

AirDefense Services Platform 9.0 User Guide



TABLE OF CONTENTS

Chapter 1: Overview

AirDefense Services Platform Deployment	1-1
Components	1-1
Sensors	1-2
ADSP Appliance	1-2
Network Connections	1-2
Deployment Lifecycle	1-3
Overview	1-3
Organization of this Manual	1-3
Initial Appliance Configuration	1-4
Configuring Data Collection	1-4
Lean Back Monitoring	1-5
ADSP Appliance Connection Options	1-5
Keyboard and Terminal	1-5
Static IP Address	1-6
Serial Port	1-6
SSH	1-6
About the User Interfaces	1-7
Your Role as a User	1-7
How Your User Account Was Created	1-7
User Types	1-7
Additional Limitations	1-8
Effect of Limiting Users to a Scope	1-8
Managing Your User Preferences	1-8
Basic Navigation	1-9
Tree Structure	1-9
Device Search	1-9
Filters	1-9
Dashboard Drill Down	1-10
AirDefense Services Platform and Time	1-10
Alarm Time Reporting	1-10
Advanced Features	1-11

Chapter 2: The Basic System

Dashboard	2-1
Dashboard Components	2-2
Network	2-6
Network Filters	2-7
Actions	2-8
Alarms	2-9
The ADSP Alarm Model	2-9
Suppressed Alarm Repetition	2-9
How an Alarm is Generated	2-9
Duration	2-10
Example	2-10
Alarm Table	2-10
Alarm Filters	2-11
Alarm Categories and Criticality	2-11
Alarm Categories	2-11
Alarm Criticality	2-12
Alarm Details	2-12
Actions	2-14
Configuration	2-14
Appliance Platform	2-15
Appliance Licensing	2-16
Tree Setup	2-20
Auto-Placement Rules	2-22
Communication Settings	2-24
Polling	2-27
Relay Server	2-27
Import / Discover Devices	2-27
Security & Compliance	2-30
Security Profiles	2-30
Wired Network Monitoring	2-31
Network Assurance	2-31
Performance Profiles	2-31
Environment Monitoring	2-32
Infrastructure Management	2-33
Device Access	2-33
RF-Domain	2-34
Operational Management	2-35
Alarm Configuration	2-35
Device Age Out	2-37
Job Status	2-38
Location Based Services	2-39
Pending State Audit	2-39
Sensor Only Settings	2-39
Sensor Operation	2-40
Account Management	2-42
Account Access	2-42
Authentication	2-46
User Preferences	2-48
Password Reset	2-49

The Menu	2-50
Open	2-51
Frame Capture Analysis	2-51
Spectrum Analysis	2-52
Forensic Analysis	2-52
Accessing Forensic Analysis	2-52
Forensic Time Window	2-53
Forensic Data	2-53
Action Manager	2-54
Add/Edit Action Rule	2-55
Action Control	2-57
Action Control Table	2-58
Action Control Commands	2-58
Reporting	2-58
Using Web Reporting	2-59
Using the Report Builder	2-60
Scheduled AP Test	2-66
Scheduled Vulnerability Assessment	2-67
Appliance Manager	2-67
Navigation	2-67
System Settings	2-67
Backups	2-70
Banner	2-74
Certificates	2-75
SSH	2-77
Scheduled Events	2-77
Monitoring Schedule Events	2-77
Altering Event Schedules	2-78
Auto Classification	2-79
Navigation	2-79
On-Demand vs Scheduled Classification	2-79
Action Rules and Rule Sets	2-80
Add Devices	2-81
BSS and Wireless Clients Fields	2-82
All Other Devices Fields	2-83
Import and Discovery	2-83
Local File Fields	2-84
Remote File Fields	2-85
SNMP Discovery Fields	2-86
Wireless Manager/Switch Fields	2-88
Import File Formats	2-89
Devices	2-96
Access Point	2-96
BSS	2-96
Wireless Clients	2-98
Sensor	2-99
Wireless Switch	2-100
Wired Switch	2-101
Unknown Devices	2-101
WLSE	2-102
AirWave	2-102

Device Functions Requiring More Explanation	2-103
Network Levels	2-109
Appliance	2-109
Country	2-109
Region	2-110
City	2-111
Campus	2-111
Building	2-112
Floor	2-112
Unplaced Devices	2-113
Network Level Properties	2-113
Chapter 3: Security	
Introduction	3-1
WIPS	3-1
Planning Your Sensor Deployment	3-2
Deployment Considerations	3-2
Sensor Placement	3-5
Sensor Placement with WEP Cloaking	3-6
Sensor Placement With Location Tracking	3-7
Sensor Monitoring	3-8
Advanced Forensics	3-9
Scope Based Forensic Analysis	3-10
Device Based Forensic Analysis	3-11
Vulnerability Assessment	3-11
On-Demand Vulnerability Assessment	3-12
Automated (Scheduled) Vulnerability Assessment	3-13
WEP Cloaking	3-13
How Does WEP Cloaking Work?	3-13
What if there Is a Problem?	3-15
Are there any Recommendations?	3-15
How Do I Configure WEP Cloaking?	3-15
Tracker Integration	3-15
Chapter 4: WLAN Management	
Introduction	4-1
Infrastructure Management	4-2
Device Firmware	4-2
Channel Settings	4-2
Radio Settings	4-2
WLAN Profiles	4-3
General Tab	4-3
Security Tab	4-4
CLI Configuration	4-5
Adding a New Profile	4-7
Applying CLI Profiles	4-7
CLI Variables	4-8
Operational Management	4-9
Pending State Audit	4-9

Appliance Platform	4-9
Relay Server	4-9
Import Relay Server Information	4-10
Chapter 5: Troubleshooting	
Introduction	5-1
AP Test	5-1
On-Demand AP Test	5-2
Automated (Scheduled) AP Test	5-3
Forensic RF	5-6
Predictive RF	5-6
Assurance Suite (Network Assurance)	5-9
Radio Share Network Assurance	5-9
Chapter 6: Location Based Services	
Introduction	6-1
LBS Profiles	6-1
Reference Material	6-2
Chapter 7: Central Management	
Introduction	7-1
Effects on the Network Tab	7-2
Effects on the Alarms Tab	7-3
Effects on the Configuration Tab	7-4
Chapter 8: Zero Touch WLAN Infrastructure Deployment	
Introduction	8-1
Deployment Requirements	8-1
Setup Prerequisites	8-2
Chapter 9: ADSPAdmin	
Introduction	9-1
Using ADSPAdmin to Configure AirDefense Services Platform	9-1
Config	9-1
IP	9-2
IPv6	9-3
NETPORT	9-3
DNS	9-4
BONDING	9-4
HNAME	9-4
DNAME	9-4
TIME	9-5
TZ	9-5
NTP	9-6
SNMPA	9-6
SNMPC	9-6

SNMPT	9-7
HTTP	9-7
PANIC	9-7
UIPORT	9-8
Manage	9-8
Dbase	9-8
Software	9-9

ABOUT THIS GUIDE

Preface

This guide is designed to help you use AirDefense™ Services Platform (ADSP) to protect your network from wireless threats and attacks, and to maximize wireless network performance and enforce policy compliance.

This guide is intended for information security administrators and people who are responsible for reporting on and analyzing wireless LAN data.

Scope of Documentation

This guide covers:

- Appliance configuration
- Operational configuration
- Device Management
- Alarm Management
- Network Security
- WLAN Management
- Troubleshooting
- Managing multiple appliances

It does not cover initial hardware installation or the basic device configuration you need to perform to get the appliance up and running.

ADSP 9.0 is a DVD-ROM upgrade. Complete instructions for installing the service module are included in the publication *AirDefense Services Platform 9.0 Upgrade Instructions*.

What's in the User Guide vs ADSP Help

The User Guide provides reference about ADSP functionality. The User Guide explains the many features of ADSP and how these features can be used to monitor and maintain your network.

The ADSP Help system provides information about using the GUI to configure the system and evaluate data. The ADSP Help describes what you see in the GUI and how to use it. See the ADSP Help for quick information about how to do things.

Notational Conventions

The following conventions are used in this document:

- *Italics* are used to highlight the following:
 - Chapters and sections in this and related documents
 - Dialog box, window and screen names
 - Drop-down list and list box names
 - Check box and radio button names
 - Icons on a screen.
- **Bold** text is used to highlight the following:
 - Key names on a keypad
 - Button names on a screen or window.
- Bullets (•) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.



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.

Service Information

If you have a problem with your equipment, contact Motorola Enterprise Mobility Support for your region. Contact information is available at: <http://www.motorola.com/enterprisemobility/contactsupport>.

When contacting Enterprise Mobility Support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number.

Motorola responds to calls by E-mail, telephone or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Motorola Enterprise Mobility Support, you may need to return your equipment for servicing and will be given specific directions. Motorola is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

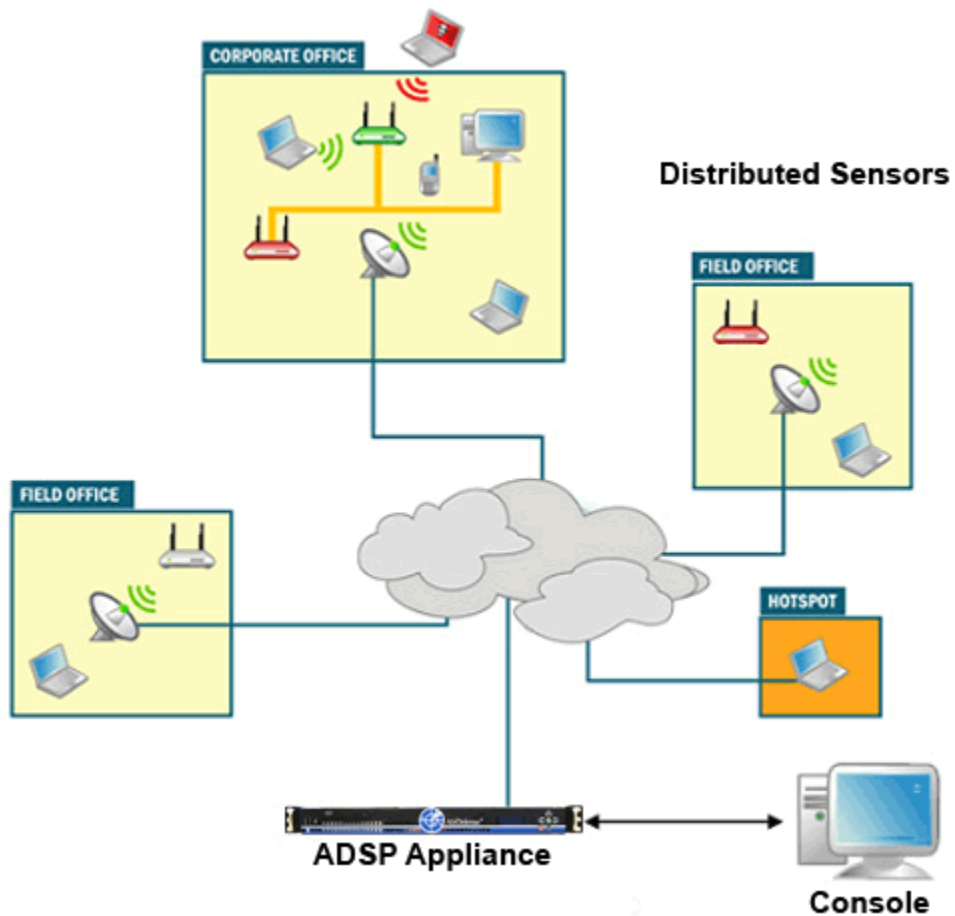
If you purchased your Enterprise Mobility business product from a Motorola business partner, contact that business partner for support.

CHAPTER 1 OVERVIEW

AirDefense Services Platform Deployment

Components

A basic AirDefense Services Platform system consists of an AirDefense Appliance and one or more sensors.



AirDefense Services Platform's remote sensors collect frames being transmitted by 802.11a-, b-, g-, and n-compliant devices, and sends that data to a central ADSP server for analysis and correlation.

ADSP provides the most advanced wireless LAN monitoring with a distributed architecture of remote sensors that communicate with a centralized server.

Sensors

WLAN monitoring requires a sensor in the vicinity of the airwaves carrying the WLAN traffic. The smart sensors from Motorola AirDefense passively observe all wireless LAN traffic within 40,000 to 60,000 square feet of typical office space.

Once the sensor collects wireless LAN traffic, the smart sensor analyzes the 802.11 frames and extracts meaningful data points to determine key attributes, such as:

- Wireless device associations
- Use of encryption and authentication
- Vendor identification of all devices
- Total data transferred.

By preprocessing the data on the sensor, the smart sensors greatly reduce the need for bandwidth. In most cases the communication from the smart sensor to the server is less than 3 kbps.

ADSP Appliance

As part of an ADSP system, the ADSP appliance is a true plug-and-play system with a hardened operating system, optimized database, automated database maintenance, and all application software included.

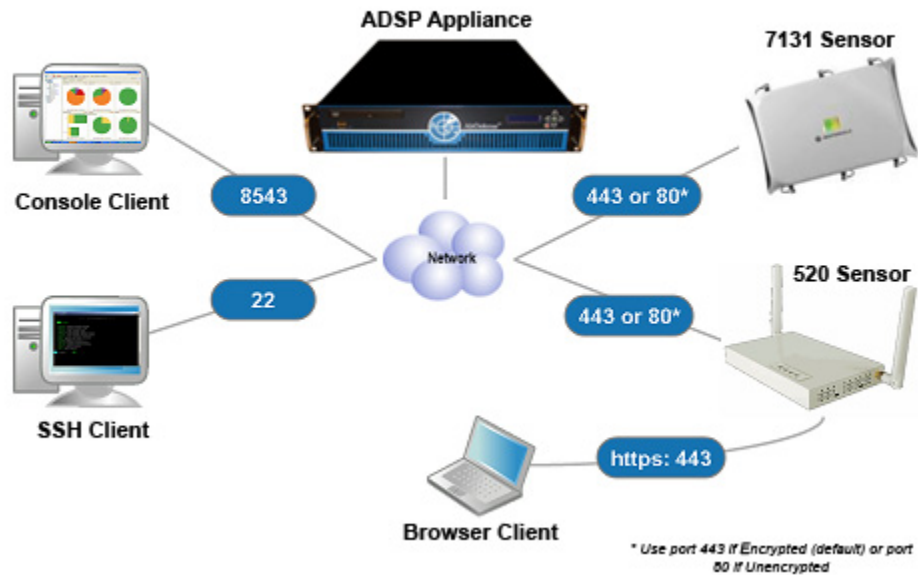
The ADSP appliance provides a scalable, secure, and manageable solution for enterprises to deploy in a single office or corporate campus. As an appliance, ADSP does not require an enterprise to buy, install, configure, lockdown, and support a server, operating system, and database. A true appliance comes ready with the application and all supporting software pre-loaded.

Network Connections

There are various methods for connecting with AirDefense Services Platform. Motorola AirDefense recommends using the most secure choice when possible. When connecting via browser, use SSL (HTTPS:443) when possible.

- Sensor-to-Server: may use unencrypted (port 80) or encrypted (port 443) communication.
- Sensor UI: new releases only allow encrypted access to the sensor UI (https: 443)
- Console-to-Server: must use encrypted (port 8543) communication.

- SSH client-to-server: must use encrypted (port 22) communication.



Deployment Lifecycle

Overview

AirDefense Services Platform is designed to be “self-managing,” meaning that after installation and an initial period of configuration activity, you should be able to focus your attention on analyzing data and responding to notifications that your specific organization is interested in. Periodic tuning should be minimal.

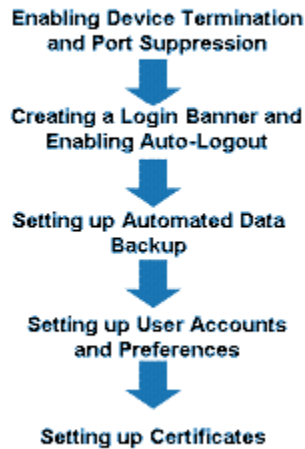
Organization of this Manual

This manual is organized to roughly reflect this deployment lifecycle. In this manual, the configuration activity is addressed as two phases: Initial Appliance Configuration and Configuring Data Collection.

Initial Appliance Configuration

The following graphic shows the basic activities in this phase.

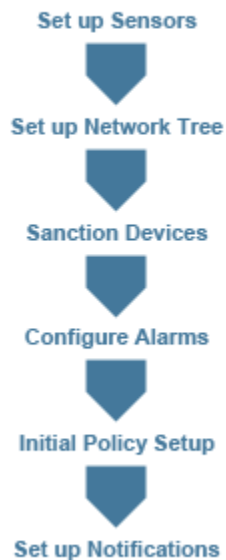
Initial Appliance Configuration



Configuring Data Collection

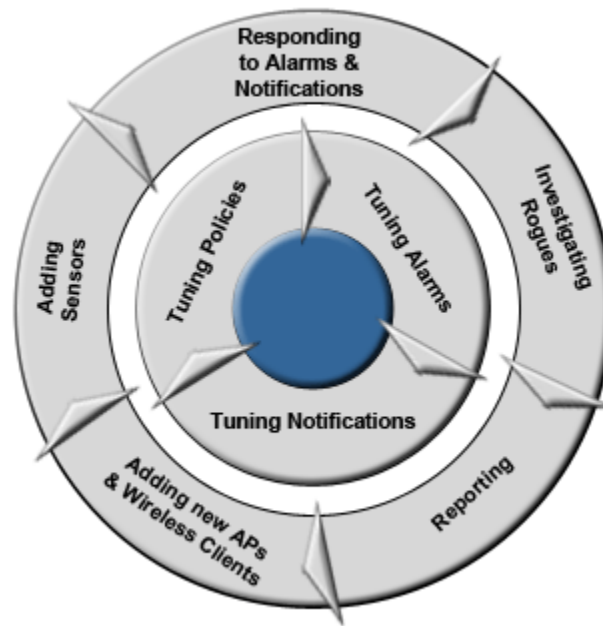
The following graphic shows the basic activities in this phase.

Configuring Data Collection



Lean Back Monitoring

The following graphic depicts the activities that constitute ongoing activities associated with monitoring your WLAN's security with AirDefense Services Platform.



ADSP Appliance Connection Options

There are four ways to communicate directly with your ADSP appliance:

- Keyboard and Terminal
- Static IP Address
- Serial Port
- SSH.

Keyboard and Terminal

You can physical access the server with a keyboard and terminal to communicate to communicate with the server. When using a keyboard and terminal, you can:

- Execute a fresh installation
- Configure a just shipped ADSP appliance
- Upgrade a server via CD
- Apply a Service Module
- Conduct Troubleshooting
- Access ADSPadmin.

Static IP Address

You can physically connect a laptop to the server's Ethernet port to communicate through an IP address. The IP address will always be 192.168.100.2 and must be configured by Motorola AirDefense Operations.

Serial Port

You can physically connect a laptop to the server's serial port to communicate with the server. This can be done only on 1150, 1250 and 3650 appliances. This feature is not available on 2230, 2270 and 4250 appliances. When communicating using the serial port, you can:

- Configure a just shipped ADSP appliance
- Apply a Service Module
- Conduct Troubleshooting
- Access ADSPadmin.

The following options must be set for the serial port:

- 9600 bits/second
- Databits "8"
- Parity "none"
- Stop bit "1"
- Software Flow Control.

SSH

You can communicate with a server using SSH on a workstation. The server must be configured with an IP address for network access. When communicating with SSH, you can:

- Apply a Service Module
- Conduct Troubleshooting
- Access ADSPadmin.

About the User Interfaces

You manage AirDefense Services Platform components using a combination of interfaces.

Each user interface has designated user names, passwords, and in, some cases, varying levels of privileges based on user roles. The table below describes the interfaces, the program area they manage, the functions within the program area, and the type of user required.

User Interfaces	Program area	Functionality	User
ADSP Command Line Interface	ADSPadmin (utilities)	Manage Dbase Software Config	Command Line User
ADSP Graphical User Interface (GUI)	AirDefense Services Platform	Dashboard Network Alarms Configuration Rogue Performance Compliance Forensic Intrusion Device Management Report Builder Reports Troubleshooting Downloads	User Note: In order to run the ADSP GUI, a minimum of 512MB of RAM is required and 1GB of RAM is recommended for the client workstation.
Sensor User Interface (sensor UI)	Motorola AirDefense sensor	Sensor Configuration	Sensor User

Your Role as a User

How Your User Account Was Created

AirDefense Services Platform has one default Admin user account. ADSP lets Admin users create numerous other users with role-based permissions that control which functionality each user can access. The Admin user who created your account assigned you a user role that determines whether or not you can use some ADSP features.

User Types

The four templates used to create user accounts and their permissions are:

- Admin—read and write access to all areas of ADSP server and sensor administration, including creation of other admin users.

- Guest—Gives users read permission to Alarm Management, Reporting, Analysis Tools, and Connection Troubleshooting. No access is provided for the other functional areas.
- Helpdesk—Gives users read/write permission to Connection Troubleshooting. No access is provided for all other function areas.
- Operation Center—Gives users read/write permission to all functional areas except Appliance Management, Network Management, and System Configuration. No access is provided for these three function areas.

The templates can be bypassed and user accounts can be customized to fit your needs.

Additional Limitations

The way AirDefense Services Platform is configured can have some other effects on how you use ADSP. Some of the features described in this book may not appear in the interface, or may be grayed out, depending on whether they are enabled or disabled.

Example: If Air Termination is disabled, you will not see options for using it.

Effect of Limiting Users to a Scope

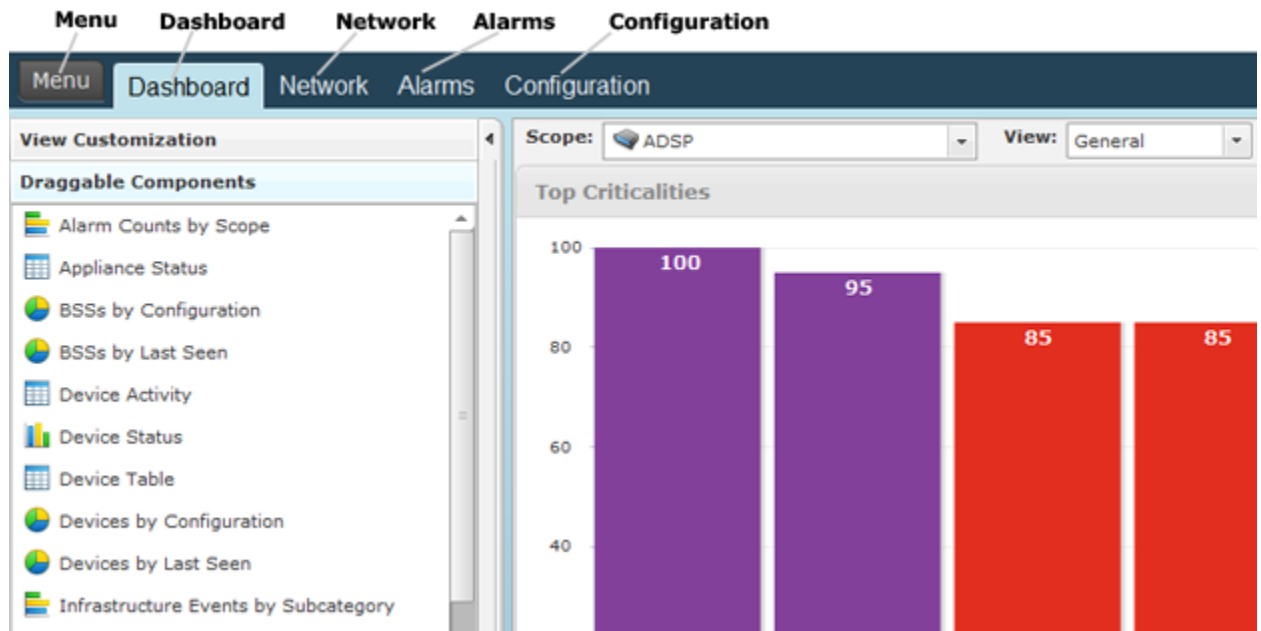
If the Admin user who configured your user account only assigns you a specific scope (network level) to access, you will only be able to view or use data for the part of the network assigned to you.

Managing Your User Preferences

No matter what user type you are, you can choose certain options, or user preferences, for how you view data in the GUI.

Basic Navigation

Understanding some basic concepts about the AirDefense Services Platform GUI will make it easy to navigate. The following graphic shows where to find the elements described below.



- **Menu**—Gives you access to the ADSP standalone features that are part of ADSP Toolkit.
- **Dashboard**—Provides a customizable view of your wireless LAN.
- **Network**—Displays a list of devices seen on your wireless network.
- **Alarms**—Displays an alarm table that shows all of the active alarms currently occurring on your network.
- **Configuration**—Allows you to configure devices plus perform other administrative tasks such as user and sensor administration.

Tree Structure

Whenever the tree structure is displayed, you can control the scope of the data you see in the right pane by selecting the appropriate network level in the tree. The scope you select in the tree is *persistent* while you drill down into the data in the right pane.

Device Search

The **Network** tab contains a search option that enables you to find specific devices that are being detected by ADSP.

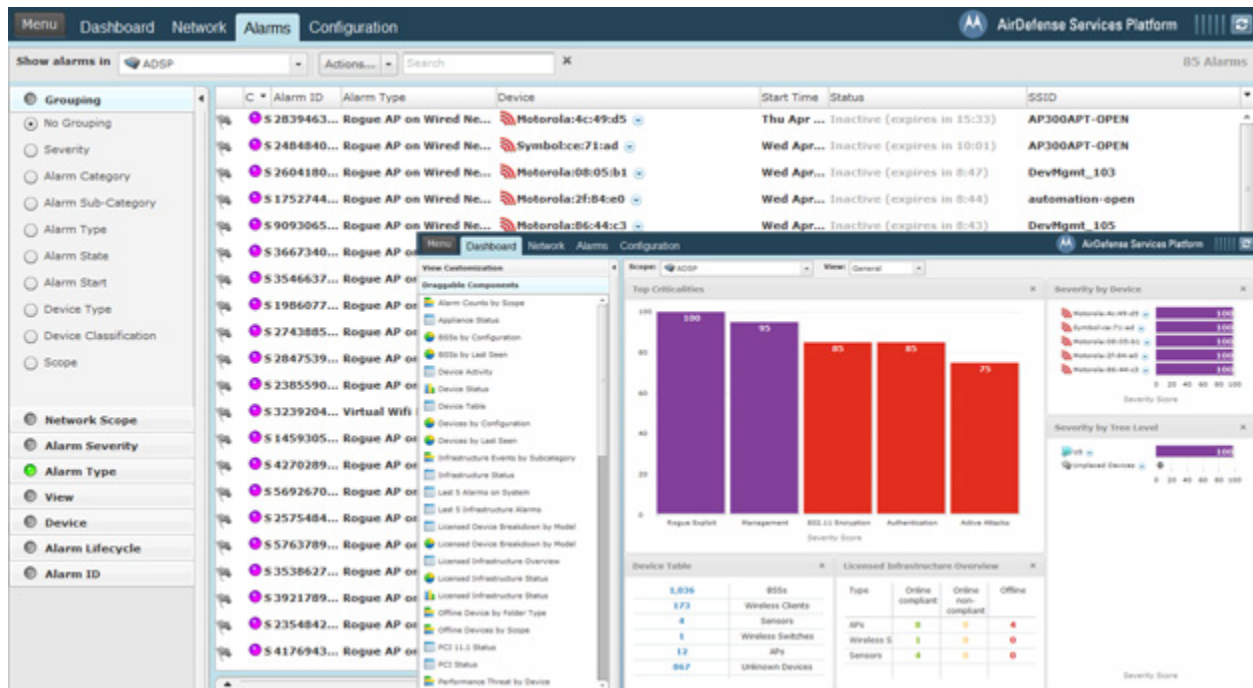
Filters

The **Network** filter and the **Alarm** filter make it easy to focus on the devices and alarms that are important to you. The **Network** filter is used in the Network tab while the Alarm filter is used in the **Alarm** tab. When you first access one of these tabs, all the data related to that tab is displayed. You can use filters to narrow down what you see.

Example: The **Network** filter can be used to view only devices that are displaying rogue activity.

Dashboard Drill Down

The dashboard lets you quickly assess your overall security and performance status, then lets you drill down into detailed information about the data the dashboard summarizes. You can then drill even farther down into specific device or event information. The following graphic shows dashboard drill-down.



By double-clicking the **Rogue Exploit** column in the **Top Criticalities** chart, the **Alarms** tab is displayed showing Rogue Exploit alarms.

AirDefense Services Platform and Time

ADSP reports alarms and device information, and traffic statistics, **every minute**.

To understand the data that appears in the ADSP, you must understand how ADSP addresses system time versus the local GUI time, particularly in regard to alarms.

Alarm Time Reporting

When an alarm occurs, ADSP detects the alarm in system time, and records this time in its database. You configure ADSP system time by using the Command Line Interface, found in the **Config** menu.

However, when reporting the alarm to the GUI, ADSP adjusts the report time to your local system time zone. It uses this time to report alarms in the **Alarms** tab, and it also reports other statistical data in this manner. The last updated time on each GUI screen (indicated by the time stamp) correlates to the local system where the browser is running. You configure the GUI time for your local system.

Advanced Features

Additional modules are available with a license that will give you an ADSP solution that fit your needs. You can add as little as one module or you can add them all.



Modules are categorized as follows:

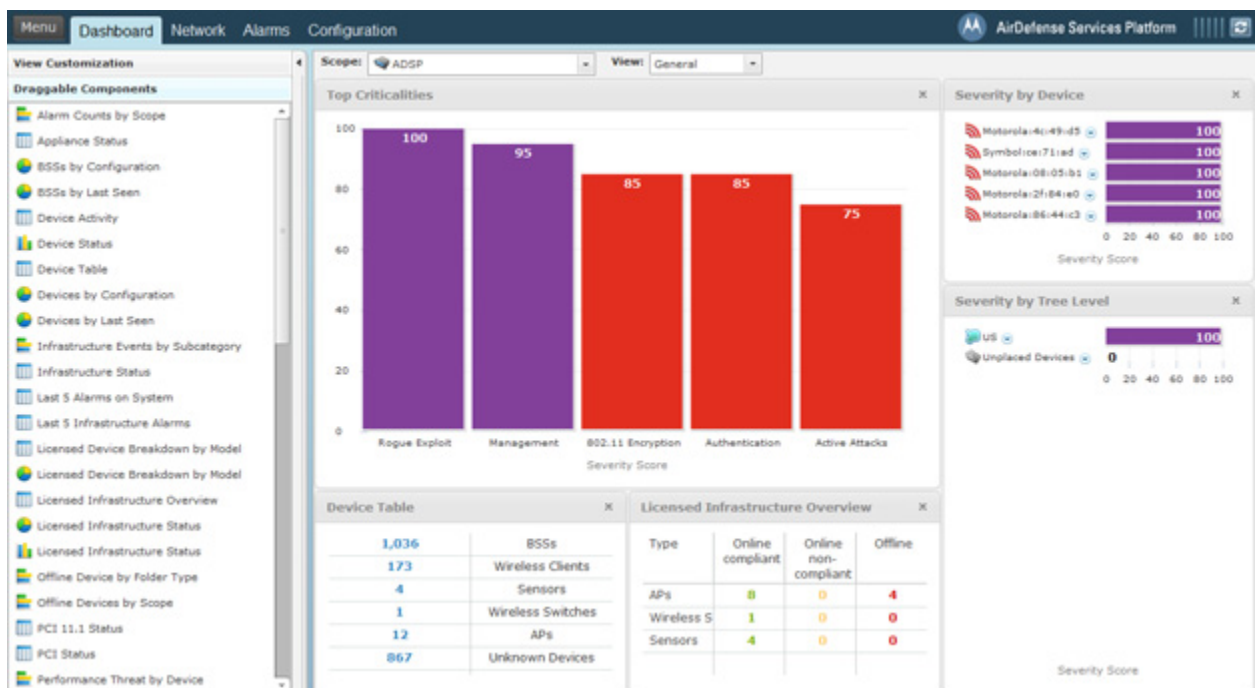
- Security
- Troubleshooting
- WLAN Management

Each of these categories are discussed in later chapters of this document. A Central Management module provides control over multiple appliances from one interface.

CHAPTER 2 THE BASIC SYSTEM

Dashboard

The Dashboard is designed to give you quick visualization of your network.



ADSP provides five default views involving the most important aspects of your network. Each view is fully customizable where you can add any one of the already defined dashboard components. The default views are:

- General—Displays general information about your network using some components of the other three views.

- Security—Displays security information about your network such as:
 - Rogue Wireless Access
 - Top Wireless Extrusions by Count
 - Top Wireless Exploits by Count
 - Policy Compliance
 - Security Threat by Tree Level
 - Security Threat by Device
 - Top Wireless Vulnerability by Count.
- Infrastructure—Displays infrastructure information such as:
 - Infrastructure Status
 - Last 5 Infrastructure Alarms
 - Device Breakdown by Model
 - Top Infrastructure Criticalities
 - Wireless Client Associations by WLAN
 - Radio Channel Breakdown.
- Performance—Displays performance information such as:
 - Performance Threat by Tree Level
 - Performance Threat by Device.
- Network—Displays network information to give you a picture quick glance of your network utilizing the following components:
 - Devices by Configuration
 - Appliance Status
 - Wireless IPS Availability
 - BSSs by Last Seen
 - Wireless Clients by Last Seen.

In addition to the default views, there are three user views which are fully customizable. The user definable views are initially empty, allowing you to add any of the dashboard components to create a mixture important to you.

Dashboard Components

The following components are available to customize the different views of the Dashboard:

Component	Description
Alarm Counts by Scope	Displays a bar chart showing the network levels with the top 5 alarm count.
Appliance Status	Displays the alarm status of the appliances on your network.
BSSs by Configuration	Displays a pie chart of BSSs by configuration (sanctioned, unsanctioned, and neighboring). Also lists the total number of BSSs seen on your network.
BSSs by Last Seen	Displays a pie chart of the BSSs seen on your network over the last five days. Also lists the total number of BSSs as well as the totals for each day.

Component	Description
Device Activity	Displays the active/inactive state of Unknown Devices, Wireless, Clients, and BSSs seen on your network in tabular form.
Device Status	Displays the active/inactive state of Unknown Devices, Wireless, Clients, and BSSs seen on your network in graphical form.
Device Table	Individually lists the total number of Sensors, Wireless Clients, BSSs, and Switches on your network.
Devices by Configuration	Displays a pie chart of devices by configuration (authorized, ignored, and unauthorized). Also lists the total number of devices seen on your network.
Devices by Last Seen	Displays a pie chart of the devices seen on your network over the last five days. Also lists the total number of devices as well as the totals for each day.
Infrastructure Events by Subcategory	Displays a bar chart showing infrastructure events by subcategory.
Infrastructure Overview	Displays a list of infrastructure devices in three columns (Online compliant, Online non-compliant, and Offline).
Infrastructure Status	Displays a list of infrastructure devices showing if they are online or offline, and the total number of each device type.
Last 5 Alarms on System	Displays a list of the last 5 alarms generated by ADSP.
Last 5 Infrastructure Alarms	Displays a list of the last 5 infrastructure alarms generated by ADSP.
Licensed Device Breakdown by Model	Displays a list of licensed devices on your network grouped by model.
Licensed Device Breakdown by Model	Displays a pie chart showing licensed devices on your network grouped by model.
Licensed Infrastructure Status	Displays a column chart showing the status of licensed infrastructure devices in your network.
Licensed Infrastructure Status	Displays a pie chart showing the status of licensed infrastructure devices in your network.
Offline Device by Folder Type	Displays a bar chart showing the offline devices and the folder type they reside in.
Offline Devices by Scope	Displays a bar chart showing the offline devices and the scope they reside in.
PCI 11.1 Status	Lists the compliance status of Rogue APs, Rogue Wireless Clients, and Accidental Associations as related to PCI Section 11.1. A green checkmark signifies you are in compliance. A red x signifies you are out of compliance.

Component	Description
PCI Status	Lists the compliance status of PCI Sections 2, 4, 11.1, and 11.4. A green checkmark signifies you are in compliance. A red x signifies you are out of compliance.
Performance Threat by Device	Displays a bar chart showing the threat score of the top devices violating your performance policy.
Performance Treat by Tree Level	Displays a bar chart showing the tree level threat score violations of your performance policy.
Performance Violations	Displays a pie chart showing the number of alarms generated by a performance violation. Also lists the overall alarm total as well as totals for individual alarms.
Policy Compliance	Displays a bar graph showing the alarm count for policy compliance.
Polled Wireless Client Associations by WLAN	Displays a pie chart showing polled Wireless Client associations by WLAN.
Quick Security View	Shows a quick view of possible security issues. A green checkmark indicates there are no issues. A red x indicates there is some type of issue.
Radio Channel Breakdown	Displays a pie chart showing configurable radios group by channel.
Radio Status	Displays the radio status by band (2.4 GHz and 5 GHz) and lists the online APs and Sensors. A count is displayed in the form of x of x.
Recent Outages	Lists devices with recent outages along with the associated appliance, start time of the outage, the type, and criticality.
Rogue AP Details	Shows BSSs and their associated scope per row. The table is sorted by alarm time with the device most recently detected on top of the table.
Rogue Wireless Access	Displays a bar chart showing the alarm count of rogue devices seen on your network.
Sanctioned Network	Displays a pie chart showing sanctioned devices on your network.
Security Alarm Counts by Scope	Displays the network levels with the top 5 alarm count using the following alarm types and sub-types: Anomalous Behavior, Exploits, Policy Compliance Violations, Reconnaissance, Rogue Exploit, Vulnerabilities.
Security Threat by Category	Displays a column chart showing the alarm count of security issues by category (Rogue Exploit, Vulnerability, Policy, and Extrusion).
Security Threat by Device	Displays a bar chart showing the threat score of the top devices violating your security policy.

Component	Description
Security Threat by Tree Level	Displays a bar chart showing the tree level threat score violations of your security policy.
Security View	Displays a bar chart showing the number of security alarms generated by ADSP.
Severity by Device	Displays a bar chart showing the severity scores of the top offending devices.
Severity by Tree Level	Displays a bar chart showing the severity scores of the top offending network levels.
Signal Strength Status	Displays a pie chart showing the number of clients and APs greater than or equal to -70dBm, and the number of clients and APs less than -70 dBm.
System Load	<p>Displays a column chart reflecting system load. Charts include percentages for:</p> <ul style="list-style-type: none"> • Sensor count • Managed network devices • Total device load • Active device load.
Termination Count by Scope	Displays a bar chart showing a total termination count by scope.
Termination Status	Displays a pie chart showing the number devices not on the termination list and number of devices on the termination list.
Top Criticalities	Displays a column chart showing top alarms observed by ADSP.
Top Infrastructure Alarms by Count	Displays a bar chart showing the top infrastructure alarms by count.
Top Infrastructure Criticalities	Displays a column chart showing the to infrastructue alarms observed by ADSP.
Top Performance Alarms by Count	Displays a bar chart showing the alarm count of the top performance policy violations.
Top Security Alarms by Count	Displays a bar chart showing the alarm count of the top security policy violations.
Top Talkers	Displays a bar chart showing the top 5 BSS and Wireless Client talkers on the network based on the combined value of sensed total TX and total RX bytes.
Top Wireless Exploits by Count	Displays a bar chart showing the alarm count for wireless exploits on your network.
Top Wireless Extrusions by Count	Displays a bar chart showing the alarm count for wireless extrusions on your network.

Component	Description
Top Wireless Vulnerability by Count	Displays a bar chart showing the alarm count for wireless vulnerability on your network.
Wireless Client by Configuration	Displays a pie chart of Wireless Clients by configuration (authorized, ignored, and unauthorized). Also lists the total number of Wireless Clients seen on your network.
Wireless Client by Last Seen	Displays a pie chart of the Wireless Clients seen on your network over the last five days. Also lists the total number of Wireless Clients as well as the totals for each day.
Wireless IPS Availability	Lists a count of online and offline Sensors on your network.

Network

The **Network** tab displays a table of the devices seen in your wireless network.

Device	IP	Severity	Last Seen	Scope	Floor	Model	Firmware	Status	Sensor...	Compliant
ap7131-14C28C	10.59.36.32	Critical	Thu Apr 12 2012 03:46:08 PM	The Falls 1125	AirDefense 2	AP7131	5.3.0.0-088R	uptime 6	Online	audited Thu A
10.59.36.37	10.59.36.37	Critical	Thu Apr 12 2012 03:45:59 PM	The Falls 1125	AirDefense 2	M520	5.3.0.4	Online	N/A	
10.59.36.46	10.59.36.46	Critical	Thu Apr 12 2012 03:46:18 PM	The Falls 1125	AirDefense 2	M510	5.3.0.4	Online	N/A	
ap7131-C78038	172.17.25.21	Severe	Thu Apr 12 2012 03:45:55 PM	The Falls 1125	AirDefense 2	AP7131	5.3.0.0-088R	uptime 5	Online	audited Thu A
Cisco1131a-CC-qaairf	172.17.25.22	Safe	Thu Apr 12 2012 03:45:35 PM	The Falls 1125	AirDefense 1	AIR-AP...	12.4(21a)3A1	uptime 1	audited Thu A	
rf94000-22091C	172.17.25.23	Severe	Thu Apr 12 2012 03:46:03 PM	The Falls 1125	AirDefense 2	RFS4000	5.3.0.0-088R	uptime 6	audited Thu A	
Cisco1131b-CC-qaairf	172.17.25.24	Safe	Thu Apr 12 2012 03:45:35 PM	The Falls 1125	AirDefense 1	AIR-AP...	12.4(21a)3A1	uptime 1	audited Thu A	

Devices are displayed in groups as follows:

- Network Devices (includes Access Points, Sensors, Wired Switches, Wireless Switches, WLSE devices, AirWave devices, and MSPs—Managed Services Providers)
- BSSs
- Wireless Clients
- Unknown Devices.

The device table is customizable and includes the following information (columns):

Column	Description
Flag	Indicates whether or not a device has been flagged.
Device	Displays the name of the device using a name hierarchy (1-user defined, 2-polled, 3-IP address, 4-MAC address prefix by the vendors abbreviated name)
Name	Displays the name of the device as it defined by a user.
MAC	Displays the MAC address of the device.
IP	Displays the IP address of the device.
Severity	Displays the severity state of the device.
First Seen	Displays the date and time when the device was first seen in your network.
Last Seen	Displays the date and time when the device was last seen in your network.
Scope	Displays the network level your devices is located in.
Floor	Displays the floor your device is located on.
Manufacturer	Displays the manufacturer of the device.
Model	Displays the model number of the device.
Firmware	Displays the firmware version installed on the device.
Status	Dspalys the uptime/offline staus of Access Points and Switches.
Sensor Status	Displays the online/offline status of Sensors.
Compliant	Displays whether or not a device is compliant its WLAN management configuration.
Last Configuration	Displays the date and time of the last WLAN management configuration of the device.
Associated Clients	Displays the associated wireless clients of an Access Point.
Adopted APs	Displays the adopted Access Points of a Switch.

Network Filters

Network filters are provided to filter the displayed network information. The different filters are:

- Grouping Filter—view devices by grouping them using similar criteria.
- Hierarchy Filter—control the level of detail seen in the Network Graph and the Association Tree.
- Network Scope Filter—view devices according to where they are in the network tree.
- First/Last Seen Filter—filter devices according to when they where first seen and/or last seen on your network.
- Flag Filter—optionally view all devices or only flagged devices.
- Severity Filter—view devices by alarm criticality.

- Classification Filter—filter devices by their classification.
- On Network Filter—display devices that are on your network and/or devices that have been seen by a sensor but not confirmed to be on your network.
- Device Filter—filter devices by model, manufacturer, and/or capabilities.
- Compliance Filter—display devices according to their state of compliance with your network policies.
- Status Filter—display devices according to their uptime/offline status.
- Signal Strength Filter—filter devices within a specific signal strength range.
- Security - Sensed Filter—display devices using a combination of the sensed method of authentication and/or the sensed method of encryption.
- Security - Polled Filter—devices using a combination of the polled method of authentication and/or the polled method of encryption.

Actions

The **Network** tab includes an **Actions** menu where you can execute an action depending on the type of devices you are viewing. A description of the actions are as follows:

Action	Description
Set Flag	Flag the selected device(s) to indicate attention is required.
Clear Flag	Remove flag from the selected device(s).
Classification	<p>Sanctioned (inherit) Classify the selected device(s) as a sanctioned device that inherits its traits from wherever its location in the network tree.</p> <p>Sanctioned (override) Classify the selected device(s) as a sanctioned device using traits that override the inherited traits. For example, a security profile can be applied to a BSS that overrides the inherited traits.</p> <p>Sanctioned Classify the selected device(s) as sanctioned (Unknown Devices only)</p> <p>Unsanctioned Classify the selected device(s) as unsanctioned.</p> <p>Neighboring Classify the selected device(s) as a neighboring device.</p>
Client Type	Classify a Wireless Client as one of the following types: Laptop VoIP Phone MCD (handheld device)
Audit Devices	Conduct a compliance audit on the selected device(s).
Remove Devices	Remove selected device(s) from monitoring.
Move Devices	Place selected device(s) on a floor.

Action	Description
Upgrade Devices	Upgrade the firmware for the selected device(s).
Import CLI Variables	Import CLI variables at the device level.
Export Devices	Export information about selected device(s) to a CSV file.

Alarms

The **Alarms** tab displays the alarms generated by ADSP.

Alarm ID	Alarm Type	Device	Start Time	Status	SSID
S.2433254...	Rogue AP on Wired Ne...	Motorola:ca:f9:d1	Fri Apr ...	Inactive (expires in 22:08)	Test_100
S.5553530...	Rogue AP on Wired Ne...	Motorola:ca:f9:d0	Fri Apr ...	Inactive (expires in 22:08)	Mayer5131
S.5122746...	Rogue AP on Wired Ne...	Motorola:ca:f9:f0	Fri Apr ...	Inactive (expires in 22:08)	Mayer5131
S.2828001...	Rogue AP on Wired Ne...	Motorola:cb:f9:f1	Fri Apr ...	Inactive (expires in 22:08)	Test_100
S.3294987...	Rogue AP on Wired Ne...	Motorola:2f:72:e0	Fri Apr ...	Active	Mayer5131
S.3984849...	Rogue AP on Wired Ne...	Motorola:2f:72:e1	Fri Apr ...	Active	Test_100
S.9319765...	Rogue AP on Wired Ne...	Motorola:2f:74:20	Fri Apr ...	Active	Mayer5131
S.1468755...	Rogue AP on Wired Ne...	Motorola:2f:74:21	Fri Apr ...	Active	Test_100
S.4159659...	Rogue AP on Wired Ne...	Cisco:bfe:7:20	Fri Apr ...	Inactive (expires in 19:48)	1140-N
S.3862793...	Rogue AP on Wired Ne...	Symbol:ce:06:51	Fri Apr ...	Inactive (expires in 18:32)	AP300APT-OPEN
S.2349844...	Rogue AP on Wired Ne...	Symbol:27:36:19	Fri Apr ...	Inactive (expires in 13:41)	AP300APT-OPEN
S.2486069...	Rogue AP on Wired Ne...	Symbol:76:0f:50	Thu Apr ...	Active	AP5131-SH
S.2410922...	Rogue AP on Wired Ne...	Motorola:08:05:b2	Thu Apr ...	Inactive (expires in 2:51)	DevMgmt_104
S.1530972...	Rogue AP on Wired Ne...	Motorola:08:05:b3	Thu Apr ...	Inactive (expires in 2:50)	DevMgmt_105
S.2059755...	Rogue AP on Wired Ne...	Motorola:86:44:c2	Thu Apr ...	Inactive (expires in 2:44)	DevMgmt_104
S.1263574...	Rogue AP on Wired Ne...	Motorola:2ca:2:27	Thu Apr ...	Inactive (expires in 2:17)	DevMgmt_108
S.1668760...	Rogue AP on Wired Ne...	Motorola:2ca:2:23	Thu Apr ...	Inactive (expires in 2:12)	DevMgmt_105
S.2926010...	Rogue AP on Wired Ne...	Motorola:2ca:2:22	Thu Apr ...	Inactive (expires in 2:10)	DevMgmt_104
S.1314810...	Rogue AP on Wired Ne...	Motorola:2ca:2:25	Thu Apr ...	Inactive (expires in 2:20)	DevMgmt_106
S.2211873...	Rogue AP on Wired Ne...	Motorola:2ca:2:24	Thu Apr ...	Inactive (expires in 2:19)	DevMgmt_105
S.2676730...	Rogue AP on Wired Ne...	Motorola:2ca:2:26	Thu Apr ...	Inactive (expires in 2:16)	DevMgmt_107

The ADSP Alarm Model

Suppressed Alarm Repetition

Motorola AirDefense has made significant advancements in the Alarm Model, dramatically decreasing the occurrence of repetitious alarms. In the new Alarm Model, the ADSP appliance leverages the extensive data it collects about security events to determine whether events are:

- Unique events
- Repeat occurrences of activities that constitute a single security event
- Repeat observances of a single, ongoing event.

