



# **AirDefense Services Platform 9.1.0 User Guide**



# TABLE OF CONTENTS

Preface .....	1-vii
Scope of Documentation .....	1-vii
Notational Conventions .....	1-viii
Service Information .....	1-ix

## Chapter 1: Overview

AirDefense Services Platform Deployment .....	1-1
Components .....	1-1
Sensors .....	1-2
ADSP Appliance .....	1-2
Network Connections .....	1-2
Deployment Life Cycle .....	1-2
Organization of this Manual .....	1-2
Initial Appliance Configuration .....	1-3
Configuring Data Collection .....	1-3
Lean Back Monitoring .....	1-4
Appliance Connection Options .....	1-4
Keyboard and Terminal .....	1-4
Static IP Address .....	1-5
Serial Port .....	1-5
SSH .....	1-5
Managing User Interfaces .....	1-6
Create User Accounts .....	1-6
User Types .....	1-6
Limitations .....	1-7
Basic Navigation .....	1-7
Tree Structure .....	1-8
Device Search .....	1-8
Filters .....	1-8
Dashboard Drill Down .....	1-8
AirDefense Services Platform and Time .....	1-9
Alarm Time Reporting .....	1-9
Advanced Features .....	1-9

**Chapter 2: The GUI**

The Menu .....	2-2
Toolkit Installation .....	2-2
Open .....	2-5
Forensic Analysis .....	2-10
Action Control .....	2-117
Reporting .....	2-120
Connection Troubleshooting .....	2-138
Scheduled AP Test .....	2-147
Scheduled Vulnerability Assessment .....	2-167
Scheduled Events .....	2-183
Add Devices .....	2-185
Import and Discovery .....	2-188
Dashboard .....	2-198
Selecting Dashboard Scope .....	2-199
Customizing Dashboard Views .....	2-200
Dashboard Components .....	2-200
Network .....	2-203
Show Menu .....	2-206
Network Filters .....	2-215
Actions .....	2-235
Advance Search .....	2-247
Alarms .....	2-249
The ADSP Alarm Model .....	2-251
Alarm Table .....	2-252
Alarm Filters .....	2-253
Alarm Categories and Criticality .....	2-265
Alarm Details .....	2-267
Actions .....	2-268
Configuration .....	2-269
Search .....	2-270
Appliance Platform .....	2-271
Tree Setup .....	2-280
Auto-Placement Rules .....	2-291
Security & Compliance .....	2-310
Network Assurance .....	2-314
Infrastructure Management .....	2-333
Operational Management .....	2-360
Appliance Management .....	2-436
Account Management .....	2-470
Automatic Configuration of WLAN Infrastructure Devices .....	2-490
Configuration Examples .....	2-496
Drop-down Menus .....	2-510
Devices .....	2-510
Network Levels .....	2-573

**Chapter 3: WLAN Management**

Introduction .....	3-1
Infrastructure Management .....	3-2
Device Firmware .....	3-2

Channel Settings .....	3-2
Radio Settings .....	3-2
WLAN Profiles .....	3-2
CLI Configuration .....	3-2
Operational Management .....	3-3
Pending State Audit .....	3-3
Appliance Platform .....	3-3
Relay Server .....	3-3

## Chapter 4: Security

Introduction .....	4-1
WIPS .....	4-1
Planning Your Sensor Deployment .....	4-2
Sensor Monitoring .....	4-9
Advanced Forensics .....	4-10
Scope Based Forensic Analysis .....	4-11
Device Based Forensic Analysis .....	4-12
Vulnerability Assessment .....	4-12
On-Demand Vulnerability Assessment .....	4-13
Automated (Scheduled) Vulnerability Assessment .....	4-14
WEP Cloaking .....	4-14
How Does WEP Cloaking Work? .....	4-14
What if there Is a Problem? .....	4-15
How Do I Configure WEP Cloaking? .....	4-16
Tracker Integration .....	4-16

## Chapter 5: Troubleshooting

Introduction .....	5-1
AP Test .....	5-1
On-Demand AP Test .....	5-2
Automated (Scheduled) AP Test .....	5-3
Connection Troubleshooting .....	5-4
Live RF .....	5-5
Forensic RF .....	5-6
Predictive RF .....	5-6
Spectrum Analysis .....	5-7
Advanced Spectrum Analysis .....	5-8
Advanced Troubleshooting .....	5-9
Assurance Suite (Network Assurance) .....	5-9
Radio Share Network Assurance .....	5-9

## Chapter 6: Location Based Services

Introduction .....	6-1
LBS Profiles .....	6-1
RSSI Scan Data .....	6-2
Reference Material .....	6-2

**Chapter 7: Central Management**

Introduction .....	7-1
Effects on the Dashboard .....	7-2
Effects on the Network Tab .....	7-3
Effects on the Alarms Tab .....	7-4
Effects on the Configuration Tab .....	7-5

**Chapter 8: ADSPadmin**

Introduction .....	8-1
Using ADSPadmin to Configure AirDefense Services Platform .....	8-1
Config .....	8-1
Manage .....	8-8
Dbase .....	8-9
Software .....	8-9

# ABOUT THIS GUIDE

---

## Preface

This guide is designed to help you use the AirDefense™ Services Platform 9.1 Service Module. ADSP is designed to protect your network from wireless threats and attacks, maximize your 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 9.1 is a service module upgrade. Complete instructions for installing the service module are included in the publication *AirDefense Services Platform 9.1 Service Module Installation Guide*, available at the following URL:

<http://support.symbol.com/support/product/manuals.do>

---

## 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, data or equipment.



**CAUTION** This symbol indicates that if this information is ignored, damage to data or equipment may occur.



**WARNING!** This symbol alerts you to situations in which 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.

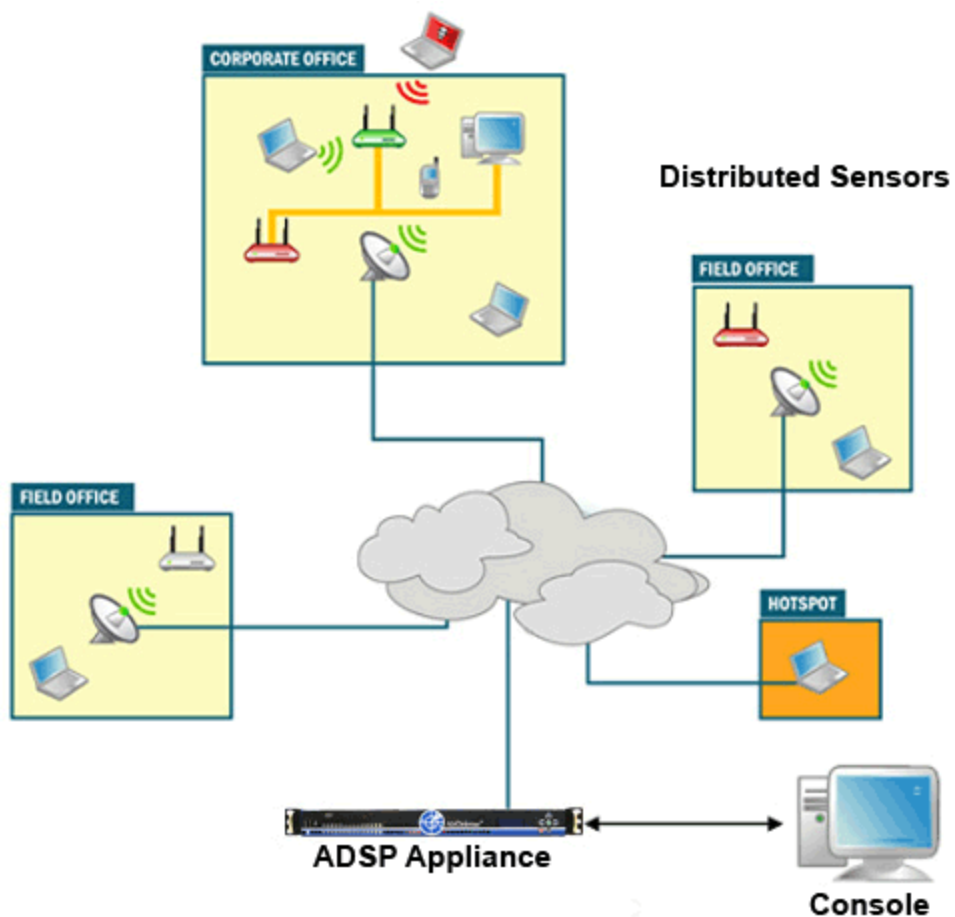


# CHAPTER 1 OVERVIEW

## AirDefense Services Platform Deployment

### Components

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



The ADSP 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, lock-down, and support a server, operating system, and database. A true appliance comes ready with the application and all supporting software preloaded.

### Network Connections

There are various methods of connecting to the AirDefense Services Platform. Motorola AirDefense recommends using the most secure connection 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.

---

## Deployment Life Cycle

The AirDefense Services Platform (ADSP) 9.1 Service Module is designed to be “self-managing.” After the installation and the initial configuration, ADSP requires minimal maintenance, except for periodic tuning. This self-managing feature allows you the freedom to focus your attention on analyzing data and responding to the needs of your organization.

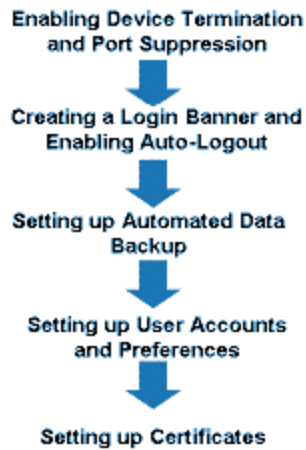
### Organization of this Manual

This manual is organized to roughly reflect the ADSP life cycle. In this manual, the configuration activity is addressed in two phases: Initial Appliance Configuration and Configuring Data Collection.

## Initial Appliance Configuration

The following graphic shows the basic activities in this phase.

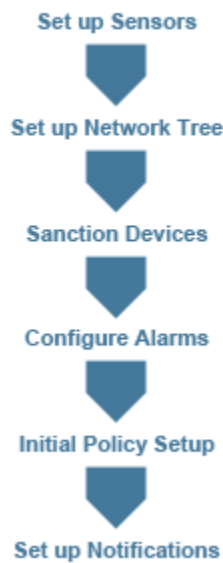
### Initial Appliance Configuration



## Configuring Data Collection

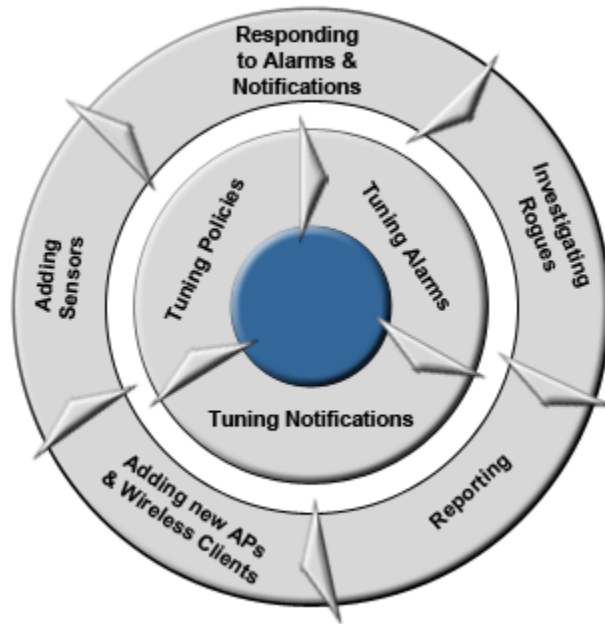
The following graphic shows the basic activities in this phase.

### Configuring Data Collection



## Lean Back Monitoring

The following graphic shows the ongoing activities involved in monitoring your WLAN's security using the ADSP service module.



---

## 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 physically 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.

## Managing User Interfaces

User interfaces allow system users to access certain ADSP components. Each user interface has permissions. The table below describes the user 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  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

## Create User Accounts

AirDefense Services Platform has one default Admin user account. ADSP allows Admin users to create numerous other users with role-based permissions that control which functionality each user can access. The Admin user creates individual accounts and assigns user roles.

## 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.

## Limitations

### System Configuration Limitations

Your particular ADSP configuration will affect what fields you may access, regardless of your user type. Some of the features described in this guide may not appear in the interface, or may be grayed out, depending on whether they are enabled or disabled.

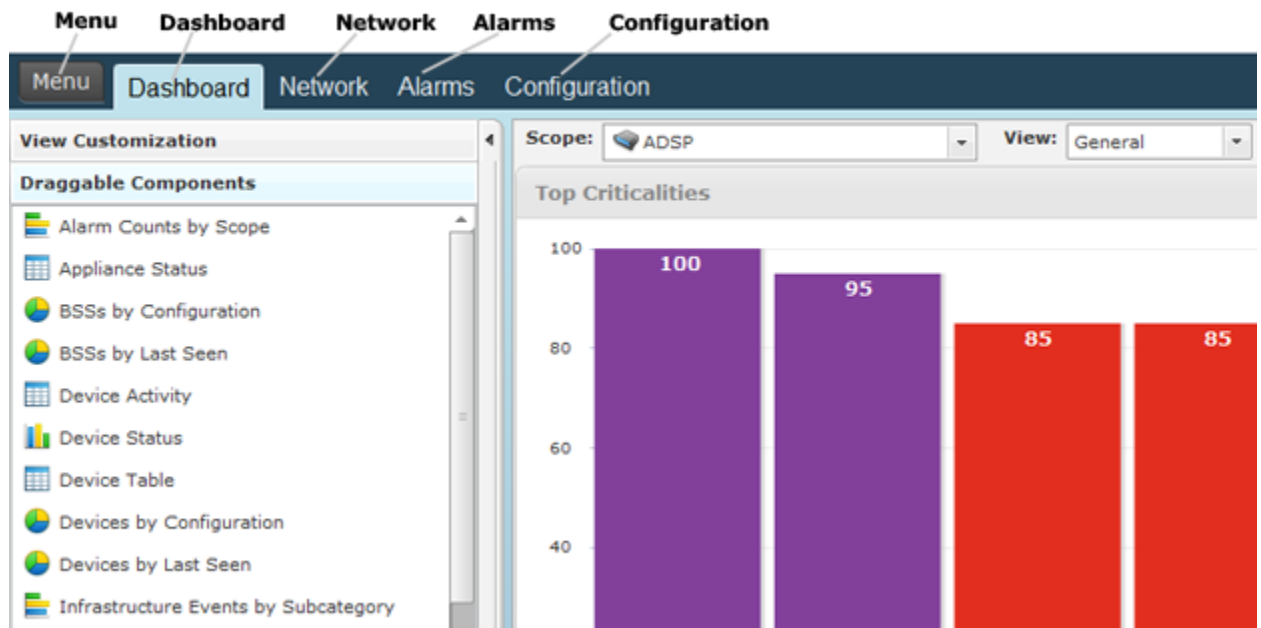
Example: If Air Termination is disabled, you will not see options for using it.

### Scope Limitations

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.

## 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 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 and perform 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.

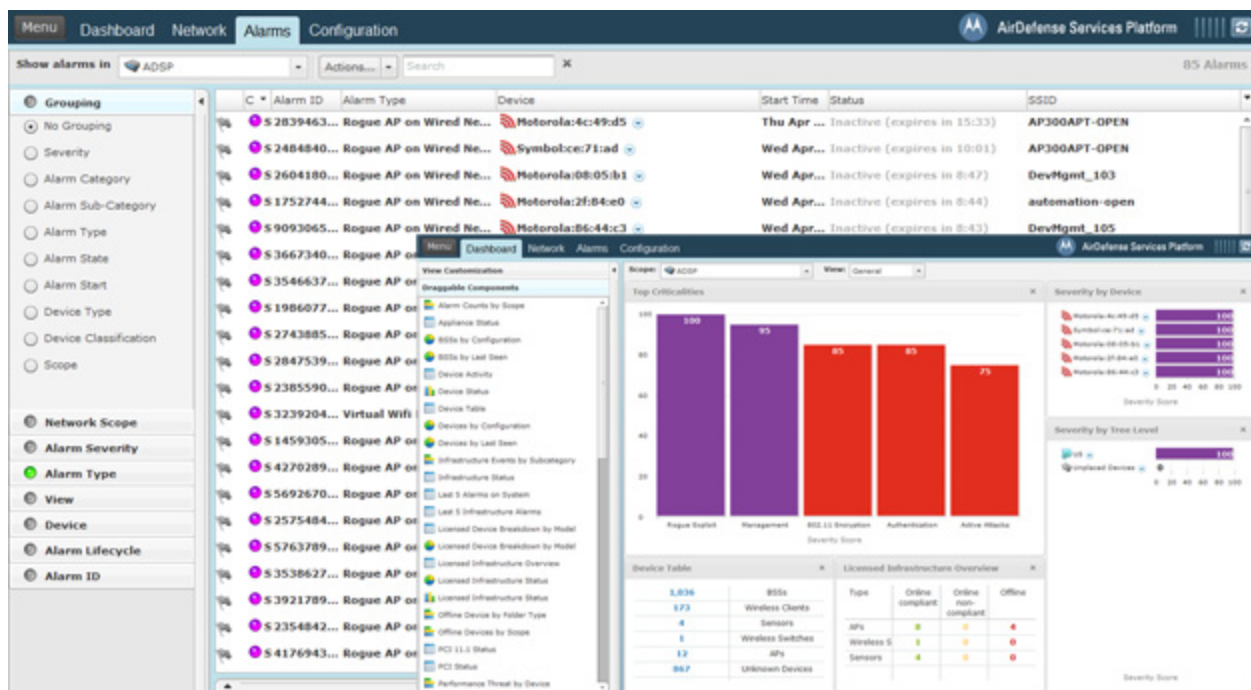
## Filters

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.



Advanced feature modules are categorized as follows:



- Security
- Troubleshooting
- WLAN Management

A Central Management module provides control over multiple appliances from one interface.

Each module is discussed in later chapters of this document.

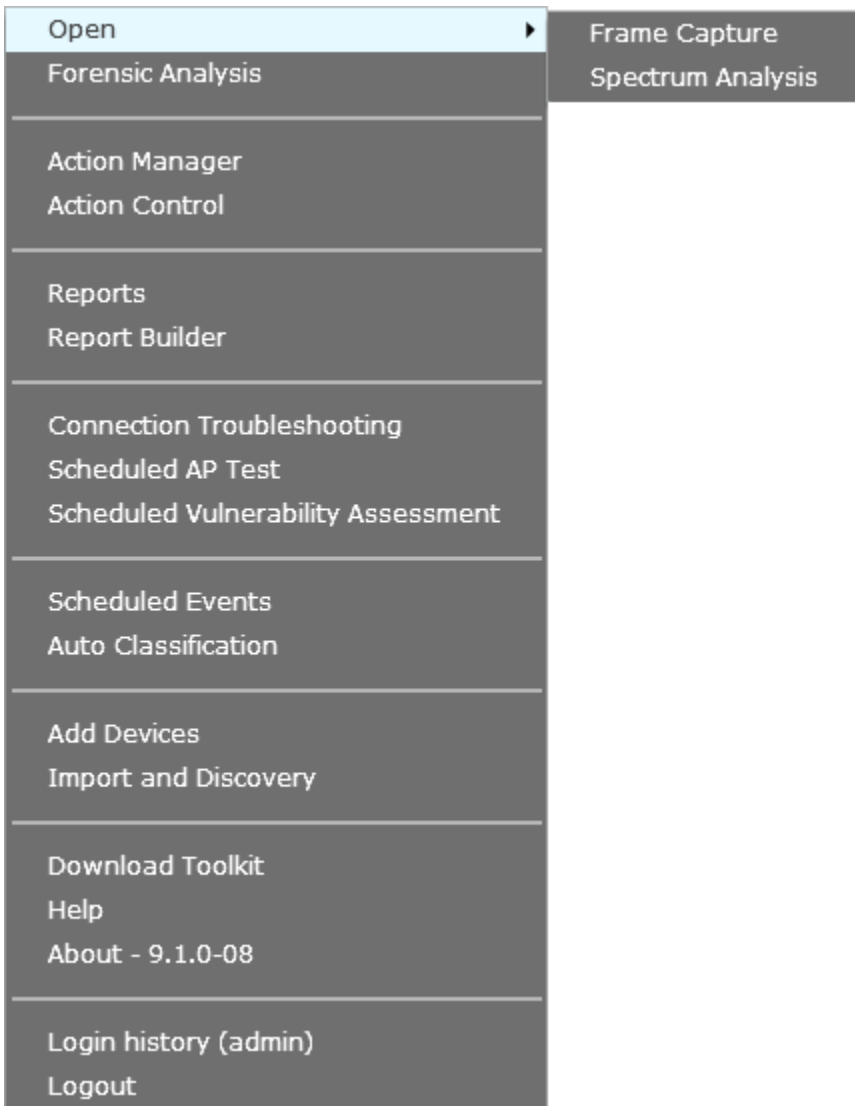


# CHAPTER 2 THE GUI

- ✓ **NOTE** Appearing throughout ADSP is a **Refresh**— button that allows you to refresh the ADSP GUI on demand. Next to the **Refresh** button is a refresh status indicator— to let you know when the GUI is being refreshed.

## 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.

## Toolkit Installation

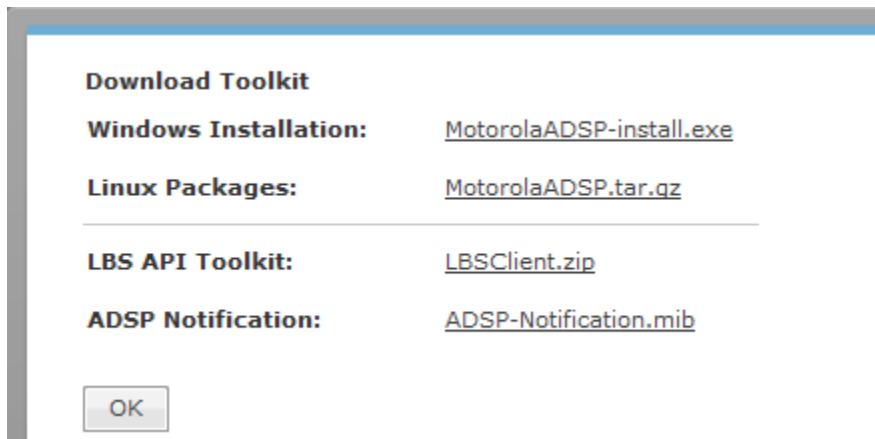
To run the Java applets, you are required to install the ADSP Toolkit on your local workstation. If you have no need to run the applets, there is no need to install the ADSP Toolkit.

✓ **NOTE** If you attempt to access a Java standalone feature and the ADSP Toolkit is not installed, you will be prompted to install it.

To install the ADSP Toolkit:

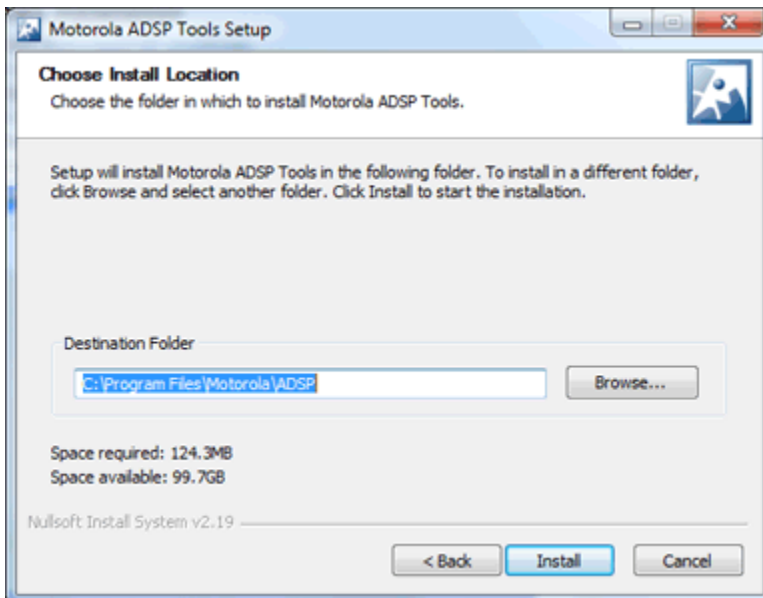
1. Access the login page and click the [Downloads](#) link in the top, right corner of the page (or if you are logged in, select [Menu](#) > [Download Toolkit](#)).

2. Select the version of the installation program that corresponds to your OS: (Windows Installation or Linux Packages) and then follow the instructions for your OS.



## Windows Installation

1. Click [MotorolaADSP-install.exe](#).  
A **Security Warning** window displays, **Continue to this website (not recommended)**.
2. Click **Run** to install the ADSP Toolkit.  
A **Download Status** window displays. Then, another security window displays.
3. Run the installer, or save the application to your workstation and then run the installer.
4. Read the license agreement, and then click **I Agree**. The installation location window appears.



5. Accept the default location or browse to another location, and then click **Install**.

✓ **NOTE** If your workstation is running Windows 7, 64-bit operating system, do not install in the default location (C:\Program Files (x86)\Motorola\ADSP). Use another location.

The installation program installs the Toolkit application, and then displays the finish screen.

## Linux Packages

1. Click **MotorolaADSP.tar.gz**.

A dialog window displays prompting you to open or save the file.

2. Save the file to a directory on your Linux system.
3. Unpack *MotorolaADSP.tar.gz* using the following command:

```
tar xzvf MotorolaADSP.tar.gz
```

The unpack files are placed in the ADSP installation directory (*/usr/local/ADSP*). If a different path is displayed as the target, you should change it to */usr/local/ADSP*. Now, when you attempt to access an ADSP application that is part of the toolkit, your browser will prompt you on what to do with the file *adeapp.adx*.

4. Select **Open with**, browse to */usr/local/ADSP/WIPS/Enterprise*, and select **adsp**. Make sure the **Do this automatically for files like this from now on** checkbox is checked, and then click **OK**. Now, when you attempt to open an ADSP application that is part of the toolkit, it will open automatically.



**NOTE** In some instances, the Firefox browser will not prompt the user on what to do with the *adeapp.adx* file. In this case, open the Firefox preferences dialog and configure the browser to point to */usr/local/ADSP/WIPS/Enterprise/adsp*.



## Open

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

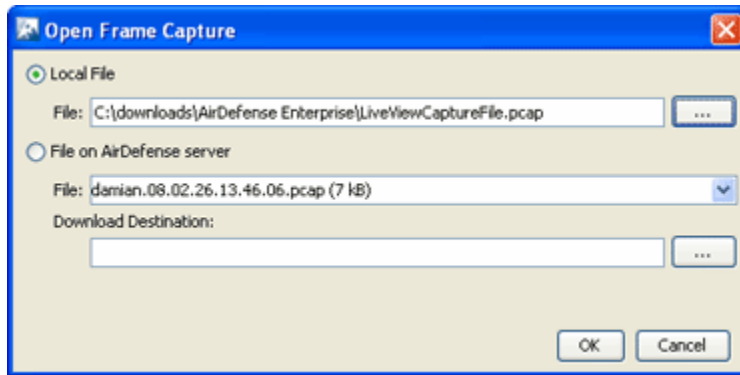
### Frame Capture Analysis

Frame Capture Analysis allows you to replay events that occurred during a Live Monitoring session. Every time you open a Live Monitoring session, a frame capture of that session is automatically saved on the appliance in a pcap file. For identification, the pcap file is stored with the user name and start time. The system will store as many capture sessions as possible up to 1 GB of total capture files. Once the 1 GB limit is reached, the oldest sessions get deleted first.

You can also manually save a Frame Capture file permanently on your server or workstation. This is done by selecting **File > Save** while in a Live Monitoring session. (Refer to Frame Capture under the Common Area topic for Live Monitoring for the procedure.)

To start a Frame Capture Analysis session:

1. Select **Menu > Frame Capture Analysis**. The **Open Frame Capture** popup window displays.

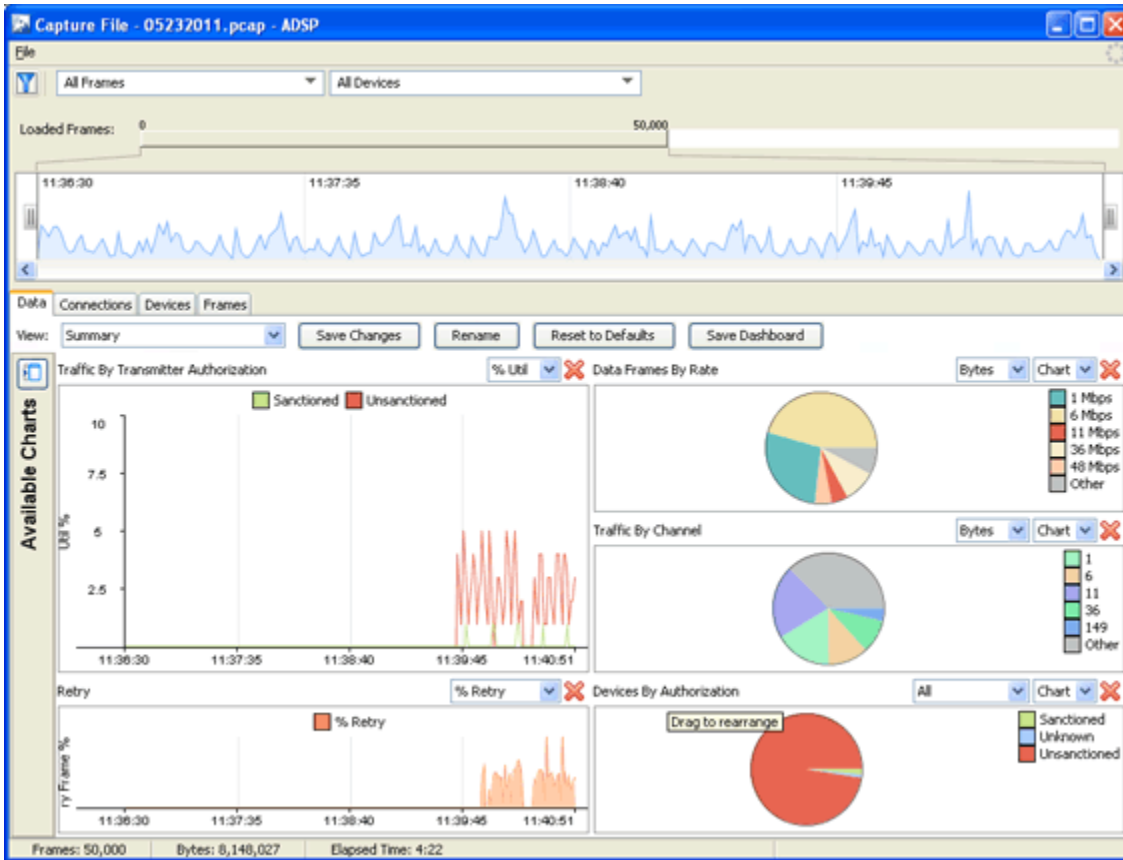


2. To open a capture file saved to your workstation:
  - a. Select the **Local File** radio button.
  - b. Click the **Select Location** button—  for the **Local File** option.
  - c. Navigate to the folder (directory) where the file was saved.
  - d. Select the file and then click **OK**. The filename along with the path name displays in the **File** field.
  - e. Click **OK**.

The capture file is opened for you to analyze.

3. To open a capture file on your ADSP server:
  - a. Select the **File on AirDefense server** radio button.
  - b. Click the **Download Destination** button—  for the **File on AirDefense server** option.
  - c. Navigate to a folder (directory) where you want to save the file on your workstation.
  - d. Click **Select**. The filename along with the path name displays in the **Download Destination** field.
  - e. Click **OK**.

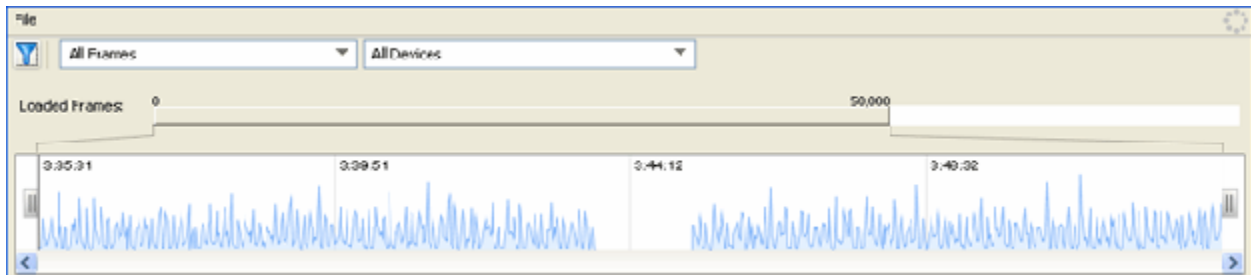
The capture file is downloaded to your workstation and opened for you to analyze.



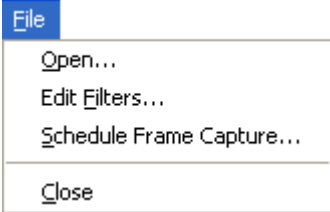
The **Capture File** window is basically the same as the **Live View** window minus the buttons and menus that are not needed for Frame Capture Analysis. The tabs display the same information as the **Live View** window.

### **Common Area**


The common area holds the menus, buttons and time window that are common to Frame Capture Analysis. If more than 50,000 frames have been capture, a **Loaded Frames** slide bar is also displayed. The common area is located at the top of the window.



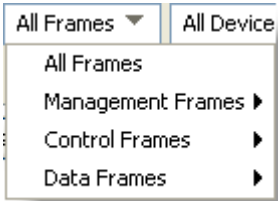
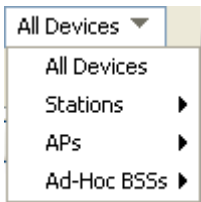
**Menus**

Menu	Option	Description
 <p>File</p>	Open	Opens a captured file.
	Edit Filters	Opens the <b>Live View Filter</b> popup window where you can set options to filter data. (See Live View Filter for more information.)
	Schedule Frame Capture	Run automatic frame captures using the scheduler. (See Automatic Frame Captures.)
	Close	Exits the Live View session and closes the <b>Live View</b> window.

**Buttons**

Button	Description
	Opens the <b>Live View Filter</b> popup window. where you can set options to filter data. (See Live View Filter for more information.)

**Drop-down Menus**

Dropdown Menu	Description
<p>Frame Selection</p> 	All Frames Acts as a quick filter to display only frames for the selected frame type. To view all types, select <b>All Frames</b> .
<p>Device Selection</p> 	All Devices Acts as a quick filter to display only frames for the selected device. To view all devices, select <b>All Devices</b> .

**Time Window**

The **Time Window** shows a frame count chart over time for the entire capture file. You can adjust the time window by moving the sliders (on either end of the time window). This allows you to view and analyze frame data for the highlighted time range.

### **Loaded Frames Slide Bar**

If a capture file contains more than 50,000 frames, only the first 50,000 frames will be loaded. A **Loaded Frames** slide bar is added that allows you to load the other frames. Just move the slide bar to load another 50,000 frames.

### ***Tabs***

Frame Capture Analysis uses the same tabs as Live Monitoring.

- **Data** tab provides the same features for Frame Capture Analysis as Live Monitoring.
- **Connections** tab shows the relationships between devices within the Frame Capture Analysis time window.
- **Devices** tab shows the devices within the Frame Capture Analysis time window.
- **Frames** tab shows the frames within the Frame Capture Analysis time window.

For more information, refer to the appropriate topic under Live Monitoring.

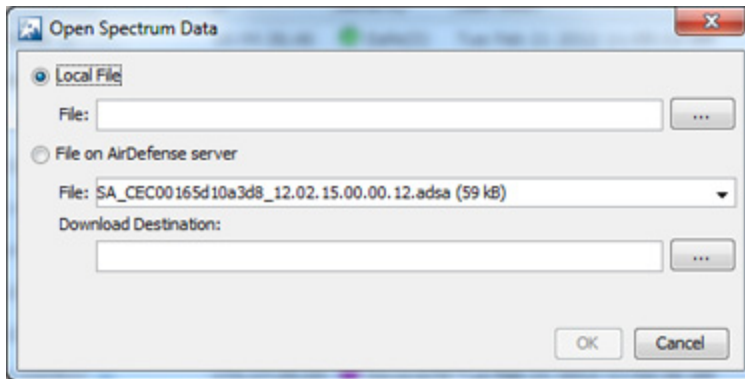
## Spectrum Analysis

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. See Spectrum Analysis topic for more information about Spectrum Analysis.

To view a saved Spectrum Analysis session:

1. Select **Menu > Open > Spectrum Analysis**. The **Open Spectrum Data** popup window displays.

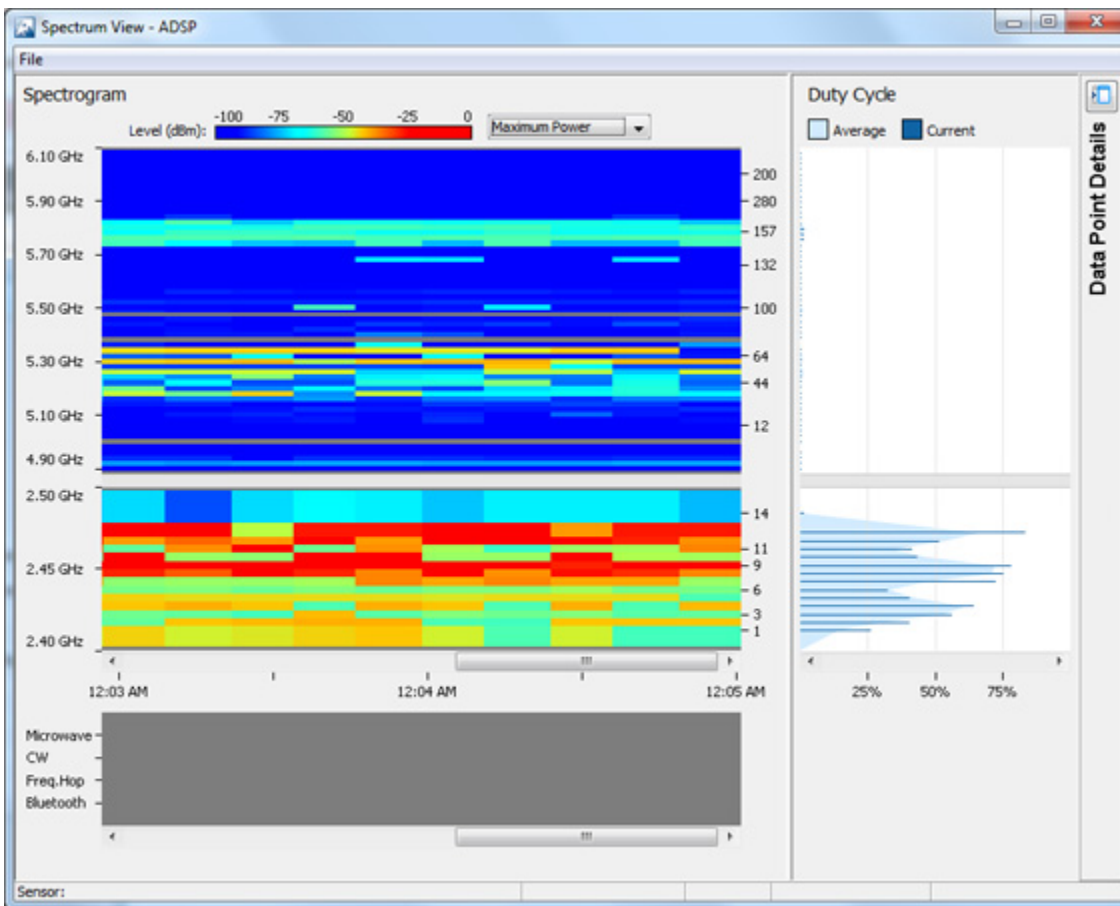


2. To open a Spectrum Analysis file saved to your workstation:
  - a. Select the **Local File** radio button.
  - b. Click the **Select Location** button—  for the **Local File** option.
  - c. Navigate to the folder (directory) where the file was saved.
  - d. Select the file and then click **OK**. The filename along with the path name displays in the **File** field.
  - e. Click **OK**.

The Spectrum Analysis file is opened for you to analyze.

3. To open a Spectrum Analysis file on your ADSP server:
  - a. Select the **File on AirDefense server** radio button.
  - b. Click the **Download Destination** button—  for the **File on AirDefense server** option.
  - c. Navigate to a folder (directory) where you want to save the file on your workstation.
  - d. Click **Select**. The filename along with the path name displays in the **Download Destination** field.
  - e. Click **OK**.

The Spectrum Analysis file is downloaded to your workstation and opened for you to analyze.



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.

### Basic Forensics vs. Advanced Forensics

There are two types of forensic analysis: Basic and Advanced. The Advanced Forensics feature requires a license and includes all the capability of Basic Forensics along with some enhancements. If you are using Basic Forensics, only certain features are available. See the following list of features that are available/unavailable with Basic Forensics.

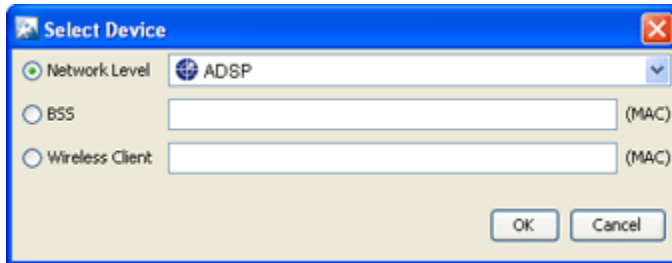
- Basic Forensics only works for BSS and Client.
- No location data is available.
- No data analysis graphical representations are available.

- Data is displayed in 24 hours increments. You cannot configure a different time period, but you can choose whatever 24 hour period that you want.
- Slide bars do not work to narrow time to specific events; only the selected 24 hour time period is displayed.

## Initiate Analysis

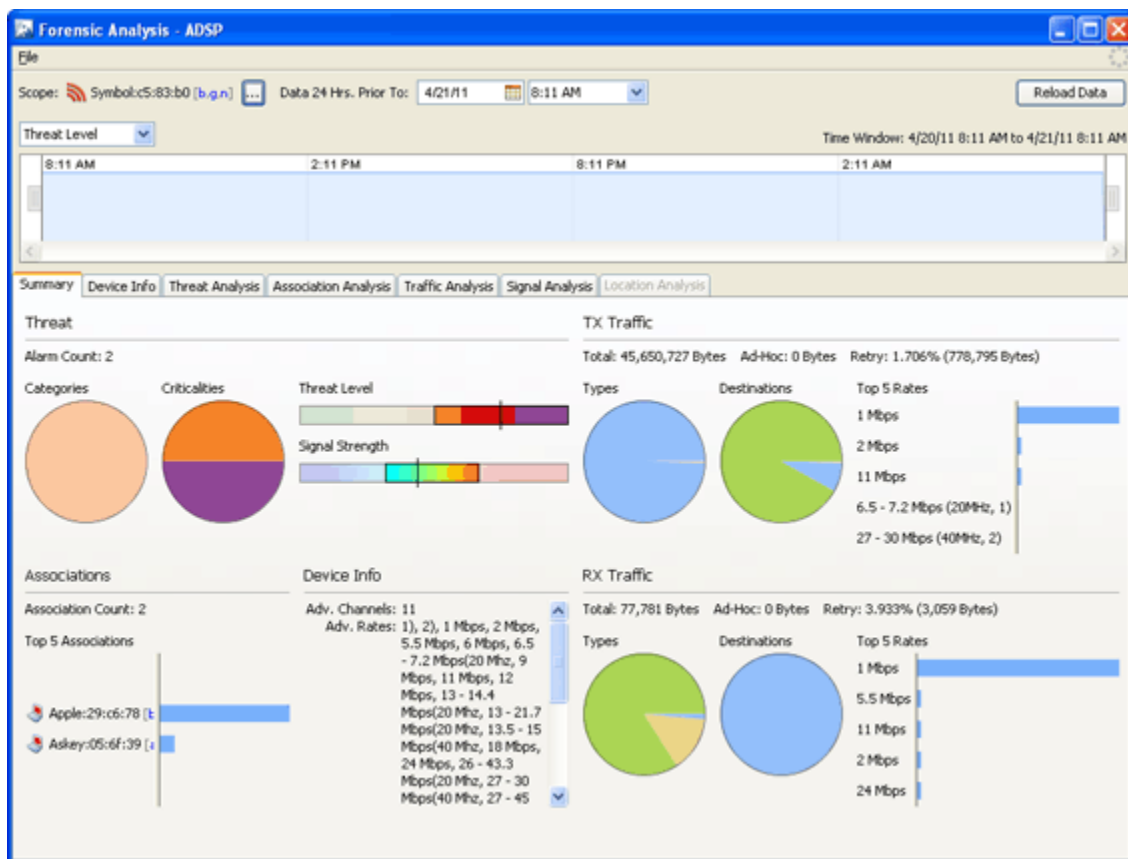
To initiate an analysis:

1. Select **Menu > Forensic Analysis**. The **Select Device** window displays.



2. Select a Sensor, AP, or Switch from the Network Level drop-down menu, or select BSS or Wireless Client and supply the MAC address.
3. Click **OK**. The **Forensic Analysis** window displays.

✓ **NOTE** Another way to run Forensic Analysis is to use the device's drop-down menu button— or right-click on a device name and then select Forensic Analysis.



## Common Area

### *Forensic Settings*

The Forensic Settings are used to set the traffic units for Traffic Analysis. To change a setting, click the **File** menu and then select **Settings**.



Click the **Traffic Unit** drop-down menu to change the traffic units. Your choices are:

- Bytes
- KBytes
- MBytes
- GBytes.

✓ **NOTE** The Location Unit drop-down menu button and Scope Base Settings are part of the Advanced Forensics. You cannot adjust these settings here.

### *Scope*

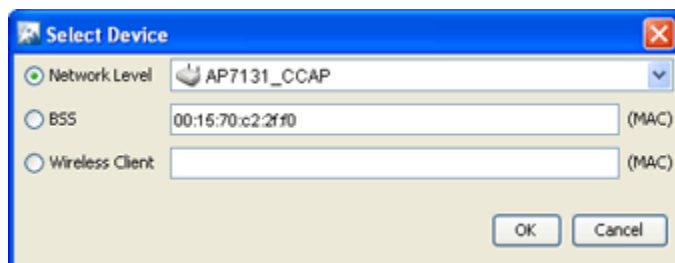
The **Scope** field displays the device that you are analyzing. An BSS icon or a Wireless Client icon along with the device name is shown.

If you right-click on the device, you can copy a device's MAC address for later use.

### *Switch Devices*

You can switch to another device if you know the device's MAC Address. To switch devices:

1. Click the  button. The **Select Device** popup will display.






2. Select a Sensor, AP, or Switch from the **Network Level** drop-down menu, or select **BSS** or **Wireless Client** and type in the MAC Address.
3. Click **OK**.

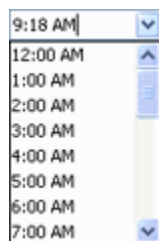
### *Date and Time Specification*

Forensic Analysis is done in 24 hour time increments. By default, the time period is set 24 hours prior to when you first access Forensic Analysis. You can change the 24 hour period by selecting a date a time of day. To specify a new time:

1. Click the first **Calendar** button— to select a starting date. A calendar displaying the current month will display.



2. Select a day of the month from the calendar. You may switch months using the arrow keys.
3. Click the **Time** drop-down button to select a new time of day. A drop-down list will display showing a list of dates by hours.



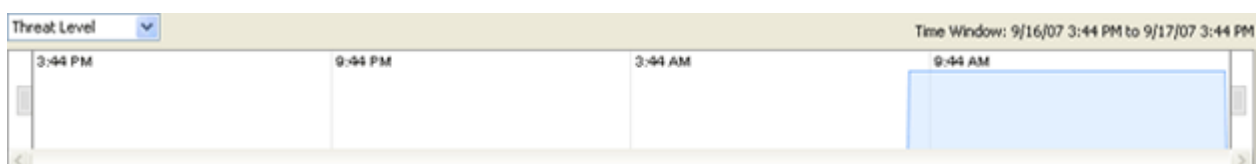
4. Select a time from the list or type in a time.
5. Click the **Reload Data** button. The **Time** window will change to reflect your time range.

✓ **NOTE** With basic forensics, you cannot configure a different time period, but you can choose whatever 24 hour period you want.

### *Time Window*

The **Time** window has three different views:

- Threat Level (default)
- Total Traffic
- Association Count.



Each view is shown across the time range which is limited to 24 hours.

## BSSs and Wireless Clients

The following six tabs are available for BSSs and Wireless Clients:

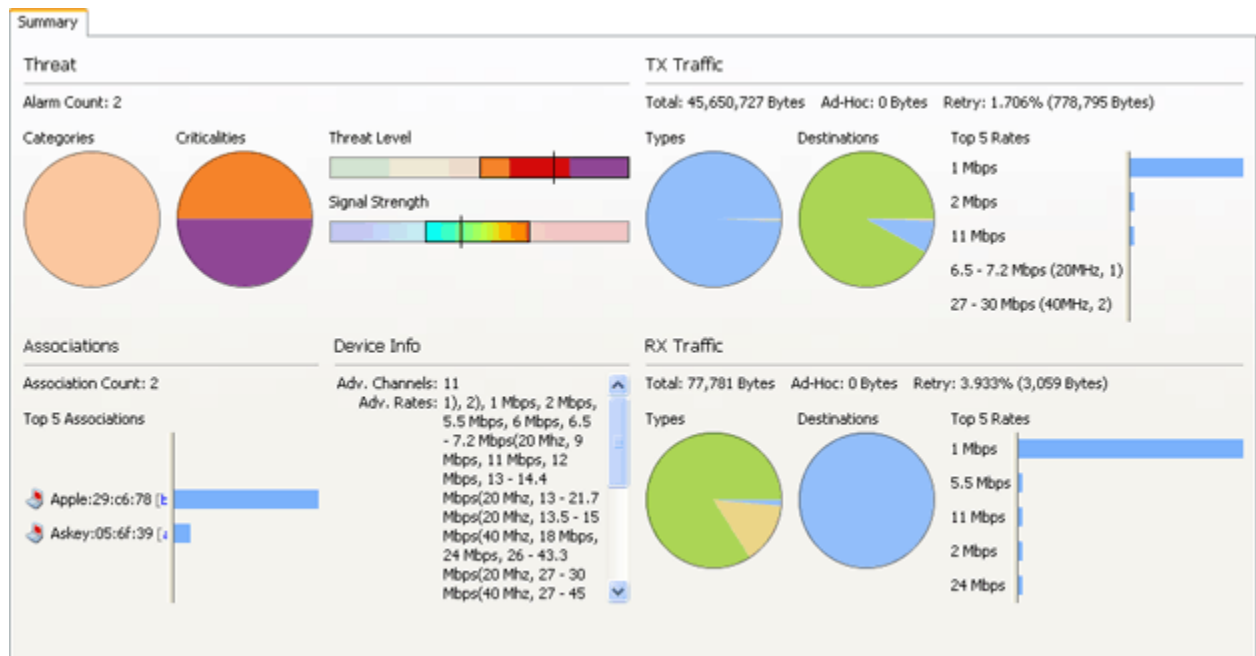
- Summary
- Device Info
- Threat Analysis
- Association Analysis
- Traffic Analysis
- Signal Analysis.

✓ **NOTE** The **Location Analysis** tab is inactive. It is part of the Advanced Forensics.

Each tab is discussed as a separate topic.

### Summary

The Summary tab provides a summary of forensic data broken down into categories that roughly match contents of the other tabs. Each time you access Forensic Analysis the Summary tab is the first one displayed.



The following information is included in the **Summary** tab:

- Threat
  - Total alarm count
  - Alarm pie charts grouped by categories and criticalities
  - Minimum, maximum, and average threat level
  - Minimum, maximum, and average signal strength



The information displayed depends on whether the device is an BSS or a Wireless Client (see table below).

Column	Description	BSS	Wireless Client
Time	The date and time of day when the device was seen.	X	X
Advanced Capabilities	An abbreviated description indicating the advanced capabilities of a BSS.	X	
Advertised Channels	The WLAN broadcast channel for the device.	X	X
Advertised Rates	The advertised data rates of the BSS in mbps.	X	
Authentication	The type of authentication supported by the BSS, i.e. password.	X	X
Capabilities	Device capabilities including: <ul style="list-style-type: none"> <li>• ESS network</li> <li>• Data confidentiality required</li> <li>• Short slot time enabled</li> <li>• APSD implemented</li> <li>• DSSS-OFDM not in use</li> <li>• RTS/CTS or CTS-to-self protection</li> <li>• Barker Preamble mode</li> <li>• DCF.</li> </ul>	X	X
Channels Used	The WLAN broadcast channel for the device.	X	
Encryption	Encryption method being used.	X	X
IP Address	A Wireless Client's Internet Protocol address.		X
IP-SEC	Internet Protocol Security method being used.	X	X
LEAP User Name	The user name used during LEAP authentication (if used).		X
Rates Used	The data rates used during association.	X	X
Reason Codes	A code representing the reason that a device did not associate or authenticate, or lost association or authentication.	X	X
SSID	The Service Set Identifier, 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.	X	X
SSID Broadcast	An indication ( <b>Yes/No</b> ) of whether a SSID is being broadcast.	X	X
Status Codes	A code representing the status of a device.	X	X

Column display and arrangement can be customized as follows:


- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

The table may be shown with one row per minute or one row for every change in the value of a particular column (category). Click the appropriate radio button in the top, left side of the **Device Info** tab.

✓ **NOTE** If you add additional columns, they will be included in the drop-down list for the **One row per change in** field.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Threat Analysis

The **Threat Analysis** tab displays a table of alarms generated by the device being analyzed.

Criticality	Category	Type	Start Time	Expiration
Major (50)	Authorization Violation	Unsanctioned AP	Before Time Range	After Time Range

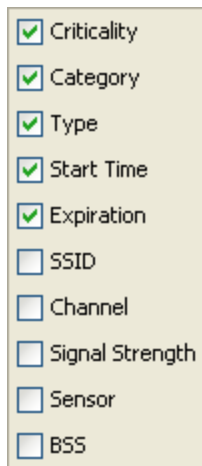
The information displayed is as follows:

Column	Description
Criticality	The color designation and name for the threat level, as follows: <ul style="list-style-type: none"> <li>Severe—Serious alarms that may have catastrophic effects on your WLAN.</li> <li>High/Critical—Serious alarms on devices that require immediate attention.</li> <li>Elevated/Major—Potentially serious alarms on devices that require priority attention.</li> <li>Guarded/Minor—Potential problem alarms on devices that may develop into worse issues if left alone.</li> <li>Safe/Low—Devices that pose no immediate threat to your WLAN network.</li> </ul>
Category	The type of category that the alarm falls under.
Type	The specific type of alarm, providing detailed information as to what generated the alarm in the first place.
Start Time	The date and time group of when the alarm first occurred.
Expiration	The date and time group of when the alarm will expire. The alarm can be an ongoing alarm which never expires.
SSID	The Service Set Identifier, 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. (Default state is hidden.)
Channel	The WLAN broadcast channel for the device. (Default state is hidden.)

Column	Description
Signal Strength	The signal strength (in dBm) of the device. (Default state is hidden.)
Sensor	The name of the Sensor that sees the device. (Default state is hidden.)
BBS	The Basic Service Set, a term used to describe the collection of Wireless Clients which may communicate with each other within a WLAN. (Default state is hidden.)

Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).

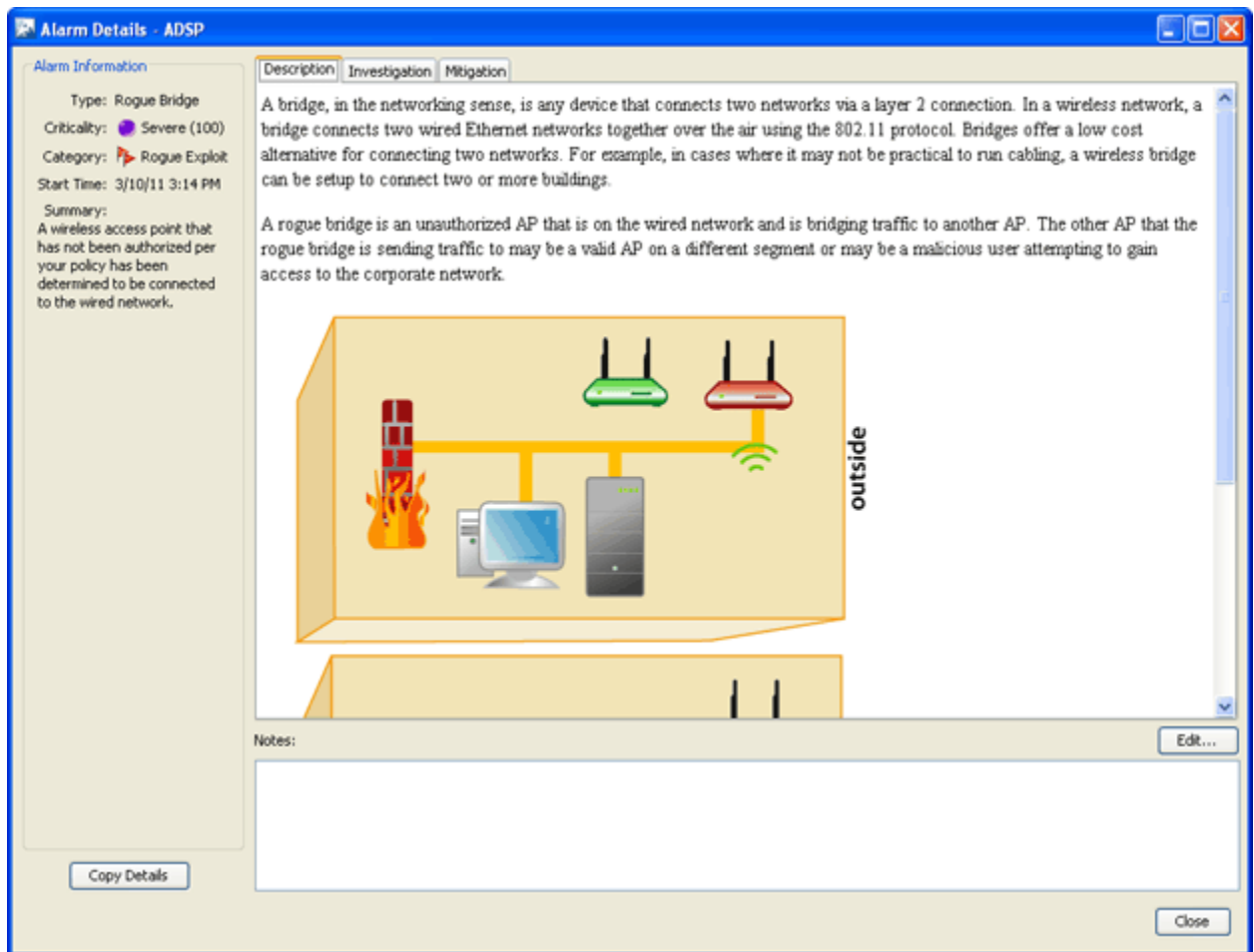



- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.



Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm.



You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Association Analysis

The **Association Analysis** tab lists the associations between the device being analyzed and other wireless devices.

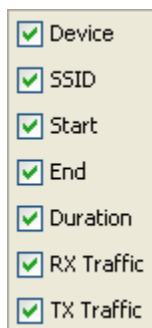
Device	SSID	Start	End	Duration	RX Traffic	TX Traffic
Apple:29:c6:78 [b.g.n]	101	Ongoing Association	4/20/11 8:03 AM	1 minute	0	0
Apple:29:c6:78 [b.g.n]	101	4/20/11 8:18 AM	4/20/11 8:31 AM	13 minutes	0	158
Apple:29:c6:78 [b.g.n]	101	4/20/11 8:45 AM	4/20/11 8:45 AM	1 minute	80	0
Apple:29:c6:78 [b.g.n]	101	4/20/11 8:58 AM	4/20/11 8:58 AM	1 minute	80	0
Apple:29:c6:78 [b.g.n]	101	4/20/11 9:10 AM	4/20/11 9:10 AM	1 minute	0	86
Apple:29:c6:78 [b.g.n]	101	4/20/11 9:22 AM	4/20/11 9:22 AM	1 minute	160	186
Apple:29:c6:78 [b.g.n]	101	4/20/11 9:35 AM	4/20/11 9:45 AM	10 minutes	802	3,529
Apple:29:c6:78 [b.g.n]	101	4/20/11 9:46 AM	4/20/11 9:46 AM	1 minute	322	768
Apple:29:c6:78 [b.g.n]	101	4/20/11 9:58 AM	4/20/11 9:58 AM	1 minute	160	1,142
Apple:29:c6:78 [b.g.n]	101	4/20/11 10:00 AM	4/20/11 10:00 AM	1 minute	0	264
Apple:29:c6:78 [b.g.n]	101	4/20/11 10:49 AM	4/20/11 10:49 AM	1 minute	80	192
Apple:29:c6:78 [b.g.n]	101	4/20/11 2:12 PM	4/20/11 2:14 PM	2 minutes	0	2,187
Apple:29:c6:78 [b.g.n]	101	4/20/11 2:17 PM	4/20/11 2:17 PM	1 minute	0	134
Askey:05:6f:39 [b.g.n]	101	4/20/11 6:22 PM	4/20/11 6:22 PM	1 minute	0	1,170

The information displayed is as follows:

Column	Description
Device	MAC address of the device.
SSID	Service Set Identifier of the associated AP.
Start	Time when the association first started.
End	Time when the association ended.
Duration	Total amount of time the association lasted.
RX Traffic	Number of bytes received during the association.
TX Traffic	Number of bytes transmitted during the association.

Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

An option is included to group by associated device. When selected, there will be only one row for each unique device. Click the **Group by associated device** checkbox to select the option.

Right-clicking on a device displays a menu of options that allow you to conduct additional functions on the device.

Copy MAC
View/Edit Policy
Forensic Analysis
All Alarms for AP
Live View
Locate (Triangulation)
Test AP Connectivity
Switch Port Lookup
Generate Tracker Files
Action Details

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### *Traffic Analysis*

The **Traffic Analysis** tab displays traffic transmitted and received by the device being analyzed.

Traffic Analysis						
Traffic Category: <input type="button" value="Retry"/>	Traffic Type: <input type="radio"/> TX <input type="radio"/> RX <input checked="" type="radio"/> All		(Traffic in Bytes)			
Time	TX % Retry	RX % Retry	TX Retryable Data	TX Retry	RX Retryable Data	RX Retry
<b>Totals</b>	0.109%	34.682%	42,143,174	46,058	346	120
4/6/11 3:48 PM	0%	0%	0	0	0	0
4/6/11 3:49 PM	0.471%	0%	37,774	178	0	0
4/6/11 3:50 PM	0%	0%	35,915	0	0	0
4/6/11 3:51 PM	0%	0%	30,635	0	0	0
4/6/11 3:52 PM	0%	0%	31,416	0	0	0
4/6/11 3:53 PM	0.566%	0%	31,427	178	0	0
4/6/11 3:54 PM	0%	0%	33,792	0	0	0
4/6/11 3:55 PM	0.576%	0%	30,910	178	0	0
4/6/11 3:56 PM	0%	0%	36,960	0	0	0
4/6/11 3:57 PM	0.503%	0%	35,398	178	0	0
4/6/11 3:58 PM	0%	0%	29,304	0	0	0
4/6/11 3:59 PM	0%	0%	30,888	0	0	0
4/6/11 4:00 PM	0.557%	0%	31,966	178	0	0
4/6/11 4:01 PM	0%	0%	32,208	0	0	0
4/6/11 4:02 PM	0%	0%	30,646	0	0	0
4/6/11 4:03 PM	0%	0%	35,640	0	0	0
4/6/11 4:04 PM	0%	0%	36,168	0	0	0
4/6/11 4:05 PM	0.522%	0%	34,078	178	0	0

The **Traffic Category** field determines the type of data displayed in the table. You can change the traffic category by selecting one of the following categories from the **Traffic Category** drop-down menu:

- Ad-Hoc
- Control Detail
- Data Details

- Destinations
- EAP Details
- Encryption Details
- Management Details
- Polled Information
- Rates
- Retry (default)
- Types.

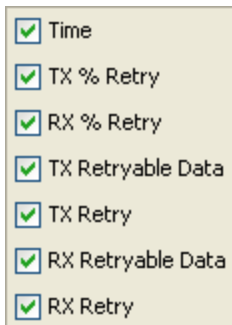
The **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types. You can change the traffic type by selecting the appropriate radio button:

- RX
- TX
- All.


The information displayed depends on the selected **Traffic Category** field. Column headings will change to reflect the traffic category.

Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Signal Analysis

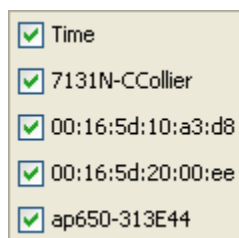
The **Signal Analysis** tab displays a device's signal strength (in dBm) as measured by various Sensors.

Time	7131N-CCollier [a.b.g]	10.59.36.46 [a.b.g]	10.59.36.37 [a.b.g]	ap650-313E44 [a.b.g]
<b>Totals</b>				
4/20/11 8:11 AM	-61	-47	-65	
4/20/11 8:12 AM	-62	-44	-66	
4/20/11 8:13 AM	-62	-46	-66	
4/20/11 8:14 AM	-63	-44	-66	
4/20/11 8:15 AM	-63	-44	-66	
4/20/11 8:16 AM	-62	-44	-66	
4/20/11 8:17 AM	-63	-44	-66	
4/20/11 8:18 AM	-62	-44	-66	
4/20/11 8:19 AM	-62	-44	-66	
4/20/11 8:20 AM	-63	-45	-66	
4/20/11 8:21 AM	-62	-45	-66	
4/20/11 8:22 AM	-62	-46	-66	
4/20/11 8:23 AM	-62	-45	-67	
4/20/11 8:24 AM	-61	-44	-66	
4/20/11 8:25 AM	-61	-44	-66	
4/20/11 8:26 AM	-61	-43	-66	
4/20/11 8:27 AM	-61	-42	-66	
4/20/11 8:28 AM	-61	-42	-66	
4/20/11 8:29 AM	-61	-44	-66	

The table view will have a **Time** column and a column for each Sensor that has seen the device being analyzed.


Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

An option is included to remove empty rows. When selected, any row with no data is removed from the table. Click the **Remove empty rows** checkbox to select the option.

