2f:8	Port Lookup (Find this device)		💱 GA27 💿	automation-wep
	96	Motorola:2f:t	Terminate		🜍 GA27 💿	automation-wpa-tkip
	94	Motorola:2f:8	Wireless Vulnerability Assessme	int	🜍 GA27 💿	automation-eap
	94	Motorola:3f:a	Conv MAC		🜍 GA27 🕤	DevMgmt_102
	94	Motorola:3f:a	Settings		🜍 GA27 🕤	DevMgmt_103
	94	Motorola:3f:a	Global Settings		💱 GA27 🕤	DevMgmt_104
	94	Motorola:3f:a	About Adobe Flash Player 11.3.3	300.268	🚱 GA27 🕤	DevMgmt_101
	94	Motorola:3f:aa:80		Safe(0)	🕄 GA27 🕤	

Figure 15: Launching On-demand AP Test

You will see the following AP Test screen.

🔝 AP Te	AP Test- ADSP							
Scope:	Scope: 💫 Symbol:e5:bb:63 [b.g]							
Sensor:	Sensor: 🖉 ap650-859A08 [a,b,g,n] Thu Nov 15 11:18:00 GM32 -							
[▼]	Save Profile					
Security	Station	Captive Portal Network Throughput						
	SSID							
Aut	hentication	Open	•					
Key	Generation	None	•					
Unicast	Encryption	None	•					
Multicast	Encryption	None	•					
		Run Test	Cancel					

Figure 16: On-Demand AP Test Window

The Scope field indicates the scope in which the BSS being tested is present.

The **Sensor** field indicates the Sensor to be used during the AP Test. The system lists all available Sensors to test the chosen BSS and automatically selects the Sensor with the strongest signal for testing this AP/BSS.

The **Profile** list box displays the name of the AP Test profile, if any, used for the AP Test.

The **Save Profile** button saves the current settings to a profile that you name.

The APT configuration involves consists of the following tabs:

- Security—configures the SSID and authentication settings.
- Station—configures MAC address, and IP/DHCP settings used for STA to connect to AP.
- Captive Portal—configures input parameters for validation of captive portal service.
- Network—configures Layer-3 tests.
- Throughput—configures the download link throughput test.

In most cases, you will not have to change any of the fields in the **Security** tab, as Sensor populates them automatically, except the user name, password, PSK key etc.

Please refer to Section 4.2.1 for more details on configuration of all these tabs.

The **Run Test** runs the AP Test with the chosen test configuration.

The **Cancel** button closes AP Test without the test.

4.3.2 Analyzing Test Results

After initiating the AP Test, the results of the test will be displayed in the **Results** window. You can see the real-time status information as the test progresses.

- Access Point field indicates the Access Point that was tested.
- **Sensor** field indicates the Sensor that was used for testing the Access Point.
- Station field indicates the virtual station used during the AP Test.

The **Summary** tab displays a list of what was tested. Each of the tested items is marked as a success (green mark) or failure (red flag). You can press on the failed test items to get more information on the status of the failure.



Figure 17: AP Test Results Window

The **Packets** tab displays frames captured during the AP Test, which is quite useful for debugging any failures during the AP Test. There are two views in this window: table and connection ladder. By default, you will see the table view as shown below.