Based on this distinction, ADSP is able to display alarms for unique events and suppress repetitive alarms for ongoing events. This provides better correlation between individual security events and individual alarms.

How an Alarm is Generated

Violations are reported internally to the appliance every minute as **events**.

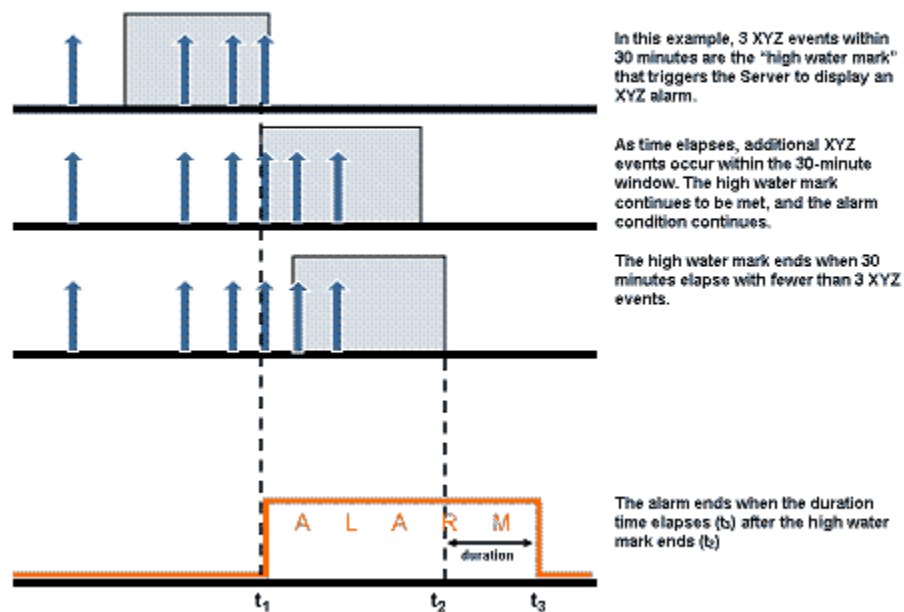
Motorola AirDefense's industry leading wireless security research team maintains algorithms for correlating observed security events, to identify when a pre-defined high water mark for the event is reached. The high water mark, in its simplest terms, is a number of identical events that occur within a specific period of time. When the high water mark is reached, it triggers an **alarm** on the GUI.

Duration

The alarm stays active for a period of time after the security event ends. This period of time is called the **duration**. The duration is user-configurable, although Motorola AirDefense has determined default duration times correlated to the expected lifecycle of each specific event. When the duration time ends, the alarm becomes inactive. You can use the forensic analysis to view historical alarms.

Example

"Three XYZ events within a 30-minute period" defines the high-water mark for XYZ events. If the appliance detects three or more such events within any 30-minute period, an alarm is triggered.



Alarm Table

The alarm table is customizable and includes the following information (columns):

Column	Description
Flag	Indicates whether or not a alarm has been flagged.
Criticality	Displays the criticality of the alarm (see Alarm Criticality for more information).
Alarm ID	Displays the alarm identification.
Alarm Type	Displays the alarm type.
Device	Displays the name of the device that triggered the alarm.

Column	Description
Start Time	Displays the time and date the alarm started.
Status	Displays the status (active/inactive) of the alarm.
SSID	Displays the SSID (Service Set Identifier) of the WLAN device triggering the alarm appears on.
Sensor	Displays the name of the Sensor that observed the device triggering the alarm.
Expire Time	Displays the time and date when the alarm expired.
Signal Strength	Displays the signal strength of the device triggering the alarm.
Channel	Displays the channel the device triggering the alarm is using.
Notes	Displays any notes that were created for the alarm.
Summary	Displays a summary describing the alarm.

Alarm Filters

Alarm filters are provided to filter the displayed alarm information. The different filters are:

- Grouping Filter—view devices by grouping them using similar criteria.
- Network Scope Filter—view alarms according to where they appear in the network tree.
- Alarm Filter—view alarms by severity and/or categories.
- View Filter—optionally view all alarms, new alarms, or flagged alarms.
- Device Filter—filter alarms by device classification and/or device type.
- Alarm Lifecycle Filter—filter alarms over an alarm's lifecycle.
- Alarm ID Filter—filter alarms by specifying an alarm ID.

Alarm Categories and Criticality

ADSP groups alarms into nine categories, and assigns a criticality to each alarm.

Alarm Categories






The nine alarm categories are as follows:

- Anomalous Behavior—Devices that operate outside of their normal behavior settings and generate events that could indicate anomalous or suspicious activity.
- Exploits—Events caused by a potentially malicious user actively interacting on your Wireless LAN using a laptop/PC as a wireless attack platform.
- Infrastructure—Events that are generated based on the SNMP traps received from the infrastructure devices.
- Performance—Wireless LAN traffic that exceeds set performance thresholds for devices.
- Platform Health—Events that provide information about the state of the AirDefense Services platform and the Sensors which report back to the appliance.

- Policy Compliance—Wireless LAN traffic that violates established or default policies for devices.
- Reconnaissance—Monitors and tracks external devices that are attempting to monitor your Wireless LAN.
- Rogue Activity—Unauthorized Devices detected by AirDefense which pose a risk to the security of your network.
- Vulnerabilities—Devices that are detected to be susceptible to attack.

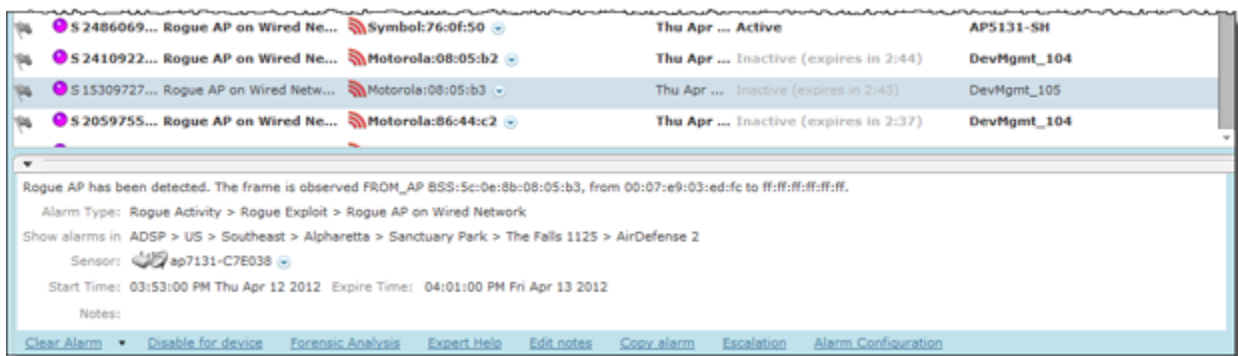
Alarm Criticality

Alarms are assign a default criticality by ADSP. You can optionally change the default criticality of each alarm to match your environment when configuring alarms under **Configuration > Operational Management > Alarm Configuration**. You must be a user with read/write permission for the Alarm Management functional area to change the criticality of an alarm.

Alarm Criticality	Description
Severe— 	Serious alarms that may have catastrophic effects on your WLAN network.
Critical— 	Serious alarms on devices that require immediate attention.
Major— 	Potentially serious alarms on devices that require priority attention.
Minor— 	Suggested potential problem alarms on devices that may develop into worse issues if left alone.
Safe— 	Devices that pose no immediate threat to your WLAN network.

Alarm Details

Additional alarm information can be displayed by selecting an alarm.



The following alarm information is displayed:

- A description of the alarm
- The alarm type
- The network level of the device
- The Sensor that observed the device
- The time when the alarm started

- The time when the alarm will expire
- Any notes added by a user.

Links are included that allow you to execute a function or provide more information.

Link	Description
Clear Alarm	Clear alarm works the same as Clear Alarm in the Actions menu.
Disable for device	Disables the alarm specifically for the device causing the alarm. If you wish to re-enable the alarm, you must go to Alarm Configuration and remove the device from the disabled list.
Forensic Analysis	Accesses Forensic Analysis where you can analyze historical information about the device.
Expert Help	Provides comprehensive descriptions on the alarm in four tabs: <ul style="list-style-type: none"> • Summary—displays a summary about the alarm type. • Description—displays detailed information about the alarm type. • Investigation—advises you on how to investigate the alarm type. • Mitigation—advises you on how to mitigate the alarm type.
Edit notes	Allows you to edit or add notes for the alarm.
Copy alarm	Copies all the detailed information about the alarm to the Clipboard for later use.
Escalation	Displays an escalation window displaying what you need to do to escalate a problem. The escalation information is defined in the alarm configuration for the specific alarm.
Alarm Configuration	Opens Alarm Configuration in the Configuration tab.

Actions

The **Alarms** tab includes an **Actions** menu where you can execute an action that affects the selected alarm. A description of the actions are as follows:

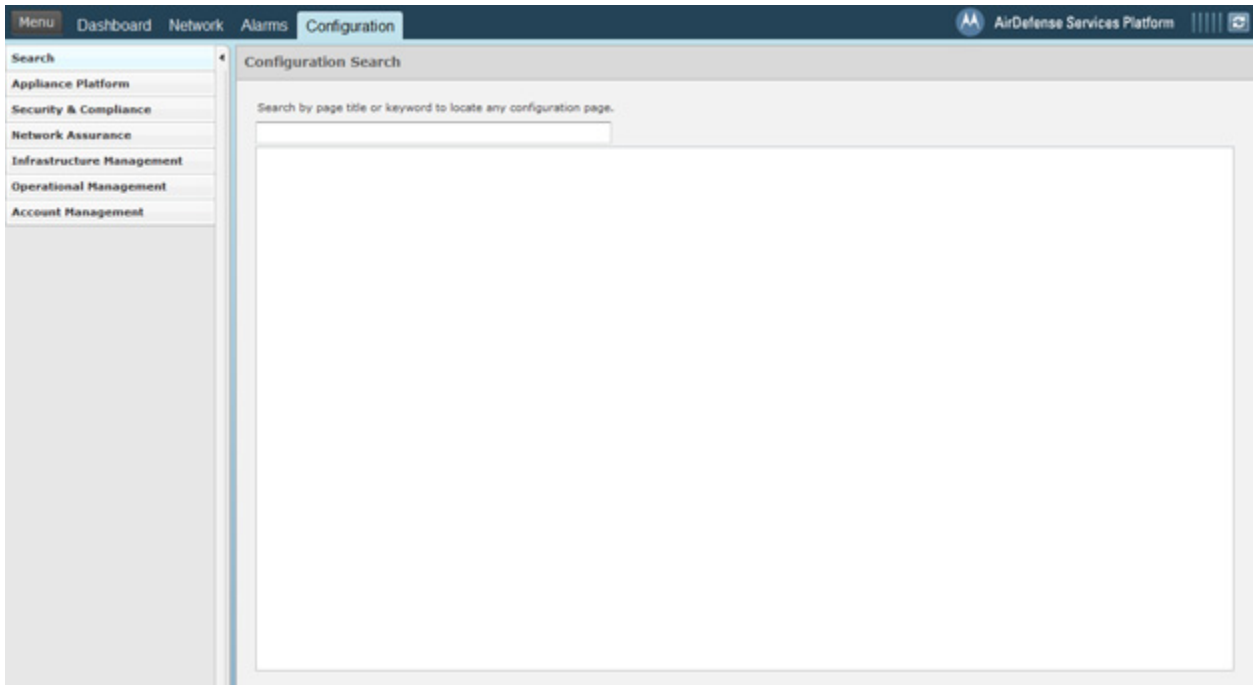
Action	Description
Clear Alarm	<p>Clear the selected alarm using one of the following options:</p> <ul style="list-style-type: none"> • Clear Alarm (no time limit) • Clear for 1 hour • Clear for 6 hours • Clear for 12 hours • Clear for 24 hours. <p>If you click one of the options with a time limit. The alarm is cleared for the specified time and then returns if the conditions that generated the alarm are not cleared.</p>
Edit Alarm Notes	Allows you to edit or add notes for the selected alarm.
Set Flag	Flag the selected alarm(s) to indicate attention is required.
Clear Flag	Remove flag from the selected alarm(s).
Mark as New	Mark the alarm as new. New alarms are displayed in bold text.
Mark as acknowledged	Mark the alarm as acknowledge which means you have selected the alarm and view details about the alarm. Acknowledge alarms are displayed in regular text.
Export Alarms	Exports the alarm information to a CSV file.
Manage Cleared Alarms	Displays an overlay where you can manage cleared alarms.

Configuration

The Configuration tab allows you to set up ADSP using the following configuration categories:

- Appliance Platform—used to initially set up ADSP.
- Security & Compliance—defines the security configurations of sanctioned Wireless Clients and monitors the wired network devices in your system.
- Network Assurance—configures Live RF settings, creates Performance Profiles, and sets up Environment Monitoring.
- Infrastructure Management—configures devices so that they can communicate on your network and be managed by ADSP.
- Operational Management—includes features that apply to the normal operations of ADSP.
- Account Management—includes the features that manage the accounts of ADSP.

- Account Management—creates and maintains user accounts.



Appliance Platform

The Appliance Platform category includes all the necessary features that are needed to initially set up ADSP. The Platform category allows you to:

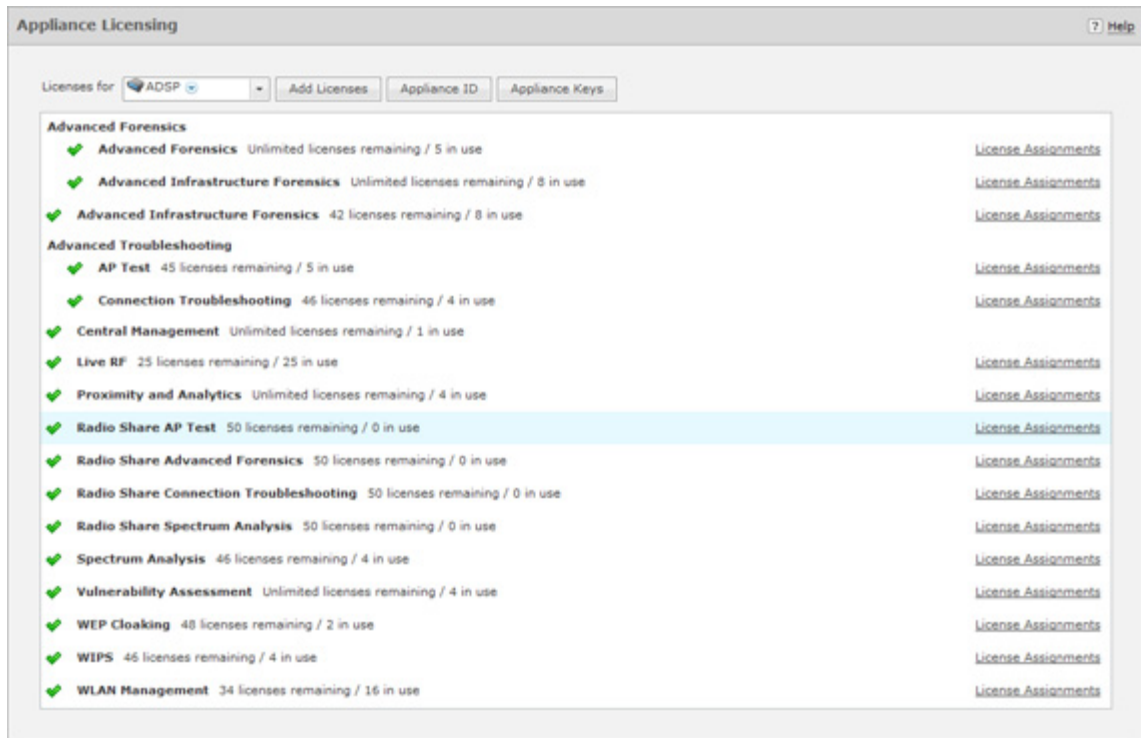
- 01. Appliance Licensing—License your appliance and devices.
- 02. Tree Setup—Establish a network tree.
- 03. Security Profiles—Create security profiles that will initiate WIPS.
- 04. Auto-Placement Rules—Define auto-placement rules that will automatically place devices in your network tree.
- 05. Device Import Rules—Establish an import policy that controls how devices are classified when imported into your network and select which licenses apply during the import process.
- 06. Communication Settings—Set up communication profiles that allow ADSP to communicate with devices in your network.
- 07. Polling—Determine how often ADSP polls your devices for status information and sets the frequency.
- 08. Relay Server—Set up a relay server that facilitates downloading/uploading configuration profiles to/from your devices. (Optional.)
- 09. Import / Discover Devices—Schedule when to import devices using an import file or discover devices using SNMP.

Each feature is numbered. When initially setting up ADSP, follow the numbered steps sequentially. Once you have completed the last step, ADSP is set up for use.

Appliance Licensing

The ADSP GUI handles license management for ADSP and any modules. Using Appliance Licensing, you can:

- View current license agreement information
- Add licenses
- Copy appliance MAC address
- Download appliance keys.



View Current License Information

License information is displayed about the following add-on modules:

- Advanced Forensics which includes:
 - Advanced Forensics
 - Advanced Infrastructure Forensics
- Advanced Troubleshooting which includes:
 - AP Test (available as a separate license)
 - Connection Troubleshooting (available as a separate license)
- Assurance Suite which includes:
 - AP Test (available as a separate license)
 - Advanced Forensics
 - Advanced Infrastructure Forensics
 - Connection Troubleshooting (available as a separate license)
 - Live RF (available as a separate license)
 - Spectrum Analysis (available as a separate license)

- Central Management
- Proximity and Analytics
- Radio Share Network Assurance which includes:
 - Radio Share AP Test (available as a separate license)
 - Radio Share Advanced Forensics (available as a separate license)
 - Radio Share Connection Troubleshooting (available as a separate license)
 - Radio Share Spectrum Analysis (available as a separate license)
- Tracker Integration
- Vulnerability Assessment
- WEP Cloaking
- WIPS
- WLAN Management



NOTE Modules are only displayed when they are installed.

License status is determine by:

- A green check mark indicates the license is OK.
- A yellow flag indicates the license requires attention. It may expire soon.
- A red **X** indicates the license has expired.

Clicking on a license will display the following information about the license.

✔
WIPS 46 licenses remaining / 4 in use
License Assignments

Order placed on 2019-06-04 (id=105472)

License count: 50 licenses

Valid from 2019-06-04 and does not expire

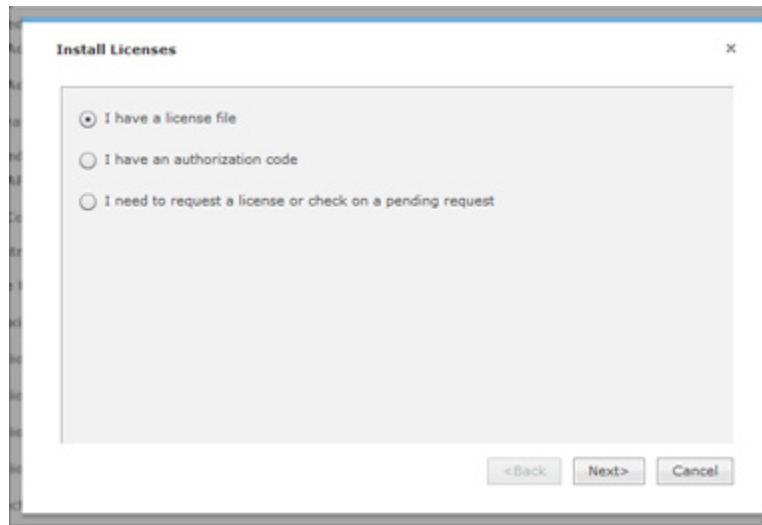
Maintenance from unspecified

Reassignments: 25 licenses / 25 licenses remaining

Field	Description
Order Date	Indicates the date the license was ordered and the license ID number.
License Count	<p>Includes the following information:</p> <ul style="list-style-type: none"> The number of units. The number of active units cannot exceed this number. Unit counts may be 0, a specific number, or unlimited. A style that specifies that the unit count is fixed or floating. Fixed licenses get consumed as they are used and are not released. Floating licenses get released when they are not being used anymore. A unit identifier. Units may be Sensors, APs, switch, etc. A maximum value limiting the number of units. A warning limit used to display an alarm that the unit count is being approached and that user should consider purchasing additional licenses.
License Valid Date	Displays the expiration date and the start date of the license. A warning date is also displayed, indicating when the customer will be issued a warning that the license will soon expire. Unlimited indicates an expiration date of 9999-12-31.
Maintenance Date	Displays the expiration date and start date of the maintenance agreement with the customer. Unlimited indicates an expiration date of 9999-12-31.
Reassignments	Displays the number of licenses that you can reassign and how many reassignments that you have left.

Add Licenses

Installing a license is easy. Just click the **Add Licenses** button to begin.



There are three ways to install a license:

- Using a license file
- Using an authorization code
- Requesting a license or checking on a pending request.

Download Appliance Keys

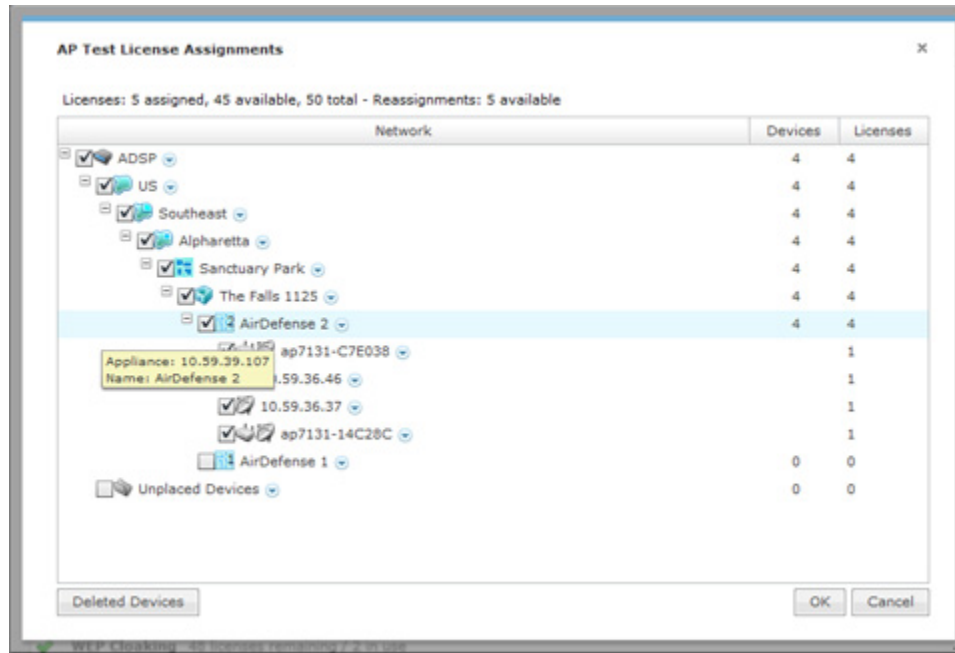
You can download appliance keys to your workstation from the **Licenses** window. Use the **Appliance Keys** button.

Copy Appliance MAC

You can display an appliance's MAC address using the **Appliance MAC** button. Once the MAC address is displayed, you can copy it for later use.

License Assignments

The **License Assignments** link allows you to view which license is assigned to a device. You can also assign a license to a device.



Open tree levels until the device that you want to assign a license to is displayed. Then, select the checkbox for the device.

Tree Setup

Tree Setup is used to configure your network tree. You must set up your network tree in order for you to take full advantage of ADSP. Your network tree starts at the system level and automatically includes your appliance and any other appliance that you have added to your system. Each appliance can be expanded into a tree with five network levels and floors. Available network levels are:

- Country
- Region
- City
- Campus
- Building.

Planning Your Network Structure (Tree)

Deciding how to structure your network tree depends on:

- Whether you want to use triangulation for location tracking
- How you plan to apply policies to devices
- How the tree affects the scope in the UI.

Triangulation Considerations

To use triangulation, you must load ADSP appliance with a two-dimensional map of the floor your sensors are located on. Maps must be loaded at the floor level. You cannot use triangulation over multiple floors which means you cannot use sensors on different floors if you want to use triangulation.

Policy Considerations

When you are creating network levels, you should create profiles for similar devices that you expect to share common policies. Although you can certainly apply policies at the device level, it is a good practice to apply them at higher network levels (preferably at the appliance (ADSP) level).

UI Scope Considerations

You control the scope of data you see at any time by selecting levels in the tree. If you want to view data from one area of your WLAN separately from data about the rest of the WLAN, such as different buildings/floors, you should consider how you can create network levels for that area. Then, viewing its data discretely is as easy as clicking on that node in the tree.

Combining Considerations**Example**

A company with four buildings with multiple floors plans to use triangulation. Two ADSP users each manage the WLAN security for one building, and a third user manages the two other buildings. An overall system security administrator oversees all users and buildings.

- Buildings A, B, C, and D = network level for each building
- Floors = network level for each floor in a building
- User management = select Scope Permissions for each user by editing User Accounts.
 - Building A is assigned to User 1
 - Building B is assigned to User 2
 - Building C and D are assigned to User 3
- For the overall administrator, select the system level in User Accounts.

Result

Each user can see only the data for the building(s) he manages. Each user can apply policy and view data by floors within their building, and perform location tracking with triangulation by importing a map for each floor.

Building Your Tree

While there are several important considerations when *planning* how to build your tree, actually building it is quite simple. Ideally, you should use **Tree Setup** under **Configuration > Appliance Platform** to build your tree. However, you can do it anywhere that there is access to the Network Tree. The person who installed ADSP may have created all or part of your tree during setup. You can always revisit **Tree Setup** to add to or adjust your tree.

Create Network Levels

In **Tree Setup**, you add network levels by selecting an existing starting point in the tree and clicking the **add child** link. Any time you add a network level and an equivalent level already exists, it appears in the tree in alphabetical order.

Add Floors

You can add floors by selecting a building and then increasing the floor number using the **Floors** field.

Importing Your Tree

You can import a tree structure using the **Import** button. Comma delimited files are used to import a tree structure. The format of the file is:

```
record type (folder),server,Name,Description,Type,Floor Number,Path(slash delimited)
```

There are different ways to create a comma delimited file but the most trouble-free way is to use a text editor, such as Notepad. Fields may be blank with no blank space between the commas (i.e., ,).

Examples:

```
folder,localhost,AirDefense 1,,Floor,1,US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125
folder,localhost,AirDefense 2,,Floor,2,US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125
```



NOTE At this time, you can only import a tree structure to your local appliance. You do so by specifying localhost as your server.

The path to the new folder must be present in the existing tree or be previously defined in the import file. For example, in the previous example, the path US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125 must already exist. Here is how you define that path:

```
folder,localhost,US,,Country,,
folder,localhost,Southeast,,Region,,US
folder,localhost,Alpharetta,,City,,US/Southeast
folder,localhost,Sanctuary Park,,Campus,,US/Southeast/Alpharetta
folder,localhost,The Falls 1125,,Building,,US/Southeast/Alpharetta/Sanctuary Park
```

Auto-Placement Rules

Auto-Placement Rules define the criteria for automatically placing devices in a predetermined scope (network level). Any device with the specified parameter(s) and qualifying value is placed into the selected scope level.

Auto-Placement can be used in two ways: one method for sensors and another method for APs and switches. Auto-Placement rules for sensors are applied every 20 minutes. If a rule exists, new sensors in the **Unplaced Devices** folder are moved into a pre-defined scope level. This only happens to sensors seen in your network since the last 20 minute poll. Sensors seen before the last 20 minute poll are excluded.

Auto-Placement rules for APs and switches are applied when APs or switches are manually added/imported into a system using the following conditions:

- If a rule exists, the AP or switch is moved into the pre-determined scope level.
- If no rule exists, the AP or switch is moved into the **Unplaced Devices** folder.
- If no Auto-Placement rules criteria match the device, it will be placed in the **Unplaced Devices** folder.
- IP based placement uses a single IP address for each device. The selected IP address for Auto-Placement is the first available address on the following ordered list of IP addresses learned by ADSP.
 1. The first IP address on the list is the Devices Management IP Address. This is the IP address that ADSP uses to communicate with the device. Due to the use of NAT in the network, this IP address may be different than the actual configured IP address of the device.
 2. The second IP address is the address that the switch provides to ADSP for the AP. In adaptive or adopted mode where the AP is discovered through the switch, the system will use the IP address

that the switch has provided for the AP. This IP address is only used by ADSP for this purpose and is not saved by ADSP. It is not used as a configured or managed IP address for the device, and it will not be displayed by ADSP.

3. The switch's IP address will be used for Auto-Placement of the AP if the previous two IP addresses are not available. The switch's management address is the IP address that is used by ADSP to communicate with the switch. It may NOT be the switch's configured IP address.

To configure Auto-Placement rules, you must select a scope (network level) to apply the rules to, select one or more of the pre-defined rules, and specify a value for each rule using the following criteria:

Field	Description
Network Address	The device's network address.
IP Range	A range of IP addresses that the device(s) must fall within.
MAC Address	A range of MAC addresses that the device(s) must fall within.
DNS Server	The DNS server that the device(s) are using. This parameter only works with sensors not access points and switches.
Uses DHCP	Specify whether or not DHCP is used (True or False). This parameter only works with sensors not access points and switches.
Device Name	The name of the device.
Model Name	The model number of the device.
Firmware Version	The firmware version the device has installed.
Serial Number	The serial number of the device.

Auto-Placement Rules are applied in sequence. You should prioritize your rules so that the most important ones are applied first.

You can import Auto-Placement Rules using the **Import** button. Comma delimited files are used to import Auto-Placement Rules. The format of the file is:

```
autoplacement_rule,server,Path,Network Address,IP Range,MAC Address,DNS Server,Uses DHCP,
Device Name,Model Name,Firware Version
```

There are different ways to create a comma delimited file but the most trouble-free way is to use a text editor, such as Notepad.

Things to Remember:

- The first field for importing Auto-Placement rules must be *autoplacement_rules*.
- At this time, the only valid server name is *localhost*.
- Fields may be blank with no blank space between the commas (i.e., ,).
- Path names must begin with a slash (/) and include a slash (/) between network levels. Also, the path must already be present in the existing network tree.
- For fields with a range, you must include a range even if there is only one IP address or one MAC address (e.g., 1.1.1.1-1.1.1.1).

Examples:

```

autoplacement_rule,localhost,/USA/AutoPlacementTest/Floor 1,,172.17.17.0-172.17.17.19,,,,,6.0.196.0
autoplacement_rule,localhost,/USA/AutoPlacementTest/Floor 6,,172.17.15.0-172.17.15.200,,,,,6.0.196.0
autoplacement_rule,localhost,/USA/AutoPlacementTest/Floor 4,172.17.18.0/24,
172.17.18.100-172.17.18.101,00:16:5d:20:47:60-00:16:5d:20:47:61,172.17.0.83,disable,BA-Sensor-240,
M520,5.2.0.11

```

Communication Settings

Communication Settings are used to configure SNMP connectivity and enable common features supported by APs and switches.

Some profiles with default settings for Motorola and Cisco devices are supplied with ADSP. When applying profiles and multiple profiles are selected, ADSP will attempt to find the best match to apply starting at the top of the list and working its way down to the bottom of the list. In order for this event to work properly, the default profiles should not be modified.

WiNG 5.x devices ship from the factory with **admin** as the username and **motorola** as the password for the HTTP and SSH credentials. The default profile uses these same credentials. However, WiNG 5.x devices require a password change when logging in for the first time using ssh/telnet. The changed password cannot be **motorola**. ADSP will use the password in the device access profile, or if one does not exist, an error message will display. Therefore, when using WiNG 5.x devices, you must create a communication profile that matches the device access profile before communications can occur between ADSP and the device.

You should always configure Communication Settings at the appliance level. When you do, the configuration is inherited for all the other levels. Then, if you have a level that needs a different configuration, you can apply that profile to that level using the override feature. For example, if most of the network devices require a console to interface with it, you can configure the Communication Settings for console interface at the appliance level. Then, if you have a small group of devices that require you to interface with it through a web UI, you can configure the Communication Settings for HTTP interface and override the appliance level configuration by selecting another network level.

The following three tabs are used to configure Communication Settings:

- SNMP
- Console
- HTTP.

SNMP Tab

The **SNMP** tab is used to configure connectivity settings for SNMP devices. Available fields are:

Field	Description
Profile Name	Enter a name that you want for the new profile. Once the profile is saved, its name cannot be changed when editing the profile.
Enable SNMP Settings	Select the checkbox to enable (default) SNMP communications settings.
Versions	Select V2 or V3 as the SNMP version used.
Read Community	Enter the Read Community string, which is used for the SNMP authentication.
Write Community	Enter the Write Community string, which is used for the SNMP authentication.

Field	Description
Port	Enter the Simple Network Management Protocol number for the devices. This is normally set to 161, but it can be different.
Timeout in MS	Enter a timeout value in milliseconds to connect to a SNMP device.
Retries	Enter a maximum number of retries that can be made while attempting to connect to a SNMP device.
User	Enter the name of the V3 user, which is configured on the switch for SNMP V3 access.
Auth Algorithm	The authentication algorithm is a SNMP V3 parameter that must match what is set on the device. The options are MD5 , SHA and None . You must also supply a passphrase which must also match what is set on the device.
Privacy algorithm	The privacy algorithm is a SNMP V3 parameter that must match what is set on the device. The options are DES , 3DES , AES128 , AES192 , AES256 and None . You must also supply a passphrase which must also match what is set on the device.

Console Tab

The **Console** tab is used to supply login credentials for devices that a console can be used to interface with them. The following fields must be set when using a console to interface with a device:

Field	Description
Enable Console Settings	Select this checkbox to enable Console communications settings.
User	The user name used to log into a device.
Password	The password used to log into a device.
Enable Password	The enable password must be supplied in order to enter the enable mode.
Protocol	The protocol used to log into a device. The available options are SSH and Telnet .
Port	The port number that is used for communications. SSH uses port 22 while telnet uses port 23.

HTTP Tab

The **HTTP** tab is used to supply login credentials for the devices that supply a web UI to interface with them. The following fields must be set when using a web UI to interface with a device:

Field	Description
Enable HTTP Settings	Select this checkbox to enable HTTP communications settings.
User	The user name used to log into a device.
Password	The password used to log into a device.
Protocol	The protocol used to log into a device. The available options are HTTP and HTTPS .
Port	The port number that is used for communications. Port 80 is normally used but it may be another port number.

Importing Communications Settings

Communications settings for a device may be imported using one of the following methods:

- Manually via **Menu > Import & Discovery**
- Through a schedule via **Configuration > Appliance Platform > Import / Discover Devices**
- Through your appliance CLI with the **import** command .

Importing communications settings require a separate import file. You should not combine importing communications settings with importing devices. Also, when importing communications settings for a device, the device must be imported into ADSP first.

Comma delimited files are used to import communications settings. There are different ways to create a comma delimited file but the most trouble-free way is to use a text editor, such as Notepad.

The import file is used to populate the fields in the four communication settings tabs. You can populate as many of the fields as you like. The import file fields required the same values as the communication settings in the four tabs.

There are two records associated with communications settings:

- **comm_settings**—used to import a named Communication Settings Profile into the ADSP system.
- **comm_settings_loc**—used to apply previously-imported Communication Settings Profiles to a level in the ADSP (either a folder or specific device).

The fields for the **comm_settings** record are:

- Import type (must be **comm_settings**)
- MAC address (required field)
- SNMP version (**1, 2, or 3**)
- SNMP read community
- SNMP write community
- SNMPv3 username
- SNMPv3 authentication passphrase
- SNMPv3 privacy passphrase
- SNMPv3 authentication algorithm (**None, MD5, or SHA**)
- SNMPv3 privacy algorithm (**3DES, DES, AES128, AES192, AES256, or None**)
- SNMP port
- SNMP timeout (in milliseconds)
- SNMP number of retries
- Console user
- Console password
- Console enable password
- Console protocol (**SSH or Telnet**)
- Console port
- HTTP user

- HTTP password
- HTTP protocol (**HTTP** or **HTTPS**)
- HTTP port

Example:

```
comm_settings,ProfileName,3,public,private,snmpV3user,snmpV3authpassphr,snmpV3privpassphr,MD5,
3DES,161,300,4,Cisco,Cisco,Cisco,SSH,22,admin,adminpassword,https,443
```



NOTE Although the above example is shown on multiple lines, all entries must be on a single line with no line breaks or carriage returns.

The fields for the **comm_settings_loc** record are:

- Import type (must be **comm_settings_loc**)
- Profile name
- MAC address or folder path (required field)
- Device type (**ap**, **switch**, or **folder**)

Once the communication settings are imported, they will override any inherited settings. To see the new communication settings, go to the device's properties and select **Communication Settings**.

Examples:

```
comm_settings_loc,ProfileName,00:23:04:5e:d3:00,ap
```

```
comm_settings_loc,ProfileName,/US/Southeast/AirDefense,folder
```



NOTE For communications settings applied to a folder, the final field (device type) must be **folder**.

Polling

ADSP uses a centralized Polling feature to manage configuration audits, status polling and data collections from one location.

You have an option to enable polling for supported devices. When enabled, WMS automatically polls for device network status at an interval defined by a user supplied frequency value (default frequency is 1 hour).

Each device model has an associated data collection profile which identifies the list of attributes collected periodically from the device. You can elect to collect these SNMP attributes at a frequency defined by you (default frequency is 8 hours). You can also enable ADSP to correct configuration compliance violations by uploading the last approved configuration to the target device.

If you have a Central Management license and there are multiple appliances in your system, after configuring polling, you can copy the configuration to all appliances in the system.

Relay Server

Relay Server is an option that is included with a WLAN Management license. If you do not have a WLAN Management license Relay Server does not appear in the list of features and the features are renumbered.

Import / Discover Devices

Import / Discover Devices is used to schedule imports from one of the following sources:

- Remote file

- SNMP discovery using a list of networks to scan.

Imported APs, switches and sensors will be placed in the network tree according to auto-placement rules. Therefore, you must configure Auto-Placement Rules before importing any of these devices.

All imported devices will be configured and classified according to the Device Import Rules.

Wireless devices (BSS/wireless client) imported from a file will be added to the primary appliance or any other appliance (based on user selection). Wireless devices imported from infrastructure will be added to the appliance that includes the infrastructure device.

You can also import a device using your appliance CLI. This import file uses the file formats described under [Import Device File Format](#) and the file formats for the individual **Import** buttons used through the GUI. The command to import devices from the appliance CLI is:

```
import -filename </path/to/import_file> -user <adsp_user> -folderId <folder_id>
```

where </path/to/import_file> is the name of the import file (preceded by the relative or full pathname), <adsp_user> is a valid ADSP user name, and <folder_id> identifies the folder to place the device. If <folder_id> is omitted, auto-placement rules are used.

Available Fields for Importing Switches Using a Remote File

- Job Name—Name of your switch import job
- Import Source—**Remote File**
- Host—Host name or IP address
- Protocol—Protocol used for communications
- Path—Path name on the remote host
- User—User name needed to log in
- Password—Password needed to log in
- Add to appliance—Appliance where you want to import device

Available Fields for SNMP Discovery

Before importing switches using SNMP discovery, you must enable SNMP on the device and verify that you can execute **snmpwalk** from the appliance. You will need the IP address and community string for the device. To verify SNMP connectivity, from the appliance, run the following command against your target device:

```
snmpwalk -v2c -c public xxx.xxx.xxx.xxx (this is the IP address).
```

- Job Name—Name of your switch import job
- Import Source—**SNMP Discovery**
- Networks—List of networks to scan
- SNMP Port—Device SNMP port number; normally set to 161 but can be different
- Timeout (ms)—Timeout in milliseconds to attempt import
- Retries—Number of retries to attempt import
- Version—SNMP version used: **V1**, **V2c** or **V3**
- Read Community—Read Community string used for the SNMP authentication
- Add to appliance—Appliance where you want to import device

Setting the Schedule

The **Schedule** tab allows you to set the schedule for importing devices. You can select **One Time Schedule**, **Intra-Day Schedule**, **Daily Schedule**, **Weekly Schedule**, or **Monthly Schedule**. Depending on the selected interval, fill in the related fields using the following table:

Field	Description
One Time Schedule	Choose a time for importing the device. Then, select a day.
Intra-Day Schedule	Select a time to begin importing the device. Then, select a frequency in hours.
Daily Schedule	Select a frequency in day, weekdays only, or weekends only. Then, select a time of day.
Weekly Schedule	Select a day or multiple days to import the device. Then, select a time of day.
Monthly Schedule	Choose the months that you want to import a device. Then, select a day of the month, the last day of the month, or a specific day of the week as it relates to the first, second, third, fourth, fifth, or last week of the month. Last, specify a time of day.

Import Device File Format

BSS

Format

bss | name | description | mac | isBridge | sanctioned/unsanctioned/ignored | performance profile | list of sec profiles

Example

```
bss,name,desc,00:01:01:01:01:01,true,sanctioned,perfprofile,secprof1;secprof2
```



NOTE **bss** must always be the first field.

Wireless Client

Format

station | name | description | mac | isWired | sanctioned/unsanctioned/ignored | performance profile | list of sec profiles

Example

```
station,name,desc,02:02:02:02:02:02,true,sanctioned,perfprofile,secprof1;secprof2
```



NOTE **station** must always be the first field.

Access Point

Format

ap | name | description | mac | ip | dnsName | model



NOTE *model* is optional and can be left blank.

Example

```
ap, apname, apdesc, 03:03:03:03:03:03, 10.10.10.10, ap.dns.name, AP650
```



NOTE `ap` must always be the first field.

Switch**Format**

```
switch | name | description | mac | ip | switchType | dnsName | model
```



NOTE `model` is optional and can be left blank. Also, if `switch` is a wired switch, `model` must be left blank.

Example

```
switch, switchname, switchdesc, 04:04:04:04:04:04, 11.11.11.11, wireless, switch.dns.name, RFS4000
```

```
switch, switchname, switchdesc, 05:05:05:05:05:05, 11.11.11.11, wired, switch.dns.name,
```



NOTE `switch` must always be the first field.

Device on Wire**Format**

```
dev_on_wire | device_MAC | device_IP | sanctioned/unsanctioned | switch_MAC | switch_IP | ifIndex | ifName | ifDescr | vlanID
```

Example

```
dev_on_wire, 00:06:06:06:06:06, 4.3.2.1, sanctioned, 00:0d:bc:78:94:81, 10.59.39.110, 0,  
interface name, interface description, 0
```



NOTE `dev_on_wire` must always be the first field.

Security & Compliance

The Security & Compliance category includes the features that define the security configurations of sanctioned Wireless Clients and monitor the wired network devices in your system so that they stay in compliance with your policies.

Security Profiles

Security Profiles define the security configurations of sanctioned wireless clients on your wireless LAN. The following three tabs are used to configure a profile.

- **General**—Names your Security Profile and specifies whether or not you want to :
 - Allow unsanctioned wireless clients.
 - Allow SSID broadcast to be seen in the beacon.
 - Enable wireless client isolation.

- Privacy—Enables privacy monitoring for:
 - Base 802.11 authentication (Open or Shared)
 - Extended 802.11 authentication (WPA, WPA2, or Symbol KeyGuard)
 - Advanced key generation
 - 802.11 encryption
 - Other encryption methods such as Cranite, AirFortress, IP-Sec, or other ethertypes.
- Rates—Selects transmit and receive data rates for BSSs to use.

Wired Network Monitoring

Wired Network Monitoring is used to monitor the wired network devices in your system.

You can generate an alarm policy for your wired network by selecting any of the following conditions:

- New device detected on the wired network. Using the **Known Vendors** button, you can select the wired equipment vendors used in your network. Any vendor selected in the list will generate a lower severity alarm condition.
- Sanctioned wired device detected at different location in tree hierarchy than when originally discovered.
- Sanction device no longer observed. You must specify a minimum time for the device to have not been seen on your network.

To detect new devices on your network, existing devices must be classified as sanctioned. The **Mass Wired Network Device Classification** button opens a dialog where you can sanction all or a selection of devices at one time. Typically, this process should be done when you initially configure policies or after major network changes.

Network Assurance

The Network Assurance category allows you to:

- Configure Live RF settings to use when displaying Live RF heatmaps. This feature is only available with an Live RF license.
- Create Performance Profiles that are used to create and edit network performance threshold policies for BSSs and Wireless Clients.
- Set up Environment Monitoring that is used to monitor your system for unobserved devices and generate alarms for missing devices.

Performance Profiles

Performance Profiles are used to create and edit network performance threshold policies for BSSs and wireless clients on your wireless LAN. New profiles are added by clicking the **New Profile** button. The following four tabs are used to configure a profile:

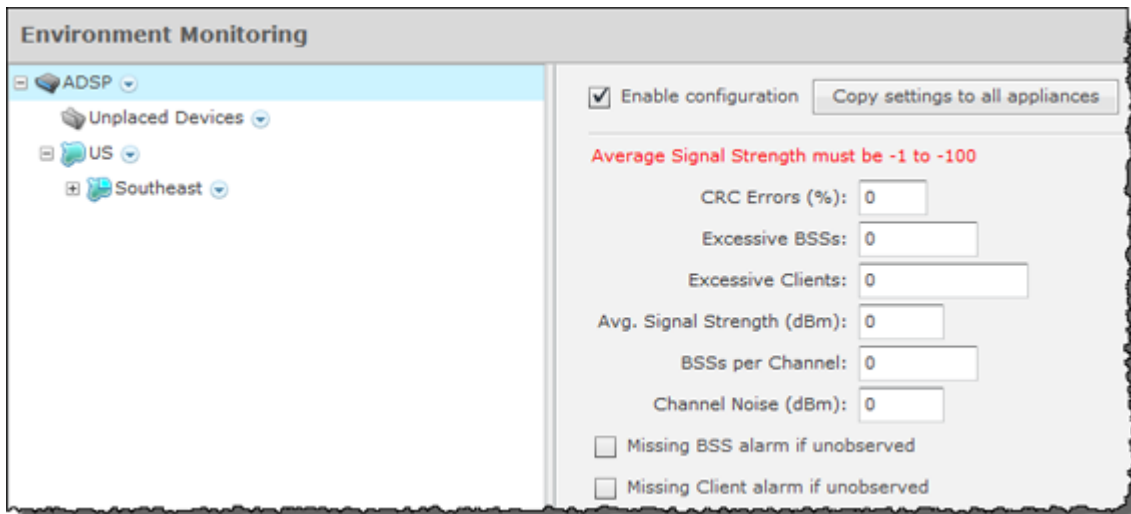
- General—Names your Performance Profile and specifies whether or not you want to:
 - Use a short time slot
 - Allow streaming traffic
 - Enable protection mode.
- Cumulative—Assigns thresholds to network characteristics for all wireless clients and traffic in the access point's BSS (Basic Service Set). ADSP generates an alarm if any of the thresholds are exceeded.