You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Sensors

The following eight tabs are available for Sensors:

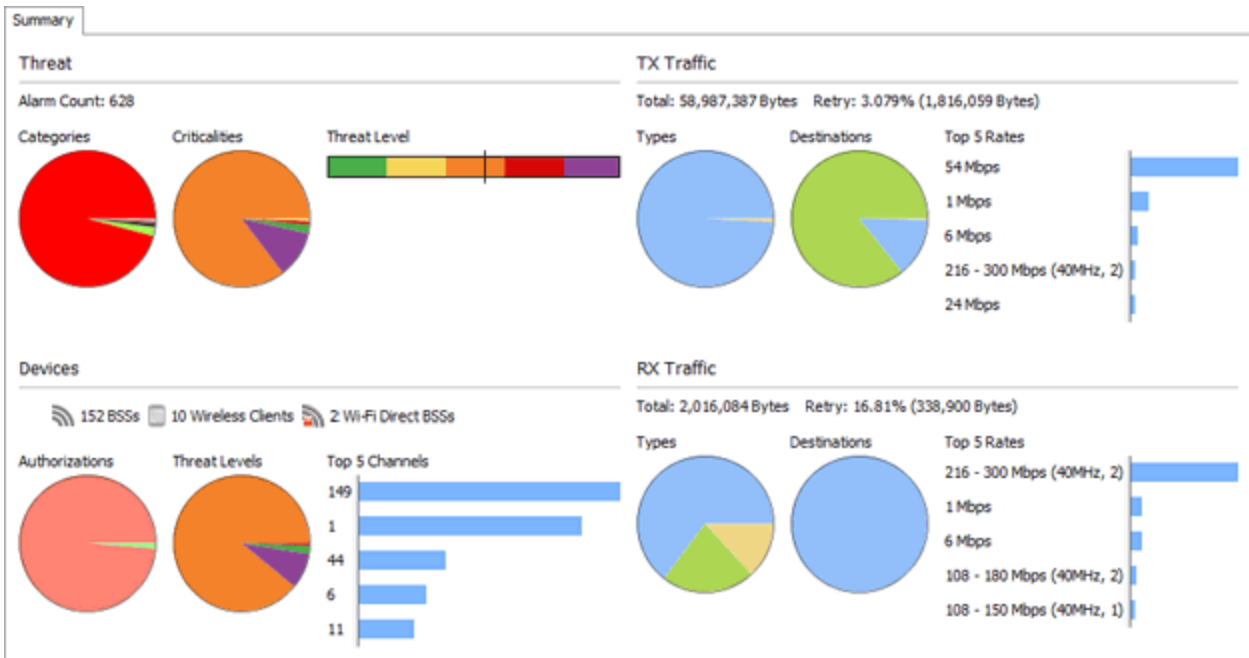
- Summary
- Threat Analysis
- Threat Breakdown
- Traffic Analysis

- Traffic Breakdown
- Channel Analysis
- Device Analysis
- Bandwidth Analysis.

Each tab is discussed as a separate topic.

**Summary**

The **Summary** tab shows high-level information about the threat level, device counts and traffic for the entire scope over the selected time range. Each time you access Forensic Analysis for Sensors the **Summary** tab is the first one displayed.



## Threat Analysis

The **Threat Analysis** tab displays a table of alarms generated by the device being analyzed.

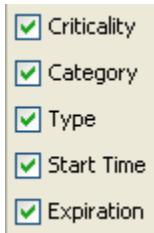
Criticality	Category	Type	Start Time	Expiration
Severe (100)	Rogue Exploit	Rogue Bridge	Before Time Range	After Time Range
Severe (100)	Rogue Exploit	Rogue AP on Wired Network	Before Time Range	After Time Range
Severe (100)	Rogue Exploit	Rogue AP on Switch	Before Time Range	After Time Range
Severe (100)	Rogue Exploit	Virtual Wifi Detected	Before Time Range	After Time Range
Severe (90)	Rogue Exploit	Rogue Client on Switch	Before Time Range	After Time Range
Critical (85)	Authentication	Extended Authentication Modes ...	Before Time Range	After Time Range
Major (50)	Authorization Violation	Unsanctioned Bridge	Before Time Range	After Time Range
Major (50)	Authorization Violation	Unsanctioned BSS	Before Time Range	After Time Range
Major (50)	Impersonation Attacks	BSS and Wireless Client Using th...	Before Time Range	After Time Range
Major (40)	Active Attacks	SSID SQL Injection Attack	4/13/11 2:28 PM	4/13/11 7:32 PM
Major (40)	Fuzzing	Duplicate Information Elements	Before Time Range	After Time Range

The information displayed is as follows:

Column	Description
Criticality	The color designation and name for the threat level, as follows: <ul style="list-style-type: none"> <li>Severe—Serious alarms that may have catastrophic effects on your WLAN.</li> <li>High/Critical—Serious alarms on devices that require immediate attention.</li> <li>Elevated/Major—Potentially serious alarms on devices that require priority attention.</li> <li>Guarded/Minor—Potential problem alarms on devices that may develop into worse issues if left alone.</li> <li>Safe/Low—Devices that pose no immediate threat to your WLAN network.</li> </ul>
Category	The type of category that the alarm falls under.
Type	The specific type of alarm, providing detailed information as to what generated the alarm in the first place.
Start Time	The date and time group of when the alarm first occurred.
Expiration	The date and time group of when the alarm will expire. The alarm can be an ongoing alarm which never expires.

Column display and arrangement can be customized as follows:

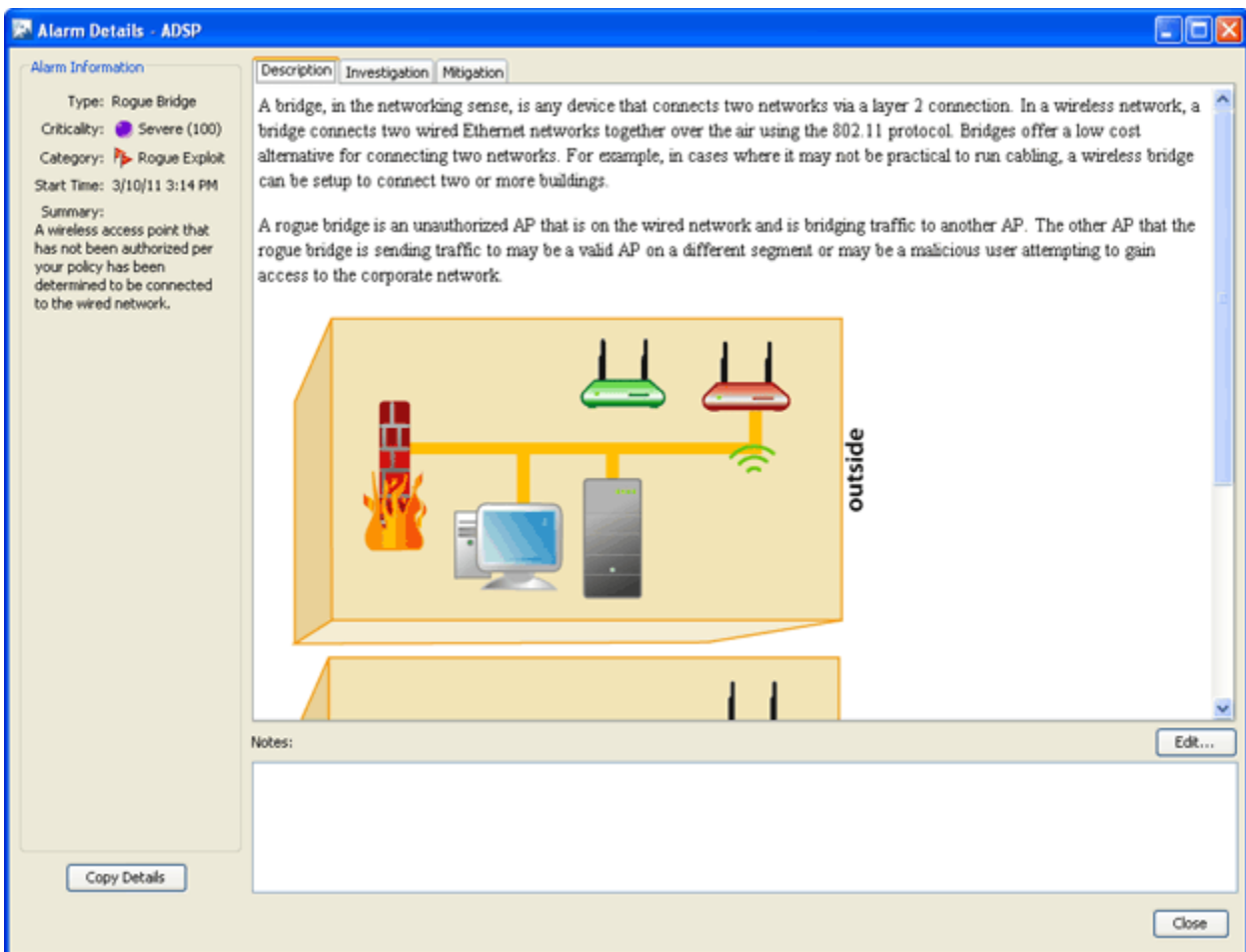
- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm.



You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.



### Threat Breakdown

The **Threat Breakdown** tab displays a table of the threat level for items within the selected scope.

The screenshot shows a 'Threat Breakdown' window with a title bar 'Threat Breakdown' and a subtitle 'Top 100 devices (by threat)'. The table has columns for 'Time' and eight device threat levels. Each device column has a header with a Wi-Fi icon and a device name: Cisco:75:55:6, Motorola:4b:7, Symbol:4e:e8, Symbol:ce:73, Motorola:4b:7, Motorola:4b:7, Symbol:ea:f3, and Symbol:6e:4b. The 'Totals' row shows a value of 100 for each device. The 'Time' column lists dates from 4/13/11 8:28 AM to 4/13/11 8:46 AM. The table is scrollable, with a vertical scrollbar on the right.

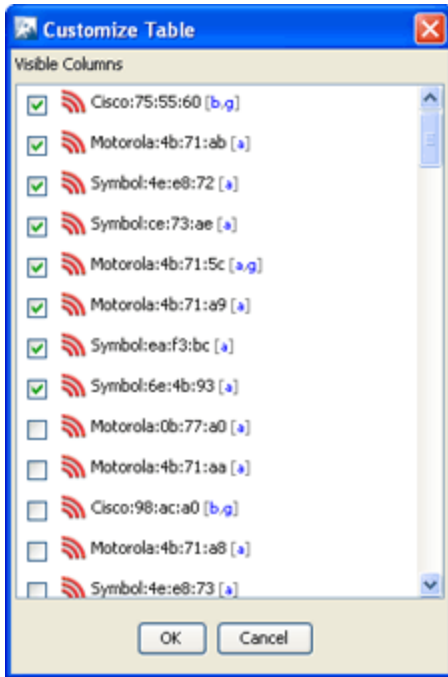
Time	Cisco:75:55:6	Motorola:4b:7	Symbol:4e:e8	Symbol:ce:73	Motorola:4b:7	Motorola:4b:7	Symbol:ea:f3	Symbol:6e:4b
Totals	100	100	100	100	100	100	100	100
4/13/11 8:28 AM	100	100	100	100	100	100	100	100
4/13/11 8:29 AM	100	100	100	100	100	100	100	100
4/13/11 8:30 AM	100	100	100	100	100	100	100	100
4/13/11 8:31 AM	100	100	100	100	100	100	100	100
4/13/11 8:32 AM	100	100	100	100	100	100	100	100
4/13/11 8:33 AM	100	100	100	100	100	100	100	100
4/13/11 8:34 AM	100	100	100	100	100	100	100	100
4/13/11 8:35 AM	100	100	100	100	100	100	100	100
4/13/11 8:36 AM	100	100	100	100	100	100	100	100
4/13/11 8:37 AM	100	100	100	100	100	100	100	100
4/13/11 8:38 AM	100	100	100	100	100	100	100	100
4/13/11 8:39 AM	100	100	100	100	100	100	100	100
4/13/11 8:40 AM	100	100	100	100	100	100	100	100
4/13/11 8:41 AM	100	100	100	100	100	100	100	100
4/13/11 8:42 AM	100	100	100	100	100	100	100	100
4/13/11 8:43 AM	100	100	100	100	100	100	100	100
4/13/11 8:44 AM	100	100	100	100	100	100	100	100
4/13/11 8:45 AM	100	100	100	100	100	100	100	100
4/13/11 8:46 AM	100	100	100	100	100	100	100	100

The information displayed is as follows:


Column	Description
Time	The date and time group of the threat level.
Device Threat Level	A column for each device considered a threat displaying a numerical value of the threat level.

Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area, selecting **Customize**, and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Traffic Analysis

The **Traffic Analysis** tab displays a table of traffic transmitted and received by devices in the selected scope.

Traffic Analysis						
Traffic Category: <b>Retry</b>	Traffic Type: <input type="radio"/> TX <input type="radio"/> RX <input checked="" type="radio"/> All		(Traffic in Bytes)			
Time	TX % Retry	RX % Retry	TX Retryable Data	TX Retry	RX Retryable Data	RX Retry
<b>Totals</b>	2.555%	32.227%	5,817,900	148,651	574,819	185,246
4/11/11 8:54 AM	0%	0%	0	0	0	0
4/11/11 8:55 AM	0%	0%	0	0	0	0
4/11/11 8:56 AM	0%	0%	0	0	0	0
4/11/11 8:57 AM	0%	41.896%	63	0	578	241
4/11/11 8:58 AM	0%	0%	228	0	0	0
4/11/11 8:59 AM	0%	0%	0	0	0	0
4/11/11 9:00 AM	0%	0%	0	0	0	0
4/11/11 9:01 AM	0.842%	0%	52,038	438	0	0
4/11/11 9:02 AM	0%	0%	0	0	0	0
4/11/11 9:03 AM	0%	35.227%	106	0	10,509	3,702
4/11/11 9:04 AM	0%	13.863%	0	0	1,082	150
4/11/11 9:05 AM	0%	0%	76	0	0	0
4/11/11 9:06 AM	0%	0%	0	0	0	0
4/11/11 9:07 AM	0%	0%	76	0	0	0
4/11/11 9:08 AM	0%	0%	0	0	0	0
4/11/11 9:09 AM	0%	0%	0	0	0	0
4/11/11 9:10 AM	0%	0%	0	0	0	0
4/11/11 9:11 AM	0%	0%	0	0	0	0

The **Traffic Category** field determines the type of data displayed in the table. You can change the traffic category by selecting one of the following categories from the **Traffic Category** drop-down menu:

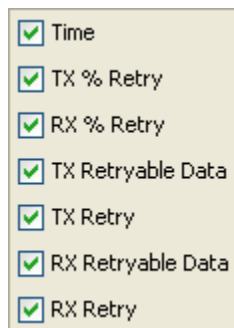
- Ad-Hoc
- Control Details
- Data Details
- Destinations
- EAP Details
- Encryption Details
- Management Details
- Rates
- Retry (default)
- Types.

The **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types. You can change the traffic type by selecting the appropriate radio button:


- RX
- TX
- All.

The **Time** column is included in every traffic category. The other columns vary according to selected traffic category. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

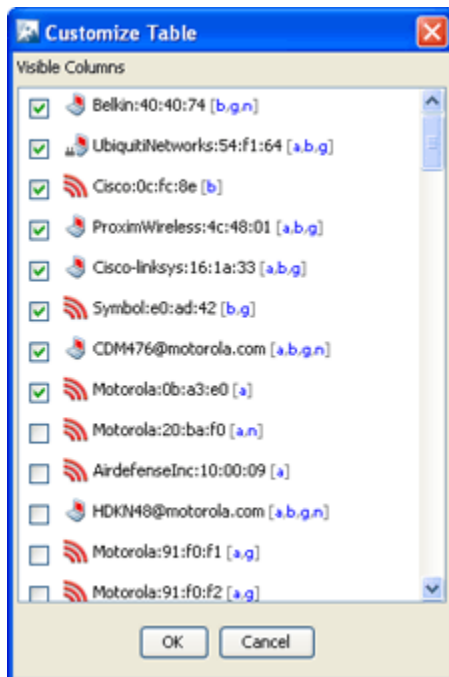
## Traffic Breakdown

The **Traffic Breakdown** tab displays a table of the total traffic for devices within the selected scope.

Traffic Breakdown								
Top 100 devices (by traffic).								
Time	Belkin:40:40:7	UbiquitiNetwo	Cisco:0c:fc:8e	ProximWireles	Cisco-linksys:1	Symbol:e0:ad	CDM476@mot	Motorola:0b:e
<b>Totals</b>	50,660,137	45,804,631	33,422,035	30,834,567	30,305,676	19,152,325	13,535,872	9,327,061
4/13/11 8:28 AM	0	0	0	0	0	0	0	0
4/13/11 8:29 AM	35,051	23,542	34,025	26,423	24,362	9,394	0	408
4/13/11 8:30 AM	48,411	25,068	25,146	17,210	24,013	13,086	0	12,011
4/13/11 8:31 AM	30,964	21,426	33,672	16,462	16,121	9,863	0	7,016
4/13/11 8:32 AM	24,105	24,733	20,581	20,091	9,973	7,050	0	1,015
4/13/11 8:33 AM	14,039	31,323	16,258	14,444	9,466	5,305	0	9,216
4/13/11 8:34 AM	39,415	28,360	19,725	23,010	5,182	7,780	0	12,818
4/13/11 8:35 AM	33,350	28,297	19,207	22,282	11,916	7,899	0	8,002
4/13/11 8:36 AM	23,336	28,364	19,687	25,497	12,759	7,082	0	1,801
4/13/11 8:37 AM	22,732	23,318	20,686	25,016	14,813	4,269	0	10,368
4/13/11 8:38 AM	25,121	30,787	19,840	17,114	12,441	6,405	0	4,378
4/13/11 8:39 AM	49,446	28,313	27,115	15,750	18,087	12,884	0	8,391
4/13/11 8:40 AM	31,973	22,531	32,198	15,862	23,389	11,084	0	230
4/13/11 8:41 AM	37,237	21,482	37,568	22,659	18,935	10,882	0	7,960
4/13/11 8:42 AM	25,023	21,966	35,845	13,700	30,279	11,771	0	5,875
4/13/11 8:43 AM	32,621	25,559	37,310	18,799	21,441	12,593	0	229
4/13/11 8:44 AM	31,739	21,972	44,389	24,301	18,015	14,045	0	870
4/13/11 8:45 AM	49,717	22,037	35,562	22,217	15,384	13,211	0	617
4/13/11 8:46 AM	28,724	18,498	37,642	23,098	17,750	12,502	0	230

The **Time** column is included in every traffic category. The first 8 items are shown in the other columns by default. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and selecting **Customize** to display the **Customize Table** popup window. Uncheck a checkbox for a column to hide that column.



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data** button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Channel Analysis

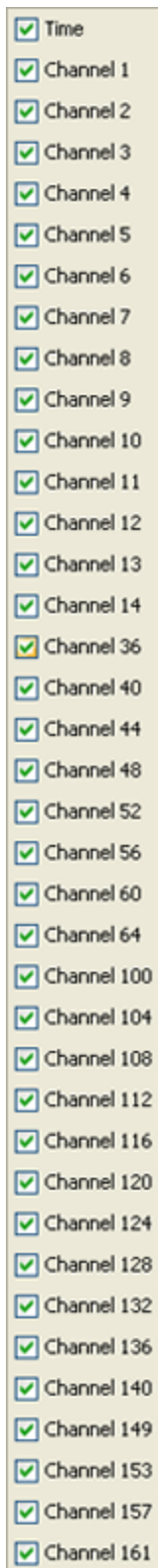
The **Channel Analysis** tab displays a table of the device count for each channel over time.

The screenshot shows the 'Channel Analysis' tab in a software interface. At the top, there are radio buttons for 'Device Type': 'Wireless Client' (selected), 'BSS', and 'All'. Below this is a table with 24 columns representing channels and multiple rows representing time intervals. The first row of data shows device counts for each channel: 2, 2, 3, 2, 2, 2, 2, 2, 2, 4, 2, 1, 1, 5, 2, 2, 1, 2, 2, 2, 1, 1, 1, 1, 1, 2, 5, 1, 2. Subsequent rows show mostly zeros, with some non-zero values scattered across the columns, such as a '1' in the 4th column of the 2nd row, a '1' in the 10th column of the 3rd row, and a '1' in the 14th column of the 4th row.


The **Device Type** field determines whether you see Channels for Wireless Clients, BSSs, or all devices in the table. You can change the device type by selecting the appropriate radio button.

The **Time** column is included in every device category. The other columns list device count of the individual channels. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and selecting **Customize** to display the **Customize Table** popup window. Uncheck a checkbox for a column to hide that column.



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### *Device Analysis*

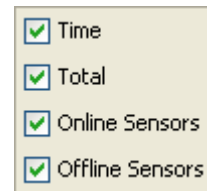
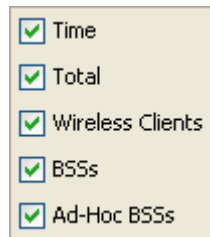
The **Device Analysis** tab displays a table of device counts for devices and Sensors.

The **Display Category** field determines whether you see a device count for Devices or Sensors. Devices may be Wireless Clients, BSSs, or Ad-Hoc BSSs. Sensors may be Online or Offline Sensors. You can change the display category by selecting the appropriate radio button:

- Devices
- Sensors.

The **Time** column is included in every display category. The other columns vary according to the selected display category. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

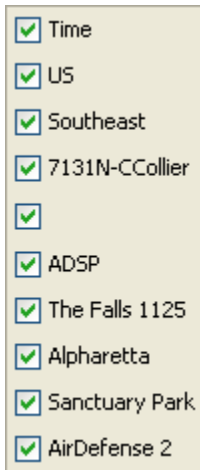
You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### *Bandwidth Analysis*


The **Bandwidth Analysis** tab displays a table of the wired bandwidth usage of the Sensors and related network levels.

A **Time** category is included in the table along with a column for each of the network levels and the Sensor being analyzed. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### APs

The following six tabs are available for APs:

- Summary
- Device Info
- Threat Analysis
- Adoption History
- Radio Analysis
- Radio Info.

Each tab is discussed as a separate topic.



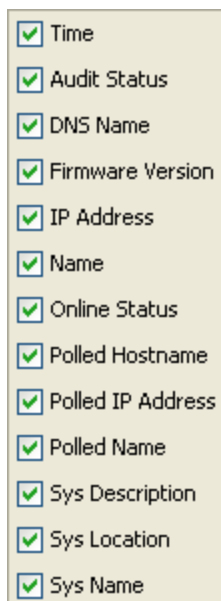


The information displayed is as follows:

Column	Description
Time	The date and time of day when the AP was seen.
Audit Status	The status of the last audit (compliant or non-compliant).
DNS Name	The DNS name assigned to the AP.
Firmware Version	The current firmware version installed on the AP.
IP Address	The AP's Internet Protocol address.
Name	The name of the AP. The name is specified by a user through the ADSP GUI.
Online Status	The online/offline status of the AP.
Polled Hostname	The hostname that is pulled from the AP by ADSP either upon import/discovery of the AP or when ADSP does a data poll.
Polled IP Address	The IP address that is pulled from the AP by ADSP either upon import/discovery of the AP or when ADSP does a data poll.
Polled Name	The device name that is pulled from the AP by ADSP either upon import/discovery of the AP or when ADSP does a data poll.
Sys Description	A description of the AP. This information is obtain from an import/discovery of the AP or when ADSP does a data poll.
Sys Location	The AP's location. This information is obtain from an import/discovery of the AP or when ADSP does a data poll.
Sys Name	The AP's name. This information is obtain from an import/discovery of the AP or when ADSP does a data poll.


Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



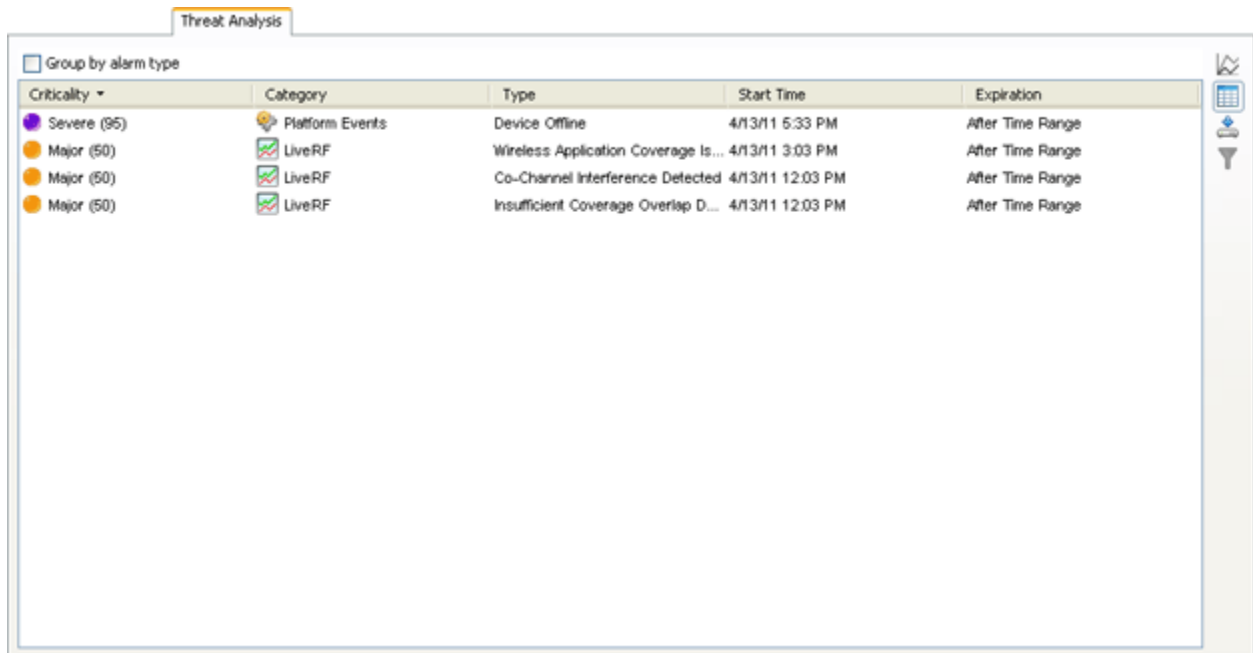
- Rearrange columns by clicking on a column heading and dragging it to a new position.

The table may be shown with one row per minute or one row for every change in the value of a particular column (category). Click the appropriate radio button in the top, left side of the **Device Info** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.






### Threat Analysis

The **Threat Analysis** tab displays a table of alarms generated by the AP being analyzed.



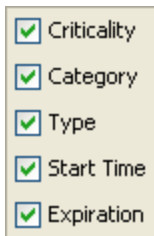
Criticality	Category	Type	Start Time	Expiration
Severe (95)	Platform Events	Device Offline	4/13/11 5:33 PM	After Time Range
Major (50)	LiveRF	Wireless Application Coverage Is...	4/13/11 3:03 PM	After Time Range
Major (50)	LiveRF	Co-Channel Interference Detected	4/13/11 12:03 PM	After Time Range
Major (50)	LiveRF	Insufficient Coverage Overlap D...	4/13/11 12:03 PM	After Time Range

The information displayed is as follows:

Column	Description
Criticality	The color designation and name for the threat level, as follows: <ul style="list-style-type: none"> <li>•  Severe—Serious alarms that may have catastrophic effects on your WLAN.</li> <li>•  High/Critical—Serious alarms on devices that require immediate attention.</li> <li>•  Elevated/Major—Potentially serious alarms on devices that require priority attention.</li> <li>•  Guarded/Minor—Potential problem alarms on devices that may develop into worse issues if left alone.</li> <li>•  Safe/Low—Devices that pose no immediate threat to your WLAN network.</li> </ul>
Category	The type of category that the alarm falls under.
Type	The specific type of alarm, providing detailed information as to what generated the alarm in the first place.
Start Time	The date and time group of when the alarm first occurred.
Expiration	The date and time group of when the alarm will expire. The alarm can be an ongoing alarm which never expires.

Column display and arrangement can be customized as follows:

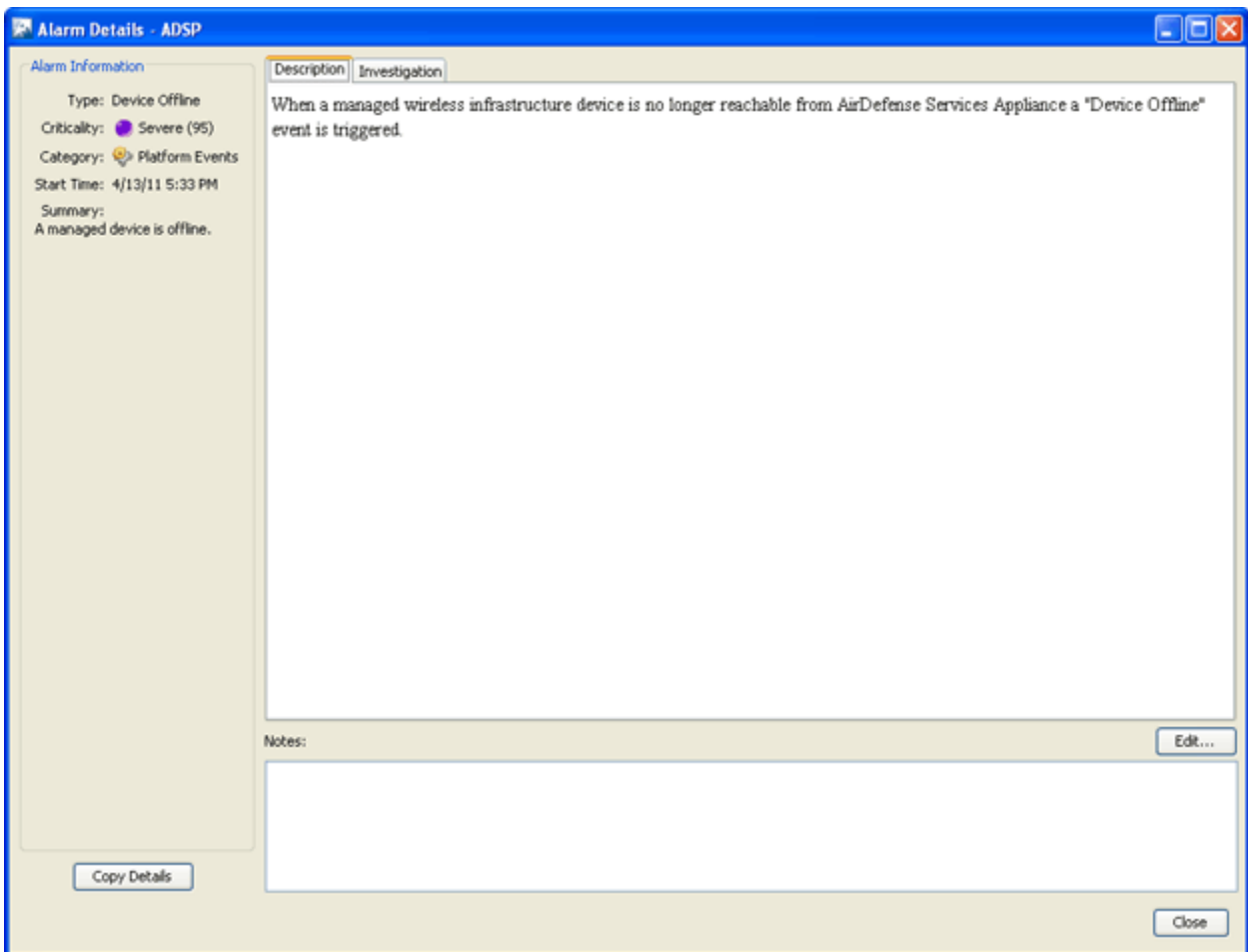
- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm.



You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Adoption History

The **Adoption History** tab displays a table of devices that have adopted an AP.

The screenshot shows a window titled "Adoption History" with a checkbox for "Group by associated device" which is unchecked. Below the checkbox is a table with the following data:

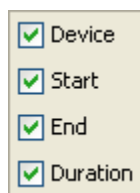
Device	Start	End	Duration
RFS4000-C Collier	Ongoing Adoption	4/13/11 8:28 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 8:33 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 8:38 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 8:43 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 8:48 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 8:53 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 8:58 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:03 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:08 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:13 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:18 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:23 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:28 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:33 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:38 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:43 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:48 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:53 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 9:58 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/13/11 10:03 AM	11.5 days

The information displayed is as follows:

Column	Description
Device	The name of the device that adopted the AP.
Start	The date and time when the adoption first occurred. This can be an ongoing adoption.
End	The date and time when the adoption last occurred.
Duration	The amount of time that the adoption has lasted.


Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by associated device** field allows you to group devices of the same type together.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Radio Analysis

The **Radio Analysis** tab displays information that can be used to analyze your AP's radios.

Time	00:15:70:c7:c2:30	00:15:70:c5:9f:40	Total
Totals	0	0	0

The information displayed varies depending on the selected radio category. The categories are:

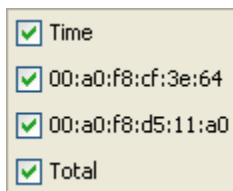
- Noise—Displays the average noise seen on each radio in dBm.
- Power—Displays the average power used by each radio over time.
- Retry—Displays the total number of retries that has occurred from data being retransmitted.
- Traffic (default)—Displays the total traffic seen on each radio in bytes.

The **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types. You can change the traffic type by selecting the appropriate radio button:


- RX
- TX
- All.

The **Time** column is included in every traffic category while the other columns reflect the MAC address of the radio which display the averages or totals of the traffic. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Radio Info

The **Radio Info** tab displays AP radio information recorded at the displayed time.

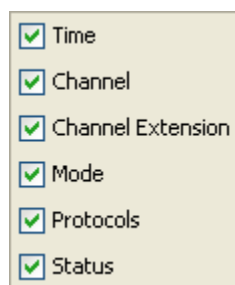
Time	Channel	Channel Extension	Mode	Protocols	Status
4/11/11 10:11 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:12 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:13 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:14 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:15 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:16 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:17 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:18 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:19 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:20 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:21 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:22 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:23 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:24 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:25 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:26 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:27 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled
4/11/11 10:28 AM	36(5180MHz)	None	Infrastructure	a,n	Enabled

The information displayed is as follows:

Column	Description
Time	The date and time of day when the information was recorded.
Channels	The WLAN broadcast channel for the device.
Channel Extension	The channel extension being used if any.
Mode	The mode the AP radio is operating in (Infrastructure or Sensor).
Protocols	The protocols being used by the AP radio (a,b,g,n).
Status	The status of the AP radio (enabled or disabled).


Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

The table may be shown with one row per minute or one row for every change in the value of a particular column (category) chosen from the drop-down menu. Click the appropriate radio button in the top, left side of the **Radio Info** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Switches

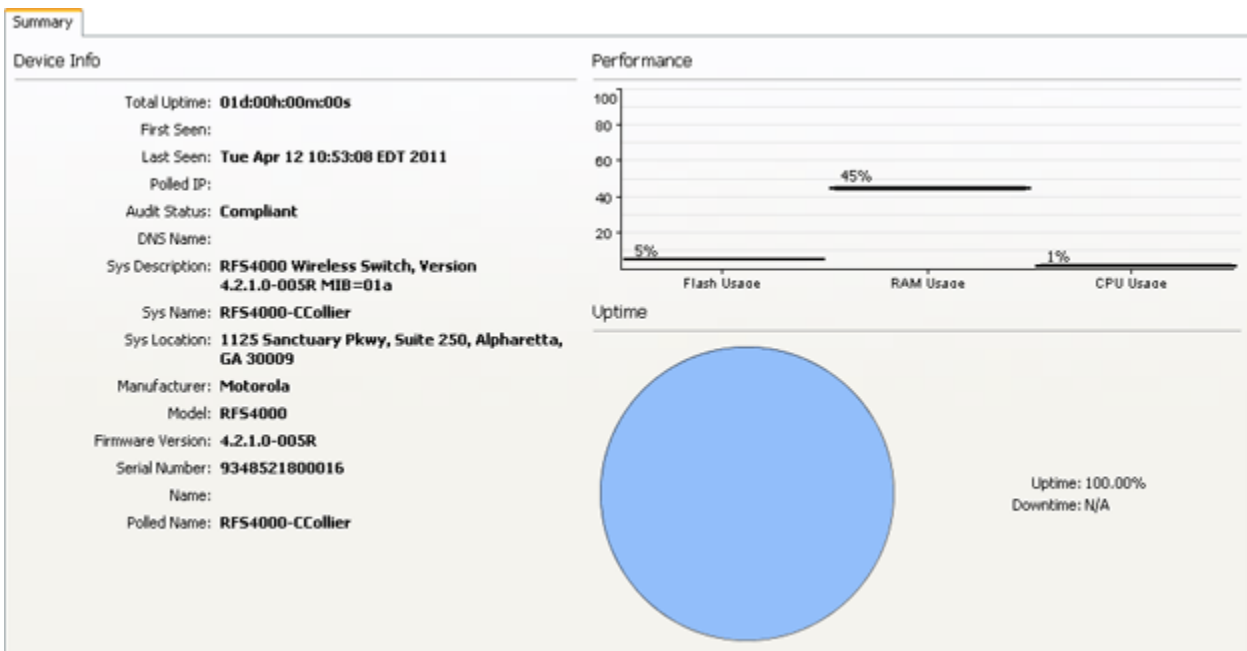
The following five tabs are available for Switches:

- Summary
- Device Info
- Threat Analysis
- Adoption History
- Performance Analysis.

Each tab is discussed as a separate topic.

### Summary

The **Summary** tab displays summary and performance information about the Switch as well as the uptime and downtime of the Switch. Each time you access Forensic Analysis for Switches the **Summary** tab is the first one displayed.





## Device Info

The **Device Info** tab displays the current settings for the Switch being analyzed.

Time	Audit St...	DNS Name	Firmwar...	IP Address	Name	Online S...	Polled H...	Polled I...	Polled N...	Sys Des...	Sys Loc...	Sys Name
4/11/11 10...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 10...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 10...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 10...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 10...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...
4/11/11 11...	Compliant		4.2.1.0-005R	172.17.25...		Online			RFS4000...	RFS4000 ...	1125 Sanc...	RFS4000...

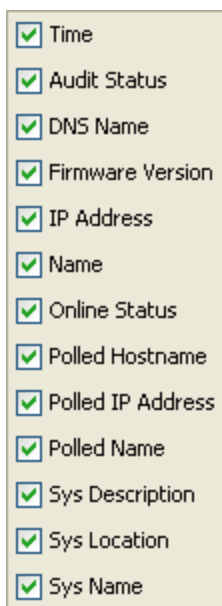
The information displayed is as follows:

Column	Description
Time	The date and time of day when the Switch was seen.
Audit Status	The status of the last audit (compliant or non-compliant).
DNS Name	The DNS name assigned to the Switch.
Firmware Version	The current firmware version installed on the Switch.
IP Address	The Switch's Internet Protocol address.
Name	The name of the Switch. The name is specified by a user through the Switch's properties.
Online Status	The online/offline status of the Switch.
Polled Hostname	The hostname that is pulled from the Switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.
Polled IP Address	The IP address that is pulled from the Switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.
Polled Name	The device name that is pulled from the Switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.

Column	Description
Sys Description	A description of the Switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.
Sys Location	The location of the Switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.
Sys Name	The name of the Switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.


Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

The table may be shown with one row per minute or one row for every change in the value of a particular column (category) selected from the drop-down menu. Click the appropriate radio button in the top, left side of the **Device Info** tab.

You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Threat Analysis

The **Threat Analysis** tab displays a table of alarms generated by the Switch being analyzed.

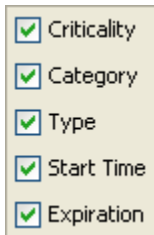
Criticality	Category	Type	Start Time	Expiration
Severe (95)	Platform Events	Device Offline	4/15/11 7:33 AM	After Time Range

The information displayed is as follows:

Column	Description
Criticality	The color designation and name for the threat level, as follows: <ul style="list-style-type: none"> <li>Severe—Serious alarms that may have catastrophic effects on your WLAN.</li> <li>High/Critical—Serious alarms on devices that require immediate attention.</li> <li>Elevated/Major—Potentially serious alarms on devices that require priority attention.</li> <li>Guarded/Minor—Potential problem alarms on devices that may develop into worse issues if left alone.</li> <li>Safe/Low—Devices that pose no immediate threat to your WLAN network.</li> </ul>
Category	The type of category that the alarm falls under.
Type	The specific type of alarm, providing detailed information as to what generated the alarm in the first place.
Start Time	The date and time group of when the alarm first occurred.
Expiration	The date and time group of when the alarm will expire. The alarm can be an ongoing alarm which never expires.

Column display and arrangement can be customized as follows:

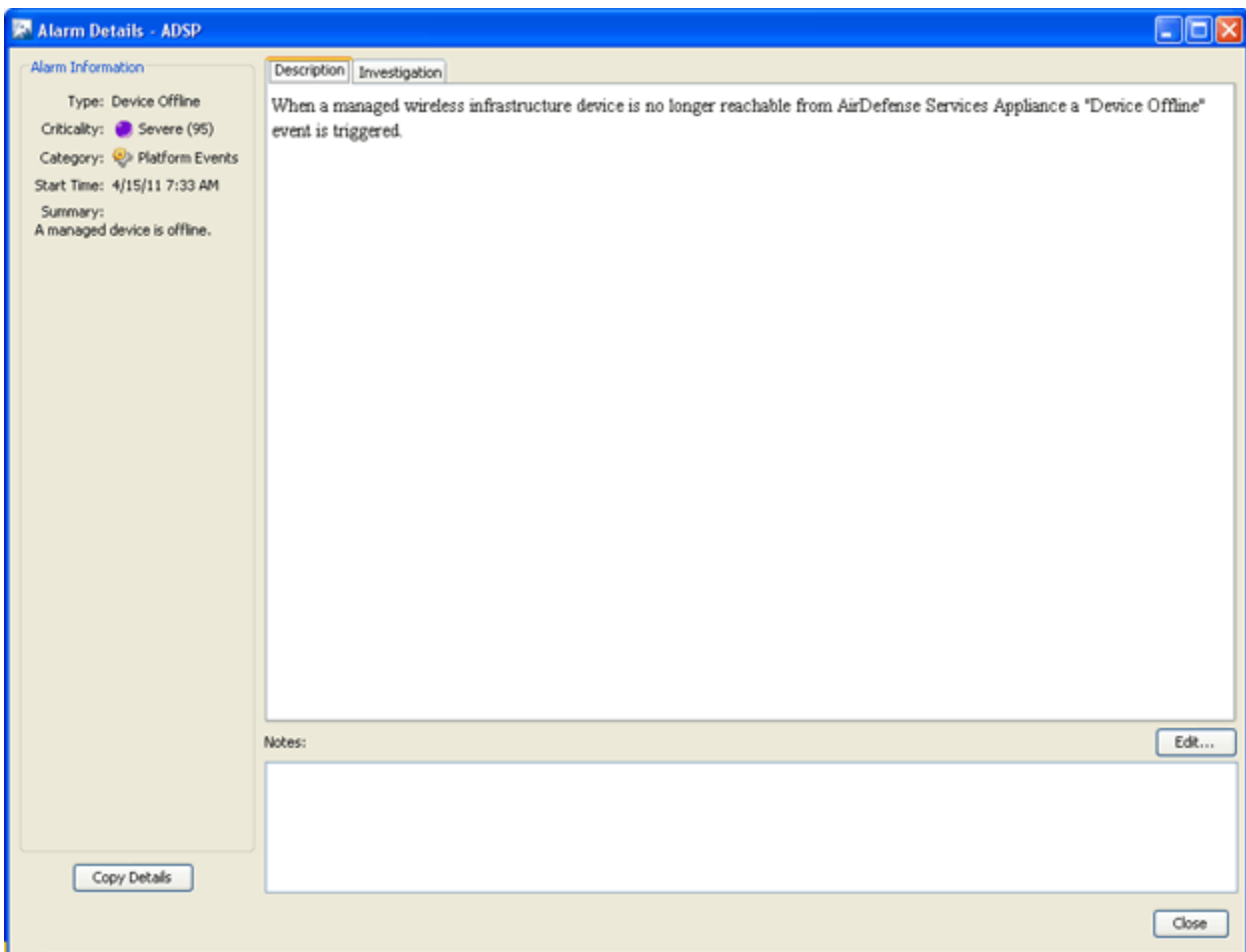
- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm.



You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Adoption History

The **Adoption History** tab displays a table of devices that the Switch has adopted.

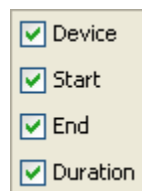
Device	Start	End	Duration
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 10:55 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 10:58 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:03 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:08 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:13 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:18 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:23 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:28 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:33 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:38 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:43 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:48 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:53 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 11:58 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 12:03 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 12:08 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 12:13 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 12:18 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 12:23 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/11/11 12:28 PM	11.5 days

The information displayed is as follows:

Column	Description
Device	The name of the device that the Switch adopted.
Start	The date and time when the adoption first occurred. This can be an ongoing adoption.
End	The date and time when the adoption last occurred.
Duration	The amount of time that the adoption has lasted.


Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



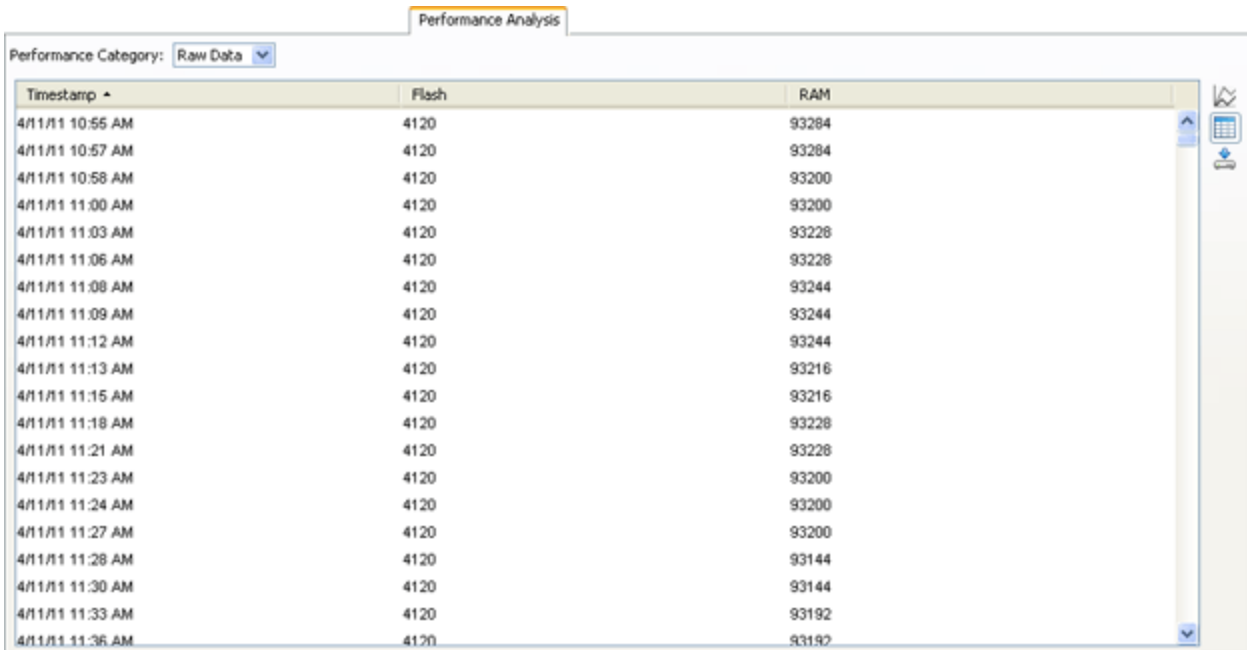
- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by associated device** field allows you to group devices of the same type together.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Performance Analysis

The **Performance Analysis** tab displays a table of performance raw data and usage percentages for a Switch.



Performance Category: Raw Data

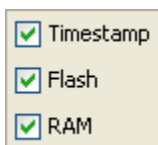
Timestamp	Flash	RAM
4/11/11 10:55 AM	4120	93284
4/11/11 10:57 AM	4120	93284
4/11/11 10:58 AM	4120	93200
4/11/11 11:00 AM	4120	93200
4/11/11 11:03 AM	4120	93228
4/11/11 11:06 AM	4120	93228
4/11/11 11:08 AM	4120	93244
4/11/11 11:09 AM	4120	93244
4/11/11 11:12 AM	4120	93244
4/11/11 11:13 AM	4120	93216
4/11/11 11:15 AM	4120	93216
4/11/11 11:18 AM	4120	93228
4/11/11 11:21 AM	4120	93228
4/11/11 11:23 AM	4120	93200
4/11/11 11:24 AM	4120	93200
4/11/11 11:27 AM	4120	93200
4/11/11 11:28 AM	4120	93144
4/11/11 11:30 AM	4120	93144
4/11/11 11:33 AM	4120	93192
4/11/11 11:36 AM	4120	93192

The **Performance Category** field determines what information is displayed in the table. You can change the performance category by making a selection from the drop-down menu:


- Raw Data
- Percentage.

The **Timestamp** column is included in every performance category. The other columns vary according to the selected display category. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Advanced Forensic Analysis

✓ **NOTE** Advanced Forensic Analysis requires an Advanced Forensic license for access.

When installed, Advanced Forensic Analysis replaces the basic Forensic Analysis that is included in the Enterprise application. Advanced Forensic Analysis has all the features of the basic Forensic Analysis plus some really useful enhancements. Advanced Forensic Analysis has two parts:

- Scope Based Forensic Analysis
- Device Based Forensic Analysis.

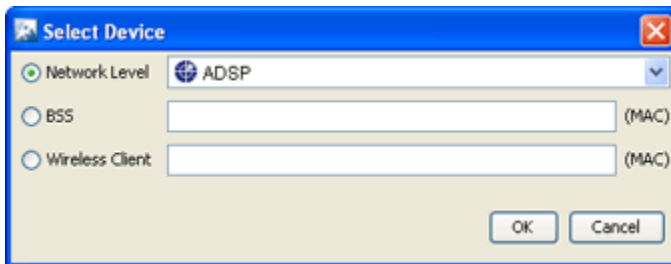
The extra features include:

- 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).

### *Scope Based*

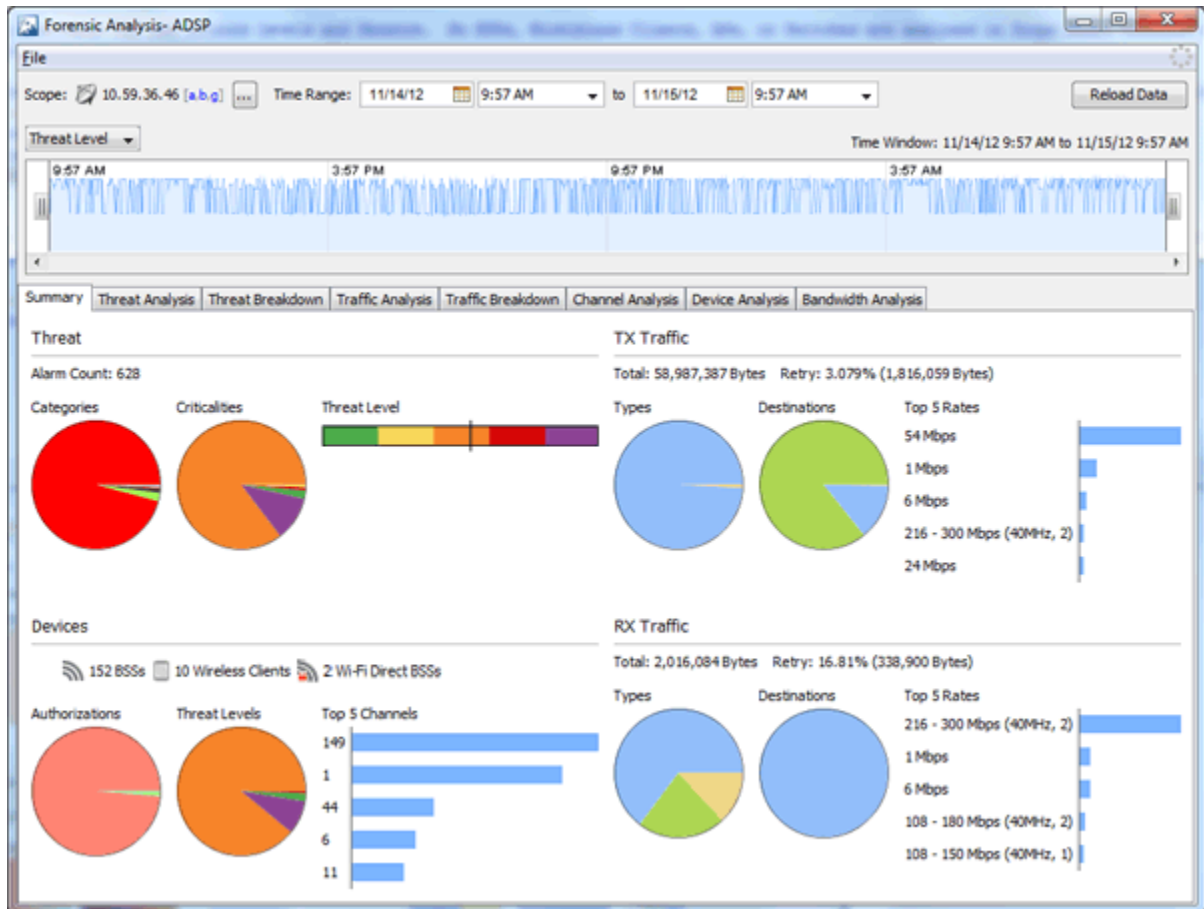
Scope Based Forensic Analysis is only available for the network levels and Sensors. No BSSs, Wireless Clients, APs, or Switches are analyzed in Scope Based Forensic Analysis. You initiate Scope Based Forensic Analysis as follows:

1. Select **Menu > Forensic Analysis**. The following popup window displays.



2. From the **Network Level** drop-down menu, select a network level or Sensor.

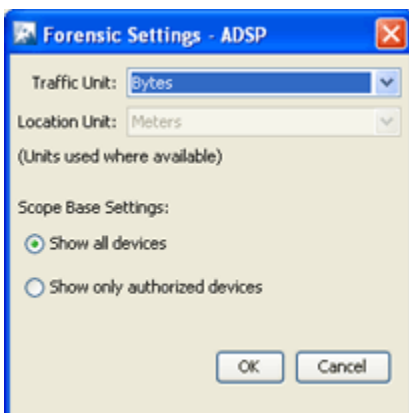
- Click OK. The Forensic Analysis window displays.



### Common Area

#### Forensic Settings

The Forensic Settings are used to set the Traffic Units and to select whether you want to **Show all devices** or **Show only authorized devices**. To change a setting, click the **File** menu and then select **Settings**.



Click the Traffic Unit drop-down menu to change the traffic units. Your choices are:

- Frames
- Bytes



- KBytes
- MBytes
- GBytes.


Click the appropriate radio button to select **Show all devices** or **Show only authorized devices**.

### Scope Field

The **Scope** field displays the Scope that you have chosen to analyze.

### Switch Devices

You can switch to another level in the Network Tree as follows:

1. Click the **Select Device**— button. The **Select Device** popup will display.




2. Select another level from the drop-down menu.

✓ **NOTE** You can also switch to Device Based Forensic Analysis if you know the MAC address of the device you want to analyze. Just select the Access Point or Wireless Client radio button and type in the MAC address (or paste the address if you have copied it).

3. Click **OK**.

### Time Range

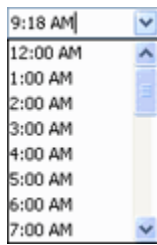
You can specify a time range (start and end) for your Forensic Analysis. To specify a time range:

1. Click the first Calendar— button to select a starting date. A calendar displaying the current month will display.



2. Select a day of the month from the calendar. You may switch months using the green arrow keys.

- Click the first **Time** drop-down button to select a starting time. A drop-down list will display showing a list of times by hours.

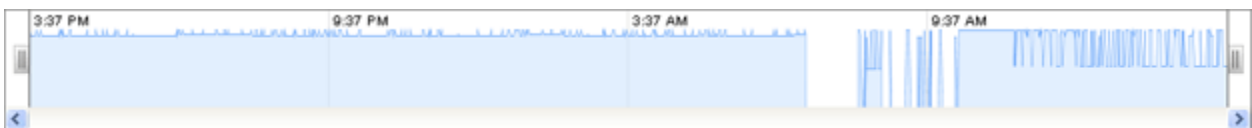


- Select a starting time from the list or type in a starting time.
- Click the second **Calendar** button to select an end date.
- Select a day of the month from the calendar.
- Click the second **Time** drop-down menu button to select an end time.
- Select an end time from the list or type in an end time.
- Click the **Reload Data** button. The **Time** window will change to reflect your time range.

### Time Window

The **Time** window has three different views:

- Threat Level (default)
- Total Traffic
- Device Count.



Each view is shown across the time range. There are sliders on each side of the **Time** window which controls the focus, allowing the user to select a portion of the loaded data to analyze. Just move the sliders in or out to adjust the focus.

### Tabs

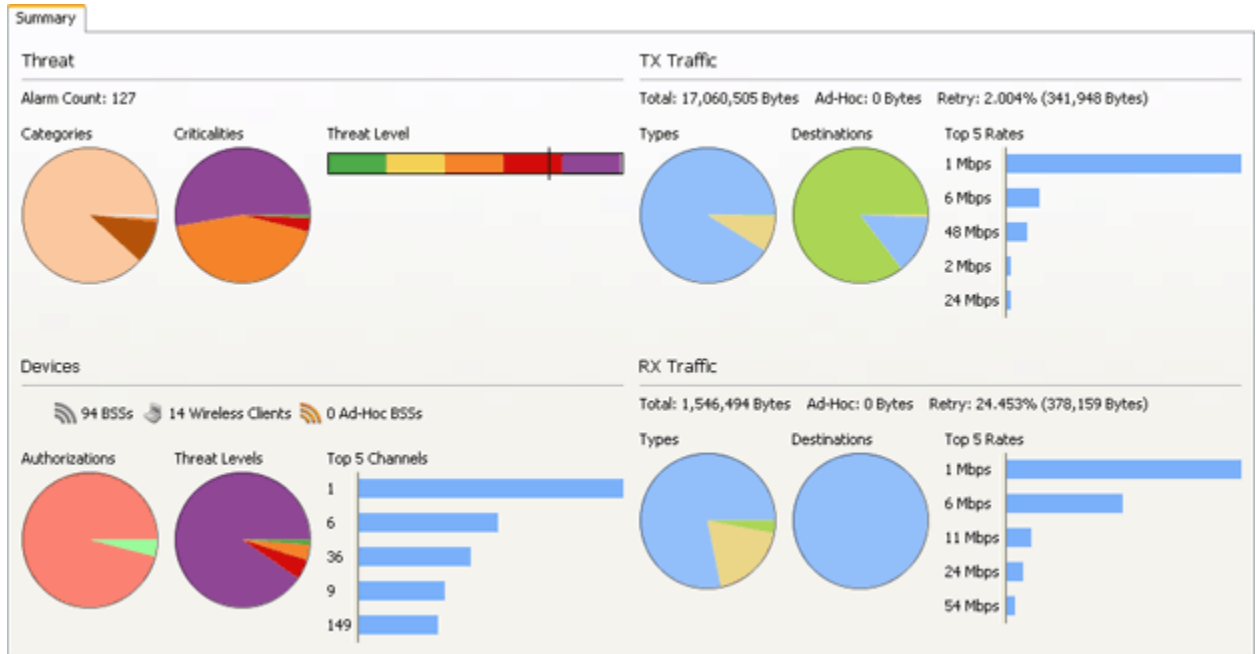
The tabs display the Forensic Analysis data. The following eight tabs are available:

- Summary
- Threat Analysis
- Threat Breakdown
- Traffic Analysis
- Traffic Breakdown
- Channel Analysis
- Device Analysis
- Bandwidth Analysis.

Each tab is discussed as a separate topic.

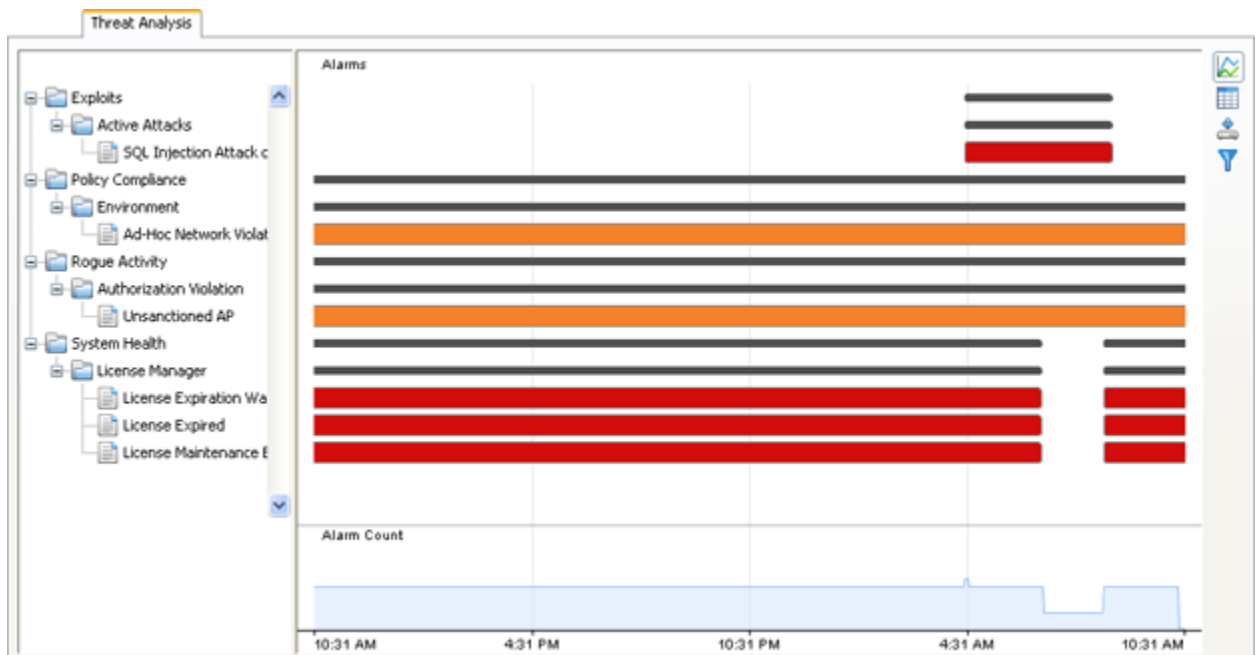
**Summary**


The **Summary** tab shows high-level information about the threat level, device counts and traffic for the entire scope over the selected time range. Each time you access Scope Based Forensic Analysis the **Summary** tab is the first one displayed.



**Threat Analysis**

The **Threat Analysis** tab provides a graphical and tabular view of active alarms. The first time you access the **Threat Analysis** tab the graphical view is displayed.




You can switch to the table view by clicking the **Data Table**— button.

Threat Analysis

Group by alarm type

Criticality	Category	Type	Start Time	Expiration
Critical (80)	License Manager	License Expired	Before Time Range	10/20/09 8:02 AM
Critical (80)	License Manager	License Expired	10/20/09 8:15 AM	After Time Range
Critical (70)	Active Attacks	SQL Injection Attack on SSID	10/20/09 4:26 AM	10/20/09 8:30 AM
Critical (70)	License Manager	License Maintenance Expired	Before Time Range	10/20/09 8:02 AM
Critical (70)	License Manager	License Maintenance Expired	10/20/09 8:15 AM	After Time Range
Critical (60)	License Manager	License Expiration Warning	Before Time Range	10/20/09 8:02 AM
Critical (60)	License Manager	License Expiration Warning	10/20/09 8:15 AM	After Time Range
Major (50)	Authorization Violation	Unsanctioned AP	Before Time Range	After Time Range
Major (30)	Environment	Ad-Hoc Network Violation Unaut...	Before Time Range	After Time Range

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

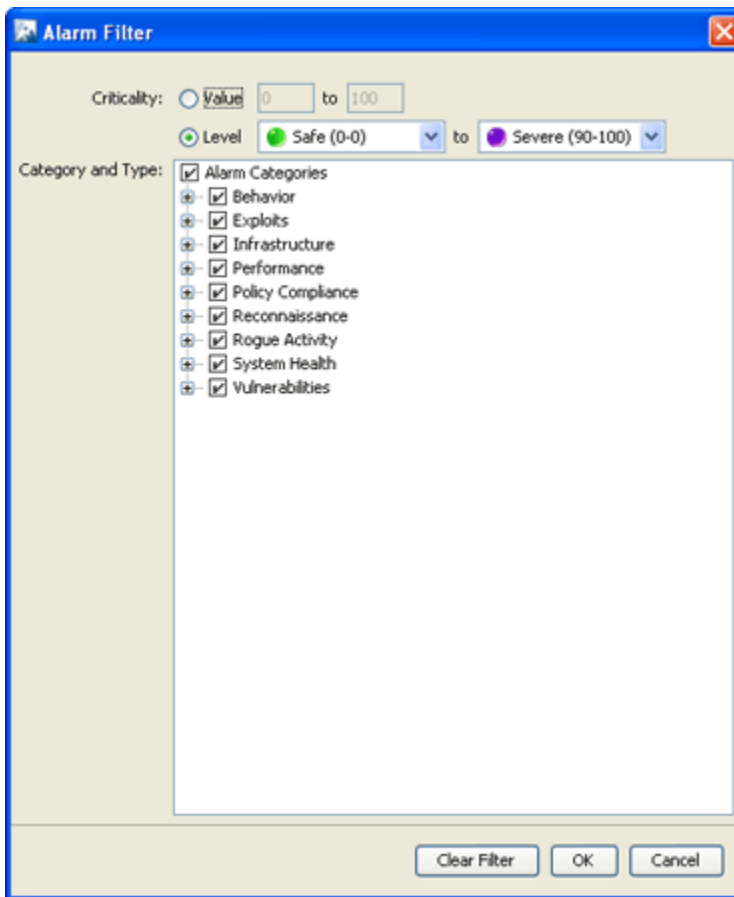
### Graphical View

The left side of the graphical view lists the available categories shown in the chart (right side). Click on the plus (+) or minus (-) sign to expand or collapse a category. The categories are:

- Behavior
- Exploits
- Infrastructure
- Performance
- Policy Compliance
- Reconnaissance
- Rogue Activity
- System Health
- Vulnerabilities.