AP Test Complete								
Access P	oint: እ 172.17.	.25.21 [a.n] Se	nsor: 💋 10.59.	36.37 [a.b.g]	Station: (00:5	::24:10:20:ca	
Summar	y Packets							
Time	Source	Destination	BSSID	Cha Rate	Sig	Size	Protocol	
13:07	172.17.25	Broadcast	172.17.25	6 1 Mbo	62	91	Beacon	
13:07	APT-Custo	172.17.25.2	172.17.25	6 1 Mbp	N/A	50	Probe request	4
13:07	172.17.25.	APT-Custor	172.17.25:	6 1 Mbp	-46	85	Probe response	6
13:07	APT-Custo	172.17.25.2	172.17.25	6 1 Mbp	N/A	30	Authentication	
13:07	APT-Custo	172.17.25.2	172.17.25	6 1 Mbp:	N/A	30	Authentication	
13:07	\$ 172.17.25.	🧟 APT-Custor	172.17.25	6 1 Mbp:	; -44	38	Authentication	
13:07	Interview APT-Custo	172.17.25.3	172.17.25	6 1 Mbp:	N/A	60	Association re	
13:07	172.17.25.	👌 APT-Custor	172.17.25	6 1 Mbp:	52	54	Association re	
13:07	Interview APT-Custo	r 🛅 Broadcast	172.17.25	36 1 Mbp:	N/A	360	DHCP Discover	
13:07	🥥 00:0f:66:0a	: 🔨 Broadcast	172.17.25	36 1 Mbp:	; <mark>-</mark> 55	608	DHCP Offer	
13:07	Interview APT-Custo	r 喧 Broadcast	172.17.25	36 1 Mbp:	N/A	360	DHCP Request	
13:07	Interview 👌 👌	r 🗓 Broadcast	172.17.25	36 1 Mbp:	s N/A	360	DHCP Request	
13:07	🥥 00:0f:66:0a	🐚 Broadcast	172.17.25	36 1 Mbp:	; 🚺 -46	608	DHCP ACK	
13:07	Interview 👌 👌	r 🗓 Broadcast	\$ 172.17.25	36 1 Mbp:	N/A	60	ARP Request	
13:07	Interview 👌 👌	r 🐚 Broadcast	172.17.25 :	36 1 Mbp:	N/A	360	DHCP Release	
13:07	Interview APT-Custo	172.17.25.2	172.17.25	36 1 Mbp:	N/A	26	Disassociation	
13:07	🥥 00:0f:66:0a	: 🌛 APT-Custor	172.17.25 :	36 1 Mbp:	; 50	60	ARP Response	

Figure 18: Packet Capture during AP Test

4.3.3 Saving APT Configuration

You can save the current AP Test configuration into a profile for later use. Once you configure APT, press the **Save Button** on the main APT window to save the current configuration.

You will see the following window prompting you to name the profile. These saved profiles can be used for testing different networks, or for automatic testing using Scheduled AP Test or Action Manager.

Save Profile	×
APT-Corp-Network APT-Public-Network	
Test-APTest	
Profile Name:	
	Save Cancel

Figure 19: Saving APT Profile

4.4 Configuring AP Test in Action Manager

The Action Manager can be configured to run AP Test automatically based on any events (for example, performance alarms) generated by ADSP. You can invoke Action Manager from Menu > Action Manager from the main GUI.

📉 Action N	Action Manager- ADSP					
🚽 Add 🛃 Edit 🔄 Copy 💥 Delete						
Name	Actions	Scope	Alarms	Exceptions	Advanced Filter	User
						Close

Figure 20: Action Manager Main Window

To select the AP Test action, click the **Add** button and enter the name for action rule, as shown below.

🔝 Edit A	Action Rule- ADSP	×
Settings	Actions Filter Advanced Filter	
Rule	e Enabled	
Name:	Congestion-AP-Test	
Notes:		
	0	Cancel

Figure 21: Creating AP Test Action Rule

In the Action tab, press the plus (+) button and you will see list of actions. Select **AP Test**, as shown below. The **AP Test** action runs an AP Test using the specified profile if the conditions defined in the **Filter** and **Advanced Filter** tabs are met.

Edit Action Rule- ADSP					
Settings Actions Filter Advanced Filter	з.				
					
AP Test Profile:	APT-Corporate-Network 💌 Edit				
	OK	Cancel			

Figure 22: Selecting AP Test Action

The **Filter** tab is where you define the scope, alarms and exceptions for an Action Rule for AP Test, as shown below. If an alarm is raised by devices within the scope selected, ADSP triggers the **AP Test** action. The **Advanced Filter** tab allows you to build a custom alarm filter.