- **Wireless Clients**—Assigns thresholds that apply to any individual wireless client in the access point's BSS and will typically be lower than the aggregate wireless client thresholds. ADSP generates an alarm if any single wireless client reaches one of these thresholds. From these alarms, you can identify the high bandwidth users, and the times they are using the network. You should base wireless client thresholds on either the normal transmission rate for your wireless LAN, or on arbitrary numbers designed to detect your high-bandwidth users.
- **BSS**—Assigns thresholds for transmitting data to/from BSSs. ADSP generates an alarm if any of the thresholds are exceeded.

Environment Monitoring

Environment Monitoring allows you to configure the thresholds for monitoring. If a threshold value is exceeded, an alarm is generated. You can also elect to monitor your system for unobserved devices and generate alarms for missing devices.

Environment Monitoring is configured at the system level of the network tree and inherited by all lower levels. Once you have defined settings at the system level, if necessary, you can override them at any of the lower network levels. This is a screen shot of Environment Monitoring at the system level.



The following thresholds can be configured for monitoring.

Threshold	Description
CRC Errors	Cyclic redundancy check (CRC) errors should not exceed the specified percentage value.
Excessive BSSs	BSSs on your network are considered excessive if the specified value is exceeded.
Excessive Clients	Wireless clients on your network are considered excessive if the specified value is exceeded.
Avg. Signal Strength (dBm)	The average signal strength (in dBm) of APs on your network should not exceed the specified value.
BSSs per Channel	The number of BSSs on any particular channel should not exceed the specified value.

Threshold	Description
Channel Noise (dBm)	Channel noise is monitored to ensure that the noise does not exceed the specified value.
Missing BSS Alarm if unobserved	Option, when selected, generates a missing BSS alarm when any of the threshold values are exceeded.
Missing Client Alarm if unobserved	Option, when selected, generates a missing Client alarm when any of the threshold values are exceeded.

Infrastructure Management

Infrastructure management involves:

- Defining how ADSP interfaces with devices
- Providing information to ADSP so that ADSP can apply the correct regulatory rules to the domain.

The following infrastructure management features are not activated until you install a WLAN Management license:

- Device Firmware
- Channel Settings
- Radio Settings
- WLAN Profiles
- CLI Configuration
- Command Run and Log
- Pending State Audit (added to the Operational Management category).

Device Access

Device Access is used to specify the passwords to access devices and specify the interfaces that can be used to access devices.



NOTE You must define how to communicate with devices. This is done under [Appliance Platform > Communication Settings](#).

There are two tabs used to configure Device Access:

- Password
- Interfaces

Password Tab

The **Passwords** tab is used to specify the passwords to access devices. The following fields are available:

Field	Description
Encrypt Passwords and Keys on Flash	Select checkbox to encrypt passwords and keys on flash.
Enable Password	Specify (set) the enable password. Must be supplied in order to enter the enable mode.
User Accounts	Specify (add) additional user accounts using the Add button. You must specify a username and password.

Interfaces Tab

The **Interfaces** tab is used to specify the interfaces that can be used to access devices. The following fields are available:

Field	Description
Telnet access enabled	Enables access to telnet.
SSH access enabled	Enables access to SSH.
HTTP access enabled	Enables access to HTTP.
HTTPS access enabled	Enables access to HTTPS.
SNMP access enabled	Enables access via SNMP. If you enable SNMP access, you must also specify the following passwords: <ul style="list-style-type: none"> • Read Community • Write Community • Trap Community • Trap Destination.

RF-Domain

RF-Domain provides information to ADSP so that ADSP can apply the correct regulatory rules to the domain. This information includes domain location and contact information of the person responsible for the domain. The country is crucial in applying the regulations. Available fields are:



NOTE You should enter data for each field on one line with no carriage returns.

Field	Description
Description	Allows you to give a meaningful description for the RF domain.
Address	Specifies the address of the RF domain.

Field	Description
Contact	Specifies contact information of the person responsible for the RF domain.
Country	Specifies the country where the RF domain resides. The setting informs ADSP which regulations to apply to the domain.
Time Zone	Specifies the time zone of the RF domain.

Operational Management

The Operational Management category includes features that apply to the normal operations of ADSP. The Operational Management category allows you to:

- Configure alarms for your network environment.
- Specify an age out value that ADSP uses to display devices in the Network tab.
- View and check on jobs initiated by users using ADSP.
- Customize the frequency in which the location of various types of devices are scanned and calculated.
- Identify devices that are in a pending state. A WLAN Management license is required to access this feature.
- Configure network settings for legacy Sensors and WiNG 5.3 (and higher) that are configured as a Sensor only device.
- Configure Sensor scan settings and Sensor in-line settings for Advanced Spectrum Analysis.

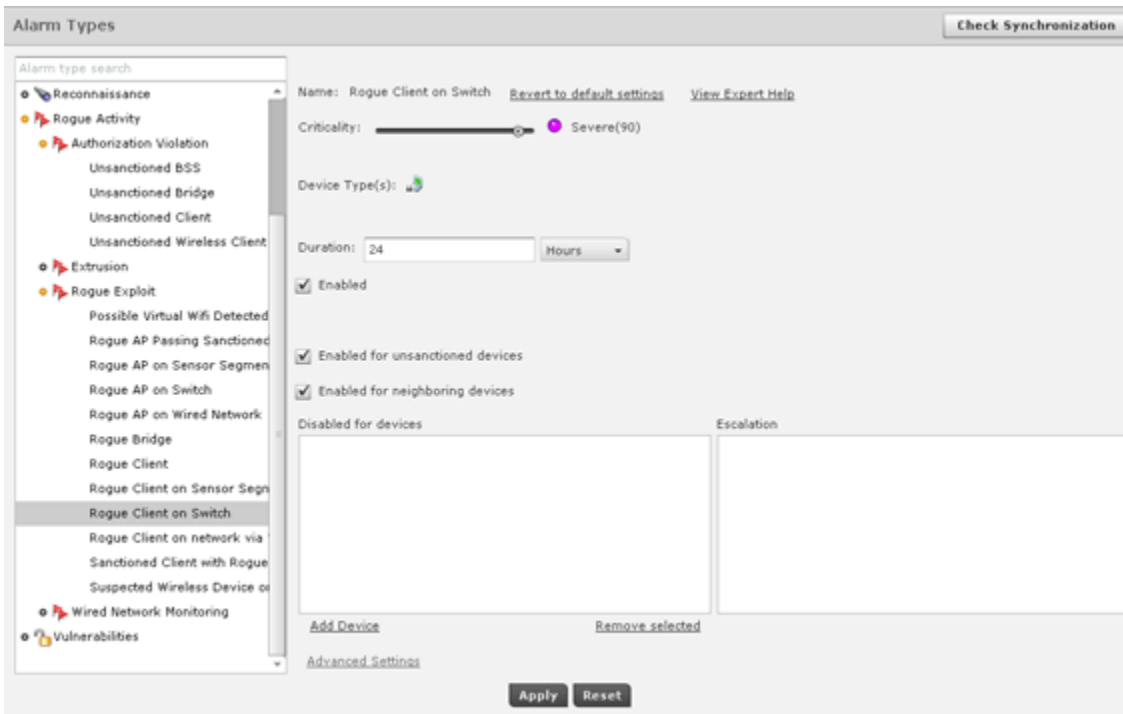
Alarm Configuration

ADSP generates alarms when certain events or conditions occur in your wireless LAN that violate a policy or performance threshold. The Alarm Types feature allows you to configure alarms for your network environment. ADSP alarms are categorized into 9 types so that you can easily identify them.

Each alarm type is broken down into sub-types and then the alarm themselves. The alarm types are:

- Behavior—Devices that operate outside of their normal behavior settings and generate events that could indicate anomalous or suspicious activity.
- Exploits—Events caused by a potentially malicious user actively interacting on your Wireless LAN using a laptop/PC as a wireless attack platform.
- Infrastructure—Events that are generated based on the SNMP traps received from the infrastructure devices.
- Performance—Wireless LAN traffic that exceeds set performance thresholds for devices.
- Platform Health—Events that provide information about the state of the AirDefense Services Platform and the sensors which report back to the appliance.
- Policy Compliance—Wireless LAN traffic that violates established or default policies for devices.
- Reconnaissance—Monitors and tracks external devices that are attempting to monitor your Wireless LAN.
- Rogue Activity—Unauthorized devices detected by ADSP which pose a risk to the security of your network.
- Vulnerabilities—Devices that are detected to be susceptible to attack.

Before you can configure an alarm, you must drill down to it using the alarm tree.



When an alarm is selected, the alarm configuration options are displayed on the right. You can view more information about an alarm by clicking the [View Expert Help](#) link. This will display another window where you can view the following alarm information by clicking the appropriate link:

- Summary—A summary description of the Alarm.
- Description—More detailed description of the alarm and what the likely cause is of the alarm.
- Investigation—Instructions for using tools and features in ADSP to investigate the Alarm.
- Mitigation—Suggestions on how to mitigate the problem detected.

You should change the options to fit your network environment. Available options are:

Option	Description
Name	The alarm's name.
Criticality	Use the sliding scale to set the alarm criticality to a value between 0 and 100. The designated color will automatically adjust as you move up or down the scale for Safe, Minor, Major, Critical, and Severe. The new numerical value will be used to calculate the Threat Score.
Duration	The Alarms View of the ADSP system displays all active alarms. An active alarm means that at least one condition occurred that triggered the alarm, and the condition still holds true. When the condition of the alarm no longer holds, the alarm will remain visible for an amount of time called the Alarm Duration. Although you can customize the Alarm Duration, the default values are based on Motorola AirDefense's extensive wireless security research. After the condition and the alarm duration have expired, the alarm becomes inactive, although it will remain visible in the historical logs, which can be viewed with Forensic Analysis. You can also clear an alarm before the duration expires.

Option	Description
Enabled	If checked, the alarm is enabled for all devices.
Enabled for sanctioned	If checked, the alarm is enabled for authorized devices.
Enabled for unsanctioned devices	If checked, the alarm is enabled for unauthorized devices.
Enabled for neighboring devices	If checked, the alarm is enabled for ignored devices.
Disabled for devices	<p>The alarm is disabled for any device listed in the table. Click the Add Device button to add a device to the list. You are prompted to enter the device's MAC address. Typing a partial MAC address will list all the devices matching your typed string. You can then select the device or devices that you want to select. When you click on a device, it is automatically added to the list. Typing the entire MAC address will list only the device matching that address.</p> <p>Clicking the Advanced link will display a Device Search dialog window. You can then search for a device using any combination of the following criteria:</p> <ul style="list-style-type: none"> • Device name • MAC address • 802.1X name • DNS name • Vendor name • SSID • Protocol used. <p>After selecting your search criteria, click the Search button to display a list of devices matching the search criteria. Click on the device or devices that you want to add to the device list. Click Close when you are done.</p> <p>You can return to the original window by clicking the Basic link where you can enter only the MAC address.</p> <p>Clicking the Remove selected link will remove the selected device from the list.</p>
Advanced Settings	Depending on the alarm, this link may or may not be active. Its function varies according to the alarm. Normally, you will enter a value to place limits on an alarm.

Device Age Out

Device Age Out allows you to specify an age out value that ADSP uses to display devices in the **Network** tab. For your convenience, a table is displayed listing the devices seen on your network.

You may set an age out value for any of the following devices:

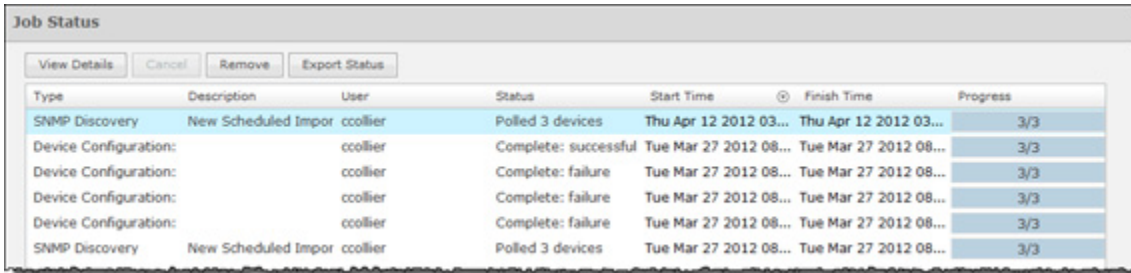
- Unsanctioned BSSs
- Ad-Hoc BSSs
- Unsanction Wireless Client
- Unknown, unsanctioned devices.

Values are specified in hours or days with a minimum of 1 hour and a maximum of 7 days. If you enter an illegal value, the field is highlighted by a red box.

After specifying an age out value, if that value is exceeded, the device will no longer be displayed in the **Network** tab but it will still be seen by forensics. Also, all alarms associated with the device are removed and will not display in the **Alarms** tab.

Job Status

Job Status allows you to view and check on jobs initiated by users using ADSP.



Type	Description	User	Status	Start Time	Finish Time	Progress
SNMP Discovery	New Scheduled Impor	ccollier	Polled 3 devices	Thu Apr 12 2012 03...	Thu Apr 12 2012 03...	3/3
Device Configuration:		ccollier	Complete: successful	Tue Mar 27 2012 08...	Tue Mar 27 2012 08...	3/3
Device Configuration:		ccollier	Complete: failure	Tue Mar 27 2012 08...	Tue Mar 27 2012 08...	3/3
Device Configuration:		ccollier	Complete: failure	Tue Mar 27 2012 08...	Tue Mar 27 2012 08...	3/3
Device Configuration:		ccollier	Complete: failure	Tue Mar 27 2012 08...	Tue Mar 27 2012 08...	3/3
SNMP Discovery	New Scheduled Impor	ccollier	Polled 3 devices	Tue Mar 27 2012 08...	Tue Mar 27 2012 08...	3/3

Job statuses are displayed in table format with seven columns.

Column	Description
Type	The job type.
Description	A description of the job. This information is collected when a user inputs a description when confirming an update.
User	The name of the user who initiated the job.
Status	Gives status information such as scheduled jobs, jobs completed successfully, jobs in progress, jobs that have failed, etc.
Start Time	The date and time the job started.
Finish Time	The date and time the job completed.
Progress	Displays a ratio representing the number of tasks completed over the total number of tasks to complete the job.

Jobs more than 7 days old will age out of the system and will not be displayed. While viewing jobs, you can:

- Cancel jobs
- Remove jobs from the Job Status list.
- Export a job's status.

- View job details. Details include:
 - The date and time the job was scheduled.
 - Which branches of the network tree are affected by the job.
 - A list of the devices that are affected by the job along with a status for each device.
 - Details about each affected device.

While viewing job details, you can:

- Export the job's status to a file on your workstation.
- Cancel the job.
- Save any changes such as changing the job description.

Location Based Services

A Proximity and Analytics license is required to access Location Based Services,

Pending State Audit

A WLAN Management license is required to access Pending State Audit.

Sensor Only Settings

Sensor Only Settings are used to configure network settings for legacy Sensors and WING 5.3 (and higher) that are configured as a Sensor only device. Legacy Sensors include Motorola AP300, AirDefense M400, M510, and M520 Sensors.

The following fields available to configure your legacy Sensor settings:

Field	Description
Primary Appliance	Specifies the IP address of the primary appliance.
Secondary Appliance	Specifies the IP address of the secondary appliance.
Sensor Admin Password	Specifies the admin password for your Sensors. Supplying this password is mandatory.
Sensor Monitor Password	Specifies the monitor password for your Sensors.
Link Speed	Selects the link speed. Link Speed Control enables you to set the Ethernet interface to either auto-negotiate (default), or to fix the interface to 10Mbps (Full or Half duplex) or 100Mbps (Full or Half duplex).
MTU	Specifies the Maximum Transmission Unit.
Enable IP Alias	Turns on IP aliasing.
CDP Interval with interval	Turns on CDP and then enter an interval in seconds.

Field	Description
Enable FIPS mode	FIPS Level Encryption is disabled by default. FIPS level encryption is generally not needed. If you want to use FIPS level encryption, select the checkbox. This setting controls the https encryption level between the Sensor and the browser. When selected, the Sensor will only allow AES encryption to the browser (Sensor UI). Only browsers that support this type of encryption will be able to connect to the Sensor UI (e.g. Firefox) once this setting is configured to 'yes. If you are using IE, do not select this option. Communication between the Sensor and the server is not affected by this setting, and is always negotiated for AES. Note: FIPS level encryption is incompatible with Internet Explorer.
Remote syslog to address	Selects if you want to use a remote Syslog host. You must enter the host IP address along with the port number.
Radio 1 (b/g) custom gain (dbi)	Increases the signal level of radio 1 antennas by the specified value (in dbi).
Radio 2 (a) custom gain (dbi)	Increases the signal level of radio 2 antennas by the specified value (in dbi).
Prevent Auto Adoption	Prevents a sensor from being adopted by a switch.

Sensor Operation

Sensor Operation settings allow you to:

- Enable Sensor-level options
- Configure the Sensor scan pattern
- Configure sensor settings for Advanced Spectrum Analysis.

The **Scan Settings** and **ASA In-Line Settings** tabs are used to configure Sensor Operation.

Scan Settings

The **Scan Settings** tab is used to enable Sensor-level options and configure the Sensor scan pattern. The scan settings are configured at the appliance level of the network tree and inherited by all lower levels.

The **Scan Settings** tab allows you to configure the following settings:

Feature/Function	Description
Air Termination	Air Termination lets you terminate the connection between your wireless LAN and any access point or Station associated with it. By default, Air Termination is disabled. It can only be enabled in the Appliance Manager.
Background SA Scan	Spectrum Analysis has the capability to run background scans. By default, background scans are disabled.
WEP Cloak	WEP Cloaking is an add-on tool that injects "noise" into a WEP-protected environment by transmitting frames that appear to be sourced from valid devices but are encrypted with an invalid WEP key. By default, WEP Cloaking is disabled.

Feature/Function	Description
Adaptive Scan	Initially scans the selected channels and then adjusts the scan to concentrate on the channels with the most traffic. By default, Adaptive Scan is disabled.
Enable Location Tracking RSSI Scan	Devices can report RSSI scan data to ADSP. This option allows you to use that data in location tracking. Once this option is selected, you can adjust the location tracking refresh rate from 1 to 60 seconds. The optimal rate is 1 second. (You must have a Promiximity and Analytics license before this option is visible.)
Scan Mode	<p>You can choose channels to monitor by selecting one of the following scan modes:</p> <ul style="list-style-type: none"> • Default Scan—the table displays the channels that will be scanned and is not editable. • Extended Channel Scan—the table displays all standard channels plus the extended channels that will be scanned. • Extended and Emergency Channel Scan—the table displays all channels including emergency channels that will be scanned. • Custom Scan—the table displays all available channels and allows you to select channels, select the 802.11N extension, and set scan weight for each selected channel. A scan weight of 1 specifies that the selected channel will be scanned once during each scan rotation. A scan weight of 2 specifies that the selected channel will be scanned twice and so forth. The scan sequence is determined by the specified scan weights. All selected channels are initially scanned once during the scan rotation. Any selected channels that have weights of 2 or more are then scanned again at the end of each rotation period for the number of times specified by the weight value. For example, if channels 1, 6 and 11 are assigned scan weights of 1, 2 and 2, the channel scan sequence is 1-6-11-6-11. Another example is if channels 1, 5, 6 and 11 are assigned scan weights of 2, 1, 3 and 3, the channel scan sequence is 1-5-6-11-1-6-11-6-11. • Channel Lock—used to lock a Sensor on a specific channel for scanning. A dropdown menu is displayed where you can select a channel. NOTEAll channels in the 2.4 and 5 GHz bands are grouped together.

ASA In-Line Settings

The **ASA In-Line Settings** tab is used to configure sensor settings for Advanced Spectrum Analysis.

These settings are for the ASA In-Line based scan, not for the Dedicated scan. There are four settings: two for 2.4 GHz band and two for 5GHz band. The values in the fields are the default settings. Normally, these levels are fine for normal use and should not have to be changed.

Threshold (dBm)—This is the master level control for ASA scanning. Any signal levels below the threshold during scanning will be dropped. Only levels greater than the threshold will be admitted for further processing.

Duty Cycle (dBm)—The duty cycle is a measure of % utilization for each frequency. 100% duty cycle for a frequency indicates the frequency is busy all the time. On the other hand, 0% duty cycle indicates the frequency is not used. The Duty Cycle controls the threshold level for duty cycle measurement. Only signal levels greater than the Duty Cycle threshold are counted in the duty cycle measurement.

Account Management

Account Management allows you to:

- **Account Access**—Create and modify user accounts and group accounts.
- **Local Authentication**—Authenticate users on the local appliance.
- **Password Reset**—Change the password of the current user.
- **Remote Authentication**—Authenticate users by using the password stored on a RADIUS or LDAP server.
- **User Preferences**—Specify the user preferences that are used to set the ADSP auto refresh rate and to specify a proxy to access the server.

Account Access

As part of the installation process, AirDefense Services Platform sets up an Admin user account. The Admin user may create other user accounts (including Admin) or group accounts. All Admin users have the ability to create additional accounts and change user or group accounts.

AirDefense Services Platform also tracks some functionality by account, regardless of role, such as keeping track of private vs shared reports and logging appliance activity.

User Roles

User roles are defined for both user and group accounts. AirDefense Services Platform contains four default role types. The Admin user who creates each account can assign one of these default roles to each account or can customize a user role regardless if the account is a user account or group account. The roles have different levels of access to ADSP functionality.

For some roles (types), some functionality may be grayed out or may not be visible in the interface at all. If there is functionality that you want to use, but that is unavailable to you, you may want to contact the system administrator to discuss your user role (type).

There are four default role types:

- **Admin**—Gives users read/write permission to all functional areas.
- **Guest**—Gives users read permission to Alarm Management, Reporting, Analysis Tools, and Connection Troubleshooting. No access is provided for the other functional areas.
- **Helpdesk**—Gives users read/write permission to Connection Troubleshooting. No access is provided for all other function areas.
- **Operation Center**—Gives users read/write permission to all functional areas except Appliance Management, Network Management, and System Configuration. No access is provided for these three function areas.

Functional Area	Capabilities (use of)
Network Management	<ul style="list-style-type: none"> • Configure performance policy • Configure configuration policy • Configure monitoring policy • Configure infrastructure profiles • Configure sub-profiles • Action Manager use • Auto classification of devices • Network setup • Map configuration • Auto Placement • Discovery policies • Manual modification to network tree hierarchy • Device placement • Inherited policy/profile assignment (network and device levels)
Threat Mitigation	<ul style="list-style-type: none"> • Manual termination • ACL • Port suppression
System Configuration	<ul style="list-style-type: none"> • Basically, configuration categories that affect the whole system
Reporting	<ul style="list-style-type: none"> • Reporting UI • Report builder
Analysis Tools	<ul style="list-style-type: none"> • Live View • LiveRF • Location Tracking • Spectrum Analysis • Advanced Forensics • Scope Forensics
AP Test	<ul style="list-style-type: none"> • On-demand or scheduled AP Test • AP Test profiles
Vulnerability Assessment	<ul style="list-style-type: none"> • On-demand or scheduled Vulnerability Assessment • Vulnerability Assessment profiles
Connection Troubleshooting	<ul style="list-style-type: none"> • Troubleshooting tools

Functional Roles

There are four functional roles for users:

- Security—Manage security alarms.
- Platform Monitoring—Manage the alarms that monitor the platform (system).
- Locationing—Manage the alarms triggered by Location Based Services.
- Performance Monitoring and Troubleshooting—Manage the alarms that monitor platform (system) performance and alarms generated by troubleshooting features such as AP Test.
- Infrastructure Management—Manage the alarms dealing with infrastructure management.

Scope Permissions

You can limit users to accessing and/or managing specific levels within the network tree. If you want users to have full access, give them permission to access the entire system. If you want users to only have access to a specific floor within a building, give them permission to access just that floor. You can limit access to any network level.

Viewing User Information

You can view the following information about existing user accounts from **Configuration > Account Management > Account Access**:

- Username
- Full Name
- Description
- Authentication Method
- Functional Area Access
- Functional Role
- Scope Permissions.

Creating and Changing User Accounts

ADSP makes it easy to balance easy access to the system with a high level of system security and the ability to track the actions of users. Admin users can create numerous user accounts with varying levels of platform (system) access.

For each account you create, you will need to enter the following information:

- Username
- Full Name
- Description
- Authentication method (Local or an external authentication profile you have previously configured. See [“Authentication”](#).)
- Password
- Functional Area Access



NOTE You can also apply one of the templates: Admin, Guest, Helpdesk, Operation Center which have predefined functional area access.

- Functional Role
- Scope Permissions.



NOTE You must save any changes by clicking the **Save** button.

Changing Passwords

If you are an Admin user, you can change passwords for other users. You do not need to know the current password. Additionally, all users can change their own password using **Password Reset** under **Configuration > Account Management**, but they must know their current password to change it. Non-admin users who have forgotten their password will need an Admin user to create a new one.

Password Criteria

Password must include lowercase letters, uppercase letters, numbers and symbols. Password must be 8-32 characters in length. Password may not contain spaces or tabs.

Important! You should change the default admin account user password at your first opportunity. Leaving the default password on the system poses a security risk.

Creating and Changing Group Accounts

Group accounts involve a group of users set up through remote authentication (either LDAP or RADIUS). When a user attempts to log into ADSP that is a member of a group, ADSP first uses local authentication to log in the user. If the user is not part of local authentication, remote authentication is used. Upon finding the user's credential using remote authentication, the group status is checked. If the user belongs to a group, ADSP uses the group account to log the user into ADSP.

For each account you create, you will need to enter the following information:

- Group name
- Description
- Disable group login (disables the login for the group)
- Test Authentication (test remote user authentication using LDAP or RADIUS)
- Feature Permissions (functions the same as in user accounts)
- Functional Roles (functions the same as in user accounts)
- Scope Permissions (functions the same as in user accounts).

Authentication

This section describes your options for controlling how ADSP appliance authenticates users. By default, when creating a new user account, local authentication is selected. However, you can alternatively use existing remote authentication sources like a RADIUS or LDAP authentication server.

Deciding which method your organization wishes to use should be done during the hardening of the infrastructure.

Remote authentication lets your organization consolidate authentication databases for easier administration. A potential problem with remote authentication may arise if the authentication server is not available because of network problems or problems on the appliance hosting the authentication service. For this reason, you should maintain one or more Admin user accounts with local authentication.

AirDefense Services Platform offers the security of being an appliance-based solution, so the default local authentication may meet your network's requirements without the introduction of remote services.

Setting users up for local authentication is a two-step process:

1. Configure local authentication on the ADSP appliance.
2. Assign local authentication to existing or new users.

Setting users up for remote authentication is a three-step process:

1. Configure remote authentication on the ADSP appliance.
2. Configure the authentication server on the ADSP appliance.
3. Assign remote authentication to existing or new users.

What you need to know

There are no special steps to set up local authentication. Just select **Local Authentication**.

To set up remote authentication, you will need to know:

- RADIUS server:
 - IP Address of the RADIUS Server
 - Protocol (PAP, CHAP, MSCHAP, and MSCHAPv2)
 - RADIUS Port (RADIUS authorization server port number)
 - RADIUS Accounting Port (RADIUS accounting authorization server port number)
 - Shared Secret (The password that is used and shared by both the Authentication Server and the Authentication Profile)
 - The time (in seconds) when a connection process will time out
 - The number of connection retries to be allowed
 - User Prefix which is the windows domain for the server (e.g., qaairdefense\)
 - User Suffix which is the internet domain name for the server (e.g., motorola.com)
 - Use RADIUS for external group based authentication. If checked the following fields are displayed:
 - Server type—For now, Active Directory is the only option. The information supplied in the other four fields are used in group identification for the Active Directory server type.
 - Search Base—String to find your domain name in the directory. Normally, the string is DC=yourdomainname.
 - User field name—String to find your user name in the directory. Normally, the string is sAMAccountName.
 - Group attribute—String to find your group name in the directory. Normally, the string is memberOf.
 - Group Reg Ex—Enter a string that is used to strip out only unnecessary information and send what's left to ADSP for use in group identification. Normally, the string is CN=([^\,]*).
 If the LDAP administrator changes any of the strings from what is normally used, he/she must inform you of the string to use.
- LDAP server:
 - IP Address of the LDAP Server
 - Protocol (LDAP or LDAPS)
 - LDAP Port (authorization server port number)
 - User Prefix which is the windows domain for the server (e.g., qaairdefense\)
 - User Suffix which is the internet domain name for the server (e.g., motorola.com).
 - Use LDAP for external group based authentication. If checked the following fields are displayed:

- **Group attribute**—Displays a list of attributes to identify a group to ADSP. When an attribute is selected, values are inserted into the **Vendor code**, **Attribute code** and **Group RegEx** fields for ADSP to use in group identification. You should not change any of the inserted values.

User Preferences

User Preferences are used to specify the ADSP auto refresh rate and to specify if a proxy should be used to access the appliance. Navigate to **Configuration > Account Management > User Preferences**.

Auto Refresh

ADSP application data is automatically refreshed according to the refresh rate that you specify. The following rates are available:

- No auto refresh—Turn off automatic refresh.
- 10 minute refresh—Automatically refresh ADSP data every 10 minutes.
- 5 minute refresh—Automatically refresh ADSP data every 5 minutes.
- 1 minute refresh—Automatically refresh ADSP data every minute (default).

Log Level

The **Log Level** field allows you to select one of the following levels for ADSP to create log entries:

- Fatal
- Error
- Warning
- Info
- Debug
- All.

Device Inactivity

You can define your own device inactivity rule by setting the **Last seen within prior** time values for the **First/Last Seen** network filter by selecting one of the following values:

- 5 minutes
- 10 minutes (default)
- 20 minutes
- 30 minutes
- 1 hour
- 12 hours
- 24 hours
- 72 hours.

For instance, if the **Device Inactivity** is set to 10 minutes, the **Last seen within prior** time values for the **First/Last Seen** network filter are set as follows:

- The **0 - 5 minutes** option is selected

- The **5 - 10 minutes** option is selected
- All other options are unselected.

When viewing devices in the **Network** tab, the row of any device that is considered inactive will have lighter text than active devices.

Copy MAC Formats

Copy MAC Formats allows you to specify the formats you can use when copying a MAC address for a device in ADSP. You may select any or all of the following formats:

- ff:ff:ff:ff:ff:ff
- ff-ff-ff-ff-ff-ff
- ffff.ffff.ffff
- ffffffff

Once set, when you copy a device's MAC address, you will have a choice of formats. Now, when you select **Copy MAC** from a device's right-click menu, a menu is displayed with the available formats for that MAC address.

Use Proxy to Access Appliance

You can specify that users must use a proxy to access your ADSP appliance. To do so, you must know the IP address and port number of the appliance. If authentication is required to access the appliance, you must also know the the username and password.

Network New Column Preferences



NOTE This feature operates only on columns affected by a system refresh (the **Sensor, AP, Associated Clients, Associated BSS, Adopted APs, Severity, Floor, and Scope** columns). Columns displaying only device information that does not change are not affected.

When adding a new column to the **Network** tab, you can set the following default refresh preferences:

- User refresh is required to populate data in the column.—You will have to refresh ADSP before the column data is populated in an added column.
- System will auto-refresh when columns are added.—ADSP automatically populates the column data when a column is added.
- Don't show dialog in network tab again.—The dialog window will not display.

These preferences are displayed as a dialog window, unless **Don't show dialog in network tab again** has been selected, whenever a new column is added to the **Network** tab. When the dialog window is displayed, you can change the auto refresh preferences.

Password Reset

Users can change their passwords by supplying their old password; then entering a new password. The new password must be verified.

The Menu

The Menu gives you access to the ADSP standalone features.



Most of the standalone features are Java applets. Reports and Help are web-based applications. Add Devices and Import/Discover Devices are an integral part of ADSP.

To run the Java applets, you are required to install the ADSP Toolkit on your local workstation. The ADSP Help and the *AirDefense Services Platform 9.0 Upgrade Instructions* have instructions on how to install the toolkit.

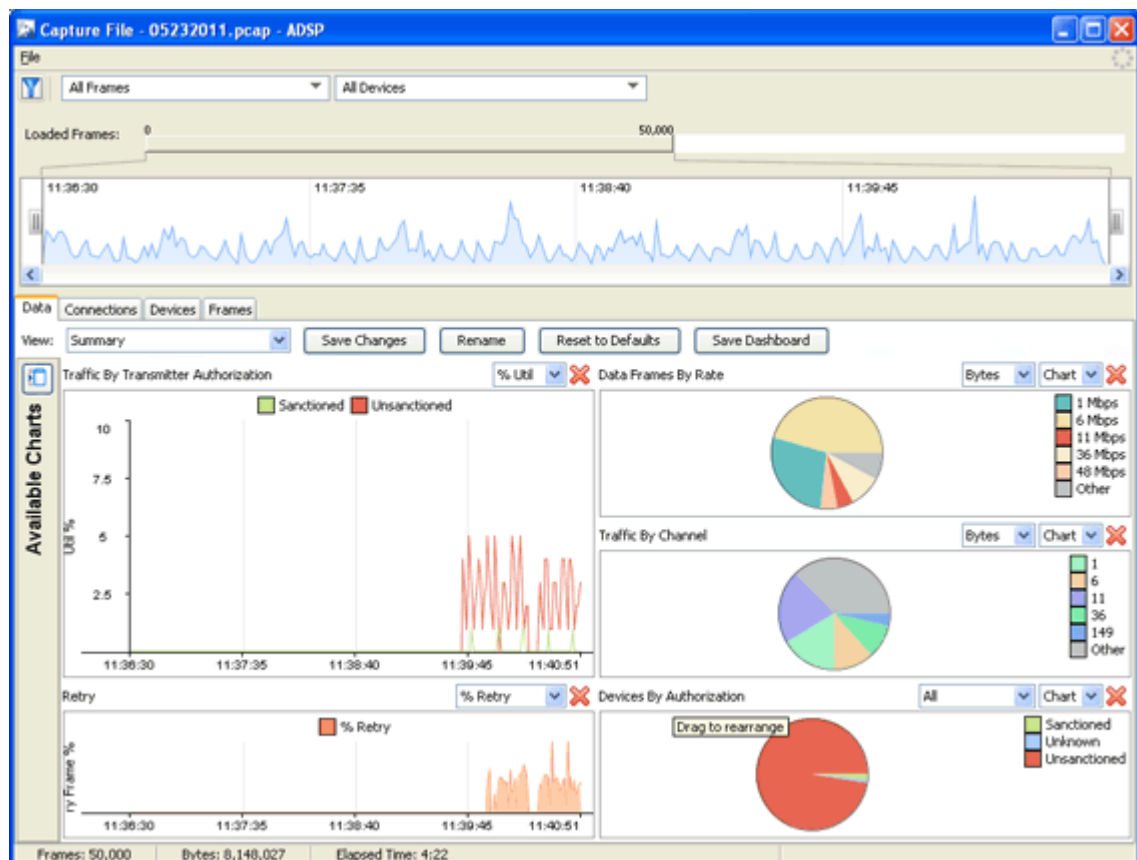
Open

Opens a saved Frame Capture file or a saved Spectrum Analysis file.

Frame Capture Analysis

Live View saves session frame data in a temporary file on your ADSP appliance. This process is called Frame Capture. You can save the temporary file to a permanent file on the appliance or to a file on your workstation. To save a file, you must first stop the Live View session and then select **File > Save** from the **Live View** window to display the **Save Frame Capture** popup window.

Once the file is saved, you can view it using Frame Capture Analysis. You can access this feature by selecting **Menu > Open > Frame Capture** and then selecting the capture file. The frame data is displayed in the **Capture File** window.

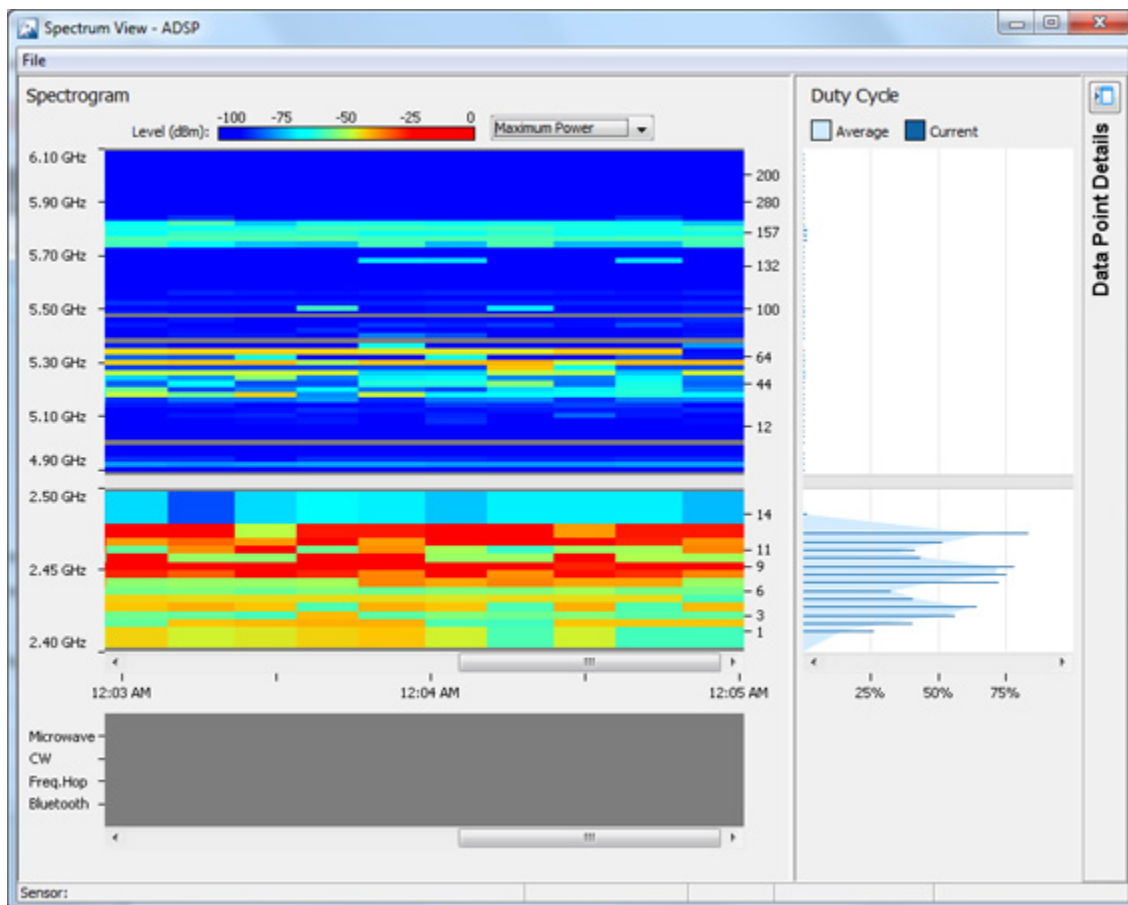


The **Capture File** window is basically the same as the **Live View** window minus the buttons and menus that are not needed for Frame Capture Analysis. The tabs display the same information as the **Live View** window.

Spectrum Analysis

After conducting a Spectrum Analysis, you can save the temporary spectrum data to a permanent file on the appliance or to a file on your workstation. To save a file, you must first stop the Spectrum Analysis and then select **File > Save** from the **Spectrum View** window to display the **Save Spectrum Data** popup window.

You can access the saved spectrum data by selecting **Menu > Open > Spectrum Analysis** and then selecting the spectrum analysis file. The spectrum data is displayed in the **Spectrum View** window.




The **Spectrum View** window is opened minus the buttons and menus that are needed for generating spectrum analysis data.

Forensic Analysis

Forensic Analysis is used to review specific device information and provides detailed device communication and association status. Whether you are investigating a suspicious device or troubleshooting a WLAN problem, use the Forensic Analysis tool to analyze any device seen by the system and display threat level of the device, device alarms, device associations, and detailed device statistics. This window is a universally applicable function, which furnishes additional detail on devices detected by ADSP. The device can be an AP, Sensor, Switch, BSS, or Wireless Client.

Accessing Forensic Analysis

To access Forensic Analysis, select **Menu > Forensic Analysis**, then select an AP, Sensor, or Switch, or supply the MAC address of a BSS or Wireless Client to analyze.

You can also click the dropdown menu button— of a device anywhere within ADSP, and then select the **Forensic Analysis** from the menu to drill down into the device statistics.

Forensic Time Window

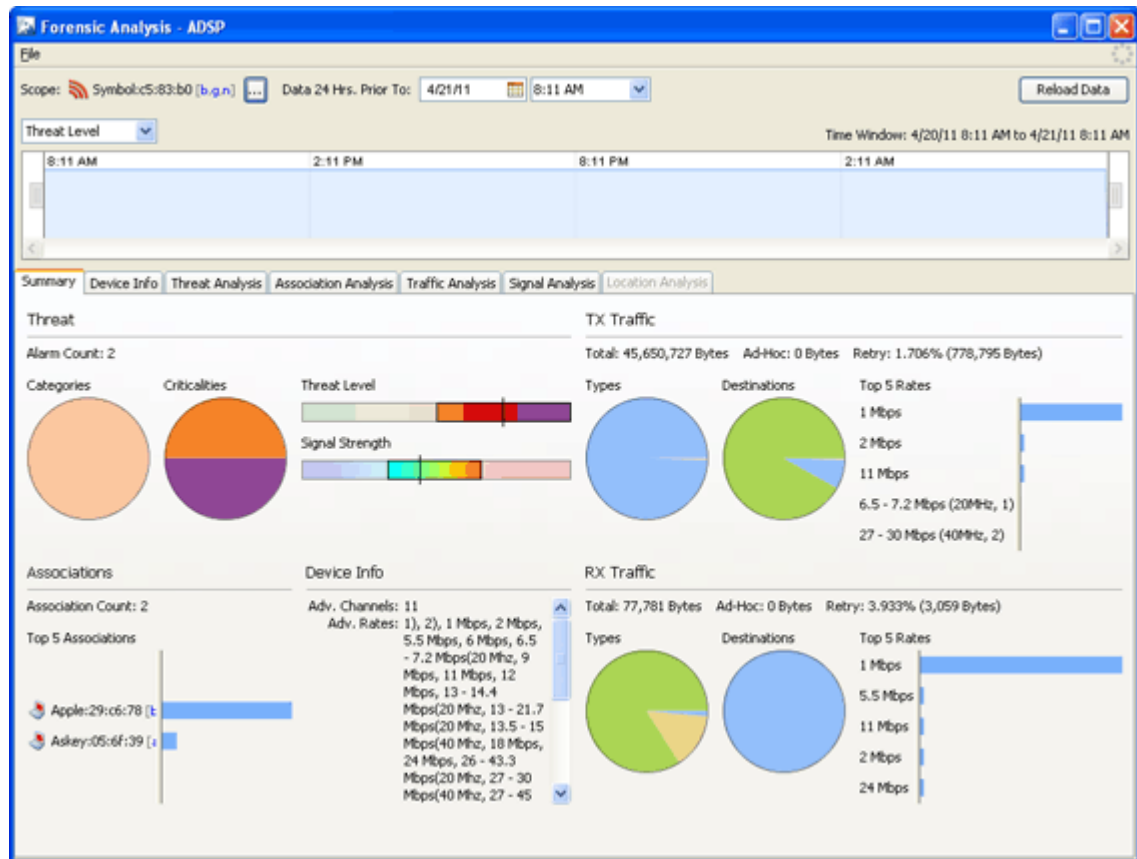
Forensic Analysis, by default, only shows 24 hours worth of data. For detailed historical analysis, you can change the 24 hour time period by selecting a new date and time. However, you cannot view more than 24 hours of data at any one time.



NOTE Advanced Forensic Analysis allows you to specify your own time period which can exceed 24 hours.

Forensic Data

When Forensic Analysis is first accessed, a summary of forensic data is provided with information about threats, associations, device information, transmitting traffic, and receiving traffic.



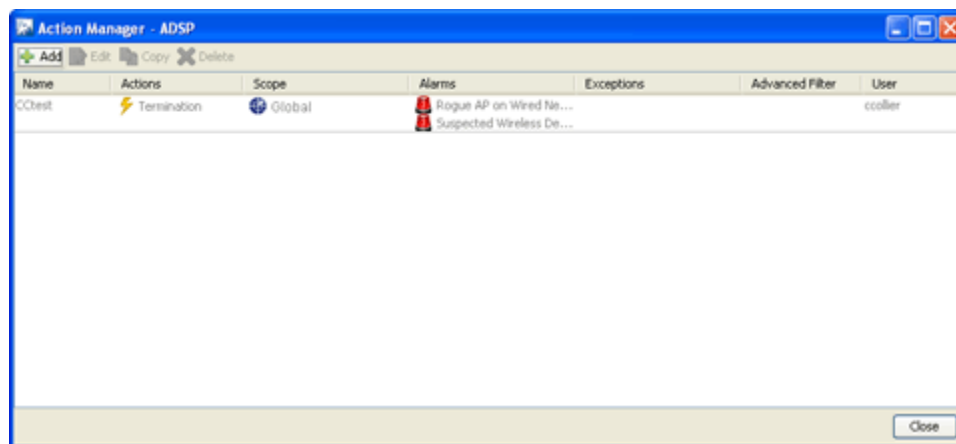
If you select one of the following tabs, the summary is expanded into more detailed forensic data so that you can learn more about the wireless device and if necessary, take immediate action:

- **Device Info** (All devices) Displays the current settings for the device being analyzed.
- **Threat Analysis** (All devices) Displays a table of alarms generated by the device being analyzed.
- **Association Analysis** (BSSs and Wireless Clients) Lists the associations between the device being analyzed and other wireless devices.
- **Traffic Analysis** (BSSs and Wireless Clients) Displays traffic transmitted and received by the device being analyzed.

- **Signal Analysis** (BSSs and Wireless Clients) displays a device's signal strength (in dBm) as measured by various Sensors.
- **Adoption History** (APs and Switches) For APs, provides a table of devices that have adopted the selected AP. For Switches, provides a table of devices that the selected Switch has adopted.
- **Radio Analysis** (APs) provides information that can be used to analyze your AP's radios.
- **Radio Info** (APs) provides AP radio information recorded at the displayed time.
- **Performance Analysis** (Switches) provides performance raw data and usage percentages for the selected Switch.

Action Manager

The Action Manager allows you to automatically respond to alarms in your system with a predetermined action called an Action Rule. You may define as many Action Rules as you need to manage your network.



Action Rules are added to the Action Manager to define an action (response) to an alarm. Multiple actions may be assigned to a rule.