If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Threat Analysis** tab.


Clicking the **Filter Data**— button displays an **Alarm Filter** window where you can filter the alarm data that is shown in graph.



Changes to the following fields will affect the filter:

Field	Description
Criticality	Change the criticality by entering exact values for a range or selecting a starting level and an ending level. To enter the values, select the <b>Value</b> radio button and then enter values from 1 to 100. To select levels, select the <b>Level</b> radio button and then select the levels using the drop-down menus.
Category and Type	By default, all categories and types are selected, to deselect a category or type, remove the checkmark in the checkbox next to the category or type. Click the plus (+) or minus (-) sign to expand or collapse a category.

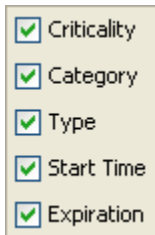
Click the **OK** button to activate your changes. The **Clear Filter** button will reset all fields back to their default state. The **Cancel** button will cancel any changes.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Table View

The table view has a column for each of the categories shown in the graphical view plus a Time category. Column display and arrangement can be customized as follows:


- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

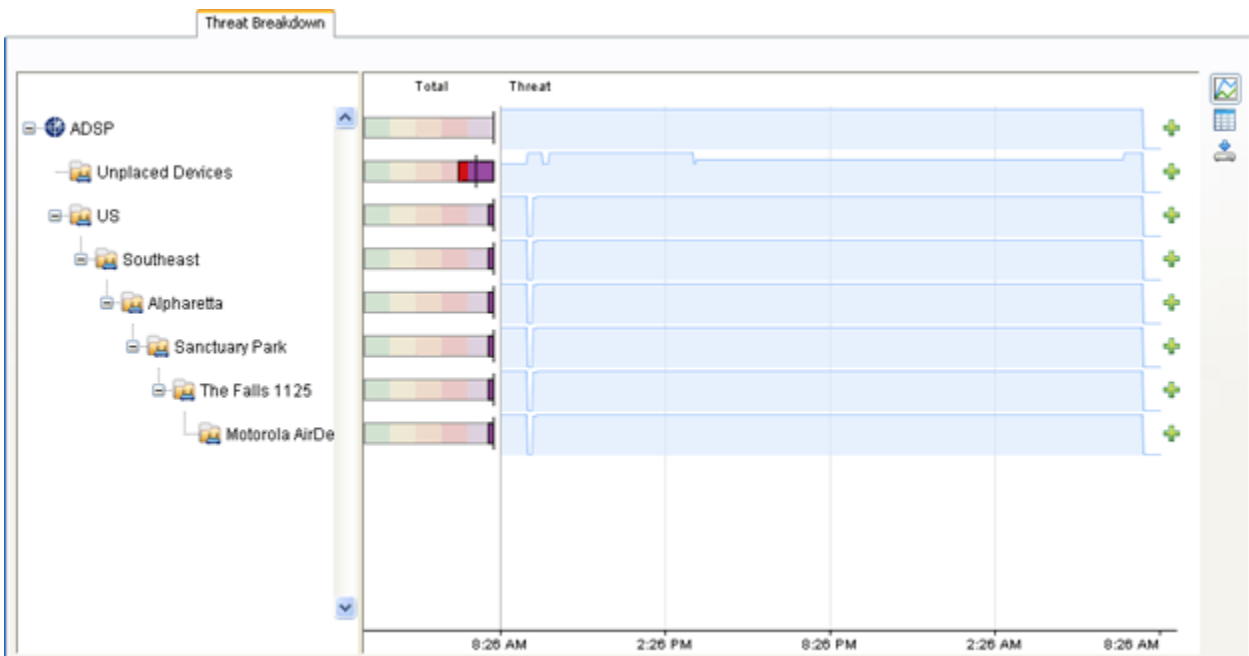
Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm. See the **Alarm Details** window topic for more information.


You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

The **Filter Data**— button works the same as it does in the graphical view.

### Threat Breakdown


The **Threat Breakdown** tab provides a graphical and tabular view of the threat level for items within the selected scope. The first time you access the **Threat Breakdown** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

Threat Breakdown

Time	ADSP	ADSP	US	Southeast	The Falls ...	Motorola ...	Alpharetta	Sanctuary...
Totals								
1/4/10 8:26 AM	100	100	100	100	100	100	100	100
1/4/10 8:27 AM	100	100	100	100	100	100	100	100
1/4/10 8:28 AM	100	100	100	100	100	100	100	100
1/4/10 8:29 AM	100	100	100	100	100	100	100	100
1/4/10 8:30 AM	100	100	100	100	100	100	100	100
1/4/10 8:31 AM	100	100	100	100	100	100	100	100
1/4/10 8:32 AM	100	100	100	100	100	100	100	100
1/4/10 8:33 AM	100	100	100	100	100	100	100	100
1/4/10 8:34 AM	100	100	100	100	100	100	100	100
1/4/10 8:35 AM	100	100	100	100	100	100	100	100
1/4/10 8:36 AM	100	100	100	100	100	100	100	100
1/4/10 8:37 AM	100	100	100	100	100	100	100	100
1/4/10 8:38 AM	100	100	100	100	100	100	100	100
1/4/10 8:39 AM	100	100	100	100	100	100	100	100
1/4/10 8:40 AM	100	100	100	100	100	100	100	100
1/4/10 8:41 AM	100	100	100	100	100	100	100	100
1/4/10 8:42 AM	100	100	100	100	100	100	100	100
1/4/10 8:43 AM	100	100	100	100	100	100	100	100
1/4/10 8:44 AM	100	100	100	100	100	100	100	100

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.



### Graphical View


Depending on the selected Scope, the graphical view displays forensic data as follows:

- If the selected scope is the entire System, the graph shows threat level for all network levels in the system.
- If the selected scope is a Country, the graph shows threat level for Region, City, Campus, Building, and Floor network levels for the country.
- If the selected scope is a Region, the graph shows threat level for City, Campus, Building, and Floor network levels for the region.
- If the selected scope is a City, the graph shows threat level for Campus, Building, and Floor network levels for the city.
- If the selected scope is a Campus, the graph shows threat level for Building and Floor network levels for the campus.
- If the selected scope is a Building, the graph shows threat level for Floor network level for the building.
- If the selected scope is a Floor or Sensor the graph shows traffic for the top 100 devices (by threat level, 8 at a time) for the Sensor or floor.

The left side of the graphical view lists the levels or devices shown in the chart (right side). You can hide or reveal items in the graph by clicking on the minus (-) or plus (+) sign to the left of the network level name.

If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Threat Breakdown** tab.

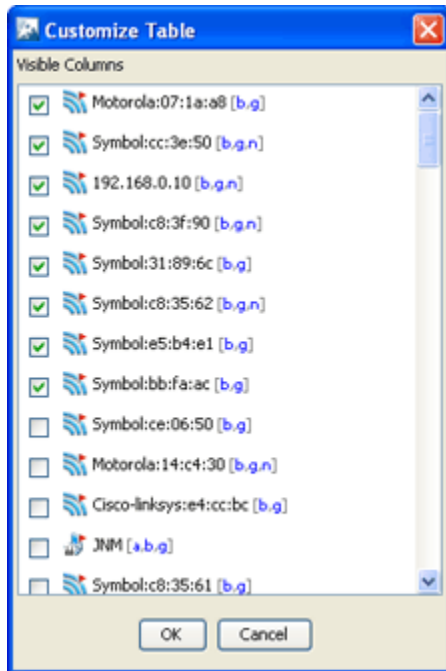
The graph for any item in the list may be expanded by clicking on the Expand— icon. The expanded graph may be reduced to normal size by clicking on the Reduce— icon.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.


### Table View

The **Time** column is included in every threat level. When the Scope is at the Floor or Sensor level, the first 8 items are shown in the other columns by default. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area to display the **Customize Table** popup window. Uncheck a checkbox for a column to hide that column.



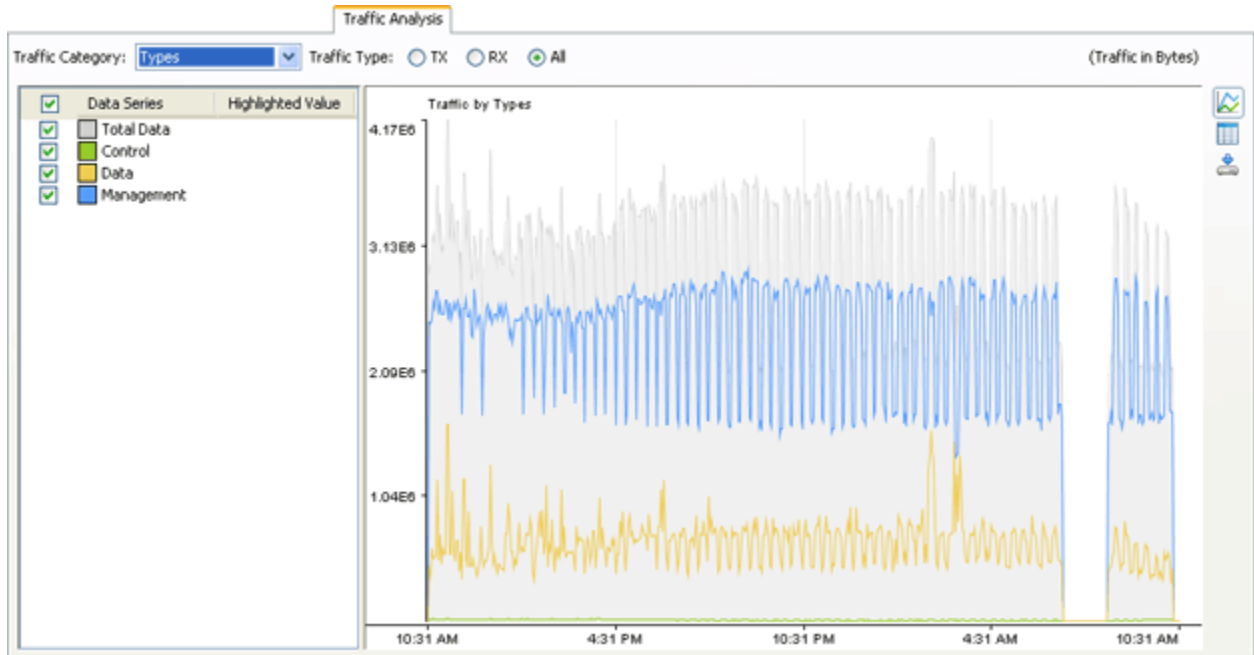
- Rearrange columns by clicking on a column heading and dragging it to a new position.


You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.



## Traffic Analysis


The **Traffic Analysis** tab provides a graphical and tabular view of traffic transmitted and received by all devices in the selected scope. The first time you access the **Traffic Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

The screenshot shows the 'Traffic Analysis' tab with the 'Types' category selected. The 'Traffic Type' is set to 'All'. The table displays traffic data by time and type. The columns are: Time, TX Total Data, TX Control, TX Data, TX Management, RX Total Data, RX Control, RX Data, and RX Management. The data is sorted by time, with the 'Totals' row at the top.

Time	TX Total Data	TX Control	TX Data	TX Management	RX Total Data	RX Control	RX Data	RX Management
<b>Totals</b>	3,672,259,598	44,000	714,508,878	2,957,714,166	70,402,601	16,303,918	52,993,802	1,105,125
10/19/09 10:31 ... 0	0	0	0	0	0	0	0	0
10/19/09 10:32 ... 2,881,327	2,881,327	0	388,916	2,492,411	51,689	17,430	33,899	360
10/19/09 10:33 ... 2,763,114	2,763,114	0	430,290	2,332,824	25,989	14,690	11,119	180
10/19/09 10:34 ... 2,844,250	2,844,250	16	365,398	2,478,836	34,665	15,400	18,670	595
10/19/09 10:35 ... 1,651,710	1,651,710	0	221,048	1,430,662	23,281	11,630	11,531	120
10/19/09 10:36 ... 1,741,101	1,741,101	16	225,805	1,515,280	29,509	8,430	21,079	0
10/19/09 10:37 ... 2,858,978	2,858,978	0	454,893	2,404,085	35,514	15,350	19,528	636
10/19/09 10:38 ... 3,088,946	3,088,946	32	578,704	2,510,210	48,531	17,390	30,425	716
10/19/09 10:39 ... 2,900,060	2,900,060	0	461,177	2,438,883	31,017	14,390	16,162	465
10/19/09 10:40 ... 3,173,060	3,173,060	0	515,925	2,657,135	28,916	15,340	12,346	1,230
10/19/09 10:41 ... 2,958,950	2,958,950	48	428,682	2,530,220	52,510	22,998	29,512	0
10/19/09 10:42 ... 3,015,201	3,015,201	16	443,889	2,571,296	28,499	16,450	11,481	568
10/19/09 10:43 ... 3,021,808	3,021,808	0	421,677	2,600,131	25,880	13,686	11,782	412
10/19/09 10:44 ... 3,047,928	3,047,928	48	485,476	2,562,404	60,254	15,460	44,236	558
10/19/09 10:45 ... 2,921,161	2,921,161	0	444,460	2,476,701	41,889	15,450	25,420	1,019
10/19/09 10:46 ... 3,127,872	3,127,872	0	534,856	2,593,016	33,638	15,926	17,534	178
10/19/09 10:47 ... 3,240,441	3,240,441	0	496,387	2,744,054	38,823	17,860	20,633	330
10/19/09 10:48 ... 3,187,000	3,187,000	0	582,404	2,604,596	63,810	17,820	45,278	712

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### Graphical View

The **Traffic Category** field determines the type of data displayed in the graph. You can change the traffic category by selecting one of the following categories from the **Traffic Category** drop-down menu:


- Ad-Hoc
- Control Details
- Data Details
- Destinations
- EAP Details
- Encryption Details
- Management Details
- Rates
- Retry
- Types (default).

The **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types. You can change the traffic type by selecting the appropriate radio button:

- RX
- TX
- All.

The left side of the graphical view has two columns:

Column	Description
Data Series	Acts as a filter to determine how the graphs are displayed. The <b>Traffic Category</b> field determines what is shown in this column. Anything with a checkmark in its checkbox will be seen in the graphs. If there is no checkmark, it is filtered out of the graph. Click on a checkbox to change states.
Highlighted Values	If you position your cursor over any part of the graph, the values for that moment is displayed in this column.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

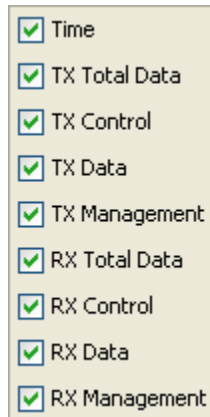
### Table View

Like the graphical view, the **Traffic Category** field determines what columns are displayed in the table. The same categories are used.


Also, the **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types in the table. You can change the traffic type by selecting the appropriate radio button.

The **Time** column is included in every traffic category. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).

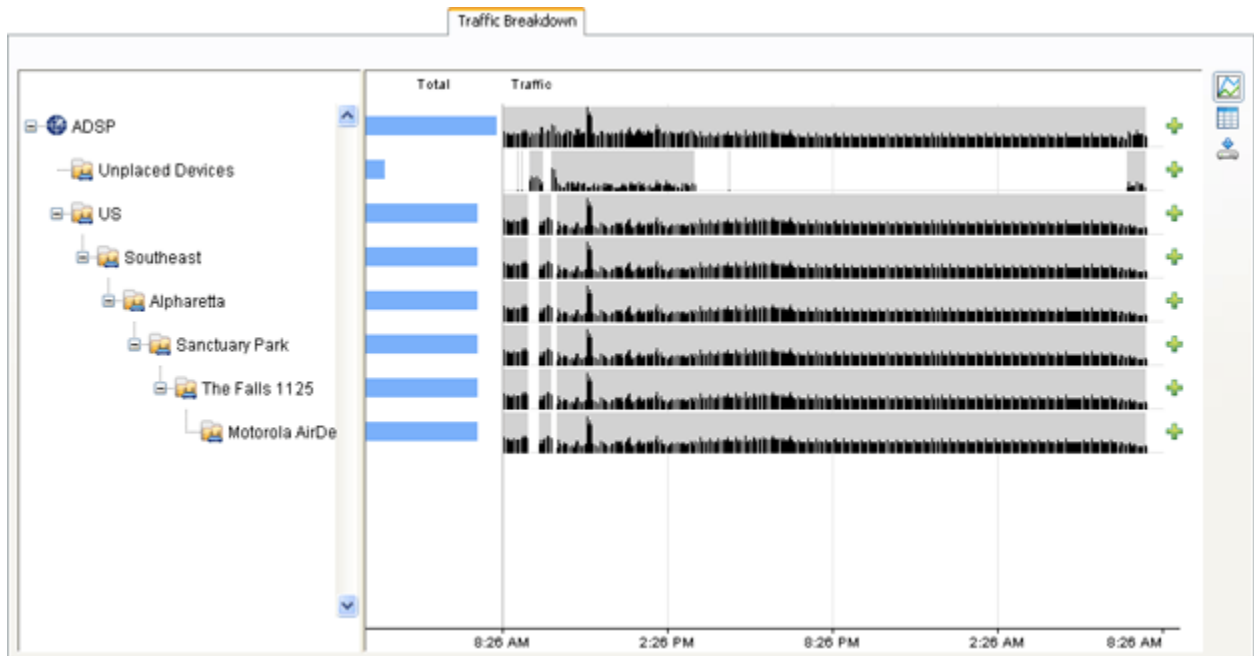



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Traffic Breakdown


The **Traffic Breakdown** tab provides a graphical and tabular view of the total traffic for devices within the selected scope. The first time you access the **Traffic Breakdown** tab the graphical view is displayed.



You can switch to the table view by clicking the Data Table— button.

Traffic Breakdown

Time	ADSP	ADSP	US	Southeast	The Falls ...	Motorola ...	Alpharetta	Sanctuary...
<b>Totals</b>	3,853,238,956	3,853,238,956	3,297,299,775	3,297,299,775	3,297,299,775	3,297,299,775	3,297,299,775	3,297,299,775
1/4/10 8:26 AM	0	0	0	0	0	0	0	0
1/4/10 8:27 AM	3,890,516	3,890,516	3,890,516	3,890,516	3,890,516	3,890,516	3,890,516	3,890,516
1/4/10 8:28 AM	2,552,566	2,552,566	2,552,566	2,552,566	2,552,566	2,552,566	2,552,566	2,552,566
1/4/10 8:29 AM	3,592,327	3,592,327	3,592,327	3,592,327	3,592,327	3,592,327	3,592,327	3,592,327
1/4/10 8:30 AM	3,791,634	3,791,634	3,791,634	3,791,634	3,791,634	3,791,634	3,791,634	3,791,634
1/4/10 8:31 AM	3,187,748	3,187,748	3,187,748	3,187,748	3,187,748	3,187,748	3,187,748	3,187,748
1/4/10 8:32 AM	3,015,433	3,015,433	3,015,433	3,015,433	3,015,433	3,015,433	3,015,433	3,015,433
1/4/10 8:33 AM	3,010,323	3,010,323	3,010,323	3,010,323	3,010,323	3,010,323	3,010,323	3,010,323
1/4/10 8:34 AM	2,464,262	2,464,262	2,464,262	2,464,262	2,464,262	2,464,262	2,464,262	2,464,262
1/4/10 8:35 AM	2,943,197	2,943,197	2,943,197	2,943,197	2,943,197	2,943,197	2,943,197	2,943,197
1/4/10 8:36 AM	3,355,645	3,355,645	3,355,645	3,355,645	3,355,645	3,355,645	3,355,645	3,355,645
1/4/10 8:37 AM	2,907,327	2,907,327	2,907,327	2,907,327	2,907,327	2,907,327	2,907,327	2,907,327
1/4/10 8:38 AM	2,984,194	2,984,194	2,984,194	2,984,194	2,984,194	2,984,194	2,984,194	2,984,194
1/4/10 8:39 AM	2,741,042	2,741,042	2,741,042	2,741,042	2,741,042	2,741,042	2,741,042	2,741,042
1/4/10 8:40 AM	2,847,541	2,847,541	2,847,541	2,847,541	2,847,541	2,847,541	2,847,541	2,847,541
1/4/10 8:41 AM	2,869,935	2,869,935	2,869,935	2,869,935	2,869,935	2,869,935	2,869,935	2,869,935
1/4/10 8:42 AM	2,787,717	2,787,717	2,787,717	2,787,717	2,787,717	2,787,717	2,787,717	2,787,717
1/4/10 8:43 AM	3,076,943	3,076,943	3,076,943	3,076,943	3,076,943	3,076,943	3,076,943	3,076,943
1/4/10 8:44 AM	2,843,923	2,843,923	2,843,923	2,843,923	2,843,923	2,843,923	2,843,923	2,843,923

Click the Data Chart— button to switch back to the graphical view.



- ✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.


### Graphical View

Depending on the selected Scope, the graphical view displays forensic data as follows:

- If the selected scope is the entire System, the graph shows traffic for all network levels in the system.
- If the selected scope is a Country, the graph shows traffic for Region, City, Campus, Building, and Floor network levels for the country.
- If the selected scope is a Region, the graph shows traffic for City, Campus, Building, and Floor network levels for the region.
- If the selected scope is a City, the graph shows traffic for Campus, Building, and Floor network levels for the city.
- If the selected scope is a Campus, the graph shows traffic for Building and Floor network levels for the campus.
- If the selected scope is a Building, the graph shows traffic for Floor network level for the building.
- If the selected scope is a Floor or Sensor the graph shows traffic for the top 100 devices (by total traffic, 8 at a time) for the Sensor or floor.

The left side of the graphical view lists the levels or devices shown in the chart (right side). You can hide or reveal items in the graph by clicking on the minus (-) or plus (+) sign to the left of the network level name.

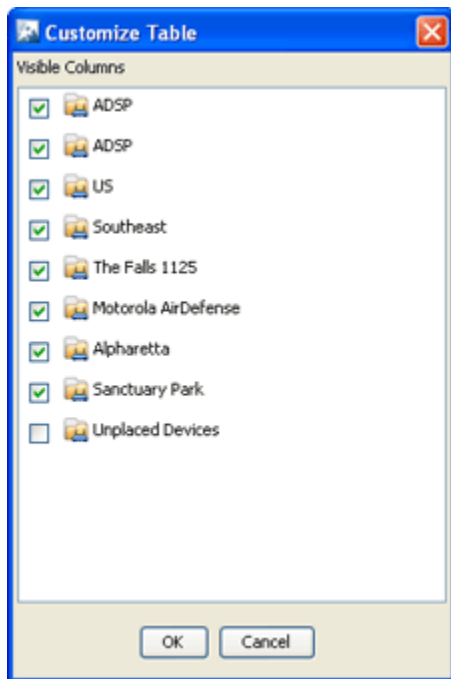
The graph for any item in the list may be expanded by clicking on the Expand— icon. The expanded graph may be reduced to normal size by clicking on the Reduce— icon.

You can export the table data to a CSV file by clicking the Export Data— button. An Export Table window will display where you can name and save the file to a location on your hard drive.


### Table View

The **Time** column is included in every traffic category. When the Scope is at the Floor or Sensor level, the first 8 items are shown in the other columns by default. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area to display the **Customize Table** popup window. Uncheck a checkbox for a column to hide that column.

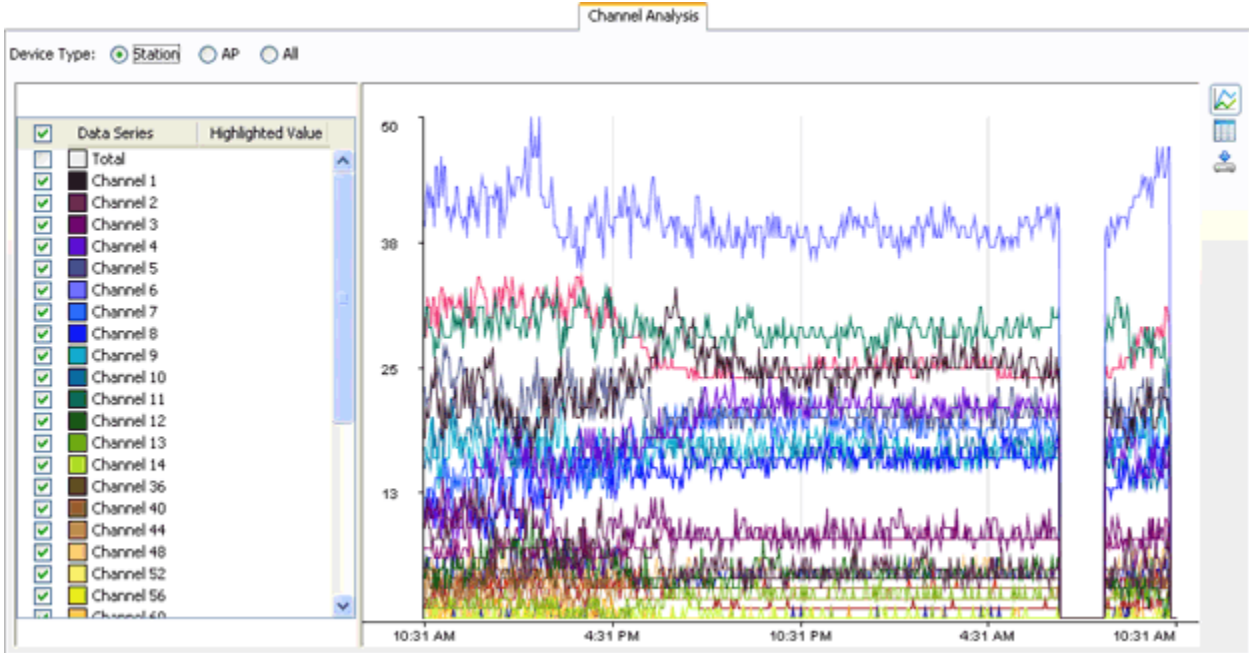



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.


**Channel Analysis**

The **Channel Analysis** tab provides a graphical and tabular view of the device count for each channel over time. The first time you access the **Channel Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

The screenshot shows the 'Channel Analysis' interface in table view. At the top, 'Device Type' is set to 'Station'. Below this is a grid of data. The grid has 10 rows and 20 columns of numerical values. The values represent device counts for different channels at different time intervals. On the right side, there are icons for zooming and data export.

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.


### Graphical View

The Device Type field determines whether you see data for Wireless Clients, APs, or all devices. You can change the device type by selecting the appropriate radio button:

- Wireless Client
- AP
- All.

The left side of the graphical view has two columns:

Column	Description
Data Series	Acts as a filter to determine how the graphs are displayed. Anything with a checkmark in its checkbox will be seen in the graphs. If there is no checkmark, it is filtered out of the graph. Click on a checkbox to change states.
Highlighted Values	If you position your cursor over any part of the graph, the values for that moment is displayed in this column.

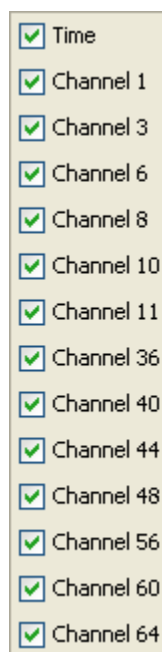
You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Table View


The **Device Type** field determines whether you see Channels for Wireless Clients, APs, or all devices in the table. You can change the device type by selecting the appropriate radio button.

The **Time** column is included in every device category. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and uncheck the checkbox for a category (see below).

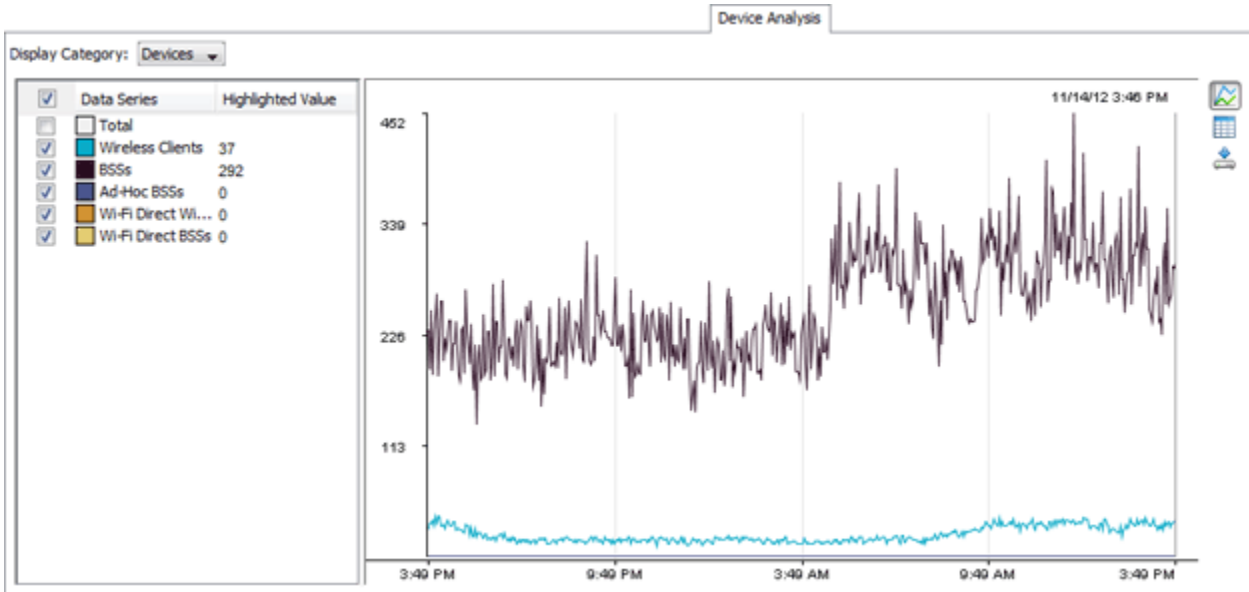



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.


### Device Analysis

The **Device Analysis** tab provides a graphical and tabular view of device counts for Devices and Sensors. The first time you access the **Device Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

Time	Total	Wireless Clients	BSSs	Ad-Hoc BSSs	Wi-Fi Direct Wireless...	Wi-Fi Direct BSSs
11/13/12 3:49 PM	260	29	231	0	0	0
11/13/12 3:50 PM	173	30	143	0	0	0
11/13/12 3:51 PM	218	26	192	0	0	0
11/13/12 3:52 PM	219	35	184	0	0	0
11/13/12 3:53 PM	179	27	152	0	0	0
11/13/12 3:54 PM	284	34	250	0	0	0
11/13/12 3:55 PM	208	32	176	0	0	0
11/13/12 3:56 PM	223	37	186	0	0	0
11/13/12 3:57 PM	189	29	160	0	0	0
11/13/12 3:58 PM	255	30	225	0	0	0
11/13/12 3:59 PM	210	32	178	0	0	0
11/13/12 4:00 PM	196	29	167	0	0	0
11/13/12 4:01 PM	280	36	244	0	0	0
11/13/12 4:02 PM	235	41	194	0	0	0
11/13/12 4:03 PM	203	34	169	0	0	0
11/13/12 4:04 PM	284	31	253	0	0	0
11/13/12 4:05 PM	300	33	267	0	0	0

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.




### Graphical View

The **Display Category** field determines whether you see a device count for Devices or Sensors. Devices may be Wireless Clients, BSSs, or Ad-Hoc BSSs. Sensors may be Online or Offline Sensors. You can change the display category by selecting the appropriate radio button:

- Devices
- Sensors.

The left side of the graphical view has two columns:

Column	Description
Data Series	Acts as a filter to determine how the graphs are displayed. This column changes depending on whether you select Devices or Sensors in the <b>Display Category</b> field. A <b>Total</b> option, when selected, displays the total device count for all the other options. Anything with a checkmark in its checkbox will be seen in the graphs. If there is no checkmark, it is filtered out of the graph. Click on a checkbox to change states.
Highlighted Values	If you position your cursor over any part of the graph, the values for that moment is displayed in this column.

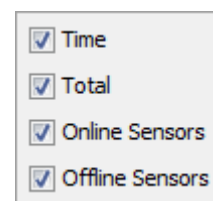
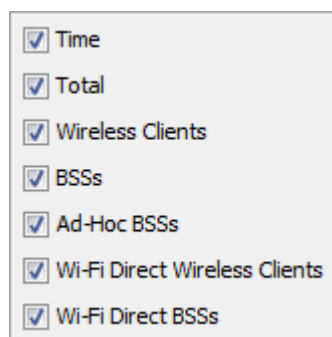
You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Table View


Like the graphical view, the **Display Category** field determines what columns are displayed in the table. The same categories are used.

The **Time** column is included in every display category. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and uncheck the checkbox for a category (see below).

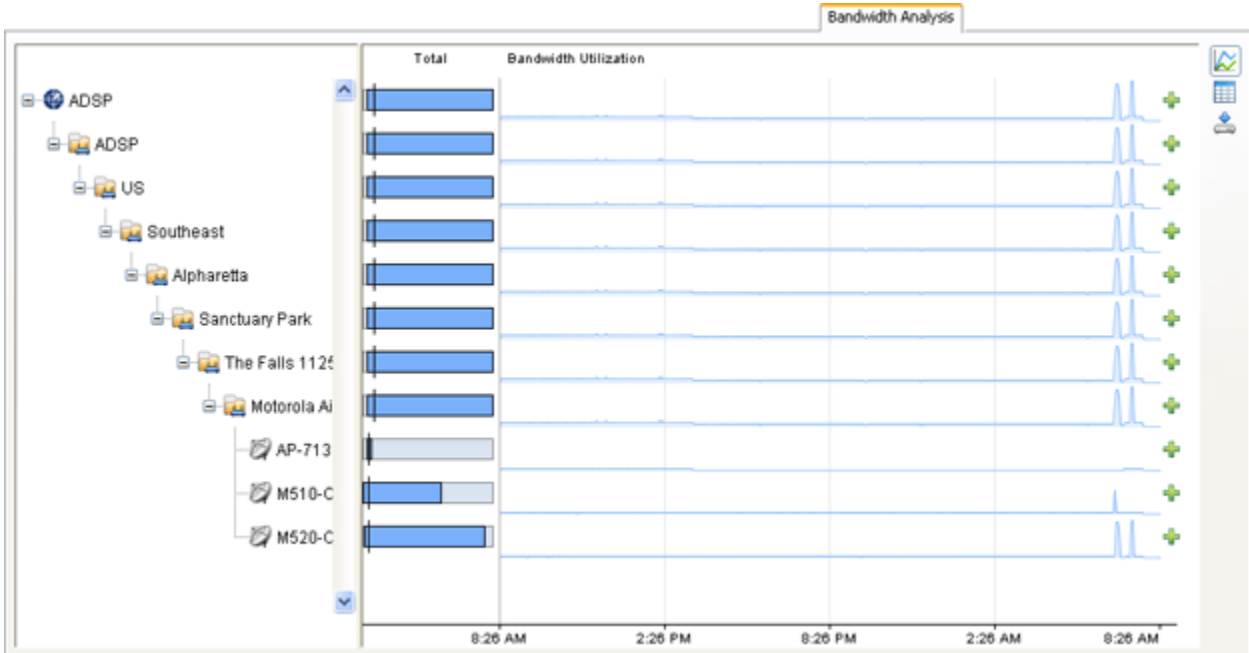



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

**Bandwidth Analysis**


The **Bandwidth Analysis** tab provides a graphical and tabular view of the wired bandwidth usage of the Sensors in the selected Scope over time. The first time you access the **Bandwidth Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

The screenshot shows the 'Bandwidth Analysis' window in table view. The table displays bandwidth usage in kbit/sec for various sensors over time. The columns represent different sensors, and the rows represent time intervals. A 'Data Chart' button is visible in the top right corner.

Time	US	Sout...	AP-7131F	ADSP	ADSP	The ...	Moto...	MS10-CC	Alph...	Sanc...	MS20-CC
Totals											
1/4/10 8:2...	47	47	18	47	47	47	47	15	47	47	14
1/4/10 8:2...	31	31	17	31	31	31	31	0	31	31	14
1/4/10 8:2...	45	45	16	45	45	45	45	15	45	45	14
1/4/10 8:3...	47	47	18	47	47	47	47	14	47	47	15
1/4/10 8:3...	46	46	17	46	46	46	46	14	46	46	15
1/4/10 8:3...	44	44	16	44	44	44	44	15	44	44	13
1/4/10 8:3...	37	37	16	37	37	37	37	14	37	37	7
1/4/10 8:3...	39	39	17	39	39	39	39	15	39	39	7
1/4/10 8:3...	44	44	16	44	44	44	44	14	44	44	14
1/4/10 8:3...	47	47	17	47	47	47	47	15	47	47	15
1/4/10 8:3...	48	48	17	48	48	48	48	16	48	48	15
1/4/10 8:3...	44	44	17	44	44	44	44	14	44	44	13
1/4/10 8:3...	45	45	17	45	45	45	45	14	45	45	14
1/4/10 8:4...	47	47	18	47	47	47	47	15	47	47	14
1/4/10 8:4...	49	49	19	49	49	49	49	15	49	49	15
1/4/10 8:4...	47	47	17	47	47	47	47	16	47	47	14
1/4/10 8:4...	45	45	17	45	45	45	45	14	45	45	14
1/4/10 8:4...	46	46	17	46	46	46	46	15	46	46	14
1/4/10 8:4...	45	45	17	45	45	45	45	14	45	45	14


Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### Graphical View

The left side of the graphical view lists the network levels shown in the graph (right side). Click on the plus (+) or minus (-) sign to expand or collapse a level.

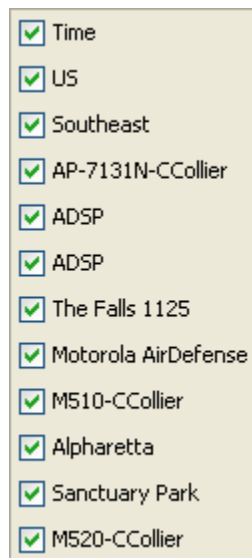
If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Bandwidth Analysis** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.


### Table View

The table view has a column for each of the categories shown in the graphical view plus a **Time** category. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



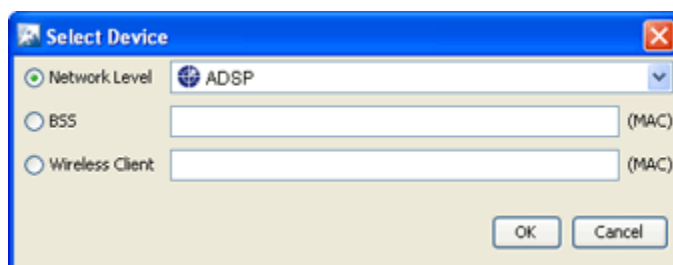
- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Device Based

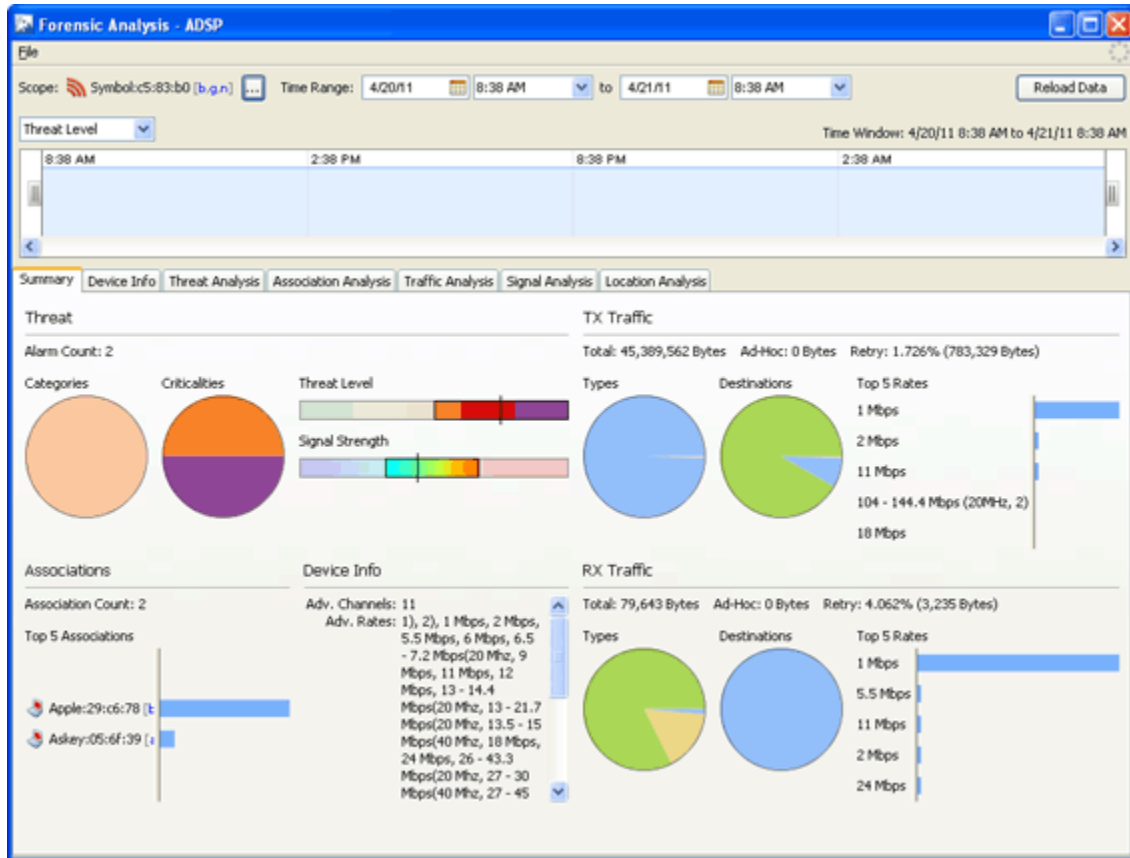
Device Based Forensic Analysis is only available for BSSs, Wireless Clients, APs, and Switches. You initiate Device Based Forensic Analysis the same way as the basic Forensic Analysis:

1. Select **Menu > Forensic Analysis**. The **Select Device** window displays.



2. Select **BSS** or **Wireless Client** and supply the MAC address, or select an AP or Switch from the Network Level drop-down menu.

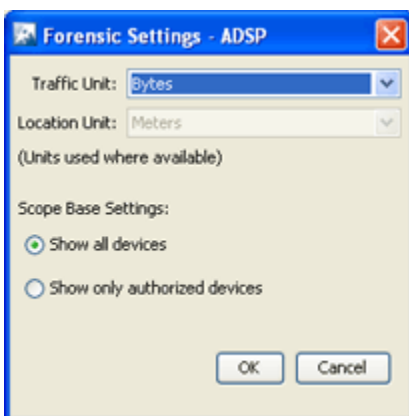
- Click **OK**. The **Forensic Analysis** window displays.



## Common Area

### Forensic Settings

The Forensic Settings are used to set the traffic units and location units for Traffic Analysis and Location Analysis, respectively. To change a setting, click the **File** menu and then select **Settings**.



### Forensic Settings

Click the **Traffic Unit** drop-down menu to change the traffic units. Your choices are:

- Frames
- Bytes
- KBytes
- MBytes
- GBytes.

Click the **Location Unit** drop-down menu button to change the location units. Your choices are:

- Meters
- Centimeters
- Feet
- Inches.

You also have the option to show all devices or show only authorized devices.


### Scope

The **Scope** field displays the device that you are analyzing. An BSS icon or a Wireless Client icon along with the device name is shown.

If you right-click on the device, you can copy the MAC address for later use.


### Switch Devices

You can switch to another device if you know the device's MAC Address. To switch devices:

1. Click  button. The **Select Device** popup will display.
2. Select the Device Type (**BSS** or **Wireless Client**).
3. Type in the MAC Address.
4. Click **OK**.

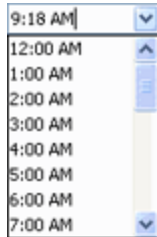
### Time Range

You can specify a time range (start and end) for your Forensic Analysis. To specify a time range:

1. Click the first Calendar–  button to select a starting date. A calendar displaying the current month will display.



2. Select a day of the month from the calendar. You may switch months using the green arrow keys.
3. Click the first Time drop-down button to select a starting time. A drop-down list will display showing a list of dates by hours.

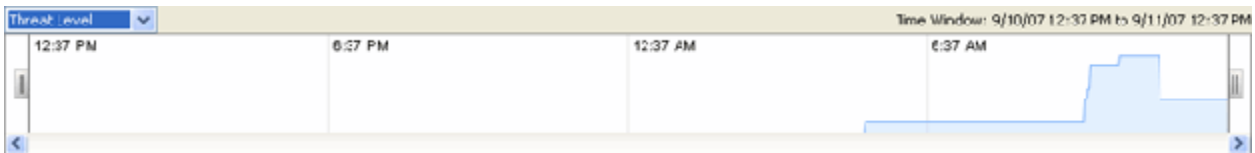


4. Select a starting time from the list or type in a starting time.
5. Click the second **Calendar** button to select an end date.
6. Select a day of the month from the calendar.
7. Click the second **Time** drop-down menu button to select an end time.
8. Select an end time from the list or type in an end time.
9. Click the **Reload Data** button. The **Time** window will change to reflect your time range.

### Time Window

The **Time** window has three different views:

- Threat Level (default)
- Total Traffic
- Association Count.



Each view is shown across the time range. There are sliders on each side of the **Time** window which controls the focus, allowing the user to select a portion of the loaded data to analyze. Just move the sliders in or out to adjust the focus.

### Tabs

The tabs display the Forensic Analysis data. The following seven tabs are available:

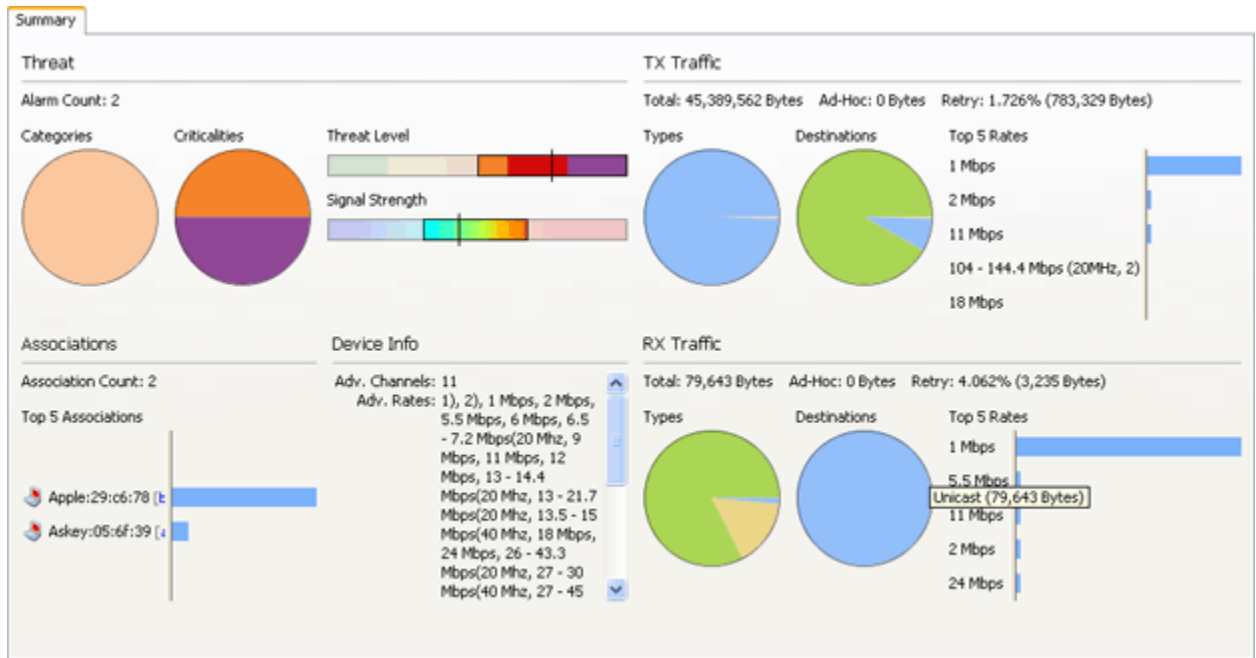
- Summary
- Device Info
- Threat Analysis
- Association Analysis
- Traffic Analysis
- Signal Analysis
- Location Analysis.

Each tab is discussed as a separate topic.

## BSSs & Wireless Clients

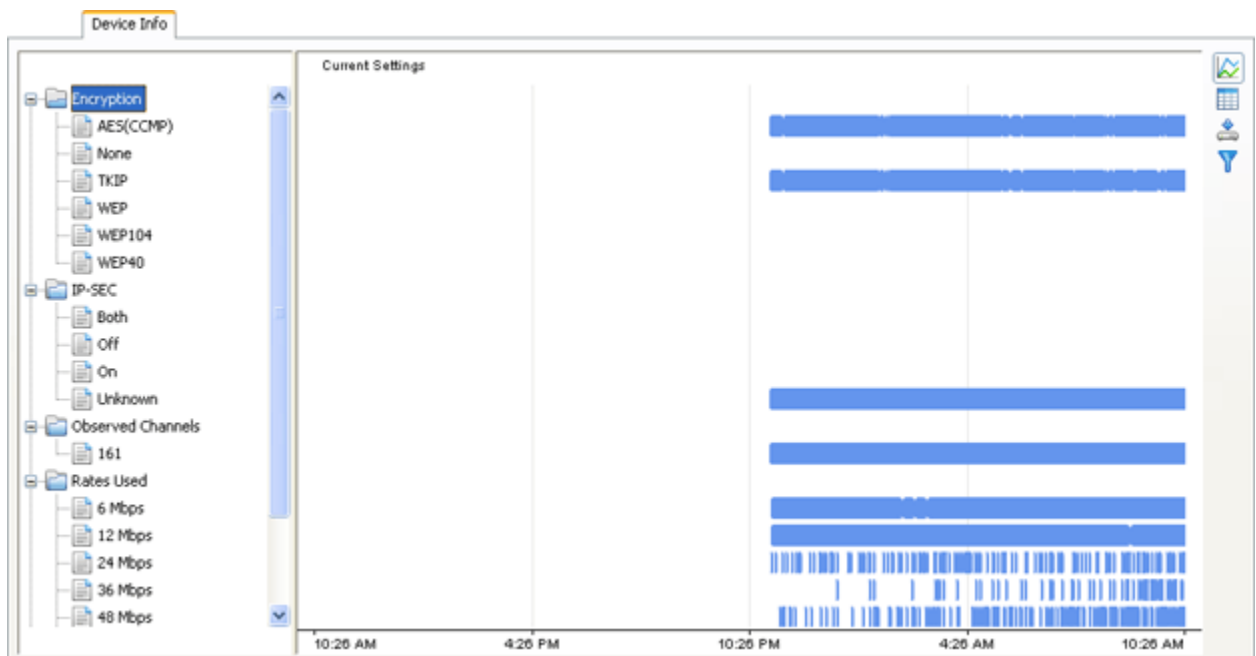
### Summary


The **Summary** tab for the Device Based Advanced Forensic Analysis is basically the same as the Basic Forensic Analysis **Summary** tab. It provides a summary of forensic data broken down into categories that roughly match what is in the other tabs. Each time you access Device Based Forensic Analysis the **Summary** tab is the first one displayed.



### Device Info

The **Device Info** tab provides a graphical and tabular view of the current settings for the device being analyzed. The first time you access the **Device Info** tab the graphical view is displayed.




You can switch to the table view by clicking the **Data Table**— button.


Device Info

One row per minute
  One row per change in Encryption

Time	Encryption	IP-SEC	Observed Channels	Rates Used	SSID Broadcast
10/20/09 10:26 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:27 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:28 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:29 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:30 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:31 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:32 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:33 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:34 AM	TKIP,AES(CCMP)	Unknown	161	161	No
10/20/09 10:35 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:36 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:37 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:38 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:39 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:40 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:41 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:42 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:43 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:44 AM	TKIP,AES(CCMP)	Unknown	161		No
10/20/09 10:45 AM	TKIP,AES(CCMP)	Unknown	161		No

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### **Graphical View**

The left side of the graphical view lists the categories shown in the chart (right side). Click on the plus (+) or minus (-) sign to expand or collapse a category. The categories are:

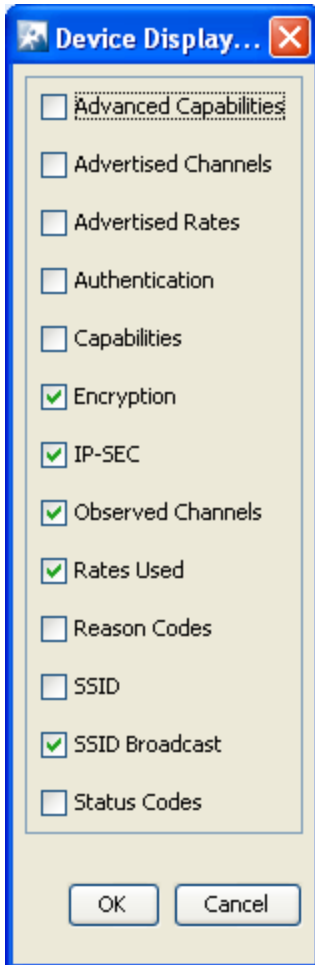
- Channels Used
- Encryption
  - AES(CCMP)
  - None
  - TKIP
  - Unknown
  - WEP
  - WEP140
  - WEP40
- IP-SEC
  - Both
  - Off
  - On
  - Unknown
- Rates Used




- SSID Broadcast
  - No
  - Yes

If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Device Info** tab.

You can add additional categories by clicking the **Filter Data**— button. The **Device Display Options** window will display.



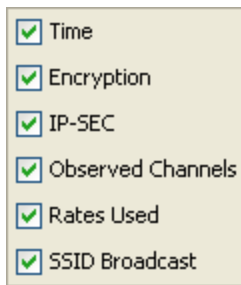
Click a checkbox to add a category and then click **OK**.


You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### **Table View**

The table view has a column for each of the categories shown in the graphical view plus a **Time** category. Column display and arrangement can be customized as follows:


- Hide a column by right-clicking in the column heading area to display the **Customize Table** popup window. Uncheck a checkbox for a column to hide that column.



- Add additional columns by clicking the **Filter Data**— button, clicking a checkbox, and then clicking **OK**.
- Rearrange columns by clicking on a column heading and dragging it to a new position.

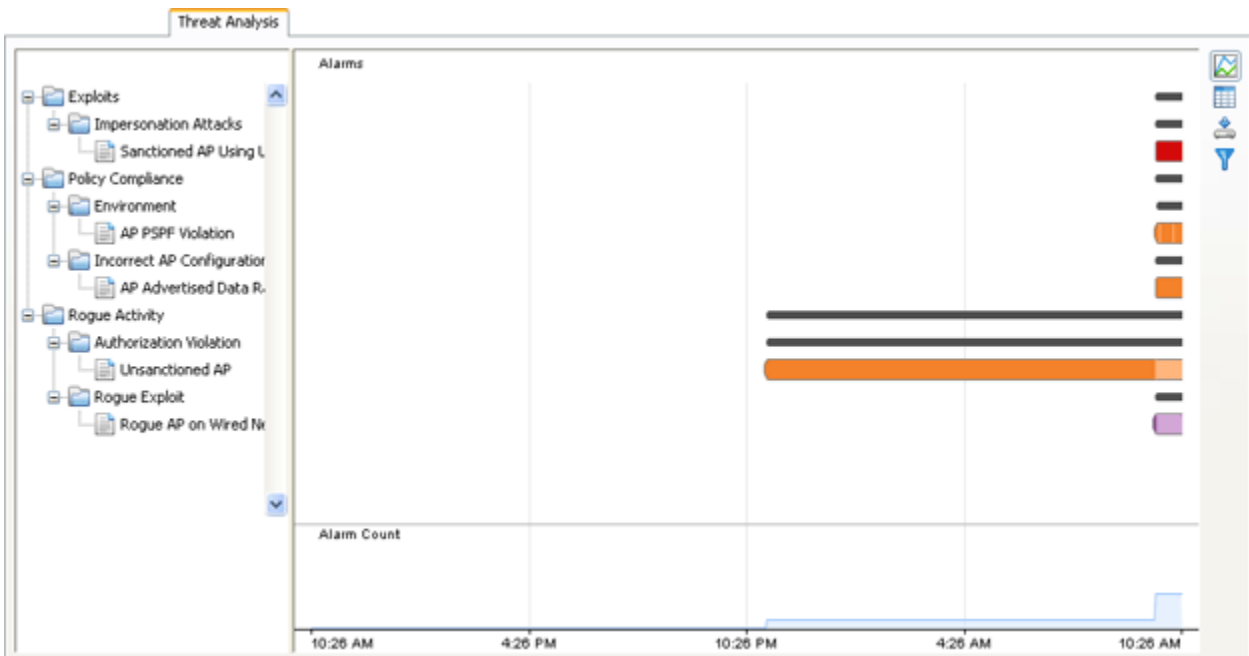
The table may be shown with one row per minute or one row for every change in the value of a particular column (category). Click the appropriate radio button in the top, left side of the **Device Info** tab.


✓ **NOTE** If you add additional columns, they will be included in the drop-down list for the **One row per change in** field.

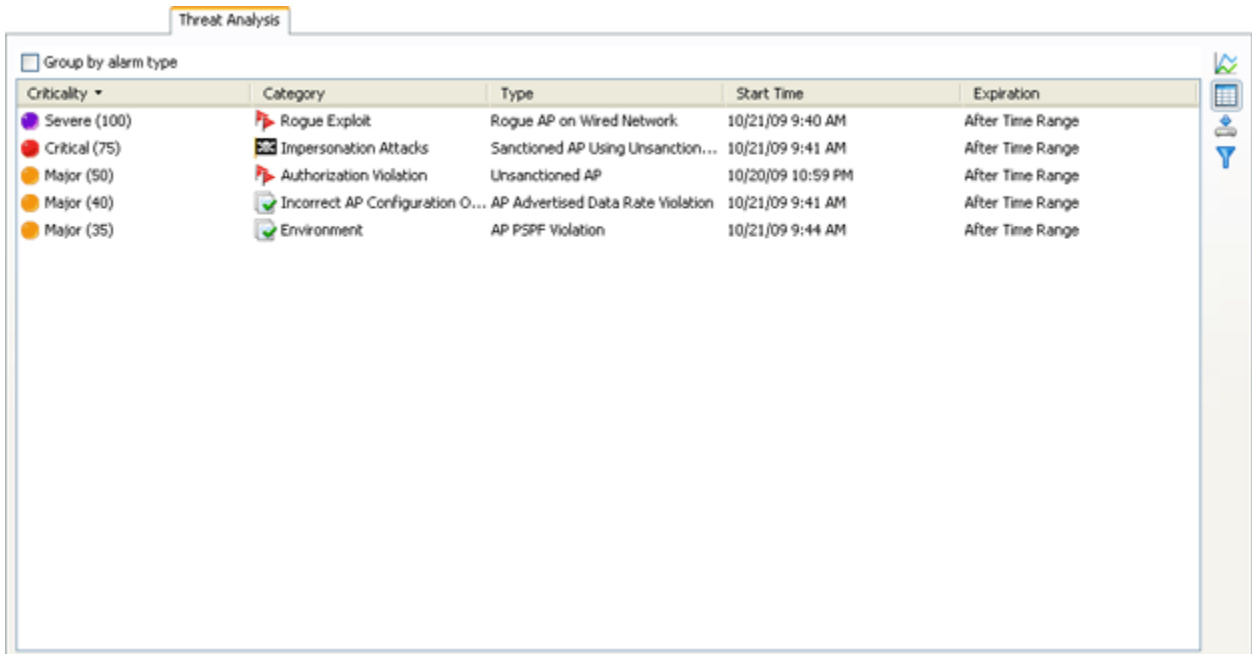
You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Threat Analysis

The **Threat Analysis** tab provides a graphical and tabular view of the alarms for the device being analyzed. The first time you access the **Threat Analysis** tab the graphical view is displayed.




You can switch to the table view by clicking the **Data Table**— button.



The screenshot shows the 'Threat Analysis' window with a table view. On the left, there is a 'Group by alarm type' section with a list of severity levels: Severe (100), Critical (75), Major (50), Major (40), and Major (35). The main table has the following columns: Criticality, Category, Type, Start Time, and Expiration. The data rows are as follows:

Criticality	Category	Type	Start Time	Expiration
Severe (100)	Rogue Exploit	Rogue AP on Wired Network	10/21/09 9:40 AM	After Time Range
Critical (75)	Impersonation Attacks	Sanctioned AP Using Unsanctioned AP	10/21/09 9:41 AM	After Time Range
Major (50)	Authorization Violation	Unsanctioned AP	10/20/09 10:59 PM	After Time Range
Major (40)	Incorrect AP Configuration O...	AP Advertised Data Rate Violation	10/21/09 9:41 AM	After Time Range
Major (35)	Environment	AP PSFP Violation	10/21/09 9:44 AM	After Time Range

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

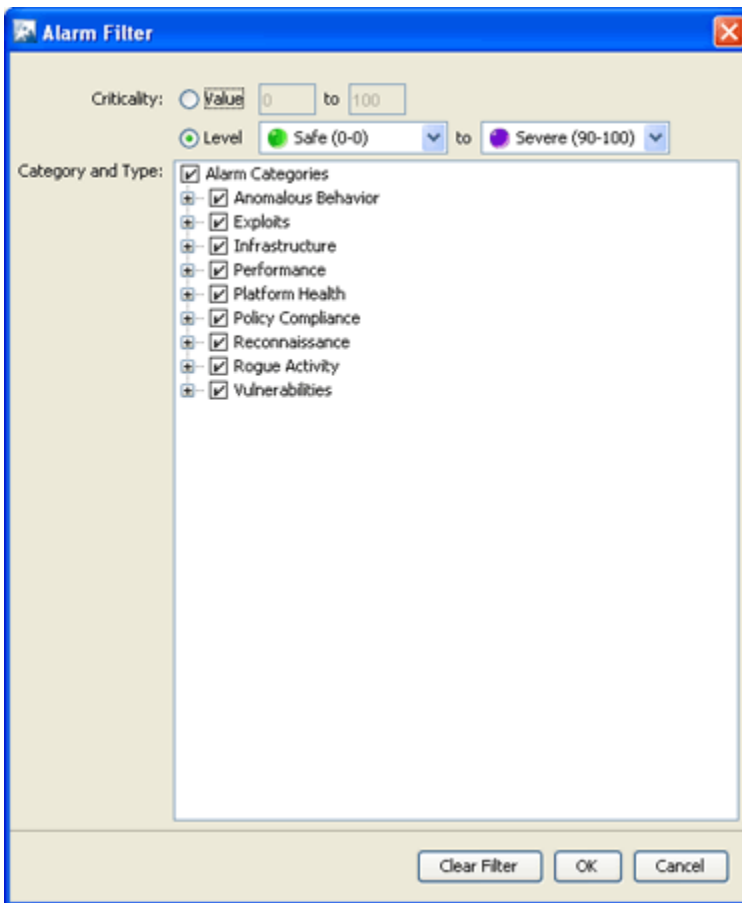
### **Graphical View**

The left side of the graphical view lists the categories shown in the chart (right side). Click on the plus (+) or minus (-) sign to expand or collapse a category. The categories are:

- Anomalous Behavior
- Exploits
- Infrastructure
- Performance
- Platform Health
- Policy Compliance
- Reconnaissance
- Rogue Activity
- Vulnerabilities
- System Health
- Vulnerabilities.

If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Threat Analysis** tab.


Clicking the **Filter Data**— button displays an **Alarm Filter** window where you can filter the alarm data that is shown in graph.



Changes to the following fields will affect the filter:

Field	Description
Criticality	Change the criticality by entering exact values for a range or selecting a starting level and an ending level. To enter the values, select the <b>Value</b> radio button and then enter values from 1 to 100. To select levels, select the <b>Level</b> radio button and then select the levels using the drop-down menus.
Category and Type	By default, all categories and types are selected, to deselect a category or type, remove the checkmark in the checkbox next to the category or type. Click the plus (+) or minus (-) sign to expand or collapse a category.

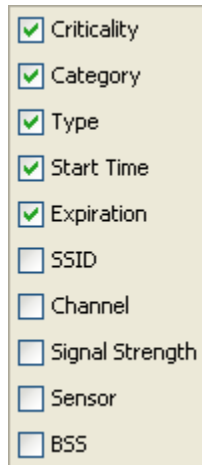
Click the **OK** button to activate your changes. The **Clear Filter** button will reset all fields back to their default state. The **Cancel** button will cancel any changes.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

***Table View***

The table view has a column for each of the categories shown in the graphical view plus a **Time** category. Column display and arrangement can be customized as follows:


- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

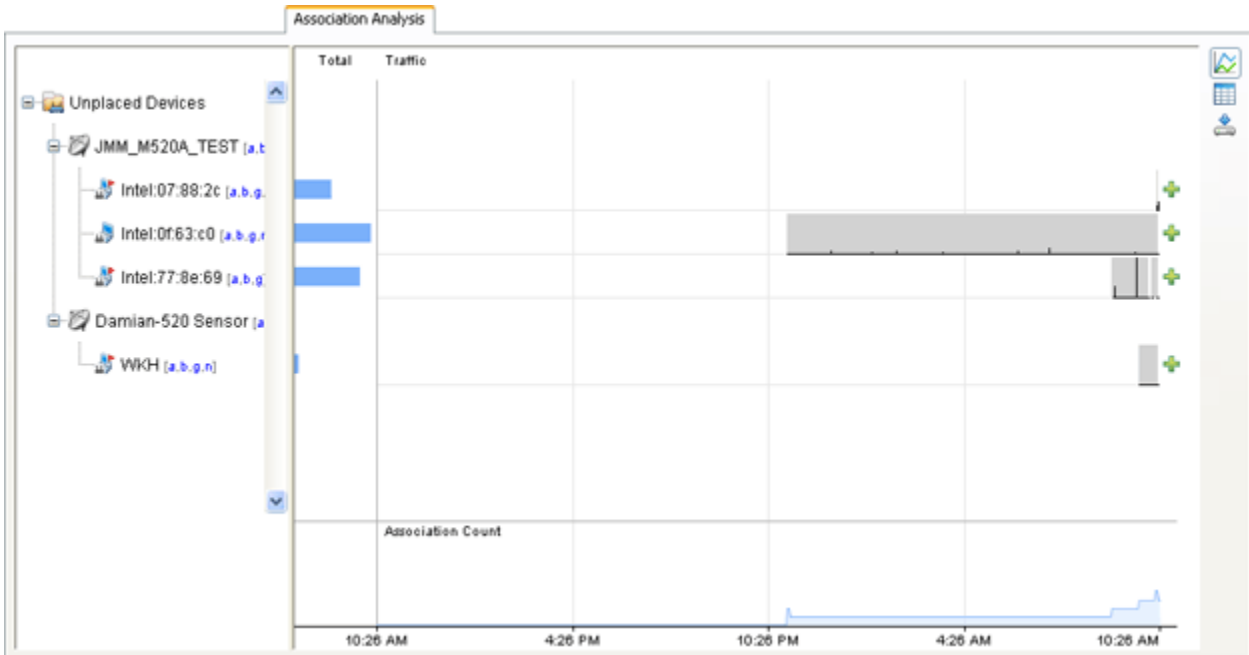
Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm. See the **Alarm Details** window topic for more information.