Figure 23: Selecting Scope and Alarms for AP Test Action

5 Interpreting AP Test Alarms

When a scheduled AP Test is carried out on a BSS, AP Test generates alarms if it is unable to reach out to network resources like DHCP, or encounters connectivity failures. These alarms can be viewed from the **Alarms** tab in the main GUI.

To find the description on all alarms related to AP Test you need to perform the steps below.

- 1. Go to Configuration > Operational Management > Alarm Configuration.
- 2. Select Performance > AP Testing.
- 3. Finally, select the desired alarm and press **View Expert Help** to get details on when this alarm would be generated and how to mitigate this failure condition.

Appliance Platform				
Security & Compliance				
Network Assurance	Anomalous Behavior	Name: Ping Test Failure <u>Revert to default settings</u> <u>View Expert Help</u>		
Infrastructure Managem	Exploits	Category: Performance > AP Testing		
Initiasti actare Hanageni		Criticality: O Major(50)		
Operational Management	E Performance	, i i i i i i i i i i i i i i i i i i i		
Alarm Configuration	E AP Testing			
Device Age Out	AB Test Incomplete	Device Type(s): 🕥		
Job Status	Base 802.11 Connection Failure			
Location Based Services	Captive Portal Failure	Duration: 3 Hours		
Location Subscriber Profiles	Captive Portal: Access Denied	10010		
Pending State Audit	Captive Portal: DNS Look-up Failed	✓ Enabled		
Sensor Only Settings	Captive Portal: HTTP Error	Enabled for sanctioned devices		
Sensor Operation	Captive Portal: Is Not Enabled			
	Captive Portal: Unable To Access Walled Gar Captive Portal: Unexpected Post Login Page	Enabled for unsanctioned devices Enabled for neighboring devices		
Account Management	DNS Response Invalid	Disabled for devices		
	Extended Authentication Failure	Disabled for devices		
	Failure Obtaining DNS Server Address from I			
	Failure Obtaining IP Configuration from DHC			
	Ping Test Failure			
	Port Scan Test Failure			
	Sensor Selection Failure			
	📈 toroughput Test - Invalid Path To File			
	📈 Throughput Test Failure - Downlink Bandwidt			
	Throughput Fest Failure FTP Server Not Rea			

Figure 24: Expert Help on AP Test Alarms

✓ NOTE The AP Testing alarms are only generated by Scheduled AP Test, not by the on-demand AP Test.

6 Supported Devices

The following table lists the firmware support for sensor and radio-share based AP Testing for various AP models.

Product	Sensor-based AP Test	RadioShare-based AP Test
AP 300	No	No
AP 5131, AP 5181	No	No
AP 510, 520	Yes (From 5.3)	No
AP 7131	Yes (from v5.2.6)	Yes (from v5.2.6)
AP 7161	Yes (from v5.2)	Yes (from v5.2)
AP 650	Yes (from v5.0)	Yes (from v5.2)
AP 6532	Yes (from 5.1)	Yes (from 5.1)
AP 621, AP 6511, AP 622, AP 6521	Yes (from 5.2)	Yes (from 5.2)
AP 7181	Yes (from v5.4)	Yes (from v5.4)
AP 8132	Yes (from v5.4)	Yes (from v5.4)

Table 2: AP/Sensor Matrix for AP Test

For detailed descriptions and installation instructions for specific APs, refer to ADSP Infrastructure Management Supported Devices at the following URL: <u>www.zebra.com/support</u>.



Zebra Technologies Corporation. Lincolnshire, IL 60069 USA

Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. The Symbol logo is a registered trademark of Symbol Technologies, Inc., a Zebra Technologies company.

©2016 Symbol Technologies, Inc.

MN-002710-01 Rev A, January 2016