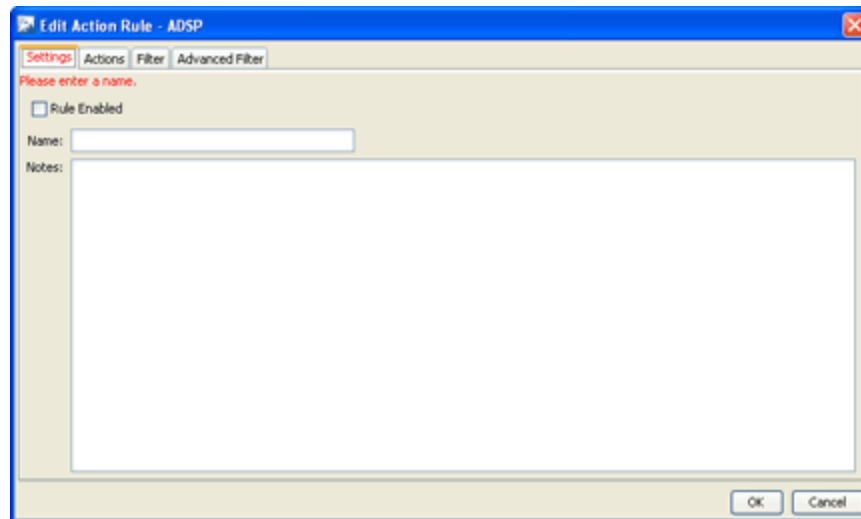
The Action Manager table displays one rule per row using the following columns:

Column	Description
Name	The name of the Action Rule.
Actions	The action(s) triggered by the Action Rule.
Scope	The scope to which the Action Rule applies.
Alarms	The alarms or alarm categories that trigger the Action Rule.
Exceptions	Exceptions to the Action Rule related to the scope, alarms, or devices.
Advanced Filter	Custom filter or expression used as a filter.
User	The name of the user who created the Action Rule.

Once an Action Rule is added to the Action Manager, you can edit, copy, or delete it by clicking on the appropriate button.

Add/Edit Action Rule

The **Edit Action Rule** window is where you add an Action Rule or edit an existing Action Rule.



The **Edit Action Rule** window has four tabs that are used to define an Action Rule.

Settings Tab

The **Settings** tab is where you identify and enable your Action Rule. You can also specify notes to provide information about the rule.

Actions Tab

The **Actions** tab is where you define the actions for your Action Rules. Available actions are:

Action	Description
Termination	Terminates devices that generate a certain alarm defined in the Filter tab.
Port Suppression	Suppresses communication between unsanctioned devices and switches on your network.
ACL	Enables the Access Control List on switches that meet the conditions defined in the Filter tab.
Report	Runs a specific report if the conditions defined in the Filter tab are met.
E-Mail	Sends information about an alarm via email to a recipient if the conditions defined in the Filter tab are met. A mail relay must be configured before E-Mail action rules will work.
Syslog	Sends an alarm notification to your Syslog server if the conditions defined in the Filter tab are met.
SNMP Trap	Sends an SNMP notification to your SNMP server if the conditions defined in the Filter tab are met.
Frame Capture	Monitors and analyzes real-time data traffic flow from devices in your wireless LAN and saves the data in a file if the conditions defined in the Filter tab are met.

Action	Description
AP Test	Runs an AP Test using the specified profile if the conditions defined in the Filter tab are met. (Requires an Advanced Troubleshooting license.)
Vulnerability Assessment	Runs a vulnerability assessment using the specified profile if the conditions defined in the Filter tab are met. (Requires a Vulnerability Assessment license.)
Data Collection/Compliance	Automatically corrects configuration compliance violations when the conditions defined in the Filter tab are met.
LiveRF	Opens the Floor Plan to display Live RF data if the conditions defined in the Filter tab are met. (Requires a LiveRF license.)

Filter Tab

The **Filter** tab is where you define the scope, alarms and exceptions for an Action Rule. Three types of filters are available:

Filter	Description
Scope	Limits the scope of the Action Rule to the system level, location level, or group level.
Alarm	Specifies an alarm that will trigger your Action Rule. The following alarms may be used as triggers: <ul style="list-style-type: none"> • Behavior • Exploits • Infrastructure • Performance • Platform Health • Policy • Reconnaissance • Rogue Activity • Vulnerabilities.
Exceptions	Adds an exception if you want to specify an exception condition for the Action Rule. There are three types of exceptions: <ul style="list-style-type: none"> • Scope • Alarms • Device.

Advanced Tab

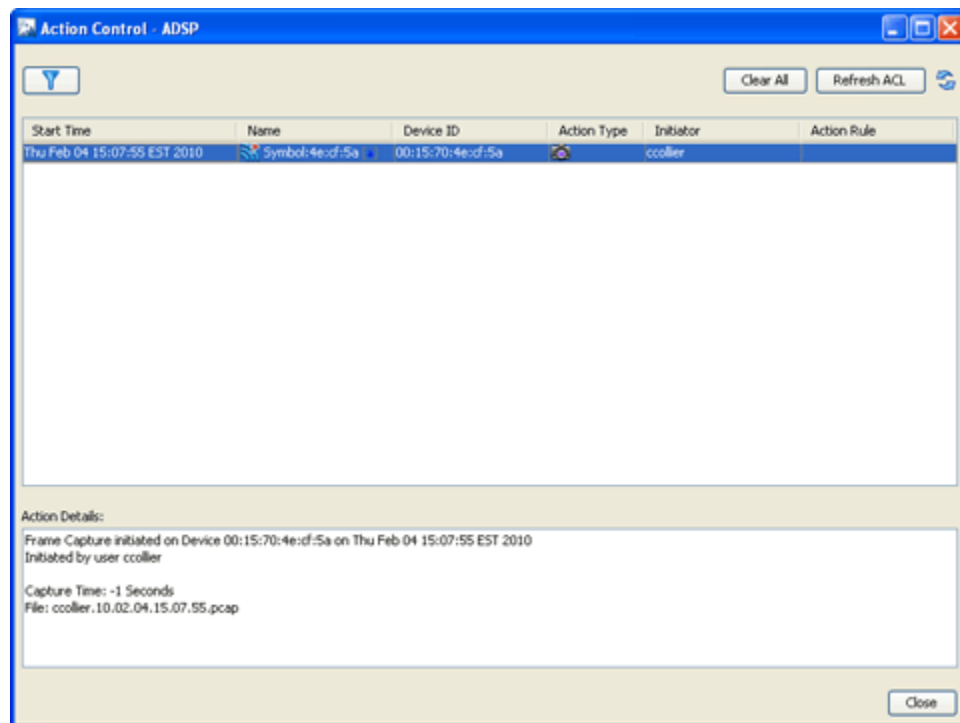
The **Advanced Filter tab** allows you to build a custom alarm filter or an expression to use as a alarm filter. Two advanced filters are available:

Filter	Description
Filter List	Builds an alarm filter using dropdown menus to form an expression.
Expression Editor	Allows you to build an alarm filter using custom expressions.

Action Control

Action Control displays a table listing specific actions that are occurring to devices seen on your WLAN. The type of actions displayed are:

- Air Termination
- Port Suppression
- ACL
- Frame Capture.



Selecting an action displays details about the action in the **Action Details** window.

Action Control Table

The Action Control table displays specific information about an action that is taking place. The following information is included:

Column	Description
Start Time	The date and time the action was initiated
Name	The name of the device the action was performed on
Device ID	The MAC address of the device
Action Type	The type of action that was performed
Initiator	The user name of the person who initiated the action
Action Rule	The name of the Action Rule if action was initiated by an Action Rule

Action Control Commands

Also, while an action is highlighted, you can right click on the action to display options (commands) that can be performed on that action. The following commands are available:

Action	Available Commands
Air Termination	Cancel
Port Suppression	Cancel Port Suppression (re-enable port)
ACL	Cancel Access Control (remove from ACL)
	Re-Apply Access Control List
	Refresh Access Control List Status
Frame Capture	Cancel Frame Capture

You may select more than one action. If you select one or more actions that are the same, the commands for that action are available. If you select one or more actions that are different, the only command available is **Cancel All** which will cancel any highlighted action.

Reporting

AirDefense Services Platform's dual approach to reporting consists of a web interface for populating report templates with data, and a flexible interface for creating additional custom report templates.

- The **Web Reporting interface** makes it easy to choose report templates and define the scope of data you want to include, then view the resulting report in a selection of formats. You can also save reports, share them with others, and schedule reports to run automatically.
- The **Report Builder application** within the GUI lets more advanced users create report templates, either basing them on the templates delivered with ADSP or designing them from scratch. Reports you create with the report builder become available as templates in the Web Reporting interface.

Using Web Reporting

Accessing Web Reporting

To access the Web Reporting web site, log into the GUI and then select **Menu > Reports**. The report names are displayed by category.

Web Reporting Navigation

The Web Reporting application consists of three tabs, described below. To move from one page to another, click the tab name.

- **Reports** —The Reports tab is the default tab; it lists standard and custom report templates by category. You can select a report, specify applicable settings, and then display the report with data.
- **Published** —The Published tab lists the reports that you have run and saved as a published report. You cannot view a report published by another user unless that user shares the report. Once a report is published, you can:
 - View published report data by clicking on the report's name.
 - Delete a published report by checking its checkbox and clicking **Delete**.
 - Share a published report by checking its checkbox and clicking **Share**.
 - Make a published report private by checking its checkbox and clicking **Unshare**.
 - Rename a published report by clicking **Rename**, typing in a new report name, and then clicking **Apply**.
- **Favorites** — The Favorites tab is where you save reports that you run often. When a report is designated as a favorite, you can:
 - Edit the favorite report settings that are set when you create a report by clicking **Edit Settings**.
 - Schedule the report to run automatically.
 - Delete a favorite report by checking the checkbox next to the report and then clicking the **Delete** button.

The Online Help describes each of these tabs in detail. It also explains how to create reports, add reports to the Favorites tab, schedule reports.

Report Descriptions

There are six types of reports:

- **Compliance Reports**—reports that show you are in compliance with certain agencies or policies.
- **Device Reports**—reports that help you view the status of devices that comprise your wireless network.
- **Performance Reports**—reports that help you assess the health and performance of your wireless network and its components.
- **Security Reports**—reports that help you assess your organization's current wireless security posture.
- **Infrastructure Management Reports**—reports that help you manage infrastructure devices.
- **Custom Reports**—reports customized by a user to show only information that is useful/helpful to that particular user. Custom reports are built using the Report Builder.

See the ADSP Help for a detailed explanation of the individual reports generated for each report type.

Using the Report Builder

Creating a Report

Report Builder lets advanced users create completely original reports from blank templates. Alternatively, you can choose a report template you like and edit it. All report components are based on whether you want a report on a single device or multiple devices. Different components are available for single device reports than for multiple device reports.

Extensive Data

ADSP collects extensive data about traffic on your WLAN. The Report Builder lets you create reports using virtually any data point the appliance collects. The graphic below shows an example tree in the Report Builder and some elements from the resultant report, along with tips on how to add different types of components.

You control what's in the header section of the report by adding the Simple Component Report Header to the tree. Simple Components are general things that are generic to all reports, like Titles.

802.11 Wireless Network Health
From 2010-02-01 14:00:19 to 2010-02-02 14:00:19

System Name: mshw-wids-mgr-013
Scope: system
Generated: 2010-02-02 14:00:33
Version: 8.0.0-24
Time Zone: EST - Eastern Standard Time

Report Builder - system

File Edit

New Open Save

Report Structure

- Performance_WLAN_Health
 - Header
 - Performance_Summary_Section
 - Column1
 - Performance_Summary
 - Perf_Alarms_By_Cat
 - Total_Performance_Alarms
 - Performance_Top_10
 - AlarmTable1
 - PageBreak1
 - Performance_Details_Section
 - Column2
 - Alarm_Details_Title
 - Config_Compat_Title
 - Config_Comp_Alarm_total_Co
 - Config_Comp_Top10
 - Congestion_Title
 - Congestion_Alarm_Total
 - Congestion_Alarm_Top_10

You can insert a new section to control how many columns appear in different parts of the report. This section has one column.

Performance Summary

Performance Alarms By SubCategory

This is an example of a chart. When you add charts, you should remember that they do not convert well to CSV format, so you should probably not combine graphs and tables in reports that you want to save as a CSV file.

Alarm Details

Top 10 Configuration/Compatibility Alarms

Alarm	Severity	Count
Auth Failed (1)	Warning	10
Auth Failed (2)	Warning	8
Auth Failed (3)	Warning	7
Auth Failed (4)	Warning	6
Auth Failed (5)	Warning	5
Auth Failed (6)	Warning	4
Auth Failed (7)	Warning	3
Auth Failed (8)	Warning	2
Auth Failed (9)	Warning	1
Auth Failed (10)	Warning	1

This is an example of a table. You add tables by selecting a node you want to add the table to, then select Insert > Table.

Creating and Saving a Report

1. Click **New** on the tool bar.

- Choose a template. Either choose an existing report to edit, or choose the blank report for either a single device or for multiple devices.



NOTE You cannot change the number of devices after you start a report on the same report; you must create a new report.

- Type the name you want to use for this report.



NOTE The name must start with a letter and cannot have any spaces or symbols, with the exception of _ (underscore).

- Click **OK**, and then click **Save**.

Building Your Report

After you have created and saved a report, regardless of whether you started with a blank template or an existing report, use the following guidelines for building it out:



NOTE Right-click menus make it easy to work with report components. Report Builder displays the right-click options that are available, and grays out those that are not.

- **Add sections**—Right-click on the name of the report in the tree. Select **Insert Simple Components**, and then select **Section**.
- Sections are simply containers for the columns in a report area. For example, if you want three tables to appear side-by-side, you create a section, add three columns, then insert the tables as described below.
- Use the up and down arrow buttons to move sections up and down in the tree to place them where you want them.
- It's a good idea to use the word Section or the letter S in the section name to help you keep track of components.
- You can add an empty buffer section between sections.
- You must have at least one column per section.
- **Add columns**—Right-click on a section, select **Insert Simple Components**, and then select **Column**.
 - Columns cause items in your report to appear side-by-side.
 - You can add one (minimum) or more columns to each section.
 - You can add an empty buffer column between columns.
 - It's a good idea to use the word Column or the letter C in the section name to help you keep track of components.
- **Add simple components**—Click **Edit** on the tool bar or right-click on the name of your report in the tree. Select **Insert Simple Components**, and then select the item you want to add.
 - In addition to sections and columns, simple components include page breaks, headers and footers, and more.
- **Add data fields, tables, and charts**—To add one of these report components to the highest level in the tree, click the name of the report in the tree (the top-level node). To add a report component to a section, click the column in that section that you want to add the component to. Then either right-click or click **Edit** on the tool bar. Select the item you want to add.

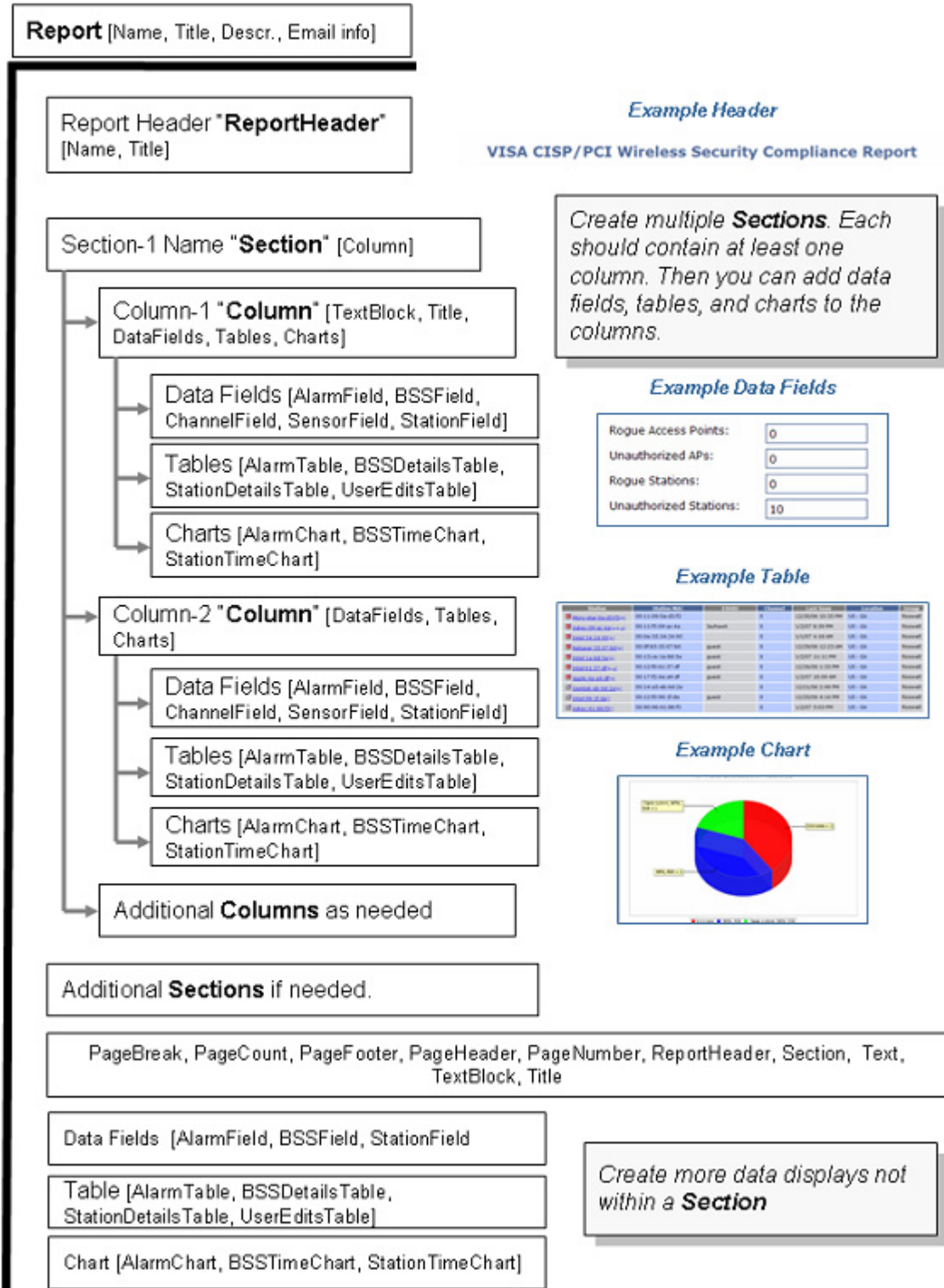


NOTE When building alarm tables with an ap_MAC column, the ap_MAC column will only show data for alarms that were triggered by a wireless client (station) associated to an AP's BSS. Other alarms will leave this field blank.

- **Use the up and down arrows** to move items within the tree.

Available Data Fields, Tables, and Charts

The following diagram shows the components, data fields, tables, and charts that are available for you to add at different points in the report tree.



Configuring Data Fields, Tables, and Charts

Every report component (data field, table, or chart) has configuration options you can use to create reports that contain the exact information you need.

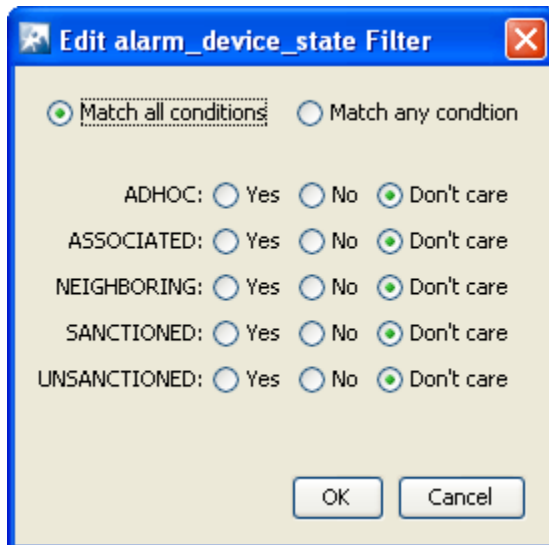
After you add a report component to your report tree, Report Builder displays the configuration options for that component. You can name the component, and then configure filters.

Hint: You may want to include the units of measure in the name you give the field. For example: Alarm (count).

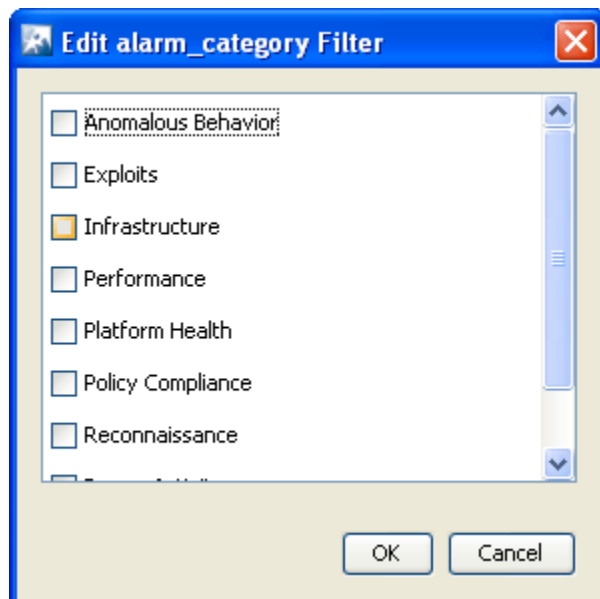
Types of Filter Windows

There are four types of filter windows. When you choose to edit a filter, Report Builder displays filter choices in the appropriate type of window:

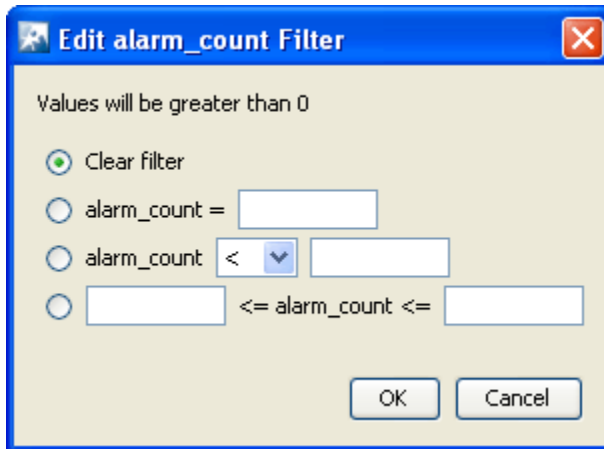
- Radio buttons (example):



- Checkboxes (example):



- Boolean (example):



Edit alarm_count Filter

Values will be greater than 0

Clear filter

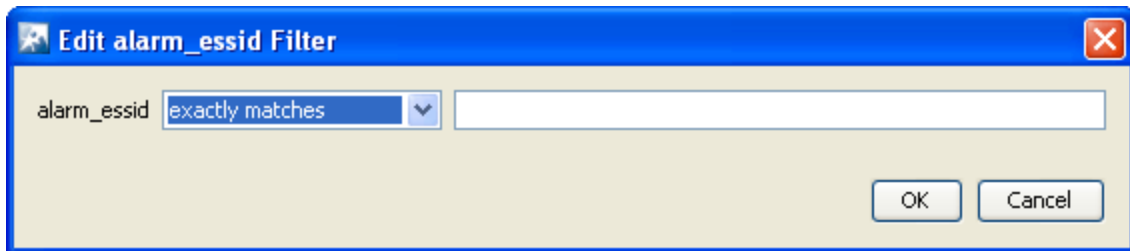
alarm_count =

alarm_count <

<= alarm_count <=

OK Cancel

- Text box (example):



Edit alarm_essid Filter

alarm_essid

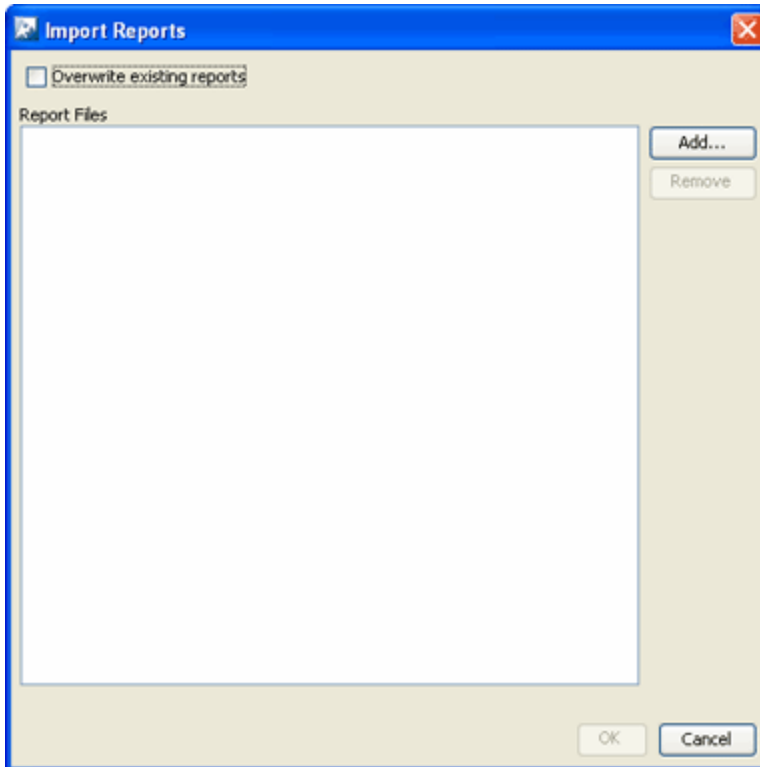
OK Cancel

Deleting a Report

1. Click **File > Delete Report** in the tool bar.
A confirmation Window appears.
2. Select (highlight) the report that you want to delete.
3. Click **Delete Report** to delete.
4. Click **Yes** to confirm.

Importing a Report

You can import a report through the **Import Reports** window.

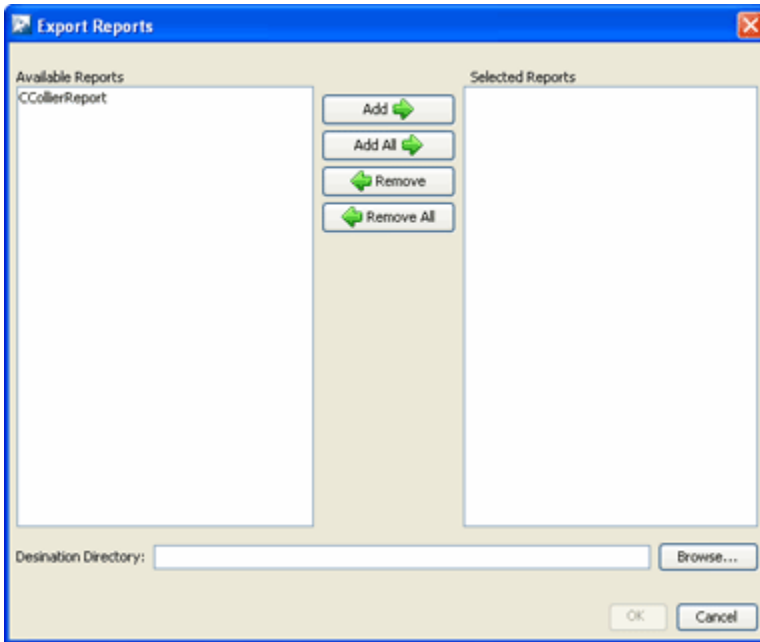


To import a report, follow these steps:

1. Select **File > Import**.
2. Click the **Add** button.
3. Navigate to the report, select (highlight) it, and click the **Open** button.
The report is added to the Report Files list. You may add as many reports as you like.
4. If a report name already exists, click the **Overwrite existing reports** checkbox.
5. Click the **OK** button.

Exporting a Report

You can export a report through the **Export Reports** window.



To export a report, follow these steps:

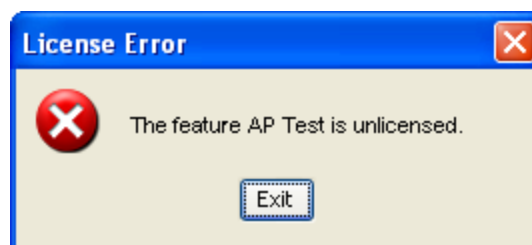
1. Click **File > Export**.
2. Select (highlight) one or more reports that you want to export.
3. Click the **Add** button to add the reports to the **Selected Reports** list.

The **Add All** button adds all of the available reports to the **Selected Reports** list. The **Remove** button removes selected (highlighted) reports from the Selected Reports list. The **Remove All** button removes all reports from the **Selected Reports** list.

4. Click the **Browse** button and navigate to the directory where you want to save the exported report(s).
5. Select the directory by clicking on it.
6. Click the **Open** button.
7. Click the **OK** button.

Scheduled AP Test

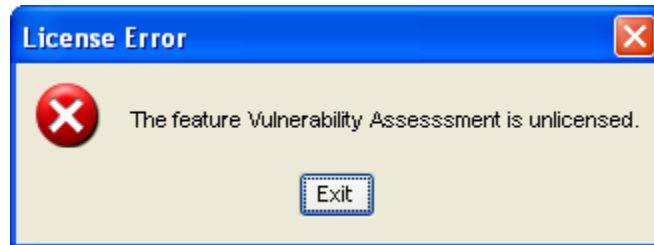
An AP Test license is required to access the Scheduled AP Test feature. AP Test is not part of the ADSP basic system. AP Test is not part of the ADSP basic system; therefore, you will receive the following error when attempting to access the Scheduled AP Test feature:



Click **Exit** to close this dialog window.

Scheduled Vulnerability Assessment

A Vulnerability Assessment license is required to access the Scheduled Vulnerability Assessment feature. Vulnerability Assessment is not part of the ADSP basic system; therefore, you will receive the following license error when attempting to access the Scheduled Vulnerability Assessment feature:



Click **Exit** to close this dialog window.

Appliance Manager

The Appliance Manager is used to configure the ADSP appliance. There are three main features associated with the Appliance Manager. They are:

- System Settings
- Backups
- Certificates.

Other features become available when they are enabled.

Navigation

[Menu](#) > [Appliance Manager](#)

System Settings

System Settings is where you configure the most basic system settings for ADSP. You can configure things such as:

- Establishing a system name and a port number to use for system access
- Enabling device termination and port suppression
- Create a login banner that displays at login time
- Create an SSH banner that displays when accessing an ADSP appliance through SSH
- Enabling and controlling auto-logout
- Setting a timeout value for a Spectrum scan
- Specifying a maximum amount of cloaking Sensors to use with the WEP Cloaking feature
- Specifying a mail relay server
- Enabling an appliance to be a FTP/SFTP relay server
- Specifying a language for your system.

You can navigate to the System Settings tab at **Menu > Appliance Manager > System**.

System Name and Port

By default, the AirDefense Services Platform appliance is named ADSP and communicates on port 8543. The appliance name appears at the top of the network tree in the UI. It also appears in Email notifications. You can change both the appliance name and port as part of your infrastructure hardening strategy.

Changing Defaults for Security Purposes

AirDefense recommends that if you want to maximize the security level of your ADSP deployment, you should change the appliance name to something that does not indicate that it is a security appliance. You should also consider changing the port to a less-well-known port.

If you keep the defaults, employees on your network or intruders can potentially identify the appliance by its name, and then attempt attacks more easily.

New Port Number

If you want to change the port number, you can choose any unused port between 1024 and 65535. AirDefense Services Platform will not let you choose a port that is already in use.

Enabling Device Termination and Port Suppression

Device termination and Port Suppression are two of the most powerful ways ADSP helps you secure your wireless network, because they let you remotely disconnect rogue devices.

Definition: Air Termination

Air termination lets you terminate the connection between your wireless LAN and any access point or station that is associated with it. If the device is an access point, AirDefense appliance de-authenticates and disassociates all wireless clients associated with the access point. If the device is a wireless client, ADSP terminates the wireless client-to-access point connection.

There are two types of device termination over the air:

- Air Termination—lets you manually disconnect a device from your network.
- Policy-Based Termination—lets you create a policy that specifies your criteria for terminating devices. AirDefense Services Platform then automatically terminates devices that do not comply with the policy.

Definition: Port Suppression

Port suppression lets you turn off the wired-side switch port that a rogue wireless device is using to communicate with your network.

Enabling These Features

Before you can *configure* these features as part of your operational configuration, you must first *enable* them as part of your basic system setup. Navigate to **Menu > Appliance Manager > System > Settings** tab and enable the features you want to use.



NOTE Policy-based termination cannot be enabled without Air Termination. Furthermore, you must have a WIPS license to fully implement any type of termination.

Enabling device termination on Sensors

In addition to enabling Device Termination on the appliance, as described in this topic, you must also enable it on the appropriate sensors. This process is described in [“Sensor Operation—used to:”](#).

Creating and Using a Login Banner

AirDefense Services Platform lets you create a custom login banner, and then enable it so that it appears whenever the ADSP GUI is launched.

Security Policy Compliance

Many organizations require a startup banner that notifies anyone logging into a system about authorizations or responsibilities regarding that system. Making it easy for you to customize a login banner is an important way that ADSP helps you enforce your security policy.

Enabling this Feature

Before you can *configure* a login banner, you must first *enable* the feature. Navigate to **Menu > Appliance Manager > System > Settings** tab and enable Login Banner.

Configuring the Login Banner

After enabling the feature, the **Banner** button appears in the Appliance Manager's button bar. Click the **Banner** button to open the Banner settings tab. AirDefense Services Platform not only lets you customize the banner text, it also lets you define the text on the **Accept/Reject** buttons. You can use html tags to format your text.

Creating and Using an SSH Banner

AirDefense Services Platform lets you add your own customized text that is displayed when accessing an ADSP appliance through SSH.

Security Policy Compliance

Many organizations require a startup banner that notifies anyone logging into a system about authorizations or responsibilities regarding that system. Making it easy for you to customize a SSH banner is an important way that ADSP helps you enforce your security policy.

Enabling this Feature

Before you can *configure* an SSH banner, you must first *enable* the feature. Navigate to **Menu > Appliance Manager > System > Settings** tab and enable SSH Banner.

Configuring the SSH Banner

After enabling the feature, the **SSH** button appears in the Appliance Manager's button bar. Click the **SSH** button to open the Banner settings tab. Enter your text exactly as you want it to appear.

Controlling Auto Logout

AirDefense Services Platform makes it easy to configure automatic log out from the GUI. Security policies and best practices sometimes call for automatically logging users out of critical systems after a specified period time. Automatic log out helps ensure that users are properly authenticated, and reduces the chance that an unauthorized person has gained physical access to an unattended computer running a critical system.

Enabling Auto Logout

Enable auto logout by navigating to **Menu > Appliance Manager > System > Settings**. Select Auto-Logout Enabled and then choose the amount of time a session can last before an automatic logout.

Setting a Timeout Value for a Spectrum Scan

AirDefense Services Platform allows you to set a timeout value for scanning during dedicated Spectrum Analysis. A dropdown menu is provided for you to select a valid value.

Specifying a Maximum Amount of Cloaking Sensors

AirDefense Services Platform has a WEP Cloaking feature that allows Sensors to be cloaked. Use this field to set the maximum amount of Sensors that can be cloaked at any one time.

Specifying a Mail Relay Server

This field defines the mail relay host. Enter an IP address or a fully-qualified host name.

Enabling Your Appliance to be a FTP/SFTP Relay Server

For special cases, you can enable your ADSP appliance to be an FTP/SFTP Relay Server.

Specifying a Language

AirDefense Services Platron allows you to select English, Chinese, Japanese, or Korean as the language to use with your appliance. A dropdown menu is provided for you to select a language.

Backups

AirDefense Services Platform lets you back up your data manually at any time, but for maximum data protection, you should also schedule backups to occur automatically on a regular basis.

AirDefense Services Platform also provides a feature that allows you to synchronize the configuration on your primary and secondary appliance. Synchronization can be done manually or automatically (scheduled).

Navigate to [Menu](#) > [Appliance Manager](#) > [Backups](#).

How Backups Work

- All backups, scheduled or on-demand, create a backup file in `/usr/local/smx/backups`.
- Backups include more than the SQL database. Many configuration files (XML files) scattered throughout ADSP are also included. These files are included in the zip archive along with the database tables.
- If an on-demand backup is done to the desktop, the system performs a regular backup to `/usr/local/smx/backups` first and then copies that file to the desktop.
- If a scheduled backup is done to a remote device via SCP or FTP, the system performs a backup to `/usr/local/smx/backups` first and then copies that file to the remote system.
- Only the most current backup is kept. Previous backups are deleted from `/usr/local/smx/backups`.
- The `/usr/local/smx/backups` directory is root protected. Users cannot delete the backup file. However, they can copy it to another location.
- The format of a backup file is: `Backup_9.0.0-23_ECRT236.am.mot.com_20120216000011.zip.enc`. The name always includes the release, the appliance name, and the year-month-day-hour-minute-second. The `enc` at the end of the name indicates that the file is encrypted. Encrypted files can be emailed securely.

Manual Backup

You should perform a manual backup whenever you plan to update your appliance, such as before you apply a Service Module or before you upgrade to a new version.

Executing a manual backup will back up all of your system configuration files.

Scheduled Backup

You should create a backup schedule that complies with either your IT backup policy or security policy, whichever is more strict.

Scheduled backups are backed up on your ADSP appliance. You may optionally back up to another ADSP appliance using SCP or FTP.

Scheduled backups are executed once, on an intra-daily basis, on a daily basis, weekly basis or monthly basis.

Manual Synchronization

You should perform a manual synchronization whenever you make a major configuration change/update and you want to copy it immediately to another appliance.

Automatic Synchronization

You should schedule appliance synchronization on a regular basis. Any every day or minor configuration changes/updates are automatically copied to the appropriate appliance(s).

You should set up automated synchronization to backup your primary appliance on a secondary appliance.



NOTE Synchronization should only be done on a primary and backup of the same build version. The database files are not compatible on different AirDefense Services Platform/Enterprise versions.

Synchronizing Primary and Secondary Appliances

This section contains the automated synchronization procedure for backup of the primary appliance to a secondary appliance.

How Synchronization Works

- Synchronization will not work if there is no backup file or if there is a backup in progress.
- On the standby appliance, during either scheduled or on-demand synchronization, the standby appliance pulls the current backup from `/usr/local/smx/backups` on the primary appliance.
- **NEVER** schedule a synchronization or perform an on-demand synchronization at the same time a backup is occurring on the primary appliance.
- **NEVER** start an on-demand backup while synchronizing appliances.
- The backup file is copied to `/usr/local/smx/backups` on the standby machine which brings up two important points:
 - **NEVER** schedule a local, remote or on-demand backup on the standby machine. If you do, it will overwrite the file transferred over from the primary appliance.
 - **NEVER** direct a backup from the primary appliance to `/usr/local/smx/backups` on a standby appliance. This will prevent synchronization from working properly.
- **NEVER** back up to the desktop from the standby appliance, because that process overwrites the existing file in `/usr/local/smx/backups`. See [How Backups Work](#).
- As the second part of synchronization, the standby appliance runs a restore to itself using the file found in its own `/usr/local/smx/backups` directory. This should be the only file ever copied over from the primary appliance.

Synchronization Rules

- You should only back up the primary appliance. **NEVER** schedule or perform a backup on the standby appliance.
- Synchronization should only be done from the standby appliance. **NEVER** schedule or perform a synchronization on the primary appliance.
- Always schedule or perform a backup on the primary appliance **one hour** before scheduling a synchronization or performing an on-demand synchronization on the standby appliance. Backups require more time as the primary appliance continues collecting configuration data.
- **NEVER** schedule backups at the same time as a synchronization. This will **NEVER** work.
- Scheduled jobs should be included when backing up an appliance before synchronization. This will save you valuable time when restoring the backup on a new appliance. Unless you have backed up your scheduled jobs, you will have to recreate them on the new appliance.

Set Up Scheduled Database Backups on the Primary Appliance

1. Log into the primary appliance's GUI.
2. Navigate to **Menu > Appliance Manager > Backups**.
3. Click on the **Configuration Backup** button.
4. Enable automatic backups by clicking the **Enable Automatic Configuration Backup** checkbox to place a checkmark in the box.
5. Click the **Add** button and type in a name for the backup (**Name** field) or select a name from the dropdown menu.



NOTE No names will display in the dropdown menu until after you have scheduled at least one other backup.

6. Decide how often you want to run the backup by selecting **One Time Schedule**, **Intra-Day Schedule**, **Daily Schedule**, **Weekly Schedule**, or **Monthly Schedule** from the dropdown menu.
7. Depending on the interval you selected in the previous step, fill in the related fields using the following table:

Interval	Action
One Time Schedule	Choose a time for the backup by selecting a time from the Time dropdown menu. Then, select a day for the backup by clicking the Calendar button in the Date field and selecting a date.
Intra-Day Schedule	Select a time to begin the backup. Then, select a frequency in hours.
Daily Schedule	Select a frequency in day, weekdays only, or weekends only. Then, select a time of day.
Weekly Schedule	Choose a frequency in days. Then, select a day or multiple days to conduct the backup by clicking the checkbox next to the day to place a checkmark in the box.
Monthly Schedule	Choose the months that you want to run a backup by clicking the checkbox next to the month(s) to place a checkmark in the box(es). Then, select a day of the month to conduct the backup. Last, specify a time of day.

8. Click **Apply** button to set the automatic backup schedule.

Set Up Automatic Synchronization



NOTE Automatic synchronization is a “pull” setup, where the backup appliance pulls the configuration from the Primary appliance. Therefore, you only need to set up automatic synchronization on the backup system (Secondary appliance) to ensure the same configuration on a Primary and Secondary appliance. No settings on the Primary appliance are required.

1. Log into the secondary appliance's GUI.
2. Navigate to **Menu > Appliance Manager > Backups**.
3. Click on the **Configuration Sync** button.
4. Enable automatic synchronization by clicking the **Enable Automatic Configuration Sync** checkbox to place a checkmark in the box.
5. Click the **Add** button and type in a name for the synchronization (**Name** field) or select a name from the dropdown menu.



NOTE No names will display in the dropdown menu until after you have scheduled at least one other synchronization.

6. In the **Address** field, type in the primary appliances's IP address.
7. In the **Port Number** field, type in the port number of the primary appliance's IP address.
8. In the **Username** field, type in an administrator's username on the primary appliance.



NOTE It is a good practice to setup an admin account (using the same username and password) on both the primary and secondary appliance.

9. In the **Password** field, type in the password of the administrator on the primary appliance.
10. Decide how often you want to run the synchronization by selecting **One Time Schedule**, **Intra-Day Schedule**, **Daily Schedule**, **Weekly Schedule**, or **Monthly Schedule** from the dropdown menu.
11. Depending on the interval you selected in the previous step, fill in the related fields using the following table:

Interval	Action
One Time Schedule	Choose a time for the synchronization by selecting a time from the Time dropdown menu. Then, select a day for the synchronization by clicking the Calendar button in the Date field and selecting a date.
Intra-Day Schedule	Select a time to begin the synchronization. Then, select a frequency in hours.
Daily Schedule	Select a frequency in day, weekdays only, or weekends only. Then, select a time of day.
Weekly Schedule	Choose a frequency in days. Then, select a day or multiple days to conduct the synchronization by clicking the checkbox next to the day to place a checkmark in the box.
Monthly Schedule	Choose the months that you want to run a synchronization by clicking the checkbox next to the month(s) to place a checkmark in the box(es). Then, select a day of the month to conduct the backup. Last, specify a time of day.

12. Click **Apply** button to set the automatic synchronization schedule.

Set Up Automatic Forensics Backup

NOTE When you first turn on automatic Forensics backup, only new forensic files are backed up. Existing forensic files will not be backed up. You will have to save old files if you want to copy them to another appliance.

1. Log into the secondary appliance's GUI.
2. Navigate to **Menu > Appliance Manager > Backups**.
3. Click on the **Forensics Backup** button.
4. Enable automatic forensics backup by clicking the **Enable AutomaticForensics Backup** checkbox to place a checkmark in the box.
5. Fill in the fields described in the following table:

Field	Description
Protocol	The file transfer protocol to use for backing up forensics.
Host Name	The name of the appliance where you want to back up forensics. This can be an IP address or a DNS name defined by your DNS server.
Port Number	The port number to use during the backup.
Username	The username used to log in on the destination appliance.
Password	The password used to log in on the destination appliance.

6. Click **Apply** button to enable automatic forensics backup.

Now, whenever a forensics file is created, it is automatically backed up on the host specified in the **Host Name** field.

Banner

The Banner function is provided for ADSP users who wish to add their own customized agreement banner which will be shown each time users log into the system.



NOTE In order for this agreement to appear, you must go to the System Settings window, and enable the Login Banner. The **Banner** button then appears on the Appliance Manager row of buttons.

The following fields are available to create a banner:

Field	Description
Approve button text	Enter the actual text that will appear for the approve button on the Startup Agreement. Default = I Agree

Field	Description
Cancel button text	Enter the actual text that will appear for the cancel button on the Startup Agreement. Default = I Disagree
Application exit message (text or HTML)	Enter the actual text that will appear as a message dialog window when you choose to cancel the Startup Agreement. Content can be text or in HTML format.
Content (text or HTML)	Enter the actual startup agreement text in this area; this text is what will appear when the ADSP application is first opened. Note: Content can be text or in HTML format.

Certificates

Certificates can prevent hijacking of sessions between your browser and the ADSP appliance, and can even alert you to physical replacement of the ADSP appliance.

Certificates install into the ADSP appliance and are sent by the appliance directly to your Windows session, enabling you to use ADSP over a secure, TLS-encrypted https web session.

You can choose from four appliance certificate options:

- AirDefense default certificate
- Tomcat (self-signed) certificates
- Root-signed (CA) certificates
- SSL certificate.



CAUTION Motorola AirDefense recommends that you replace the pre-installed security certificate with at least a self-signed certificate for every ADSP appliance in your network.

AirDefense Default Certificate

Motorola AirDefense ships the ADSP appliance with a pre-installed security certificate. The AirDefense certificate represents a **minimal level** of security. It is a working certificate that provides TLS encryption, but has not been verified and digitally signed by a root Certificate Authority (CA). The host name identified in the certificate will not match the actual host name of your ADSP appliance.

Tomcat certificates

The ADSP appliance has a default certificate pre-installed, but it can also issue and use self-signed Tomcat Certificates. A self-signed certificate represents an **intermediate level** of security. When you generate a Tomcat certificate, you specify the host name of the ADSP appliance in the certificate, but do not have the certificate verified and digitally signed by a root Certificate Authority.

Client stations attempting to access the appliance may not recognize these certificates. If that happens, you will be prompted to accept the connection on a temporary or permanent basis.

Root-signed certificates

AirDefense Services Platform also supports external root-signed certificates. A root-signed certificate represents a **high level** of security. A root-signed certificate is a public certificate verified by a root Certificate Authority (CA). This is a digitally signed certificate that ensures the authenticity of the ADSP appliance.

These may be generated by your organization using your own certificate authority (CA) or may come from a third party CA.

Your organization's own CA

- Using your own CA lets you create and manage certificates internally to comply with your organization's security policy.
- Certificates from your own CA do not have the additional expense of a third-party CA.
- Certificates from your own CA require more work than using the built-in Tomcat certificates.

A third-party CA

- Useful when two or more organizations are working together and require highly secure communications and external validation of clients.
- Adds significant cost in deployment due to the introduction of third party services and related overhead and expense.