You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

The **Filter Data**— button works the same as it does in the graphical view.


## Association Analysis

The **Association Analysis** tab provides a graphical and tabular view of the associations between the device being analyzed and other wireless devices. The first time you access the **Association Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

Device	SSID	Start	End	Duration	RX Traffic	TX Traffic
Intel:0f:63:c0	M-Wireless	10/20/09 10:57 PM	10/20/09 10:57 PM	1 minute	98	2,046
Intel:0f:63:c0	M-Wireless	10/20/09 10:59 PM	8/31/70 3:14 AM	1 minute	0	412
Intel:0f:63:c0	M-Wireless	10/20/09 11:00 PM	8/31/70 3:15 AM	1 minute	0	120
Intel:0f:63:c0	M-Wireless	10/20/09 11:01 PM	8/31/70 3:15 AM	1 minute	0	240
Intel:0f:63:c0	M-Wireless	10/20/09 11:02 PM	8/31/70 3:15 AM	1 minute	0	488
Intel:0f:63:c0	M-Wireless	10/20/09 11:03 PM	8/31/70 3:15 AM	1 minute	0	364
Intel:0f:63:c0	M-Wireless	10/20/09 11:04 PM	10/20/09 11:04 PM	1 minute	0	1,224
Intel:0f:63:c0	M-Wireless	10/20/09 11:06 PM	8/31/70 3:15 AM	1 minute	0	316
Intel:0f:63:c0	M-Wireless	10/20/09 11:07 PM	8/31/70 3:15 AM	1 minute	482	1,175
Intel:0f:63:c0	M-Wireless	10/20/09 11:08 PM	8/31/70 3:15 AM	1 minute	0	1,024
Intel:0f:63:c0	M-Wireless	10/20/09 11:09 PM	8/31/70 3:15 AM	1 minute	0	240
Intel:0f:63:c0	M-Wireless	10/20/09 11:10 PM	8/31/70 3:15 AM	1 minute	0	690
Intel:0f:63:c0	M-Wireless	10/20/09 11:11 PM	8/31/70 3:15 AM	1 minute	0	648
Intel:0f:63:c0	M-Wireless	10/20/09 11:12 PM	8/31/70 3:15 AM	1 minute	0	120
Intel:0f:63:c0	M-Wireless	10/20/09 11:13 PM	10/20/09 11:14 PM	1 minutes	0	1,545
Intel:0f:63:c0	M-Wireless	10/20/09 11:16 PM	8/31/70 3:15 AM	1 minute	0	408
Intel:0f:63:c0	M-Wireless	10/20/09 11:17 PM	10/20/09 11:18 PM	1 minutes	0	1,329
Intel:0f:63:c0	M-Wireless	10/20/09 11:20 PM	8/31/70 3:15 AM	1 minute	0	176
Intel:0f:63:c0	M-Wireless	10/20/09 11:21 PM	8/31/70 3:15 AM	1 minute	0	416
Intel:0f:63:c0	M-Wireless	10/20/09 11:22 PM	8/31/70 3:15 AM	1 minute	0	425

Click the **Data Chart**— button to switch back to the graphical view.


✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### Graphical View

The left side of the graphical view lists the associated devices grouped by network group and location. Click on the plus (+) or minus (-) sign to expand or collapse a category.

The right side of the graphical view uses a stepped area chart to show traffic over time per association. There are two sub-charts displayed to the left of the main chart and below the main chart. The sub-chart on the left groups the data over time, showing the total traffic per association as a horizontal bar. The sub-chart below the main chart groups the data over all associations, showing the association over time.

If you position your cursor over any part of the main chart and the sub-chart below the main chart, the exact reading for that moment is displayed in the top, right side of the **Association Analysis** tab. If you position your cursor over any part of the sub-chart to the left of the main chart, the numerical total is displayed in the top, right side of the **Association Analysis** tab.

You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

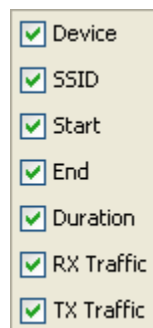
### Table View

The table view has the following columns:

Column	Description
Device	MAC address of the device.
SSID	Service Set Identifier of the associated AP.
Start	Time when the association first started.
End	Time when the association ended.
Duration	Total amount of time the association lasted.
RX Traffic	Number of bytes received during the association.
TX Traffic	Number of bytes transmitted during the association.

Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

An option is included to group by associated device. When selected, there will be only one row for each unique device. Click the **Group by associated device** checkbox to select the option.

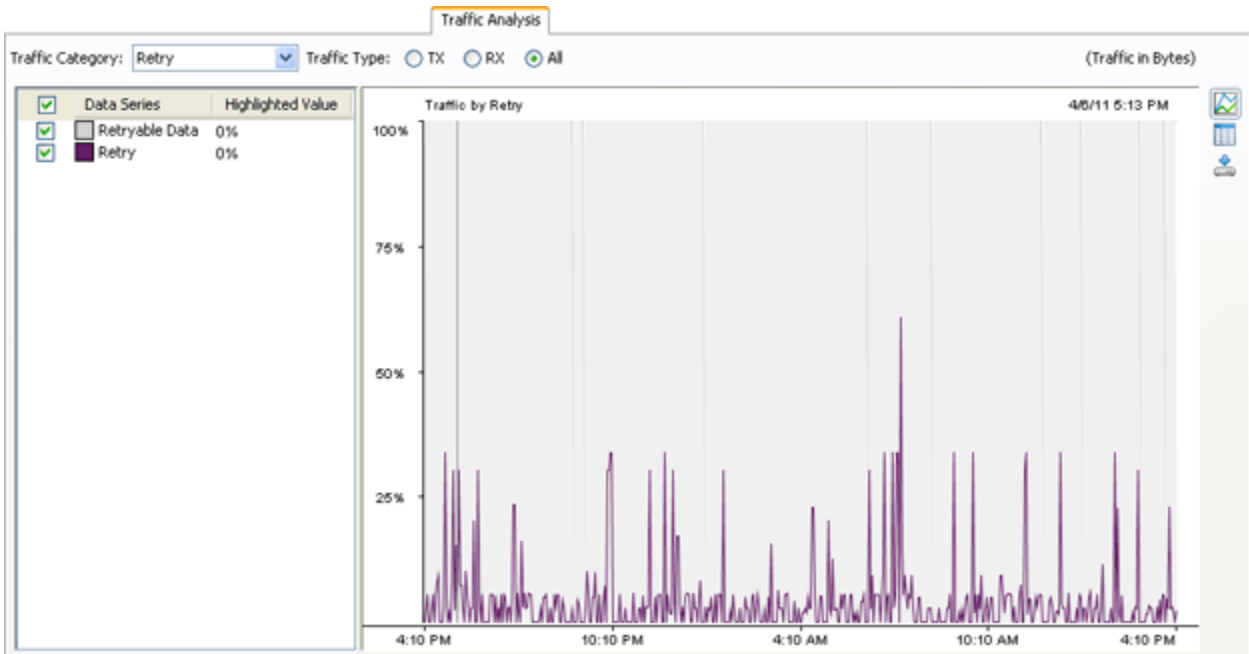
Right-clicking on a device displays a menu of options that allow you to conduct additional functions on the device.

Copy MAC
View/Edit Policy
Forensic Analysis
All Alarms for AP
Live View
Locate (Triangulation)
Test AP Connectivity
Switch Port Lookup
Generate Tracker Files
Action Details


You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Traffic Analysis

The **Traffic Analysis** tab provides a graphical and tabular view of the traffic transmitted and received by the device being analyzed. The first time you access the **Traffic Analysis** tab the graphical view is displayed.






You can switch to the table view by clicking the **Data Table**— button.

Traffic Analysis

Traffic Category:  Traffic Type:  TX  RX  All (Traffic in Bytes)

Time	TX % Retry	RX % Retry	TX Retryable Data	TX Retry	RX Retryable Data	RX Retry
<b>Totals</b>	1.467%	1.694%	3,874,076	56,835	3,920	66
4/6/11 4:10 PM	0%	0%	0	0	0	0
4/6/11 4:11 PM	2.892%	0%	4,565	132	0	0
4/6/11 4:12 PM	0%	0%	824	0	0	0
4/6/11 4:13 PM	0%	0%	2,266	0	0	0
4/6/11 4:14 PM	5.444%	0%	5,400	294	0	0
4/6/11 4:15 PM	0%	0%	2,472	0	0	0
4/6/11 4:16 PM	0%	0%	2,266	0	0	0
4/6/11 4:17 PM	0%	0%	0	0	0	0
4/6/11 4:18 PM	0%	0%	0	0	0	0
4/6/11 4:19 PM	0%	0%	0	0	0	0
4/6/11 4:20 PM	0%	0%	2,266	0	0	0
4/6/11 4:21 PM	2.96%	0%	4,966	147	0	0
4/6/11 4:22 PM	0%	0%	2,060	0	84	0
4/6/11 4:23 PM	0%	0%	2,266	0	0	0
4/6/11 4:24 PM	5.444%	0%	2,700	147	0	0
4/6/11 4:25 PM	0%	0%	4,532	0	0	0
4/6/11 4:26 PM	0%	0%	0	0	84	0
4/6/11 4:27 PM	0%	0%	4,120	0	0	0

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### Graphical View

The **Traffic Category** field determines the type of data displayed in the graph. You can change the traffic category by selecting one of the following categories from the **Traffic Category** drop-down menu:

- Ad-Hoc
- Control Details
- Data Details
- Destinations
- EAP Details
- Encryption Details
- Management Details
- Polled Information
- Rates
- Retry (default)
- Types.


The **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types. You can change the traffic type by selecting the appropriate radio button:

- RX
- TX

- All.

The left side of the graphical view has two columns:

Column	Description
Data Series	Acts as a filter to determine how the graphs are displayed. The <b>Traffic Type</b> field determines what is shown in this column. Anything with a checkmark in its checkbox will be seen in the graphs. If there is no checkmark, it is filtered out of the graph. Click on the checkbox to change the state.
Highlighted Value	If you position your cursor over any part of the graph, the values for that moment is displayed in this column.

You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

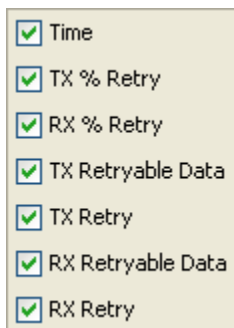
### Table View

Like the graphical view, the **Traffic Category** field determines what columns are displayed in the table. The same categories are used.


Also, the **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types in the table. You can change the traffic type by selecting the appropriate radio button.

The **Time** column is included in every traffic category. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).

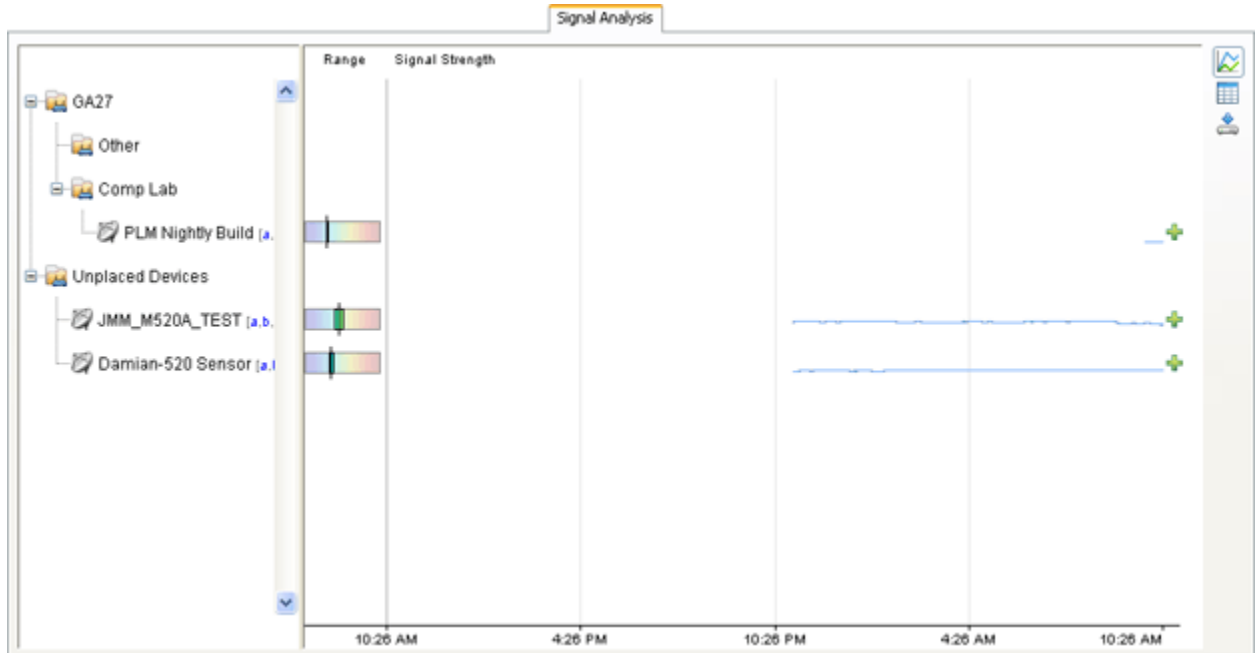



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.


## Signal Analysis

The **Signal Analysis** tab provides a graphical and tabular view of device signal strength as measured by various Sensors. The first time you access the **Signal Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

Time	JMM_M520A_TEST [a.b.g]	Damian-520 Sensor [a.b.g]	PLM Nightly Build [a.b.g]
<b>Totals</b>			
10/20/09 10:59 PM	-54	-67	
10/20/09 11:00 PM	-53	-67	
10/20/09 11:01 PM	-53	-67	
10/20/09 11:02 PM	-53	-67	
10/20/09 11:03 PM	-53	-67	
10/20/09 11:04 PM	-53	-67	
10/20/09 11:05 PM	-53	-67	
10/20/09 11:06 PM	-53	-67	
10/20/09 11:07 PM	-53	-67	
10/20/09 11:08 PM	-52	-67	
10/20/09 11:09 PM	-52	-67	
10/20/09 11:10 PM	-53	-67	
10/20/09 11:11 PM	-53	-66	
10/20/09 11:12 PM	-53	-66	
10/20/09 11:13 PM	-53	-66	
10/20/09 11:14 PM	-53	-66	
10/20/09 11:15 PM	-53	-66	
10/20/09 11:16 PM	-53	-66	
10/20/09 11:17 PM	-53	-66	

Click the **Data Chart**— button to switch back to the graphical view.


✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### **Graphical View**

The left side of the graphical view will have a list of Sensors that have seen the device being analyzed. The Sensors are grouped by network group and location. Click on the plus (+) or minus (-) sign to expand or collapse a category.

The right side of the graphical view displays a line chart for each Sensor to show the signal strength over time. A strength indicator is shown to the left of each line chart to show the minimum, maximum, and average signal strength for the entire time period.

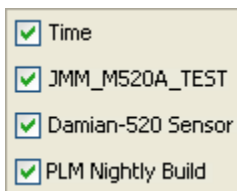
If you position your cursor over any part of a line chart, the exact reading for that moment is displayed in the top, right side of the **Signal Analysis** tab. If you position your cursor over any part of a strength indicator, the signal strength range is displayed (in dBm) in the top, right side of the **Signal Analysis** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### **Table View**


The table view will have a **Time** column and a column for each Sensor that has seen the device being analyzed. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

An option is included to remove empty rows. When selected, any row with no data is removed from the table. Click the **Remove empty rows** checkbox to select the option.

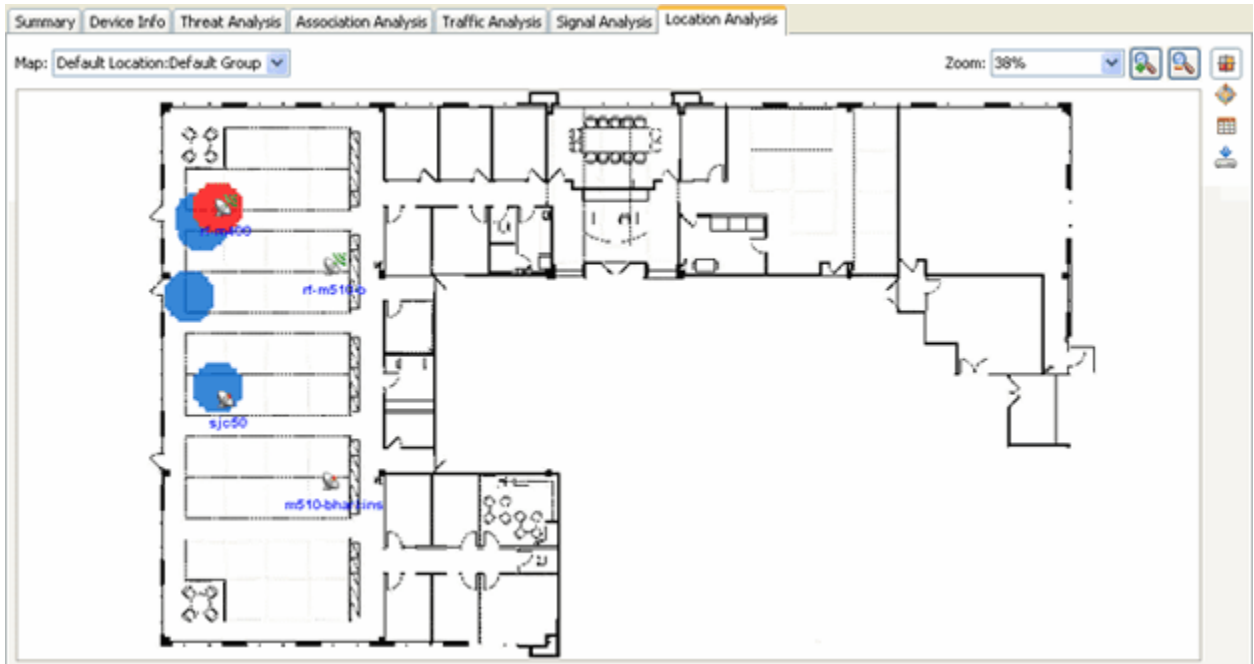
You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.


### **Location Analysis**

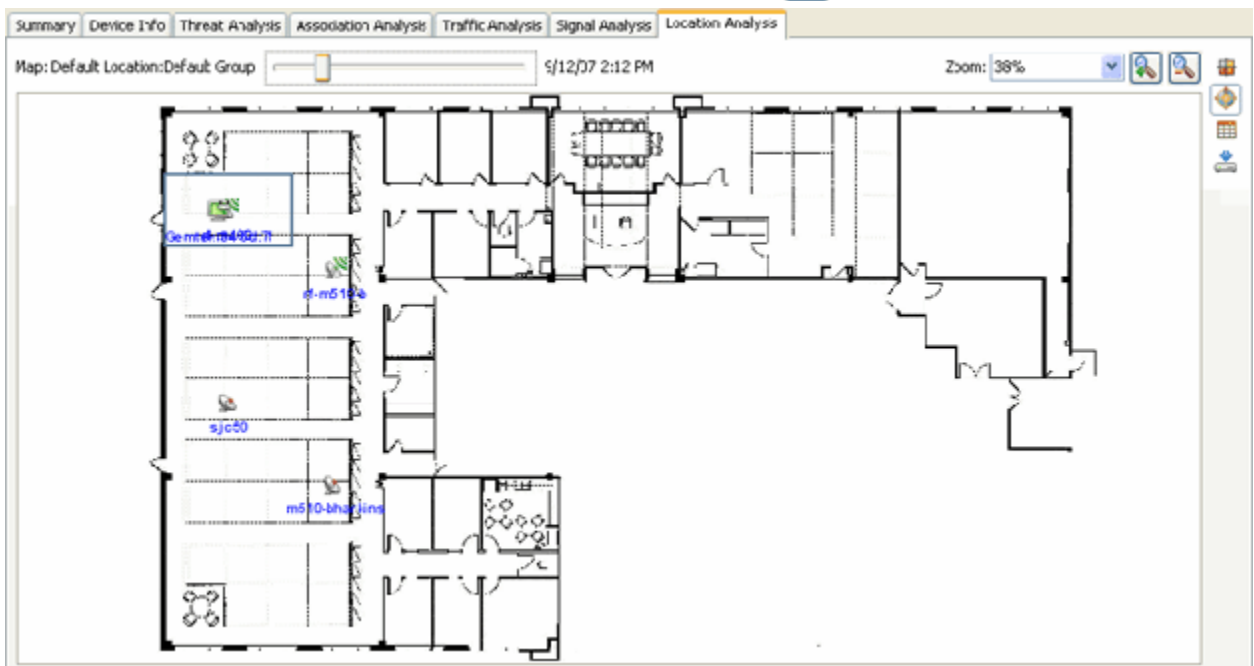
The **Location Analysis** tab provides a graphical and tabular view of the device location. The following three views are available:


- Heat Map
- Location Map
- Table View.

The first time you access the **Location Analysis** tab the Heat Map view is displayed.




You can switch to the Location Map by clicking the **Location Map**— button.



You can switch to the table view by clicking the **Data Table**— button.

Time	Map	X Offset Left (meters)	Y Offset from Top (meters)	Probability
3/12/07 13:00 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:01 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:02 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:03 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:04 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:05 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:06 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:12 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:13 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:14 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:15 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:16 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:17 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:18 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:19 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	75%
3/12/07 13:25 AM	Default Location:Default Group	16.112 Meters	16.369 Meters	73%
3/12/07 13:31 AM	Default Location:Default Group	16.112 Meters	27.342 Meters	59%
3/12/07 13:32 AM	Default Location:Default Group	16.112 Meters	27.342 Meters	59%
3/12/07 13:33 AM	Default Location:Default Group	14.347 Meters	22.229 Meters	64%
3/12/07 13:34 AM	Default Location:Default Group	14.347 Meters	22.229 Meters	64%
3/12/07 13:35 AM	Default Location:Default Group	15.229 Meters	17.373 Meters	68%

Click the **Heat Map**— button to switch back to the Heat Map.






**NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### Heat Map

The Heat Map uses a heat map to show where the device was located during the entire forensic period. Higher temperatures indicate that the device was at a particular location for a longer period of time. You may select any location-tracking map in the system for display as a Heat Map. Use the **Map** drop-down menu to select another map.

You may zoom in or out while viewing a map as follows:

- Use the **Zoom** drop-down menu to select a zoom value.
- Use the **Zoom In**— button to zoom in (make map larger).
- Use the **Zoom Out**— button to zoom out (make map smaller).

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Location Map

The Location Map displays a device's location at a specific point in time. Use the **Time** slider to adjust the time to a specific minuter during the forensic analysis period. As the slider is moved the device's location is adjusted on the location map. In addition, the map is automatically switched if the device moves between maps during the time period.

The zoom controls and buttons work the same as they do in the Heat Map.

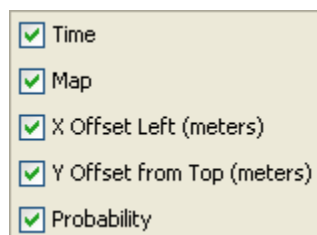
### Table View

Table view displays the device location over a period of time in a tabular form. Location data is given in the following columns:


Column	Description
Time	Time of day in 1 minute increments.
Map	Name of location map.
X Offset Left	Distance from the left (in meters).
Y Offset from Top	Distance from the top (in meters).
Probability	A percentage representing the probability that the device will not move for its current position.

Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## APs

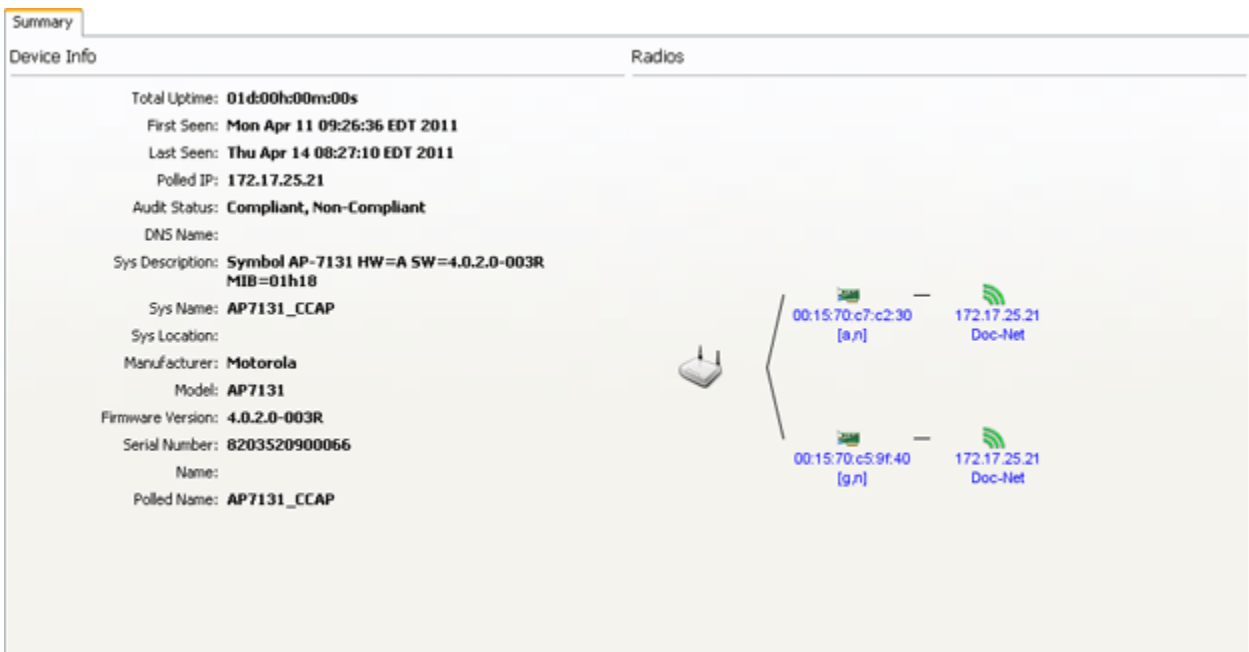
The following six tabs are available for APs:

- Summary
- Device Info
- Threat Analysis
- Adoption History
- Radio Analysis
- Radio Info.

Each tab is discussed as a separate topic.

## Summary

The **Summary** tab for the Device Based Advanced Forensic Analysis for APs is basically the same as the Basic Forensic Analysis **Summary** tab for APs. It provides information about the AP as well as the MAC address of each radio and the protocol that is being used. Also, BSS information is displayed (IP address and SSID). Each time you access Device Based Forensic Analysis for APs the **Summary** tab is the first one displayed.



**Summary**

**Device Info**

Total Uptime: **01d:00h:00m:00s**  
 First Seen: **Mon Apr 11 09:26:36 EDT 2011**  
 Last Seen: **Thu Apr 14 08:27:10 EDT 2011**  
 Polled IP: **172.17.25.21**  
 Audit Status: **Compliant, Non-Compliant**  
 DNS Name:  
 Sys Description: **Symbol AP-7131 HW=A SW=4.0.2.0-003R MIB=01h18**  
 Sys Name: **AP7131\_CCAP**  
 Sys Location:  
 Manufacturer: **Motorola**  
 Model: **AP7131**  
 Firmware Version: **4.0.2.0-003R**  
 Serial Number: **8203520900066**  
 Name:  
 Polled Name: **AP7131\_CCAP**

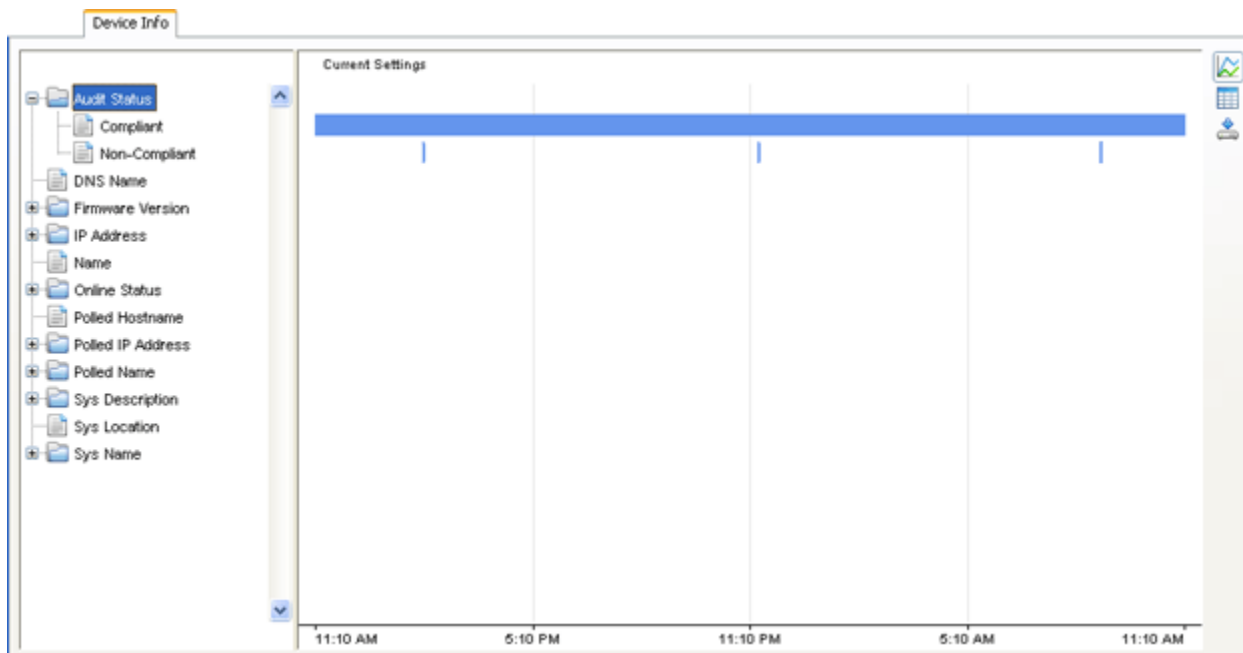
**Radios**


00:15:70:c7:c2:30 [a,n] 172.17.25.21 Doc-Net  
 00:15:70:c5:9f:40 [g,n] 172.17.25.21 Doc-Net




### Device Info

The **Device Info** tab provides a graphical and tabular view of the current settings for the AP being analyzed. The first time you access the **Device Info** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

Time	Audit St...	DNS Name	Firmwar...	IP Address	Name	Online S...	Polled H...	Polled I...	Polled N...	Sys Des...	Sys Loc...	Sys Name
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...
4/12/11 11...	Compliant		4.0.2.0-003R	172.17.25...		Online		172.17.25...	AP7131_C...	Symbol AP...		AP7131_C...

Click the **Data Chart**— button to switch back to the graphical view.


✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### ***Graphical View***

The left side of the graphical view lists the categories shown in the chart (right side). Click on the plus (+) or minus (-) sign to expand or collapse a category which will show any changes in the category. The categories are:

- Audit Status
- DNS Name
- Firmware Version
- IP Address
- Name
- Online Status
- Polled Hostname
- Polled IP Address
- Polled Name
- Sys Description
- Sys Location
- Sys Name.

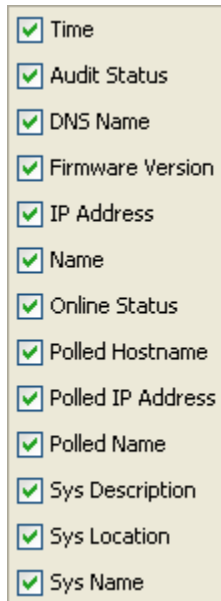
If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Device Info** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### ***Table View***


The table view has a column for each of the categories shown in the graphical view plus a **Time** category. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



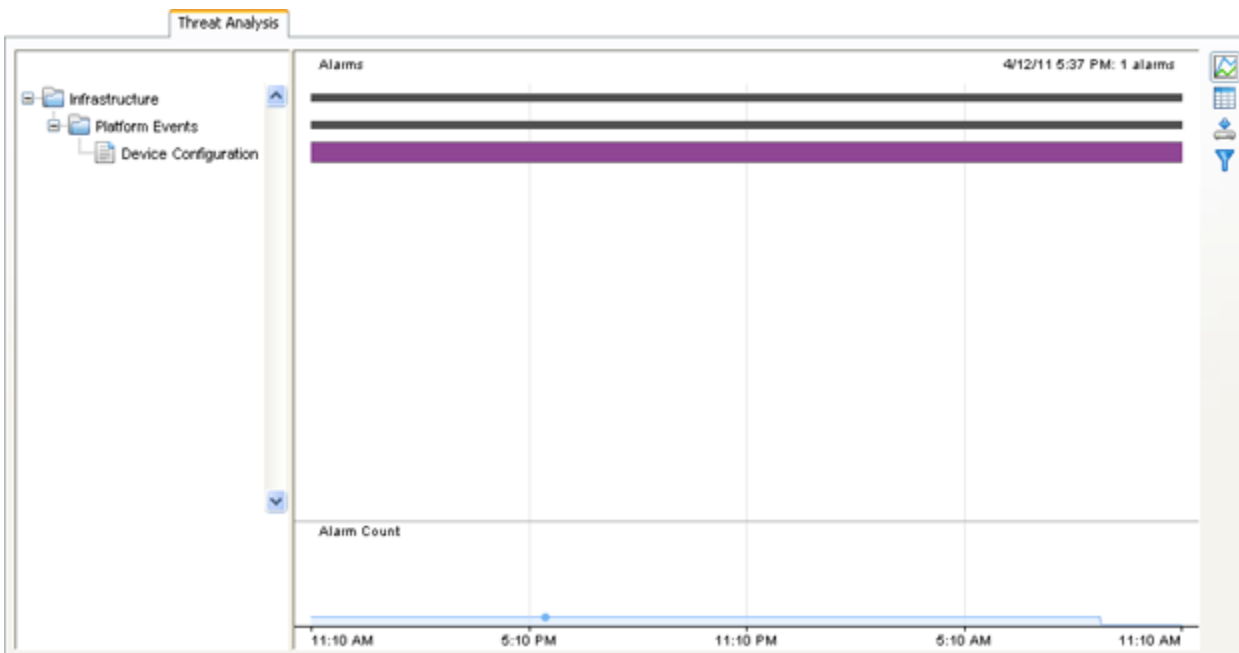
- Rearrange columns by clicking on a column heading and dragging it to a new position.


The table may be shown with one row per minute or one row for every change in the value of a particular column (category). Click the appropriate radio button in the top, left side of the **Device Info** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## Threat Analysis


The **Threat Analysis** tab provides a graphical and tabular view of the alarms for the device being analyzed. The first time you access the **Threat Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

The screenshot shows the 'Threat Analysis' interface in table view. The table has columns for 'Criticality', 'Category', 'Type', 'Start Time', and 'Expiration'. A single row is displayed with the following data:

Criticality	Category	Type	Start Time	Expiration
Severe (95)	Platform Events	Device Configuration Not Compl...	Before Time Range	After Time Range

Click the **Data Chart**— button to switch back to the graphical view.

- ✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

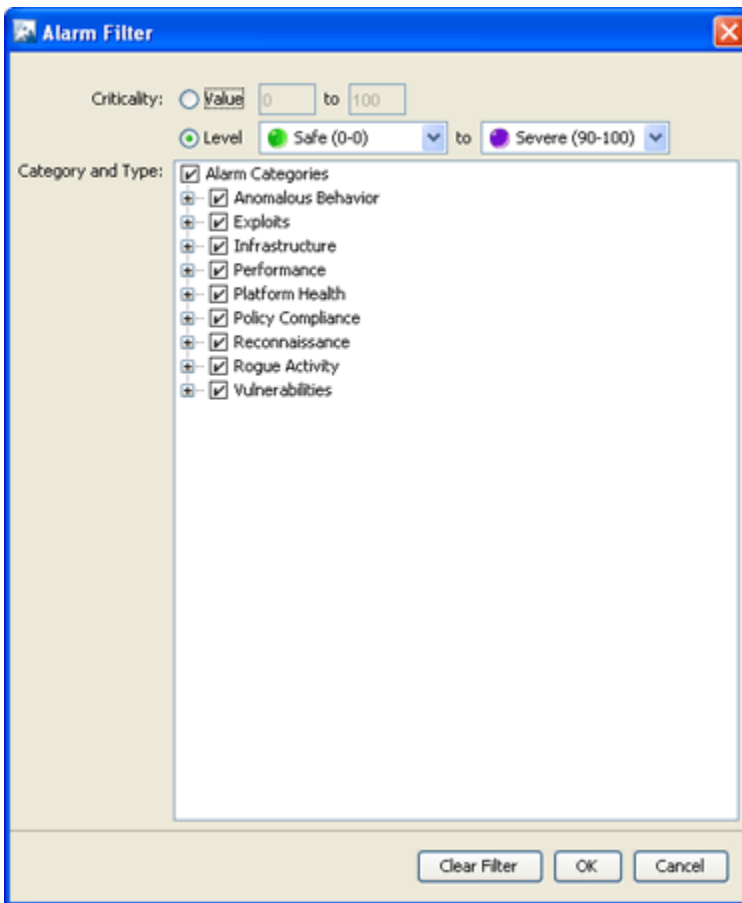
### **Graphical View**

The left side of the graphical view lists the categories shown in the chart (right side). Click on the plus (+) or minus (-) sign to expand or collapse a category which will show any changes in the category. The categories are:

- Anomalous Behavior
- Exploits
- Infrastructure
- Performance
- Platform Health
- Policy Compliance
- Reconnaissance
- Rogue Activity
- Vulnerabilities
- System Health
- Vulnerabilities.

If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Threat Analysis** tab.


Clicking the **Filter Data**—  button displays an **Alarm Filter** window where you can filter the alarm data that is shown in graph.



Changes to the following fields will affect the filter:

Field	Description
Criticality	Change the criticality by entering exact values for a range or selecting a starting level and an ending level. To enter the values, select the <b>Value</b> radio button and then enter values from 1 to 100. To select levels, select the <b>Level</b> radio button and then select the levels using the drop-down menus.
Category and Type	By default, all categories and types are selected, to deselect a category or type, remove the checkmark in the checkbox next to the category or type. Click the plus (+) or minus (-) sign to expand or collapse a category.

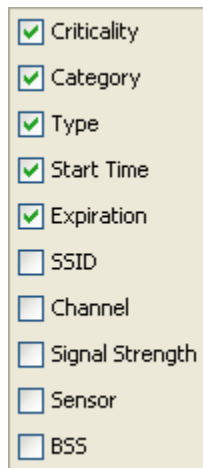
Click the **OK** button to activate your changes. The **Clear Filter** button will reset all fields back to their default state. The **Cancel** button will cancel any changes.

You can export the table data to a CSV file by clicking the **Export Data**—  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### ***Table View***

The table view has a column for each of the categories shown in the graphical view plus a **Time** category. Column display and arrangement can be customized as follows:


- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm. See the **Alarm Details** window topic for more information.


You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

The **Filter Data**— button works the same as it does in the graphical view.

### Adoption History

The **Adoption History** tab provides a graphical and tabular view of the devices that have adopted an AP. The first time you access the **Adoption History** tab the graphical view is displayed.




You can switch to the table view by clicking the **Data Table**— button.

Adoption History

Group by associated device


Device	Start	End	Duration
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:10 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:13 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:18 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:23 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:28 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:33 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:38 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:43 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:48 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:53 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 11:58 AM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:03 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:08 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:13 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:18 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:23 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:28 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:33 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:38 PM	11.5 days
RFS4000-C Collier	Ongoing Adoption	4/12/11 12:43 PM	11.5 days

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

### Graphical View

The left side of the graphical view lists the devices shown in the chart (right side). The network levels are also shown so that you can see where the device is located. Click on the plus (+) or minus (-) sign to expand or collapse a category.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Table View

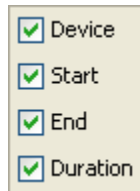
The table view displays the following information in tabular form:

Column	Description
Device	The name of the device that adopted the AP.
Start	The date and time when the adoption first occurred. This can be an ongoing adoption.
End	The date and time when the adoption last occurred.
Duration	The amount of time that the adoption has lasted.

Column display and arrangement can be customized as follows:




- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



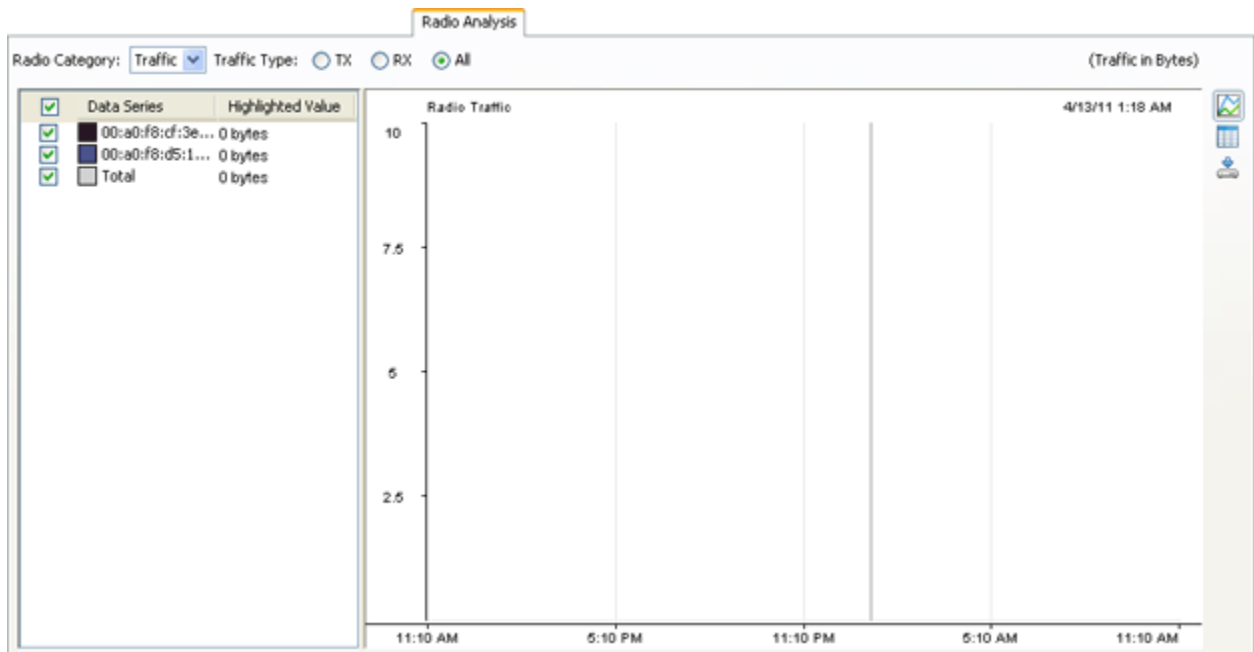
- Rearrange columns by clicking on a column heading and dragging it to a new position.


The **Group by associated device** field allows you to group devices of the same type together.

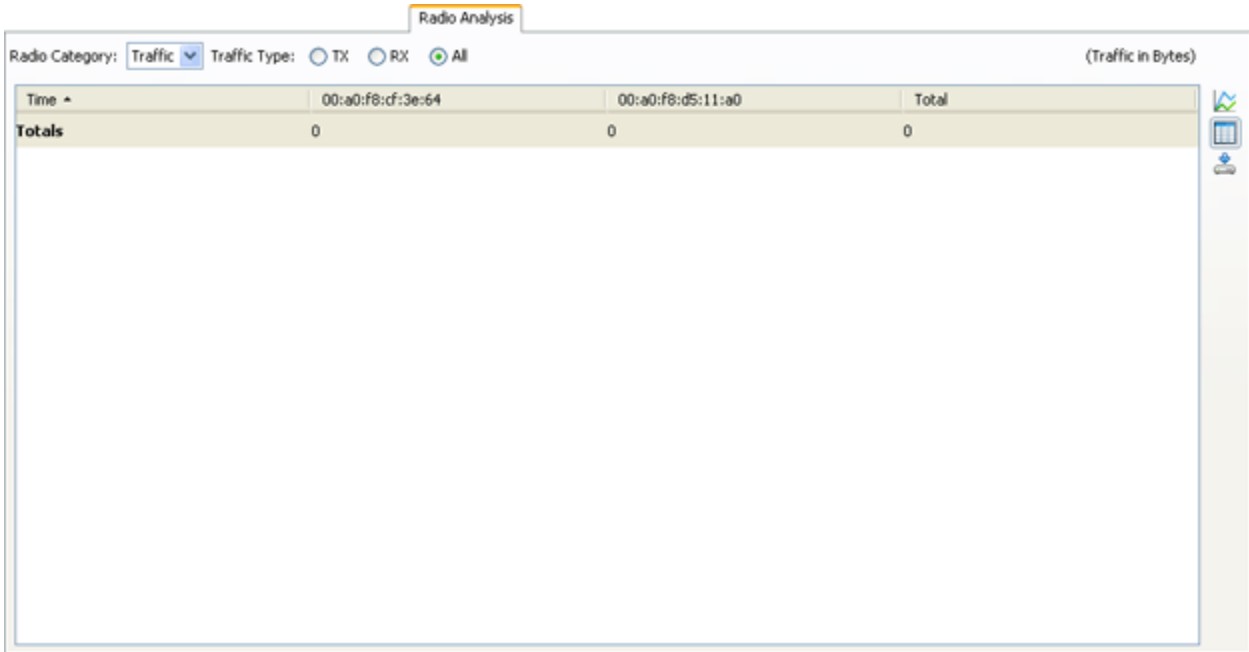
You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.


### Radio Analysis

The **Radio Analysis** tab provides information that can be used to analyze your APs radios. The first time you access the **Radio Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.



Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

**Graphical View**

The information displayed varies depending on the selected radio category. The categories are:


- Noise—Displays the average noise seen on each radio in dBm.
- Power—Displays the average power used by each radio over time.
- Retry—Displays the total number of retries that has occurred from data being retransmitted.
- Traffic (default)—Displays the total traffic seen on each radio in bytes.

The **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types. You can change the traffic type by selecting the appropriate radio button:

- RX
- TX
- All.

The left side of the graphical view has two columns:

Column	Description
Data Series	Acts as a filter to determine how the graphs are displayed. The <b>Radio Category</b> field determines what is shown in this column. Anything with a checkmark in its checkbox will be seen in the graphs. If there is no checkmark, it is filtered out of the graph. Click on the checkbox to change the state.
Highlighted Value	If you position your cursor over any part of the graph, the values for that moment is displayed in this column.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

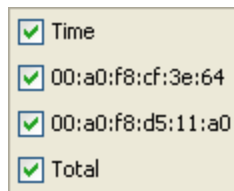
### **Table View**

Like the graphical view, the **Radio Category** field determines what columns are displayed in the table. The same categories are used.


The **Traffic Type** field determines whether you see transmitting data, receiving data, or all data types in the table. You can change the traffic type by selecting the appropriate radio button.

The **Time** column is included in every traffic category while the other columns reflect the MAC address of the radio which display the averages or totals of the traffic. Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).

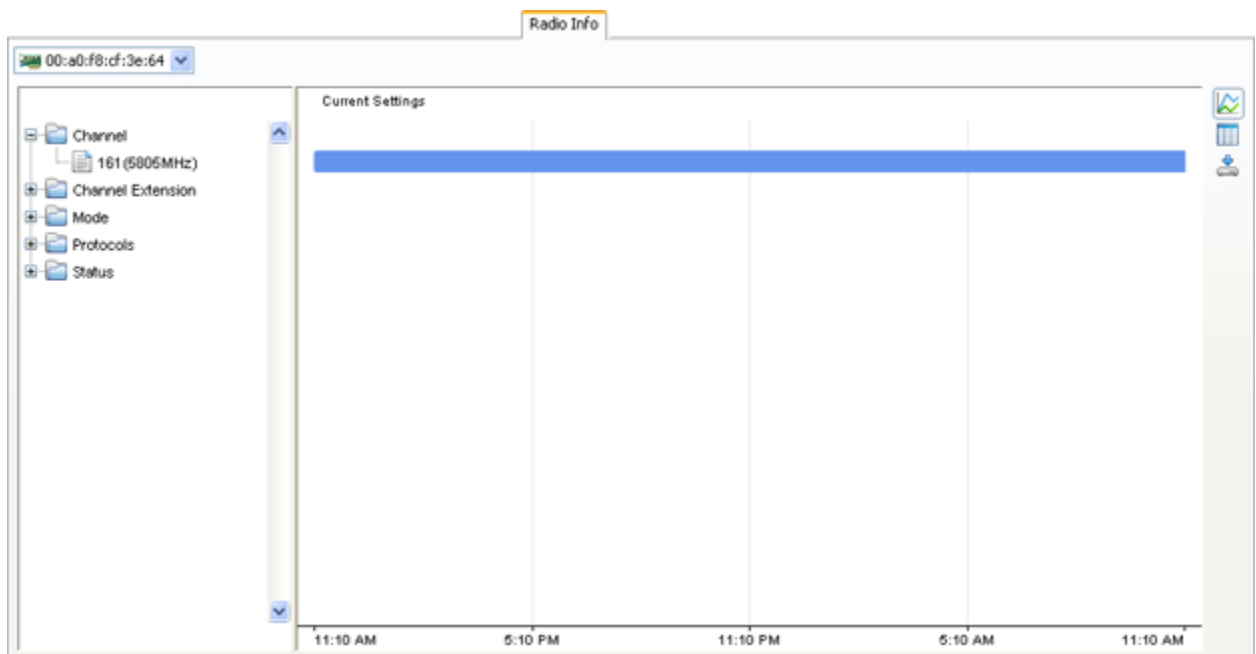



- Rearrange columns by clicking on a column heading and dragging it to a new position.

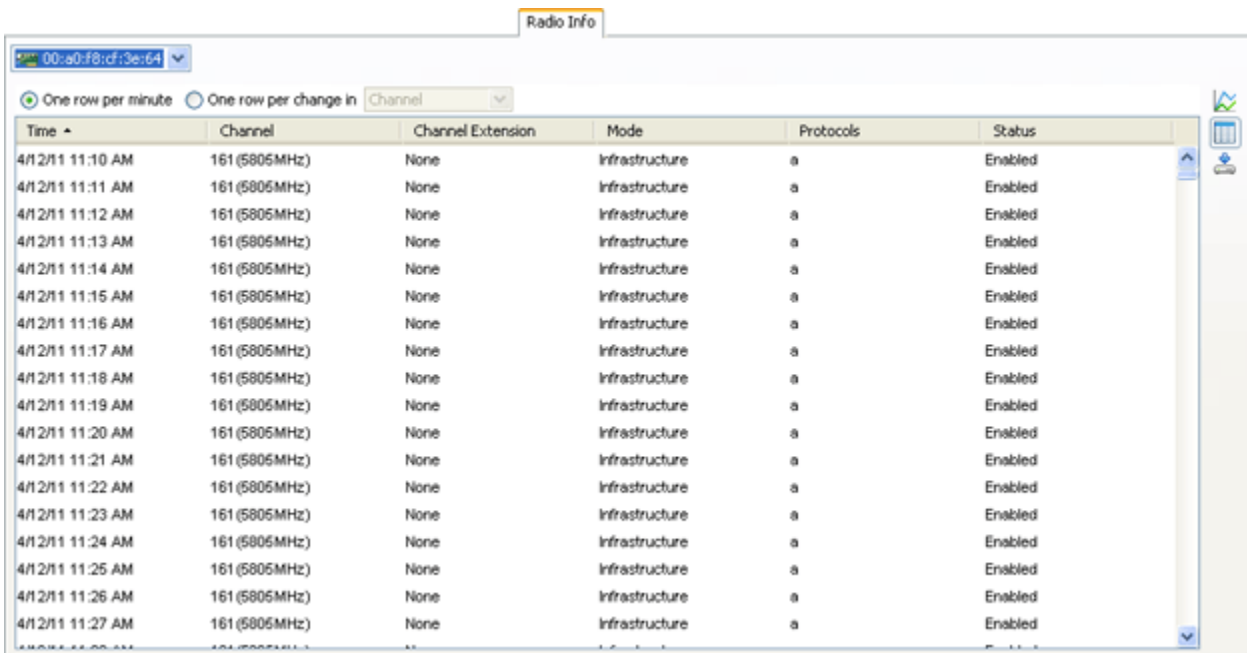
You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### **Radio Info**


The **Radio Info** tab provides AP radio information recorded at the displayed time. The first time you access the **Radio Info** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.



Time	Channel	Channel Extension	Mode	Protocols	Status
4/12/11 11:10 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:11 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:12 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:13 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:14 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:15 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:16 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:17 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:18 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:19 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:20 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:21 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:22 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:23 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:24 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:25 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:26 AM	161 (5805MHz)	None	Infrastructure	a	Enabled
4/12/11 11:27 AM	161 (5805MHz)	None	Infrastructure	a	Enabled

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.


### **Graphical View**

The left side of the graphical view lists the categories shown in the chart (right side). Click on the plus (+) or minus (-) sign to expand or collapse a category which will show any changes in the category. The categories are:

- Channel
- Channel Extension
- Mode
- Protocols
- Status.

These categories are the same as the column headers in the table view which are explained below.

If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Radio Info** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

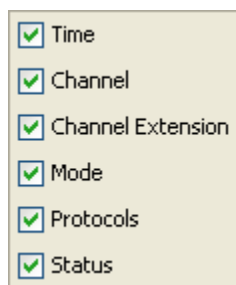
**Table View**

The information displayed is as follows:

Column	Description
Time	The date and time of day when the information was recorded.
Channel	The WLAN broadcast channel for the device.
Channel Extension	The channel extension being used if any.
Mode	The mode the AP radio is operating in (Infrastructure or Sensor).
Protocols	The protocols being used by the AP radio (a,b,g,n).
Status	The status of the AP radio (enabled or disabled).


Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

The table may be shown with one row per minute or one row for every change in the value of a particular column (category) chosen from the drop-down menu. Click the appropriate radio button in the top, left side of the **Radio Info** tab.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

**Switches**

The following five tabs are available for Switches:

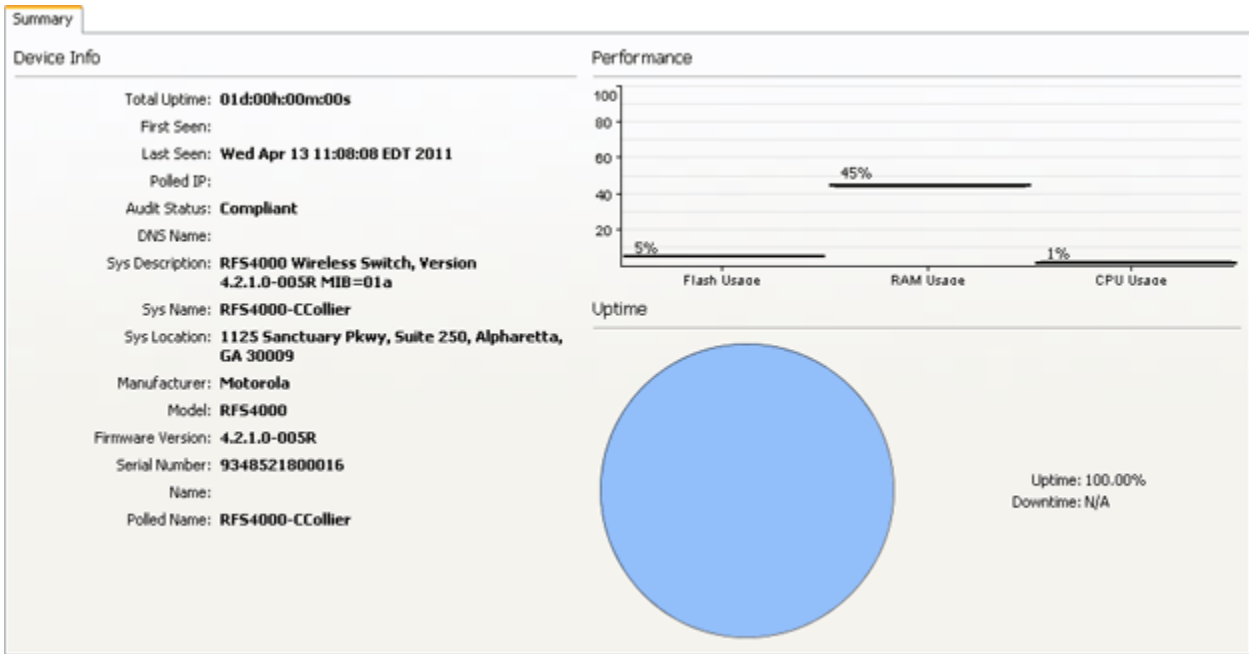
- Summary
- Device Info
- Threat Analysis
- Adoption History
- Performance Analysis.

Each tab is discussed as a separate topic.

**Summary**

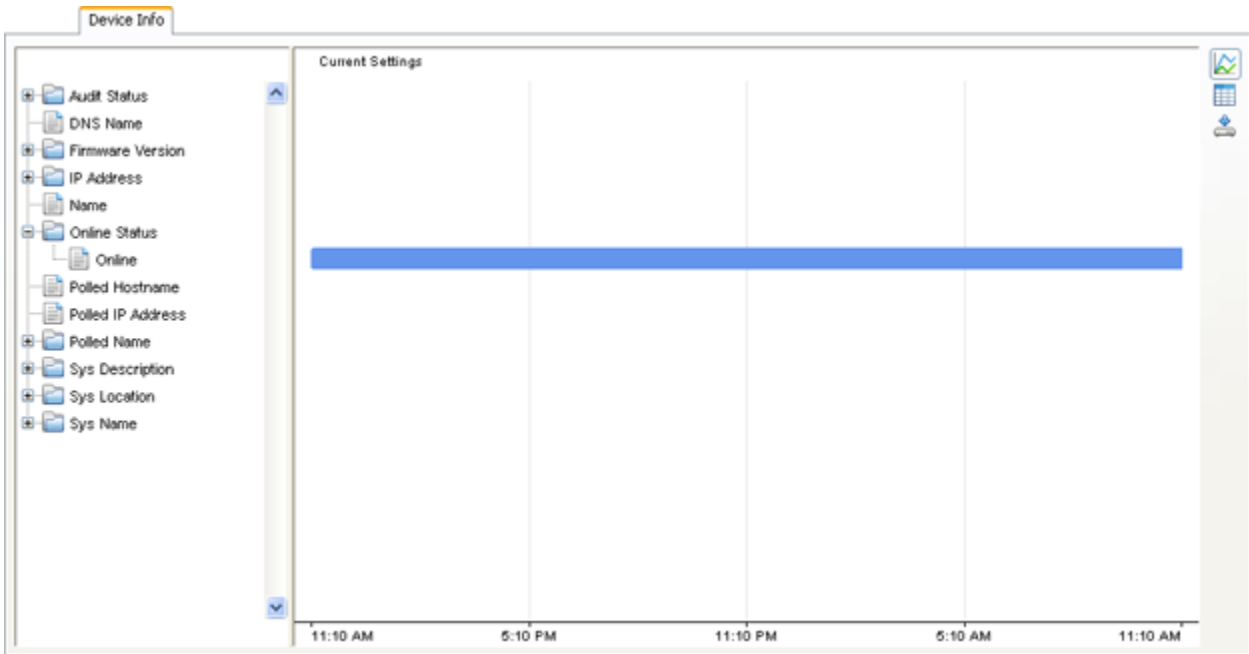
The **Summary** tab for the Device Based Advanced Forensic Analysis for Switches is basically the same as the Basic Forensic Analysis **Summary** tab for Switches. It provides summary and performance information about

the Switch as well as the uptime and downtime of the Switch. Each time you access Device Based Forensic Analysis for Switches, the **Summary** tab is the first one displayed.




### Device Info

The **Device Info** tab displays the current settings for the Switch being analyzed. The first time you access the **Device Info** tab the graphical view is displayed.





You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### ***Table View***

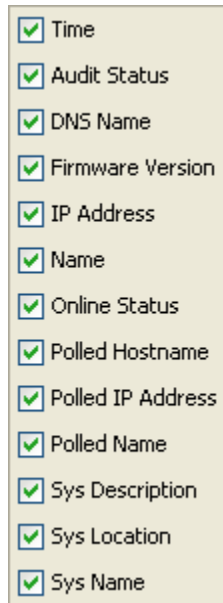
The table view has a column for each of the categories shown in the graphical view plus a **Time** category.

<b>Column</b>	<b>Description</b>
Time	The date and time of day when the Switch was seen.
Audit Status	The status of the last audit (compliant or non-compliant).
DNS Name	The DNS name assigned to the Switch.
Firmware Version	The current firmware version installed on the Switch.
IP Address	The Switch's Internet Protocol address.
Name	The name of the Switch. The name is specified by a user through the Switch's properties.
Online Status	The online/offline status of the Switch.
Polled Hostname	The hostname that is pulled from the Switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.
Polled IP Address	The IP address that is pulled from the Switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.
Polled Name	The device name that is pulled from the Switch by ADSP either upon import/discovery of the switch or when ADSP does a data poll.
Sys Description	A description of the Switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.
Sys Location	The location of the Switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.
Sys Name	The name of the Switch. This information is obtain from an import/discovery of the switch or when ADSP does a data poll.

Column display and arrangement can be customized as follows:




- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



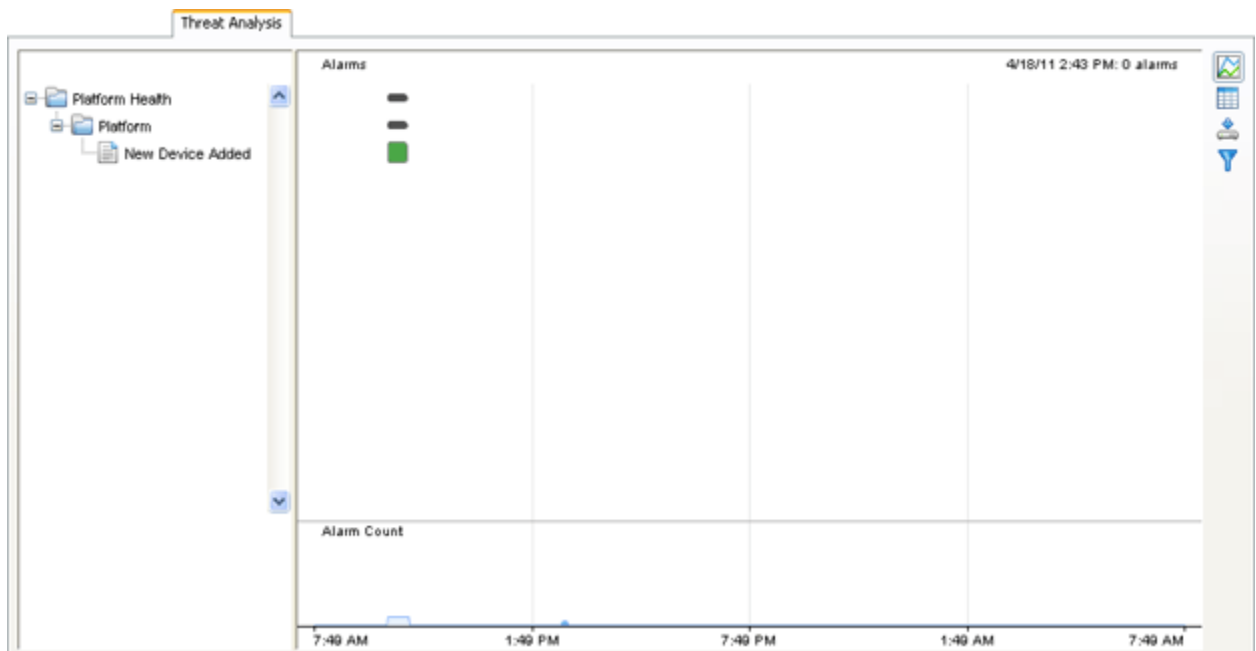
- Rearrange columns by clicking on a column heading and dragging it to a new position.


The table may be shown with one row per minute or one row for every change in the value of a particular column (category). Click the appropriate radio button in the top, left side of the **Device Info** tab.

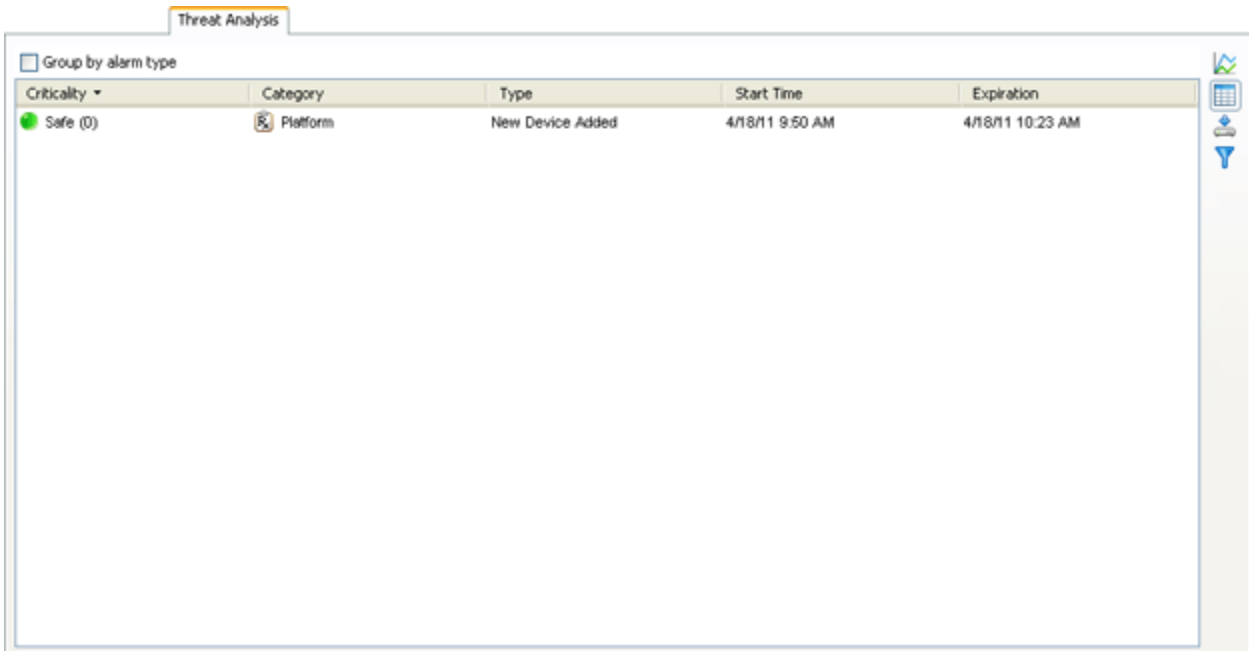
You can export the table data to a CSV file by clicking the **Export Data**  button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

### Threat Analysis


The **Threat Analysis** tab displays the alarms generated by the Switch being analyzed. The first time you access the **Threat Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.