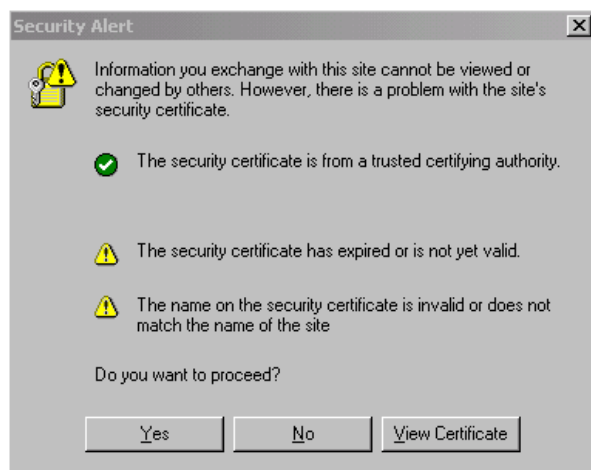
SSL Certificate

A SSL certificate represents the **highest level** of security. SSL certificates create a secure connection between a client and an appliance. The client is usually a web browser transmitting private information over the internet. The URL for SSL connections start with **https://** instead of **http://**.

Security Alerts

You may receive self-descriptive alert screens if certain certificate criteria are not met when you open a session with ADSP appliance, regardless of what type certificate you are using.

Security Alert Window.



The Security Alert window appears if the certificate does not meet all of the following criteria:

- The ADSP appliance must have a certificate signed by a trusted Certificate Authority installed, and the certificate must be applied to the ADSP GUI.



NOTE After you install a certificate, you must use **ADSPadmin** to restart the ADSP processes.

- Your workstation's current date range must be within the range of valid dates generated for the certificate.

- The host name generated for the certificate must match the name of the ADSP appliance.

Java Security Warning—host name mismatch

The Java Security Warning window for host name mismatch appears during initial login if your certificate host name does not match the host name of the security certificate.

SSH

The SSH function is provided for ADSP users who wish to add their own customized text for users accessing the ADSP appliance through SSH.

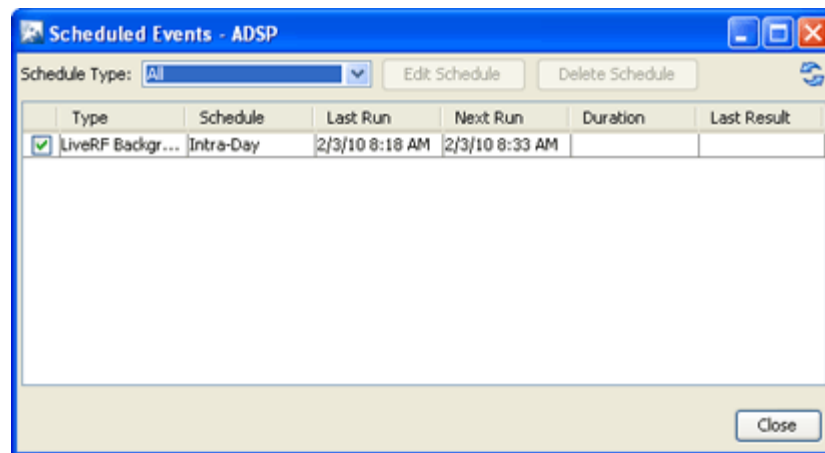
- ✓ **NOTE** In order for this agreement to appear, you must go to the System Settings window, and enable the SSH Banner. The **SSH** button then appears on the Appliance Manager row of buttons.

There is only one field available to create an SSH banner: **Content (text)**. Use it to enter text that users will see when accessing an ADSP appliance through SSH.

Scheduled Events

Monitoring Schedule Events

AirDefense Services Platform allows you to schedule events throughout the application. The Scheduled Events feature allows you to monitor all scheduled events from one source. You can access Scheduled Events by selecting **Menu > Scheduled Events**.



You can elect to view all the scheduled events (default) or you can narrow the events to one of the following types:

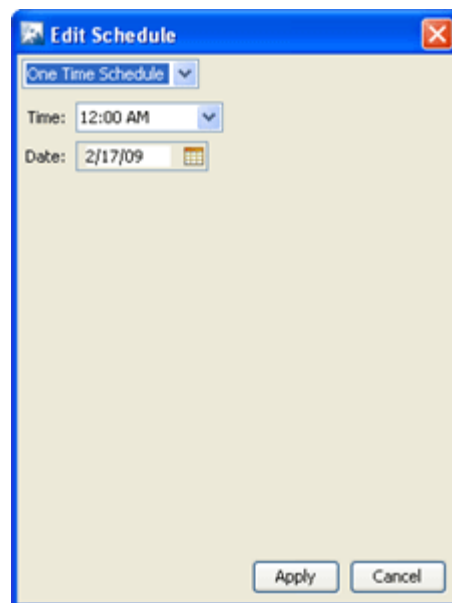
- AP Test
- Auto Classification
- Backups
- Firmware Upgrade
- Frame Capture
- Appliance Synchronization
- Forensic Backup
- Device Import
- Vulnerability Assessment
- Device Management Poll
- Device Configuration
- LiveRF Background Analysis.

You cannot schedule new events using the Scheduled Events feature. You can only view, edit, or delete Scheduled Events. The following information is displayed for each event:

Column	Description
Type	Type of event that is scheduled.
Schedule	How often the scheduled event will be conducted.
Last Run	Last time the scheduled event was conducted.
Next Run	Next time the scheduled event will be conducted.
Duration	Amount of time the scheduled event lasted.
Last Result	Result of the last scheduled event.

Altering Event Schedules

You can alter an event schedule by highlighting the scheduled event and clicking the **Edit Schedule** button.



You can change how often the event is conducted by selecting **One Time Schedule**, **Intra-Day Schedule**, **Daily Schedule**, **Weekly Schedule**, or **Monthly Schedule** from the dropdown menu. Depending on the interval you select, fill in the related fields using the following table:

Interval	Action
One Time Schedule	Choose a time for the backup by selecting a time from the Time dropdown menu. Then, select a day for the backup by clicking the Calendar button in the Date field and selecting a date.
Intra-Day Schedule	Select a time to begin the backup. Then, select a frequency in hours.

Interval	Action
Daily Schedule	Select a frequency in day, weekdays only, or weekends only. Then, select a time of day.
Weekly Schedule	Choose a frequency in days. Then, select a day or multiple days to conduct the backup by clicking the checkbox next to the day to place a checkmark in the box.
Monthly Schedule	Choose the months that you want to run a backup by clicking the checkbox next to the month(s) to place a checkmark in the box(es). Then, select a day of the month to conduct the backup. Last, specify a time of day.

Auto Classification

ADSP's auto-classification feature makes it easy to classify large numbers of devices automatically. Two of the main advantages of auto-classification are:

- You can **automatically** classify whole groups of devices that don't interest you by classifying them as neighboring, to limit the alarm count caused by unsanctioned devices.

Example: In an environment with many transient or neighboring devices, you can schedule ADSP to periodically classify all devices below a specified signal strength as neighboring.

- You can **automatically sanction** whole groups of devices that you need to rapidly add to ADSP.

Example: If your company deploys a large number of new wireless devices, you can specify criteria they need to meet (configuration, vendor, etc.), and then ADSP will automatically sanction all that meet your criteria.

You can also **unsanction** and **delete** devices automatically.

Navigation

[Menu](#) > [Auto Classification](#)

On-Demand vs Scheduled Classification

You can auto-classify devices on demand or you can schedule auto-classification to occur periodically.

Manual/On-Demand

The **on-demand** option lets you classify all devices in the system at any time. You should consider this option for initial system setup, but it is also useful whenever new, unsanctioned devices are discovered by ADSP sensors.

After you start an on-demand classification, ADSP displays a list of discovered devices, along with data about how they compare to your auto-classification criteria. You can edit the list, manually overriding the auto-classification for single or multiple devices. The devices are actually assigned the new classification only after you confirm that you want to apply the results.

Scheduled

Scheduled auto-classification is very helpful when you want to *classify* groups of devices with certain attributes as neighboring, such as low signal strength or those from unapproved vendors.

*Important! You should schedule auto-classification to **sanction** devices with caution, considering the rules that control which devices are sanctioned (below) carefully, to avoid accidentally sanctioning a device in error.*

Because auto-classification places a minor burden on the system, Motorola AirDefense recommends that you schedule auto-classification to occur only once or twice a day.

Action Rules and Rule Sets

AirDefense Services Platform uses a combination of Action Rules and Rule Sets to let you specify exactly which devices to sanction, unsanction, classify as neighboring, or even delete. First, you create Action Rules, and then you create Rule Sets, which are combinations of Action Rules.

Action Rules

The Action Rules tab of the Auto Classification page lets you create a very specific set of rules for classifying devices. **The more criteria you include, the more accurate the resultant classification will be, and the less likely it is that a device will be mis-classified.**

After you add or select a rule, you specify the type of device the rule classifies, whether the rule is intended to sanction, unsanction, classify as neighboring, or delete devices, and whether you want the classification to occur if the devices match the criteria or do not match the criteria.

You then specify the criteria that control whether each device is classified according to the rule. You can use any or all of the following fields to include or exclude devices that do not meet your criteria:

- MAC
- IP Address
- Vendor
- Channel
- SSID
- Signal Strength
- Protocol
- Classification
- 802.x Username
- Last Seen
- Connectivity
- Association
- Extended Authentication
- Key Generation
- Specific EAP Type
- Encryption



NOTE Each field you add to the filter changes to bold onscreen, to help you track your actions.

Rule Sets

After you create Action Rules specifying exactly what criteria you want to use to auto-classify devices, you combine the Action Rules into Rule Sets to simplify auto-classification, and to let you schedule multiple auto-classification actions in a single Rule Set.

Example: You can create a rule to classify all BSSs with a very low signal strength as neighboring and a rule to sanction all BSSs that meet your standard vendor and configuration criteria. You then combine those rules in a single Rule Set that you schedule to run every morning at 3 am.

Sequence of Rules in Rule Sets

After you add Action Rules to a Rule Set, you should consider the order in which they appear in the list. As ADSP examines devices during auto-classification, it looks for the first match between a device and an Action Rule in the Rule Set. You should place the least restrictive Action Rule at the top of the list, and the most restrictive at the bottom of the list.

Add Devices

The **Add Devices** action is used to add devices to your network.

The screenshot shows the 'Add Devices' dialog box. The 'Device Type' is set to 'BSS'. The 'MAC Address' field is empty, and a red error message 'Invalid MAC Address' is displayed at the bottom left. The 'Name' and 'Description' fields are also empty. The 'Add to appliance' section has 'All appliances' selected. The 'Annotations' section has 'Flagged' and 'Bridge' unchecked. The 'Classification' section has 'Sanctioned (inherit)' selected. A scrollable list below shows 'AD_raTenator_Security_Profil' with a checkbox.

You can add any of the following devices by selecting the device from the **Device Type** menu:

- BSS
- Wireless Client
- Access Point
- Wired Switch
- Wireless Switch
- WLSE
- AirWave
- MSP.

The fields change according to the selected device.

BSS and Wireless Clients Fields

The following fields are available when adding BSSs and Wireless Clients:

Field	Description
MAC Address	The MAC address of the device
Name	The name you want your device to display in your network
Description	A description of the device
Add to appliance	You may add the device to your primary appliance or all appliances that AirDefense Services Platform is monitoring. Select the appropriate radio button.
Annotations	Specify if the device should be flagged or if it will be bridged. Select the appropriate checkbox.
Classification	Specify if the device should be classified as: <ul style="list-style-type: none"> • Neighboring • Unsanctioned • Sanctioned (inherit) • Sanctioned (override)—a list of available profiles is displayed to use as the override profile(s). You may select one or more profiles.

All Other Devices Fields

The following fields are available when adding devices other than BSSs and Wireless Clients:

Field	Description
MAC Address	The MAC address of the device
Name	The name you want your device to display in your network
Scope	Select a scope (usually a floor network level) from the dropdown menu
Host	The host name of the device
Description	A description of the device

When adding devices, you can only add one devices at a time.

Import and Discovery

Import and Discovery is used to import or discover devices from one of the following sources:

- Local file
- Remote file
- SNMP discovery using a list of networks to scan
- Wireless Manager/Switch.

All imported devices will be configured and classified according to the Device Import Rules. You may also use Auto-Placement Rules to place the device in your network, or you may place the device yourself.

You can also import Connectivity profiles for AP Test and Vulnerability Assessment using Import and Discovery. The import file is used to populate the fields in the three tabs in the AP Test and Vulnerability Assessment profiles.

Importing profile settings require a separate import file. You should not combine importing profiles with importing devices.

Once a profile has been created (by importing or through the GUI), you can schedule an AP Test or a Vulnerability Assessment to run using Import and Discovery.

Local File Fields

Job Type:

Descriptions:

Path:

? Not sure how to format a file for import?

1. Open a preformatted sample file.
2. Enter the appropriate information.
3. Save to a local drive.
4. return to this screen, and import to ADSP.

Add to appliance:

Use auto-placement rules
 Place devices in a single folder

The following fields are available when importing local files:

Field	Description
Job Type	Import Local File
Descriptions	System generated description. You may change if you want to.
Path	Browse to specify a path on your local workstation including the import filename (e.g., <i>c:\temp\filename</i>)
Select a sample CSV file	Selects a sample CSV file from the dropdown list. Once a file is selected, click the Open in New Window button. A new window is opened containing the selected file. You can copy this file and use it to create an import file.
Add to appliance	Appliance where you want to import device (will only list your appliance unless you have a Central Management license)
Device placement	You have the option of using the auto-placement rules or selecting a folder from your network tree.

Remote File Fields

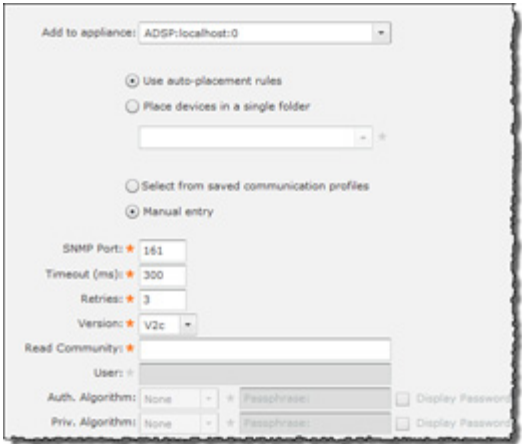
The following fields are available when importing remote files:

Field	Description
Job Type	Import Remote File
Descriptions	System generated description. You may change if you want to.
Host	Host name or IP address
Protocol	Protocol used for communications
Path	Path name on the remote host including the import filename (e.g., <i>/usr/local/tmp/filename</i>)
User	User name needed to log in
Password	Password needed to log in
Add to appliance	Appliance where you want to import device (will only list your appliance unless you have a Central Management license)

SNMP Discovery Fields

The following fields are available during SNMP discovery:

Field	Description
Job Type	SNMP Discovery
Descriptions	System generated description. You may change if you want to.
Networks	List of networks to scan separated by commas. You may enter a single IP address, a range of IP addresses, a subnet mask, or an IP address that includes a wild card such as asterisk (*).

Field	Description
Add to appliance	Appliance where you want to import device (will only list your appliance unless you have a Central Management license).
Device placement	You have the option of using the auto-placement rules or selecting a folder from your network tree.
Execution Method	<p>You have the option of selecting an existing profile or entering the import information manually. If you elect to enter the information manually, additional options are displayed.</p>  <p>The additional options for manual entry are:</p> <ul style="list-style-type: none"> • SNMP Port—Device SNMP port number; normally set to 161 but can be different • Timeout (ms)—Timeout in milliseconds to attempt import • Retries—Number of retries to attempt import • Version—SNMP version used: V1, V2c or V3 • Read Community—Read Community string used for the SNMP authentication • User—Name of the V3 user, which is configured on a switch for SNMP V3 access. This option is inactive until V3 is selected as the version. • Authentication/Privacy Algorithm—You may optionally supply an authentication and privacy algorithm along with a passphrase for each. These parameters must match settings on the switch exactly. These options are inactive until V3 is selected as the version. Selecting the Display Password checkbox displays the passphrase as text.

Wireless Manager/Switch Fields

The following fields are available when importing wireless managers or switches:

Field	Description
Job Type	Import from Wireless Manager/Switch
Descriptions	System generated description. You may change if you want to.
Basic Search	Specify a partial or full MAC address of a Switch or enter the name; then, click Search. The search results are listed in the Select from search results box. Select a device from the list and then click one of the Start Import buttons. Devices associated with the Wireless Manager/Switch are imported into ADSP.
Advanced Search	Enter search criteria in one or more fields, then click Search . The search results are listed in the Select from search results box. Select a device from the list and then click one of the Start Import buttons. Devices associated with the Wireless Manager/Switch are imported into ADSP. The following search criteria are available: <ul style="list-style-type: none"> • MAC address • Name • DNS name • Vendor name.
Add to appliance	Appliance where you want to import device (will only list your appliance unless you have a Central Management license).
Device placement	You have the option of using the auto-placement rules or selecting a folder from your network tree.

Import File Formats

Comma delimited files are used to import devices and profiles. There are different ways to create a comma delimited file but the most trouble-free way is to use a text editor, such as Notepad.



NOTE CSV files can be used instead of comma delimited files.

There are different file formats for Devices and Profiles.

Devices

Import Device File Format

BSS

Format

bss | name | description | mac | isBridge | sanctioned/unsanctioned/ignored | performance policy | list of sec policies

Example

```
bss,name,desc,00:01:01:01:01:01,true,sanctioned,perfpolicy,secpol1;secpol2
```



NOTE **bss** must always be the first field.

Wireless Client

Format

station | name | description | mac | isWired | sanctioned/unsanctioned/ignored | performance policy | list of sec policies

Example

```
station,name,desc,02:02:02:02:02:02,true,sanctioned,perfpolicy,secpol1;secpol2
```



NOTE **station** must always be the first field.

Access Point

Format

ap | name | description | mac | ip | dnsName | model



NOTE *model* is optional and can be left blank.

Example

```
ap,apname,apdesc,03:03:03:03:03:03,10.10.10.10,ap.dns.name,AP650
```



NOTE **ap** must always be the first field.

Switch

Format

switch | name | description | mac | ip | switchType | dnsName | model



NOTE *model* is optional and can be left blank. Also, if switch is a wired switch, model must be left blank.

Example

```
switch, switchname, switchdesc, 04:04:04:04:04:04, 11.11.11.11, wireless, switch.dns.name, RFS4000
switch, switchname, switchdesc, 05:05:05:05:05:05, 11.11.11.11, wired, switch.dns.name,
```



NOTE **switch** must always be the first field.

Device on Wire

Format

dev_on_wire | device_MAC | device_IP | sanctioned/unsanctioned | switch_MAC | switch_IP | ifIndex | ifName | ifDescr | vlanID

Example

```
dev_on_wire, 00:06:06:06:06:06, 4.3.2.1, sanctioned, 00:0d:bc:78:94:81, 10.59.39.110, 0,
interface name, interface description, 0
```



NOTE **dev_on_wire** must always be the first field.

Profiles

AP Test

There are two records associated with importing AP Test profiles:

- apt_profile
- apt_profile_info

When creating the profiles, always enter the apt_profile records first and then any apt_profile_info records should follow. The fields for an apt_profile record are:



NOTE All fields have an equivalent field in the GUI.

- Profile name
- SSID
- Authentication (**Open**, **SharedKey**, or **NetworkEAP**)
- Key generation (**None**, **PSK**, **EAP**, **Dynamic WEP**, or **802.1x**)
- Unicast encryption (**None**, **WEP**, **TKIP**, or **AES/CCMP**)



NOTE **AES/CCMP** can also be set up from **AES** or **CCMP**.

- Multicast encryption (**None**, **WEP**, **TKIP**, **AES/CCMP**)



NOTE **AES/CCMP** can also be set up from **AES** or **CCMP**.

- EAP method (**None**, **LEAP**, **EAP Fast Auto**, **EAP Fast Manual**, **EAP TLS**, **PEAP MSCHAPv2**, **PEAP GTC**, or **PEAP TLS**)
- WPA protocol (**None**, **WPA**, or **WPA2**)
 - ✓ **NOTE** The next two fields key1 and key2 change based on previous information. For EAP with a username and password, key1 is the username and key2 is the password. For WEP, key1 is the key index and key2 is the WEP key. For PSK, key2 is the pre shared key.
- key1
- key2
- WEP key size (**WEP64** or **WEP128**)
- ASCII WEP (**true** or **false**)
- Verify appliance certificates (**true** or **false**)
- Station MAC address
- DHCP enabled
- IP address
- Subnet mask
- Default gateway
- Auto DNS
- Primary DNS
- Secondary DNS
- Domain name

Examples:

```
apt_profile,ProfileName1,SSID,Open,802.1x,WEP,WEP,LEAP,,username,password,
WEP128,,,00:11:22:33:44:55,FALSE,192.168.1.100,255.255.255.0,192.168.1.1,
FALSE,192.168.1.200,192.168.1.201,test.com
apt_profile,ProfileName2,SSID,Open,PSK,AES/CCMP,TKIP,,WPA,,psk key,,,,
00:11:22:33:44:55,TRUE,,,,TRUE,,,
```

✓ **NOTE** Although the records in the above examples are shown on multiple lines, all entries must be on a single line with no line breaks or carriage returns.

Possible additional entries for apt_profile_info are:

- certificate
 - certificate name
 - certificate type (**user**, **inner**, **outer**, or **server**)
- traceroute (field is host domain name or IP address)
 - host to traceroute to
- dns
 - host to perform lookup on
 - optional resolve to ip address test

- ping
 - whether to ping default gateway or not (**ping** or **ignore**)
 - 0 or more additional addresses to ping
- port
 - 1 or more host:port pairs to scan

Examples:

```
apt_profile_info,ProfileName1,certificate,usercertificate,user
apt_profile_info,ProfileName1,traceroute,192.168.2.200
apt_profile_info,ProfileName1,dns,test.domain.com
apt_profile_info,ProfileName1,ping,ping
apt_profile_info,ProfileName2,ping,ping
apt_profile_info,ProfileName2,port,192.168.1.2:80,192.168.1.3:80,192.168.2.1:443
```

Vulnerability Assessment

There are two records associated with importing Vulnerability Assessment profiles:

- wva_profile
- wva_profile_info

When creating the profiles, always enter the wva_profile records first and then any wva_profile_info records should follow. The fields for a wva_profile record are:



NOTE All fields have an equivalent field in the GUI.

- Profile name
- SSID
- Authentication (**Open**, **SharedKey**, or **NetworkEAP**)
- Key generation (**None**, **PSK**, **EAP**, **Dynamic WEP**, or **802.1x**)
- Unicast encryption (**None**, **WEP**, **TKIP**, **AES/CCMP**)



NOTE AES/CCMP can also be set up from **AES** or **CCMP**.

- Multicast encryption (**None**, **WEP**, **TKIP**, or **AES/CCMP**)



NOTE AES/CCMP can also be set up from **AES** or **CCMP**.

- EAP method (**None**, **LEAP**, **EAP Fast Auto**, **EAP Fast Manual**, **EAP TLS**, **PEAP MSCHAPv2**, **PEAP GTC**, or **PEAP TLS**)
- WPA protocol (**None**, **WPA**, **WPA2**)



NOTE The next two fields key1 and key2 change based on previous information. For EAP with a username and password, key1 is the username and key2 is the password. For WEP, key1 is the key index and key2 is the WEP key. For PSK, key2 is the pre shared key.

- key1
- key2
- WEP key size (**WEP64** or **WEP128**)

- ASCII WEP (**true** or **false**)
- Verify server certificates (**true** or **false**)
- Station MAC address
- DHCP enabled
- IP address
- Subnet mask
- Default gateway
- Auto DNS
- Primary DNS
- Secondary DNS
- Domain name
- Scan type (**whitelist** or **blacklist**)
- Scan timeout (integer value; defaults to 30)
- Scan speed (integer value between 0 and 255)
- Check internet (**true** or **false**)
- Check internet host
- Check internet port
- Perform reverse lookups (**true** or **false**)
- Traceroute DNS (**true** or **false**)
- Additional ports (colon delimited list of ports)
- Scan unpingable (**true** or **false**)
- Traceroute host

Examples:

```
wva_profile,ProfileName1,SSID,Open,EAP,TKIP,WEP,EAP TLS,WPA2,username,
password,,,TRUE,,,,TRUE,,,,whitelist,30,0,TRUE,www.google.com,80,TRUE
wva_profile,ProfileName2,SSID,NetworkEAP,PSK,TKIP,TKIP,,,,psk key,,,,
00:11:22:33:44:55,TRUE,,,,TRUE,,,,blacklist,60,255,FALSE,,,FALSE
```



NOTE Although the records in the above examples are shown on multiple lines, all entries must be on a single line with no line breaks or carriage returns.

Possible additional entries for apt_profile_info are:

- certificate
 - certificate name
 - certificate type (user, inner, outer, or server)
- entry—0 or more records of the following type:
 - host network
 - color(:) delimited ports
 - source
 - ping status (Allowed or Not Allowed)

Examples:

```
wva_profile_info,ProfileName1,certificate,usercertificate,user
wva_profile_info,ProfileName2,entry,192.168.10.0/24,80:443,,Allowed
```

Scheduling AP Test or Vulnerability Assessment

Once you have created a profile (by importing or through the GUI), you can schedule an AP Test or a Vulnerability Assessment to run. This is done with a record named `scheduled_test`.

The `scheduled_test` record can part of an import file that creates a profile or it can be its own separated import file. If it is part of an import file that creates a profile, all `scheduled_test` records must be entered at the end of the file.

The fields for a `scheduled_test` record are:



NOTE All fields have an equivalent field in the GUI.

- Is this a scheduled AP Test (versus Vulnerability Assessment)—**true** if it's an AP Test; **false** if it's a Vulnerability Assessment
- Profile name
- Scope [BSS MAC address or path to folder separated by a slash (/)]
- Number of retries
- Switch Sensors on retry (**true** or **false**)
- Signal threshold
- Last seen time in minutes
- Skip test on sensor busy (**true** or **false**)
- Filter on SSID (**true** or **false**)
- Time to wait for Sensor in minutes
- Number of tests (assessments) to run in parallel
- Prefer OTA tests (true or false)
- Schedule name

- Schedule type (**daily**, **intraday**, **monthly**, **weekly**, or **onetime**)

daily has the following sub-fields:

- hours (the hour of the day)
- minutes (the minute of the hour)
- type (**interval**, **weekdays**, or **weekends**)—**interval** means run in every x days. **weekdays** means run on weekdays. **weekends** means run on weekends.
- interval (in days)—an interval of 1 means every day; an interval of 4 means every four days (this sub-field is only used if type is **interval**)

intraday has the following sub-fields:

- hours (the hour of the day)
- minutes (the minute of the hour)
- number of hours between runs (must be > 1)

monthly has the following sub-fields:

- hours (the hour of the day)
- minutes (the minute of the hour)
- months to run [colon(:) delimited]; i.e., **January:February**:etc
- type (**day**, **last**, or **specific**)—**day** means run on the nth day of the month. **last** means run on last day of the month. **specific** means run on the **last**, **first**, **second**, **third**, **fourth**, or **fifth** occurrence on the specified day of the week (**Monday**, **Tuesday**, **Wednesday**, etc).

weekly has the following sub-fields:

- hours (the hour of the day)
- minutes (the minute of the hour)
- days to run [colon(:) delimited]; i.e., **Sunday:Wednesday**
- interval (weeks between runs)

onetime has the following sub-fields:

- hours (the hour of the day)
- minutes (the minute of the hour)
- month (1 - 12 with 1 being January and 12 being December)
- day of the month (1 - 31)
- year (i.e., 2012)

Examples:

```
scheduled_test,TRUE,APT_ProfileName1,00:11:22:33:44:55,2,TRUE,-70,10,
TRUE,TRUE,10,20,Schedule1,onetime,6,30,5,5,2012
scheduled_test,FALSE,WVA_ProfileName1,ADSP/Unplaced Devices,2,TRUE,-70,
10,TRUE,TRUE,10,20,TRUE,Schedule2,daily,interval,10,20,1
```



NOTE Although the records in the above examples are shown on multiple lines, all entries must be on a single line with no line breaks or carriage returns.

Dropdown Menus

Dropdown menus are located throughout ADSP. Whenever a device or network level is displayed, it will have an associated dropdown menu. There are different dropdown menus associated with devices and network levels.

Devices

Access Point

The dropdown menu for Access Points contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Access Point.
Properties	Opens the Properties overlay for the selected Access Point.
Readiness Test	Validates that the AP is management ready (that is, it can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrades the firmware for the selected Access Point.
Rename	Opens a dialog window to rename the selected Access Point.
Move	Moves the selected Access Point to another network level (floor).
Remove	Removes the selected Access Point from your network.
Audit	Conducts a compliance audit on the selected Access Point.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup	This feature is disabled unless you have a WIPS license.
Forensic Analysis	Opens the Forensic Analysis window for the specified Access Point.
Direct Connect	Accesses the user interface (UI) for the selected Access Point.
Copy MAC	Copies the MAC address of the selected Access Point for later use.

BSS









The dropdown menu for BSSs contain the following functions:



Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected BSS.
Properties	Opens the Properties overlay for the selected BSS.
Rename	Opens a dialog window to rename the selected BSS.
Remove	Removes the selected BSS from your network.

Function	Description
Classification	Classifies the BSS using one of the following classifications: <ul style="list-style-type: none"> • Sanctioned (inherit)—Classify the selected BSS as a sanctioned device that inherits its traits from wherever its location in the network tree. • Sanctioned (override)—Classify the selected BSS as a sanctioned device using traits that override the inherited traits. For example, a security profile can be applied to a BSS that overrides the inherited traits. When using this classification, select the profile and click the Apply link. • Unsanctioned—Classify the selected BSS as unsanctioned. • Neighboring—Classify the selected BSS as a neighboring device.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Forensic Analysis	Opens the Forensic Analysis window for the specified BSS.
Generate Tracker Files	Generates Tracker ADT files to be used in the Tracker application on a laptop. A Tracker Integration License is required to access this feature.
Locate	Opens the device Location tracking window so that you can quickly locate the selected BSS.
Live View	Opens the Live View window for the selected BSS; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the Port Lookup window where you can locate the physical port where the BSS is accessing your network.
Terminate	Opens the Termination options so that you can terminate the connection of the BSS to your network.
AP Test	Tracks network failures from an automated or manual AP connectivity test.
Wireless Vulnerability Assessment	Opens the Vulnerability Assessment window so that you can scan your wireless network for vulnerabilities.
Copy MAC	Copies the MAC address of the selected BSS for later use.

Wireless Clients

The dropdown menu for Wireless Clients contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Wireless Client.
Properties	Opens the Properties overlay for the selected Wireless Client.
Rename	Opens a dialog window to rename the selected Wireless Client.
Remove	Removes the selected Wireless Client from your network.
Classification	<p>Classifies the Wireless Client using one of the following classifications:</p> <ul style="list-style-type: none"> Sanctioned (inherit)—Classify the selected Wireless Client as a sanctioned device that inherits its traits from wherever its location in the network tree. Sanctioned (override)—Classify the selected Wireless Client as a sanctioned device using traits that override the inherited traits. For example, a security profile can be applied to a Wireless Client that overrides the inherited traits. When using this classification, select the profile and click the Apply link. Unsanctioned—Classify the selected Wireless Client as unsanctioned. Neighboring—Classify the selected Wireless Client as a neighboring device.
Client Type	<p>Client Type appears in the menu only when a Wireless Client is sanctioned. As default, Wireless Clients are assumed to be laptops, displaying a laptop icon. This menu item allows you to differentiate phones and handheld devices from laptops in ADSP.</p> <ul style="list-style-type: none"> Default Type— Employee Device— Employee Laptop— Employee Phone— High Priority Visitor Device— Laptop— Low Priority Visitor Device— MCD—

Function	Description
Client Type (contd)	<ul style="list-style-type: none"> Visitor Device—  VoIP Phone—  <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Client Type ▶</p> <ul style="list-style-type: none"> Default Type Employee Device Employee Laptop Employee Phone High Priority Visitor Device Laptop Low Priority Visitor Device MCD Visitor Device VoIP Phone </div> <p>Select the appropriate device to represent a Wireless Client and use its icon for the selected Wireless Client throughout the GUI.</p>
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Add to ACL	Adds the selected Wireless Client to the Access Control List (ACL).
Forensic Analysis	Opens the Forensic Analysis window for the specified Wireless Client.
Locate	Opens the device Location tracking window so that you can quickly locate the selected Wireless Client.
Live View	Opens the Live View window for the selected Wireless Client; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the Port Lookup window where you can locate the physical port where the Wireless Client is accessing your network.
Terminate	Opens the Termination options so that you can terminate the connection of the Wireless Client to your network.
Copy MAC	Copies the MAC address of the selected Wireless Client for later use.

Sensor

The dropdown menu for Sensors contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Sensor.
Properties	Opens the Properties overlay for the selected Sensor.
Upgrade	Upgrades the firmware for the selected Sensor.
Rename	Opens a dialog window to rename the selected Sensor.

Function	Description
Move	Moves the selected Sensor to another network level (floor).
Remove	Removes the selected Sensor from your network.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup	This feature is disabled unless you have a WIPS license.
Forensic Analysis	Opens the Forensic Analysis window for the specified Sensor.
Live View	Opens the Live View window for the selected Sensor; allows you to analyze current WLAN activity on the device.
Spectrum Analysis	This feature is disabled unless you have a Spectrum Analysis license.
Direct Connect	Accesses the user interface (UI) for the selected Sensor.
Copy MAC	Copies the MAC address of the selected Sensor for later use.

Wireless Switch

The dropdown menu for Wireless Switches contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Wireless Switch.
Properties	Opens the Properties overlay for the selected Wireless Switch.
Readiness Test	Validates that the Wireless Switch is management ready (that is, it can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrades the firmware for the selected Wireless Switch.
Rename	Opens a dialog window to rename the selected Wireless Switch.
Move	Moves the selected Wireless Switch to another network level (floor).
Remove	Removes the selected Wireless Switch from your network.
Audit	Conducts a compliance audit on the selected Wireless Switch.
Scan MACs	Scans MAC Addresses to view a list of switch ports.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Forensic Analysis	Opens the Forensic Analysis window for the specified Wireless Switch.
Direct Connect	Accesses the user interface (UI) for the selected Wireless Switch.
Copy MAC	Copies the MAC address of the selected Wireless Switch for later use.

Wired Switch

The dropdown menu for Wired Switches contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Wired Switch.
Properties	Opens the Properties overlay for the selected Wired Switch.
Readiness Test	Validates that the Wired Switch is management ready (that is, it can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrades the firmware for the selected Wired Switch.
Rename	Opens a dialog window to rename the selected Wired Switch.
Move	Moves the selected Wired Switch to another network level (floor).
Remove	Removes the selected Wired Switch from your network.
Audit	Conducts a compliance audit on the selected Wired Switch.
Scan MACs	Scans MAC Addresses to view a list of switch ports.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Direct Connect	Access the user interface (UI) for the selected Wired Switch.
Copy MAC	Copies the MAC address of the selected Wired Switch for later use.

Unknown Devices

The dropdown menu for unknown devices contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected unknown device.
Properties	Opens the Properties overlay for the selected unknown device.
Rename	Opens a dialog window to rename the selected unknown device.
Remove	Removes the selected unknown device from your network.
Classification	Classifies the unknown device as Sanctioned or Unsanctioned.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Add to ACL	Adds the selected Unknown Device to the Access Control List (ACL).
Forensic Analysis	Opens the Forensic Analysis window for the specified unknown device.
Live View	Opens the Live View window for the selected unknown device; allows you to analyze current WLAN activity on the device.

Function	Description
Port Lookup	Opens the Port Lookup window where you can locate the physical port where the Unknown Device is accessing your network.
Terminate	Accesses the Termination options so that you can terminate the connection of the Unknown Device to your network.
Copy MAC	Copies the MAC address of the selected unknown device for later use.

WLSE

The dropdown menu for WLSE devices contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected WLSE device.
Properties	Opens the Properties overlay for the selected WLSE device.
Readiness Test	Validates that the WLSE device is management ready (that is, it can be manage through ASDP). You are alerted of problem areas.
Rename	Opens a dialog window to rename the selected WLSE device.
Move	Moves the selected WLSE device to another network level (floor).
Remove	Removes the selected WLSE device from your network.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Direct Connect	Accesses the user interface (UI) for the selected WLSE device.
Copy MAC	Copies the MAC address of the selected WLSE device for later use.

AirWave


The dropdown menu for AirWave devices contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected AirWave device.
Properties	Opens the Properties overlay for the selected AirWave device.
Readiness Test	Validates that the AirWave device is management ready (that is, it can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrade the firmware for the selected AirWave switch.
Rename	Opens a dialog window to rename the selected AirWave device.
Move	Moves the selected AirWave device to another network level (floor).
Remove	Removes the selected AirWave device from your network.
Audit	Conduct a compliance audit on the selected AirWave switch.
Scan MACs	Scan MAC addresses to view a list of switch ports.

Function	Description
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Forensic Analysis	Opens the Forensic Analysis window for the specified AirWave switch.
Direct Connect	Accesses the user interface (UI) for the selected AirWave device.
Copy MAC	Copies the MAC address of the selected AirWave device for later use.

Device Functions Requiring More Explanation

Live View

ADSP gives you a Live View of the devices operating in your wireless LAN. Live View capability exists throughout the GUI, wherever a device icon appears. You access Live View by clicking on the dropdown menu button of the device— and selecting **Live View**, which automatically limits the data to the specific device you choose.

Only five Live View sessions can be running at one time. If you attempt to open more than five sessions, an error displays. A **Live View** window will open but the monitoring session will not start.

You cannot run Spectrum Analysis and Live View at the same time on any one sensor. If Spectrum Analysis is running and you attempt to start a Live Monitoring session on the same sensor, a warning displays.

Live View consists of four main categories of information:

- Data
- Connections
- Devices
- Frames.

Data

Live View **Data** provides a variety of charts that allows you to analyze different types of data transmitted and received to/from a particular device.

Different charts are displayed according to four customizable views.

View	Description
Summary	<p>Provides a summary of frame data using the following charts:</p> <ul style="list-style-type: none"> • Traffic By Transmitter Authorization • Retry • Traffic By Rate • Traffic By Channel • Devices By Authorization. <p>This is the default view.</p>
Device Analysis	Changes the frame data focus to device information. Charts relating to device information are displayed.
Channel Analysis B/G	Changes the frame data focus to channel information for 802.11b/g network traffic. Charts relating to channel information are displayed.
Channel Analysis A	Changes the frame data focus to channel information for 802.11a network traffic. Charts relating to channel information are displayed.

Connections

Live View **Connections** display device relationships (connections) between your wireless and wired networks with BSSs being the central point. Options are provided to display devices with broadcast frames, devices with multicast frames, or both.

Devices

Live View **Devices** display the devices that have been seen during a Live Monitoring session in tabular form. Options are provided to show all devices, only BSSs, or only Stations (wireless clients). If more than 50,000 frames have been captured during the live monitoring session, only the most recent 50,000 frames are displayed.

The device table can be customized to display the following information:

Column	Description
Device	Lists the different devices that have been seen during the Live Monitoring session.
MAC Address	Displays the MAC address of the seen device.
SSID	Lists the Service Set Identifiers, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS (Basic Service Set) and are the logical groups that access points belong.
Channel	Lists the WLAN channel that the device is operating on.
Channel Extension	Lists the WLAN channel extension that the device is operating on.
Signal (dBm)	Lists the device's signal strength connectivity on the WLAN.

Column	Description
Frames	Displays number the frames, which are the actual packets of 802.11 protocol, that have been observed by the ADSP sensor for the given device.
Bytes	Displays the byte count seen by the device.
First Seen	Displays the time and date the device was first seen.
Last Seen	Displays the time and date the device was last seen.
WEP IVs	Displays the number of unique WEP IVs seen by the device.
Authentication	Lists the authentication method used to authenticate the device.
Encryption	Displays the encryption method used by the device.

Frames

Live View **Frames** display the frames that were captured during a Live Monitoring session. If more than 50,000 frames have been captured during the live monitoring session, only the most recent 50,000 frames are displayed.

Frames data is displayed as follows:

- Frames table (located on top)
- Hex values for a selected frame (located on bottom left)
- Decodes for a selected frame (located on bottom right).

The frame table can be customized to display the following information:

Column	Description
Time	Displays the time the frame was seen.
Source	Lists the device where the frame originated.
Destination	Lists the device where the frame was sent.
BSSID	Displays the Basic Service Set Identifier.
Transmitter	Lists the device that transmitted the frame.
Receiver	Lists the device that actually received the frame.
Address 1	Lists the first address in the frame.
Address 2	Lists the second address in the frame.
Address 3	Lists the third address in the frame.
Address 4	Lists the fourth address in the frame.
Observed Channel	Lists the WLAN channel that the device is operating on.
Channel Extension	Lists the WLAN channel extension that the device is operating on.
Rate	Displays the data rate (in Mbps) being used by the device that sent the packet.
Signal (dBm)	Lists the device's signal strength connectivity on the WLAN.

Column	Description
Size	Displays the size of the frame.
802.11 Type	Displays the 802.11 protocol type used in the frame.
Protocol	Displays the protocol type used in the frame.
Sensor	Displays the MAC address of the sensor that observed the device that sent the packet.

Locate (Location Tracking)

Location Tracking is a technology that enables you to locate and track rogue devices that may be threatening your wireless LAN. Location Tracking uses the RSSI (Received Signal Strength Indications) of the device as seen by at least 3 sensors to triangulate a position relative to the sensor locations. To use this feature, the user must first import a building map and place at least 3 sensors on their corresponding location.

Implementing Location Tracking in ADSP

Location Tracking enables you to locate and track rogue devices that may be threatening your wireless LAN.



NOTE In order for Location Tracking to open and function properly you must have:

- One (minimum) ADSP appliance
- Three (minimum) ADSP compatible sensors per map loaded.

Accessing Location Tracking

You can open the Location Tracking window anywhere in the application when you select a BSS or wireless client and select **Locate** from the device's dropdown menu button—. To track a device, the floor plan (map) must be loaded and sensors positioned on the map).

Importing Maps

To use the built-in Location Tracking feature, you will need to import a map first and place the sensors at their specific locations.



NOTE Each map can be loaded by floor. You may have to re-arrange the sensors to accommodate a map for each floor. You will also need a minimum of three sensors per map.



NOTE A map can only be linked to sensors on the same floor. In a multi floor building, sensors should be grouped by floors and each floor associated with its own map. At least 3 sensors per floor plan are required for location triangulation.

Example: If a location has 2 floors, there must be at least three sensors on each floor (total of six) for Location Tracking to work.

Floor Manipulation Tools

The floor manipulation tools, located in the upper-right side of the window are used to adjust the size of the floor plan image and/or move the floor plan image by dragging it to a new position.



Function	Description
Zoom In	Enlarges the size (zoom in) a floor plan image. Clicking the image area will zoom into another level.
Zoom Out	Reduces the size (zoom out) a floor plan image. Clicking the image area will zoom out to another level.
Zoom to File	Fills the floor plan area with an image. Depending on the size of the image, the image will expand to fit or reduce to fit the floor plan area.
Pan	Moves/re-positions the floor plan image. A hand is used to move/re-position the image.

Setting Images

Select an empty floor and then click the **Design Floorplan** link to import a map. This will open a sub-window and you can upload the appropriate map, which can be in *.gif*, *.jpg*, or *.bmp* files (less than 500kb in size). Select the desired floor plan and select **Open**. The map is then displayed. Scale the image as directed and click **Next: Add to floor** when you are satisfied with the image.

Important! File sizes of imported maps cannot exceed 500kb per map and the pixel depth of the file should be no more than 1500x1500.

Floor Plan Prerequisite

One or more maps or floor plans of the tracking coverage area are needed for this to work. You can obtain floor plans from any source, including producing your own by using drawing tools. Most applications will require multiple maps, for example, if you are setting up multiple buildings. You must supply a map for each floor in a building.

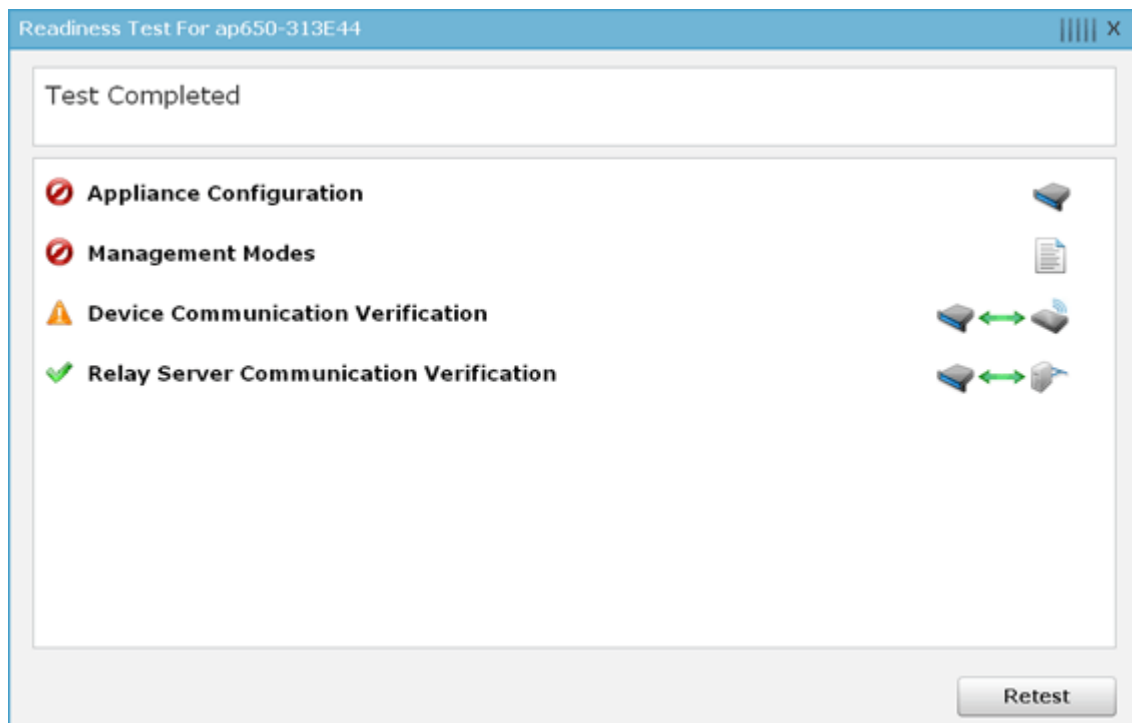
Device Tracking Information

Place your cursor over the tracked device to display statistics and information about the device.




Readiness Test

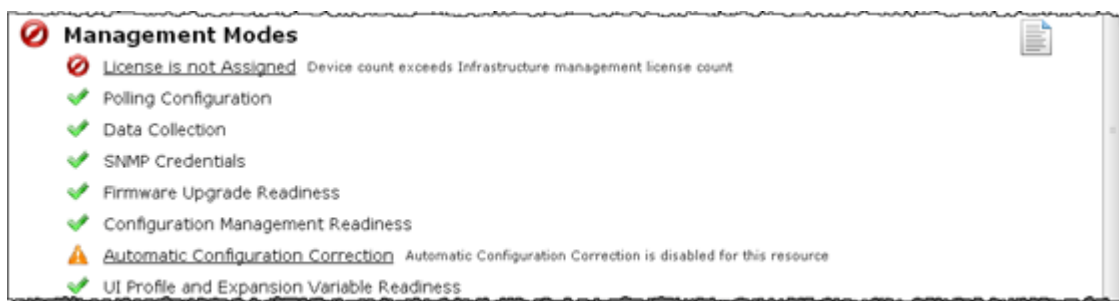
The Readiness Test checks the connections and the communication settings between ADSP and devices in your network. The devices may be an Access Point, a Sensor, or a Switch. You may also run the Readiness Test to check a group of devices by using the network level as a starting point.