Criticality	Category	Type	Start Time	Expiration
Safe (0)	Platform	New Device Added	4/18/11 9:50 AM	4/18/11 10:23 AM

Click the **Data Chart**— button to switch back to the graphical view.



**NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

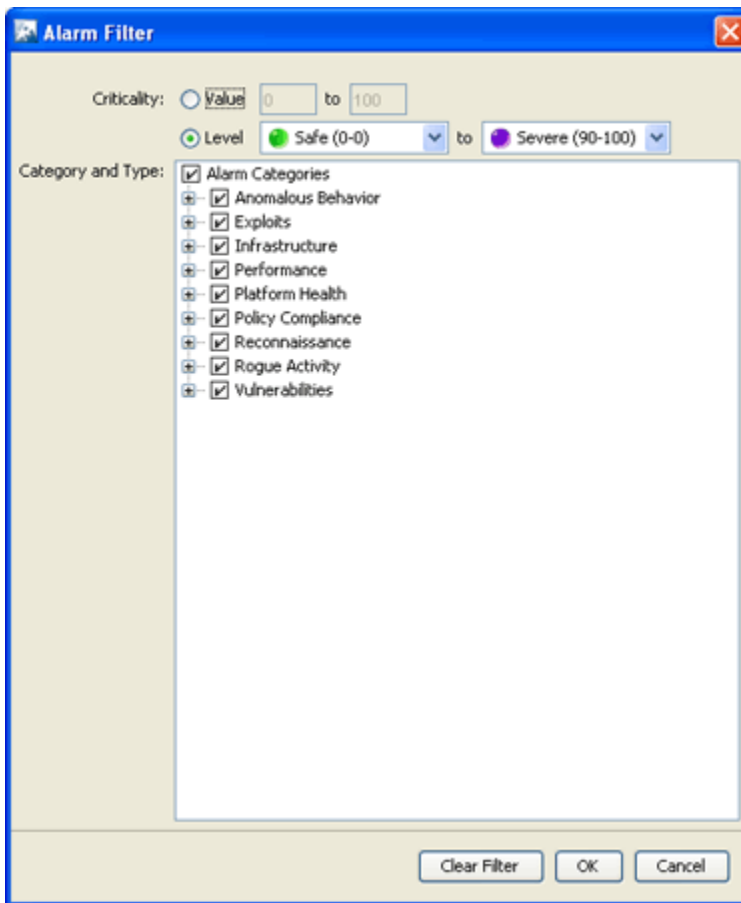
### **Graphical View**

The left side of the graphical view lists the categories shown in the chart (right side). Click on the plus (+) or minus (-) sign to expand or collapse a category. The categories can be any of the following:

- Anomalous Behavior
- Exploits
- Infrastructure
- Performance
- Platform Health
- Policy Compliance
- Reconnaissance
- Rogue Activity
- Vulnerabilities
- System Health
- Vulnerabilities.

If you position your cursor over any part of the graphical data, the exact reading for that moment is displayed in the top, right side of the **Threat Analysis** tab.


Clicking the **Filter Data**— button displays an **Alarm Filter** window where you can filter the alarm data that is shown in graph.



Changes to the following fields will affect the filter:

Field	Description
Criticality	Change the criticality by entering exact values for a range or selecting a starting level and an ending level. To enter the values, select the <b>Value</b> radio button and then enter values from 1 to 100. To select levels, select the <b>Level</b> radio button and then select the levels using the drop-down menus.
Category and Type	By default, all categories and types are selected, to deselect a category or type, remove the checkmark in the checkbox next to the category or type. Click the plus (+) or minus (-) sign to expand or collapse a category.

Click the **OK** button to activate your changes. The **Clear Filter** button will reset all fields back to their default state. The **Cancel** button will cancel any changes.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

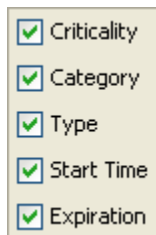
***Table View***

The information displayed is as follows:

Column	Description
Criticality	The color designation and name for the threat level, as follows: <ul style="list-style-type: none"> <li><span style="color: purple;">●</span> Severe—Serious alarms that may have catastrophic effects on your WLAN.</li> <li><span style="color: red;">●</span> High/Critical—Serious alarms on devices that require immediate attention.</li> <li><span style="color: orange;">●</span> Elevated/Major—Potentially serious alarms on devices that require priority attention.</li> <li><span style="color: yellow;">●</span> Guarded/Minor—Potential problem alarms on devices that may develop into worse issues if left alone.</li> <li><span style="color: green;">●</span> Safe/Low—Devices that pose no immediate threat to your WLAN network.</li> </ul>
Category	The type of category that the alarm falls under.
Type	The specific type of alarm, providing detailed information as to what generated the alarm in the first place.
Start Time	The date and time group of when the alarm first occurred.
Expiration	The date and time group of when the alarm will expire. The alarm can be an ongoing alarm which never expires.

Column display and arrangement can be customized as follows:

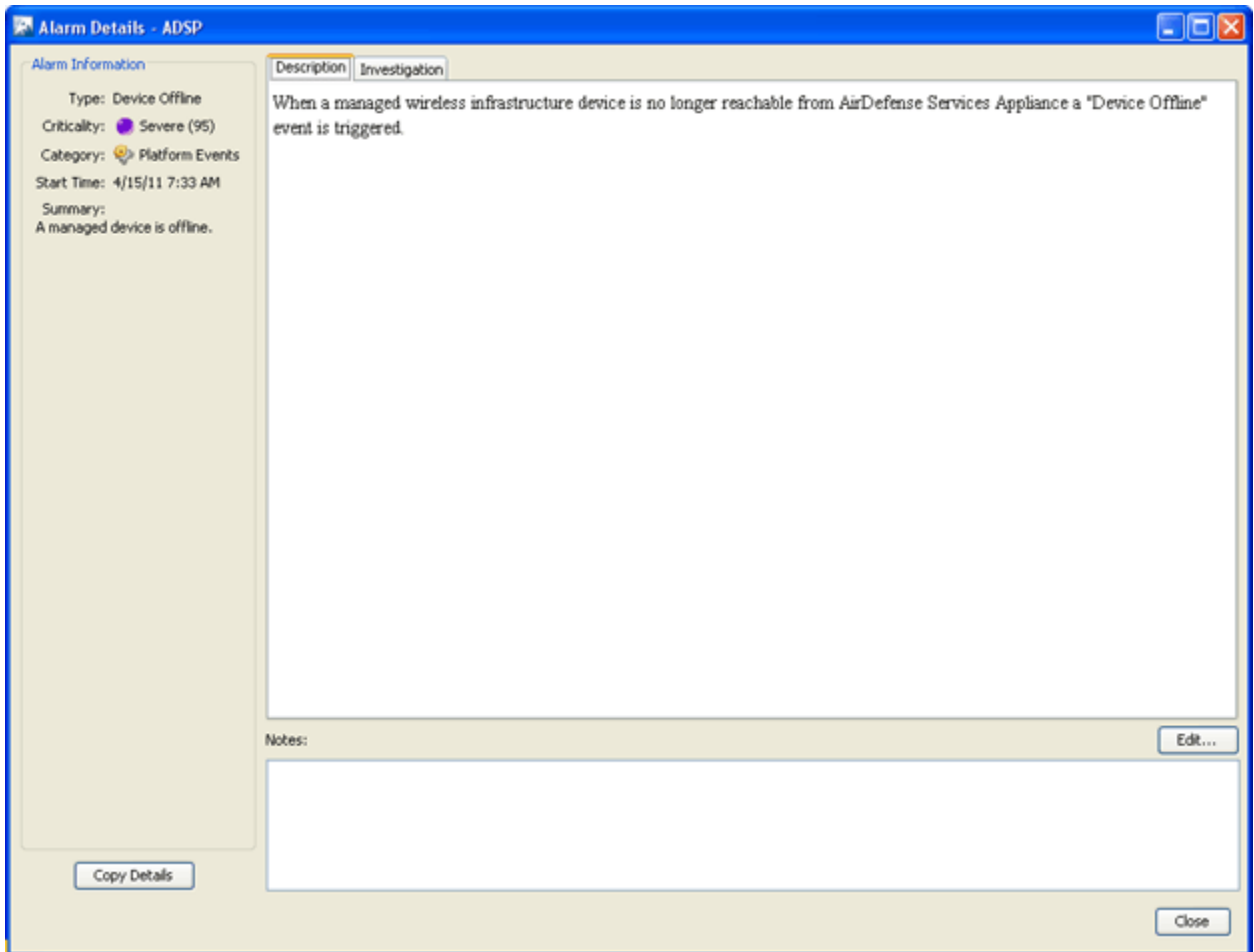
- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).





- Rearrange columns by clicking on a column heading and dragging it to a new position.

The **Group by alarm type** field allows you to group all alarms of the same type together. Only the alarm type is displayed in the table.

Right-clicking on an alarm and selecting **Alarm Details** displays the **Alarm Details** window where you can find detailed information about an alarm.

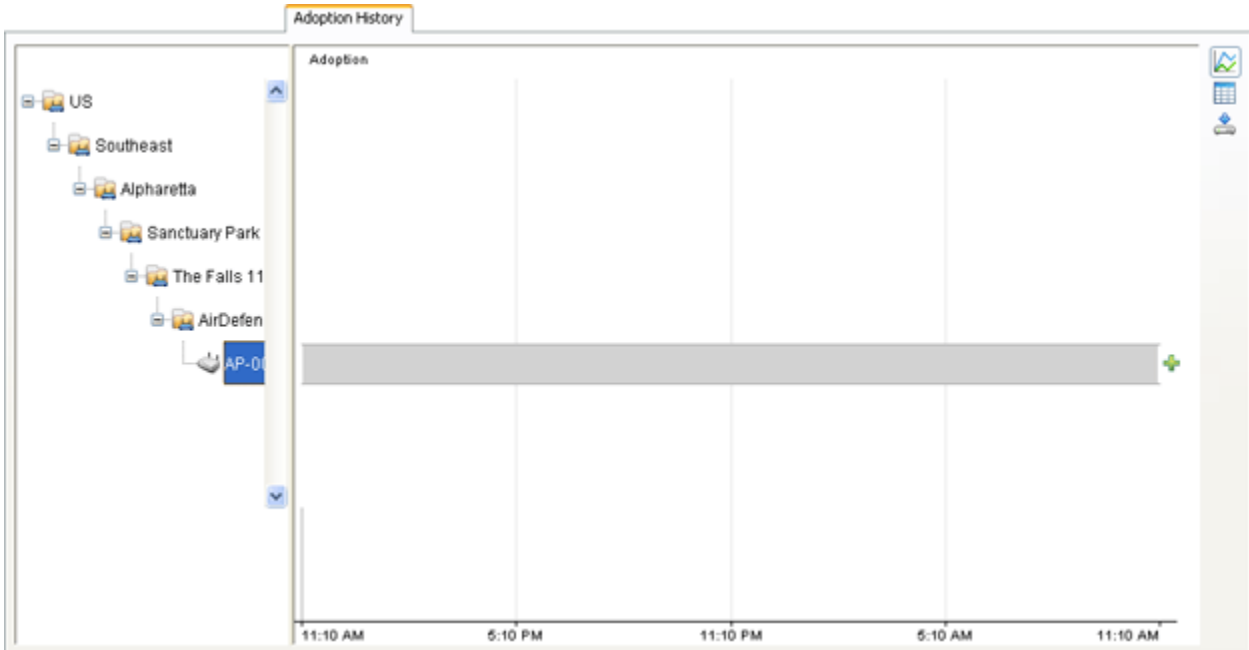



You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

The **Filter Data**— button works the same as it does in the graphical view.


## Adoption History

The **Adoption History** tab gives you a method to determine which devices a Switch has adopted. The first time you access the **Adoption History** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.


Device	Start	End	Duration
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:10 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:13 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:18 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:23 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:28 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:33 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:38 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:43 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:48 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:53 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 11:58 AM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:03 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:08 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:13 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:18 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:23 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:28 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:33 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:38 PM	11.5 days
AP-00-A0-F8-8B-B9-E2	Ongoing Adoption	4/12/11 12:43 PM	11.5 days

Click the **Data Chart**— button to switch back to the graphical view.

✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.

**Graphical View**

The left side of the graphical view lists the devices shown in the chart (right side). The network levels are also shown so that you can see where the device is located. Click on the plus (+) or minus (-) sign to expand or collapse a network level.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

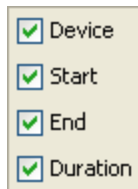
**Table View**

The table view displays the following information in tabular form:

Column	Description
Device	The name of the device that adopted the AP.
Start	The date and time when the adoption first occurred. This can be an ongoing adoption.
End	The date and time when the adoption last occurred.
Duration	The amount of time that the adoption has lasted.


Column display and arrangement can be customized as follows:

- Hide a category by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.


The **Group by associated device** field allows you to group devices of the same type together.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

**Performance Analysis**


The **Performance Analysis** tab provides performance raw data and usage percentages for a Switch. The first time you access the **Performance Analysis** tab the graphical view is displayed.



You can switch to the table view by clicking the **Data Table**— button.

The screenshot shows the 'Performance Analysis' window in table view. The 'Performance Category' is 'Raw Data'. The table below shows the following data:

Timestamp	Flash	RAM
4/12/11 11:10 AM	4120	93228
4/12/11 11:12 AM	4120	93228
4/12/11 11:13 AM	4120	93284
4/12/11 11:15 AM	4120	93284
4/12/11 11:18 AM	4120	93292
4/12/11 11:21 AM	4120	93292
4/12/11 11:23 AM	4120	93236
4/12/11 11:24 AM	4120	93236
4/12/11 11:27 AM	4120	93236
4/12/11 11:28 AM	4120	93116
4/12/11 11:30 AM	4120	93116
4/12/11 11:33 AM	4120	93256
4/12/11 11:36 AM	4120	93256
4/12/11 11:38 AM	4120	93228
4/12/11 11:39 AM	4120	93228
4/12/11 11:42 AM	4120	93228
4/12/11 11:43 AM	4120	93340
4/12/11 11:45 AM	4120	93340
4/12/11 11:48 AM	4120	93248
4/12/11 11:51 AM	4120	93248

Click the **Data Chart**— button to switch back to the graphical view.


✓ **NOTE** The last view is memorized and will be displayed until you change views. This is true even if you exit the application.



### Graphical View

The graphical view displays a graph of raw data for the CPU, flash memory, or RAM usage (in percentage) according to the selected Performance Category field (Raw Data or Percentage). The left side of the graphical view has two columns:

Column	Description
Data Series	Acts as a filter to determine how the graphs are displayed. The <b>Performance Category</b> field determines what is shown in this column. Anything with a checkmark in its checkbox will be seen in the graphs. If there is no checkmark, it is filtered out of the graph. Click on the checkbox to change the state.
Highlighted Value	If you position your cursor over any part of the graph, the values for that moment are displayed in this column.

You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

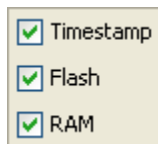
### Table View

The **Performance Category** field determines what information is displayed in the table. You can change the performance category by making a selection from the drop-down menu:


- Raw Data
- Percentage.

The **Timestamp** column is included in every performance category. The other columns vary according to the selected display category. Column display and arrangement can be customized as follows:

- Hide a column by right-clicking in the column heading area and uncheck the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

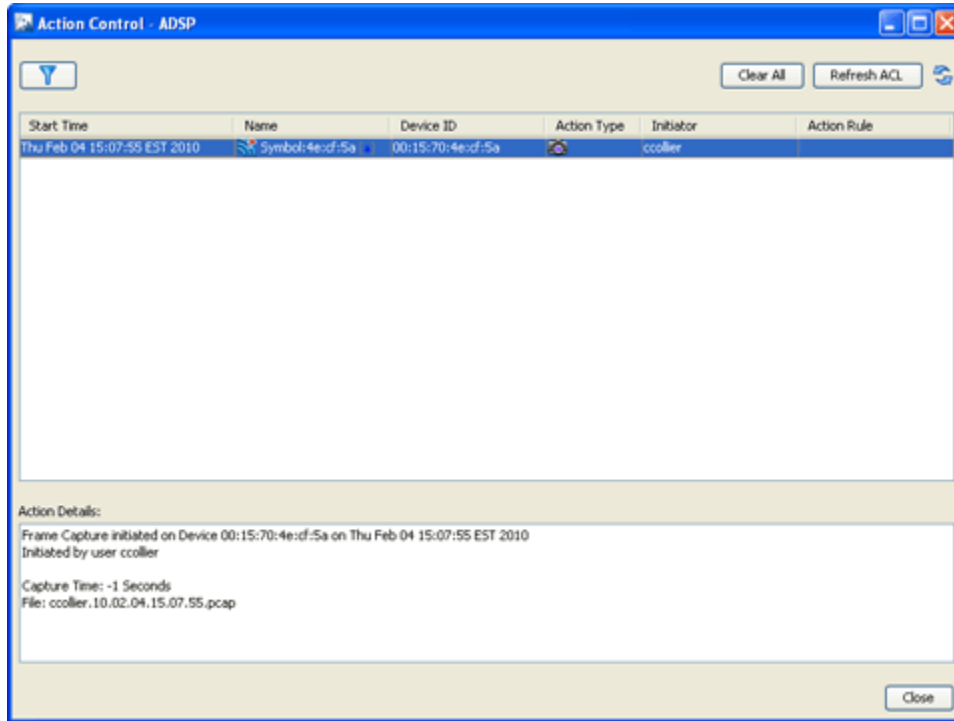
You can export the table data to a CSV file by clicking the **Export Data**— button. An **Export Table** window will display where you can name and save the file to a location on your hard drive.

## 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

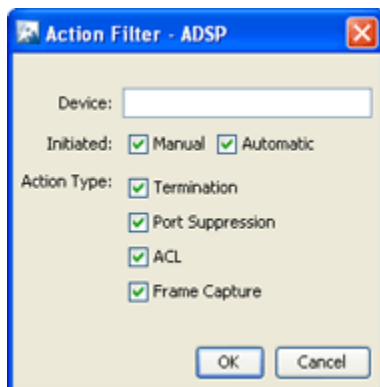
Also, while an action is highlighted, you can right click on the action to display options (commands) that can be performed on that action. The following commands are available:

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.

## Action Filter

The Action Filter is used to control which actions are displayed in the Action Control table. Click the **Action Filter**—  button to display the Action Filter.



The following fields are available:

Field	Description
Device	Identifies the MAC address of the device that you want focus on. Devices may be a BSS, Wireless Client, Sensor, or Unknown Device.
Initiated	Specifies if manual actions and/or automatic actions are displayed in the Action Control table. Manual actions are performed manually by a user. Automatic actions are performed by an Action Rule in the Action Manager. Place a checkmark in the checkbox of <b>Manual</b> or <b>Automatic</b> to activate that option.
Action Type	Specifies which actions are displayed in the Action Control table. Place a checkmark in the checkbox of the actions that you want to display. All actions are displayed by default.

# 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.

### Creating a Report

From the **Reports** tab, follow these steps:

1. Click on the report name that you want to run. The report settings for that report will display.
2. Specify a start and end time for your report. The default time is the last 24 hours.

Range:

Start:	<input type="text" value="15:49:16"/>	<input type="text" value="09/02/2008"/>	
End:	<input type="text" value="15:49:16"/>	<input type="text" value="09/03/2008"/>	

3. Select the report scope.

Scope:

4. If you wish to publish the report, click the **Publish report data** checkbox, type in a simple name in the **Name** field, and select whether you want the report to be private or shared.

Publish report data

Name:

Use a simple directory name

Sharing:  Private  Shared

5. If you wish to email the report to someone, click the **Email** checkbox and type in the email address in the **To** field.

E-Mail

To:

Use semicolons to separate multiple addresses

Format:  ▼

6. Select a format for the report (**HTML**, **PDF**, or **CSV**) from the drop-down menu.
7. Click **Run Report**.



**NOTE** If you are publishing or emailing a report, you have the option of running the report in the background. Just click the **Run Unattended** button.

### *Adding Favorites*

From the **Reports** tab, follow these steps:

1. Click the **Add to Favorites** link next to the report name. The report settings for a favorite report will display.
2. Specify a report range by selecting **Hour(s)**, **Day(s)**, or **Week(s)**, and typing in the number of hours days, or weeks. For example, if you select **Hour(s)** and type in 12, this specifies the previous 12 hours.

Range:

Report range includes the previous:

12 Hours

3. If you wish to email the report to someone, click the **Email** checkbox and type in the email address in the **To** field.

E-Mail

To:

Use semicolons to separate multiple addresses

Format: HTML

4. Select a format for the report (**HTML**, **PDF**, or **CSV**) from the drop-down menu.
5. Click **Apply**.

✓ **NOTE** If you want to change any of the settings later, go to the **Favorites** tab and click the **Edit Settings** link next to the report name.

### *Scheduling a Report*

✓ **NOTE** A report must be in your Favorites tab before you can schedule the report to run automatically.

From the **Favorites** tab, follow these steps:

1. Click the **Edit Schedule** link next to the report that you want to run automatically. The report settings for schedules will display.
2. Click the **Enable Schedule Execution** checkbox to enable scheduling for the report.

Enable scheduled execution

3. In the **Time(s)** field, type in the times that you want to run the report.

Time(s):

4. If you want to run the report weekly, click the checkbox next to the day of the week that you want to run the report.

Weekly Schedule

Sunday       Monday       Tuesday       Wednesday       Thursday

Friday       Saturday

✓ **NOTE** You may choose more than one day of the week.

5. If you want to run the report monthly, click the checkbox next to the day of the month that you want to run the report.

Monthly Schedule

1       2       3       4       5

6       7       8       9       10

11       12       13       14       15

16       17       18       19       20

21       22       23       24       25

26       27       28       29       30       31

✓ **NOTE** You may choose more than one day of the month.

6. Click **Apply**.

### ***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.

### **Compliance Reports**

The Compliance Analysis reports display information that you can use to show you are in compliance with certain agencies or policies. The following Compliance reports are available:

- Alberta Netcare Provincial Organizational Wireless Readiness Assessment
- Department of Defense
- FISMA Federal Information Security Management Act
- GLBA Compliance
- HIPAA Compliance

- No Wireless Compliance
- North American Electric Reliability Corporation - Critical Infrastructure Protection Standard
- PCI DSS v1.1 Compliance
- PCI DSS v1.2 Compliance
- PCI Visa CISP Security Compliance Report
- SOX
- SOX Summary.

### **Alberta Netcare Provincial Organizational Wireless Readiness Assessment**

The Alberta Netcare Provincial Organizational Wireless Readiness Assessment provides a report that helps assess the ability of health service providers to protect the privacy and security of provincial health information databases. This assessment must be made before individuals can be authorized to access Alberta Network. In addition to the assessment, authorized users must also sign an information manager agreement with Alberta Health and Wellness that limits how health information in Alberta Netcare may be collected, used and disclosed.

### **Department of Defense Report**

The Department of Defense report is based on Department of Defense Directive Number 8100.2. It displays details that apply to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense.

### **FISMA Federal Information Security Management Act Report**

The Federal Information Security Management Act (FISMA) report displays security information that is required from each federal agency. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

### **GLBA Compliance Report**

Use the completed GLBA Compliance report to show that your wireless LAN is compliant with GLBA regulations.

### **HIPAA Compliance Report**

Use the completed HIPAA Compliance report to show that your wireless LAN is compliant with HIPAA regulations.

### **No Wireless Compliance Report**

The No Wireless Compliance report provides a status of your policy for a No Wireless LAN zone. Security posture and the associated vulnerabilities that could potentially lead to compromising of your network security. The key areas analyzed in this report include:

- Presence of Rogue wireless APs in your enterprise - including Hardware and Software based APs
- Presence of wireless stations - including Laptops, Desktops, PDAs, Hand-held scanners, printers, projectors etc which utilize 802.11 wireless networks
- Presence of Ignored devices in your air waves is also reported.



### **North American Electric Reliability Corporation - Critical Infrastructure Protection Standard**

The North American Electric Reliability Corporation - Critical Infrastructure Protection Standard generates a report showing access to Access Points (APs) twenty-four hours a day, seven days a week. The report also displays annual cyber vulnerability data of APs.

### **PCI DSS v1.1 Compliance Report**

The PCI DSS v1.1 Compliance report provides a summary of your Wireless LAN Security compliance with reference to the Payment Card Industry (PCI) Security Standards Council Compliance requirements. PCI Data Security Standards (DSS) compliance is required of all merchants and service providers that store, process, or transmit cardholder data. PCI DSS offers a single approach to safeguarding sensitive data for all card brands. The PCI DSS requirements specified in this report are directly from the PCI DSS standard which can be found at <https://www.pcisecuritystandards.org>.

### **PCI DSS v1.2 Compliance Report**

The PCI DSS v1.2 Compliance report is an update to PCI DSS v1.1. It provides a summary of your Wireless LAN Security compliance with reference to the Payment Card Industry (PCI) Security Standards Council Compliance requirements. PCI Data Security Standards (DSS) compliance is required of all merchants and service providers that store, process, or transmit cardholder data. PCI DSS offers a single approach to safeguarding sensitive data for all card brands. The PCI DSS requirements specified in this report are directly from the PCI DSS standard which can be found at <https://www.pcisecuritystandards.org>.

### **PCI Visa CISP Security Compliance Report**

This report provides a summary of your Wireless LAN Security compliance with reference to the VISA CISP Compliance requirements. CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data. To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of a collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements.

### **SOX Report**

The SOX report is a wireless security report for Sarbanes-Oxley that is based on COBIT IT Control Guidance. The COBIT IT Control Guidance is used to define, monitor and enforce a wireless security policy. The SOX report is actually a collection of five reports that help verify that the protective measures are being used effectively. The five reports are:

- Wireless Asset Inventory Report
- Authentication Report
- Encryption & Authentication Report
- Vulnerability Assessment Report
- Policy Violations Report.

### **SOX Summary**

The SOX Summary identifies all Access Points and user Wireless Clients connected to the network. It is used to ensure that connected Access Points and user Wireless Clients are properly configured. This summary will also identify and recognize wireless LAN risks such as rogue WLANs, insecure WLAN connections to unauthorized APs, and attacks against WLAN infrastructure that risk security and exposure of confidential information. It can also be used to monitor compliance with Access Point configuration policy.

### **Device Reports**

The Device reports are reports that Motorola AirDefense provides to help you assess the status of the devices that comprise your wireless network. The following Device reports are available:

- BSS Inventory
- Offline Sensor
- Sensor Inventory
- Single BSS Analysis
- Single Wireless Client Analysis
- Wireless Client Inventory.

### **BSS Inventory Report**

The BSS Inventory report displays details about authorized BSSs on your wireless LAN during a specific time period.

### **Offline Sensor Report**

The Offline Sensor report displays a list of Sensors that are offline. Information about each offline Sensor is included.

### **Sensor Inventory Report**

The Sensor Inventory report displays a Sensor Report Table listing all Sensors on your wireless LAN. Information about each Sensor is included.

### **Single BSS Analysis Report**

The Single BSS Analysis report displays details about one specific Access Point, using the APs MAC address. Displayed information includes:

- BSS statistics
- A BSS traffic summary including a Wireless Client association chart
- BSS security information
- BSS performance information.

### **Single Wireless Client Analysis Report**

The Single Wireless Client Analysis report displays details about one specific Wireless Client, using the Wireless Clients MAC address. Displayed information includes:

- Wireless Client statistics
- A traffic summary
- Number of associations
- Security information
- Performance information.

### **Wireless Client Inventory Report**

The Wireless Client Inventory report displays details about authorized Wireless Clients on your wireless LAN that have associated with a BSS during a specific time period.

## **Performance Reports**

Performance Reports are reports AirDefense provide to help you assess the health and performance of your wireless network and its components. The following Performance reports are available:

- Access Point Testing Analysis
- Performance Alarms Analysis
- Performance Network Utilization
- Performance WLAN Health Summary.

### **Access Point Testing Analysis Report**

The Access Point Testing Analysis report displays detailed results about AP connectivity test failures for the selected scope and time range.

### **Performance Alarms Analysis Report**

The Performance Alarms Analysis report displays details about all the performance alarms in the system for the selected scope and time range. The alarms are also shown by:

- Subcategory
- Quantity
- Location
- Criticality.

### **Performance Network Utilization Report**

The Performance Network Utilization report displays details that allow you to observe the areas of your wireless LAN that are actually in use, and to what degree they are in use. Details include:

- Information on authorized APs
- Authorized Wireless Clients
- Sensors Collecting Traffic.

### **Performance WLAN Health Summary Report**

The Performance WLAN Health Summary report displays a comprehensive health report on wireless LAN activities. The contents of this report is the same as contained in the daily and weekly management reports.

## **Security Reports**

Security reports are reports AirDefense provide to help you assess your organization's current wireless security posture. The following Security reports are available:

- Activity Log
- Security AdHoc Networks
- Security BSS Policy Violations
- Security Discovered BSSs
- Security Discovered Wireless Clients
- Security Probing Wireless Clients
- Security Rogue Detail

- WiFi Direct Network Activity
- Wireless Security Posture Details
- Wireless Vulnerability Assessment (WVA) Scan.

### **Activity Log**

The Activity Log report displays user activity information. A message is displayed highlighting the user activity and if the activity affect a Sensor or a device. The reports also displays alarm information if generated the user. The Activity Log should only be used for forensic queries. Live queries will always return no rows for this table.

### **Security AdHoc Networks Report**

The Security AdHoc Networks report displays details on Wireless Clients engaged in ad hoc networking, by MAC address/Name, Group, Location, and Sensor. You can use this information to monitor ad hoc networks in your wireless LAN. An ad hoc network can be a threat to the integrity of your network.

### **Security BSS Policy Violations Report**

Security BSS Policy Violations report displays details on BSSs that have violated your wireless network security policy.

### **Security Discovered BSSs Report**

The Security Discovered BSSs report displays details about the last observed state of BSSs being observed in your wireless LAN.

### **Security Discovered Wireless Client Report**

The Security Discovered Wireless Client report displays details about the observed last state of Wireless Clients being observed in your wireless LAN.

### **Security Probing Wireless Clients Report**

The Security Probing Wireless Clients report displays details on Wireless Clients that are engaged in reconnaissance activities against your wireless LAN, possibly for attack.

### **Security Rogue Detail Report**

The Security Rogue Detail report displays details on rogue devices detected on your wireless network. Rogue devices can be either Access Points or Wireless Clients.

### **WiFi Direct Network Activity**

The WiFi Direct Network Activity report displays details on WiFi Direct device/network activities by:

- Wireless Client
- SSID
- Signal Strength
- Security (open/WEP/WPA1/WAP2)
- Last Seen
- Location
- Group.

### **Wireless Security Posture Details Report**

The Wireless Security Posture Details report displays information that is useful in determining how vulnerable your wireless LAN is. It includes information on:

- Rogues
- Ad Hoc Wireless Clients
- Wireless Clients that accidentally connect to your wireless LAN
- Roaming violations
- Probing Wireless Clients
- Devices not configured correctly
- Intrusion violations
- Leakage of wired side traffic into the airwaves.

### **Wireless Vulnerability Assessment (WVA) Scan**

The Wireless Vulnerability Assessment (WVA) Scan report displays detailed results about wireless Vulnerability Assessment scans for the selected scope and time range. The following vulnerabilities are displayed:

- Unapproved devices
- Unapproved services
- Internet accessibility.

### **Infrastructure Management Reports**

Infrastructure Management reports display an inventory of infrastructure devices, device status, and AP traffic information. The following Infrastructure Management reports are available:

- Access Point Inventory Report
- Wireless Switch Inventory Report
- WLAN Infrastructure Status
- WLAN Infrastructure Utilization Details.

#### **Access Point Inventory Report**

The Access Point Inventory report displays details about the Access Points that are on your network.

#### **Wireless Switch Inventory Report**

The Wireless Switch Inventory report displays details about the Wireless Switches that are on your network.

## WLAN Infrastructure Status Report

The WLAN Infrastructure Status report displays status information about the infrastructure devices on your network and the alarms generated by the devices. The status information includes:

- Switch Details
- AP Details
- Infrastructure Generated Events.

## WLAN Infrastructure Utilization Details

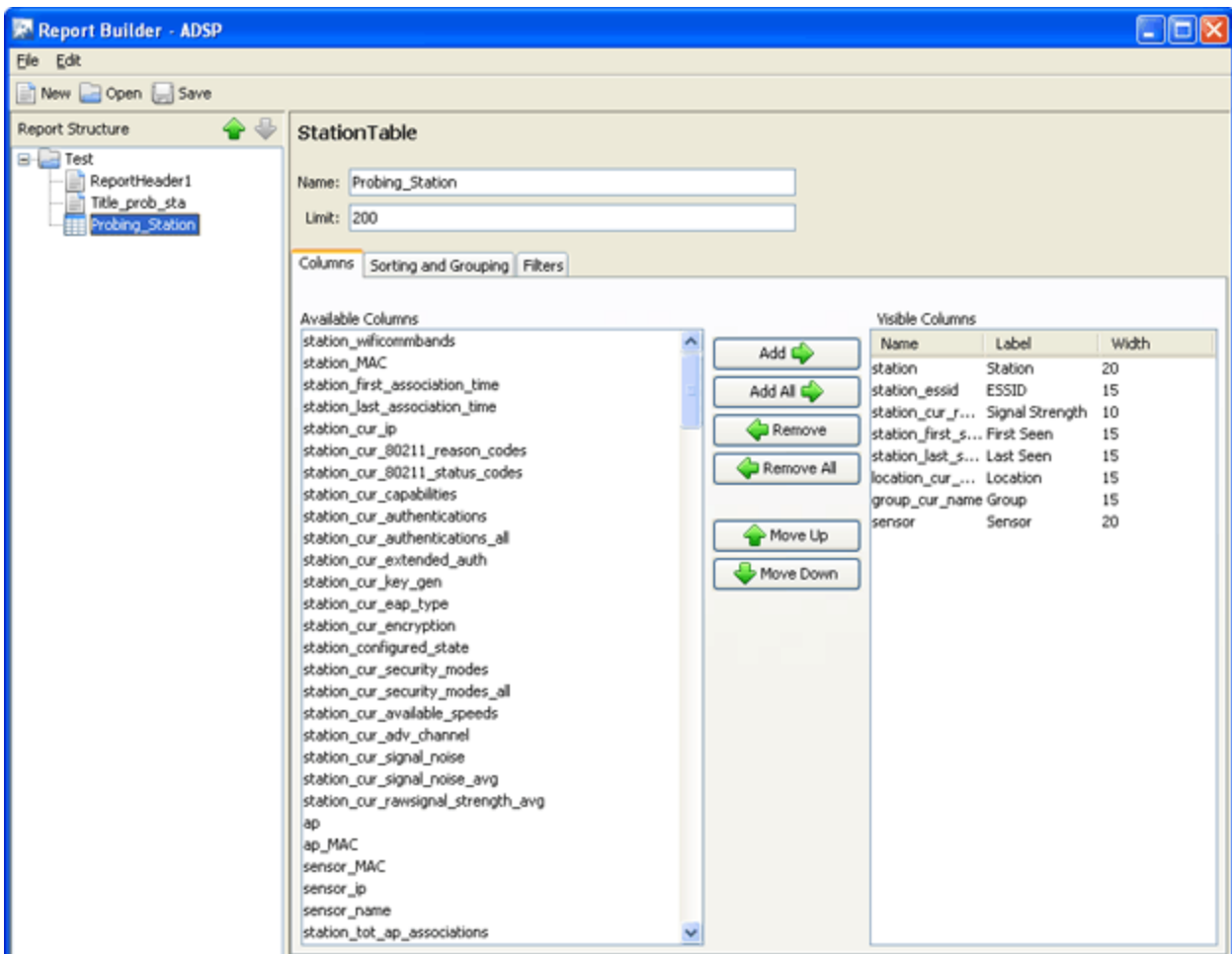
The WLAN Infrastructure Utilization Details show AP traffic information flowing over your network. Information about the top 50 APs are displayed.

## Custom Reports

The Custom reports are reports customized by a user to show only information that is useful/helpful to that particular user. Custom reports are built [Using Web Reporting](#).

## Using the Report Builder

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 Traffic 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.

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

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.

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.

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

System Name: maher-wds-mgr-015  
Scope: system  
Generated: 2010-02-02 14:01:33  
Version: 8.0.0-14  
Time Zone: EST - Eastern Standard Time

Performance Summary

Performance Summary

Performance Alarms By SubCategory

Top 10 Configuration/Compatibility Alarms	Alarm	Severity	Count
1	Auth Auth-Auth (1)	Warning	100
2	Auth Auth-Auth (2)	Warning	100
3	Auth Auth-Auth (3)	Warning	100
4	Auth Auth-Auth (4)	Warning	100
5	Auth Auth-Auth (5)	Warning	100
6	Auth Auth-Auth (6)	Warning	100
7	Auth Auth-Auth (7)	Warning	100
8	Auth Auth-Auth (8)	Warning	100
9	Auth Auth-Auth (9)	Warning	100
10	Auth Auth-Auth (10)	Warning	100

## Creating and Saving a Report

1. Click **New** on the tool bar.
2. Choose a template. A description of each template is displayed when you highlight it. 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.
3. 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).
4. Click **OK**, and then click **Save**.

After creating and saving a report, if you want to change the name of the report, follow these steps:

1. Open the report by clicking **File > Open**.
2. Save the report by clicking **File > Save As** and then type a new name.
3. Click **OK**.

### ***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.

---



---

- 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.



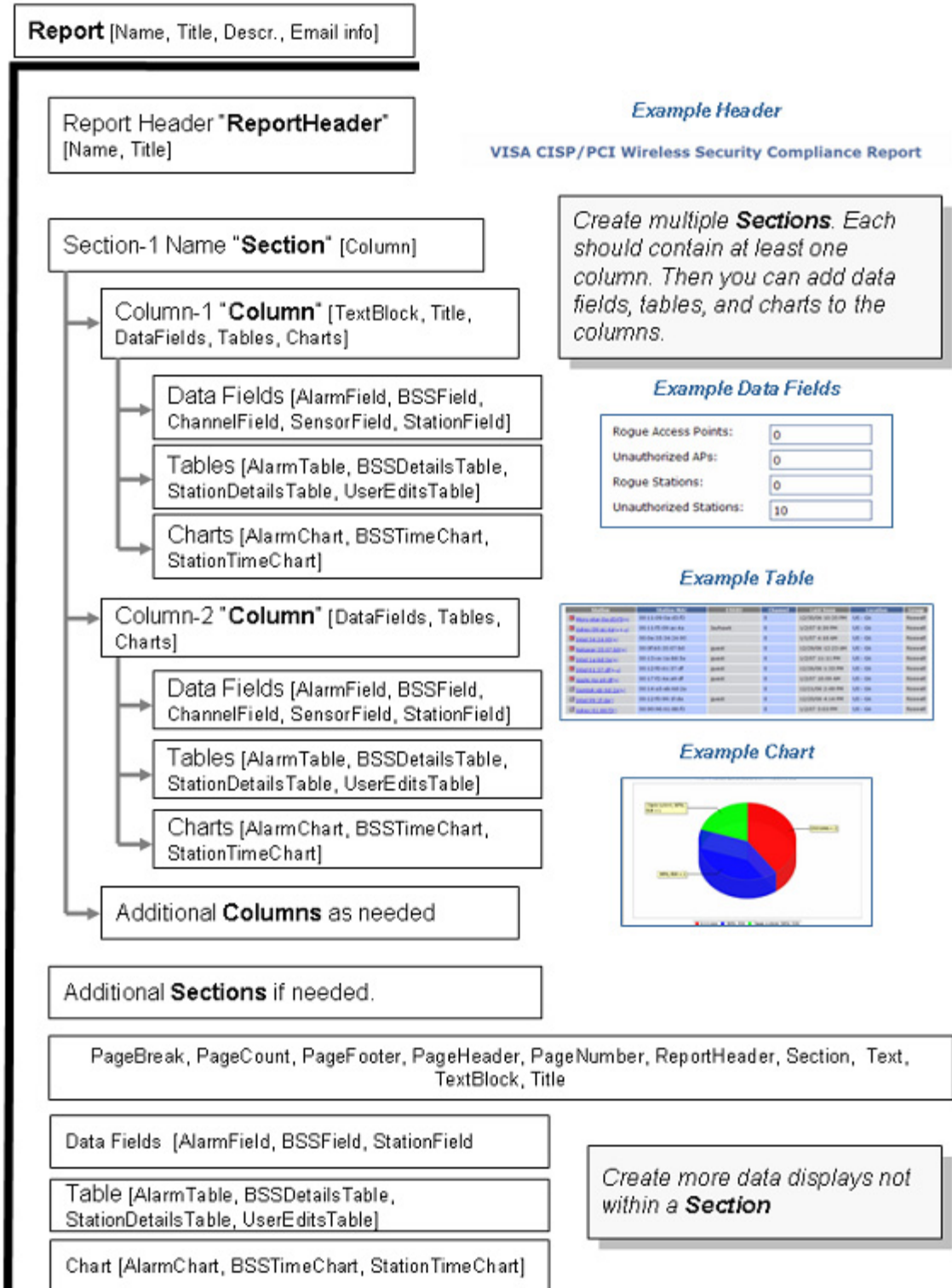
**NOTE** When building alarm tables with an ap\_MAC column, the ap\_MAC column will only show data for alarms that were triggered by a wireless client (station) associated to an AP's BSS. Other alarms will leave this field blank.

- 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.

---

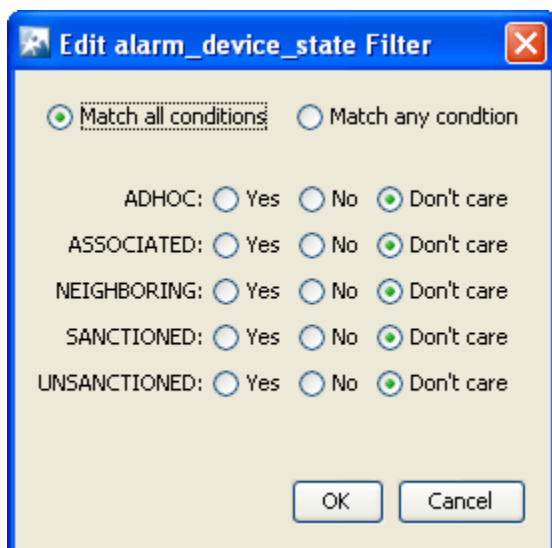
**Hint: You may want to include the units of measure in the name you give the field. For example: Alarm (count).**

---

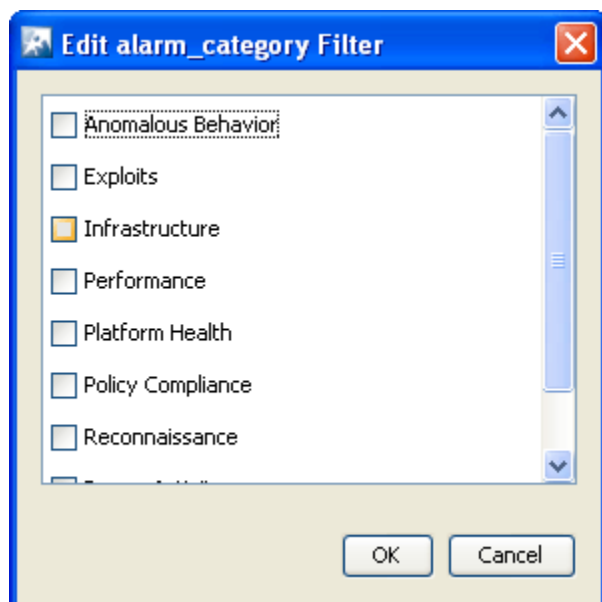
### *Types of Filter Windows*

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):



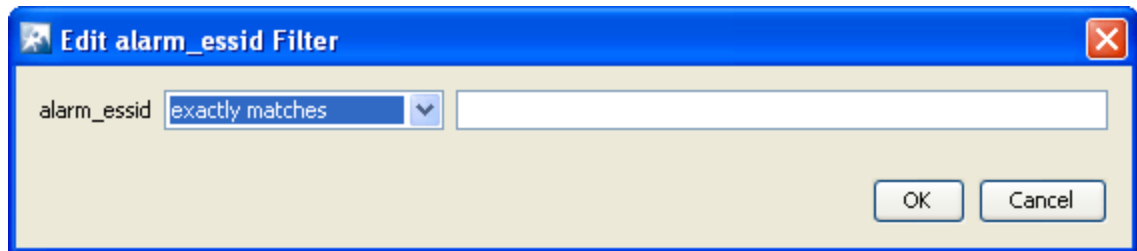
- Checkboxes (example):



- Boolean (example):



- Text box (example):

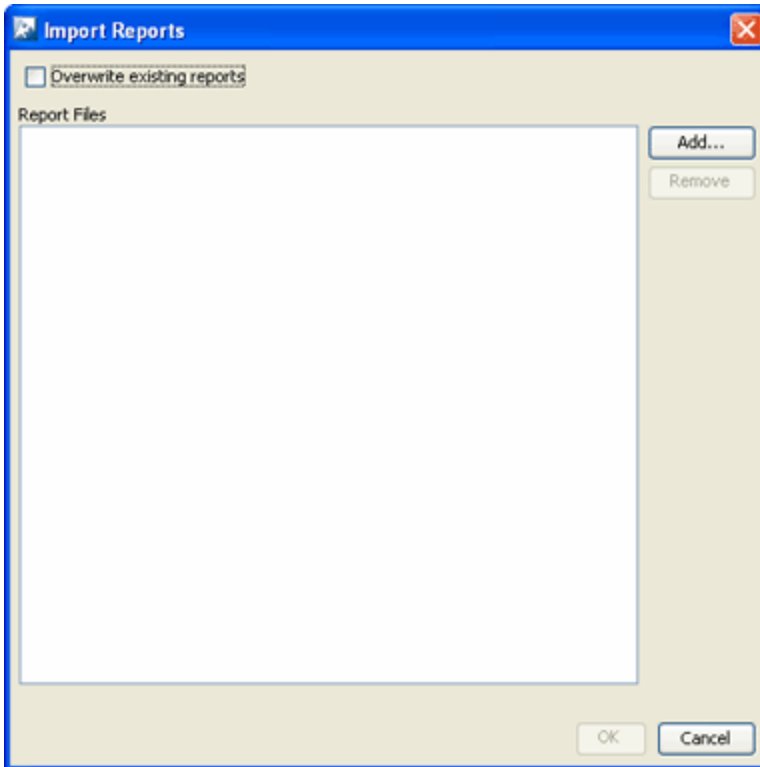


### *Deleting a Report*

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.

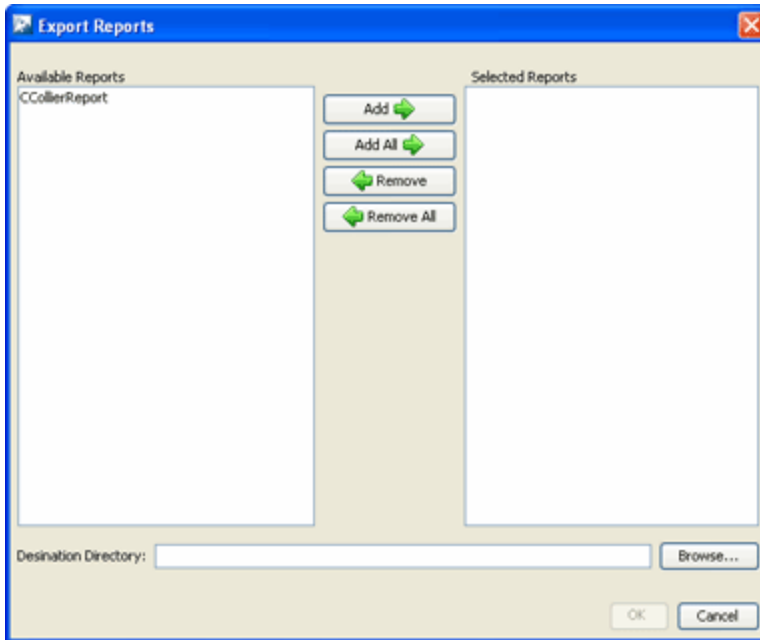


To import a report, follow these steps:

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.

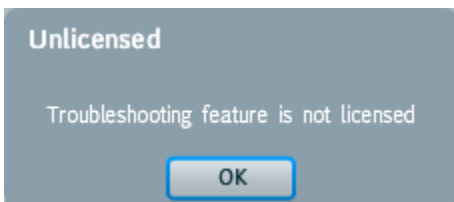
The **Add All** button adds all of the available reports to the **Selected Reports** list. The **Remove** button removes selected (highlighted) reports from the Selected Reports list. The **Remove All** button removes all reports from the **Selected Reports** list.

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.

## Connection Troubleshooting

The Troubleshooting tool allows you to troubleshoot a Wireless Client's ability to connect to your wireless network. Using the MAC address or device name of a Wireless Client, the Troubleshooting tool can run tests to determine the status of a Wireless Client within your wireless network and display results summarizing the status.

You must have a valid Advanced Troubleshooting license before you can access the Troubleshooting tool. If you attempt to access Troubleshooting without a license, the following message displays:



### Getting Started

You must first determine the MAC address of the Wireless Client or the device name of the Wireless Client. One way to do this is to right-click on the Wireless Client while in the GUI and copy the MAC address. If for some reason you cannot copy the MAC address, you can click the question mark next to the **Troubleshoot Device** field to display hints on how to determine the MAC address or device name.



Once you know the MAC address or device name of the Wireless Client, type in one of them and click the **Start** button near the center of the Troubleshooting webpage.



✓ **NOTE** If you enter a device name that is not recognized, the [Device Selection Wizard](#) will display where you can search for the device.

The Troubleshooting tool runs the troubleshooting test and starts loading troubleshooting data into the application.



When 100% of the troubleshooting data is loaded, the data is displayed in the application. For an explanation of the loaded data, refer to the [Wireless Client Status](#), [Results Summary](#), and [Observed Network](#) topics.

### MAC Address Hints

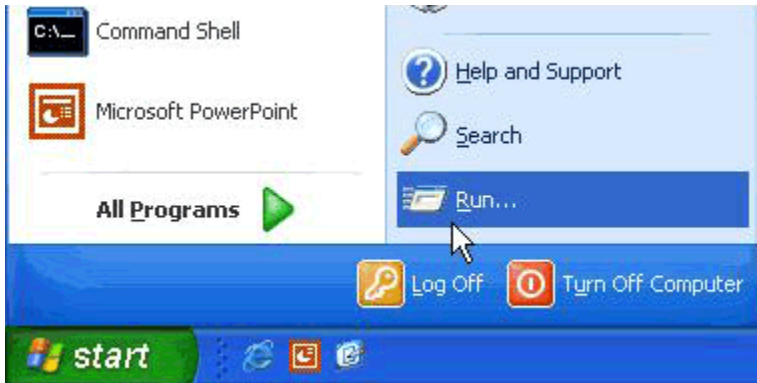
Click on the question mark next to the **Troubleshoot Device** field to display hints on how to determine the MAC address or device name of a Wireless Client.



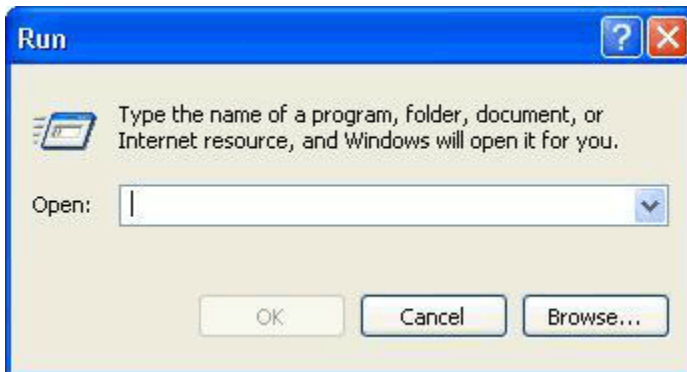
### Instruction for Find MAC Address

#### Windows

To find the MAC address on a Windows system, go to **Start** menu and click **Run**.



The **Run** window will open. Enter `cmd` and click **OK**.



In the `cmd` window that opens, type `ipconfig /all<Enter>` to get the list of network interfaces. If the system has multiple wireless adapters, search for the wireless adapter. In the example below, the wireless adapter is

Ethernet adapter *Wireless Network Connection 14*:. Once the adapter has been identified, the MAC address is the physical address. The wireless mac in the example below is *00-19-9E-E0-93-9E*.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : workgroup
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : dns.net

Ethernet adapter Wireless Network Connection 14:

    Media State . . . . . : Media disconnected
    Description . . . . . : AirDefense Mobile 11a/b/g Wireless LAN Mini PCI Express Adapter #4
    Physical Address. . . . . : 00-19-9E-E0-93-9E

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : dns.net
    Description . . . . . : Intel(R) PRO/1000 PL Network Connection
    Physical Address. . . . . : 00-1A-6B-BD-A9-74
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.1.1.116
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 192.1.1.1
    DHCP Server . . . . . : 192.2.1.1
    DNS Servers . . . . . : 192.2.1.1
                          192.2.1.14
    NetBIOS over Tcpip. . . . . : Disabled
    Lease Obtained. . . . . : Wednesday, September 24, 2008 1:39:04 PM
    Lease Expires . . . . . : Monday, September 29, 2008 1:39:04 PM

C:\Documents and Settings>
```



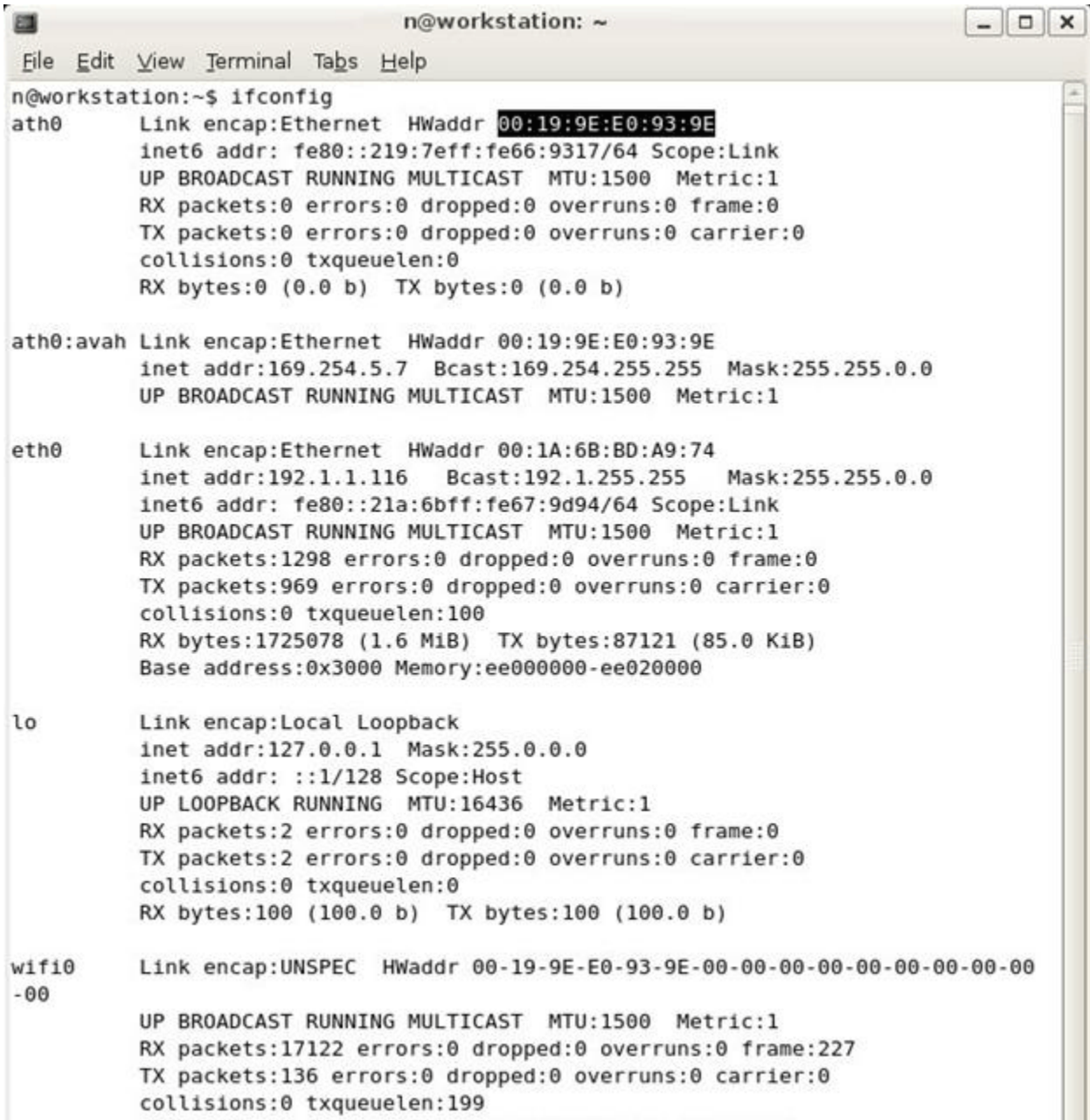
## MAC OSx

Open **System Preferences** and select **Network**. Select the wireless interface from the list in the show drop down. The MAC address is the Ethernet ID which is `00:0d:31:83:dd:37` in the screen shot below.



### Linux Variants

Open a terminal and type `ifconfig`<Enter> at the prompt. This will display information for all network adapters on the machine. Identify the wireless adapter. The HWaddr is the MAC address which is `00:19:9e:e0:93:9e` in the screen shot below.