To access the Readiness Test, click **Readiness Test** from the dropdown menu of an AP, a Sensor, a Switch, or a network folder (level). A series of test are run and displayed in a Readiness Test overlay.



If you are running the Readiness Test from a device, it is run only on that device. If you are running the Readiness Test from a network folder (level), the test is run on all the devices included in that folder.

There are four categories of tests. Each category can be expanded to review individual tests for that category by clicking the category. Each of the tested items is marked as a success—, a problem—, or a caution area—. If all the tests under a category are successful, the category is marked as a success. If one test under a category has a problem, the category is marked as a problem area.



Network Levels

Appliance

The dropdown menu for appliances contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Appliance.
Properties	Opens the Properties overlay for the selected Appliance.
Readiness Test	Validates that devices in the appliance scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Rename	Opens a dialog window to rename the selected Appliance.
Frame Capture Analysis	Accesses Frame Capture Analysis.
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.
Action Manager	Accesses the Action Manager.
Action Control	Accesses Action Control.
Reports	Accesses Reports.
Report Builder	Accesses the Report Builder.
Scheduled AP Test	Accesses Scheduled AP Test.
Scheduled Vulnerability Assessment	Accesses Scheduled Vulnerability Assessment.
Appliance Manager	Accesses the Appliance Manager.
Scheduled Events	Accesses Scheduled Events.
Auto Classification	Accesses Auto Classification.

Country

The dropdown menu for countries contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Country.
Properties	Opens the Properties overlay for the selected Country.
Readiness Test	Validates that devices in the country scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.

Function	Description
Upgrade	Upgrades the firmware for devices in the selected Country.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	Copies the network scope of a Country. You are prompted to enter a name for the country and select if you want the to include the floor plans or not.
Rename	Opens a dialog window to rename the selected Country.
Remove	Removes the selected Country from your network.
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.

Region

The dropdown menu for regions contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Region.
Properties	Opens the Properties overlay for the selected Region.
Readiness Test	Validates that devices in the region scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrades the firmware for devices in the selected Region.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	Copies the network scope of a Region. You are prompted to enter a name for the region and select if you want the to include the floor plans or not.
Rename	Opens a dialog window to rename the selected Region.
Remove	Removes the selected Region from your network.
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.

City

The dropdown menu for cities contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected City.
Properties	Opens the Properties overlay for the selected City.
Readiness Test	Validates that devices in the city scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrades the firmware for devices in the selected City.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	Copies the network scope of a City. You are prompted to enter a name for the city and select if you want the to include the floor plans or not.
Rename	Opens a dialog window to rename the selected City.
Remove	Removes the selected City from your network.
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.

Campus

The dropdown menu for campuses contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Campus.
Properties	Opens the Properties overlay for the selected Campus.
Readiness Test	Validates that devices in the campus scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrades the firmware for devices in the selected Campus.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	Copies the network scope of a Campus. You are prompted to enter a name for the campus and select if you want the to include the floor plans or not.
Rename	Opens a dialog window to rename the selected Campus.
Remove	Removes the selected Campus from your network.

Function	Description
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.

Building

The dropdown menu for buildings contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Building.
Properties	Opens the Properties overlay for the selected Building.
Readiness Test	Validates that devices in the building scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.
Floor Plan	Views the floor plan for a building where you can manipulate the floor plan, add devices, and track devices.
Upgrade	Upgrades the firmware for devices in the selected Building.
Copy Folder	Copies the network scope of a Building. You are prompted to enter a name for the building and select if you want the to include the floor plans or not.
Rename	Opens a dialog window to rename the selected Building.
Remove	Removes the selected Building from your network.
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.

Floor

The dropdown menu for floors contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Floor.
Properties	Opens the Properties overlay for the selected Floor.
Readiness Test	Validates that devices in the building scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.
Floor Plan	Views the floor plan for a building where you can manipulate the floor plan, add devices, and track devices.
Upgrade	Upgrades the firmware for devices in the selected Floor.
Rename	Opens a dialog window to rename the selected Floor.

Function	Description
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.
Add Device	Adds devices to the AirDefense Services Platform.

Unplaced Devices

The dropdown menu for unplaced devices contain the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Unplaced Devices level.
Properties	Opens the Properties overlay for the selected Unplaced Devices level.
Readiness Test	Validates that devices in the building scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas.
Upgrade	Upgrades the firmware for devices in the selected Unplaced Devices level.
Forensic Analysis	Accesses Forensic Analysis.
AP Test	Accesses AP Test.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment.
Add Device	Adds devices to the AirDefense Services Platform.

Network Level Properties

All network level properties display the same information except the appliance level.

Appliance Level

The screenshot shows a web-based configuration interface titled 'PROPERTIES' for an ADSP appliance. On the left is a sidebar with a list of configuration categories: Information, Channel Settings, Device Access, Sensor Operation, Legacy Sensor Settings, Performance Profile Assignments, Polling, RF-Domain, Radio Settings, Relay Server, Environment Monitoring, Security Profile Assignments, Communication Settings, WLAN Profile Assignments, and Pending State Audit. The main area displays the 'Information' section with the following fields: Name (ADSP), Host (localhost), Port (0), and Status (OK). Below these fields are two buttons: 'Autoplace' and 'Push Configuration'. A 'Save' button is visible in the top right corner of the window.

The following information is displayed:

Function	Description
Name	The name of the appliance.
Host	The host name of the appliance.
Port	The port number of the appliance.
Status	The status of the appliance in your network.

The **Autoplace** button is used to place all devices located in the selected network folder to the proper network level using Auto-Placement Rules.

The **Push Configuration** button is used to push the existing configuration for all devices in the selected network folder out to their respective device.

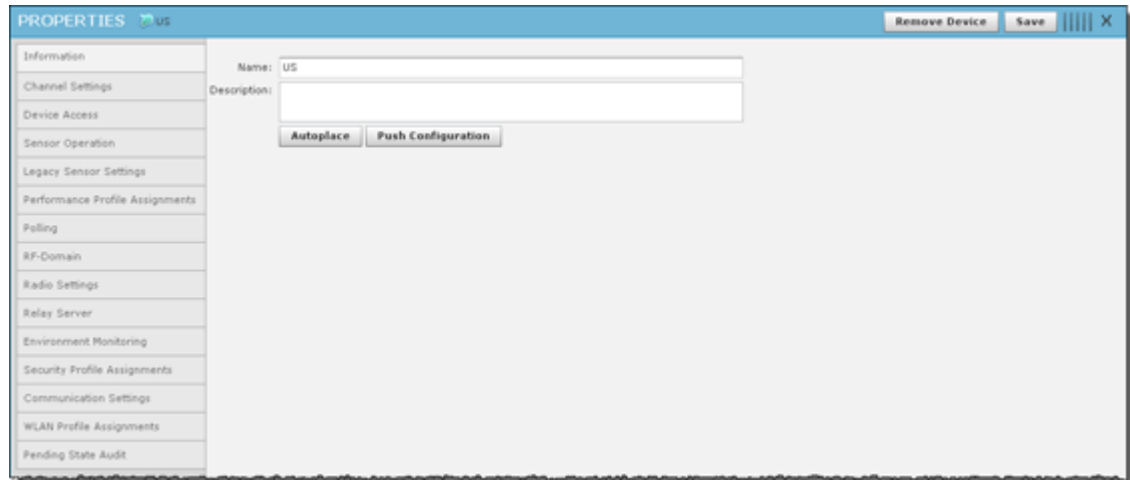
You can view and/or override an appliance's configuration by selecting:

- Channel Settings
- Device Access
- Sensor Operation
- Sensor Only Settings
- Performance Profiles
- Polling
- RF-Domain
- Radio Settings
- Relay Server
- Environment Monitoring
- Security Profiles
- Communication Settings

- WLAN Profiles
- Location Based Services
- Pending State Audit.

These configuration settings (or profiles) are equivalent to the ones described earlier in the *Configuration* section of this chapter. You must save any changes that you make.

All Other Levels



The following information is displayed:

Function	Description
Name	The name of the network level.
Description	A description of the network level.

The **Autoplace** button is used to place all devices located in the selected network folder to the proper network level using Auto-Placement Rules.

The **Push Configuration** button is used to push the existing configuration for all devices in the selected network folder out to their respective device.

You can view and/or override a network level's configuration by selecting:

- Channel Settings
- Device Access
- Sensor Operation
- Sensor Only Settings
- Performance Profiles
- Polling
- RF-Domain
- Radio Settings
- Relay Server

- Environment Monitoring
- Security Profiles
- Communication Settings
- WLAN Profiles
- Location Based Services
- Pending State Audit.

These configuration settings (or profiles) are equivalent to the ones described earlier in the *Configuration* section of this chapter. You must save any changes that you make.

CHAPTER 3 SECURITY

Introduction

ADSP has several modules that you can install to provide security for your network. You can enhance ADSP with:

- The WIPS module that will eliminate detected rogues from your network
- The Advanced Forensic Analysis module that unlocks the more advanced features of Forensic Analysis
- The Vulnerability Assessment module that allows you to view your network through a hacker's point of view
- The WEP Cloaking module that allows you to use your legacy equipment while you are upgrading to equipment with the latest technology
- The Tracker Integration module that provides the tracker files to be used with Motorola AirDefense Tracker.

✓ **NOTE** Each of these modules require a separate license available from Motorola.

WIPS

By installing an ADSP WIPS license, you add the ability to detect wireless attacks to your network and analyze anomalous behavior of devices in your network. Meaningful security problems are detected while events that cause false alarms are filtering out.

ADSP WIPS protects your network from threats such as:

- Reconnaissance
 - Rogue APs
 - Open/misconfigured APs
 - Ad-Hoc networks

- Sniffing
 - Dictionary attacks
 - Leaky APs
 - WEP/WPA/LEAP cracking
- Masquerade
 - MAC spoofing
 - Evil twin attacks/Wi-Phishing attacks
- Insertion
 - Man-in-the-middle attack
 - Multicast/broadcast injection
- Denial-of-service attacks
 - Disassociation
 - Duration field spoofing
 - RF jamming

ADSP WIPS can mitigate wireless threats via the air by disabling wireless connections between intruders and authorized devices. A WIPS license enables the Air Termination feature which is extremely precise at ensuring that only the offending device is prohibited from operating.

Port suppression is also able to identify switch ports that have offending devices connected to them. Once detected, the port is turned off to prevent the rogue device from accessing the network.

A WIPS license also enables Sensor Monitoring which is added to the **Configuration** tab. Sensors are used to monitor your network for threats.

Planning Your Sensor Deployment

When adding a WIPS license, you should plan where you will be placing your sensors. ADSP uses remote sensors to collect data transmitted by 802.11a-, b-, g-, and n-compliant devices and to send that data to a your central ADSP appliance for analysis and correlation. Because the sensors are passive devices that function primarily in listen-only mode, a single sensor can monitor multiple APs.

You should leverage any site surveys you conduct for placement of access points as aids to sensor placement decisions.

Deployment Considerations

Building Structure

Many materials used in building construction may significantly impact the propagation of signals in the 2.4 GHz spectrum or the 5 GHz spectrum.

- Concrete reinforcement bars
- Elevator shafts
- Electric motors (for example, blowers and generators)
- Lighting fixtures.

Physical and Electromagnetic Interference

Many devices can interfere with sensors' monitoring of the wireless network, including:

- Cordless phones and headsets
- Bluetooth devices
- Microwave ovens
- Consumer cordless devices (for example, surveillance cameras, baby monitors, and video transmission extenders).

802.11a, b, g, n Device Density

You should consider the density of 802.11a, b, g, and n devices:

- Support of a high number of users
- Support of high bandwidth consumption
- Localization of wireless network service.

AP Placement

The sensors should be separated by at least 10 feet from any installed AP's to avoid radio desense. The active transmissions of an AP can desensitize the sensor receiver radio on the same channel when placed in close proximity of an AP.

Device Location Information

While a single Motorola AirDefense sensor can monitor a very large area, distributing multiple sensors in such an area can provide a much better idea of where a rogue device is physically located. By comparing the RSSI values each sensor detects, you can find the device more easily. Three or more sensors are required for the location tracking to work because triangulation is a requirement for the location tracking to work.

Desired Monitoring and Intrusion Protection Functionality

Your decisions about sensor placement should also take into account what functionality you plan to use. Five important functions that are somewhat dependent on sensor density or placement are:

- **WEP Cloaking**—For effective WEP Cloaking, several sensors should be deployed around the perimeter of a building. Higher sensor density will typically yield better protection for your legacy encryption devices.
- **Location Tracking**—To track a device, the device must be observed by three or more sensors on the same floor plan. Higher sensor density will typically yield more accurate results.
- **Connection Termination**—To terminate a device's connection to your network, the device must be in range of a sensor sending termination signals.
- **Policy Enforcement**—To ensure adherence to policies or to detect attacks against managed devices, sensors must be able to receive a representative sampling of traffic sent by all devices they are monitoring.
- **Rogue Detection**—Even sporadic emanations from wireless clients and access points can reveal the presence of rogues. You need to place sensors where transmissions from rogue devices can be detected as soon as they enter the scanning area.

Assets to be Protected

- Wireless-capable devices that contain sensitive data must be protected.

- Wired networks protecting the wire from wireless breach. This approach is key to making wireless monitoring deployment decisions in very large installations, such as military bases, airports, power plants, campuses, etc.
- A common perception is that wireless devices must be detected and monitored throughout a given property. This becomes impractical in many cases. A more practical approach is one that protects the wired network while using more sane decisions for monitoring.

Sensor Quantity, Location, and Installation

Application choice will significantly impact the sensor density and sensor placement. For example, rogue detection in a no wireless zone needs fewer sensors as even sporadic emanations from a wireless device, at the lowest data rate and longest range, can reveal the presence of a rogue. As the applications become more complex, they may require a representative sample of frames or meet certain minimum signal level thresholds, increasing the sensor density requirement.

Using these factors in baseline decisions with regard to sensor placement, the following coverage area guidelines may be applied to establish an effective deployment.

Application	RSSI
Rogue Detection	> -90dBm
Policy Enforcement	> -80dBm
Mitigation (Termination)	> -70dBm
Location Tracking	Every device has to be seen by three or more sensors and/or infrastructure APs on the same floor plan.

Sensors that may be exposed to harsh environments can be placed in accessory enclosures (NEMA-4) that protect the sensor and provide code, regulatory compliance, or both.

Power and Data Cabling

Sensors are often placed in areas that take advantage of pre-existing power and data cabling. These areas include wiring closets and other areas where IDFs may be located. Where these locations are somewhat shielded from the wireless environment, the sensor may be extended to just outside of these spaces using standard power cords and pre-terminated data cables, obviating the need for additional, costly fixed runs. Choosing facilities that come as close to centrally locating the sensors in the intended monitoring space should be done when practical. In instances where wiring closets, IDFs, or both are not ideally located for sensor placement, sensors may take advantage of Power Over Ethernet, either from a single power injector or a compliant switch. PoE injectors are available from AirDefense.

If there are gaps in coverage, or if deployment cost is a factor (due to the required density of sensors or the cost of wiring to place sensors in strategic locations), there are several relatively inexpensive remedies. Where wiring for placement in an ideal location is impractical, employ additional sensors to correct as necessary. FCC Rules regulate the use of antennas as aids to reception for the sensors, in regard to the sensor's 802.11 component. If antennas would greatly enhance the overall deployment, Motorola AirDefense is available to advise on the best approach for antenna application, considering both regulatory guidelines and the physical design of the sensors.

In either case, always use facility floor plans to indicate where sensors are placed and to indicate areas where a coverage test was done.

Sensor Placement

Using Motorola LAN Planner to Plan Sensor Placement

Motorola LAN Planner is a revolutionary software package that enables you to efficiently design, model, and measure 802.11a, 802.11b, 802.11g, and 802.11n networks, as well as plan your sensor coverage. Building facilities and campus environments can be quickly modeled using menus that guide you step-by-step. You can quickly place access points and predict signal coverage during the WLAN design phase. Post-WLAN deployment, you can use Motorola LAN Planner's powerful features for measuring network performance and validating network designs.

Features

- **Rapidly Design and Deploy More Efficient Networks:** Motorola LAN Planner helps design quality wireless networks by helping to overcome the challenges of coverage holes, poor service areas and improper capacity and network resource allocation.
- **Avoid Costly Retrofits:** Motorola LAN Planner minimizes design and deployment costs by helping the designer visualize the physical location and configuration of installed network equipment, automatically placing and configuring access points, and accurately predicting network coverage and capacity.
- **Simplify Complex Wireless Environments:** Designers can quickly compare site-survey measurements to the expected network performance, enabling real-time and accurate design modifications. Motorola LAN Planner is intuitive and helps users rapidly operate and design in all phases of WLAN build-out and management.
- **Included:** Motorola Site Scanner functionality, which provides real-time, in-field measurements for site surveys. Seamlessly integrated into Motorola LAN Planner, measurements from Motorola Site Scanner can be used to optimize and compare its predictions.

In addition to planning all your access points prior to deployment, LAN Planner also offers a sensor planning feature. You can use the same building maps to carefully plan sensor placement, ensuring maximum coverage and no dead spots.

Using Motorola AirDefense Mobile to Plan Sensor Placement

After you map out anticipated sensor locations, you can assess the effectiveness of coverage by correlating site survey data and assumptions discussed previously. You can also use the test procedure described here to validate sensor location.

Because sensors are passive devices that do not have the capability to transmit data, the process of determining sensor coverage depends on a "reverse site survey" process in which a device introduces a signal in your Wireless LAN, and then the signal is tracked through the facility using the deployed sensors.

Prerequisites

Documents that can help you determine sensor placement include:

- Floor Plans
- Existing Site Surveys
- Wiring layouts
- Regulatory rules and codes for wiring, construction, materials, etc., where applicable.

Tools you will need:

- A laptop running Motorola AirDefense Mobile r4.0 or later (or Motorola Site Scanner)

- An 802.11a/g/n wireless device (wireless client or access point). The ideal output power for this device (around 40 mW) would be that of a retail quality wireless client card or access point, as these are likely rogue candidates.



NOTE A soft access point on a laptop is often an ideal target because it can be Locked On a channel and is battery powered through being hosted on a laptop.

- Wiring layouts
- Regulatory rules and codes for wiring, construction, materials, etc., where applicable
- During the survey, access to all areas to be monitored is required.

Procedure

1. Following is a step-by-step process to accomplish this task.
2. Obtain Maps/Layouts of the facility and determine the traversal plan.
3. Start AirDefense Mobile.
4. Turn on the target device (access point, soft access point, or laptop/PDA with wireless client card).
5. AirDefense Mobile should detect the target device.
6. Identify the target device in the AirDefense Mobile device tree and use your mouse to right-click on it to display a list of options.
7. Use AirDefense Mobile Options to Lock On the channel on which the target device is discovered.
8. Right-click select the device in the Dashboard tree; select LiveView.
9. Focus on "Signal Strength" in the **Decode** tab in LiveView. Verify that the target device is being tracked by AirDefense Mobile.
10. When a wireless client (station) card is being used as a target, significant peaks and valleys are observable in signal strength as the card rotates through channels probing for an access point. The peaks are indicative of the effective signal strength relative to AirDefense Mobile.
11. Move the target device to the anticipated fringe where a neighboring sensor would become primary.
12. At the fringe of coverage, signal strength should be no less than -70 dBm to assure termination ability.
13. Move AirDefense Mobile to the anticipated location of the next sensor and use the same procedure to ensure that its anticipated coverage area is valid.
14. If the above sensor placement proves adequate from a coverage and cost of placement perspective, factors observed during this analysis may be extrapolated to other locations of similar construction.

Sensor Placement with WEP Cloaking

WEP Cloaking will typically require a higher density of sensor deployment than most other applications. This puts WEP cloaking in the highest category sensor density deployments similar to Location Tracking.

Considerations

For effective WEP Cloaking, there are two important considerations:

- **Spatial coverage** - The sensors enabled with WEP Cloaking must at a minimum cover the same area as the access points and wireless clients they are protecting.

For this requirement, you should leverage any site surveys you conduct or have conducted for placement of access points as aids to sensor placement decisions. Another option is using a WLAN simulation tools such as Motorola LAN Planner.

For example, in a typical retail location most wireless point-of-sale devices will be in the front of the store near the check-out stations. Assuming the hacker would be outside of the building, sitting in the front parking lot, it would make sense to place at least 2 sensors in each of the corners in the front of the store. If there is public access from the back of the building or the retail location is surrounded by parking areas, you may want to consider additional sensors in the back for complete protection.

- **Channel coverage** - A single sensor should not be required to cloak more than 3 access points at a time.

For effective cloaking there must be sufficient chaff WEP frames to confuse the statistical WEP cracking tools. At the same time, the sensors must perform regular Wireless IPS scanning on other channels. The sensors are designed to intelligently adjust their frequency scanning patterns. However, to maximize cloaking effectiveness and scan all other channels for possible intrusions, sensors should not be expected to cloak more than three AP's, or more specifically 3 unique communication channels at a time.

For Adequate Protection

Typically, it will take several sensors deployed at the perimeter of the building to adequately protect all wireless devices with WEP Cloaking. This also implies that, even in small stores, it may take more than one sensor for adequate WEP Cloaking protection; the higher the density of sensors you deploy, the better your legacy encryption devices will be protected. Any deployment should start with a site survey or RF simulation of the WLAN environment, followed by a mapping of sensor coverage to access point coverage of unique channels.

Sensor Placement With Location Tracking

Sensor density and sensor placement are the most important factors regarding overall positioning resolution. To achieve accurate results, the system requires RSSI values from at least three independent sensors on the same floor plan.

Due to the nature of high frequency signals (2.4 GHz and 5 GHz) and limited signal strength resolution in 802.11 devices, the positioning resolution and stability tends to be better near receivers/sensors.

Therefore, Motorola recommends placing a sensor in each area where accurate resolution is required or to increase overall sensor density to ensure high RSSI values.

Considerations

Every site is unique in terms of actual sensor coverage; this section merely describes sensor placement and respective coverage in a simplified way. Actual signal propagation is a very complex issue due to environmental factors like the reflection/absorption properties of materials (walls, furniture), large moving object, etc.

- **Sensors should be placed in corners**, preferably in a way which minimizes random fluctuations in signal strength caused by people moving around, opening / closing doors, windows or large objects which may be moved during operation, etc.
- **Sensors should not be placed in a straight line**—to eliminate the possibility of having two or more similar RSSI values from sensor combinations for different location, combined coverage areas for the sensors should not be “symmetric”.
- **Place additional sensors in areas where accuracy is important**—to achieve repeatable and consistent positioning resolution, sensors should be placed so that they measure unique signal strengths and sensor combinations for each location considered significant.

IDS versus Location Tracking

Ideal sensor placement for Wireless IDS differs from that for Location Tracking.



For Intrusion Detection System



With Location Tracking

Example 1

You have a small office of 10,000 sq. ft. For Wireless IDS/IPS you would only need 1 sensor; to maximize the coverage it makes sense to place the sensor in the center of the building. When location tracking is needed in this same scenario, a minimum of 3 sensors for each floorplan would be required, and recommended placement is at the corners.

Example 2

You have a multi-floor building with 3 floors. Depending on floor construction the RF may travel through each floor. If only Wireless IDS/IPS is required, you may be able to leverage detection through the floor and ceiling and place sensors on every other floor. Depending on the floor characteristics, you may need a sensor on each floor, however it may make sense to off-set each sensor on each floor and take advantage of the detection through the floor and ceiling. If location tracking is needed, the same 3 sensors for each floor plan would be required and the recommended placement is 3 sensors in the corners of each floor.

Sensor Monitoring

ADSP allows you to define system profiles that help monitor:

- Sensor performance
- Sensor security
- Sensor policies.

You should set up profiles to assist you in monitoring your system. If thresholds set in the profiles are exceeded, an alarm is generated for the violation which alerts you of the problem.

Sensor monitoring profiles are located in the **Configuration** tab under different categories. The various profiles include:

✓ **NOTE** Each of these features are discussed in *Chapter 2, The Basic System*.

- Sensor Operation—used to:
 - Enable Sensor-level options
 - Configure the Sensor scan pattern
 - Configure sensor settings for Advanced Spectrum Analysis.

Navigation: [Configuration](#) > [Operational Management](#) > [Sensor Operation](#)
- Environment Monitoring—used to configure the thresholds for monitoring. If a threshold value is exceeded, an alarm is generated. You can also elect to monitor your system for unobserved devices and generate alarms for missing devices.

Navigation: [Configuration](#) > [Network Assurance](#) > [Environment Monitoring](#)
- Performance Profiles—used to create and edit network performance threshold policies for BSSs and wireless clients on your wireless LAN.

Navigation: [Configuration](#) > [Network Assurance](#) > [Performance Profiles](#)
- Security Profiles—used to define the security configurations of sanctioned wireless clients on your wireless LAN.

Navigation: [Configuration](#) > [Appliance Platform](#) > [Security Profiles](#)
[Configuration](#) > [Security & Compliance](#) > [Security Profiles](#)
- Wired Network Monitoring—used to monitor the wired network devices in your system and generate an alarm under certain conditions.

Navigation: [Configuration](#) > [Security & Compliance](#) > [Wired Network Monitoring](#)

Advanced Forensics

The Advanced Forensic Analysis module unleashes the full potential of AirDefense Services Platform's Forensic Analysis. When installed, Advanced Forensic Analysis replaces the basic Forensic Analysis that is included in AirDefense Services Platform.

Advanced Forensic Analysis has all the features of the basic Forensic Analysis plus some very powerful enhancements. There are two categories of Advanced Forensic Analysis:

- Scope Based Forensic Analysis
- Device Based Forensic Analysis

The extra features include:

- The ability to show forensic data for the entire system, a single network level, or a single sensor (Scope Based only)
- The ability to analyze for more than a 24 hour time period
- The ability to adjust the time window using sliders
- Graphical views added to all tabs
- Data filters are enabled

- Location Analysis tab is activated (Device Based only).

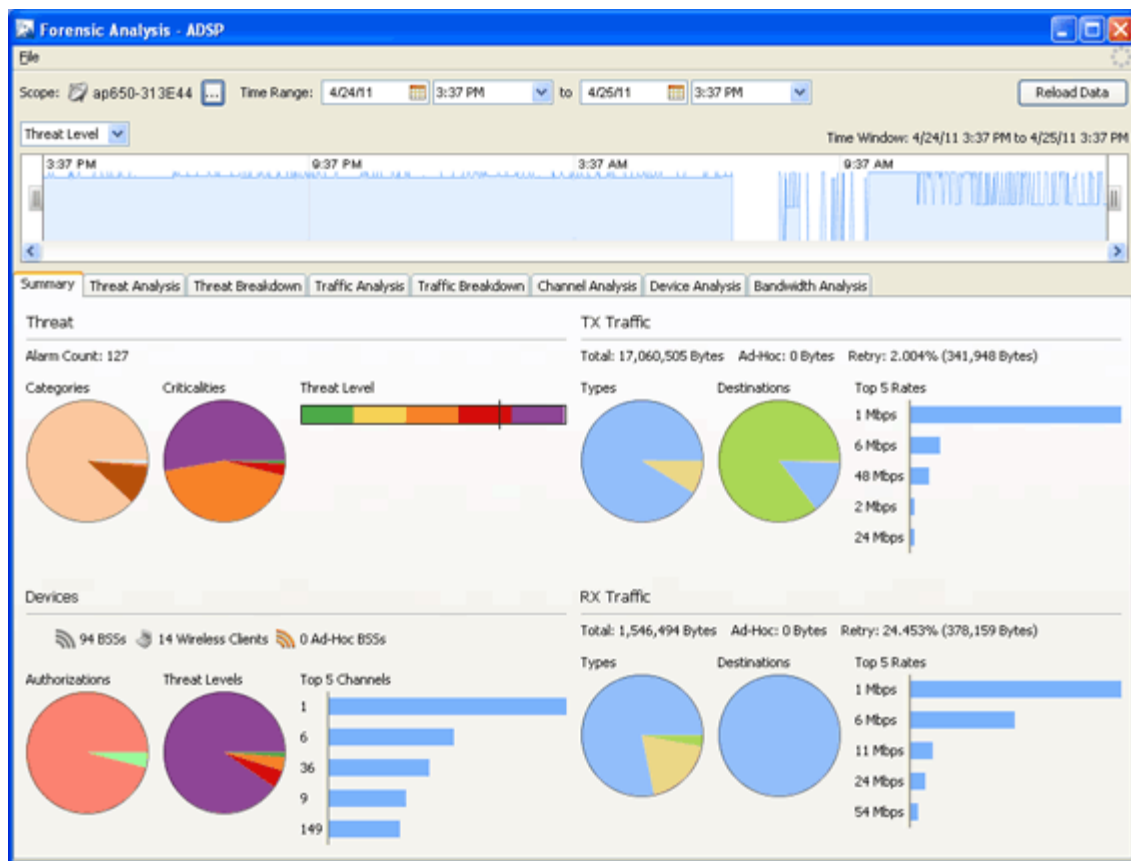
Administrators can view the activity of a suspect device over a period of months and drill down to minute-by-minute detail of wireless activity. Records are kept over a long period of time so that administrators can review events months later to improve network security posture, assist in forensic investigations, and ensure policy compliance. These records can be used to provide evidence that an attacker has made repeated attempts to break into the wireless network and to know where the attack was launched.

Advanced Forensic Analysis stores and manages 325 data points every minute for each wireless device on a network. This feature provides administrators more insight into wireless LAN performance and specific wireless device activity. Trends in network usage can easily be visualized to assist in performance troubleshooting such as identification of abnormal usage and capacity planning.

See the ADSP Help for details on how to use Advanced Forensic Analysis.

Scope Based Forensic Analysis

Scope Based Forensic Analysis provides forensic data for the the network levels and sensors in the Network Tree. No BSSs, Wireless Clients, APs, or Switches are analyzed in Scope Based Forensic Analysis.



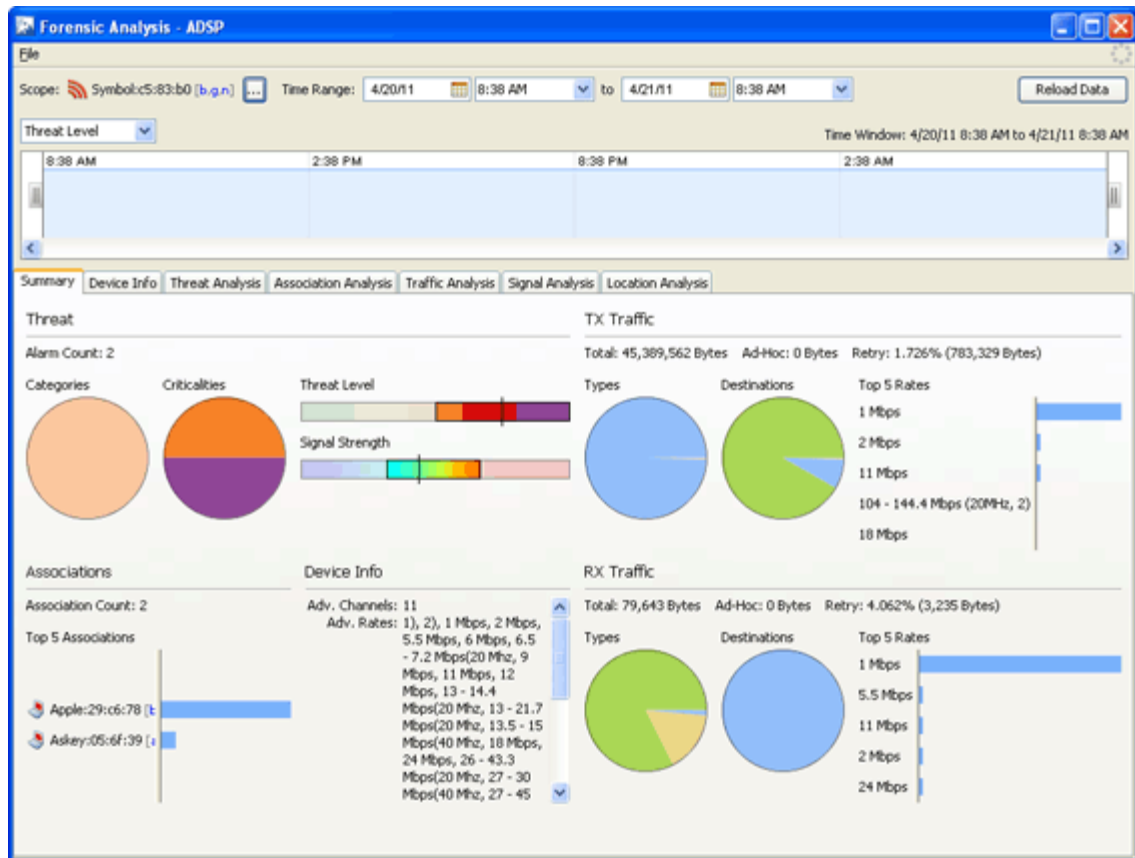
The following forensic data is included with Scope Based Forensic Analysis:

- A summary that includes high-level information about the threat level, device counts and traffic for the entire scope over the selected time range (**Summary** tab).
- Active alarm information (**Threat Analysis** tab).
- Threat level information on items within the selected scope (**Threat Breakdown** tab).
- Transmitted and received traffic by all devices in the selected scope. (**Traffic Analysis** tab).

- Total traffic seen by the top 100 devices in the selected scope (**Traffic Breakdown** tab).
- Device count for each channel over time (**Channel Analysis** tab).
- Device counts for devices and sensors (**Device Analysis** tab).
- Wired bandwidth usage of the sensors in the selected Scope over time (**Bandwidth Analysis** tab).

Device Based Forensic Analysis

Device Based Forensic Analysis provides forensic data on BSSs, Wireless Clients, APs, and Switches.



Device Based Forensic Analysis provides Administrators with the same forensic data that Basic Forensic Analysis does, but includes the extra features mentioned earlier. The same tabs are included plus an extra **Location Analysis** tab for BSSs and Wireless Clients.

The **Location Analysis** tab provides information to help administrators locate devices in their wireless network. A Heat Map and a Location Map are used to locate a device. A table view is provided to display the coordinates of a device. To use the map feature, you must first import the location map that is used by Location Analysis.

Vulnerability Assessment

Using your existing sensor deployment, Vulnerability Assessment scans your wireless network for vulnerabilities utilizing a hacker's point-of-view. This allows you to:


- Identify network security issues before a hacker does

- Remotely scan for and discover wireless network vulnerabilities
- Generate alarms to bring attention to vulnerabilities.

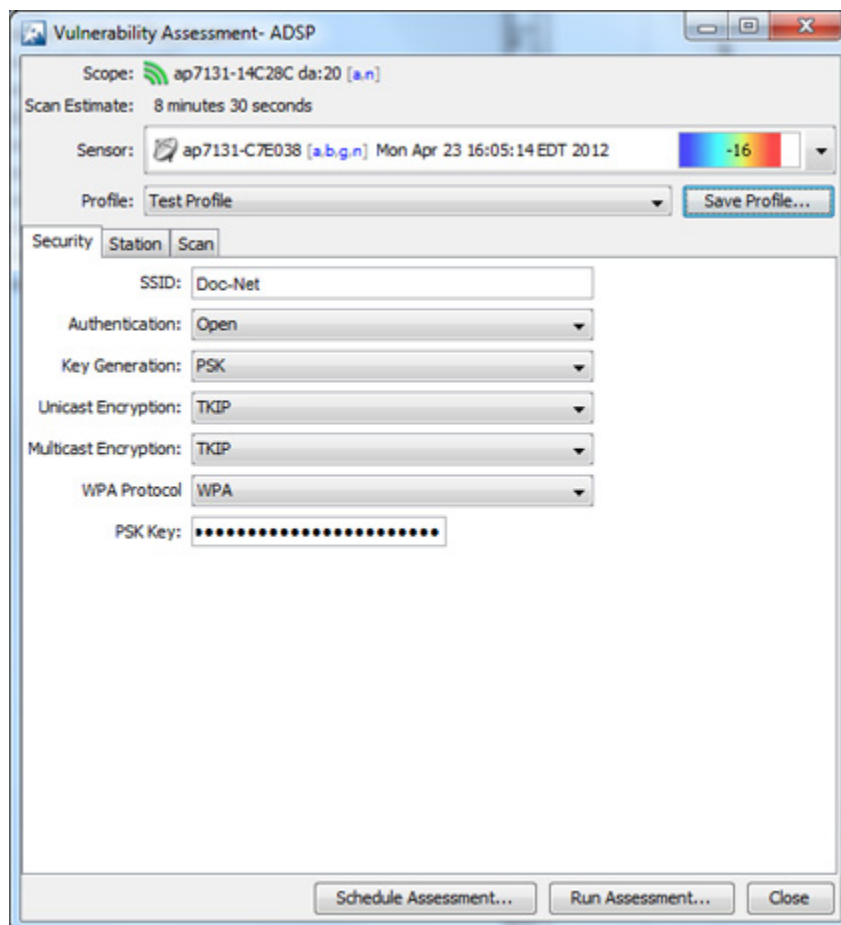
The assessment is accomplished by using deployed sensors as a wireless client to connect to an AP and scan network resources. Vulnerability Assessment can be run automatically or manually, providing proactive notification that network resources may be compromised.

- ✓ **NOTE** For ADSP 8.1.1, Vulnerability Assessment is only supported on the M510 and M520 Sensors with firmware version 5.3 or higher installed. Vulnerability Assessment is also supported on the AP650 and AP-7131 Sensors with WiNG 5.1 or higher installed.

On-Demand Vulnerability Assessment

You can conduct an Vulnerability Assessment anytime you need by using an on-demand assessment. To initiate an on-demand assessment, click on the dropdown menu button— for a BSS or network level, and select **Wireless Vulnerability Assessment**.

- ✓ **NOTE** When the scope is a network level, all APs in the scope are assessed.

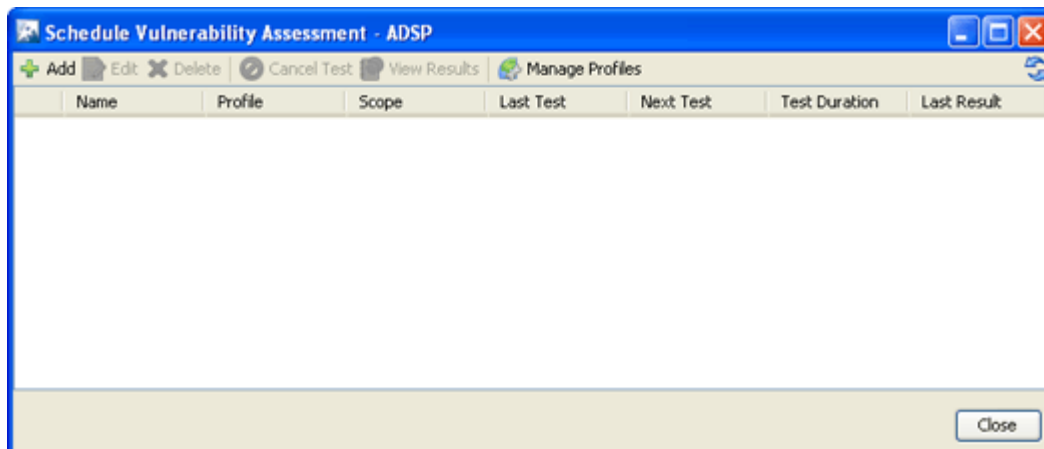


The **Vulnerability Assessment** window allows you to configure and run the assessment. After you have configured an assessment, you can save it as a profile. A profile can be selected later to run test on a similar scope.

See the ADSP Help for details on how to set up and run Vulnerability Assessments on demand.

Automated (Scheduled) Vulnerability Assessment

Automated Vulnerability Assessments must be scheduled using the [Schedule Vulnerability Assessment](#) window. To schedule a Vulnerability Assessment, navigate to [Menu > Scheduled Vulnerability Assessment](#).



The [Schedule Vulnerability Assessment](#) window displays a list of all scheduled assessments. From the [Schedule Vulnerability Assessment](#) window you can:

- Add, edit, delete, and cancel assessments
- View detail assessment results
- Manage the profiles that are used to run assessments on similar scopes.

See the ADSP Online Help for details on how to schedule Vulnerability Assessments and use the [Schedule Vulnerability Assessment](#) window.

WEP Cloaking

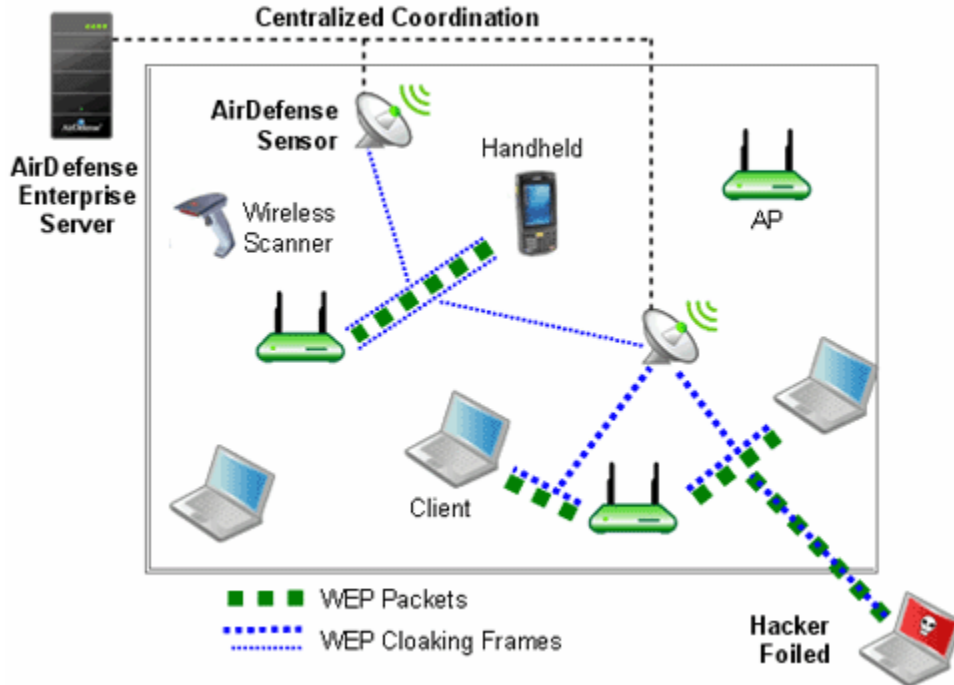
In order to extend the life of some older legacy equipment that only supports WEP encryption, Motorola AirDefense has implemented a feature known as WEP Cloaking. This technology injects "noise" into a WEP-protected environment by transmitting frames that appear to be sourced from valid devices but are encrypted with an invalid WEP key. This has very little impact on the devices that know the correct WEP key and serves to confuse any attackers which might be attempting to crack the WEP key.

- ✓ **NOTE** By default, the sensor is a passive wireless monitoring device and does not transmit (provided termination has not been enabled). Enabling the sensors for WEP Cloaking will cause the sensors to actively transmit on the channels of the access points it is protecting.

How Does WEP Cloaking Work?

ADSP sensors communicate with the ADSP appliance to coordinate cloaking operation. The server can be configured to instruct a group of sensors to cloak sanctioned devices in a given location. Sensors are designed to intelligently adjust their frequency scanning patterns to maximize cloaking effectiveness while performing regular Wireless IPS scanning on other channels. More than one sensor can cloak a single wireless device depending on spatial coverage.

Once configured for cloaking, sensors intelligently analyze local traffic and insert carefully timed cloaking frames as shown in the figure below. To attackers, who do not have the secret WEP key, these cloaking frames appear as legitimate WEP traffic between sanctioned devices. Sanctioned devices, configured with the production WEP key, automatically ignore the cloaking frames as their integrity test fails.



An attacker sniffing traffic will not be able to distinguish between cloaking frames and legitimate frames, and therefore, cannot filter out the cloaked frames. When statistical WEP cracking tools are run on the captured data, they simply fail to decode the key. The following figure shows a screenshot of Aircrack-ng with WEP Cloaking enabled.

```

Aircrack-ng
[00:10:45] Tested 1894657 keys (got 711357 IVs)

KB  depth  byte(vote)
0  0/ 1  01< 74> 99< 22> 95< 7> DA< 3> 2B< 3> 72< 0>
1  0/ 1  23< 107> 94< 40> 26< 18> F2< 16> DA< 15> 6A< 13>
2  0/ 1  45< 122> CA< 21> 6C< 3> 70< 1> 42< 0> AD< 0>
3  0/ 1  67< 124> 21< 15> 80< 10> 81< 5> 62< 3> B3< 3>
4  0/ 1  89< 45> B3< 9> 2A< 8> DD< 8> F4< 8> 45< 5>
5  1/ 2  AC< 10> 82< 7> B4< 5> 66< 1> 81< 0> F5< 0>
6  5/ 6  F6< 10> CB< 9> 6D< 9> FF< 9> 3C< 5> D2< 5>
7  0/ 1  97< 35> F4< 13> FF< 13> 3C< 12> F6< 11> E4< 11>
8  1/ 2  CB< 30> 4B< 10> 5D< 5> 28< 5> 08< 5> 2A< 5>
9  6/ 7  59< 15> 32< 13> 6B< 12> 1E< 11> 73< 11> 52< 9>
10 0/ 1  92< 61> 05< 30> EC< 20> 17< 16> CD< 15> EF< 14>
11 0/ 7  46< 43> 18< 32> 71< 31> 0C< 30> 4B< 26> 98< 25>

Attack failed. Possible reasons:
* Out of luck: you must capture more IVs. Usually, 104-bit WEP
  can be cracked with about one million IVs, sometimes more.
* If all votes seen equal, or if there are many negative votes,
  then the capture file is corrupted, or the key is not static.
* A false positive prevented the key from being found. Try to
  disable each Korek attack (-k 1 .. 17), raise the fudge factor
  (-f)

```

What if there Is a Problem?

In the event of a wired network outage, if sensors lose connection with the centralized server, they will continue to cloak. In addition, WEP Cloaking is optimized to not disturb the wireless environment or impact Wireless LAN performance. The sensors use countermeasures, correlation through the server, and mutual coordination over the air to maximize the effectiveness of cloaking with nominal wired and wireless bandwidth consumption.

Are there any Recommendations?

- You should use a layered security approach to fortify your wireless network. Motorola AirDefense recommends that you follow these guidelines to secure a wireless network utilizing WEP wireless devices:
- Use WEP Cloaking to protect the wireless network using WEP Encryption.
- Enable policy-based termination on a Rogue Wireless Client and Replay Injection Attack alarms.
- If the access points support PSPF (Public Secure Packet Forwarding) mode, also referred to as AP isolation, you must enable it. PSPF mode prevents wireless client to wireless client communication and will limit the effectiveness of typical replay attack.
- When choosing your WEP key, it is best to use a randomly chosen hexadecimal key.
- Analyze the power output of APs to ensure that the AP is not transmitting any further than is necessary.
- Authorize only specific data rates:
 - Check the AP's allowed data rates to ensure that unnecessarily distant wireless associations, which would result in a low negotiated data rate, do not provide a wireless client access to the network through the AP.
 - If the AP is 802.11b/g and the wireless clients which require WEP are 802.11b devices and not 802.11g, disable the AP from supporting data rates higher than 11 Mbps.
- Use a combination of VLANs, ACLs, and firewall rules to restrict wireless client access to wireless LANs. This adds multiple layers of security to the wired network to reduce the damaging consequences of a successful wireless breach.
- Use statically assigned wireless client IP addresses.
- Disable DNS.

How Do I Configure WEP Cloaking?

Follow these steps to configure WEP Cloaking:

1. Go to **Configuration > Operational Management > Sensor Operation**.
2. Select a network level. If you want to enable WEP Cloaking for all levels, select the appliance level.
3. Select **Enable** for the **WEP Cloak** feature.
4. Click **Apply**.

System automatically detects the APs to protect and starts WEP Cloaking.

Tracker Integration

AirDefense Tracker is used to track and locate unwanted APs on your wireless network. A Tracker Integration license allows you to automatically generate the tracker files used by AirDefense Tracker.

CHAPTER 4 WLAN MANAGEMENT

Introduction

WLAN Management gives you the tools to configure wireless infrastructure devices regardless of device type or vendor. WLAN Management simplifies the WLAN configuration process by providing the same configuration interface for all wireless infrastructure devices, eliminating the need to understand the individual syntax for multiple vendors / device types.

A WLAN Management license gives you access to:

- Perform Device Configuration
- Automate Configuration Audit & Correction
- Monitor Device Health
- Receive Infrastructure Faults
- Collect Network Traffic Statistics
- Visualizing Network Topology
- Maintaining Consistent Configuration
- Monitoring and Prioritizing Critical Events
- Reporting on Network Health and Utilization.

In the **Configuration** tab of the GUI, the following **Infrastructure Management** features/functions are activated (unlocked):

- Device Firmware
- Channel Settings
- Radio Settings
- WLAN Profiles
- CLI Configuration.

Also, in the **Configuration** tab of the GUI, the Pending State Audit and the Relay Server features are activated, and added to the **Operational Management** and **Appliance Platform** categories.

Infrastructure Management

Infrastructure Management is used to configure devices so that they can communicate on your network.

Device Firmware

Device Firmware configuration allows you to upload new AP or sensor firmware from a workstation to a network server. Once the firmware is uploaded, you can upgrade your APs and/or sensors using ADSP.

Uploaded firmware images are listed by device type, version number, and image file name.

Use the **Upload Firmware Image** button to upload firmware.

Channel Settings

Use Channel Settings to select power and channel settings for the B/N/G radio and the A/N radio. The settings are applied to APs and wireless switches.

By default, Channel Settings are enabled, and are set for maximum power and automatic channel selection. The configuration fields for each radio are:

Setting	Description
Power (dBm)	Enter the maximum power value (in dBm) that APs and wireless switches must have. Default setting is 20 dBm.
Channel Selection	Select one of three options: <ul style="list-style-type: none"> • Automatic—ADSP automatically sets which channel is used. • Manual—Select a channel to use from the dropdown menu and then select the extension range (none, upper, or lower). • Random—ADSP randomly sets the channel Default setting is automatic.

Radio Settings

Radio Settings allow you to specify the radio settings used in your network. Using ADSP, you specify the supported rates and other settings for each radio. If a radio in your network is detected operating outside the set specifications, ADSP issues an alarm.

The settings apply to APs and wireless switches. You may also define a radio as a sensor.

There are three possible radio configurations:

- B/G/N Radio
- A/N Radio
- 3rd Radio.

By default, Radio Settings are enabled, and all data rates are selected for both 2.4 and 5ghz radio settings. Use the individual radio tabs to configure each radio.

The configuration fields for each B/G/N Radio and the A/N Radio are:

Field	Description
Function	Defines the radio as a sensor or an infrastructure device (AP or wireless switch). You can also disable the radio.
Data Rates	Sets the data rates for the radios. You can set rates for 802.11 a/b/g as a group or 802.11 n.
DTIM Period	Specifies the supported Delivery Traffic Indication Message (DTIM) interval. The default value is 1.
RTS Threshold	Specifies the supported Request to Send (RTS) threshold. This can be a value between 0 and 2339 bytes. The default value is 2312.
Max Retries	Specifies the supported number of RTS retries. This can be a value between 1 and 128. The default value is 32.
Preamble	Specifies that the preamble is short or long.
Beacon Period	Specifies the supported beacon interval (period) in kilomicroseconds. The default value is 0.
Max Data Retries	Specifies how often to resend packets. This can be a value between 1 and 128. The default value is 32.
Fragmentation Threshold	Specifies the level that traffic fragments. This can be a value between 256 and 2346 bytes. The default is 2346.
Ethernet Encapsulation	Specifies that the ethernet encapsulation is 802.1h or RFC1042.

You may also specify the frame aggregation as A-MSDU, A-MPDU, or both.

WLAN Profiles

WLAN Profiles are used to configure the WLAN settings for devices utilizing your network. After creating a WLAN Profile using the **New Profile** button, it can be applied by selecting the profile and clicking the **Apply** button. When a WLAN Profile is applied to your system, if the WLAN thresholds for that profile are exceeded, a security alarm is generated. If there are no WLAN Profiles applied to your system, no alarms are generated. There are two tabs associated with WLAN Profiles: **General** and **Security**.

General Tab

The **General** tab is where you name your WLAN Profile and specify the general settings not related to security. Available fields are:

Field	Description
Name	Specifies the profile name.
Description	Allows you to specify a short description of the profile.
SSID	Specifies the Service Set Identifier (SSID) for devices.
Protocol	Specifies the protocol that the device can use [a, b, g, n (2.4 GHz), or n (5 GHz)].

Field	Description
VLAN	Specifies the Virtual Local Area Network (VLAN) the device is authorized to use.
Association Limit	Specifies the number of associations allowed per device.
Station Timeout	Specifies the number of seconds or minutes that a device has to become a sanctioned device.
Other Options	Specifies which of the following options may a device perform: <ul style="list-style-type: none"> • Respond to all probe requests • Broadcast SSID in Beacon • Wireless Client Isolation • Locally Bridged.

Security Tab

The **Security** tab is where you define the security aspects of your WLAN Profile. Available fields are:

Field	Description
Authentication	Specifies the type of authentication devices may use (Open , Shared , WPA , WPA PSK , WPA2 , WPA2 PSK , or Legacy EAP).
Encryption	Specifies the type of encryption devices may use (Static WEP , WEP64 , WEP128 , TKIP , CCMP , or Keyguard). You may select one or more encryption types.

Field	Description
PSK	Specifies a pre-shared key (PSK) / password used by devices. The PSK may be ASCII or HEX.
WEP Keys	Specifies the WEP keys used to connect to the network. The WEP key may be ASCII or HEX. You may also elect to transmit the WEP key.
RADIUS Servers	<p>NOTE This field is displayed only when the authentication method is WPA, WPA2, or Legacy EAP.</p> <p>Lists any RADIUS servers used in authentication. You can edit or delete a highlighted server by clicking the appropriate button.</p> <p>New servers may be added to the list by clicking the New Server button. You must supply the following information:</p> <ul style="list-style-type: none"> • A name for the RADIUS Server Profile. • The IP address or host name of the RADIUS server. • The RADIUS server port used for communications. • The shared password of the RADIUS server. Select the Display Passwords checkbox if you wish the password to be displayed while typing it. • A protocol selected from the drop-down menu (PAP, CHAP, MSCHAP, or MSCHAPv2). • A timeout value and a time interval selected from the drop-down menu (Seconds or Minutes). • The maximum number of retries to connect to the RADIUS server.

CLI Configuration

The Command Line Interface (CLI) for devices is a powerful tool that gives you direct access to access points and switches. The CLI commands can be used to configure and control how devices interface with your network.

AirDefense Services Platform uses the CLI to construct device profiles that can be used to control and manage devices in your network. You can push the CLI profiles out to devices in your network that ensure all devices in your network conform to your company policies.

AirDefense Services Platform creates and updates device configurations by revising the configuration files and their CLI command set. CLI profiles are created using configuration templates that you can use as is or change to meet the configuration requirements of your devices. Once a profile is created, you can apply it to any or all of the devices in your network. Devices are typically access points and switches. The following devices are currently supported:

- Brocade BR v5.x
- Brocade BR51X1
- Brocade BR71X1
- Brocade BRX000
- Cisco Airespace
- Cisco Autonomous 12x0/11x00

- Extreme Networks AP35X0
- Extreme Networks AP47X0
- Extreme Networks EX v5.x
- Extreme Networks WM2000
- Extreme Networks WM3X00
- Motorola AP51X1
- Motorola AP650
- Motorola AP7131
- Motorola AP7181
- Motorola CB3000
- Motorola RFSX000
- Motorola WiNG v5.x
- Motorola WS2000
- Motorola WS5100.

The screenshot shows the CLI Configuration interface for Motorola AP7131. The interface is divided into several sections:

- Left Panel:** A tree view showing the hierarchy of devices. The path is: ADSP > Unplaced Devices > US > Southeast > Alpharetta > Sanctuary Park > The Falls 1125 > AirDefense 2 (selected) > AirDefense 1.
- Top Right:** A dropdown menu set to 'Motorola AP7131' and a checkbox 'Only show device type in system'.
- Middle:** Radio buttons for 'Override settings' (selected) and 'Inherit settings from: ADSP'.
- New Template Section:** A table with columns 'Assignment' and 'Template Name'. Two entries are listed: 'AP7131 Adaptive' and 'AP7131 Standalone' (selected).
- Variables Section:** A table with columns 'Applied Scope', 'Variable Name', 'Variable Value', and 'Template'. It lists several variables for the 'AP7131 Adaptive' template.

Applied Scope	Variable Name	Variable Value	Template
ADSP	HOSTNAME		AP7131 Adaptive
ADSP	MASK		AP7131 Adaptive
ADSP	DNS2		AP7131 Adaptive
ADSP	DNS1		AP7131 Adaptive
ADSP	GATEWAY		AP7131 Adaptive
Unset Value	IP("1")		AP7131 Adaptive
Unset Value	IP("ixp0")		AP7131 Adaptive
Unset Value	DNS1("ixp0")		AP7131 Adaptive

Adding a New Profile

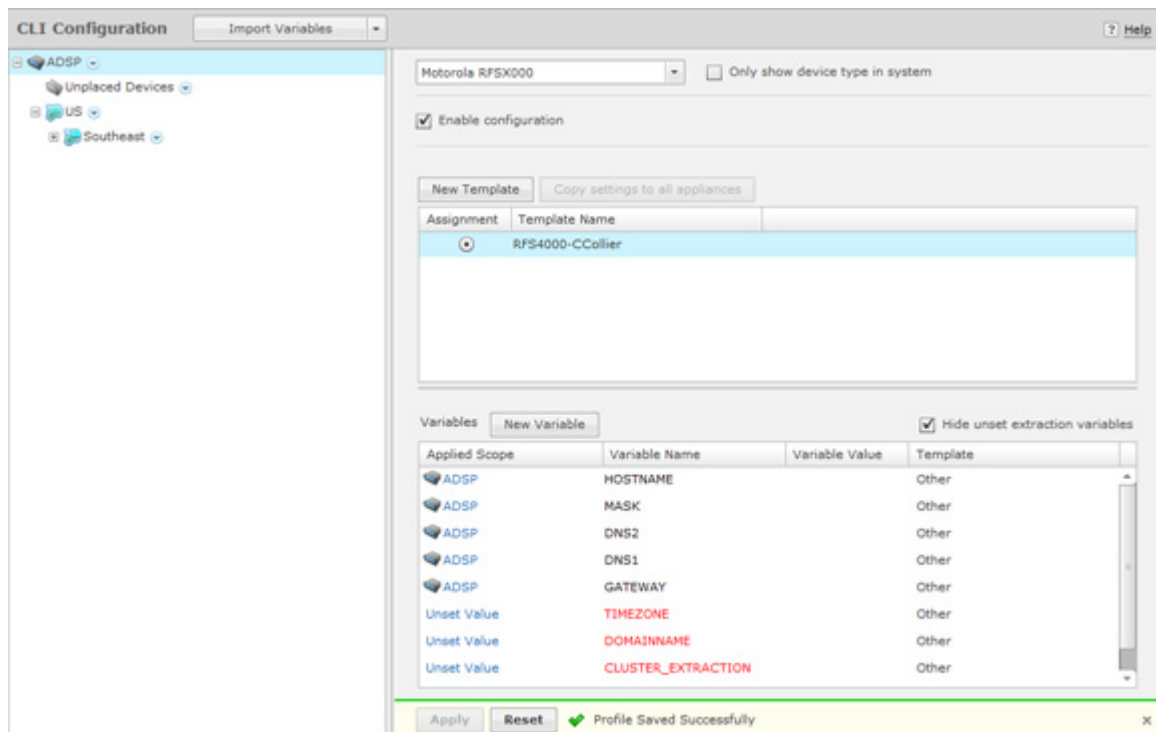
To create a new profile, select a device from the **CLI Configuration** dropdown menu and then click the **New Template** button. The following fields are available:

Field	Description
Name	This field is used to name your new profile.
Device Type	This field displays the device that was selected from the CLI Configuration dropdown menu. You cannot change the device once it has been chosen.
CLI Commands	Displays the CLI commands that are part of the selected template. These commands are editable. Be very careful when making changes. Only make changes to CLI commands if you have knowledge about the commands for the device associated with the template.

Applying CLI Profiles

After creating a CLI Profile, you must apply the profile to your network. Usually, you will have a CLI profile that can be used on a large majority of devices in your network. However, there will be times where you may need a special profile for a specific building or even a specific floor within a building.

If you have a CLI profile that works on a large majority of devices in your network, you should apply it at the appliance level. Then, if you have a special profile that fits the needs of a specific building or a specific floor in a building, you can override the appliance level profile and apply it to a lower network level.



To apply a CLI profile to a device type, select a device type from **CLI Configuration** dropdown menu.

If you want to apply the CLI profile to the appliance level, select the appliance level and then select the **Enable configuration** checkbox. Next, select the profile from the list of profiles. If there is only one profile, it is selected automatically. Click **Apply** to apply the selected profile to devices in the appliance level.

If you want to apply the CLI profile to a specific lower network level, select the lower network level and then select the **Override settings** radio button. Next, select the profile from the list of profiles. If there is only one profile, it is selected automatically. Click **Apply** to apply the selected profile to devices in the selected network level.

If you have a Central Management license and you want to use the same configuration on other ADSP appliances, you can copy configuration settings to all your managed appliances by clicking **Copy settings to all appliances**.

CLI Variables

Variables can be used in the CLI commands to get information (values) from other sources. They are global in nature and can be assigned to any network level. There are three types of variables: user-defined variables, extraction variables, and expansion variables.

User-defined variables are displayed in the **Variables** section. You can edit user-defined variables by selecting a network level from the tree and assigning values to one or more variables.

Use the **Variables** section to define configuration variances unique to the specific device parameters listed. For example, highlight the "Gateway" parameter and click under the **Device Value** column to display a field used to assign a unique Gateway address to this specific profile. Select and assign new default values as needed for each available profile.

New user-defined variables can be added to the **Variables** section by adding a variable in the CLI Commands section when creating a new profile or editing an existing profile. Use the following format:

```
$_[VARIABLE_NAME]
```

Once a variable is added to the CLI Commands section and the profile is saved, its name is displayed in the **Variables** section with an empty default value. Only the following characters are supported in user-defined variables:

A-Z, a-z, 0-9, and _

Below is a list of current extraction variables and the associated device types they are applicable for:

- IP(iface)— All
- MASK(iface)—5131, 7131, WS2K, CiscoThick
- MASK—5131, 7131, WS2K
- GATEWAY—All
- GATEWAY(iface)—5131, 7131, WS2K
- HOSTNAME—All
- DOMAINNAME—RFS*, WS5100, CiscoThick
- DOMAINNAME(iface)—5131, 7131, WS2K
- DNS1—5131, 7131, RFS*, WS2K, WS5100
- DNS1(iface)—5131, 7131, WS2K
- DNS2—5131, 7131, WS2K
- DNS2(iface)—5131, 7131, WS2K
- WINS(iface)—5131, 7131, WS2K

Expansion variables are used to include information from profiles that are configured in ADSP. An expansion variable will always end with `_EXPANSION`. For example, `$_[WLAN_RADIO_CHANNEL_EXPANSION]` is an

expansion variable that includes configuration information from WLAN Profiles, Radio Settings, and Channel Settings.

The Status column displays the status of the variable (inherited, overridden, or removed).

- **Inherited**—Variable is inherited from a higher network level. The inherited level is displayed in this field.
- **Overridden**—Variable is overridden at the current network level.
- **Removed**—Variable is not used at the current network level. Removed variables are displayed in red text.

Operational Management

Pending State Audit is added to Operational Management as part of the WLAN Management module.

Pending State Audit

Pending State Audit is used to identify any devices that are in a pending state. Devices in a pending state have been scheduled or need to be scheduled for configuration.

Folders with a checkmark identifies that folder as having devices that in a pending state. Devices with a checkmark identifies that device as a device that are in a pending state.

You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later using **Job Status** under **Device Monitoring**. A list of device types along with the number of affected devices that will be updated is displayed. Also, if applicable, a list of unsupported settings is displayed.

Appliance Platform

Relay Server is added to Appliance Platform as part of the WLAN Management module.

Relay Server

Define or update the Relay Servers used to access managed devices. Relay Servers are FTP/TFTP servers that devices access to fetch configuration, firmware, and provisioning information. Use the Relay Server to set the configurations of both the Device Relay and Appliance Relay Servers.

✓ **NOTE** You can use your appliance as the relay server. To do so, select the **Internal Relay Server** option.

Set the following values for **Device Relay Server (download)**:

- Enter the **Host** name of the relay server ADSP uses to access and fetch device configurations. Normally, this is the IP address of the relay server. This can be an internal relay server (your appliance) or an external relay server.
- Select a protocol from the drop-down menu (**FTP**, **TFTP**, **SFTP**, **SCP**, **HTTP**, or **HTTPS**). If you are using your appliance as the relay server, you can only use **FTP** or **SFTP**.
- Specify the **Path** ADSP uses to download information. You should either leave the path blank or use root (/). Use **/pub** if you are using your appliance as a relay server.

- Define the **Port** ADSP uses to connect to the Device Relay Server. If you are using your appliance as the relay server, use port 21 when **FTP** is the selected protocol or port 22 when **SFTP** is the selected protocol.
- Enter the **Username** needed to update the Device Relay Server used by ADSP.
- Enter the **Password** required to update the Device Relay Server used by ADSP.

If different than the Device Relay, set the following values for **Appliance Relay Server (upload)**:

- ✓ **NOTE** Use the **Same as Device Relay Server** option if the Relay Server connection address and login credentials will always be the same for both the ADSP appliance and the device. The option to unsynchronized these configuration fields will only be needed in cases where the address of the Relay Server will depend upon whether it is being accessed by the device or the ADSP appliance. This type scenario will be encountered in network deployments where NAT'ing is utilized in such a way that the relay server address will depend upon where the accessing device is located on the network.
- Enter the **Host** name of the relay server ADSP uses to access and fetch device configurations. Normally, this is the IP address of the relay server. This can be an internal relay server (your appliance) or an external relay server.
 - Select a protocol from the drop-down menu (**FTP**, **TFTP**, **SFTP**, **SCP**, **HTTP**, or **HTTPS**). If you are using your appliance as the relay server, you can only use **FTP** or **SFTP**.
 - Specify the **Path** ADSP uses to upload information. You should either leave the path blank or use root (/). Use **/pub** if using your appliance as a relay server.
 - Define the **Port** ADSP uses to connect to the Appliance Relay Server. If you are using your appliance as the relay server, use port 21 when **FTP** is the selected protocol or port 22 when **SFTP** is the selected protocol.
 - Enter the **Username** needed to update the Appliance Relay Server used by ADSP.
 - Enter the **Password** required to update the Appliance Relay Server used by ADSP.

Import Relay Server Information

You can import relay server information using the **Import Parameters** button. Comma delimited files are used to import relay server information. The format of the file is:

```
relay_params,server,folderpath,deviceHost,deviceProtocol,devicePath,devicePort,deviceUsername,
devicePassword,applianceHost,applianceProtocol,appliancePath,appliancePort,applianceUsername,
appliancePassword
```

- ✓ **NOTE** Although the above format is shown on multiple lines, each import entry must be one line with no line breaks or carriage returns.

There are different ways to create a comma delimited file but the most trouble-free way is to use a text editor, such as Notepad.

Things to Remember:

- The first field for importing relay server information must be *relay_params*.
- At this time, the only valid server name is *localhost*.
- Servers must be specified in pairs. You must specify a Device Relay Server and an Appliance Relay Server in one entry.

- If the server information is the same, you still must enter information for both servers. Also, if the information for both relay servers match, the **Same as Device Relay Server** checkbox is selected in the GUI after the import.
- Normally, you will supply a username and password. However, when using the TFTP protocol, the username and password fields can be left blank with no blank space between the commas (i.e., ,).
- *deviceHost* designates the IP address of the host.
- *deviceProtocol* designates the protocol to use for communications. Valid protocols are FTP, TFTP, SFTP, SCP, HTTP, or HTTPS. These are the same protocols listed in the Protocol drop-down menu of the GUI.
- *folderpath* designates the network level path and must include a slash (/) at the beginning of the path and between network levels. Also, the path must already be present in the existing network tree. To specify an appliance level, just enter the appliance name.
- *devicePath* and *appliancePath* designate the path where the configuration file is located on the individual servers.
- *devicePort* and *appliancePort* designate the port to use for communications.

Examples:

```
relay_params,localhost,/ADSP,172.17.0.80,ftp,/,21,anonymous,anonymous,172.17.0.80,ftp,/,21,anonymous,anonymous
```

```
relay_params,localhost,/US/Southeast/AirDefense,172.17.0.80,ftp,/,21,anonymous,anonymous,172.17.0.80,ftp,/,21,anonymous,anonymous
```

```
relay_params,localhost,/relay_test,172.17.0.80,tftp,/,69,,,172.17.0.85,ftp,/,21,anonymous,anonymous
```

If you have a Central Management license, you can copy the Relay Server configuration to all your appliances.

CHAPTER 5 TROUBLESHOOTING

Introduction

This chapter discusses the modules and solutions (packages) available through ADSP that assists you in troubleshooting your network. The individual modules are:

- AP Test
- Connection Troubleshooting
- Live RF
- Spectrum Analysis.

The available solutions (packages) are:

- Advanced Forensics
- Advanced Troubleshooting
- Assurance Suite (Network Assurance).

AP Test


AP Testing tracks network failures from an automated or manual AP connectivity test. Alarms are generated to indicate a failure of one of the test conditions in the test profile and should be considered a high priority event as it may be preventing the wireless applications from operating properly.

AP Testing is a tool that performs remote end to end network testing from a wireless perspective. The test is accomplished by using the deployed sensors as a wireless client to connect to an AP and validate the appropriate resources 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.

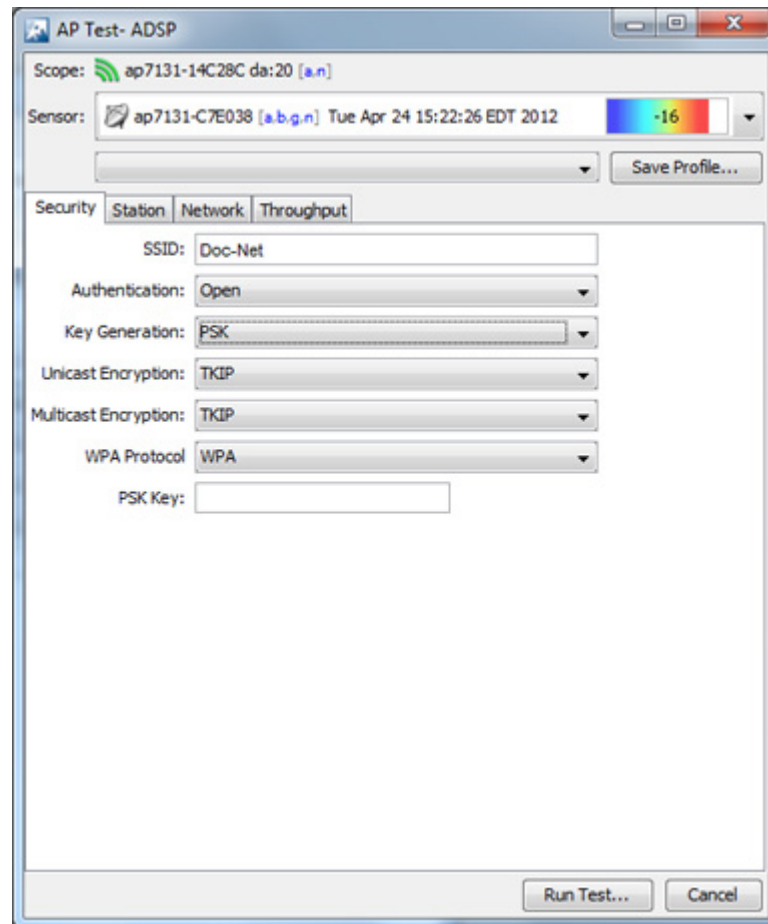


NOTE For ADSP 8.1.3, AP Testing is only supported on the M510 and M520 Sensors with firmware version 5.3 or higher installed. AP Testing is also supported on the AP650 and AP-7131 Sensors with WiNG 5.1 or higher installed.

On-Demand AP Test

On-demand AP Tests are run directly from the AirDefense Services Platform GUI using the **AP Test** window. To initiate an on-demand test, click the dropdown menu button——for a BSS or network level, and select AP Test.

✓ **NOTE** When the scope is a network level, all APs in the scope are tested.

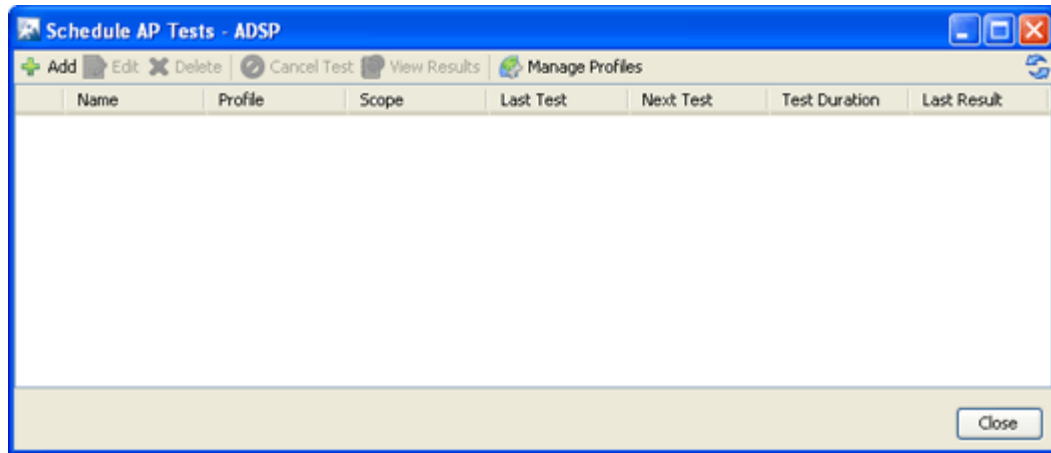


The **AP Test** window allows you to configure and run the AP Test with the click of a button. You must configure AP Test using the **Security**, **Station**, **Network**, and **Throughput** folders. After you have configured an AP Test, you can save it as a profile. A profile can be selected later to run test on a similar access point.

See the ADSP Help for details on how to set up and run AP Tests on demand.

Automated (Scheduled) AP Test

Automated AP Tests must be scheduled using the **Schedule AP Tests** window accessed via **Menu > Scheduled AP Test**.



The **Schedule AP Tests** window displays a list of all scheduled AP Tests. From the **Schedule AP Tests** window you can:

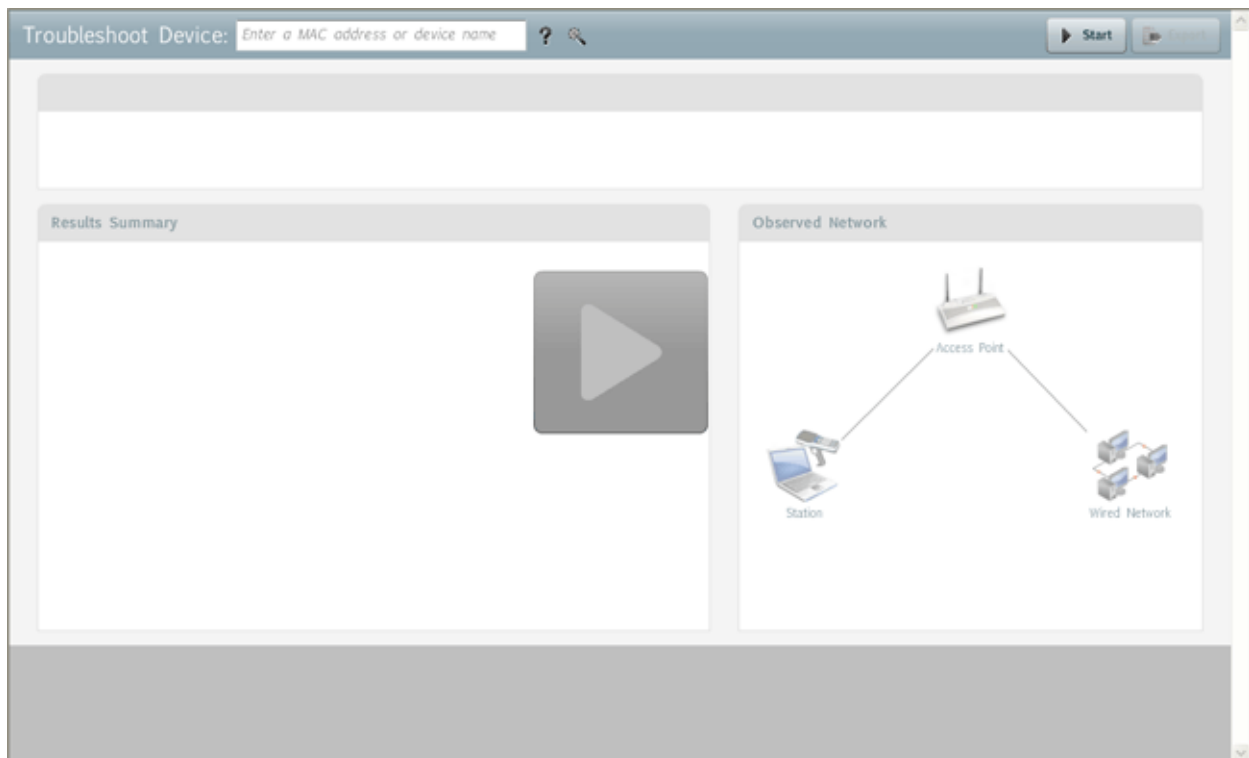
- Add, edit, delete, and cancel tests
- View detail test results
- Manage the profiles that are used to run tests on similar access points.

See the AirDefense Services Platform Online Help for details on how to schedule AP Tests and use the **Schedule AP Tests** window.

Connection Troubleshooting

Connection Troubleshooting provides a web application that allows you to troubleshoot a Wireless Client's ability to connect to your wireless network. Using a Wireless Client's MAC address or device name, the Troubleshooting tool can run tests to determine the status of a Wireless Client within your wireless network and display results summarizing the status.

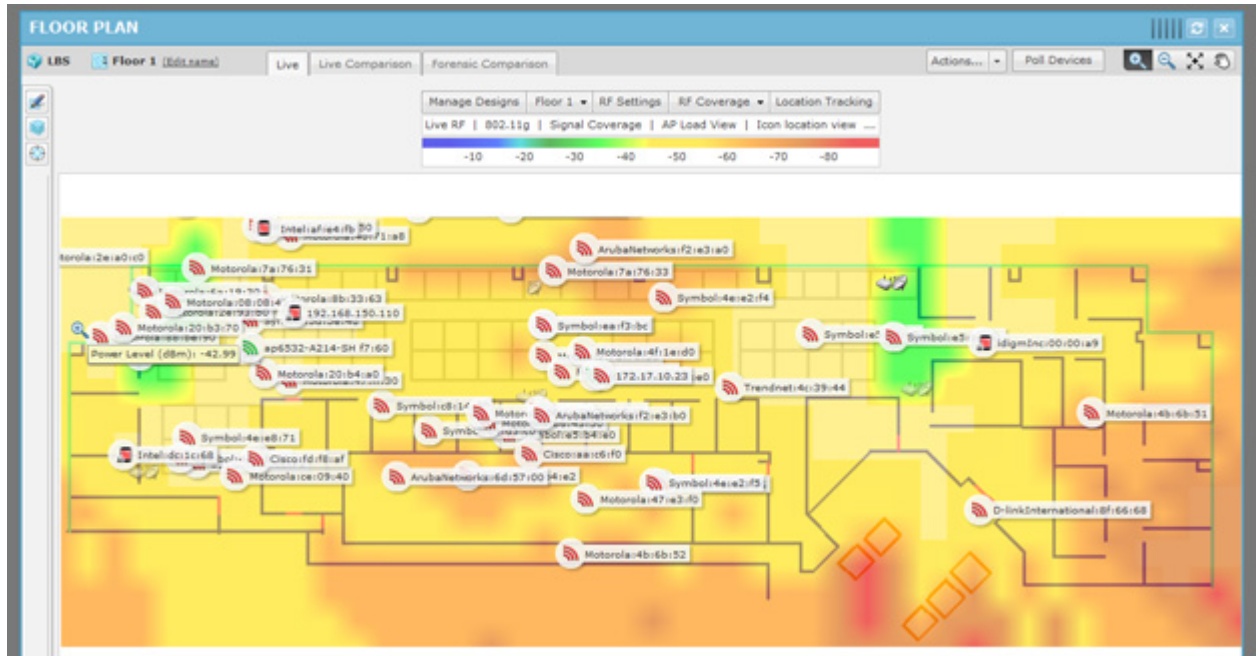
The Troubleshooting tool is accessed through the ADSP GUI.



ADSP Help is provided that fully explains how to use the Connection Troubleshooting tool.

Live RF

Live RF displays a heat map that represents signal coverage for APs placed on a floor plan. When the Floor Plan is accessed, if devices are in place, Live RF starts and a heat map is displayed.



Live RF data is available on all Floor Plan pages. When the Floor Plan is refresh (manually or automatically), RF data is updated using the latest data (radio, power, channel, live status, etc.) about the devices. This data comes from the last polling cycle for the devices. If the **Poll Devices** button is clicked, the devices are refreshed first by ADSP and then the RF data is updated and displayed in the Floor Plan.

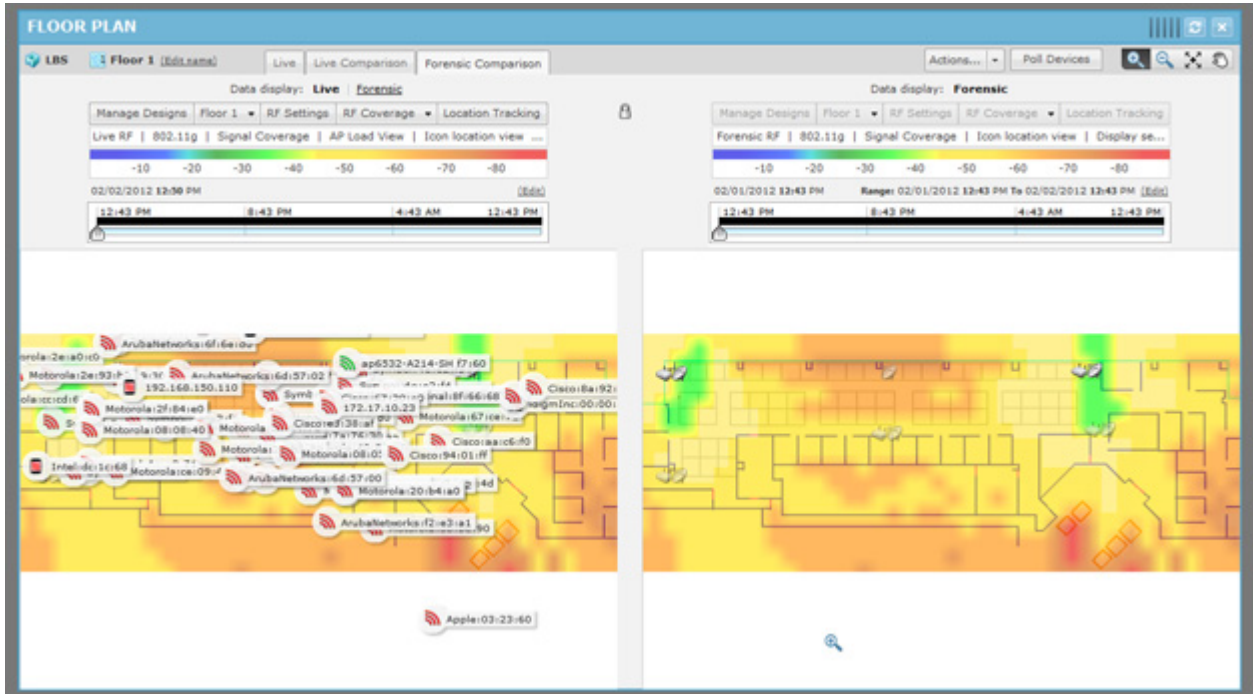
The heat map can be filtered according to:

- Visualization/Application—Uses the visualizations and applications that configured in **Configuration > Network Assurance > LiveRF Settings**.
- Protocol—Uses one of the available protocols (802.11a, 802.11b, 802.11g, and 802.11n).
- Devices—Filters RF data by a single device, a group of devices determined by SSID, or all devices.

ADSP Help is provided that fully explains how to use Live RF.

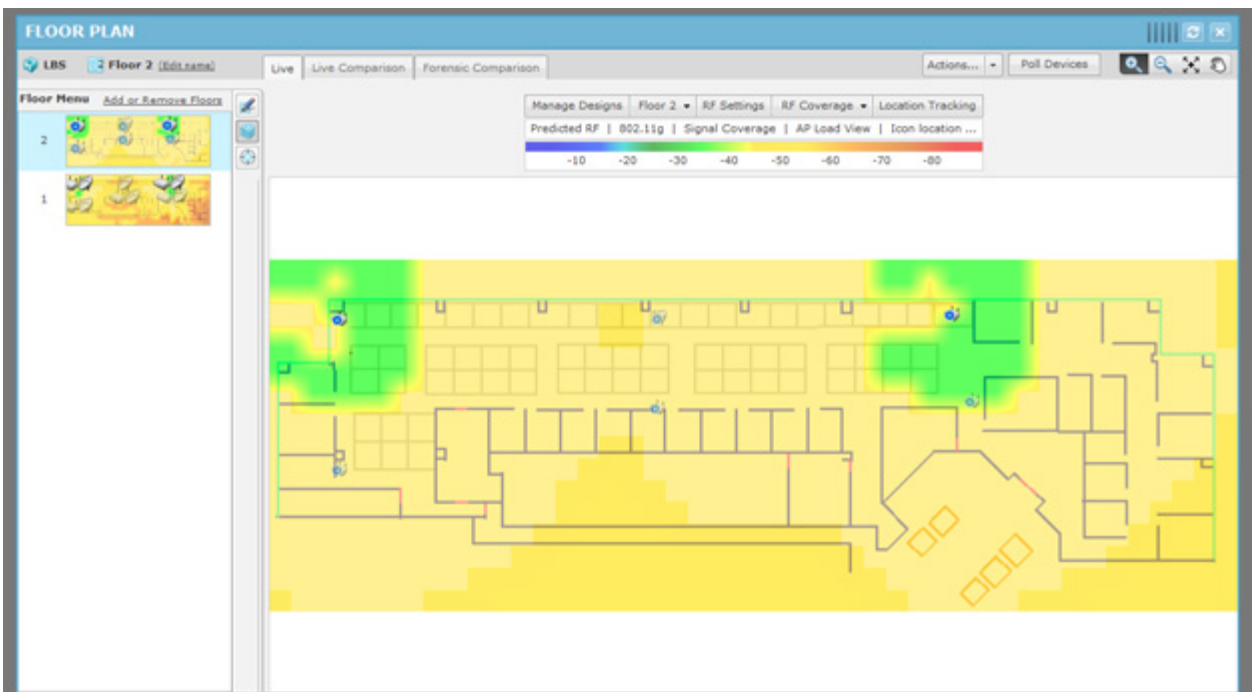
Forensic RF

The Forensic RF feature, include with a Live RF license, visualizes forensic data to display coverage over a specific time range.



Predictive RF

The Predictive RF feature, included with a Live RF license, allows you to place planned devices in your floor plan that ADSP uses to predict RF behavior. This allows you to view heat maps of devices before you purchase them, allowing you to plan additions/changes to your network.



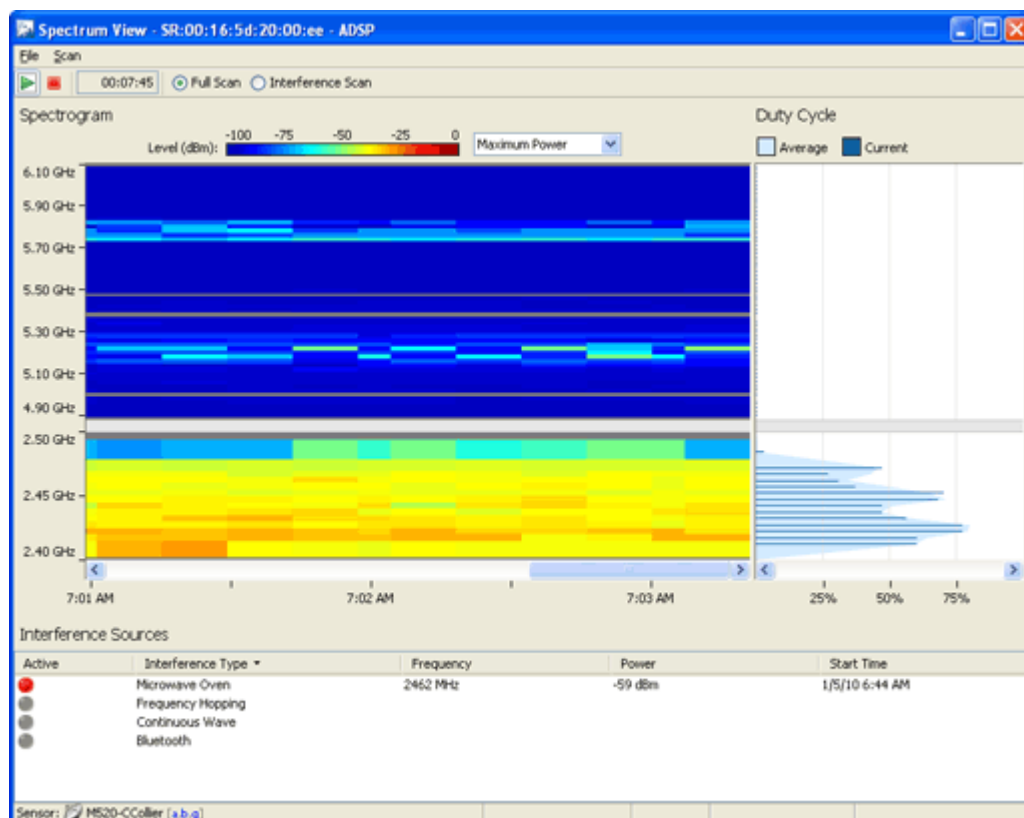
There must be enough unassigned LiveRF licenses to cover the number of planned devices in the floor plan.

Spectrum Analysis

The Spectrum Analysis module gives you a tool to identify and locate interference sources on your wireless network. The analysis is conducted using only ADSP software; no extra hardware is required.

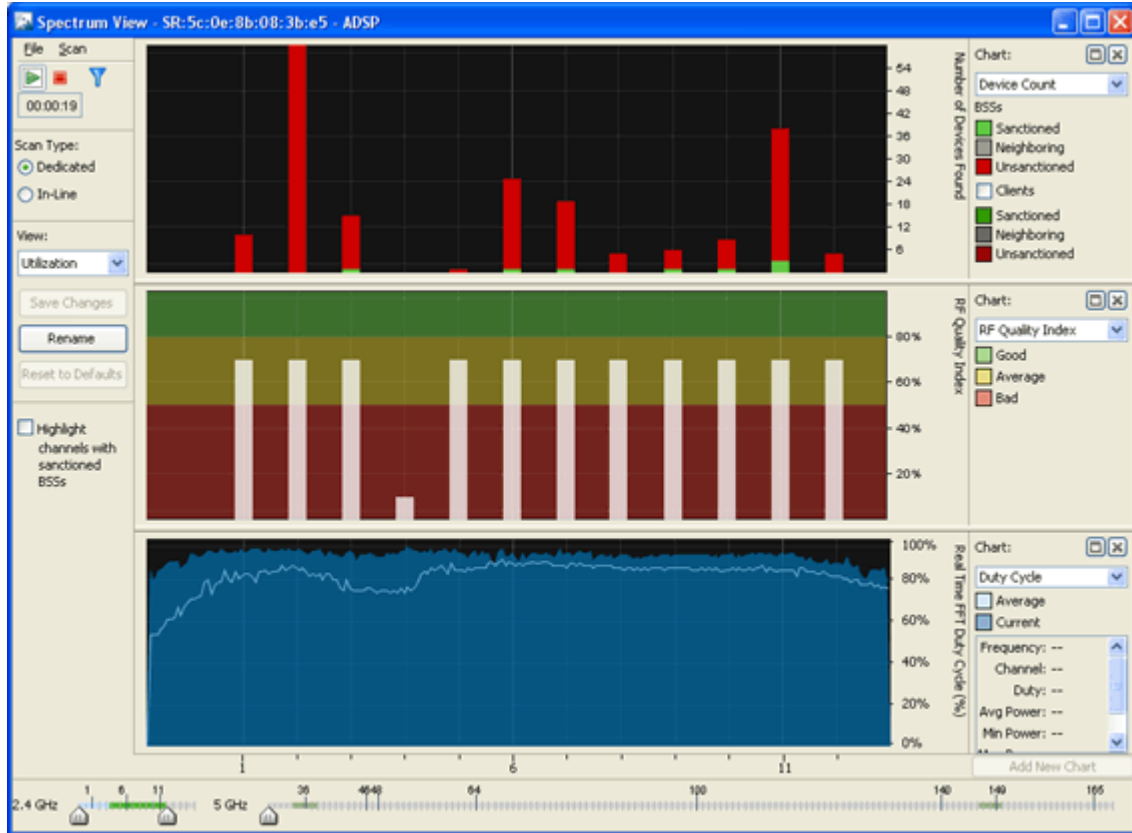
You must possess a valid Spectrum Analysis license from Motorola Solutions for each sensor that you wish to conduct an analysis from. Spectrum Analysis supports two modes of operation:

- Background Scanning
 - Part-time scanning of power spectral density (Layer 1), while sensor continues to scan for WIPS (Layer 2).
 - Generate 'RF Spectrum Analysis' alerts (BlueTooth, Microwave, Frequency Hopper, Continuous Wave)
- Dedicated Spectrum View
 - Sensor temporarily dedicated to Spectrum Analysis
 - While in Spectrum View the sensor provides no protocol analysis (after user-configured time period, sensor defaults back to WIPS)
 - Scanning options:
 - Full Scan Mode - scan full 2.4-2.5 GHz and 4.9-6.1 GHz spectrum to identify presence of interference (scan more channels, spend less time on each channel)
 - Interference Scan Mode - scan specific bands to classify type of interference source (scan fewer channels, spend more time on each channel)



Advanced Spectrum Analysis

Advanced Spectrum Analysis is Motorola AirDefense's next generation of Spectrum Analysis. Advanced Spectrum Analysis will only run on devices with the MB92 or newer chipsets. At this time, only the Motorola AP6511, AP621, and AP6521 are able to run this enhanced version of Spectrum Analysis.



Advanced Spectrum Analysis has four customizable views; each with its own set of default charts:

- Utilization—Displays charts showing how your network is being utilized. The default charts are:
 - Device Count
 - RF Quality Index
 - Duty Cycle.
- Physical Layer—Displays charts that highlight the physical layer of your network. The default charts are:
 - Spectrogram
 - Duty Cycle.
- Interference—Displays charts showing interference sources in your network. The default charts are:
 - Interference
 - Spectral Density.
- Spectrum Detail—Displays charts showing the spectrum details of your network. The default charts are:
 - Spectrogram
 - Real Time FFT (Fast Fourier Transform)
 - Spectral Density.

Advanced Troubleshooting

An Advanced Troubleshooting license gives you access to two modules: AP Test and Connection Troubleshooting. As discussed earlier in this chapter, AP Test provides a way to remotely test connectivity to access points while Connection Troubleshooting allows you to remotely troubleshoot stations. You can obtain a separate license for each module, or you can obtain an Advanced Troubleshooting license and get both modules.

Assurance Suite (Network Assurance)

ADSP has a Assurance Suite (Network Assurance) solution that includes several modules that assists you in:

- Improving your wireless network availability while reducing network downtime.
- Reducing expenses associated with wireless network performance and maintenance.
- Resolving problems via remote management.

With a Assurance Suite (Network Assurance) license, you receive the following modules:

- Advanced Troubleshooting which includes AP Test and Connection Troubleshooting
- Advanced Forensics discussed in *Chapter 3, Security*
- Live RF
- Spectrum Analysis.

You get all of these modules in one package without having to obtain an individual license for each module.

Radio Share Network Assurance

ADSP has a Network Assurance solution that goes hand-in-hand with Sensor or AP radio sharing. With a Radio Share Network Assurance license, you receive the following modules:

- Radio Share Access Point Testing
- Radio Share Advanced Forensics
- Radio Share Client Connectivity Troubleshooting
- Radio Share Spectrum Analysis.

CHAPTER 6 LOCATION BASED SERVICES

Introduction

Location Based Services is a feature of Proximity and Analytics and gives you an easy method to customize the frequency (and subsequent methodology) in which the location of various types of devices is scanned and calculated. For example, it may be desirable to continually track high priority client devices in a short frequency such as seconds, but there may be no need for such continual tracking of infrastructure APs.

Location Based Services utilizes the concept of Device Type, which is an extension of the existing Client Type concept. As devices are assigned a Device Type, ADSP then knows how to track the device in terms of its location going forward due to the assigned LBS (Location Based Services) Profile.

LBS Profiles

LBS Profiles are created in [Configuration > Operational Management > Location Based Services](#). Profile information includes the following information:

Field	Description
Profile Name	Specifies the configuration profile name.
Device Type Assignment	Sets the valid device types for you system. Options must be specified for each device type. Devices types are: <ul style="list-style-type: none">• Default Type• Employee Device• Employee Laptop• Employee Phone• High Priority Visitor Device• Laptop• Low Priority Visitor Device• MCD• Visitor Device• VoIP Phone.
Location Refresh Rate	Sets the rate at which the device type is to have its location updated by ADSP.

Field	Description
Device Age Out	Sets the time span that a device's location is considered valid. The specified time span must be greater than the Location Refresh Rate. Valid entries are 1 - 48 hours, 1 - 120 minutes, or 2 - 120 seconds.
Location Confidence Threshold	Sets the confidence level for seeing a tracked device in your network.
Filter by Network Association	Indicates whether you want to track all devices or only track network devices.
Virtual Region Event Trigger	Identifies which of the available virtual region events the given device can trigger: Enter , Exit , Proximity , and/or Contained .
Presence Base Event	Identifies which of the available presence based events the given device can trigger: On Detect and/or On Exit . Also includes a threshold for RSSI which the device would have to exceed before triggering the presence event. A repeat option is provided which allows you to repeat this event every minute, hour, or day.

In order to use Location Based Services to pinpoint a device location, a Sensor survey must be done using Motorola AirDefense Mobile 6.2 or higher. AirDefense Mobile takes information from ADSP and uses it during the survey. After the survey is complete, information is exported back to ADSP that is vital in the accuracy of location tracking.

Reference Material

A good source for information is the *Location Based Services Best Practice* document. It explains how to set up and use Location Based Services and how AirDefense Mobile 6.2 is used to conduct Sensor surveys. To obtain a copy of the *Location Based Services Best Practice* document, go to the Motorola Solutions support website for product manuals (<http://supportcentral.motorola.com/support/product/manuals.do>).

CHAPTER 7 CENTRAL MANAGEMENT

Introduction

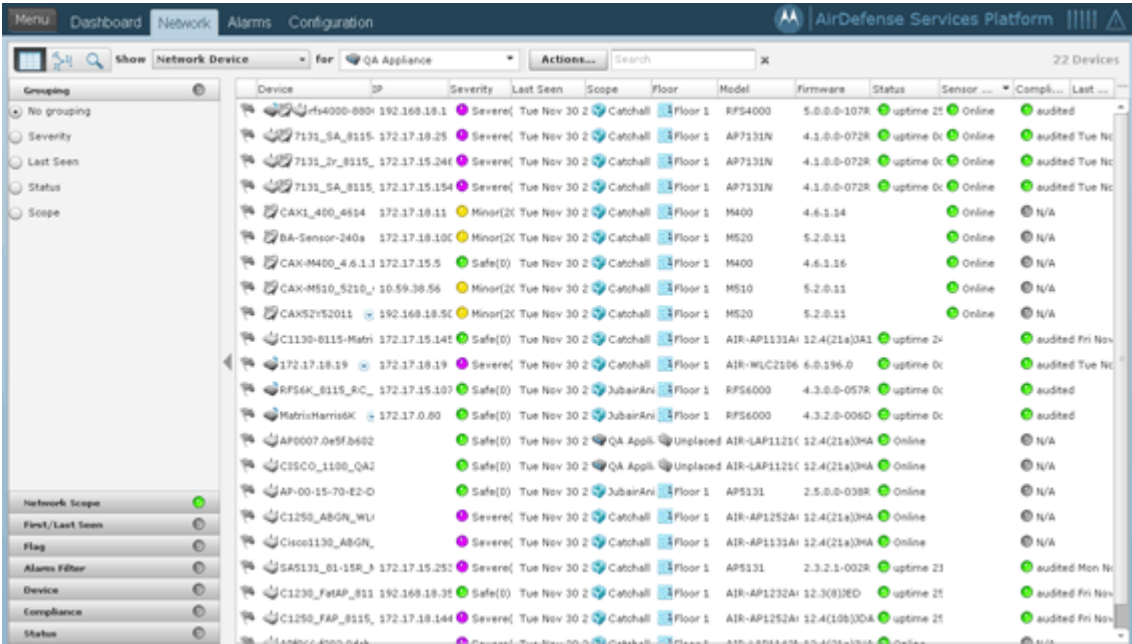
Central Management is a centralized management system that allows an administrator to administer multiple ADSP appliances from one location. Central Management can be used to ensure that configurations are the same across multiple appliances. Administrators no longer have to configure their appliances separately.

Once a Central Management license is installed, you must add the other appliances by navigating to **Menu > Add Devices**. Select **Appliance** as your device type.

When you add an appliance, here are some things to remember:

- The user accounts must exist on both appliances (master and slave) with the same username and password.
- The GUI software version of the appliances must be the same.
- You can only use the licenses installed on the master appliance. For example, you must have a Spectrum Analysis license on the master appliance to use it on the slave appliance.

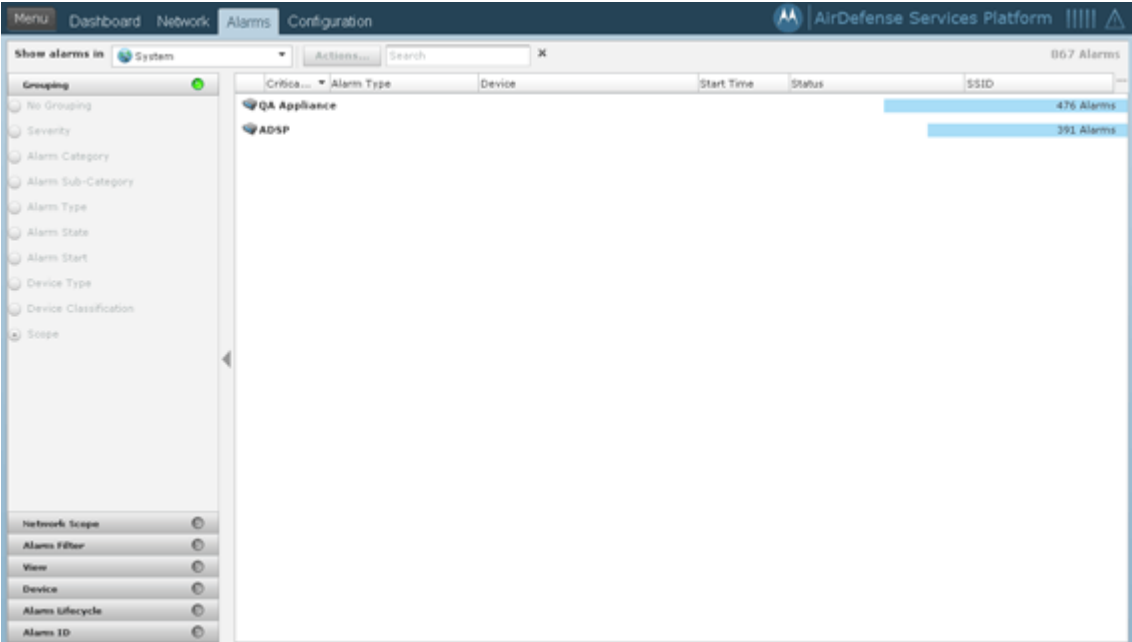
If displaying devices on an appliance level or a network level, only the devices for that appliance or network level are shown.



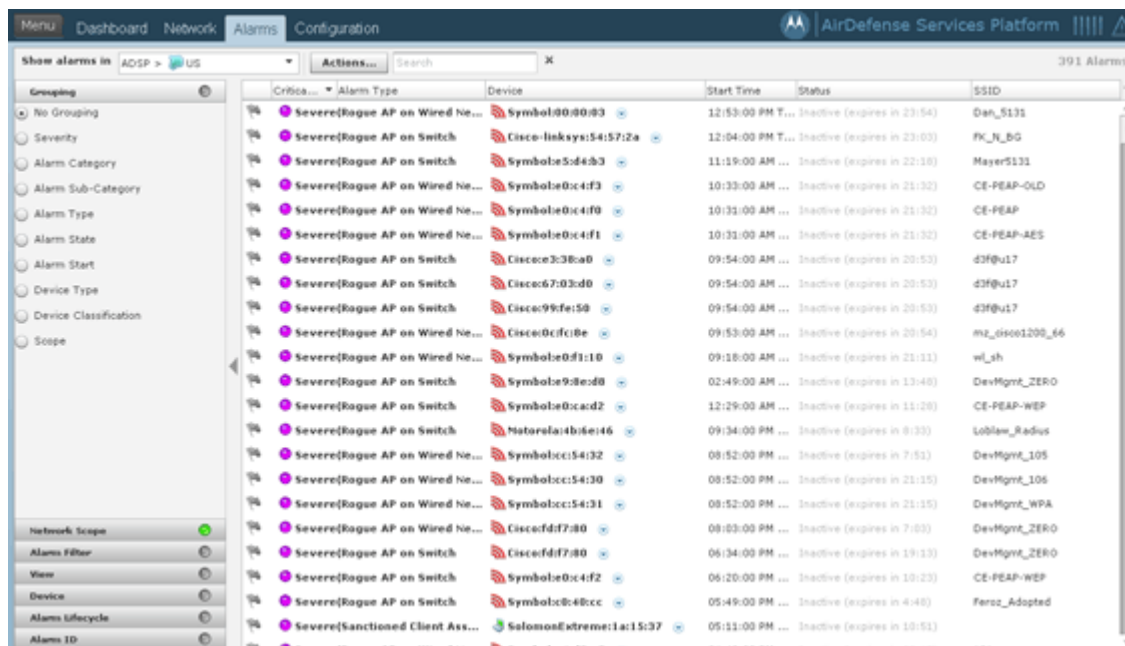
All other functions in the Network tab work the same.

Effects on the Alarms Tab

A Central Management license allows you to display alarms generated on any managed appliance in the Alarms tab. If displaying alarms on a system level, on the alarm totals for the appliances are shown.



If displaying alarms on an appliance level or a network level, only the alarms generated by that appliance or network level are shown.



All other functions in the **Alarms** tab work the same.

Effects on the Configuration Tab

With a Central Management license, you can create configuration profiles that can be applied to all your managed appliances. Once a profile has been created, you can synchronize the appliances so that they are the same using the **Check Synchronization** button. You can also copy settings from one appliance to all the other appliances using the **Copy settings to all appliances** button.

An example of using **Check Synchronization** is to synchronize user accounts. This checks all the accounts on all your managed appliances and lists the differences. You then have the option of synchronizing selected appliances or synchronizing all appliances.

To copy settings to all appliances, when you access a feature that has the button and you want to copy the settings, just click the **Copy settings to all appliances** button.

All other functions in the **Configuration** tab work the same.

CHAPTER 8 ZERO TOUCH WLAN INFRASTRUCTURE DEPLOYMENT

Introduction

Zero touch configuration enables taking Motorola wireless LAN infrastructure products directly out of the box and simply plugging it into the network for operational use. By coordination with the management platform, the infrastructure is able to automatically receive the configuration needed to allow it to be used for operational needs. This process eliminates the need for any manual configuration or staging greatly simplifying deployments of WLAN infrastructure for client access and sensors. Zero touch works through a simple 3 step process.

1. Infrastructure boots and sends a trap to ADSP to notify it's a new device on the network.
2. ADSP receives the trap, recognizing it is from an unknown device will perform a single device discovery to import the newly added device into the management platform.
3. Once placed in the tree hierarchy appropriately the system will automatically push a configuration template to the device setting the appropriate configuration for this device. The device is now fully up and operational without any manual staging or configuration.

Deployment Requirements

The following deployment requirements must be met:

- ADSP 8.1.2 or newer
 - WLAN infrastructure management licenses are required to enable this feature
- Motorola WLAN infrastructure running WiNG 5.1 or newer
- Network with DHCP enabled
- DNS entry for the host *AirDefense1* in the domain of the DHCP scope the WLAN device will be initially attached to
 - This solution does support DNS devolution

- Network which is able to route traffic and permit the following flows:
 - SNMP traps (UDP port 162) traffic from the infrastructure to the ADSP appliance
 - SNMP query traffic (UDP port 161) between ADSP and the infrastructure
 - SSH application traffic between the ADSP appliance and the infrastructure
 - SFTP or FTP traffic between the device and the Relay server (can be same system as the ADSP appliance)
 - SFTP or FTP traffic between ADSP and the external relay server when one is used.

Setup Prerequisites

1. Enable SNMP Trap reception on the ADSP appliance:
 - a. From the ADSPadmin utility on the appliance console, select **C** for Config then **SNMP** for Enable/Disable SNMP trap reception.
 - b. Select **E** for enable and save changes as shown below.

```
SNMP currently disabled

      (E) Enable SNMP

(Q) to quit (return to previous menu)  ->

Save the SNMP state as shown above? (yes/no): yes

iptables: Flushing firewall rules:          [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Uploading modules:                [ OK ]
iptables: Applying firewall rules:          [ OK ]
iptables: Loading additional modules: ip_conntrack_tftp [ OK ]

(Press <CR> to return to previous menu)
```

2. Verify Discovery SNMP Parameters:
 - a. In the appliance GUI, go to **Configuration > Appliance Platform > Communication Settings**.
 - b. Click on the **Unplaced Devices** folder.

✓ **NOTE** When performing a discovery based on receiving a SNMP trap from a device, the system will use credentials based on the profile(s) set on the **Unplaced Devices** folder. The **Unplaced Devices** folder must have the default credentials for the device being deployed for the discovery to work successfully.
 - c. Uncheck default profiles for device types which will not be placed on your network.

For example, for deployments of just WiNG 5.1 devices, you would uncheck all default profiles but the Motorola WiNG 5.x Default.

If more than one device type is being deployed, setting the unplaced device folder to inherit rather than override is sufficient.
3. Verify Device Communication Settings:
 - a. In the appliance GUI, go to **Configuration > Appliance Platform > Communication Settings**.
 - b. Click on the top level of the tree to show currently applied profiles.
 - c. Uncheck default profiles for device types which will not be placed on your network.

For example, for deployments of just WiNG 5.1 devices, you would uncheck all default profiles but the Motorola WiNG 5.x Default.

- ✓ **NOTE** Leaving all profiles checked will not prevent the zero touch feature from working but it will slow down the process.

WHAT IS NEEDED?

- d. Add a new profile which uses the non default production credentials that the infrastructure will have after completion of the zero touch configuration.

Communication Settings Profile

Profile Name:

SNMP Console HTTP

Enable Console settings

User:

Password: Display Passwords

Enable Password:

Protocol:

Port:

Save Cancel

Once complete, profile assignment should look like below:

New Profile... Copy... Edit... Delete Check Synchronization	
Assigned	Profile
<input type="checkbox"/>	Cisco Default
<input type="checkbox"/>	Cisco Thin Default
<input type="checkbox"/>	Motorola AP Default
<input type="checkbox"/>	Motorola Switch Default
<input checked="" type="checkbox"/>	Motorola WiNG 5.x Default
<input checked="" type="checkbox"/>	Production
<input type="checkbox"/>	Unplaced Devices

4. Setup network device configuration action:
 - a. The system must be enabled to allow configuration push to the new infrastructure devices. To set this up, go to **Configuration > Appliance Platform > Polling**.
 - b. Enable the following settings:
 - Automatically Correct Configuration Compliance Violations
 - Device Configuration Management
 - Template Based Configuration Management

Copy settings to all appliances

Enable automatic status polling
Frequency: 8 Hours

Enable automatic data collection
Frequency: 20 Hours

Automatically correct configuration compliance violations

Enable ACL

Enable port suppression

Enable background switch port scanning

Enable Device Configuration Management

Audit Only

Template Based Configuration Management

5. Set up Relay Server:
 - a. Configure the relay server for use with configuration management. The relay server setup is not specific to the zero touch feature, instructions for setup can be found in **Menu > Help > Search for Relay**
6. Configure non default device credentials:
 - a. Some infrastructure devices require changing the administrator password at first login. The ADSP system must be setup with the credentials to use for configuring the device. The credentials can be set by going to **Configuration > Infrastructure Management > Device Access**.
 - b. Enable configuration.

- c. Add an **admin** user with password. Make sure this password is different than the default since most devices will reject resetting the password to the default value.

Enable configuration **Copy settings to all appliances**

Passwords Interfaces

Encrypt Passwords and Keys on Flash

Enable Password: Display Passwords

Add **Delete**

Username	Password
admin	*****

- ✓ **NOTE** For devices which require password change at first login, this is the password the system shall use when rotating the password. Also, it should match the console and the http password for the “production” communication profile.

- d. Specify the interfaces to be used. If using SNMP access, specify read and write community passwords.

Enable configuration **Copy settings to all appliances**

Passwords Interfaces

Telnet access enabled

SSH access enabled

HTTP access enabled

HTTPS access enabled

SNMP access enabled

Read Community: ***** Display Passwords

Write Community: *****

Trap Community:

Trap Destination:

- e. Click **Apply** to save changes.

7. Set up CLI configuration push:

- a. Set up a CLI template to push the configuration to the device. This template can include just a few lines of code to set the device as a sensor or can include a complete configuration to set and configure all parameters on the device. To create a configuration template, go to **Configuration > Infrastructure Management > CLI Configuration** and select the specific device type of interest.

- b. CLI expansions can also be used but the corresponding profiles (WLAN, Radio, Channel, Device Access, RF Domain, ...) need to be configured as well.

- ✓ **NOTE** Make sure that the configuration template and related profiles (WLAN, Radio, Channel, Device Access, RF Domain, ...) are well tested and validated prior to using them in zero config. A poorly written CLI template has the potential to isolate the device from the network.
- ✓ **NOTE** After initial discovery, the process to fully import the device and place it in a compliant state may take up to 2 data collection cycles.

CHAPTER 9 ADSPADMIN

Introduction

You use the **ADSPadmin** utilities in the Command Line Interface to perform the initial AirDefense Services Platform configurations, then use the GUI for ongoing configuration. The functions provided in ADSPadmin are:

- Manage
- Dbase
- Software
- Config.

Using ADSPadmin to Configure AirDefense Services Platform

Config

The **ADSPadmin Config** program area provides the following utilities for configuring ADSP:

- IP—use this to change the IP address, subnet mask, and default gateway of the ADSP appliance.
- IPv6—use this to change the IPv6 address of the ADSP appliance.
- NETPORT—use this to change network interface settings, and to toggle Autonegotiation on and off.
- DNS—use this to add or delete a DNS nameserver (Domain Name Server).
- BONDING—use this to enable the High Availability Ethernet.
- HNAME—use this to change the name of the ADSP appliance.
- DNAME—use this to change the domain domain to which the ADSP appliance belongs.
- TIME—use this to configure the AirDefense appliance's operating time and date.
- TZ—use this to configure the time zone in which the ADSP appliance operates.
- NTP—use this to configure a specific network time server, instead of setting TIME and TZ.

- SNMPA—use this to enable or disable reception SNMP agent requests.
- SNMPC—use this to configure SNMP agent community string.
- SNMPT—use this to enable or disable SNMP trap reception.
- HTTP—use this to enable or disable unencrypted Sensor connections.
- PANIC—use this to enable or disable reboot on a system error.
- UIPORT—use this to display the network port you are using for the GUI.

To use **ADSPadmin Config** program, you must:

1. Access the Command Line Interface.

✓ **NOTE** If your **<Backspace>** key does not work (**^H** is displayed instead), you need to change your terminal settings so that backspace works properly. As a temporary solution, you can use **<Ctrl-Backspace>**.

2. Type **c**, then press **<Enter>** at the command prompt.

The **Config** screen displays.

```

root@wips-ralfenator:~
*** ADSPadmin ***

(C) Config

(IP) IP address config
(IPv6) IPv6 address config
(NETPORT) Network port speed/duplex config
(DNS) Define DNS servers
(BONDING) High Availability Ethernet config
(HNAME) Set hostname
(DNAME) Set domain name
(TIME) Time/Date config
(TZ) Set timezone
(NTP) Enable/disable NTP
(SNMPA) Enable/disable reception Snmp agent requests
(SNMPC) Configure Snmp agent community string.
(SNMPT) Enable/disable SNMP trap reception
(HTTP) Enable/disable unencrypted sensor connections
(PANIC) Enable/disable reboot on system error
(UIPORT) Display network port for dashboard access

(Q) to quit (return to previous menu) ->

```

IP

1. Type **ip**, then press **<Enter>** at the prompt to change the IP address, subnet mask, and default gateway of the AirDefense appliance you are logged onto.

The IP configuration screen opens, displaying the current network configuration.

2. Type a new IP address at the prompt. Press **<Enter>**.
3. Type a new subnet mask. Press **<Enter>**.
4. Type a new gateway address. Press **<Enter>**.

Your new values display in bold text.

5. Type **yes** at the prompt to commit the changes.

This returns you to the previous network screen.

AirDefense reboots on exit from the **ADSPadmin**.

Important! If you are logging in remotely using SSH, check these values carefully for accuracy before typing yes or no to commit the changes. Committing incorrect information will cause you to lose connectivity to the ADSP appliance when it reboots.

IPv6

1. Type **ipv6**, then press **<Enter>** at the prompt to change the IPv6 address.

The **IPv6** configuration screen opens, displaying the current network configuration.

2. If this is your first time using IPv6, you are prompted to enable IPv6. Just type **yes** and press **<Enter>**.
3. Type a new IPv6 address at the prompt. Press **<Enter>**.
4. Type **yes** at the prompt to commit the changes.

This returns you to the previous network screen.

AirDefense reboots on exit from the **ADSPadmin**.

NETPORT

Use **NETPORT** to configure the network interface link speed, duplex setting, and to toggle Autonegotiation on and off. The Autonegotiation feature enables the ADSP appliance to analyze the network and find the most efficient network interface available in some cases.

1. Type **netport**, then press **<Enter>** at the prompt to configure network link speed, duplex, and to turn Autonegotiation On and Off.

The **Netport configuration** screen opens, displaying “current network interface configuration...Enter **“on”** of **“off”** for Autonegotiation.”

2. At the prompt, press **<Enter>** to keep the Autonegotiation at its current status, or type in **on** or **off** to change the configuration. Press **<Enter>** again.



NOTE The following steps appear only if the “off” option is selected.

3. At the prompt, press **<Enter>** to keep the current link speed, or type in the desired value. Choices are: 10, 100, or 1000 Mb/s. Press **<Enter>** again.

The screen displays the duplex setting selections.

4. At the prompt, press **<Enter>** to keep the current duplex setting, or type in the desired setting. Choices are half (for half duplex) and full (for full duplex). Press **<Enter>** again.

The screen displays the new network interface configuration.

5. At the prompt, type **yes** to commit the changes, or **no** to cancel the operation.
6. Press **<Enter>**.

You are returned to the **Config** settings screen.

DNS

1. Type **dns**, then press **<Enter>** at the prompt to define DNS servers.

This adds or deletes a DNS nameserver (Domain Name Server). This is the name of the server you give to your DNS server.

The NameServer screen opens, displaying your current DNS server's IP address in bold text.

2. At the prompt, type either **a** to add a new DNS server, or **d** to delete a server.
 - **To add an entry:** type **a** at the prompt and type the IP address at the ensuing prompt. Press **<Enter>** to add the new DNS server to the list of nameServers.
 - **To delete an entry:** type **d** at the prompt. At the next prompt, type in the number of the nameserver you want to delete. (If you delete a DNS server that is followed by other servers, all the ones with a lower preference will move up in priority.)

Important! Multiple DNS servers process DNS requests in order. The first DNS server on the list (identified by the number 1) is the first to offer name resolution, the second DNS server on the list (identified by the number 2) is the second to process the request if the first is unable to do so. To change the order preference of multiple servers, you must delete them all, and re-enter them in the order you want them to process your DNS requests. The first DNS server you enter will become number 1—the first to process name resolution.

3. Type **q**, then press **<Enter>** to quit and return to the main screen.

You are prompted to save your changes.

4. Type **yes**, then press **<Enter>**.

BONDING

1. At the command prompt, type **bonding**, then press **<Enter>** to enable the High Availability Ethernet.
2. Type **b**, then press **<Enter>**.
You will receive confirmation that bonding is enabled.
3. Type **q**, then press **<Enter>** to return to the **Config** settings screen.

HNAME

1. At the command prompt, type **hname**, then press **<Enter>** to change the hostname.
The current hostname is displayed.
2. Type in the new hostname for your ADSP appliance, then press **<Enter>**.
You are prompted to save your changes.
3. Type **yes**, then press **<Enter>**.

DNAME



NOTE If your system is set up to use DHCP, you will not be able to change the domain name using the **ADSPadmin Config** program.

1. At the command prompt, type **dname**, then press **<Enter>** to change the domain name.
The current domain name is displayed.

2. Type in the new domain name for your ADSP appliance, then press **<Enter>**.
You are prompted to save your changes.
3. Type **yes**, then press **<Enter>**.

TIME

Important! Changing the system time/date could affect the integrity of the database. Any change will cause a system reboot on exit from ADSPadmin.

Setting AirDefense time consists of setting the Time and Date (TIME) and the Timezone (TZ), or alternately, enabling an NTP server (NTP). You must set the correct time—time of day, timezone, and date—or alternately, enable an NTP server when you first setup AirDefense. Changing the time configurations after your system has accumulated data can have an adverse affect on the integral state, time, and event associations that are essential to accurate data reporting.

1. Type **time**, then press **<Enter>** at the prompt to change the ADSP appliance's operating time and date
The current date and time displays.
You are prompted to enter a date in MMDDYYYY format. (Do not use colon, forward slash, or other delimiters.)
2. Press **<Enter>**.
You are prompted to enter a time in 24-hour HHMM or HHMMSS format.
3. Press **<Enter>**.
You are prompted to save your changes.
4. Type **yes**, then press **<Enter>**.

TZ

Important! Any change will cause a system reboot on exit from ADSPadmin.

1. Type **tz**, then press **<Enter>** at the prompt to change the ADSP appliance's time zone.
The Time zone screen displays a list of global, continental regions.
AirDefense prompts you to choose a global area in which your ADSP appliance resides.
2. Enter the corresponding number (to the left of your region name). Press **<Enter>**.
A list of nations appears.
3. Enter the abbreviation of your nationality (to the left of the nation) in which the ADSP appliance resides.
Press **<Enter>**.
A list of nationalities appears.
4. Enter the number of the region within your nationality in which the ADSP appliance resides. Press **<Enter>**.
You are prompted to save your changes.
5. Type **yes**, press **<Enter>**.
Typing yes or no reboots and clears the database on exit from **ADSPadmin**.

NTP

Instead of setting the AirDefense Time (TIME) and Timezone (TZ), you can enable automatic time synchronization with an NTP.

Example: If you change the AirDefense time such as when you move the ADSP appliance's location from the east to west coast of the United States, you must also locate a new network time server in the same time zone.

1. Type **ntp** at the command prompt to enable or disable a specific network time server (NTP).
The NTP screen displays your current status in bold text, whether or not you are currently set to use NTP.
2. Type **e** to enable NTP.
You are prompted to enter the IP address or fully qualified host name (hostname.domainname.com) of a network time server.
Alternately, you can type **d** to disable NTP. No additional input is required—NTP is immediately disabled.
3. To save the network time server settings, type **q** to quit.
You are prompted to save your settings.

Important! Entering an invalid time server generates an error and logs you out of **ADSPadmin**.

Also, changing the time configurations after your AirDefense has accumulated data can have an adverse affect on the integral state, time, and event associations that are essential to accurate data reporting.

SNMPA

You can enable SNMP agent by following these steps:

1. Type **SNMPA** at the command prompt.
A SNMP agent status message is displayed to alert you that SNMP agent is enabled or disabled.
2. At the prompt, type **e** to enable SNMP agent.
3. Type **q** to return to the Config menu.
You are prompted to save your change.
4. Type **yes** and press **<Enter>** to save your change (or **no** to disregard your change).
Status messages for **iptables** are displayed indicating if the status is **OK** or not.
5. Press **<Enter>** to display the **Config** menu.

SNMPC

You can configure the SNMP community string by following these steps:

1. Type **SNMPC** at the command prompt.
2. At the prompt, type the community string and press **<Enter>**. If you want to keep the current community string, just press **<Enter>**.

✓ **NOTE** The default community string is **public**.

A status message displays the new community string.

3. Type **yes** and press <Enter> to save your change (or **no** to disregard your change).
The SNMP daemons are stopped and then restarted. Then, the **Config** menu is displayed.

SNMPT

You can enable SNMP trap reception by following these steps:

1. Type **SNMPT** at the command prompt.
A SNMP status message is displayed to alert you that SNMP trap reception is enabled or disabled.
2. At the prompt, type **e** to enable SNMP trap reception.
3. Type **q** to return to the Config menu.
You are prompted to save your change.
4. Type **yes** and press <Enter> to save your change (or **no** to disregard your change).
Status messages for **iptables** are displayed indicating if the status is **OK** or not.
5. Press <Enter> to display the **Config** menu.

HTTP

You can enable HTTP unencrypted Sensor connections by following these steps:

1. Type **HTTP** at the command prompt.
A HTTP status message is displayed to alert you that HTTP unencrypted Sensor connections are enabled or disabled.
2. At the prompt, type **e** to enable HTTP unencrypted Sensor connections.
3. Type **q** to return to the Config menu.
You are prompted to save your change.
4. Type **yes** and press <Enter> to save your change (or **no** to disregard your change).
Status messages for **iptables** are displayed indicating if the status is **OK** or not.
5. Press <Enter> to display the **Config** menu.

PANIC

You can enable reboot on a system error by following these steps:

1. Type **panic** at the command prompt.
A message is displayed to alert you the reboot on system error is not currently enabled.
2. At the prompt, type **e** to enable reboot on system error.
3. Type **q** to return to the Config menu.
You are prompted to save your change.
4. Type **yes** and press <Enter> to save your change (or **no** to disregard your change).
5. Press <Enter> to display the **Config** menu.

UIPORT

You can change the port the GUI is using.

1. Type **UIPORT** at the command prompt to change the port the GUI is currently using.
The UIPORT screen displays the current UI port in use.
2. At the prompt, type **yes** to change the current port, or **no** to keep the current port.
 - If you typed **no**, go to step 3.
 - If you typed **yes**, go to step 4.
3. If you type **no**, the operation is canceled. Press **<Enter>** to return to the **Config** menu.
4. If you type **yes**, the system asks you to enter a new port. Enter a new port number and press **<Enter>**.
AirDefense automatically accepts the change.
5. Press **<Enter>** again.
You are returned to the **Config** settings screen.

Manage

ADSPadmin Utility	Use this utility to...
STATUS	Display the process and disk status of the system.
SYSLOG	Display system log entries resulting from authentication and sendmail failures. You can either display the logs on screen, or write logs to a text file (syslogdata.txt).
TRIMLOG	Truncate system log files when they become too large.
ADMU	Reset the administrator password back to the system default.
PASSWD	Change the password of a Command Line User (smxmgr and smxarchive).
RESTART	Restart ADSP processes (<i>not a full reboot!</i>).
REBOOT	Reboot ADSP appliance (<i>full reboot</i>).
HALT	Halt ADSP (<i>stop processes</i>).

Dbase

ADSPadmin Utility	Use this utility to...
IRESTORE	Restore Forensics files.
IREPAIR	Repair Forensics files.
INTCK	Check integrity of databases.
OUI	Update vendor MAC address information in the database.
FIX7131	Handle AP7131 4.x to 5.x MAC address changes.

Software

ADSPadmin Utility	Use this utility to...
SERVMOD	Update the current version of ADSP software with feature enhancements or improvements.

INDEX

A

- Access Point dropdown menu 2-96
- accessing location tracking 2-106
- Account Access 2-42
- Account Management 2-42
- Action Control commands 2-58
- Action Control table 2-58
- Action Manager 2-54
- Action Rules 2-54
- Action rules 2-80
- Adaptive Scan 2-41
- Add Devices 2-81
- add devices 2-83
- Add Devices - BSS and Wireless Clients Fields 2-82
- Add Floors 2-22
- adding a CLI Profile 4-7
- Admin 1-7, 2-42
- ADMU 9-8
- ADSP 2-68
- ADSP system time 1-10
- ADSPadmin 9-1, 9-6
- Advanced Spectrum Analysis 5-8
- Advanced Troubleshooting 5-9
- Air Termination 2-40
- AirDefense Server 1-1
- AirWave dropdown menu 2-102
- Alarm Configuration 2-35
- Alarm Model 2-9
- Alarm Table 2-10
- AP placement 3-3
- AP Test 5-1
- AP Test import file formats 2-90
- appliance dropdown menu 2-109
- Appliance form factor 2-47
- appliance keys 2-19
- appliance level properties 2-114
- Appliance Licensing 2-16
- Appliance Manager 2-67
- Appliance Platform 4-9
- appliance synchronization 2-70
- Applying CLI Profiles 4-7
- apt_profile 2-90
- apt_profile_info 2-91, 2-93
- Assurance Suite (Network Assurance) 5-9
- Authentication, local 2-47
- Authentication, remote 2-46
- auto logout 2-69
- Auto Refresh 2-48
- Automated (Scheduled) Vulnerability Assessment 3-13
- Automated AP Test 5-3
- automated synchronization 2-71
- Automatic Forensics Backup 2-74
- automatic server synchronization 2-71
- Automatic synchronization 2-73
- Autoplace 2-114, 2-115
- Auto-Placement Rules 2-22

B

- Background SA Scan 2-40
- Background Scanning 5-7
- backing up data 2-70
- Backups 2-70
- Basic navigation 1-9
- BONDING (ADSPadmin utility--also see Config program area) 9-1, 9-4
- BSS dropdown menu 2-96
- buildi a report 2-61
- Building a new report 2-60
- building dropdown menu 2-112
- Building your tree 2-21

C

CA	2-76
campus dropdown menu	2-111
cancel jobs	2-38
Certificate Authority	2-75
Certificate Security Alerts	2-76
Certificates	2-75
Changing, passwords	2-46
Channel Settings	4-2
Charts, in reports	2-61
CLI Configuration	4-5
cloaking Sensors	2-70
Columns, in reports	2-61
Command Line Interface	1-7
Command Line User	1-7
Communication Settings	2-24
Config (ADSPAdmin program area--also see ADSPAdmin utilities)	9-1
Config settings screen	9-2
Connection Termination, and sensor placement	3-3
Connection Troubleshooting	5-4
Copy MAC Formats	2-49
country dropdown menu	2-109
create a report	2-60
Create Network Levels	2-21
Create, report template	2-60
creating a report	2-60
Creating Reports	2-59

D

Dashboard Components	2-2
Data fields, in reports	2-61
Database backups on the primary appliance	2-72
Dbase (ADSPAdmin program area--also see ADSPAdmin utilities)	9-8
Dedicated Spectrum View	5-7
default certificate	2-75
default user roles (types)	2-42
Deleting a report	2-64
Deployment Considerations	3-2
Deployment overview	1-1
deployment requirements	8-1
Device Access	2-33
Device Age Out	2-37
Device Based Forensic Analysis	3-9, 3-11
Device Density	3-3
Device Firmware	4-2
Device Functions Requiring More Explanation	2-103
Device Inactivity	2-48
Device termination, enabling	2-68
device tracking information	2-107
devices dropdown menu	2-96

DNAME (ADSPAdmin utility--also see Config program area)	9-1, 9-4
DNS (ADSPAdmin utility--also see Config program area)	9-1, 9-4
DNS servers	9-4
Domain Name Server	9-1
dropdown menu for Access Points	2-96
dropdown menu for AirWave	2-102
dropdown menu for appliances	2-109
dropdown menu for BSSs	2-96
dropdown menu for buildings	2-112
dropdown menu for campuses	2-111
dropdown menu for cities	2-111
dropdown menu for floors	2-112
dropdown menu for network levels	2-109
dropdown menu for regions	2-110
dropdown menu for Sensors	2-99
dropdown menu for unknown devices	2-101
dropdown menu for unplaced devices	2-113
dropdown menu for Wired Switches	2-101
dropdown menu for Wireless Switches	2-100
dropdown menu WLSE	2-102
dropdown menus	2-96
dropdown menus for devices	2-96
dropdown menus for network levels	2-109
dropdown menus for Wireless Clients	2-98
Duration	2-10

E

Enable Location Tracking RSSI Scan	2-41
enabling FTP/SFTP relay server	2-70
Environment Monitoring	2-32, 3-9
exporting a report	2-66

F

File Format	2-29, 2-89
Filters, in reports	2-63
FIX7131	9-8
floor dropdown menu	2-112
floor manipulation tools	2-107
Floor Plan	5-5
floor plan prerequisite	2-107
Forensic Analysis	3-9, 3-10
Forensic Analysis, accessing	2-52
Forensic Analysis, Device Based	3-11
forensic data	2-53
Forensic RF	5-6
Forensic Time window	2-53
Forensics Backup	2-74
Frame Capture Analysis	2-51
FTP/SFTP relay server, enabling	2-70
Functional Roles	2-45

G

Graphical User Interface (GUI) 1-7
 Guest 1-8, 2-42

H

HALT 9-8
 Helpdesk 1-8, 2-42
 HHMM format 9-5
 HHMMSS format 9-5
 High-water mark 2-10
 HNAME (ADSPAdmin utility--also see Config
 program area) 9-1, 9-4
 Host name mismatch 2-77
 How Backups Work 2-70
 How Synchronization Works 2-71
 HTTP 9-7
 HTTP (ADSPAdmin utility--also see Config
 program area) 9-2

I

Import and Discovery 2-83
 import appliance CLI command 2-28
 import Auto-Placement Rules 2-23
 import communications settings 2-26
 import device file format 2-29, 2-89
 import file formats, AP Test 2-90
 import file formats, scheduling AP Test or
 Vulnerability Assessment 2-94
 import file formats, Vulnerability Assessment 2-92
 import relay server information 4-10
 import remote file 2-85
 Import/Discover Devices 2-83
 import/discover devices 2-85, 2-86, 2-88
 Import/Discover Devices - Local File 2-84
 Import/Discovery 2-27
 importing a report 2-65
 importing communications settings 2-26
 importing maps 2-106
 Infrastructure Management 2-33, 4-2
 INTCK 9-8
 IP (ADSPAdmin utility--also see Config
 program area) 9-1, 9-2
 IP address 9-6
 IPv6 9-1
 IPv6 (ADSPAdmin utility--also see Config
 program area) 9-3
 IREPAIR 9-8
 IRESTORE 9-8

J

Java Security Warning 2-77
 Job Status 2-38

L

LAN Planner, and sensor placement 3-5
 language, for system 2-70
 LDAP server 2-47
 license management 2-16
 Live View 2-51
 LiveRF 5-5
 Local authentication 2-47
 local file import 2-84
 local system time 1-10
 Location Based Services 6-1
 Location Tracking 2-106
 Location Tracking, and sensor placement 3-3, 3-7
 Log Level 2-48
 Login Banner 2-74
 Login banner 2-69

M

mail relay server, specifying 2-70
 Manage (ADSPAdmin utility--also see Config
 program area) 9-8
 Manual data backup 2-70
 manual server synchronization 2-71
 MMDDYYYY format 9-5
 Mobile, and sensor placement 3-5
 Motorola AirDefense Sensor 1-7

N

NETPORT 9-1, 9-3
 Network Assurance 2-31, 5-9
 network level properties 2-113
 network levels dropdown menu 2-109
 Network New Column Preferences 2-49
 Network Structure 2-20
 NTP (ADSPAdmin utility--also see Config
 program area) 9-1, 9-6

O

On-demand AP Test 5-2
 On-Demand auto classification 2-79
 On-Demand Vulnerability Assessment 3-12
 Operation Center 1-8, 2-42
 Operational Management 2-35, 4-9
 OUI 9-8

P

PANIC (ADSPadmin utility--also see Config program area) 9-2, 9-7
 PASSWD 9-8
 Password Reset 2-49
 Passwords, changing 2-46
 Pending State Audit 4-9
 Performance Profiles 2-31, 3-9
 Physical and Electromagnetic Interference 3-2
 planned devices limitations 5-7
 Policy Enforcement, and sensor placement 3-3
 Polling 2-27
 Port 2-68
 Port Suppression, enabling 2-68
 Power and Data cabling 3-4
 Predictive RF 5-6
 predictive RF 5-6
 properties for other levels except appliance level 2-115
 Push Configuration 2-114, 2-115

R

Radio Settings 4-2
 RADIUS setup 2-47
 Readiness Test 2-107
 REBOOT 9-8
 region dropdown menu 2-110
 Relay Server 4-9
 Remote authentication 2-46
 Remote File Fields 2-85
 Report Builder 2-58, 2-60
 report descriptions 2-59
 Reports, building 2-60
 Reports, creating 2-59
 Reports, templates 2-60
 RESTART 9-8
 RF-Domain 2-34
 Rogue Detection, and sensor placement 3-3
 Root-signed certificate 2-75
 Root-signed certificates 2-75
 Rule sets 2-80

S

save a report 2-60
 Scan Mode 2-41
 Scheduled AP Test 2-66, 5-3
 Scheduled data backup 2-71
 Scheduled database backups on the primary
 appliance 2-72
 Scheduled device classification 2-79
 Scheduled Vulnerability Assessment 2-67, 3-13
 Scheduling AP Test import file formats 2-94

Scheduling Vulnerability Assessment import
 file formats 2-94
 Scope Based Forensic Analysis 3-9, 3-10
 Scope Permissions 2-45
 Sections, in reports 2-61
 Security & Compliance 2-30
 Security Alert Window 2-76
 Security Profiles 2-30, 3-9
 Sensor Coverage Survey Process 3-5
 Sensor dropdown menu 2-99
 Sensor Monitoring 3-8
 Sensor Operation 2-40
 Sensor placement 3-2
 Sensor placement, and Location Tracking 3-7
 Sensor Quantity, Location, and Installation 3-4
 Sensor User Interface (Sensor UI) 1-7
 Sensors 1-1
 SERVMOD 9-9
 setup prerequisites for zero touch WLAN
 infrastructure deployment 8-2
 Simple Components 2-61
 SNMP Discovery 2-86
 SNMPA 9-6
 SNMPA (ADSPadmin utility--also see Config
 program area) 9-2
 SNMPC 9-6
 SNMPC (ADSPadmin utility--also see Config
 program area) 9-2
 SNMPT 9-7
 SNMPT (ADSPadmin utility--also see Config
 program area) 9-2
 Software (ADSPadmin utility--also see Config
 program area) 9-9
 specify amount of cloakin Sensors 2-70
 specifying a mail relay server 2-70
 Spectrum Analysis 5-7
 SSH banner 2-69, 2-77
 SSL certificate 2-76
 STATUS 9-8
 Synchronization 2-73
 synchronization 2-71
 Synchronization Rules 2-72
 SYSLOG 9-8
 system language 2-70
 System name 2-68
 System Settings 2-67

T

Tables, in reports 2-61
 Third-party CA 2-76
 TIME (ADSPadmin utility--also see Config
 program area) 9-1, 9-5
 Time Stamp 1-10

TLS encryption 2-75
 Tomcat certificate 2-75
 Tree 2-20
 Tree Setup 2-20, 2-21
 Triangulation considerations, and tree
 organization 2-21
 TRIMLOG 9-8
 Troubleshooting tool 5-4
 TZ (ADSPadmin utility--also see Config
 program area) 9-1, 9-5

U

UI scope considerations, and tree organization ... 2-21
 UIPORT (ADSPadmin utility--also see Config
 program area) 9-2, 9-8
 unknown devices dropdown menu 2-101
 unplaced devices dropdown menu 2-113
 user accounts, creating and changing 2-45
 User Preferences 2-48
 user roles 2-42
 User types 1-7
 User types (roles) 2-42

V

Viewing User Information 2-45
 Vulnerability Assessment import file formats 2-92

W

Web Reporting interface 2-58, 2-59
 WEP Cloak 2-40
 WEP Cloaking 3-3, 3-15
 Wired Network Monitoring 2-31, 3-9
 Wired Switch dropdown menu 2-101
 Wireless Clients dropdown menu 2-98
 Wireless Manager/Switch 2-88
 Wireless Switch dropdown menu 2-100
 WLAN Management 4-1
 WLAN Profiles 4-3
 WLSE dropdown menu 2-102
 wva_profile 2-92

Z

zero touch configuration 8-1



Motorola Solutions, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196-1078, U.S.A.
<http://www.motorolasolutions.com>

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.
© 2012 Motorola Solutions, Inc. All Rights Reserved.