```
n@workstation: ~
File Edit View Terminal Tabs Help
n@workstation:~$ ifconfig
ath0      Link encap:Ethernet  HWaddr 00:19:9E:E0:93:9E
          inet6 addr: fe80::219:7eff:fe66:9317/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

ath0:avah Link encap:Ethernet  HWaddr 00:19:9E:E0:93:9E
          inet addr:169.254.5.7 Bcast:169.254.255.255 Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0      Link encap:Ethernet  HWaddr 00:1A:6B:BD:A9:74
          inet addr:192.1.1.116 Bcast:192.1.255.255 Mask:255.255.0.0
          inet6 addr: fe80::21a:6bff:fe67:9d94/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1298 errors:0 dropped:0 overruns:0 frame:0
          TX packets:969 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1725078 (1.6 MiB)  TX bytes:87121 (85.0 KiB)
          Base address:0x3000 Memory:ee000000-ee020000

lo         Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:100 (100.0 b)  TX bytes:100 (100.0 b)

wifi0     Link encap:UNSPEC  HWaddr 00-19-9E-E0-93-9E-00-00-00-00-00-00-00-00-00-00
-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17122 errors:0 dropped:0 overruns:0 frame:227
          TX packets:136 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:199
```

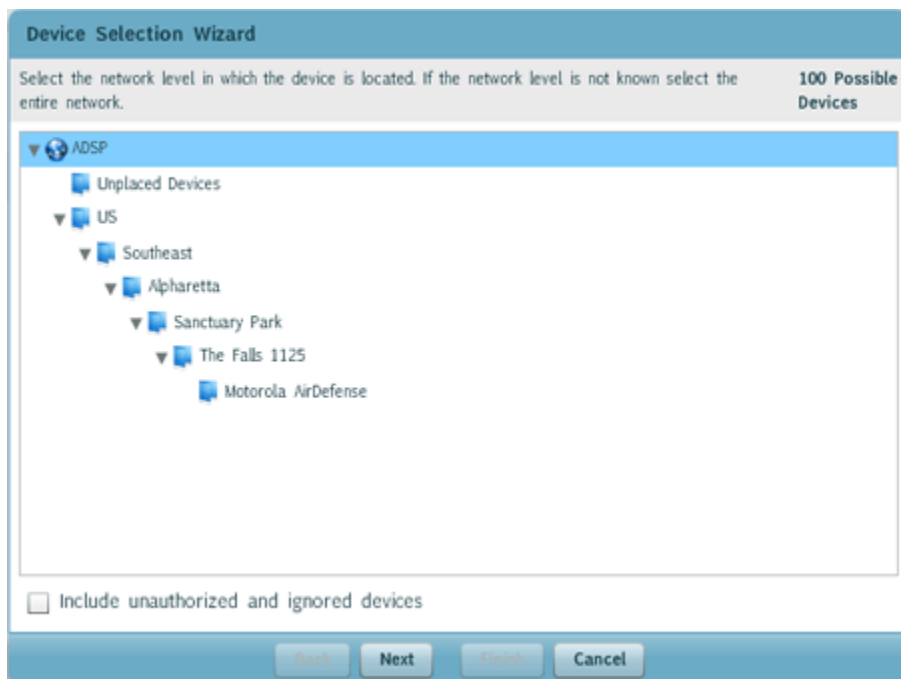
### Device Selection Wizard



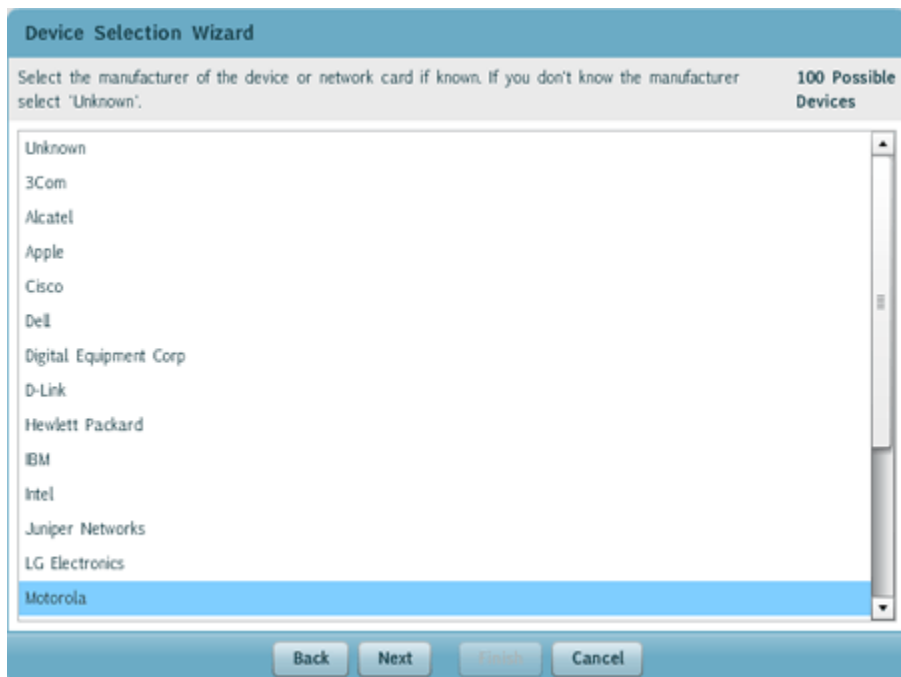
The Device Selection Wizard is used to locate and select a Wireless Client for troubleshooting. Click the wand to access the Device Selection Wizard and then follow these steps to select a Wireless Client.

1. Select a scope by highlighting the appliance or a network level. You should try to narrow the scope as much as possible. Only authorized stations are included in the device list. To include unauthorized or

ignored devices, click the checkbox near the bottom of the wizard to place a checkmark in the checkbox. Click **Next** to continue.



2. Highlight the vendor name by clicking on it. If you are unsure of the vendor, you can select **Unknown**. Click **Next** to continue.



- Type in any identifying information. You may type partial names or addresses. The wizard will find all devices matching the information. Click **Next** to continue.

**Device Selection Wizard**

Enter as much identifying information as known. Partial names or addresses are accepted, all matching devices will be found. 2 Possible Devices

Device Name:   
The device name is configured on the WPS system for the specific device

802.1X Name:   
The 802.1X name or LEAP name is the name used for the device on an authenticated network

MAC Address:   
The MAC address is a unique identifier for each network device in the form  
 XXXX:XXXX:XXXX:XX

IP Address:   
The IP address is a unique identifier for each network device in the form  
 XXX.XXX.XXX.XXX

- Check the list of devices on the left side of the window below. If there is only one device in the list, it most likely the Wireless Client you are searching for. Select it and click **Finish**.

The Wireless Client's MAC address is placed in the **Troubleshoot Device** field where you can proceed to troubleshoot it. If there is more than one device listed, follow these instructions:

- Select the nearest Sensor from the drop-down list.
- Turn the Wireless Client off and then click the **Device is Off** button. The wizard starts collecting data.
- After the data status bar reaches 100%, turn the Wireless Client back on and then click the **Device is On** button. The wizard collects more data.
- After the data status bar reaches 100%, the wizard does a comparison on when the device was off and when it was on. If only one device is found, a **Device Found** popup window displays with the device listed.

**Device Found**

One matching device found:

 00:1F:E1:78:AE:6D

Click **Use this Device**. The Wireless Client's MAC address is placed in the **Troubleshoot Device** field where you can proceed to troubleshoot it. If more than one device is found, the list of devices will update. Click **Try Again** and then repeat steps. You may have to keep trying again until there is only one device found.



**NOTE** After following these steps and the device list is empty, please choose another Sensor when you try again.

### Troubleshoot Another Wireless Client

To troubleshoot another station, enter its MAC address or device name in the **Troubleshoot Device** field and then click the **Start** button.



Troubleshooting data loads.

### Wireless Client Status

A Wireless Client status message is displayed after troubleshooting has completed. If no problems were observed, a green message box is displayed that indicates so.



If a problem was observed that needs further investigation, an orange message box is displayed stating the problem.

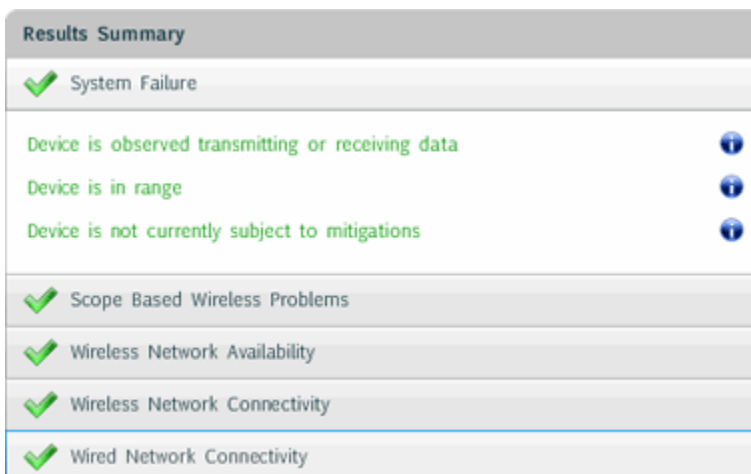


If a problem was observed that is definitely the reason a station cannot connect to the network, a red message box is displayed showing the reason for failure.

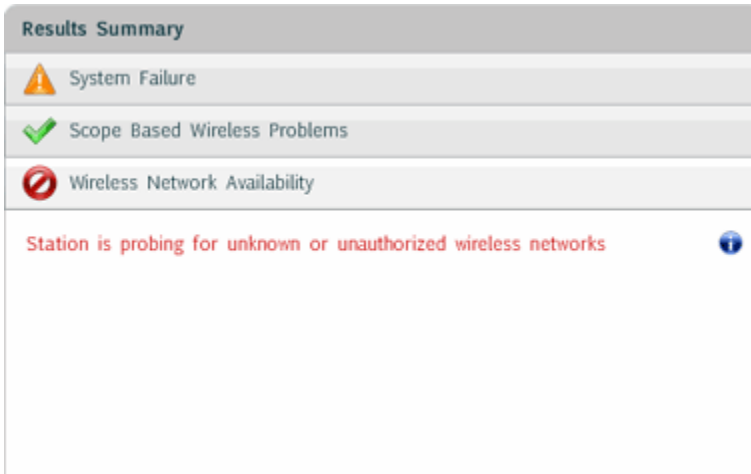


### Results Summary




Troubleshooting results are summarized in the **Results Summary** window. If no problems were observed, you may see a **Results Summary** window similar to the one shown below.




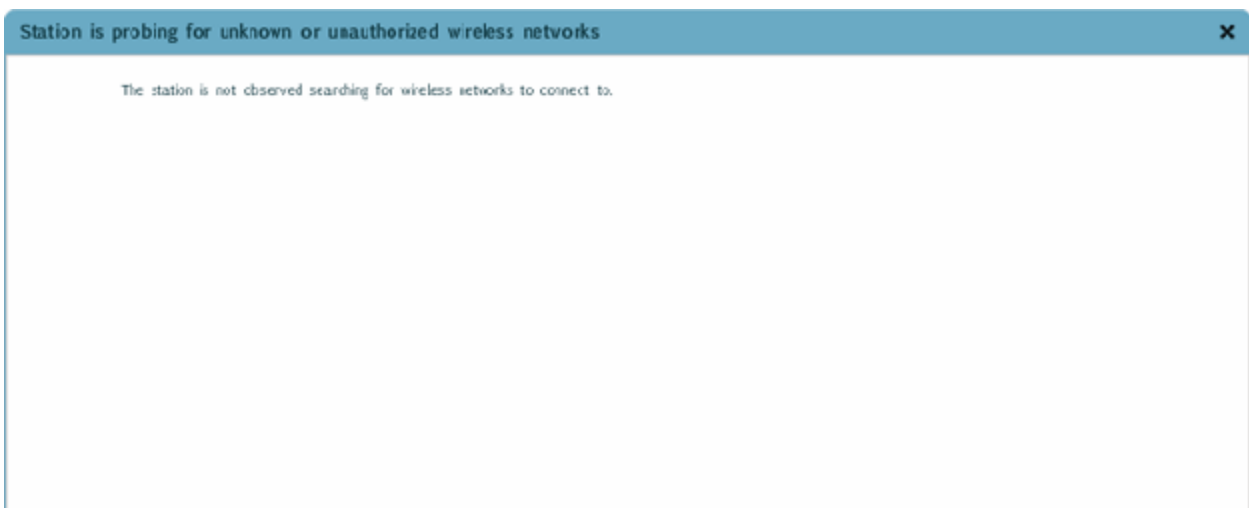
If problems were observed, you may see a **Results Summary** window similar to the one shown below.



The Results Summary will change according to the results but the symbols remain constant.

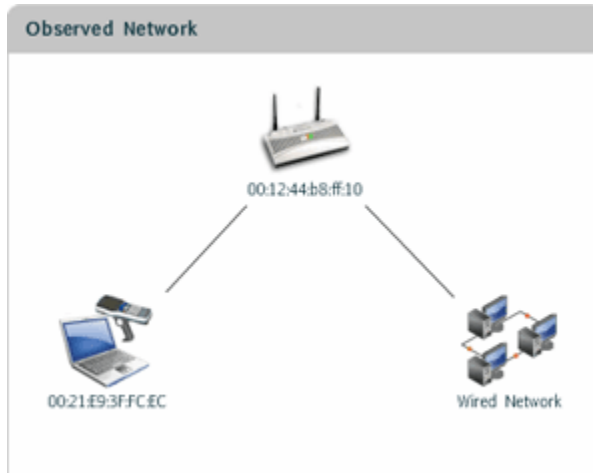
-  No problem observed.
-  Possible problem; needs further investigation.
-  Definite problem observed.

To view the individual summary sections, just click on the section name. To get a more detailed explanation of the summary, click on the Information icon— to the right of a message. A dialog window opens displaying the details.



## Observed Network

The Observed Network displays how the troubleshooted Wireless Client appears in the network. It shows any wireless or wired connections.



A dark gray line between devices signifies the connection was checked and communications are good. A red line between devices signifies the connection was checked and there is a problem. No line between devices signifies no connection was observed.

The MAC address of the Wireless Client and Access Point are displayed under the device.

## Export Captured Frames

During troubleshooting, as a Wireless Client's communications is being analyzed, the communications frames are saved in a PCAP file on the server. The saved frames can be exported to your local workstation by clicking on the [Export Captured Frames](#) button.



A dialog window opens where you can name and save the exported file to your local hard drive. Once saved on your workstation, the exported file can be opened in the Frame Capture Analysis tool to analyze the sequence of events that occurred during troubleshooting.

You can only export captured frames from the current Troubleshooting test. Therefore, you must export captured frames that you want to save before running the next test.


## Scheduled AP Test

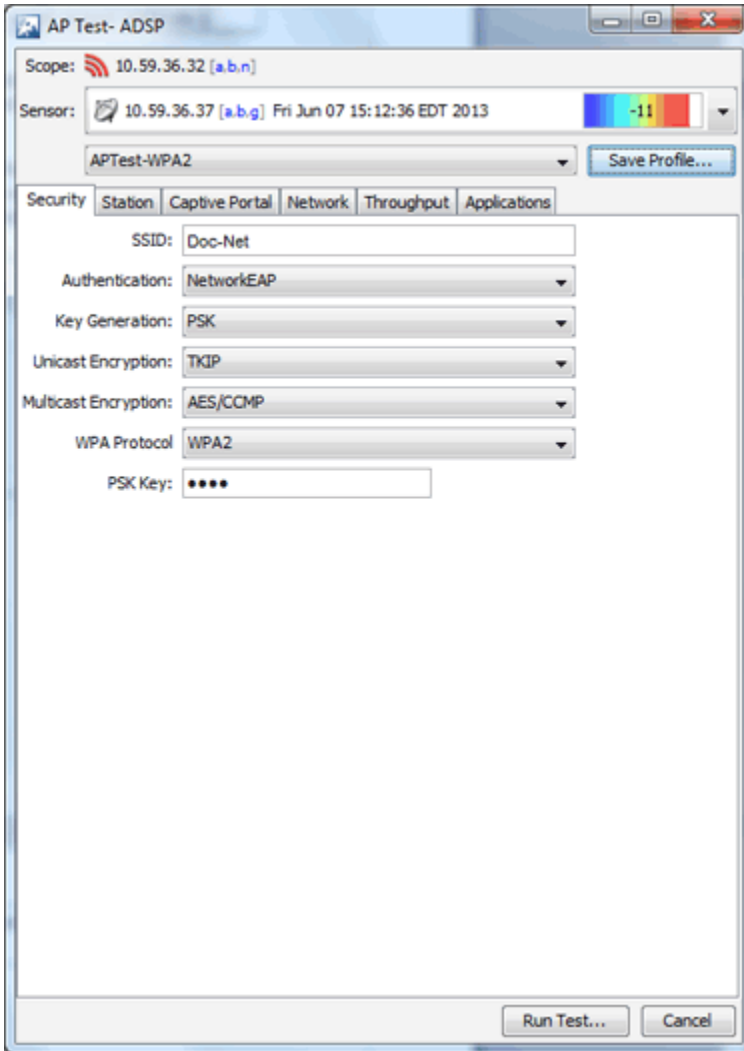
✓ **NOTE** AP Test is part of the Advanced Troubleshooting module and requires an Advanced Troubleshooting license for access.

AP Test 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 station 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.

## On-Demand Tests

You can conduct an AP Test at anytime by using an on-demand test. To initiate an on-demand test, click the drop-down menu button—  for a BSS or network level, and select AP Test.

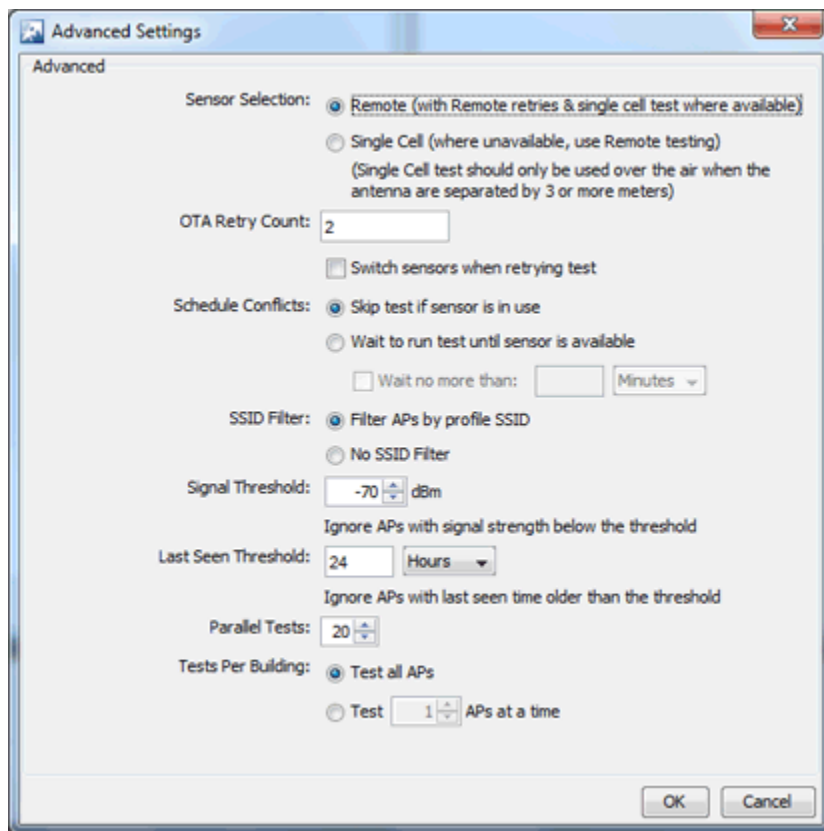


After accessing the AP Test window, follow these steps:

1. Set or change any configurable options in the **Security**, **Station**, **Captive Portal**, **Network**, **Throughput**, or **Applications** tabs. If any changes are made, save the current profile or save a new profile.



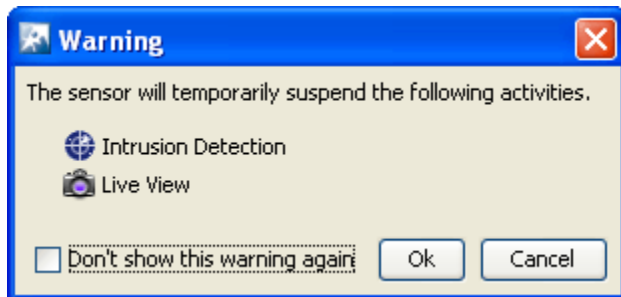
- Run the on-demand test by clicking the **Run Test** button. If the scope is a BSS, the test runs and the **AP Test Results** window displays (see [Test Results](#) topic). If the scope is a network level, the **Advanced Settings** window displays:



- If the **Advanced Settings** window displays, configure the advanced settings using the following fields:

Field	Description
Sensor Selection	Decide if you want to use a remote Sensor or a single cell Sensor. Single cell Sensors should only be selected if the antenna are separated by 3 or more meters.
OTA Retry Count	Specify the number of times to retry the test. You can also elect to switch Sensors when retrying tests.
Schedule Conflicts	Specify that you want to skip the test if the Sensor is in use or that you want to wait to run the test until the Sensor is available. If you elect to wait, you may also limit the waiting time.
SSID Filter	Decide if you want to filter APs by SSID profile or not.
Signal Threshold	Limit test to APs with a signal strength above a value that you specify.
Last Seen Threshold	Limit test to APs that were last seen on your network within a time limit that you specify.
Parallel Tests	Specify the number of buildings to run the test (maximum of 20).
Tests Per Building	Specify a limit on the number of BSSs to test per building. You have the option to specify all or specify a specific number.

- Click **OK** to set the advanced settings. A **Warning** window displays.



This window alerts you to the fact that any of the listed activities will be suspended while running the test.



**NOTE** You can elect not to display future warnings by selecting the **Don't show this warning again** checkbox.

- Click **OK** to run the test.

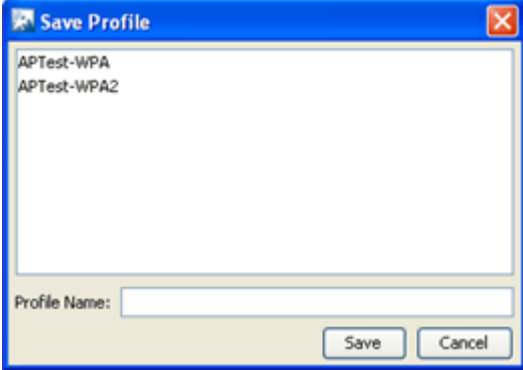
### ***Common Area***

The common area includes everything not included in a tab and is always in view. There three are fields and three buttons included in the common area.

#### **Fields**

<b>Fields</b>	<b>Description</b>
Access Point	Displays the name of the AP that is being tested.
Sensor	Displays/selects the Sensor to use during the AP Test. The default is the Sensor with the strongest signal as seen by the AP.
Profile	Selects/displays the name of the current profile to use for the AP Test.

**Buttons**

Buttons	Description
Save Profile	<p>Saves the current settings to a profile that you name. Profiles make it easy to apply the same settings to different AP Test. When selected, a <b>Save Profile</b> window is displayed.</p>  <p>Type in a new profile name and click <b>Save</b>. Once saved, you can apply the profile to set up an AP Test.</p>
Run Test	Conducts the AP Test. (See <a href="#">Test Results</a> for details.)
Cancel	Exits AP Test without running a test.

### Security Tab

The **Security** tab for AP Test provides fields for SSID, authentication, encryption, key generation and WEP keys or EAP username/password. The fields will be initialized to the current profile settings of the AP. In most cases, you will not have to change any of the field. In some cases, you may have to change a field because a field was not set in the AP profile or the profile was not set up correctly.

The screenshot shows the Security tab configuration interface with the following fields and values:

- SSID: Doc-Net
- Authentication: NetworkEAP
- Key Generation: PSK
- Unicast Encryption: TKIP
- Multicast Encryption: AES/COMP
- WPA Protocol: WPA2
- PSK Key: ••••

✓ **NOTE** Depending on the field options, some fields may or may not be visible.

Field	Description
SSID	Service Set Identifier (SSID) of the Access Point.
Authentication	Type of authentication used to authenticate users on a local or remote (LDAP or RADIUS) server. Choices are <b>Open</b> , <b>Shared Key</b> , or <b>NetworkEAP</b> .
Key Generation	Method used to generate the keys that are necessary to encrypt data. Choices are <b>None</b> , <b>802.1x</b> , <b>PSK</b> , or <b>EAP</b> . If Key Generation method is <b>EAP</b> , you may have to verify a user certificate, a Root CA certificate, or a server certificate. Details on when you verify a certificate can be found under EAP Key Generation and Certificates.
Unicast Encryption	Encryption method used during unicast transmissions.
Multicast Encryption	Encryption method used during multicast transmissions.
WPA Protocol	(Wi-Fi Protected Access (WPA) method used to secure the connection to the wireless network. Choices are <b>WPA</b> or <b>WPA2</b> .
PSK Key	Pre-shared key (shared secret) used to authenticate user access to the AP.
Key Size	Key sized used for a WEP key. Choices are <b>64 bits 10 hex digits</b> or <b>128 bits 26 hex digits</b> .
WEP Key	Wireless Equivalent Privacy (WEP) key used to authenticate user access to the AP.
Key Index	Index number used to identify a WEP key.
EAP Method	Extensible Authentication Protocol (EAP) method used in LAN authentication. Choices are <b>LEAP</b> , <b>EAP/Fast Auto</b> , <b>EAP/Fast Manual</b> , <b>EAP-TLS</b> , <b>PEAP-MSCHAPv2</b> , <b>PEAP-GTC</b> , or <b>PEAP-TLS</b> . All methods except <b>LEAP</b> and <b>EAP/Fast Auto</b> , when selected, allow you to use certificates (User Certificate, Root CA, or EAP-FAST PAC) when testing AP connectivity.
EAP Username	EAP username used in LAN authentication.
EAP Password	EAP password used in LAN authentication.

### EAP Key Generation and Certificates

Verification of certificates is done when **EAP** is selected as the **Key Generation** with one of the following **EAP Methods**:

- EAP-TLS
- PEAP-MSCHAPv2
- PEAP-GTC
- PEAP-TLS.

With EAP-TLS selected, you must verify your User Certificate and Root CA certificate:

The screenshot shows the configuration interface for the EAP-TLS method. The 'EAP Method' dropdown is set to 'EAP-TLS'. Below it are fields for 'EAP Username', 'User Certificate (PKCS12)', and 'Root CA (PEM/DER)'. The 'User Certificate' and 'Root CA' dropdowns are both marked with a red 'X' icon, indicating that certificates are required for this method.

With PEAP-MSCHAPv2 selected, you may optionally verify your Root CA certificate by selecting the **Verify Server Certificate** checkbox:

The screenshot shows the configuration interface for the PEAP-MSCHAPv2 method. The 'EAP Method' dropdown is set to 'PEAP-MSCHAPv2'. Below it are fields for 'EAP Username', 'EAP Password', and 'Outer Identity'. At the bottom, there is a checkbox labeled 'Verify Server Certificate' which is currently unchecked.

With PEAP-GTC selected, you may optionally verify your Root CA certificate by selecting the **Verify Server Certificate** checkbox:

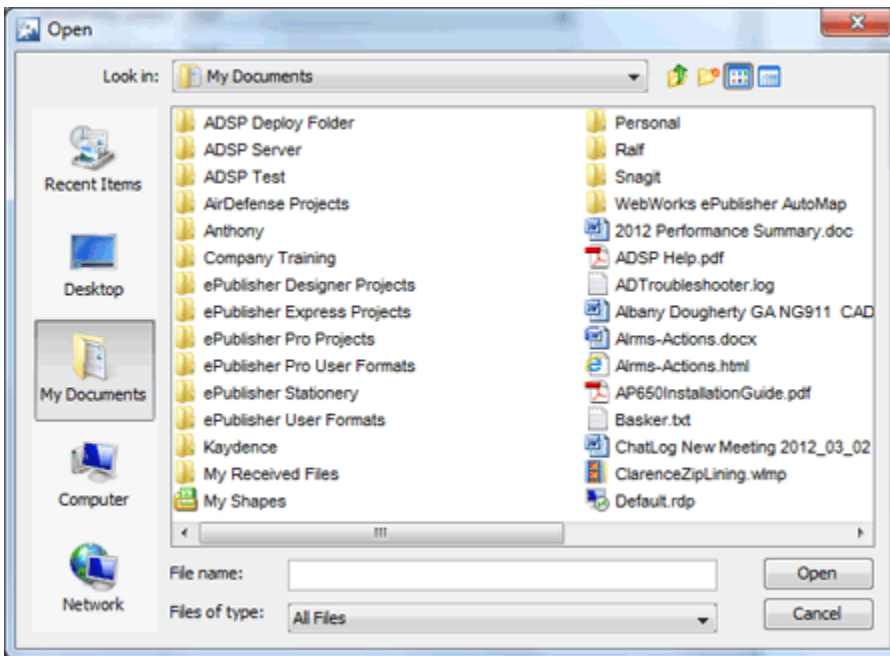
The screenshot shows the configuration interface for the PEAP-GTC method. The 'EAP Method' dropdown is set to 'PEAP-GTC'. Below it are fields for 'EAP Username', 'EAP Password', and 'Outer Identity'. At the bottom, there is a checkbox labeled 'Verify Server Certificate' which is currently unchecked.

With PEAP-TLS selected, you must verify your User Certificate and optionally verify your Root CA certificate by selecting the **Verify Server Certificate** checkbox:

The screenshot shows the configuration interface for the PEAP-TLS method. The 'EAP Method' dropdown is set to 'PEAP-TLS'. Below it are fields for 'EAP Username', 'Outer Identity', and 'User Certificate (PKCS12)'. There is also a checkbox labeled 'Verify Server Certificate' which is currently unchecked. The 'User Certificate' dropdown is marked with a red 'X' icon, indicating that a user certificate is required.

If an **Outer Identity** field is added to any of the EAP Methods, you should use the same name as the EAP Username.

To add certificates to a field, mouse over the three dots (...) and then click the button to browse to the certificate file.



Once you locate the file, select it and then click the **Open** button.



You have the option of naming your certificate or keeping the default name. Make a choice and then click **OK**. The certificate is added to the field.

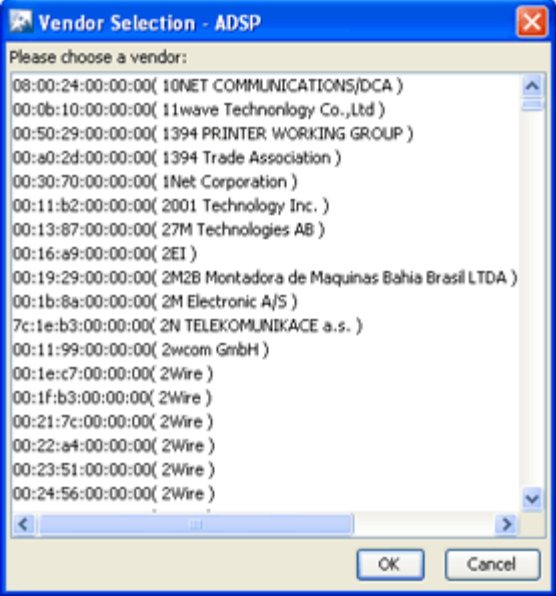


To remove a certificate (User or Root CA) from the dialog, click the **Remove**—**X** icon next to the certificate.

### *Station Tab*

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

The screenshot shows a configuration window titled "Station". At the top, there is a tab labeled "Station". Below the tab, the "MAC Address" is set to "00:e0:d4:5b:6b:b0". To the right of the MAC address field are two buttons: "Random Address" and "Vendor Address". Below this, there are two checked checkboxes: "Obtain IP address using DHCP" and "Obtain DNS server address automatically". Under the DHCP checkbox, there are three input fields: "IP Address:", "Subnet Mask:", and "Default Gateway:". Under the DNS checkbox, there are three input fields: "Primary DNS:", "Secondary DNS:", and "Domain Name:".

Field	Description
MAC Address	<p>Since AP Test uses a virtual station for its test, an artificial MAC address must be specified for the test station. The <b>MAC address</b> field is initialized to the most recently used test station MAC address. If no previous address is found, a random MAC address is used.</p> <p>You may change the MAC address by typing one in the field or click the <b>Random Access</b> button to generate one. You may also generate a MAC address by clicking the <b>Vendor Address</b> button and selecting a vendor from a list of vendors.</p>  <p>The first 3 hexadecimal codes are vendor specific. The last 3 codes are generated when you make a selection to form a simulated MAC address.</p> <p>A warning message is displayed if you select a MAC address that matches an observed device. Also, if you attempt to save a profile and the MAC address matches a MAC address of a station in another profile, an error message is displayed.</p>
Obtain IP address using DHCP	<p>You can obtain an IP address using DHCP or specify a static IP address. If you want to specify a static IP address, you must also specify the subnet mask and default gateway. The default is to obtain IP address using using DHCP. Uncheck the checkbox to activate the fields and to specify a static IP address, subnet mask, and default gateway.</p>
Obtain DNS server address automatically	<p>You can obtain DNS server information automatically or specify the information yourself. The default is to obtain the information automatically. If you want to specify the information, uncheck the checkbox to activate the fields and then specify the primary DNS, secondary DNS, and domain name.</p>



### Captive Portal Tab

Some companies/businesses require users to access their Internet through a web portal when on a public-access network. Once the portal is accessed, the user is required to either authenticate with a username and password, or accept a use policy by clicking a button to accept the policy.

The **Captive Portal** tab allows you to configure AP Test to connect to a captive portal to test the connection.

Field	Description
Enable Captive Portal Test	Turns on captive portal testing for AP Test.
Captive Portal Plugin	Specifies a captive portal plugin containing information about the captive portal. The drop-down menu contains a list of plugins. You can import plugins with the <b>Import</b> button. You can export plugins with the <b>Export</b> button. The <b>Revert</b> button resets all fields to their previous stats. Some fields may be hidden because the information is contained in the plugin. Selecting the <b>Show complete test profile</b> reveals the hidden fields.
Response Timeout	Sets the response timeout for the initial redirected login page or post login page. The default response timeout is 20 seconds.
Walled Garden URLs	If the captive portal being tested supports the Walled Garden feature with a list of white list URLs, AP Test will verify that the system allows access to the white list. AP Test can verify a maximum of 5 URLs.

Field	Description
User's Target URL	Specifies an IP address or URL that will be checked by AP Test to ensure that it can't be accessed before captive portal log-in. The same URL will also be checked by AP Test to see whether captive portal grants access to it, after successful log-in.
Verification text	Specifies some text that appears on the target website as specified in User's Target URL.
Agreement / Login URL	Specifies the agreement web page or the login web page where a user has to accept the use policy or authenticate with a username and password.
Form Name	The form name used to submit acceptance of the use policy or authentication credentials.
Required validation	Provides a list of names that require validation. The name must be specified by type (dynamic or static) and value.
Validation check URL	Specifies the web page used to validate names in the <b>Required validation</b> field.
Welcome URL	Specifies a welcome page the user accesses once he/she have accepted the use policy or authenticated with a username and password.
Logout URL	Specifies a logout page after the user has terminated from the target URL.

### *Network Tab*

The **Network** tab allows you to configure layer 3 tests.

The following fields may be selected when performing an AP test:

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

### Throughput Tab

The **Throughput** tab allows you to connect to a FTP server and upload a test file during an AP Test while specifying the acceptable bandwidth throughput.

The screenshot shows the 'Throughput' configuration window. It is divided into two main sections: 'Enable Download Test' and 'Enable Upload Test'. Each section has a checkbox to enable the respective test. Below each checkbox are several input fields: 'FTP Server Address', 'Path' (with a note '(include file name)'), 'Port' (pre-filled with '21'), 'User', and 'Password'. Additionally, there is a 'Maximum Transfer' field (pre-filled with '2' and a unit dropdown set to 'MB') and a 'Minimum acceptable bandwidth throughput' field (pre-filled with '10' and units 'bytes/s per second'). A checkbox labeled 'Copy download test settings for use in upload test' is positioned between the two test sections.

There is a download test and an upload test. You can select one or both of the tests by selecting the appropriate checkbox. The fields are same for each test. You may copy the settings for the upload test to the download test by selecting the **Copy download test settings for use in upload test** field. The following fields are available for each type of tests:



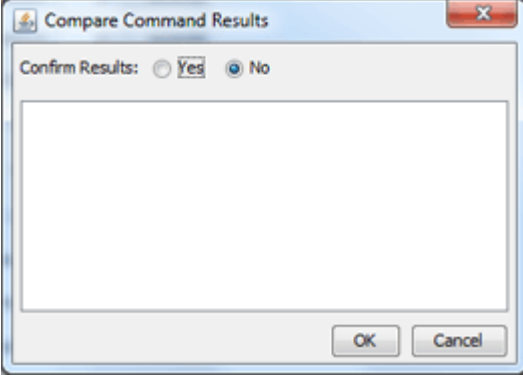
Field	Description
FTP Server Address	IP address of your ftp server that you want to test.
Path	Full path of the file that you want to use in your test.
Port	Port number to your FTP server. (Usually 21 for FTP servers.)
User	User name used to log into the FTP server.
Password	Password of the user specified in the <b>User</b> field.
Maximum Transfer	Maximum amount of data that can be transferred during the test. In addition, a minimum acceptable bandwidth throughput can be specified. If bandwidth throughput is less than the specified value, an error occurs and is displayed in the <b>Results</b> .

### Applications Tab

The **Applications** tab allows you to configure a specialized test using telnet or SSH that tests a connection to a specific server.

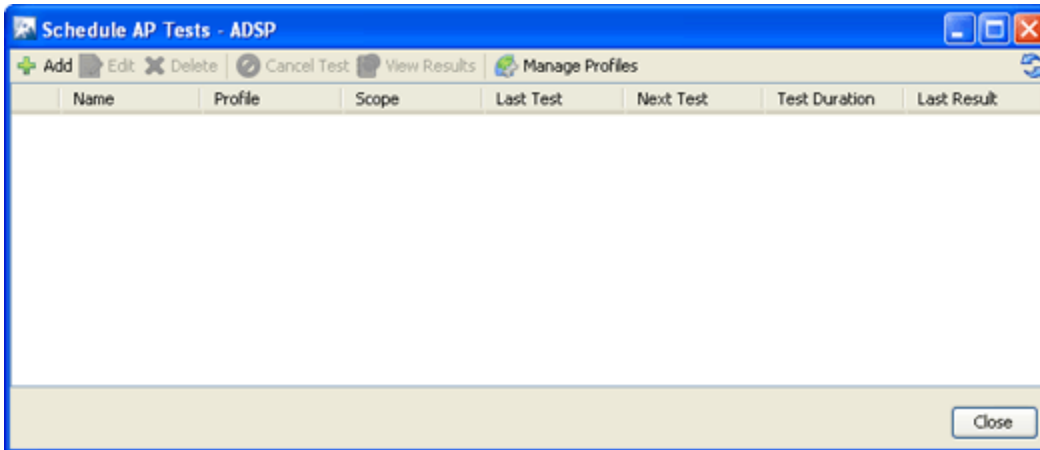
The following fields are available to conduct your applications test:

Field	Description
Enable Applications Test	Turns on applications test so that it runs when conducting an AP Test.
Connection Method	Specifies how to connect to a application server: <b>Telnet</b> or <b>SSH</b> . <b>Note:</b> Telnet does not work with Cisco devices.
Login Timeout	Specifies a timeout value (in seconds) to keep a login active before disconnecting. (Default is 10 seconds.)
Command Timeout	Specifies a timeout value (in seconds) to allow a command to execute. (Default is 10 seconds.)
Command Delay	Specifies a delay (in seconds) before executing a command. (Default is 10 seconds.)
Host	Specifies the IP address or FQDN (fully qualified domain name) or the applications server.
Port	Specifies the port to use.
User	Specifies a username to log into the applications server.
Password	Specifies a password to log into the applications server.
Login Prompt	Specifies the login prompt for the applications server. The specified prompt must match the server's login prompt.

Field	Description
Login Confirm	Specifies a string that appears in the login confirmation. This can be anything within the login confirmation.
Command Prompt	Specifies the command line prompt that is displayed after login to the applications server.
Commands	<p>Specifies command(s) to execute after establishing a connection. You may add up to five commands using the <b>Add Command</b>— icon. The  button is used to specify command results.</p>  <p>You can specify the exact results that are expected from a command when executed. Just select the <b>Yes</b> radio button (default is <b>No</b>) and type in the exact results that are expected. Click <b>OK</b> to close the dialog window.</p>
Logout Command	The command used to log out of the application server (for example, <b>exit</b> ).

## Scheduled Tests

You can schedule AP Tests and view scheduled tests using the **Scheduled AP Tests** window. To access the **Scheduled AP Tests** window, select **Menu > Scheduled AP Test**.



### General Area

The general area includes the table fields and six buttons. This area is always constant.

### Fields

Field	Description
Name	Name of the scheduled AP Test.
Profile	Name of the profile to use in the AP Test.
Scope	Scope (network level or BSS) of the AP Test.
Last Test	Date and time of the last test.
Next Test	Date and time of the next test.
Test Duration	Length (measured in time) of the AP Test.
Last Result	Result of the last test.

### Buttons

Button	Description
Add	Schedules a new test.
Edit	Edits an existing scheduled test.
Delete	Deletes an existing scheduled test.
Cancel Test	Cancels a test that is currently running.
View Results	Displays detailed results of an AP Test.
Manage Profiles	Displays all profiles where you can select and make changes to the individual profiles.
Close	Exits the <b>Scheduled AP Tests</b> window.

### *Adding New AP Test*

To schedule a new AP test, click the **Add** button.

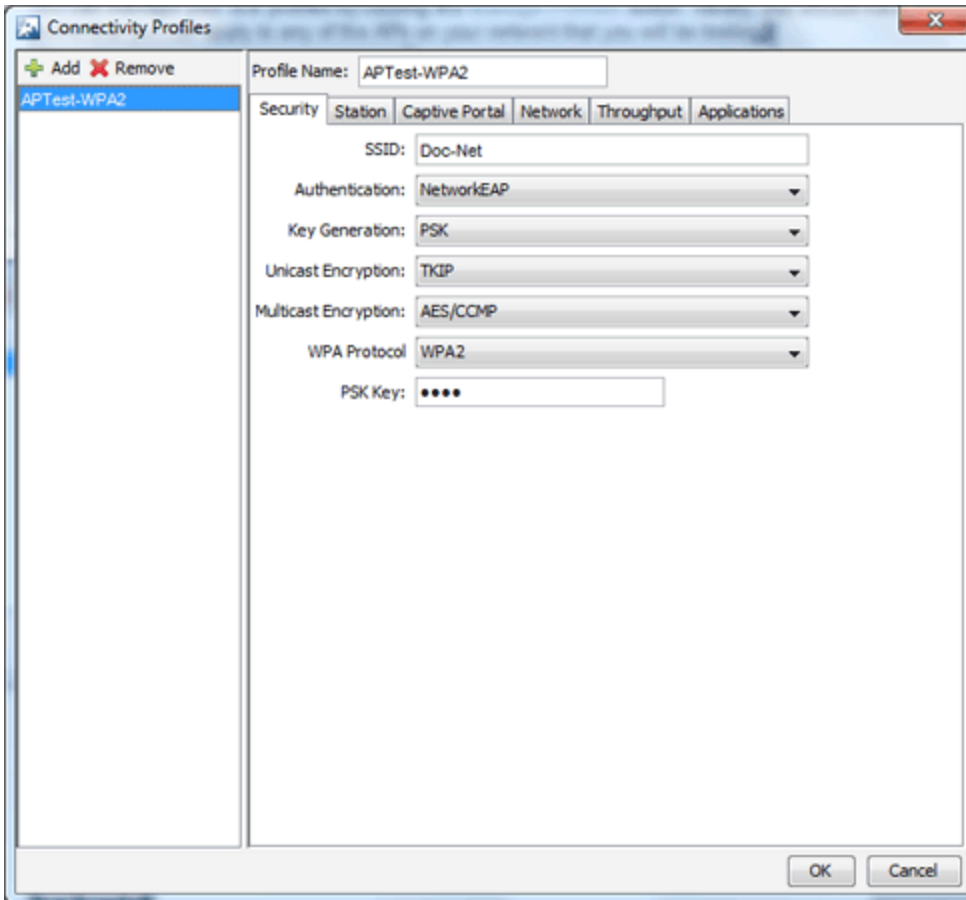
All fields are inactive (grayed out) until you check the **Tests Enabled** checkbox. The window has four sections:

Section	Description
General	The General section is where you name your AP Test and select a profile for the test. You can also edit profiles by clicking the <b>Edit</b> button.
Scope	The Scope section is where you can limit the scope of your AP Test. You can test all of the APs in a specific network level. You can also select one AP as your scope.
Schedule	<p>There are five options to schedule a test:</p> <ul style="list-style-type: none"> <li>• One Time Schedule</li> <li>• Intra-Day Schedule</li> <li>• Daily Schedule</li> <li>• Weekly Schedule</li> <li>• Monthly Schedule.</li> </ul> <p>Once you have selected an option, you must select a time and date for the test.</p>
Advanced	<p>The Advanced section is where you can select specific criteria for the test. There are seven fields that you can configure:</p> <ul style="list-style-type: none"> <li>• <b>Retry Count</b>—Specify the number of times the test should be repeated if not completed. You can elect to switch Sensors on each retry.</li> <li>• <b>Schedule Conflicts</b>—Select to skip a test if the Sensor or profile is already in use or select to wait until the Sensor or profile is available. If you select to wait, you can specify how long to wait in minutes or hours.</li> <li>• <b>SSID Filter</b>—Select whether or not to filter APs using the SSID specified in the profile.</li> <li>• <b>Signal Threshold</b>—Select a signal strength that the AP must have in order to conduct the test. Any AP below the threshold is ignored and will not be tested.</li> <li>• <b>Last Seen Threshold</b>—Specify a threshold in minutes, days, or hours that an AP was last seen on the network. Any AP that has a last seen time older than the one specified will be ignored and will not be tested.</li> <li>• <b>Parallel Tests</b>—Specify the number of buildings to run the test (maximum of 20).</li> <li>• <b>Tests Per Building</b>—Specify a limit on the number of BSSs to test per building per scheduled test. You have the option to specify all or specify a specific number. If you specify a number (like 10) and you have 100 BSSs in a building, the first instance of the scheduled test will run on the first 10 BSSs. Consequently, the next instance of the schedule test will run on the next 10 BSSs and so forth until all 100 BSSs have been tested.</li> </ul>

Once you have set all the options, click **OK** to schedule the test.

## Managing Profiles

You can manage your test profiles by clicking the **Manage Profiles** button. Ideally, you should have a test profile that you can apply to any of the APs on your network that you will be testing.



To edit a profile, click (highlight) the profile name. The profile name will display in the **Profile Name** field. Go to the **Security**, **Station**, **Captive Portal**, **Network**, **Throughput** or **Applications** tab and make changes. These tabs are described in the [On-Demand Tests](#) topic. Click **OK** to save your changes.

You can add a new profile by clicking the **Add** button. You can remove a profile by clicking the **Remove** button.

## Test Results

Test results are displayed in the **Test Results** window which is divided into three parts:

- Common Area
- Summary Tab
- Packets Tab.

### Common Area

This area supplies the overall test results. If the test runs successfully, **AP Test Complete** is highlighted in gray at the top of the **Test Results** window. If there was a test failure, **AP Test Failure** is highlighted in red at the top of the **Test Results** window.

Under the overall test results, a list of devices used in the test is displayed. This list includes:

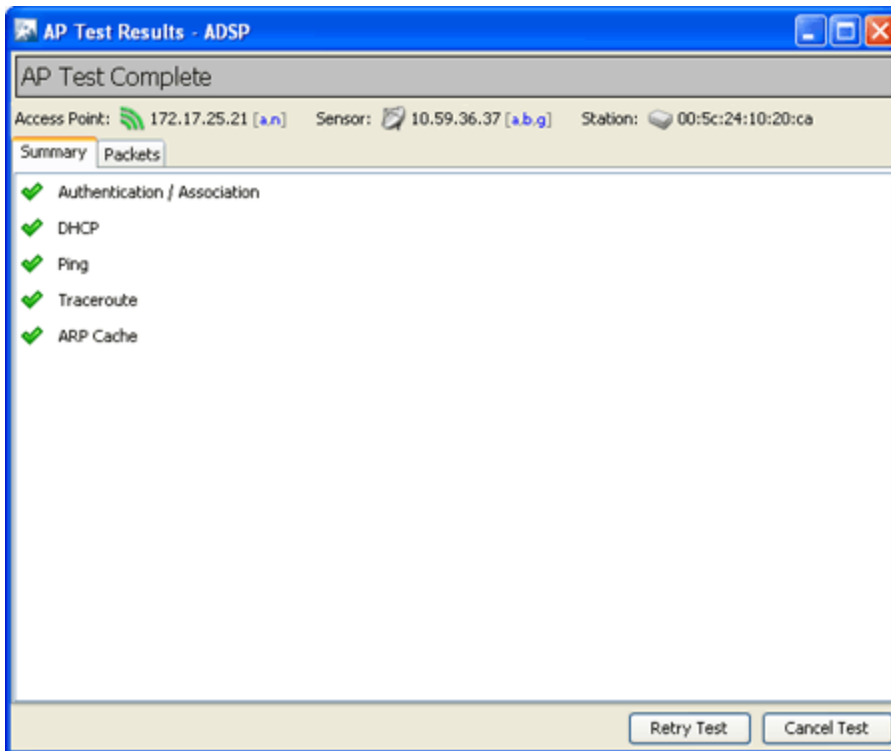
- The AP that was tested



- The Sensor used during the test
- The virtual Wireless Client used during the test.

### **Summary Tab**

The **Summary** tab displays a list of what was tested. Each of the tested items is marked as a success (green checkmark) or failure (red flag). If a tested item is not marked, it was skipped because of a failure of one or more of the test conducted before it.



All tested items are a link that, when clicked, will expand to supply more information about the test.

### **Packets Tab**

The **Packets** tab displays packet information about the items that were tested. There are two views: table and connection ladder. The first time you access the **Packets** tab the table view is displayed.

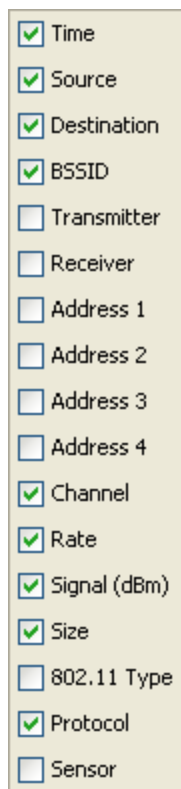
In table view, the following information is displayed:

Column	Description
Time	The time the packet was seen.
Source	The device where the packet originated.
Destination	The device where the packet was sent.
BSSID	The Basic Service Set Identifier.
Transmitter	The device that transmitted the packet.
Receiver	The device that actually received the packet.
Address 1	The first address in the packet.


Column	Description
Address 2	The second address in the packet.
Address 3	The third address in the packet.
Address 4	The fourth address in the packet.
Channel	The WLAN channel that the device is operating on.
Rate	The data rate (in Mbps) being used by the device that sent the packet.
Signal (dBm)	The device's signal strength connectivity on the WLAN.
Size	The packet size.
802.11 Type	The 802.11 protocol type used in the packet
Protocol	The protocol used during transmission of the packet.
Sensor	The MAC address of the Sensor that observed the device that sent the packet.

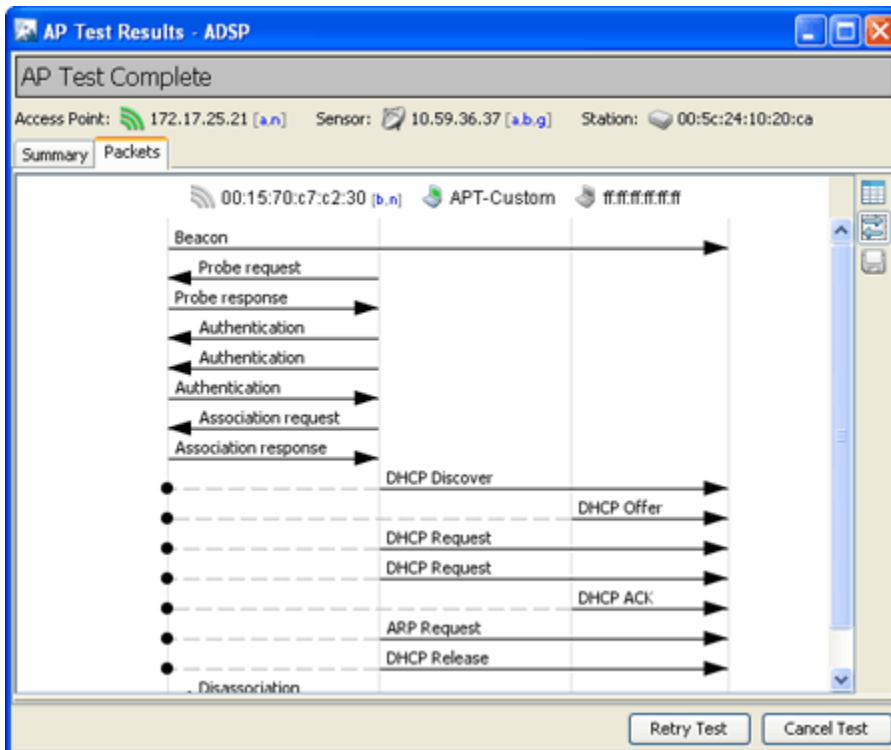
Column display and arrangement can be customized as follows:

- Hide or un-hide a category by right-clicking in the column heading area, and uncheck or checking the checkbox for a category (see below).




- Rearrange columns by clicking on a column heading and dragging it to a new position.

To switch to connection ladder view, click the **Connection Ladder View**— button.



When the **Packets** tab is viewed as a connection ladder, the results are displayed with a vertical line for each device and horizontal lines for each packet. The vertical line is there to show where the packet information is flowing. The horizontal line is there to show which the direction the packet is flowing.

You can switch back to the table view by clicking the **Table View**— button.

You can save the frame information to a file by clicking the **Save Frame to File**— button.

## Scheduled Vulnerability Assessment


✓ **NOTE** Vulnerability Assessment requires a Vulnerability Assessment license for access.

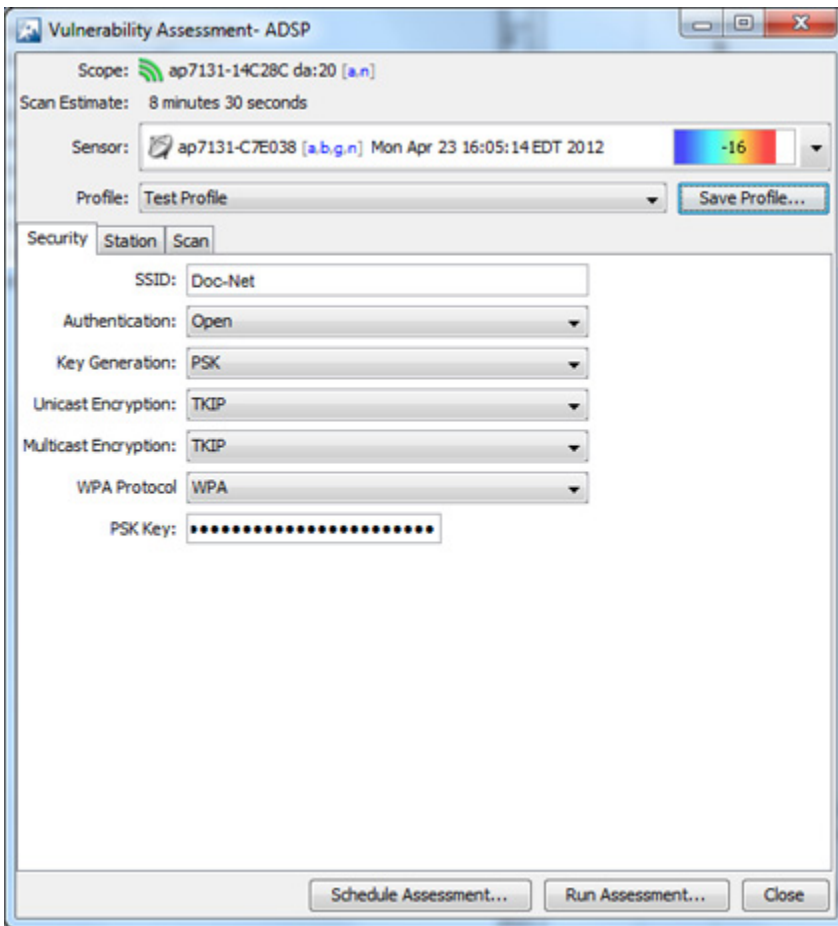
Using your existing Sensor deployment, Vulnerability Assessment scans your wireless network using a hacker's point-of-view. This allows you to:

- Identify network security issues before a hacker does
- Remotely scan for and discover wireless network vulnerabilities
- Generate reports identifying your network vulnerabilities.

The assessment is accomplished by using deployed Sensors as a wireless station 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.

## On-Demand Assessment

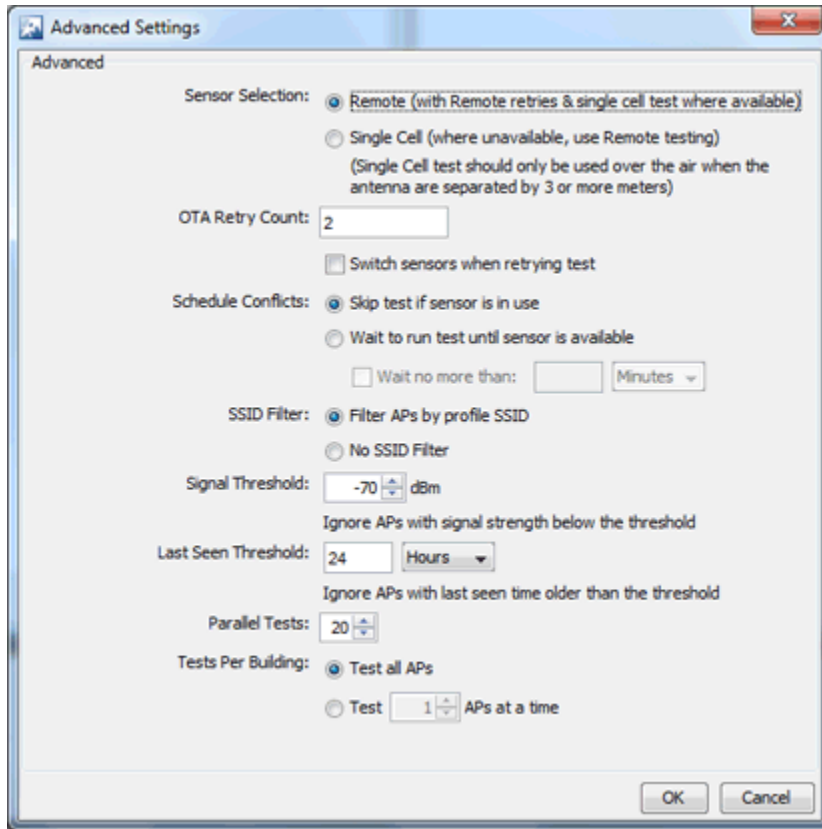
You can conduct a Vulnerability Assessment anytime you need by using an on-demand assessment. To initiate an on-demand assessment, click on the drop-down menu—  button for a BSS or network level, and select **Wireless Vulnerability Assessment**.



After accessing the **Vulnerability Assessment** window, follow these steps:

1. Set or change any configurable options in the **Security**, **Station**, or **Scan** folders. If any changes are made, save the current profile or save a new profile.

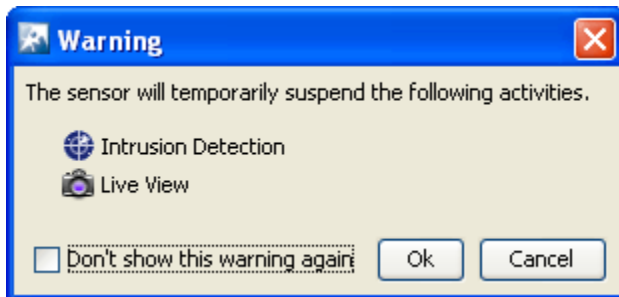
- Run the on-demand assessment by clicking the **Run Assessment** button. If the scope is a BSS, the assessment runs and the **Vulnerability Assessment Results** window displays (see [Assessment Results](#) topic). If the scope is a network level, the **Advanced Settings** window displays:



- If the **Advanced Settings** window displays, configure the advanced settings using the following fields:

Field	Description
Retry Count	Specify the number of times to retry the assessment. You can also elect to switch Sensors when retrying assessments.
Schedule Conflicts	Specify that you want to skip the assessment if the Sensor is in use or that you want to wait to run the assessment until the Sensor is available. If you elect to wait, you may also limit the waiting time.
SSID Filter	Decide if you want to filter APs by SSID profile or not.
Signal Threshold	Limit assessment to APs with a signal strength above a value that you specify.
Last Seen Threshold	Limit assessment to APs that were last seen on your network within a time limit that you specify.
Parallel Tests	Specify the number of buildings to run the assessment (maximum of 20).
Tests Per Building	Specify a limit on the number of BSSs to assess per building. You have the option to specify all or specify a specific number.

- Click **OK** to set the advanced settings. A **Warning** window displays.



This window alerts you to the fact that any of the listed activities will be suspended while running the assessment.



**NOTE** You can elect not to display future warnings by selecting the **Don't show this warning again** checkbox.

- Click **OK** to run the assessment.

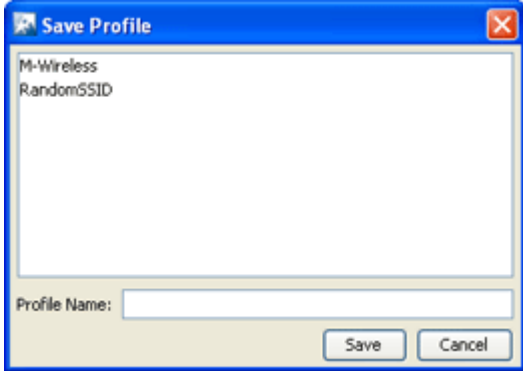
### ***Common Area***

The common area includes everything not included in a tab and is always in view. There are three fields and four buttons included in the common area.

#### **Fields**

Field Description	
Scope	Displays the scope of the assessment. The scope may be a single AP, all the APs in your system, all the APs in a location, or all the APs in a group.
Scan Estimate	Displays the approximate time it will take to run the a network scan for the Vulnerability Assessment.
Profile	Selects/displays the name of the current profile to use for the Vulnerability Assessment.

**Buttons**

Button	Description
Save Profile	<p>Saves the current settings to a profile that you name. Profiles make it easy to apply the same settings to different Vulnerability Assessments. When selected, a <b>Save Profile</b> window is displayed.</p>  <p>Type in a new profile name and click <b>Save</b>. Once saved, you can apply the profile to set up an Vulnerability Assessment.</p>
Schedule Assessment	Opens the <b>Add Scheduled Vulnerability Assessment</b> window where you can add a new assessment to the schedule.
Run Assessment	Conducts the Vulnerability Assessment. (See <a href="#">Assessment Results</a> for details.)
Close	Exits <b>Vulnerability Assessment</b> window without running an assessment.

**Security Tab**

The **Security** tab for Vulnerability Assessment provides fields for SSID, authentication, encryption, key generation and WEP keys or EAP username/password. The fields will be initialized to the current profile settings of the AP. In most cases, you will not have to change any of the field. In a some cases, you may have to change a field because a field was not set in the AP profile or the profile was not set up correctly.

✓ **NOTE** Depending on the field options, some fields may or may not be visible.

Field	Description
SSID	Service Set Identifier (SSID) of the Access Point.
Authentication	Type of authentication used to authenticate users on a local or remote (LDAP or RADIUS) server. Choices are <b>Open</b> , <b>Shared Key</b> , or <b>NetworkEAP</b> .
Key Generation	Method used to generate the keys that are necessary to encrypt data. Choices are <b>None</b> , <b>802.1x</b> , <b>PSK</b> , or <b>EAP</b> .
Unicast Encryption	Encryption method used during unicast transmissions.
Multicast Encryption	Encryption method used during multicast transmissions.
WPA Protocol	Wi-Fi Protected Access (WPA) method used to secure the connection to the wireless network. Choices are <b>WPA</b> or <b>WPA2</b> .
PSK Key	Pre-shared key (shared secret) used to authenticate user access to the AP.

Field	Description
Key Size	Key size used for a WEP key. Choices are <b>64 bits 10 hex digits</b> or <b>128 bits 26 hex digits</b> .
WEP Key	Wireless Equivalent Privacy (WEP) key used to authenticate user access to the AP.
Key Index	Index number used to identify a WEP key.
EAP Method	Extensible Authentication Protocol (EAP) method used in LAN authentication. Choices are <b>LEAP</b> , <b>EAP/Fast Auto</b> , <b>EAP/Fast Manual</b> , <b>EAP-TLS</b> , <b>PEAP-MSCHAPv2</b> , <b>PEAP-GTC</b> , or <b>PEAP-TLS</b> . All methods except LEAP and EAP/FAST Auto, when selected, allow you to use certificates (User Certificate, Root CA, or EAP-FAST PAC) when assessing vulnerability.
EAP Username	EAP username used in LAN authentication.
EAP Password	EAP password used in LAN authentication.

### ***Station Tab***

Vulnerability Assessment uses a virtual station for its connectivity test. The **Station** tab allows you to configure the virtual station used during the Assessment.

Station

MAC Address:

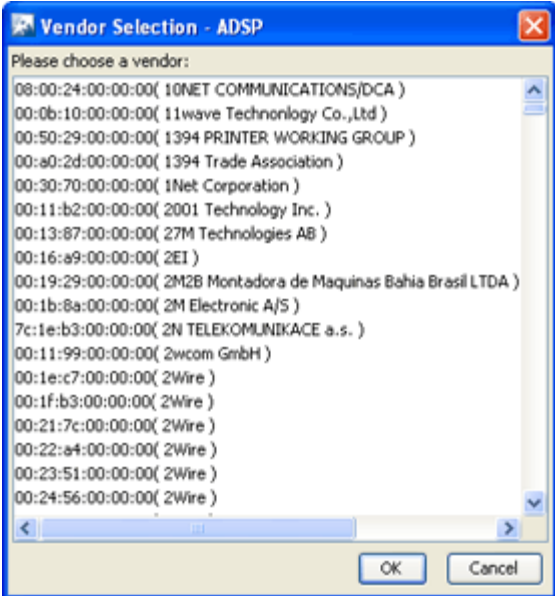
Obtain IP address using DHCP
 

IP Address:   
 Subnet Mask:   
 Default Gateway:

Obtain DNS server address automatically
 

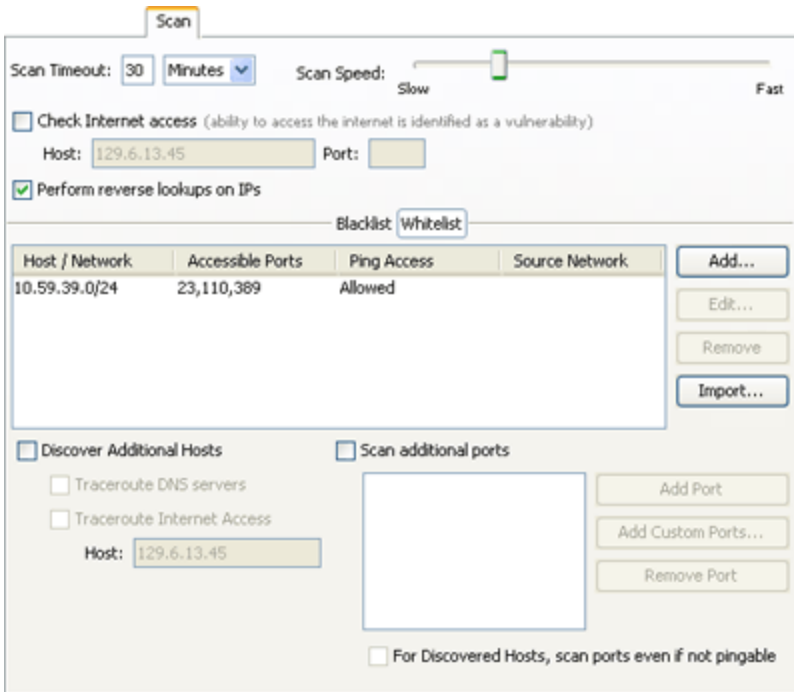
Primary DNS:   
 Secondary DNS:   
 Domain Name:



Field	Description
MAC Address	<p>Since Vulnerability Assessment uses a virtual station for its assessment, an artificial MAC address must be specified for the test station. The MAC address field is initialized to the most recently used test station's MAC address. If no previous address is found, a random MAC address is used.</p> <p>You may change the MAC address by typing one in the field or click the <b>Random Access</b> button to generate one. You may also generate a MAC address by clicking the <b>Vendor Address</b> button and selecting a vendor from a list of vendors.</p>  <p>The first 3 hexadecimal codes are vendor specific. The last 3 codes are generated when you make a selection to form a simulated MAC address.. A warning message is displayed if you select a MAC address that matches an observed device. Also, if you attempt to save a profile and the MAC address matches a MAC address of a station in another profile, an error message is displayed.</p>
Obtain IP address using DHCP	<p>You can obtain an IP address using DHCP or specify a static IP address. If you want to specify an static IP address, you must also specify the subnet mask and default gateway. The default is to obtain IP address using DHCP. Uncheck the checkbox to activate the fields and to specify a static IP address, subnet mask, and default gateway.</p>
Obtain DNS server address automatically	<p>You can obtain DNS server information automatically or specify the information yourself. The default is to obtain the information automatically. If you want to specify the information, uncheck the checkbox to activate the fields and then specify the primary DNS, secondary DNS, and domain name.</p>

**Scan Tab**

The **Scan** tab allows you to configure the options used during a Vulnerability Assessment.

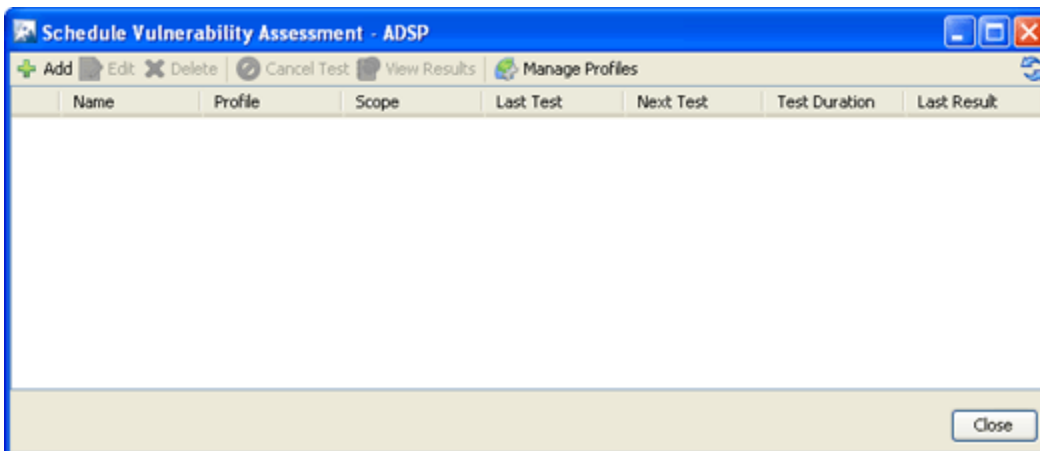


Field	Description
Scan Timeout	Limits the time that the scan will run to x amount of minutes or hours.
Scan Speed	Sets the scan speed from slow to fast.
Check Internet access	Checks to see if users have Internet access for a specific host and/or port. If access is available, it is identified as a vulnerability. If checked supply a host IP address and port number.
Perform reverse lookups on IPs	Performs a reverse lookup to find IP addresses.

Field	Description
Blacklist/Whitelist	<p>Configures either a blacklist or a whitelist for the assessment. If configuring a blacklist, specify a list of devices and services that should not be accessible. If configuring a whitelist, specify a list of devices and services that should be accessible.</p> <p><b>Note:</b> Whitelist cannot be used when scheduling assessments.</p> <p>Click the <b>Add</b> button to configure the list. For the <b>Host / Network</b> field, type in a host name, an IP address, or IP network. For the <b>Accessible Ports</b> field, type in the port number or click <b>Add Port</b> and select ports from the popup list. For the <b>Ping Access</b> field, select <b>Allowed</b>, <b>Not Allowed</b>, or <b>Don't Care</b> from the drop-down menu. For the <b>Source Network</b> field, type in the source network if the host IP address is in the source network. Leave the <b>Source Network</b> field blank to ignore the source network.</p> <p>You can edit an entry in a blacklist or whitelist by selecting (highlighting) the entry and then clicking the <b>Edit</b> button.</p> <p>You can import a blacklist or whitelist by clicking the Import button. A preformatted CSV file must be selected as your import file. The file format is:  "Host/IP/Network", "Ports", "Ping Access", "Source"</p> <p>Each line in the import file contains four fields and a comma must separate the fields. Quotation marks are mandatory if multiple items make up a field. Otherwise, they are optional. Multiple items in a field are also separated by commas. A blank field designates an empty field.</p> <p><b>Example:</b> 192.168.1.3, "53,79,80", Allowed,</p>
Discover Additional Hosts	<p>Only available with whitelist. Discover additional hosts using one or more of the following methods:</p> <ul style="list-style-type: none"> <li>• Tracing routes to DNS servers</li> <li>• Tracing routes of a host with Internet access.</li> </ul>
Scan additional ports	<p>Only available with whitelist. Scan additional ports that you specify. Click <b>Add Port</b> to select from a list of ports. Click <b>Add Custom Ports</b> to type in a list of ports. You also have the option of scanning ports even if they cannot be pinged. You can remove a port from the list by selecting (highlighting) it and clicking <b>Remove Port</b>.</p>

## Scheduled Assessment

You can schedule a Vulnerability Assessment using the **Schedule Vulnerability Assessment** window. To access the **Schedule Vulnerability Assessment** window, select **Menu > Scheduled Vulnerability Assessment**.



All scheduled Vulnerability Assessments are listed in the table.

### General Area

The general area includes the table and six buttons. This area is always constant.

### Fields

All scheduled Vulnerability Assessments are listed in the table. The following fields are available:

Field	Description
Name	Name of the scheduled Vulnerability Assessment.
Profile	Name of the profile to use in the Vulnerability Assessment.
Scope	Scope (system, location, group, or a single AP) of the Vulnerability Assessment.
Last Test	Date and time of the last assessment.
Nest Test	Date and time of the next assessment.
Test Duration	Length (measured in time) of the Vulnerability Assessment.
Last Result	Result of the last assessment.

### Buttons

The following buttons are available while scheduling Vulnerability Assessments:

Button	Description
Add	Schedules a new assessment.
Edit	Edits an existing scheduled assessment.
Delete	Deletes an existing scheduled assessment.

Button	Description
Cancel Test	Cancels an assessment that is currently running.
View Results	Displays detailed results of a Vulnerability Assessment.
Manage Profiles	Displays all profiles where you can select and make changes to the individual profiles.

### *Adding New Assessments*

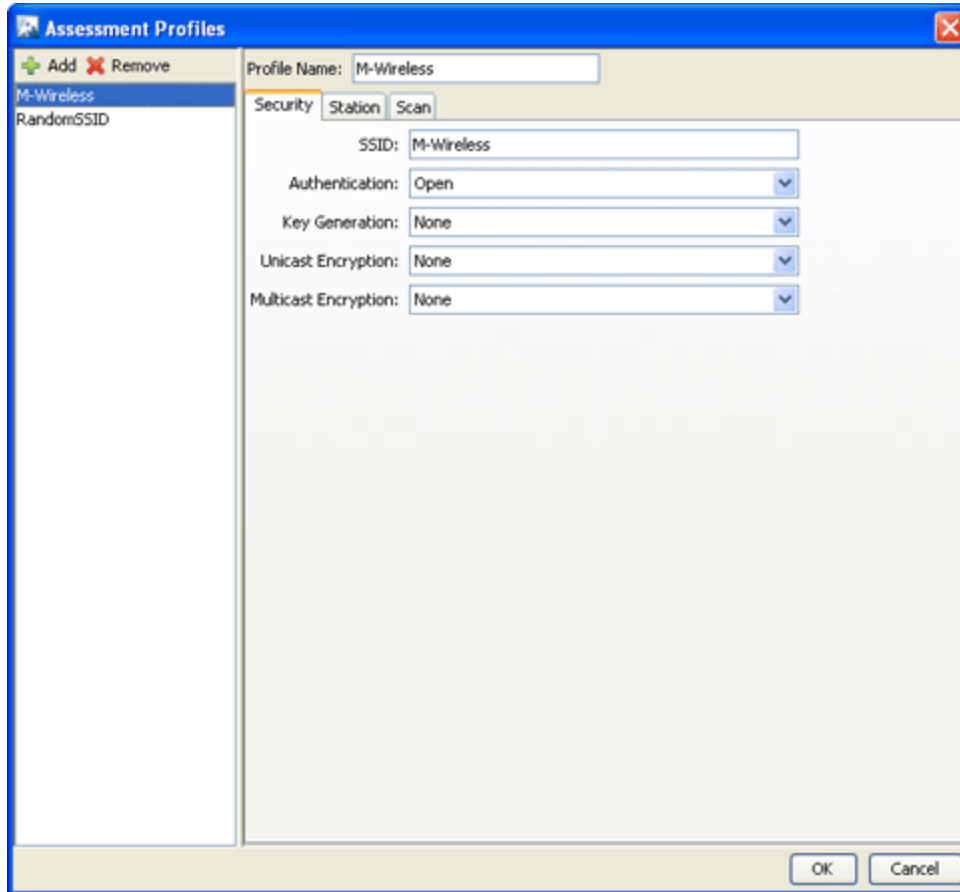
To schedule a new Vulnerability Assessment, click the **Add** button.

All fields are inactive (grayed out) until you check the **Assessment Enabled** checkbox. The window has four sections:

Section	Description
General	The General section is where you name your Vulnerability Assessment and select a profile for the assessment. You can also edit profiles by clicking the <b>Edit</b> button.
Scope	The <b>Scope</b> section is where you can limit the scope of your Vulnerability Assessment. You can test all of the APs in a specific network level. You can also select one AP as your scope.
Schedule	<p>There are five options to schedule an assessment</p> <ul style="list-style-type: none"> <li>• One Time Schedule—Choose a time for the assessment by selecting a time from the <b>Time</b> drop-down menu. Then, select a day for the assessment by clicking the <b>Calendar</b> button in the <b>Date</b> field and selecting a date.</li> <li>• Intra-Day Schedule—Select a time to begin the assessment. Then, select a frequency in hours.</li> <li>• Daily Schedule—Select a frequency in day, weekdays only, or weekends only. Then, select a time of day.</li> <li>• Weekly Schedule—Choose a frequency in days. Then, select a day or multiple days to conduct the assessment by clicking the checkbox next to the day to place a checkmark in the box.</li> <li>• Monthly Schedule—Choose the months that you want to run a assessment 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 assessment. Last, specify a time of day.</li> </ul> <p>Once you have selected an option, you must select a time and date for the assessment.</p>
Advanced	<p>The <b>Advanced</b> section is where you can select specific criteria for the assessment. There are seven fields that you can configure:</p> <ul style="list-style-type: none"> <li>• OTA Retry Count—Specify the number of times the assessment should be repeated if not completed. You can elect to switch Sensors on each retry.</li> <li>• Schedule Conflicts—Select to skip an assessment if the Sensor or profile is already in use or select to wait until the Sensor or profile is available. If you select to wait, you can specify how long to wait in minutes or hours.</li> <li>• SSID Filter—Select whether or not to filter APs using the SSID specified in the profile.</li> <li>• Signal Threshold—Select a signal strength that the AP must have in order to conduct the assessment. Any AP below the threshold is ignored and will not be assessed.</li> <li>• Last Seen Threshold—Specify a threshold in minutes, days, or hours that an AP was last seen on the network. Any AP that has a last seen time older than the one specified will be ignored and will not be assessed.</li> <li>• Parallel Tests—Specify the number of buildings to run the assessment (maximum of 20).</li> <li>• Tests Per Building—Specify a limit on the number of BSSs to assessment per building per scheduled assessment. You have the option to specify all or specify a specific number. If you specify a number (like 10) and you have 100 BSSs in a building, the first instance of the scheduled assessment will run on the first 10 BSSs. Consequently, the next instance of the schedule assessment will run on the next 10 BSSs and so forth until all 100 BSSs have been tested.</li> </ul>

## Managing Profiles

You can manage your assessment profiles by clicking the **Manage Profiles** button. Ideally, you should have an assessment profile that you can apply to any of the APs on your network that you will be assessing.



To edit a profile, click (highlight) the profile name. The profile name will display in the **Profile Name** field. Go to the **Security**, **Station**, or **Scan** tabs and make changes. These tabs are described in the [On-Demand Tests](#) topic. Click **OK** to save your changes. You can add a new profile by clicking the **Add** button. You can remove a profile by clicking the **Remove** button.

## Assessment Results

Assessment results are displayed in the **Assessment Results** window which is divided into two parts:

- Common Area
- Results Area.

### Common Area

This area supplies the overall assessment results. If there were no vulnerabilities found, **No Vulnerabilities Found** is highlighted in green at the top of the **Vulnerability Assessment Results** window. If there were vulnerabilities found, **Vulnerabilities Found** is highlighted in red at the top of the **Vulnerability Assessment Results** window. If the virtual Wireless Client cannot be associated with any AP in the selected scope, **APs not Accessible** is highlighted in red at the top of the **Vulnerability Assessment Results** window.

Under the overall assessment results, a list of items used in the assessment is displayed. This list includes:

- The profile used for the assessment
- The SSID used for the assessment
- The scan type used for the assessment
- The scope used for the assessment.

Under the above list are two options that affect how the results are displayed in the **Results** area:

Option	Description
Show only vulnerabilities	Only show the APs with vulnerabilities. Vulnerabilities are displayed under the AP.
Show network scope	Show network scope down to the APs with vulnerabilities. Vulnerabilities are displayed under the AP.

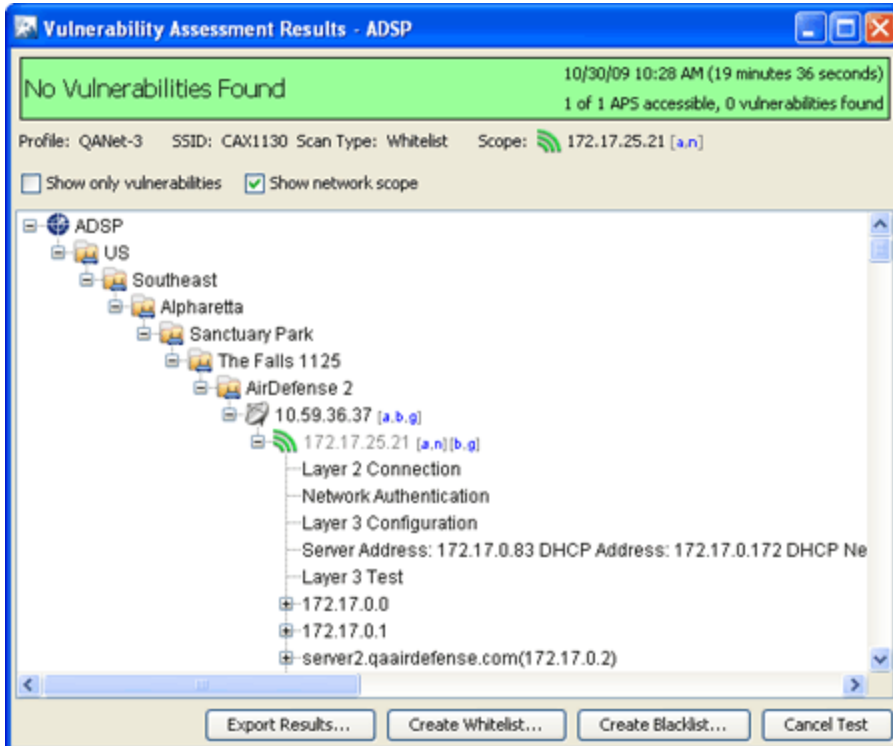
At the bottom of the window, the following four buttons are available:

Option	Description
Export Results	Exports the results of the assessment to a CSV file on your workstation. An <b>Export Results</b> window displays where you can specify a destination and a file name for the exported file.
Create Whitelist	Opens the <b>Vulnerability Assessment</b> window where you can define a whitelist in the <b>Scan</b> tab. The whitelist must be saved in the current profile or a new profile. You can then run a new assessment.
Create Blacklist	Opens the <b>Vulnerability Assessment</b> window where you can define a blacklist in the <b>Scan</b> tab. The blacklist must be saved in the current profile or a new profile. You can then run a new assessment.
Cancel Test	Cancels any further assessments and exits the <b>Vulnerability Assessment Results</b> window.

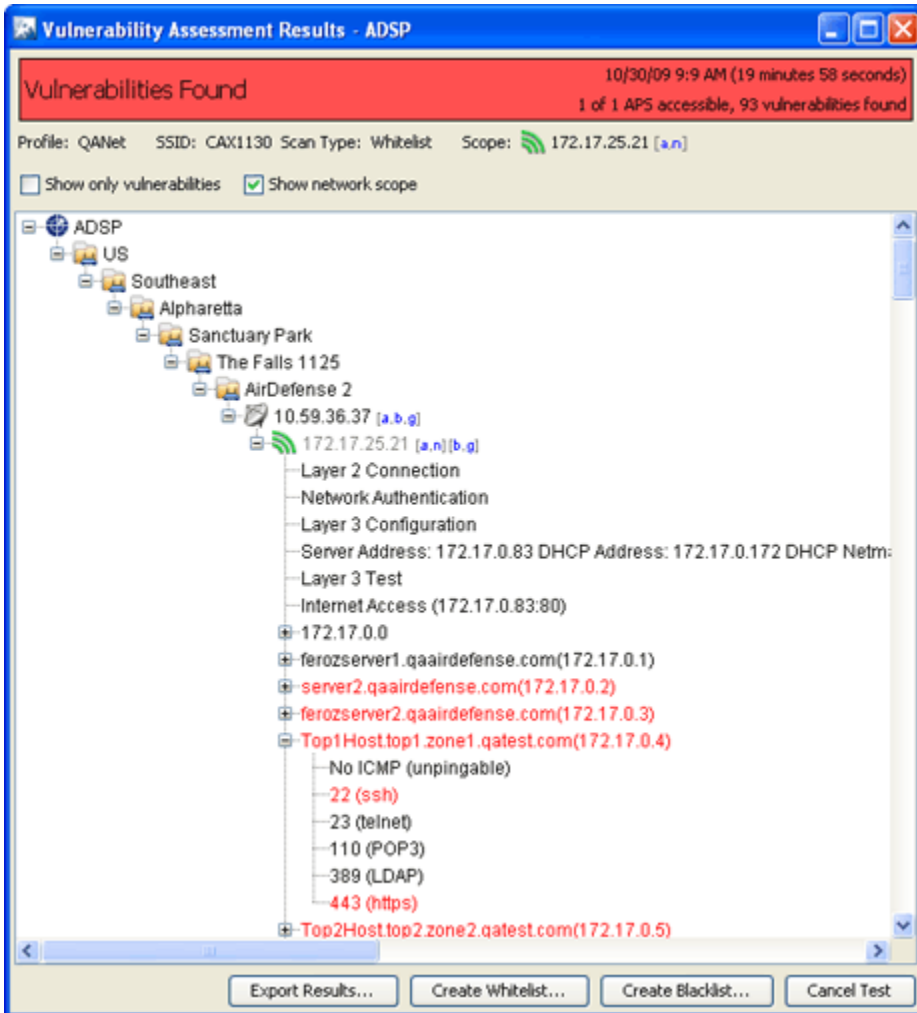


### Results Area

The results area displays a list of assessment results. If no vulnerabilities were found, only a list of discovered resources are displayed.



If vulnerabilities were found, they are displayed according to the display option that was chosen.



Vulnerabilities are listed under the AP that was assessed. The type of vulnerability is displayed along with the IP address (or host name) where the vulnerability was discovered. If the plus sign (+) next to the vulnerability is clicked, the ICMP information and the port numbers used are displayed.



## 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**.

Type	Schedule	Last Run	Next Run	Duration	Last Result
<input checked="" type="checkbox"/> Device Mana...	Intra-Day	4/18/13 4:05 PM	4/18/13 4:10 ...	15 seconds	Success
<input checked="" type="checkbox"/> Device Mana...	Intra-Day	4/18/13 11:06 ...	4/18/13 7:06 ...	0 seconds	Success
<input checked="" type="checkbox"/> Device Mana...	Intra-Day	4/18/13 4:08 PM	4/18/13 4:11 ...	0 seconds	Success
<input checked="" type="checkbox"/> Device Mana...	Intra-Day	4/18/13 4:07 PM	4/18/13 5:07 ...	0 seconds	Success
<input checked="" type="checkbox"/> Device Mana...	Intra-Day	4/18/13 4:08 PM	4/18/13 5:08 ...	0 seconds	Success
<input checked="" type="checkbox"/> LiveRF Backg...	Intra-Day	4/18/13 3:59 PM	4/18/13 4:14 ...	1 seconds	Success
<input checked="" type="checkbox"/> Device Import	Monthly		12/31/13 12:0...		
<input checked="" type="checkbox"/> Spectrum Ana...	One Time				
<input checked="" type="checkbox"/> System	Intra-Day	4/18/13 4:04 PM	4/18/13 4:24 ...		Success
<input checked="" type="checkbox"/> Backups	Daily	4/18/13 12:00 ...	4/19/13 12:00 ...	10 seconds	Success

4/18/13 12:00 AM

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

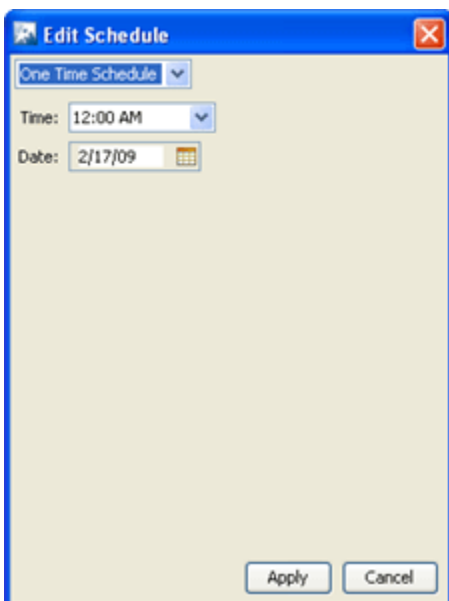
- AP Test
- Auto Classification
- Backups
- Firmware Upgrade
- Frame Capture
- Server Sync
- System
- Forensic Backup
- Device Import
- Vulnerability Assessment
- Device Management Poll
- Device Configuration
- Deferred Device Configuration
- LiveRF Background Analysis
- Primary Appliance Poll
- Spectrum Analysis
- Wing Integration: Keep Alive
- Logs Backup.

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 drop-down 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 <b>Time</b> drop-down menu. Then, select a day for the backup by clicking the <b>Calendar</b> button in the <b>Date</b> 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.

Once you have made your changes, click the **Apply** button.

You can delete a scheduled event by clicking the **Delete** button. A confirmation window will display. Click **Yes** to delete the schedule event.

## Add Devices

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

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
- Appliance (must have a Central Management license to add appliances).

✓ **NOTE** Once you add an appliance (slave), it is added to your network tree in an offline state. Before the slave becomes online, you must share the master and slave certificates ([Sharing Certificates](#)). You can then add network levels under the slave appliance just like you would your own appliance (master).

The fields change according to the selected device. Click the **Add** button to add the device.

### BSS and Wireless Clients Fields

**Add Devices**

Device Type: **BSS**

MAC Address:

Name:

Description:

Add to appliance:  Primary appliance only  All appliances

Annotations:  Flagged  Bridge

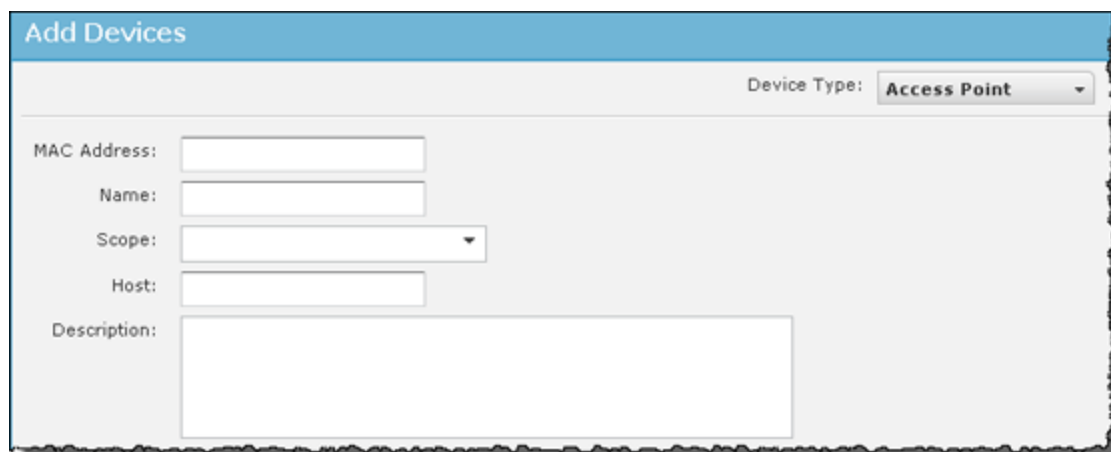
Classification:  Neighboring  
 Unsanctioned  
 Sanctioned (inherit)  
 Sanctioned (override)

AD\_ralfenator\_Security\_Profil

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"> <li>• Neighboring</li> <li>• Unsanctioned</li> <li>• Sanctioned (inherit)</li> <li>• Sanctioned (override)—a list of available profiles is displayed to use as the override profile(s). You may select one or more profiles.</li> </ul>

### All Other Devices Fields



The screenshot shows a web form titled "Add Devices". At the top right, there is a "Device Type:" label followed by a dropdown menu currently showing "Access Point". Below this, the form contains several input fields: "MAC Address:" with a text box, "Name:" with a text box, "Scope:" with a dropdown menu, "Host:" with a text box, and "Description:" with a large, empty text area.

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 drop-down 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 classified according to Auto-Licensing. 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

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., c:\temp\filename)



Field	Description
Select a sample CSV file	Selects a sample CSV file from the drop-down list. Once a file is selected, click the <b>Open in New Window</b> 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

Job Type:

Descriptions:

Host:

Protocol:

Path:

User:

Password:

Add to appliance:

Use auto-placement rules  
 Place devices in a single folder

? 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.

Select a sample CSV file ...

Open in New Window

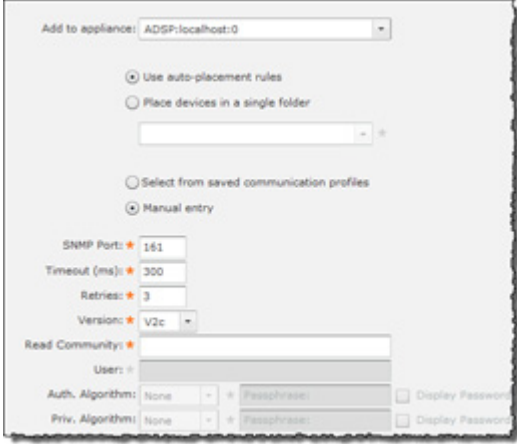
The following fields are available when importing remote files:

Field	Description
Job Type	<b>Import Remote File</b>
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 (*).
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.

Field	Description
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"> <li>• <b>SNMP Port</b>—Device SNMP port number; normally set to 161 but can be different</li> <li>• <b>Timeout (ms)</b>—Timeout in milliseconds to attempt import</li> <li>• <b>Retries</b>—Number of retries to attempt import</li> <li>• <b>Version</b>—SNMP version used: V1, V2c or V3</li> <li>• <b>Read Community</b>—Read Community string used for the SNMP authentication</li> <li>• <b>User</b>—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.</li> <li>• <b>Authentication/Privacy Algorithm</b>—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.</li> </ul>

## 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 <b>Search</b> . The search results are listed in the <b>Select from search results</b> box. Select a device from the list and then click one of the <b>Start Import</b> buttons. Devices associated with the Wireless Manager/Switch are imported into ADSP. The following search criteria are available: <ul style="list-style-type: none"> <li>• MAC address</li> <li>• Name</li> <li>• DNS name</li> <li>• Vendor name.</li> </ul>
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 two types of file formats:

- Devices
- Profiles and Configurations.

Import files contain records, made up of columns (fields), that are used to import devices or profiles and configuration settings into ADSP. Here is some guidance on creating import files:

- There can only be one record on a line.
- The record name must always be the first column.
- Each record has a default column sequence. For instance, an AP record default column sequence is:  
AP ; NAME ; DESCRIPTION ; MAC\_ADDRESS ; IP ; DNS\_NAME ; MODEL ; ADD\_OR\_DEL ; FIRMWARE
- The default column sequence must always come before any other columns. Optional columns may follow in any order.
- Some columns (fields) are mandatory. You must include mandatory columns for each record.
- Some columns (fields) are flexible. Flexible columns may be left out of the record; however, ADSP will (depending on the column) supply a value for a flexible column.

Information about the records can be found under Devices or Profiles and Configurations.

### **Devices**

To view the information, click on a link below in the ADSP Help.



**NOTE** You can only access this information in the ADSP Help. Also, you may have to scroll down to find the information you want if you are using Firefox as your browser.

- AP
- AUTOLIC\_IMPORT
- BSS
  - Requirements:  
Importing BSSs require performance and security policy information. The relevant policies must be created prior to importing the file or created within the file. You can create the BSS in line 1 of the file and the policies later in the file. The sequence does not matter.
- DEV\_IMPORT\_CLASS
- DEV\_ON\_WIRE
- STATION
  - Requirements:  
Importing Stations require performance and security policy information. The relevant policies must be created prior to importing the file or created within the file. You can create the Station in line 1 of the file and the policies later in the file. The sequence does not matter.
  - Allowed Values of Station Type:

- New Client Type
  - Scanner
  - Employee Personal Device
  - Laptop
  - Tablet
  - Loyalty Customer
  - In Store Customer
  - Potential Customer
  - Phone
  - Uncategorized Device
  - Guest Wi-Fi User.
- STATIONLITE
  - SWITCH

### *Profiles and Configurations*

Profiles and configuration settings can be created by importing the data from an import file. The import file supplies data that match the fields of a particular profile or configuration in the ADSP GUI. There is a column for each field in the profile or configuration that exists in the GUI.

There is a special record for scheduling AP Tests or Wireless Vulnerability Assessments. Before you can schedule an AP Test or Wireless Vulnerability Assessment, profile data must be created by importing through an import file or through the GUI. Information about scheduling AP Tests or Wireless Vulnerability Assessments can be found in the [Scheduling AP Test or Vulnerability Assessment](#) topic.

To view the information, click on a link below in the ADSP Help.

✓ **NOTE** You can only access this information in the ADSP Help.

- FOLDER
- ACCESS\_CONFIG
- APT\_PROFILE
- AUTOPLACEMENT\_RULE
- CHANNEL\_CONFIG
- CLEAR\_COMM
- CLI\_CONF
  - Mapping for Device Type:
    - ap51x1=1
    - ap71x1=2
  
    - ws2000=4
    - ws5100=5
    - rfsx000=6
    - airespace=7
    - wm3x00=8
    - ap35x0=9
    - ap47x0=10
    - brx000=11
    - br51x1=12

- br71x1=13
- ap7181=14
- Cisco1200Plugin=20
- cb3000=23
- ap650SA5000R=24
- Wing 5.2=25
- IRIS=26
- SILK=27
- ArubaPlugin=28
- extreme.WM2000Plugin=50
- CLI\_PROF
- COMM\_SETTINGS
- COMM\_SETTINGS\_LOC
- DELETE\_PROFILE
- IDS\_FREQ
- IDS\_PROFILE
- KEY\_PROFILE
- LBS\_CONFIG
- LOC\_RSSI
- LOC\_REGION
- LOC\_PRESENCE
- LOC\_SUB
- NAMED\_PROFILE
- PERF\_POLICY
- POLL\_SETTINGS
- RADIUS\_CONFIG
- RADIUS\_INFO
- REALM\_CONFIG
- RELAY\_PARAMS
- SCHEDULED\_IMPORT
- SECURITY\_PROFILE
- SENSOR\_SETTINGS
- SYSTEM\_SETTINGS
- USER\_INFO
- WLAN\_PROFILE
- Import Rules:

- The last field NUM\_KEYS\_RADIUS\_SERVERS is zero by default.
  - For protocol EAP,WPA and WPA2, RADIUS server information is expected.
  - RADIUS Server information is preceded by record name radius\_info and followed by RADIUS server name.
  - For WPA\_PSK and WPA2\_PSK, the primary shared key and ascii value need to be made available.
  - If the protocol is Shared or Open, then Key information needs to be provided. The key information is specified as follows:  
KEY\_PROFILE,<Index 1,2..>, <transmit key/default TRUE>, <ascii/default TRUE>,<The WEP Key>
  - If the number of keys/radius servers are greater than 0, no further WLAN profiles will be accepted until all keys or RADIUS server information is provided. Information can be sent in any sequence except for WLAN profiles and LBS profiles which require information in that order.
- WVA\_PROFILE

### 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)

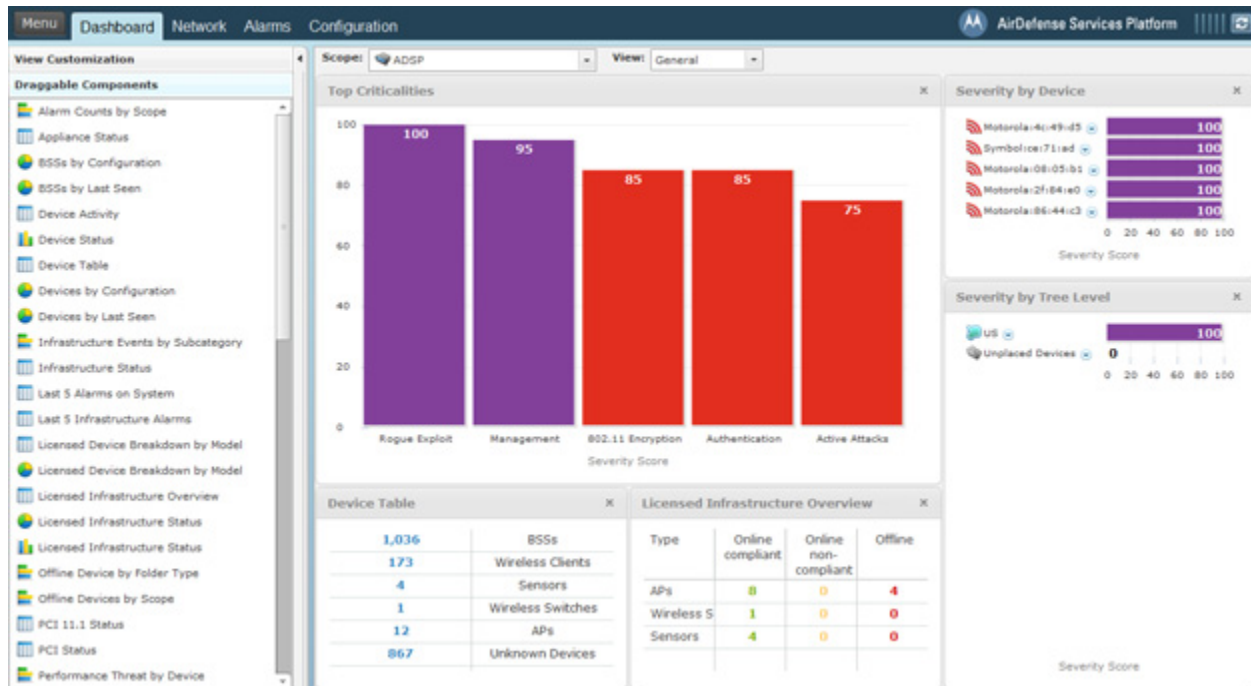
Examples:

```
scheduled_test,TRUE,APT_ProfileName1,00:11:22:33:44:55,2,TRUE,-70,10,TRUE,TRUE,10,20,Schedule1,0
netime,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
```

## Dashboard

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



✓ **NOTE** You must have the latest version of Flash installed in order to view the Dashboard. If you do not, you will be prompted to install the latest Flash.

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.

You can customize the custom views or the default views by selecting a view from the **View** drop-down menu, then dragging and dropping components located on the left side of the window.

Double-clicking on an individual component of any view accesses the related tab of that component. For example, if you double-click on **APs** of the **Infrastructure Overview** component, the **Network** tab is accessed displaying only APs.

See the [Dashboard Components](#) topic for a description of all the available components.

You can hide dashboard components by clicking Hide Dashboard Components bar— .

You can show (un-hide) dashboard components by clicking the Show Dashboard Components bar— .

## Selecting Dashboard Scope

The **Scope** field allows you to narrow or expand the scope of the **Dashboard**. Scopes are defined as the following network levels:

- System—Displays information for your entire network (system).
- ADSP—Displays server information including all the network levels (Country, Region, City, Campus, Building, and Floor) as defined in the **Configuration** tab under **Appliance Platform > Tree Setup**.
- Country—Displays information about a specific country including regions, cities, campuses, buildings, and floors.
- Region—Displays information about a specific region including cities, campuses, buildings, and floors.
- City—Displays information about a specific city including campuses, buildings, and floors.
- Campus—Displays information about a specific campus including buildings and floors.
- Building—Displays information about a specific campus including floors.
- Floor—Displays information about a specific floor.

If you have a Central Management license, you may include information about other servers in your network. When you include other servers in your **Dashboard**, all scope information is included.

## Customizing Dashboard Views

You may customize any of the existing views as well as the empty custom views. The components panel contains all of the components that can be viewed in the **Dashboard**. You may add components to the **Dashboard** by dragging and dropping a component onto the **Dashboard**. To customize the **Dashboard**, follow these instructions:

1. Select a view from the **View** drop-down menu.
2. Click the **Show Dashboard Components** bar to display the components if not already in view.
3. Click on a component while continuing to hold the mouse button down.
4. Drag the component to the **Dashboard** to the location where you want it.

✓ **NOTE** If you keep the component stationed in one spot without releasing the right mouse button, the component will expand to fill in an area. Also, after moving a component to the **Dashboard**, you can drag the mouse to expand the component or reduce the area the component is displayed.

5. Release the mouse button.

✓ **NOTE** If you decide you do not want to keep your changes, click the **Revert** button to return the view to its original state.

6. Click **Save** to save the customized view.

You can change the name of a view by clicking the **Rename** button, typing in the new name, and then clicking **OK**.

The **Dashboard** is displayed in a 2-by-2 defined area or a 3-by-3 defined area. To switch the defined display area, click the **2x2** or **3x3** button.

## 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.
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.

Component	Description
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 Overview	Displays a list of infrastructure devices in three columns (Online compliant, Online non-compliant, and Offline).
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.
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.

Component	Description
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.
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.

Component	Description
System Load	Displays a column chart reflecting system load. Charts include percentages for: <ul style="list-style-type: none"> <li>• Sensor count</li> <li>• Managed network devices</li> <li>• Total device load</li> <li>• Active device load.</li> </ul>
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 infrastructure 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.
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 list of devices seen in your wireless network, depending on the type of device selected in the **Show** menu.


Also displayed is a total device count. You can narrow the scope by selecting an ADSP appliance, country, region, city, campus, building, or floor from the network tree or from the for menu. You can also filter device information using the Network Filters.

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
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-C7E038	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
Cisco1131a-CC.qasind	172.17.25.22	Safe	Thu Apr 12 2012 03:45:35 PM	The Falls 1125	AirDefense 1	AIR-AP...	12.4(21a)1A1	uptime 1		audited Thu
rfs4000-22D91C	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
Cisco1131b-CC.qasind	172.17.25.24	Safe	Thu Apr 12 2012 03:45:35 PM	The Falls 1125	AirDefense 1	AIR-AP...	12.4(21a)1A1	uptime 1		audited Thu

The information displayed depends on the type of device selected. You can sort device information according to information in a column by clicking the column header.

In a large list of devices, you can use the **Search** field to find a device or group of similar devices. Entering a string will reduce the list of devices to the ones that has information matching the string. Entering a device name will display the device matching the typed name.



You can hide (uncheck) or view (check) columns by clicking the drop-down button—  located in the last column. The menu changes according to the selected device in the **Show** drop-down menu.

Network Device	BSS	Wireless Client	Unknown Devices
<ul style="list-style-type: none"> <li>✓ Flag</li> <li>✓ Device                             <ul style="list-style-type: none"> <li>Name</li> <li>MAC</li> </ul> </li> <li>✓ IP</li> <li>✓ Severity                             <ul style="list-style-type: none"> <li>First Seen</li> </ul> </li> <li>✓ Last Seen</li> <li>✓ Scope</li> <li>✓ Floor                             <ul style="list-style-type: none"> <li>Manufacturer</li> </ul> </li> <li>✓ Model</li> <li>✓ Firmware</li> <li>✓ Status</li> <li>✓ Sensor Status</li> <li>✓ Compliant                             <ul style="list-style-type: none"> <li>Device Actions</li> <li>Associated Clients</li> <li>Adopted APs</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ Flag</li> <li>✓ Device                             <ul style="list-style-type: none"> <li>Name</li> <li>MAC</li> <li>IP</li> </ul> </li> <li>✓ Severity                             <ul style="list-style-type: none"> <li>First Seen</li> </ul> </li> <li>✓ Last Seen</li> <li>✓ Scope</li> <li>✓ Floor                             <ul style="list-style-type: none"> <li>Channel</li> </ul> </li> <li>✓ Signal Strength</li> <li>✓ SSID                             <ul style="list-style-type: none"> <li>Manufacturer</li> <li>Classification</li> <li>Sensed Authentication</li> <li>Sensed Encryption</li> <li>Protocols</li> </ul> </li> <li>✓ Rogue                             <ul style="list-style-type: none"> <li>Device Actions</li> <li>Sensor</li> </ul> </li> <li>✓ AP                             <ul style="list-style-type: none"> <li>Associated Clients</li> <li>Security Policy</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ Flag</li> <li>✓ Device                             <ul style="list-style-type: none"> <li>Name</li> <li>MAC</li> <li>IP</li> </ul> </li> <li>✓ Severity                             <ul style="list-style-type: none"> <li>First Seen</li> </ul> </li> <li>✓ Last Seen</li> <li>✓ Scope</li> <li>✓ Floor                             <ul style="list-style-type: none"> <li>Manufacturer</li> <li>On Network</li> <li>Classification</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ Flag</li> <li>✓ Device                             <ul style="list-style-type: none"> <li>Name</li> <li>MAC</li> <li>IP</li> </ul> </li> <li>✓ Severity                             <ul style="list-style-type: none"> <li>First Seen</li> </ul> </li> <li>✓ Last Seen</li> <li>✓ Scope</li> <li>✓ Floor                             <ul style="list-style-type: none"> <li>Manufacturer</li> <li>On Network</li> <li>Classification</li> </ul> </li> </ul>

You can hide the Network Filters by clicking **Hide Network Filters** bar—  . You can show (un-hide) the Network Filters by clicking the **Show Network Filters** bar—  s.

## Show Menu

The **Show** menu is used to select the devices that you want displayed in the **Network** tab. You can choose to display the **Network** tab in a tabular or graphical view as follows:

In the tabular view, the following items are displayed in the **Show** menu:

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

In the graphical view, the following items are displayed in the Show menu:

- Association Tree
- Network Graph.

You can select the different views by selecting the appropriate view button.



The first button selects the tabular view. The second button selects the graphical view. The last button is the **Advanced Search** button which is explained later.

## Network Device

Selecting **Network Device** from the **Show** drop-down menu displays a list of Access Points, Sensors, Wireless Switches, and Wired Switches seen in your network.

Grouping	Device	IP	Severity	Last Seen	Scope	Floor	Model	Firmware	Status	Sense...	Co...
No grouping	10.59.36.46	10.59.36.46	Safe(0)	Fri Nov 11 ...	The Falls		Air(M510	5.3.0.4	Online	Online	N/A
	10.59.36.37	10.59.36.37	Safe(0)	Fri Nov 11 ...	The Falls		Air(M520	5.3.0.4	Online	Online	N/A
	AP-00-A0-F8-EC-14-31		Safe(0)	Fri Nov 11 ...	The Falls		Air(AP300	01.00-2290r	Online	Online	N/A
	ap650-313E64	10.59.36.39	Safe(0)	Fri Nov 11 ...	The Falls		Air(AP650	5.2.1.3	Online	Online	N/A
	ap7131-14C28C	10.59.36.32	Severe(95)	Fri Nov 11 ...	The Falls		Air(AP7131	5.2.0.0-069R	uptime 00d, 2	Online	aud
	ap7131-C7E038	172.17.25.21	Severe(95)	Fri Nov 11 ...	The Falls		Air(AP7131	5.2.0.0-069R	uptime 01d, 2	Online	aud
	Cisco1131a-CC.qairdefense.co	172.17.25.22	Safe(0)	Fri Nov 11 ...	The Falls		Air(AIR-AP1131A...	12.4(21a)JA1	uptime 04d, 0	Online	aud
	Cisco1131b-CC.qairdefense.co	172.17.25.24	Safe(0)	Fri Nov 11 ...	The Falls		Air(AIR-AP1131A...	12.4(21a)JA1	uptime 04d, 0	Online	aud
	RFS4000-CColler	172.17.25.23	Safe(0)	Fri Nov 11 ...	The Falls		Air(RFS4000	4.2.1.0-005R	uptime 109d,	Online	aud

The list of Network Devices are displayed in a tabular format using a combination of the following columns:

Column	Description
Flag	Indicates if a Network Device has been flagged (blue flag—). (default header)
Device	Displays the Network Device's icon along with the its name. (default header)
Name	Displays the name of the Network Device.
MAC	Displays the Network Device's MAC address.
IP	Displays the Network Device's IP address. (default header)
Severity	Displays the Network Device's threat level to your network. (default header)

Column	Description
First Seen	Displays the date and time the Network Device was first seen in your network.
Last Seen	Displays the date and time the Network Device was last seen in your network.
Scope	Displays where the Network Device is located within the network scope. (default header)
Floor	Displays the floor that the Network Device is located on. (default header)
Manufacturer	Displays the manufacturer of the Network Device.
Model	Displays the Network Device's model number. (default header)
Firmware	Displays the Network Device's installed firmware number. (default header)
Status	Displays the Network Device's status (online or offline). (default header)
Sensor Status	Displays the Sensor status (online or offline). (default header)
Compliant	Indicates if the Network Device is in compliance with defined ADSP policies. (default header)
Last Configuration	Displays the date and time of the last configuration that took place with the Network Device.
Associated Clients	Displays the number of clients that have associated with the Network Device.
Adopted APs	Displays the number of APs that the Network Device has adopted.






## BSS

Selecting **BSS** from the **Show** drop-down menu displays a list of BSSs seen in your wireless network.

Device	Sev.	Last Seen	Scope	Floor	Cha...	Signal Stre...	SSID	Rogue	AP
Trendnet:4c:39:44	0	Ma, Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	11(...	-69 dbm	StarTrek	--	
Trapezef Networks:21:14	0	Ma, Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	48(...	-65 dbm	Larry_Nort...	--	
Trapezef Networks:21:14	0	Ma, Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	62(...	-65 dbm	Larry_Nort...	--	
Symbol:ea:f5:02	0	Ma, Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	157...	-51 dbm	DevMgmt...	--	
Symbol:ea:f5:01	0	Ma, Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	157...	-51 dbm	DevMgmt...	--	
Symbol:ea:f5:00	0	Ma, Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	157...	-51 dbm	DevMgmt...	--	
Symbol:ea:c2:e3	0	Sal Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	161...	-86 dbm	AP300APT...	--	
Symbol:ea:c2:e2	0	Sal Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	161...	-77 dbm	AP300APT...	--	
Symbol:ea:c2:e1	0	Sal Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	161...	-85 dbm	AP300APT...	--	
Symbol:ea:c2:e0	0	Sal Mon Nov 14 2011 0...	The Falls 1125	AirDefense 2	161...	-77 dbm	Symbol5100	--	

The list of BSSs are displayed in a tabular format using a combination of the following columns:

Column	Description
Flag	Indicates if a BSS has been flagged (blue flag—). (default header)
Device	Displays the BSS icon along with the vendors ID. (default header)
Name	Displays the name of the BSS.
MAC	Displays the BSS's MAC address.
IP	Displays the BSS's IP address.
Severity	Displays the BSS threat level to your network. (default header)

Column	Description
First Seen	Displays the first time the BSS was seen on the network.
Last Seen	Displays the last time the BSS was seen on the network. (default header)
Scope	Displays where the Access Point is located within the network scope. (default header)
Floor	Displays the floor the BSS is on. (default header)
Channel	Displays the communications channel the BSS is using. (default header)
Signal Strength	Displays the signal strength of the BSS. (default header)
SSID	Displays 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 Wireless Client tries to connect to the BSS. (default header)
Manufacturer	Displays the manufacturer of the device.
Classification	Displays how BSSs are classified.
Sensed Authentication	Displays the sensed method of authentication.
Sensed Encryption	Displays the sensed method of encryption.
Protocols	Displays the protocols being utilized by the BSS.
Rogue	Indicates if a BSS is a rogue (true or false). (default header)
Device Actions	<p>Indicates a current live state.</p> <ul style="list-style-type: none"> <li>• AP Test—</li> <li>• Wireless Vulnerability Assessment—</li> <li>• Termination—</li> <li>• Dedicate Spectrum Analysis —</li> <li>• Inline Spectrum Analysis—</li> </ul>
Sensor	Displays the name of the Sensor that sees the BSS.
AP	Displays the name of the Access Point. (default header)
Associated Clients	Displays the number of clients that have associated with the BSS.

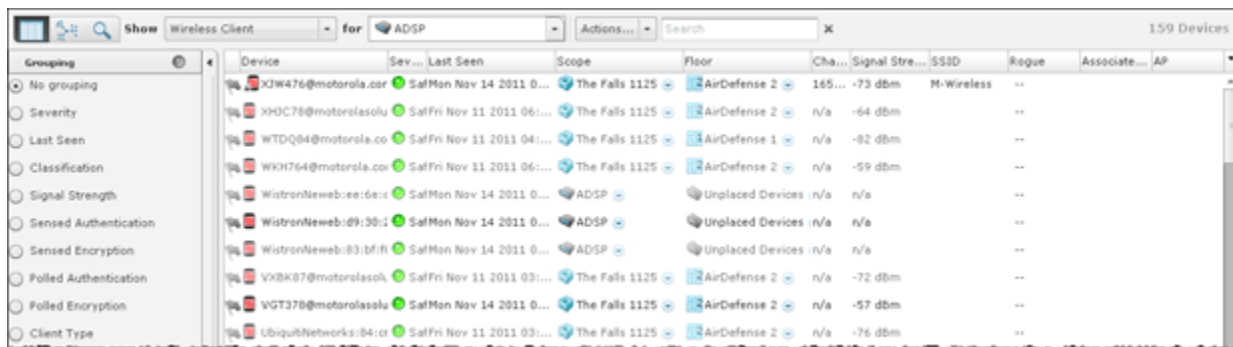
### ***Meru Network Support***

✓ **NOTE** Live View is not supported on Meru Networks.


Meru Networks only display virtual MAC addresses in the **Network** tab. To display the true MAC addresses, contact Customer Support and have them enable Meru Network support on your appliance. When enabled, the true MAC addresses are displayed in the **Network** tab.






## Wireless Client

Selecting **Wireless Client** from the **Show** drop-down menu displays a list of Wireless Clients seen in your wireless network.



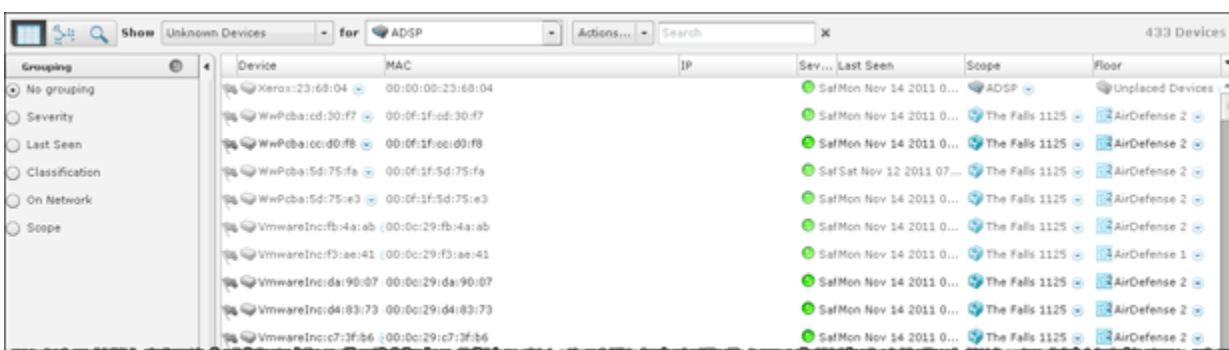
The list of Wireless Clients are displayed in a tabular format using a combination of the following columns:

Column	Description
Flag	Indicates if a Wireless Client has been flagged (blue flag—  ). (default header)
Device	Displays the Wireless Client icon along with the vendors ID. (default header)
Name	Displays the name of the Wireless Client.
MAC	Displays the Wireless Client's MAC address.
IP	Displays the Wireless Client's IP address.
Severity	Displays the Wireless Client threat level to your network. (default header)
First Seen	Displays the first time the Wireless Client was seen on the network.
Last Seen	Displays the last time the Wireless Client was seen on the network. (default header)
Scope	Displays where the Wireless Client is located within the network scope. (default header)
Floor	Displays the floor the Wireless Client is on.
Channel	Displays the communications channel the Wireless Client is using. (default header)
Signal Strength	Displays the signal strength of the Wireless Client. (default header)
SSID	Displays 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 Wireless Client tries to connect to the Wireless Client. (default header)
Client Type	Displays the client type of the Wireless Client.
802.1x Name	Displays the 802.1x name of the Wireless Client.
Manufacturer	Displays the manufacturer of the device.
Classification	Displays how the Wireless Client is classified.
Sensed Authentication	Displays the sensed method of authentication.
Sensed Encryption	Displays the sensed method of encryption.

Column	Description
Polled Authentication	Displays the polled method of authentication.
Polled Encryption	Displays the polled method of encryption.
Protocols	Displays the protocols being utilized by the Wireless Client.
Rogue	Indicates if a Wireless Client is a rogue (true or false). (default header)
Device Actions	Indicates if any of the following actions have occurred: <ul style="list-style-type: none"> <li>AP Test—</li> <li>Wireless Vulnerability Assessment—</li> <li>Termination—</li> <li>Dedicate Spectrum Analysis —</li> <li>Inline Spectrum Analysis—</li> </ul>
Associated BSS	Displays the BSS that the Wireless Client has associated with.
AP	Displays the name of the Access Point. (default header)
Sensor	Displays the name of the Sensor that sees the Wireless Client.


## Unknown Devices

Selecting **Unknown Devices** from the **Show** drop-down menu displays a list of Unknown Devices seen in your network. Unknown devices are defined from the source or destination address detected in communication to or from a wireless device. ADSP can identify the wireless device the frame is sent from or received by, but if the MAC address listed as the ultimate source or destination is not a device identified by ADSP, it is considered 'unknown'. These are almost always infrastructure devices on the wired network.



Device	MAC	IP	Sev...	Last Seen	Scope	Floor
Xerox:23:68:04	00:00:00:23:68:04		SafMon	Nov 14 2011 0...	ADSP	Unplaced Devices
WwPcba:cd:30:f7	00:0f:1f:0d:30:f7		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 2
WwPcba:cc:d0:f8	00:0f:1f:0c:d0:f8		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 2
WwPcba:5d:75:fa	00:0f:1f:5d:75:fa		SafSat	Nov 12 2011 07...	The Falls 1125	AirDefense 2
WwPcba:5d:75:e3	00:0f:1f:5d:75:e3		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 2
VmwareIncrfb:4a:ab	00:0c:29:fb:4a:ab		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 2
VmwareIncrf3:ae:41	00:0c:29:f3:ae:41		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 1
VmwareIncrda:90:07	00:0c:29:da:90:07		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 2
VmwareIncrd4:83:73	00:0c:29:d4:83:73		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 2
VmwareIncr7:3f:b6	00:0c:29:c7:3f:b6		SafMon	Nov 14 2011 0...	The Falls 1125	AirDefense 2

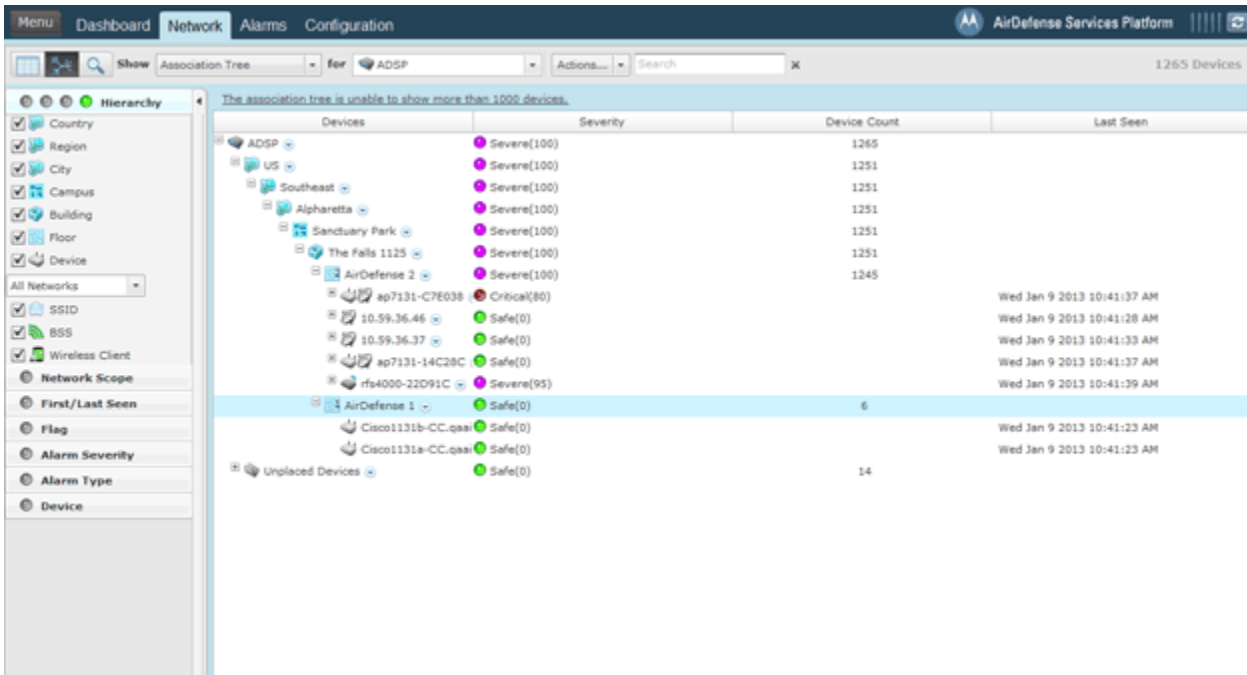
The list of Unknown Devices are displayed in a tabular format using a combination of the following columns:

Column	Description
Flag	Indicates if a Unknown Device has been flagged (blue flag—  ). (default header)
Device	Displays the Unknown Device icon along with the switch name. (default header)
Name	Displays the name of the Unknown Device.
MAC	Displays the Unknown Device's MAC address. (default header)

Column	Description
IP	Displays the Unknown Device's IP address. (default header)
Severity	Displays the Unknown Device threat level to your network. (default header)
First Seen	Displays the first time the Unknown Device was seen on the network.
Last Seen	Displays the last time the Unknown Device was seen on the network. (default header)
Scope	Displays where the Unknown Device is located within the network scope. (default header)
Floor	Displays the floor the Unknown Device is on. (default header)
Manufacturer	Displays the manufacturer of the device.
On Network	<p>Identifies how ADSP obtained the MAC address of a non-wireless device. The different entries are:</p> <ul style="list-style-type: none"> <li>• Sensor Segment—The frame containing MAC address was detected by a sensor on it's wired port. This device is therefore known to be on a LAN segment containing the sensor and is therefore on the same wired infrastructure.</li> <li>• Switch—This MAC address was obtained from a data poll of the tables of a wireless switch. At some time, a know wireless device communicated with this unknown device. The unknown device is on the infrastructure somewhere, but the LAN segment is unknown.</li> <li>• Blank—This MAC address was detected by a sensor radio and the wireless device communicating with this MAC is not sanctioned in ADSP. This is most likely a device on a neighboring network and not part ofthe ADSP protected infrastructure.</li> <li>• Sanctioned BSS—This MAC address has been seen by a sensor in communication with a Sanctioned BSS and is likely to be a device on the ADSP protected infrastructure, but has not been reported to ADSP as being on the wired network by poll or discovery.</li> </ul>
Classification	Displays how the Unknown Device is classified.



## Association Tree

The Association Tree displays your network from the top down starting at the appliance going all the way down to the associated Wireless Clients. Clicking the **Network Graph** icon— gives you access to the Association Tree via the **Show** drop-down menu. Select **Association Tree** from the menu to display the association tree for your network.



The screenshot shows the AirDefense Services Platform interface. The top navigation bar includes Menu, Dashboard, Network, Alarms, and Configuration. The main content area is titled 'Association Tree' and shows a hierarchical tree view of the network. The tree starts with 'ADSP' and branches down through 'US', 'Southeast', 'Alpharetta', 'Sanctuary Park', 'The Falls 1125', and 'AirDefense 2'. Below the tree is a table with the following columns: Devices, Severity, Device Count, and Last Seen. The table contains the following data:

Devices	Severity	Device Count	Last Seen
ADSP	Severe(100)	1265	
US	Severe(100)	1251	
Southeast	Severe(100)	1251	
Alpharetta	Severe(100)	1251	
Sanctuary Park	Severe(100)	1251	
The Falls 1125	Severe(100)	1251	
AirDefense 2	Severe(100)	1245	
ap7131-C7E038	Critical(80)		Wed Jan 9 2013 10:41:37 AM
10.59.36.46	Safe(0)		Wed Jan 9 2013 10:41:28 AM
10.59.36.37	Safe(0)		Wed Jan 9 2013 10:41:33 AM
ap7131-14C28C	Safe(0)		Wed Jan 9 2013 10:41:37 AM
rfs4000-22D91C	Severe(95)		Wed Jan 9 2013 10:41:39 AM
AirDefense 1	Safe(0)	6	
Cisco1131b-CC.qas	Safe(0)		Wed Jan 9 2013 10:41:23 AM
Cisco1131a-CC.qas	Safe(0)		Wed Jan 9 2013 10:41:23 AM
Unplaced Devices	Safe(0)	14	


Click the Expand— button to open a branch of the tree. Click the Collapse— button to close a branch of the tree.

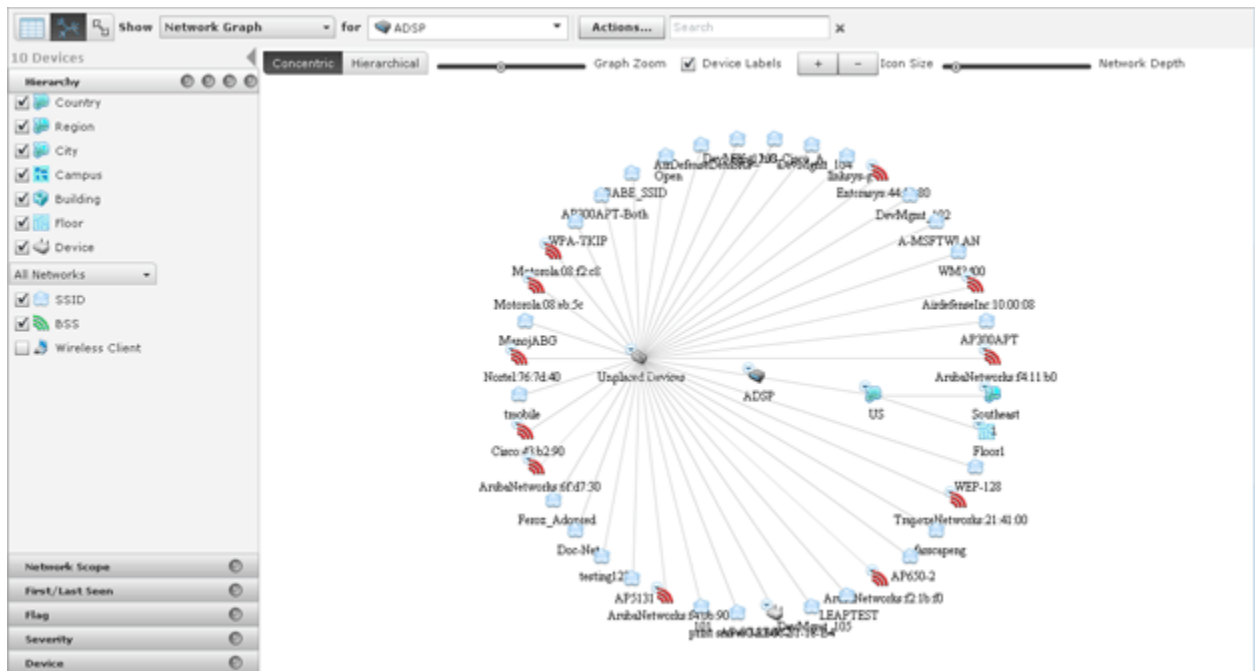
The table columns for the Association Tree are:

Column	Description
Devices	Displays the name of the devices on your network.
Severity	Displays the threat level to your network for a floor and all the devices on that floor.
Device Count	Displays the number of devices on a tree level.
Last Seen	Displays the last time a device was seen on the network.

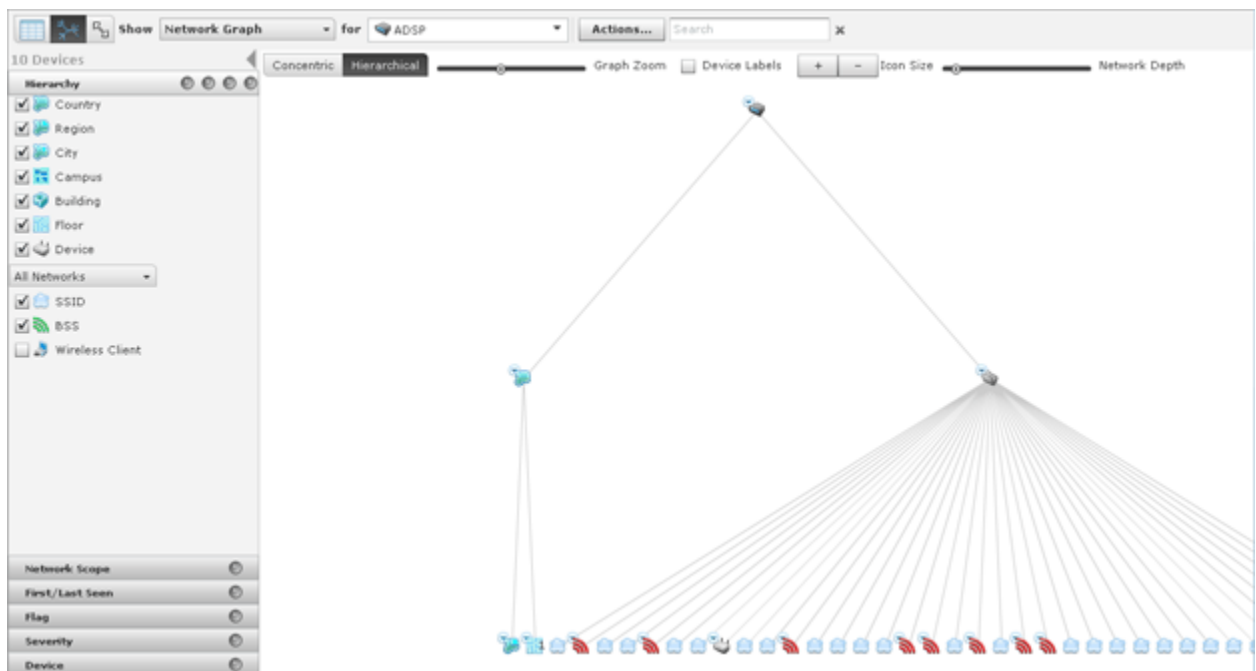


## Network Graph

The Network Graph displays your network in a graphical view. Clicking the **Network Graph** icon— gives you access to the Network Graph via the **Show** drop-down menu and displays a Network Graph of managed devices seen in your network. There is a Concentric view (default) and a Hierarchical view.



To switch to the Hierarchical view, click the **Hierarchical** button.

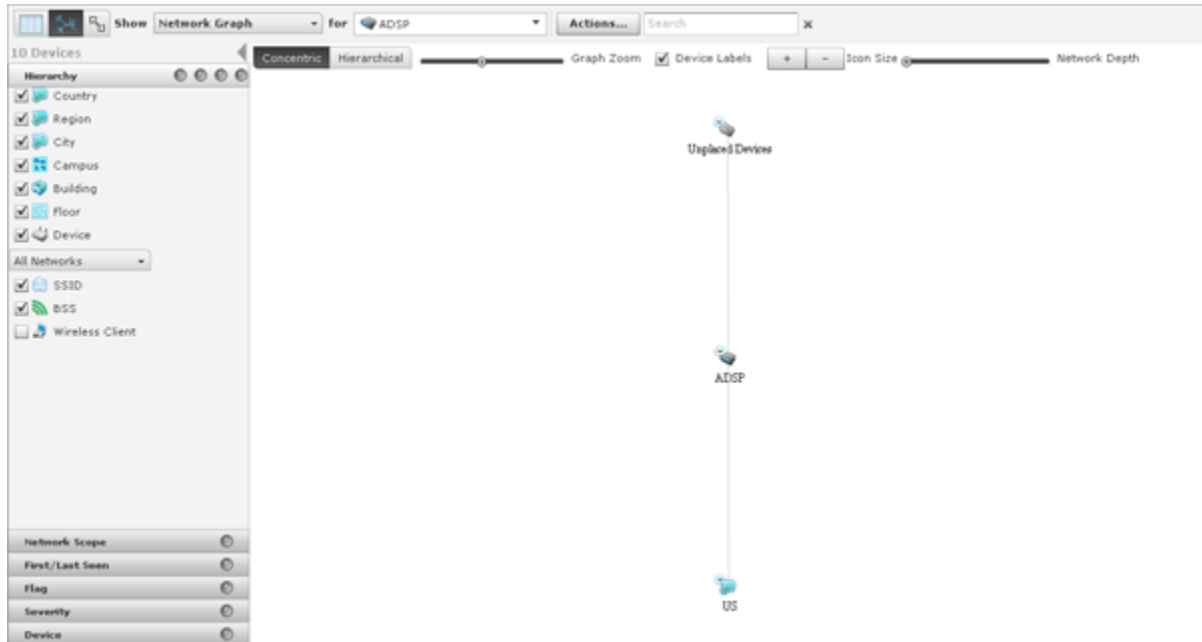


Click the **Concentric** button to return to the Concentric view.

You can manipulate the graph by using:










- Graph Zoom to zoom the graph in and out.

- Device Labels to remove or display the device labels.
- Icon Size to increase or decrease the size of the icons.
- Network Depth to see more devices or less devices in your network.



## Network Filters

Network filters are provided to filter the displayed network information. They are displayed on the left side of the **Network** tab.


<b>Grouping</b>	
<input checked="" type="radio"/> No grouping	
<input type="radio"/> Severity	
<input type="radio"/> Last Seen	
<input type="radio"/> Status	
<input type="radio"/> Scope	
<b>Network Scope</b>	
<b>First/Last Seen</b>	
<b>Flag</b>	
<b>Alarm Severity</b>	
<b>Alarm Type</b>	
<b>Device</b>	
<b>Compliance</b>	
<b>Status</b>	

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 were 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.

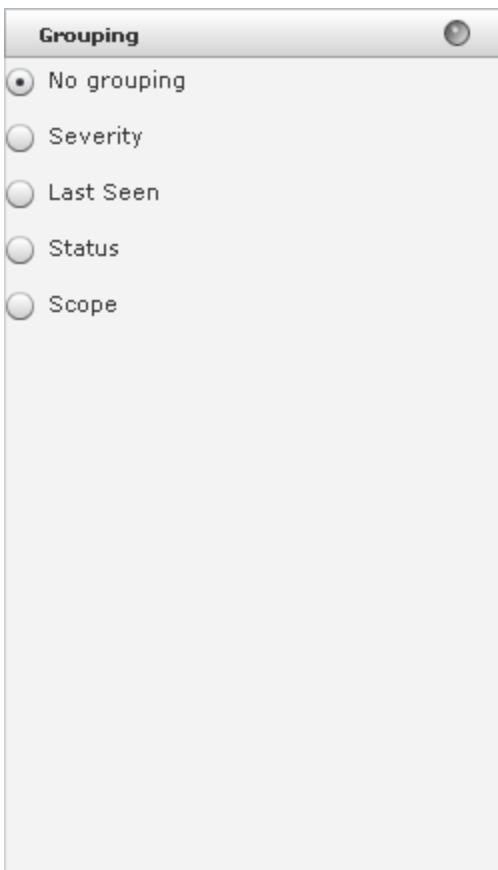
- Classification Filter—filter devices by their classification.
- On Network Filter—display devices that are on your network and/or devices that have been seen by a sensor but not confirmed to be on your network.
- Device Filter—filter devices by model, manufacturer, and/or capabilities.
- Compliance 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.

The filters are initially set to display the maximum amount of devices. You can adjust any filter or combination of filters to fine tune the display of devices. This allows you to display only the devices that you want to view.

The indicator on the right of each filter turns green— when you change a filter from its original state. Click the green indicator to return a filter to its default state.

### Grouping Filter

The **Grouping** filter allows you to view devices by grouping them using similar criteria. The views vary depending on the type of devices being displayed.

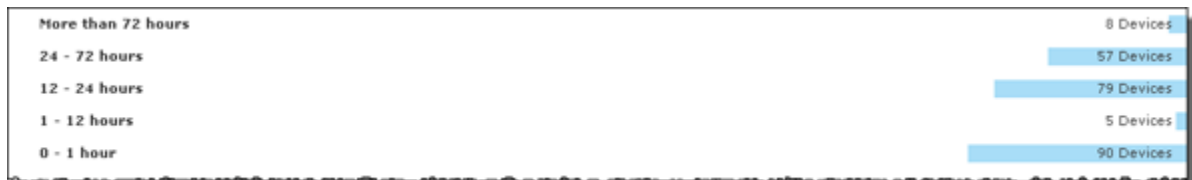


The following views are available:

- No Grouping—Displays all devices without grouping. This view is accessible when displaying any type of device.
- Severity—Groups devices into the different threat levels to your network. Threat levels that are not sensed are not shown. This view is accessible when displaying any type of device.



- Last Seen—Groups devices by a time frame when the devices were last seen on your network. This view is accessible when displaying any type of device.



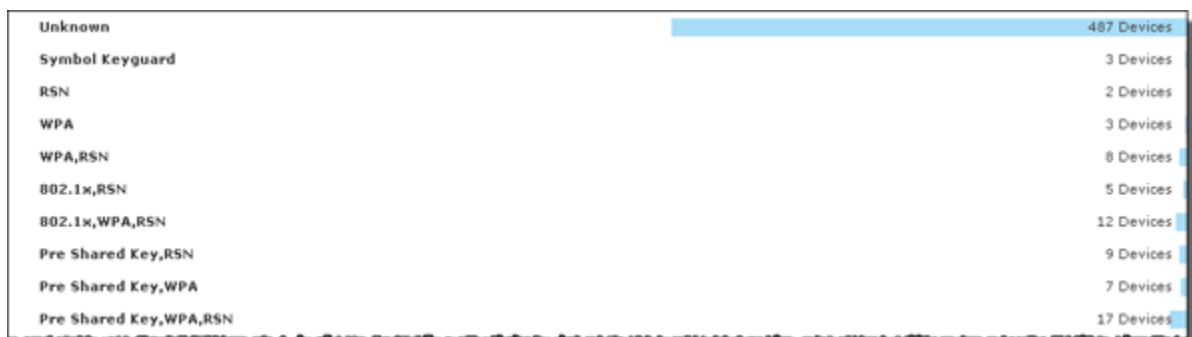
- Classification—Groups devices by how they are classified. This view is accessible when displaying BSSs, Wireless Clients, or Unknown Devices.



- Signal Strength—Groups devices in a range of signal strengths. This view is accessible when displaying BSSs or Wireless Clients.



- Sensed Authentication—Groups devices based on their sensed method of authentication. This view is accessible when displaying BSSs or Wireless Clients.



- Sensed Encryption—Groups devices based on their sensed method of encryption. This view is accessible when displaying BSSs or Wireless Clients.



- Polled Authentication—Groups devices based on their polled method of authentication. This view is accessible only when displaying Wireless Clients.



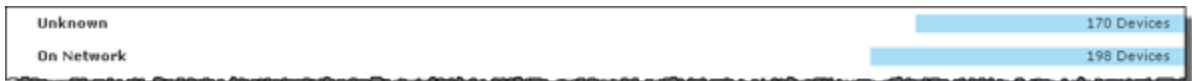
- Polled Encryption—Groups devices based on their polled method of encryption. This view is accessible only when displaying Wireless Clients.



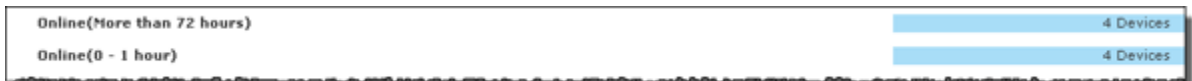
- Client Type—Groups devices based on their client type. This view is accessible only when displaying Wireless Clients.



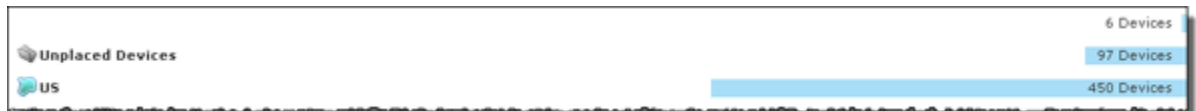
- On Network—Groups devices based whether they are on the network or not. This view is accessible only when displaying Unknown Devices.



- Status—Groups devices based on their online/offline status. This view is accessible when displaying Network Devices.



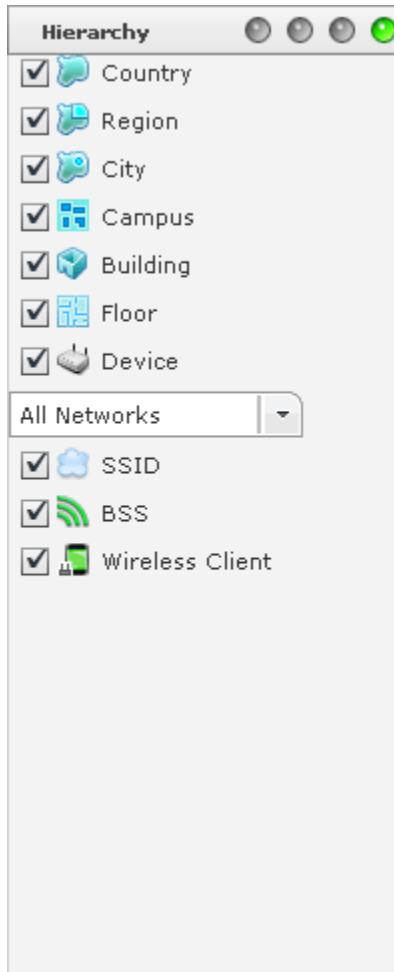
- Scope—Groups devices based on where they are in the network. The highest network level under the appliance level is displayed as the group. This view is accessible when displaying any type of device.



Clicking on a group will display the devices in that group.

## Hierarchy Filter

The **Hierarchy** filter is used in the Network Graph and the Association Tree to control the level of detail seen. One or more levels in the hierarchy can be removed from view so that they will not be seen in the Network Graph or Association Tree.



Check a checkbox to display hierarchy level. Uncheck a checkbox to remove a level from view. The following hierarchy levels may be displayed or removed from view:

- Country
- Region
- City
- Campus
- Building
- Floor
- Device (includes APs, Sensors and Switches)
- SSID
- BSS
- Wireless Client.

You also have the ability to display via a drop-down menu:

- All networks (provided and sensed)
- Only provided networks
- Only sensed networks.

### Network Scope Filter

The **Network Scope** filter is used to view devices according to where they are in the network tree. By selecting a network level, you limit the displayed devices to only the ones under that particular network level.





## First/Last Seen Filter

The **First/Last Seen** filter allows you to filter devices according to when they were first seen and/or last seen on your network.

**First/Last Seen** ⊙

**Last seen within prior**

- 0 - 5 minutes
- 5 - 10 minutes
- 10 - 20 minutes
- 20 - 30 minutes
- 30 - 60 minutes
- 1 - 12 hours
- 12 - 24 hours
- 24 - 72 hours
- More than 72 hours

**First seen within prior**

- Last Hour
- 1 - 12 hours
- 12 - 24 hours
- 24 - 72 hours
- More than 72 hours

The last seen times may be:

- Any time period
- 0 - 5 minutes
- 5 - 10 minutes
- 10 - 20 minutes
- 20 - 30 minutes
- 30 - 60 minutes
- 1 - 12 hours
- 12 - 24 hours
- 24 - 72 hours
- More than 72 hours.

The first seen times may be:

Any time period

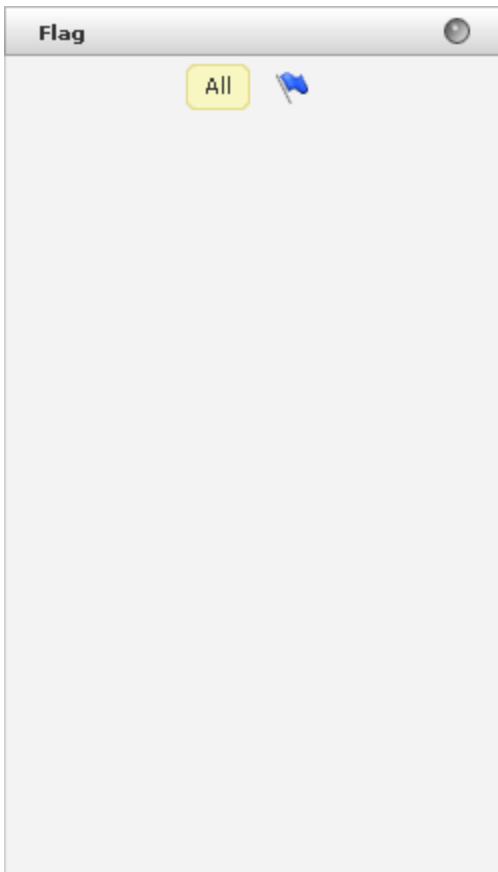
- 1 - 12 hours

- 12 - 24 hours
- 24 - 72 hours
- More than 72 hours.

For example, if **30 - 60** minutes is selected as the last seen time and no other times are selected (first/last seen), only devices that were last seen within 30 to 60 minutes are displayed.

### Flag Filter

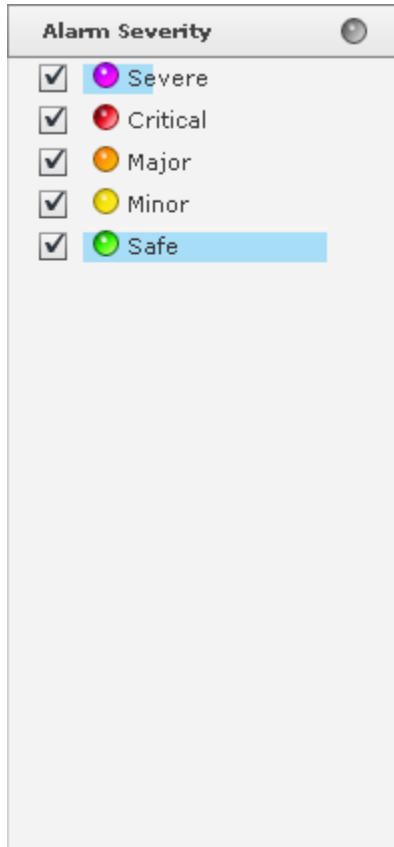
The **Flag** filter gives you the option of viewing all devices or only flagged devices.








To select an option, click **All** or the blue flag—.

## Alarm Severity Filter

The **Alarm Severity** filter allows you to view devices by alarm severity. Devices are grouped together according to their alarm threat to your network.



The severities are:

- Severe——Displays only Severe alarms.
- Critical——Displays Critical and Severe alarms.
- Major——Displays Major, Critical, and Severe alarms.
- Minor——Displays Major, Critical, and Severe alarms.
- Safe——Displays alarms of all criticalities.

You can select the alarms that you want to view by checking the checkbox.

### Alarm Type Filter

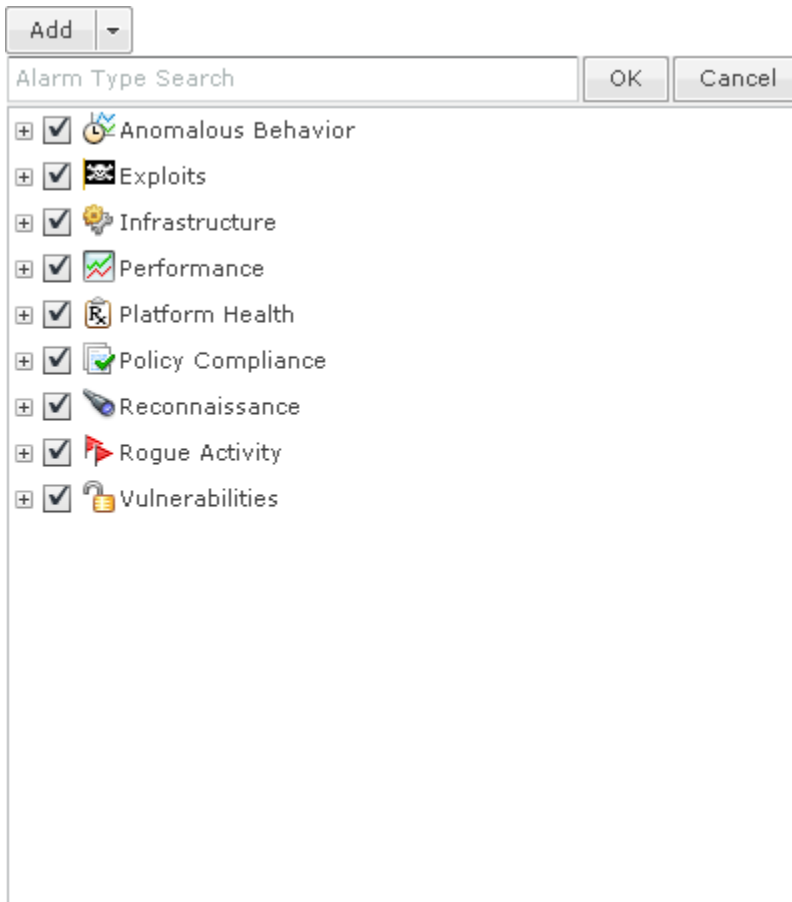
The **Alarm Type** filter allows you to view devices by alarm type. Devices are grouped together according to their alarm threat to your network.



You also have the option of displaying all alarm types or you may filter alarms by a specific type. The different alarm types are:

- Anomalous Behavior
- Exploits
- Infrastructure
- Performance
- Platform Health
- Policy Compliance
- Reconnaissance
- Rogue Activity
- Vulnerabilities.

The **Add** button is used to select the alarm types that you want to display.



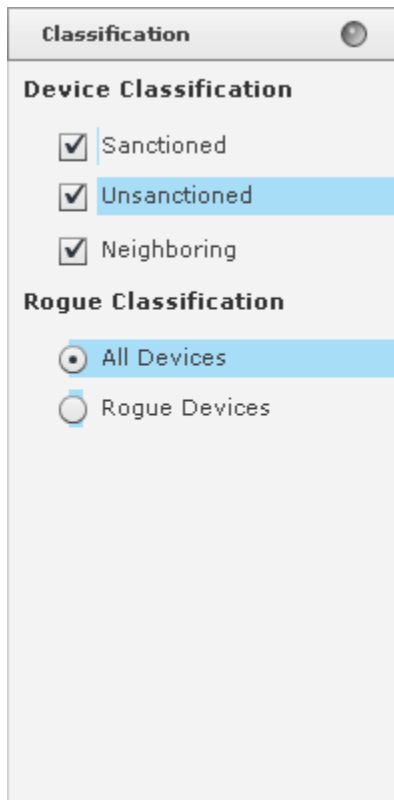
Click the **Add** button, select the alarm type(s), and then click **OK**. The following screen shots shows that you only want to display rogue alarms.



To remove an alarm type, select (highlight) the alarm type and click the **Remove** button.

## Classification Filter

The **Classification** filter is used to filter devices by their device classification.



**Classification**

**Device Classification**

- Sanctioned
- Unsanctioned
- Neighboring

**Rogue Classification**

- All Devices
- Rogue Devices

✓ **NOTE** This filter is not available when displaying Network Devices

Devices are displayed by the following classifications:

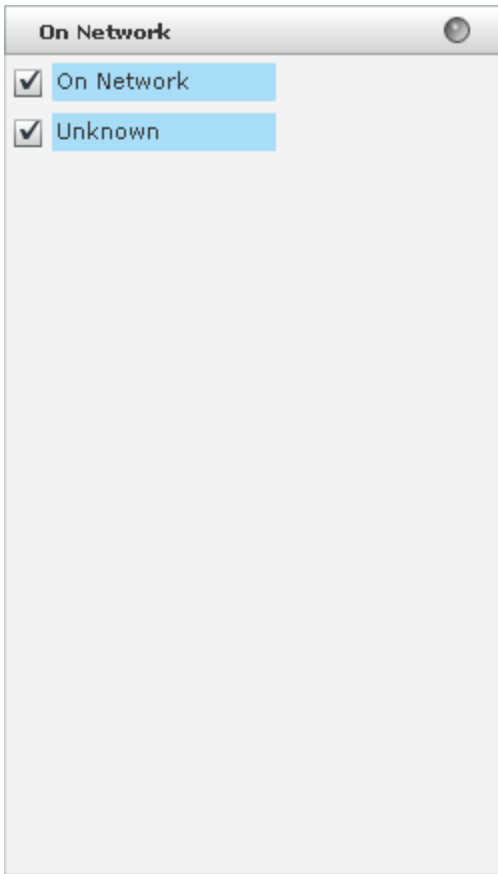
- Sanctioned—Display sanctioned devices.
- Unsanctioned—Display unsanctioned devices.
- Neighboring—Display neighboring devices.

Select the checkbox(es) for the classification(s) that you want to display.

You can also display devices by rogue classification. You options are display all devices or display rogue devices. Select the appropriate radio button.

### On Network Filter

The **On Network** filter is used to 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. This filter is only available when displaying Unknown Devices.



Check the checkbox to display either or both conditions.



## Device Filter

The **Device** filter is used to filter devices by model, manufacturer, and/or capabilities.

The screenshot shows a dialog box titled "Device". It has a close button in the top right corner. Below the title bar, there are two sections:

- Model:** A dropdown menu with "Any" selected.
- Capabilities:** A list of five items, each with a checked checkbox:
  - Access Point
  - Wireless Switch
  - Sensor
  - Wired Switch
  - Network Manager

The filters change depending on the type of devices being displayed.

- **Model**—Filters Network Devices based on the model selected from the Model drop-down menu.
- **Manufacturer**—Filters BSSs, Wireless Clients, or Unknown Devices based on the manufacturer selected from the Manufacturer drop-down menu. You may also type in the manufacturer's name, including a partial name.
- **Capabilities**—Filters Network Devices or Wireless Clients based on the capability of the device. When you select a capability, only devices with that capability are displayed. For Network Devices, you may select:
  - Access Point
  - Wireless Switch
  - Sensor
  - Wired Switch
  - Network Manager.

For Wireless Clients, you may select:

- Default Type
- MCD
- VoIP Phone
- Laptop
- Employee Laptop

- Employee Phone
- Employee Device
- High Priority Visitor Device
- Visitor Device
- Low Priority Visitor Device.

**Device**

**Manufacturer**

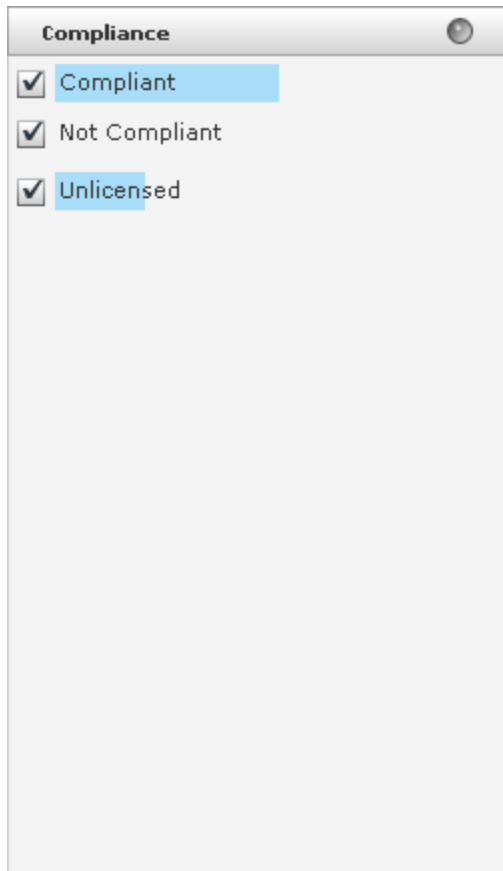
Select from list or enter name  
(partial name is ok)

**Client Type**

- Default Type
- MCD
- VoIP Phone
- Laptop
- Employee Laptop
- Employee Phone
- Employee Device
- High Priority Visitor Device
- Visitor Device
- Low Priority Visitor Device

## Compliance Filter

The **Compliance** filter is used to display devices according to their state of compliance with your network policies. This filter is only available when displaying Network Devices.



Devices are displayed if you have their compliance state checked. The different states are:

- Compliant—Displays devices that are compliant.
- Not Compliant—Displays devices that are not compliant.
- Unlicensed—Displays devices that do not have the required license.

## Status Filter

The **Status** filter is used to display devices according to their uptime/offline status. This filter is only available when displaying Network Devices.

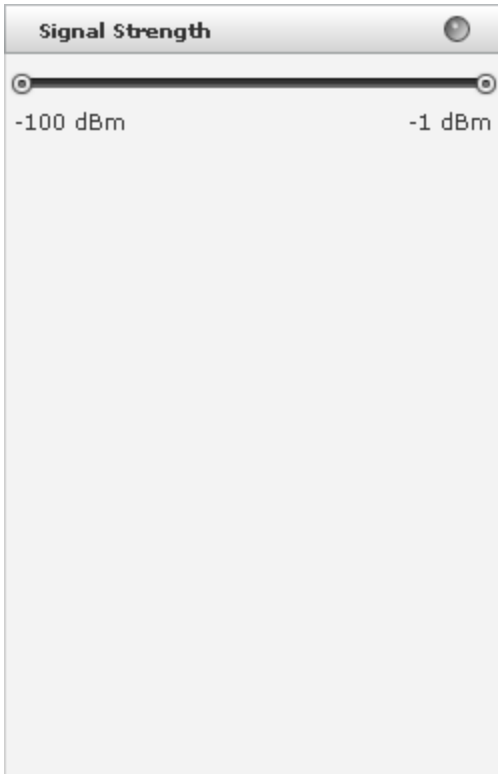
You may select one or more of the following statuses:

- Offline—Displays any offline devices.
- Uptime (0 - 1 hours)—Displays devices that have been online from 0 to 1 hour.
  - ✓ **NOTE** Devices that do not track uptime are shown in this time slot.
- Uptime (1 - 12 hour)—Displays devices that have been online from 1 to 12 hours.
- Uptime (12 - 24 hours)—Displays devices that have been online from 12 to 24 hours.
- Uptime (24 - 72 hours)—Displays devices that have been online from 24 to 72 hours.

- Uptime (More than 72 hours)—Displays devices that have been online longer than 72 hours.

### Signal Strength Filter

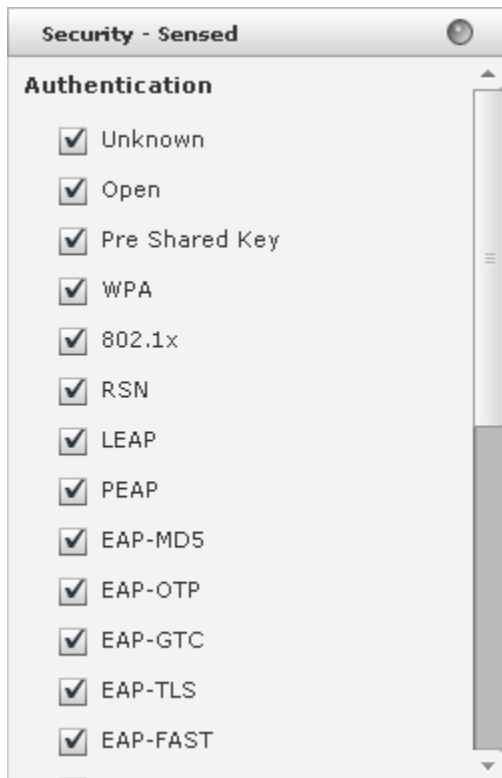
The **Signal Strength** filter is used to filter devices within a specific signal strength range. This filter is only available when displaying BSSs and Wireless Clients.



You may adjust the signal strength range by sliding the adjusters. The maximum range is -100 dBm to -1 dBm. Sliding the left slider adjusts the minimum signal strength. Sliding the right slider adjusts the maximum signal strength.

## Security - Sensed Filter

The **Security - Sensed** filter is used to display devices using a combination of the sensed method of authentication and/or the sensed method of encryption. This filter is only available when displaying BSSs and Wireless Clients.



You may select any combination of authentication methods and/or encryption methods. The available authentication methods are:

- Unknown
- Open
- Pre Share Key
- WPA
- 802.1x
- RSN
- LEAP
- PEAP
- EAP-MD5
- EAP-OTP
- EAP-GTC
- EAP-TLS
- EAP-FAST
- EAP-TTLS

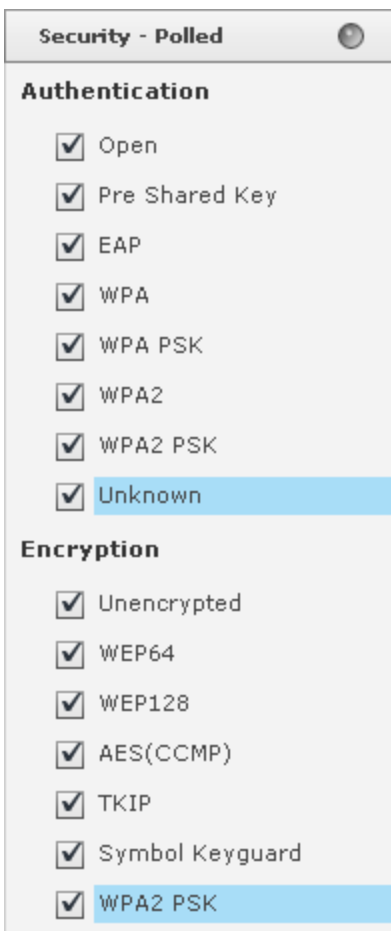
- RSA EAP-SIP
- RAS EAP-PKA
- Network EAP
- Symbol Keyguard
- Other.

The available encryption methods are:

- Unknown
- Unencrypted
- WEP
- TKIP
- AES(CCMP)
- Other Encryption.

### Security - Polled Filter

The **Security - Polled** filter is used to display devices using a combination of the polled method of authentication and/or the polled method of encryption. This filter is only available when displaying Wireless Clients.



The screenshot shows a window titled "Security - Polled" with a close button in the top right corner. The window is divided into two sections: "Authentication" and "Encryption".

**Authentication**

- Open
- Pre Shared Key
- EAP
- WPA
- WPA PSK
- WPA2
- WPA2 PSK
- Unknown

**Encryption**

- Unencrypted
- WEP64
- WEP128
- AES(CCMP)
- TKIP
- Symbol Keyguard
- WPA2 PSK

You may select any combination of authentication methods and/or encryption methods. The available authentication methods are:

- Open
- Pre Share Key
- EAP
- WPA
- WPA PSK
- WPA2
- WPA2 PSK
- Unknown.

The available encryption methods are:

- Unencrypted
- WEP64
- WEP128
- AES(CCMP)
- TKIP
- Symbol Keyguard
- WPA2 PSK.

## Actions

The **Network** tab includes an **Actions** menu where you can execute an action depending on the type of devices you are viewing.

Depending on the device type, the **Actions** button displays one of the following menus:

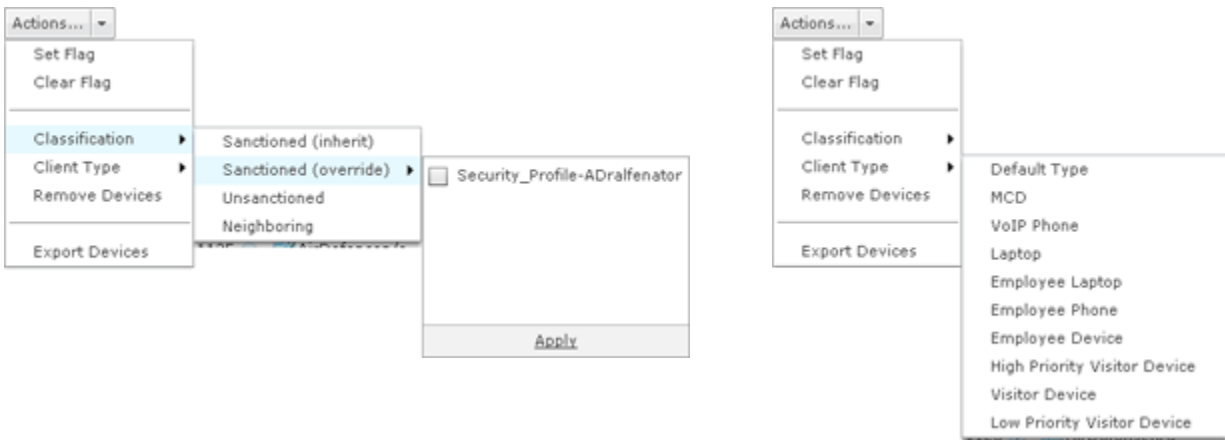
Network Device Actions



### BSS Actions



### Wireless Client Actions



### Unknown Devices Actions



Actions are active (selectable) or inactive (un-selectable) depending on the device type selected in the Show menu. Some actions are executed when you select a device and then select an action. In this case, no other



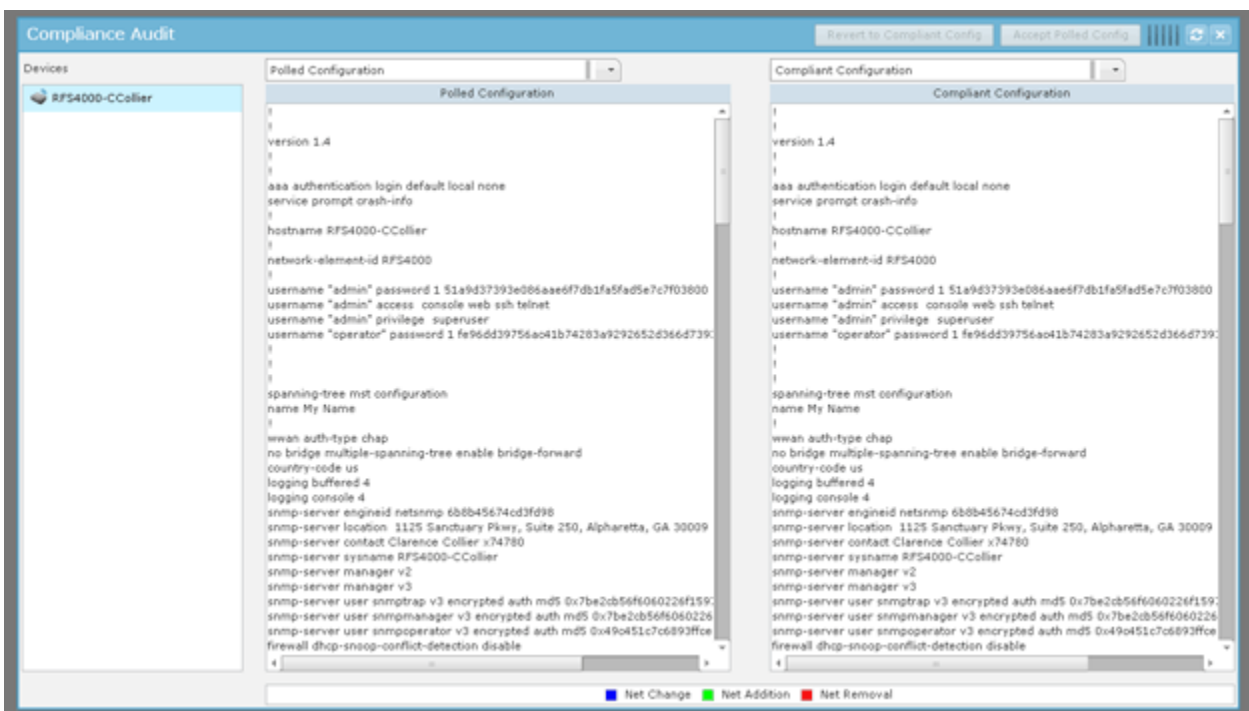
input is required. Other actions will display a dialog that require more input. A description of the actions are as follows:

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><b>Sanctioned (inherit)</b> Classify the selected device(s) as a sanctioned device that inherits its traits from wherever its location in the network tree.</p> <p><b>Sanctioned (override)</b> 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><b>Sanctioned</b> Classify the selected device(s) as sanctioned (Unknown Devices only)</p> <p><b>Unsanctioned</b> Classify the selected device(s) as unsanctioned.</p> <p><b>Neighboring</b> Classify the selected device(s) as a neighboring device.</p>
Client Type	<p>Classify a Wireless Client as one of the following types:</p> <ul style="list-style-type: none"> <li>• Default Type</li> <li>• MCD</li> <li>• VoIP Phone</li> <li>• Laptop</li> <li>• Employee Laptop</li> <li>• Employee Phone</li> <li>• Employee Device</li> <li>• High Priority Visitor Device</li> <li>• Visitor Device</li> <li>• Low Priority Visitor Device</li> </ul>
Audit Devices	Conduct a compliance audit on the selected device(s). (See <a href="#">Audit Devices.</a> )
Retrieve Diagnostic Logs	Display the diagnostic logs for the selected device(s). If no logs are available, you will receive a message stating so. (See <a href="#">Retrieve Diagnostic Logs.</a> )
Remove Devices	Remove selected device(s) from monitoring. (See <a href="#">Remove Devices.</a> )
Move Devices	Place selected device(s) on a floor. (See <a href="#">Move Devices.</a> )
Upgrade Devices	Upgrade the firmware for the selected device(s). (See <a href="#">Upgrade Devices.</a> )

Action	Description
Import CLI Variables	Import CLI variables at the device level. (See <a href="#">Import CLI Variables.</a> )
Export Devices	Export information about selected device(s) to a CSV file. (See <a href="#">Export Devices.</a> )
Command Run and Log	Execute CLI commands for selected device(s) and save results in a log file. (see <a href="#">Command Run and Log.</a> )

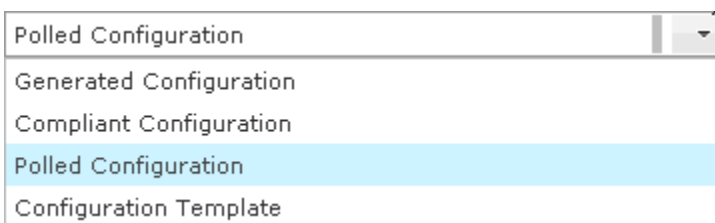
## Audit Devices

The **Audit Devices** action runs a compliance audit on the selected device(s). When selected, a **Compliance Audit** overlay displays and the audit starts.



Once the audit is complete, the device(s) are listed in the **Devices** sub-window. When a device is selected (highlighted), the audit results are displayed in two parts: the **Polled Configuration** and the **Compliant Configuration**. The **Polled Configuration** is a list of CLI commands that were pulled from the device. The **Compliant Configuration** is a list of CLI commands that were pulled from the CLI Profile for the device. If there are differences, they are highlighted. Also, the **Revert to Compliant Config** and **Accept Polled Config** buttons are activated. Otherwise, the buttons are inactive.

You may change the displayed configuration by selecting a configuration type from the drop-down menu.



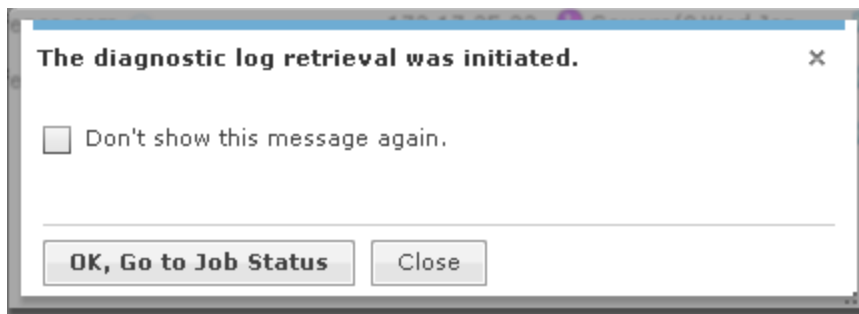
When you change a configuration type, the CLI commands for that type are displayed. If there are differences, they are highlighted.

Click the **Revert to Compliant Config** button to update the highlighted device with the CLI commands from the **Compliant Configuration**. Click the **Accept Polled Config** button to accept the CLI commands from the **Polled Configuration** section.

Click the **Close**—X button exit the **Compliance Audit** overlay.

## Retrieve Diagnostic Logs

The **Retrieve Diagnostic Logs** action collects your appliance's diagnostic logs for the selected device and consolidates them into one file. Just select (highlight) a device and then click **Actions > Retrieve Diagnostic Logs**.



✓ **NOTE** You can elect not to show this message again by selecting the checkbox.

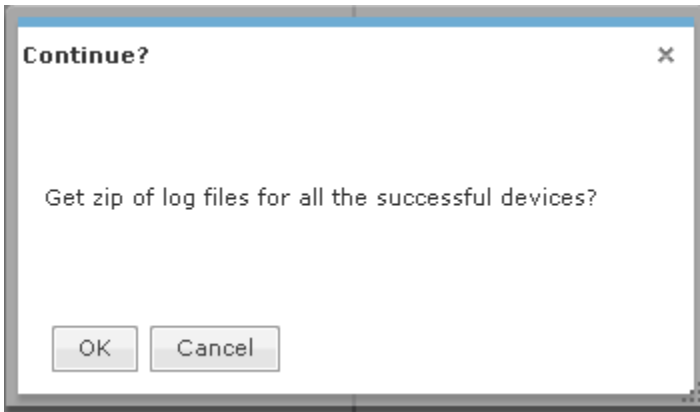
At this point, ADSP starts retrieving the diagnostic logs. When the **OK, Go to Job Status** button is clicked, the Job Status is displayed.

Type	Description	User	Status	Start Time	Finish Time	Progress
Device Configuration	On Demand Log Retr	collier	Complete: successfu	Wed Jan 25 2012 ...	Wed Jan 25 2012 ...	1/1

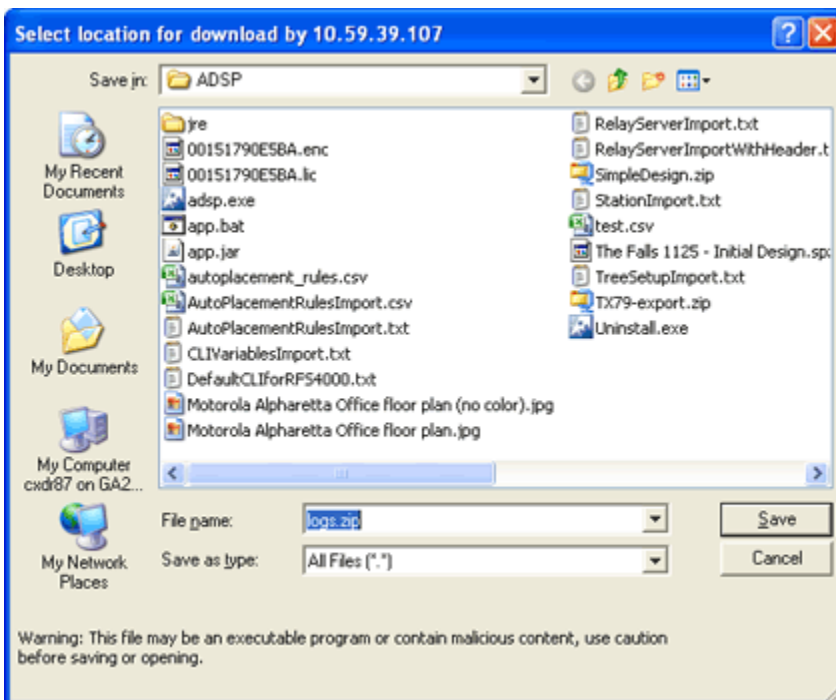
Select your job and then click the **View Details** button to display the job details.

To view your diagnostic logs, you will have to export them to your workstation using the **Export Consolidated Logs** button.

- ✓ **NOTE** The **Export Consolidated Logs** button is inactive until the status changes to Pass and the diagnostic logs are ready to export.



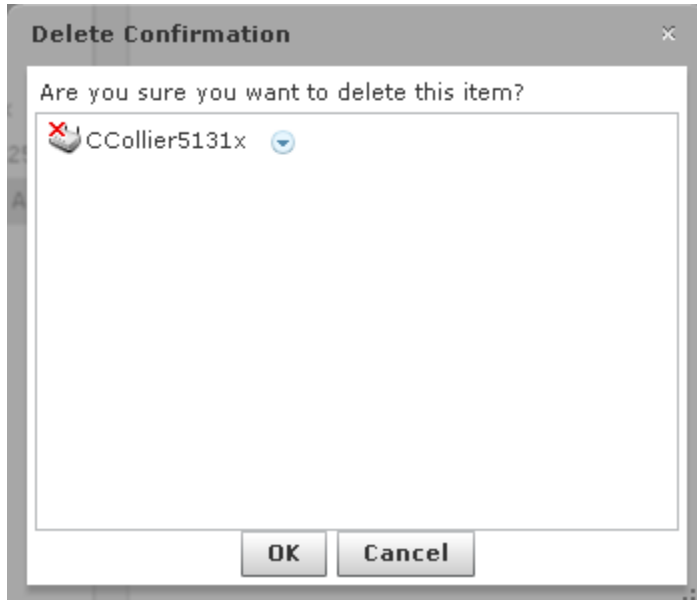
Click **OK** to continue.



Navigate to a location and click the **Save** button. The consolidated logs are saved in a ZIP file using the specified file name. You can now view the logs.

## Remove Devices

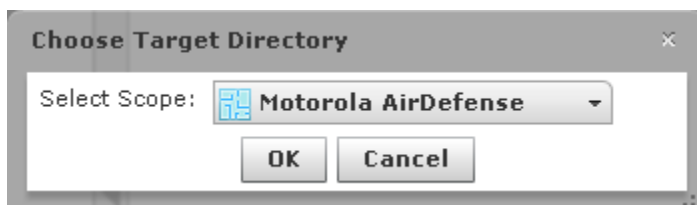
The **Remove Devices** action removes any selected (highlighted) device. When selected, you are prompted to confirm removal.



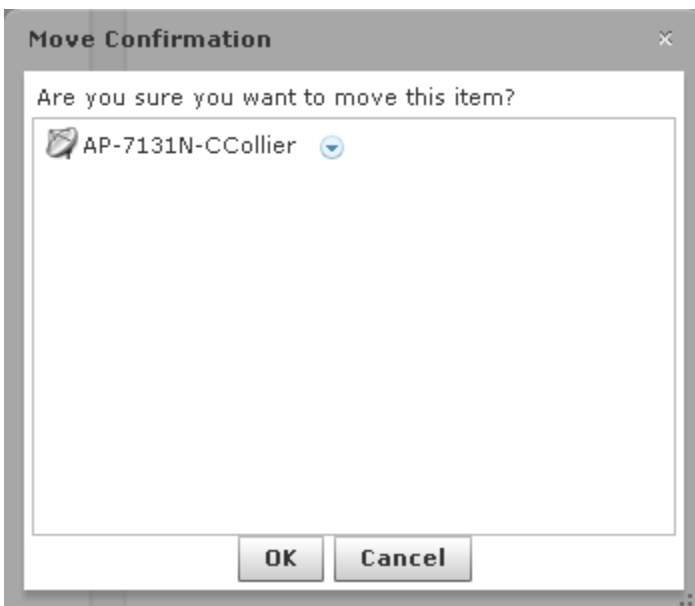
Click **OK** to remove the listed devices. Click **Cancel** to exit without removing the device(s).

## Move Devices

The **Move Devices** action moves the selected device(s) to a scope (floor) that you specify. When selected, you are prompted to select a scope.



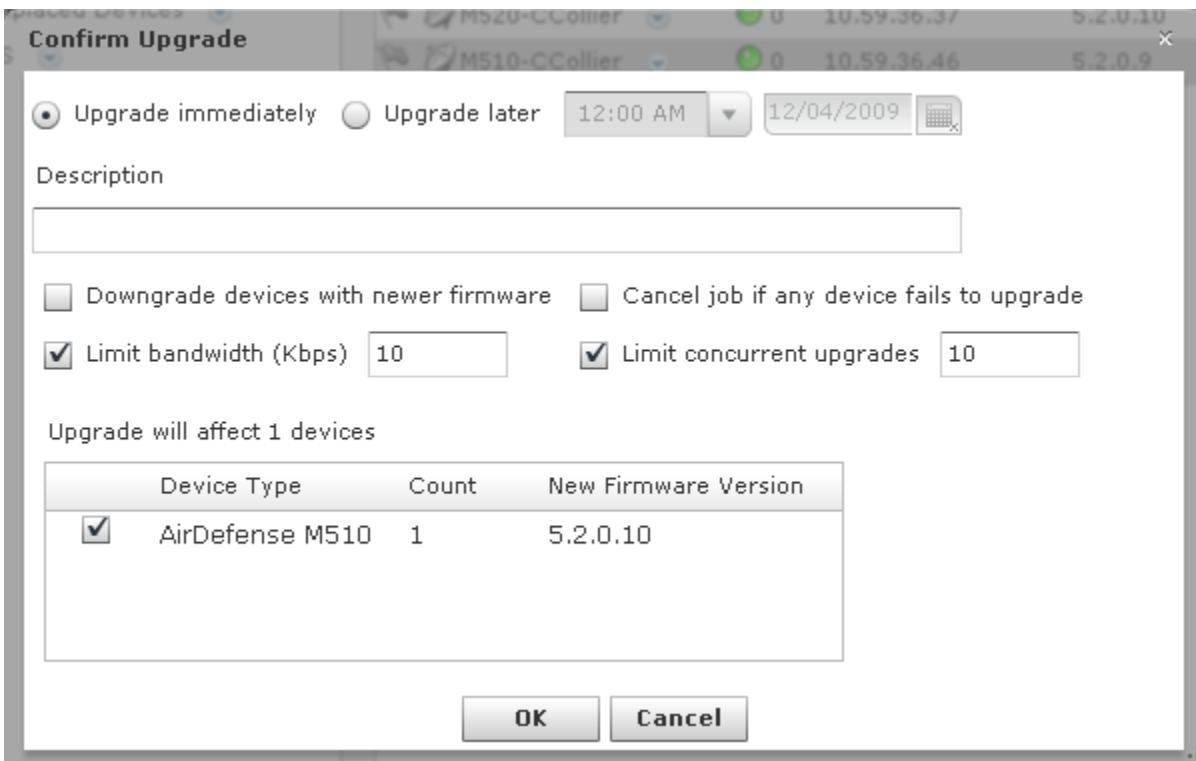
Click the drop-down menu to make your selection and then click **OK**. You are prompted to confirm your selection.



Click **OK** to move the device(s). Click **Cancel** to exit without moving the device(s).

## Upgrade Devices

The **Upgrade Devices** action is used to upgrade the firmware for devices on your network. Select (highlight) the device(s) and then select **Upgrade Devices** from the menu.



You have the option of upgrading immediately or upgrading later. If you decide to upgrade later, select **Upgrade Later** and then select a time from the drop-down menu and a date from the calendar.

You may enter a description in the **Description** field. This information is displayed when you check the [Job Status](#) and helps identify the job.

There are four checkbox options that you can select. They are:

- Downgrade devices with newer firmware.
- Cancel job if any device fails to upgrade.
- Limit bandwidth that the upgrade can occupy. By entering a value, you will limit the bandwidth to the entered value. The default is 10 Kbps.
- Limit concurrent upgrades. By entering a value, you limit the number of upgrades that can run at one time. The default is 10.

A list of device that will be upgraded are displayed. The list will display:

- The type of device
- The total number of devices
- The new firmware version that will be used for the upgrade.

By default, all devices are selected. If you decide not to upgrade one or more devices, uncheck the checkbox for that type of device.

Click **OK** to start or schedule the upgrade. Click **Cancel** to exit and not upgrade.

### Import CLI Variables

✓ **NOTE** A WLAN Management license is required to import CLI variables.

The **Import CLI Variables** action is used to import CLI variables at the device level. Naturally, the CLI variable should already exist in the device's profile or it will not be applied.

Comma delimited files are used to import CLI variables. The format of the file is:

```
cli_variables,server,deviceMAC or folderPath,deviceType,var1,var1_value,var2,var2_value,var3,var3_value,[etc.]
```

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.

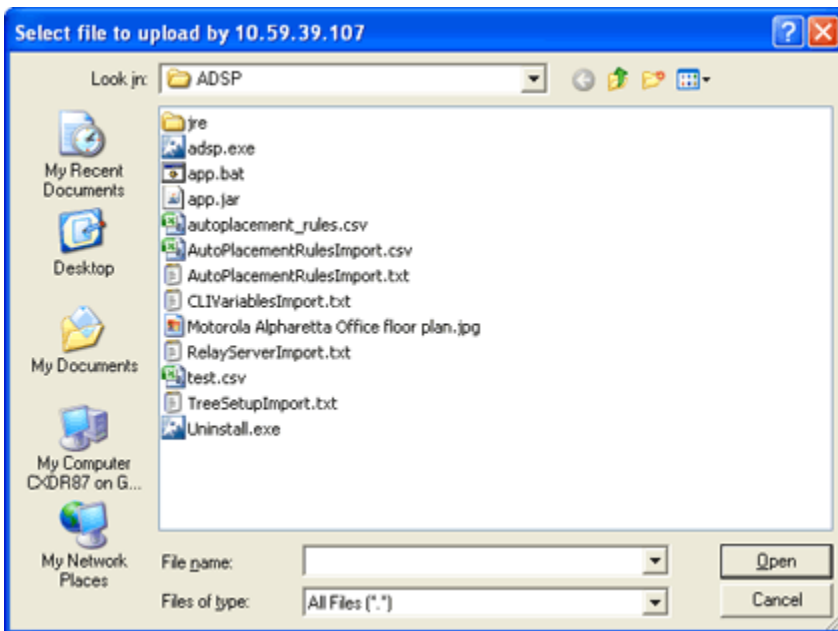
The first line is reserved for header information. If you do not want to include header information, make the first line a blank line.

Examples:

```
cli_variables,localhost,00:00:00:a0:e7:33,ap,MASK,255.255.0.0
cli_variables,localhost,00:00:00:c7:00:39,ap,HOSTNAME,AP7131_Cube44,MASK,255.255.0.0,GATEWAY,192.10.1.1
cli_variables,localhost,US/Southeast/Alpharetta/Floor1,,HOSTNAME,AP7131_Cube44
```


✓ **NOTE** deviceType can be blank if designating a folderPath.

When the **Import CLI Variables** action is selected, a dialog window opens where you can specify the directory (folder) and name of the CSV file.



Select the import file and then click **Open** to import the CLI variables.

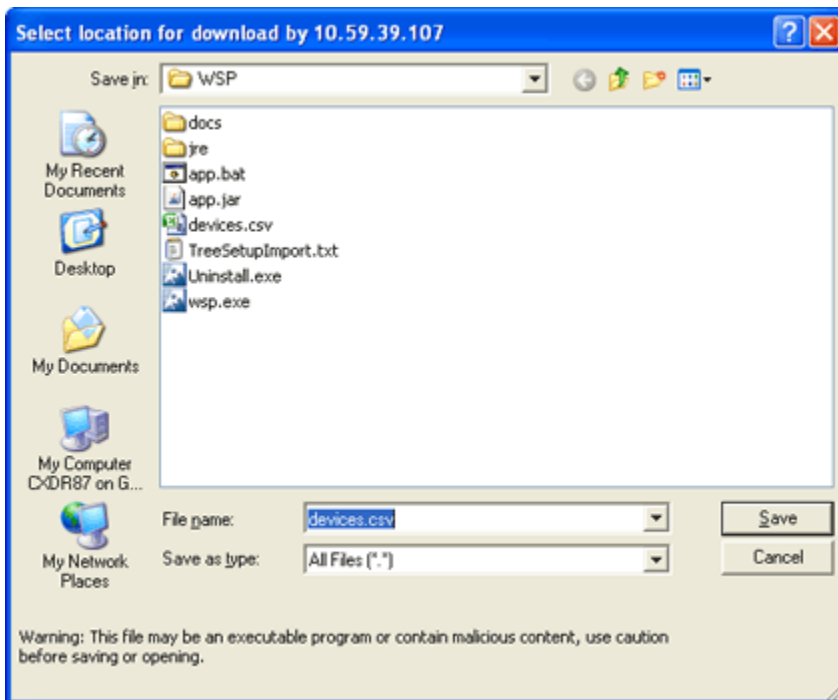
To verify that the CLI variables were imported:

1. Click the device's drop-down menu button—.
2. Select **Properties** from the menu.
3. Select the CLI Profile for the device. The imported CLI variables should be visible in the **Variables** section.



## Export Devices

The **Export Devices** action is used to export information about your devices to a CSV file on your local workstation. When selected, a dialog window opens where you can specify the directory (folder) and name of the CSV file.



- ✓ **NOTE** At this time, files exported using **Export Devices** are for external viewing only. They cannot be imported back into ADSP.

AirDefense Services Platform will name the CSV file `devices.csv` by default. You can keep that name or change it.

Click the **Save** button to save the CSV file. Click **Cancel** to exit without saving the file.

Once the file is saved, you can view the file at any time.

## Command Run and Log

The **Command Run and Log** action allows you to run CLI commands on devices that are in the Audit mode (not template based) and then store the results in a log file for viewing later.

- ✓ **NOTE** In order for **Command Run and Log** to work properly, a [Communication Settings](#) profile must exist for the affected devices.

**Command Run and Log**

Devices that will be affected

172.17.25.21

Enter any sequence of commands that are valid on the device CLI interface:

**⚠ Please note:** ADSP will respond "Yes" to all device confirmation requests.

Import updated compliant configuration from device(s) after successful command run.

Submit Cancel

The commands are applied to all devices selected in the **Network** tab. Selected devices are listed in the **Devices that will be affected** field.

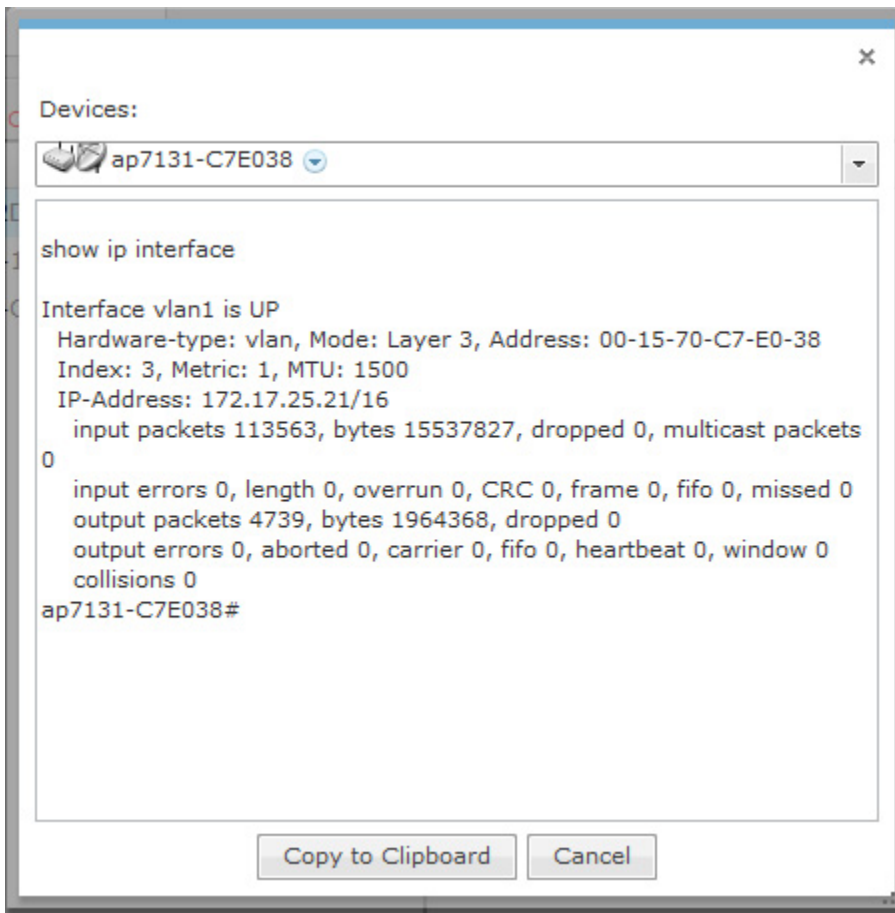
Each command must be on a line by itself. If a command requests a confirmation from a device, ADSP will respond Yes.

You may import an updated configuration from device(s) after a command has run successfully. Just select the **Import** checkbox.

The logs for the **Command Run and Log** are placed at: `/usr/local/smx/device-mgmt/jobs`. For each job, there is a job ID. The interaction with all devices for a job is placed in a sub-folder whose name is the job ID number.


Click **Submit** to run the commands. Click **Cancel** to exit without running any commands.

You can check the job status by navigating to **Configuration > Operational Management > Job Status**. While viewing the job details, you can view the logs by selecting a device and then clicking the **View Log** link.



You can view the log of another device by selecting the device from **Devices** drop-down menu. The **Copy to Clipboard** button copies the log contents to the clipboard. The **Cancel** button exits the log.

## Advance Search

The **Network** tab has an advance search feature that allows you to supply additional criteria to the basic search. Click the **Advance Search** icon——to access the advance search feature.

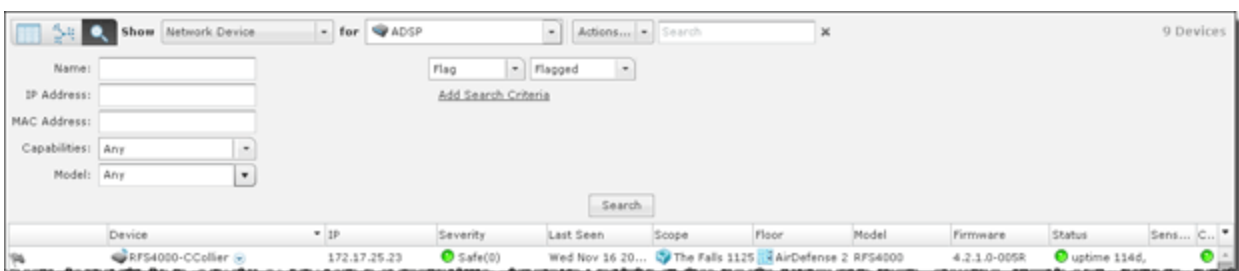


With the advance search feature, you can supply additional information such as:

- The name of the device
- The IP address of the device
- The MAC address of the device

- The capabilities of the device (Any, Access Point, Sensor, Wireless Switch, Wired Switch, or Network Manager selected from a drop-down menu)
- The model number of a device or any model.
- The SSID of the device
- The client type of the device
  - Default Type
  - MCD
  - VoIP Phone
  - Laptop
  - Employee Laptop
  - Employee Phone
  - Employee Device
  - High Priority Visitor Device
  - Visitor Device
  - Low Priority Visitor Device
- The manufacturer of the device
- The source
  - All
  - Sensor Segment
  - Switch
  - Authorized AP
  - Unknown

You may add additional criteria as needed by clicking the **Add Search Criteria** link. When the link is clicked, the first additional criteria (Flag) is added.



You can change the added search criteria by clicking the drop-down menu and selecting another criteria. The menu contains criteria that relate to the type of devices being displayed. If you want to use more than one of the listed criteria, you can click the **Add Search Criteria** link to add the next criteria in the list.



Additional criteria may be added until you added all the search criteria for the type of devices being displayed. Added criteria may be removed by hovering your cursor over the criteria and then clicking the **X** located to the right of the criteria.

Additional criteria includes:

Criteria	Description
Flag	Select whether you want to display flagged or un-flagged devices.
Firmware	Supply a firmware version for devices you want to display.
First Seen	Supply a range of first seen hours for devices you want to display.
Last Seen	Supply a range of last seen hours for devices you want to display.
Classification	Select whether you want to display sanctioned, unsanctioned or neighboring devices.
Channel	Supply a range of channels for devices you want to display.
Signal Strength	Supply a range of signal strengths (in dBm) for devices you want to display.
Sensed Authentication	Select a sensed authentication method from the drop-down menu.
Sensed Encryption	Select a sensed encryption method from the drop-down menu.
Polled Authentication	Select a polled authentication method from the drop-down menu.
Polled Encryption	Select a polled encryption method from the drop-down menu.
Up Time	Supply a range of up time hours for devices you want to display.
Online	Select whether you want to display online or offline devices.
Compliant	Select whether you want to display compliant, non-compliant, or unlicensed devices.

Once you have entered or selected your search criteria, click the **Search** button. Devices matching your search criteria is displayed.

---


## Alarms

The **Alarms** tab displays an alarm table that shows all of the active and inactive alarms currently occurring on your network, sorted in columns by:

- flag
- alarm criticality
- alarm type
- offending device
- start time
- alarm status
- SSID of the offending device.

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 22:00)	Test_100
S 5553530...	Rogue AP on Wired Ne...	Motorola:ca:f9:d0	Fri Apr ...	Inactive (expires in 22:00)	Mayer5131
S 5122746...	Rogue AP on Wired Ne...	Motorola:cb:f9:f0	Fri Apr ...	Inactive (expires in 22:00)	Mayer5131
S 2020001...	Rogue AP on Wired Ne...	Motorola:cb:f9:f1	Fri Apr ...	Inactive (expires in 22:00)	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 1466755...	Rogue AP on Wired Ne...	Motorola:2f:74:21	Fri Apr ...	Active	Test_100
S 4159659...	Rogue AP on Wired Ne...	Cisco:bfe7:20	Fri Apr ...	Inactive (expires in 19:48)	1140-N
S 3862793...	Rogue AP on Wired Ne...	Symbol: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	APS131-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 alarms listed in the table are determined by the network level selected in the **Show alarms in** drop-down menu and the filters you utilize in the [Alarm Filters](#).

You can hide (uncheck) or view (check) columns by clicking the drop-down button—  — located to the right of the last column.

- Flag
- Criticality
- Alarm ID
- Alarm Type
- Device
- Device Actions
- Start Time
- Status
- SSID
- Sensor
- Expire Time
- Signal Strength
- Channel
- Notes
- Summary

You can hide the Alarm Filters by clicking **Hide Alarm Filters** bar—  . You can show (un-hide) the Alarm Filters by clicking the **Show Alarm Filters** bar—  .

## 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.

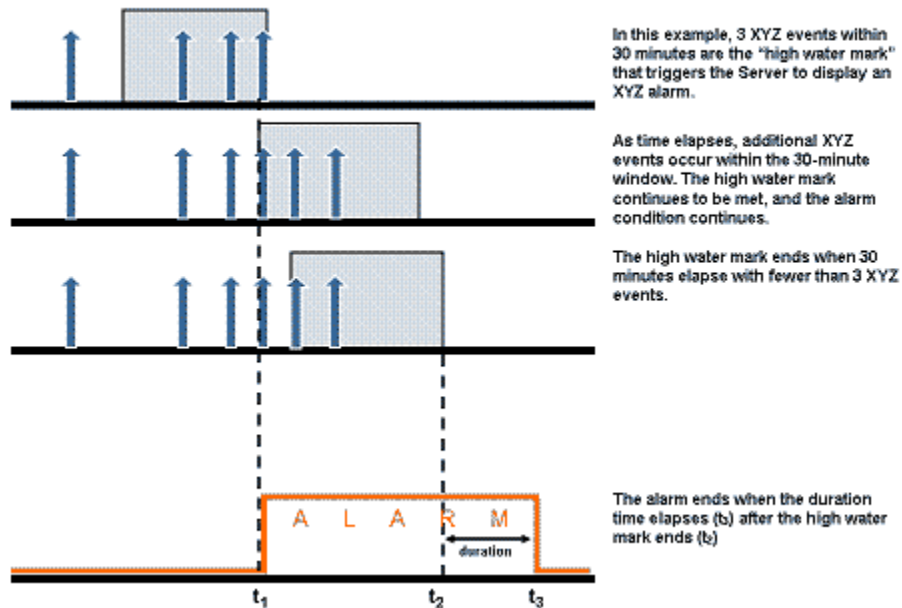
Motorola AirDefense's industry leading wireless security research team maintains algorithms for correlating observed security events, to identify when a pre-defined high water mark for the event is reached. The high water mark, in its simplest terms, is a number of identical events that occur within 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 <a href="#">Alarm Criticality</a> 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.
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.



Column	Description
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

The Alarm Filters are used to filter the displayed alarm information. The filters are displayed on the left side of the window.

The screenshot shows a vertical panel with the following elements:

- Grouping** (header with a grey indicator)
- No Grouping
- Severity
- Alarm Category
- Alarm Sub-Category
- Alarm Type
- Alarm State
- Alarm Start
- Device Type
- Device Classification
- Scope
- Network Scope** (category with a green indicator)
- Alarm Severity** (category with a green indicator)
- Alarm Type** (category with a green indicator)
- View** (category with a green indicator)
- Device** (category with a green indicator)
- Alarm Lifecycle** (category with a green indicator)
- Alarm ID** (category with a green indicator)

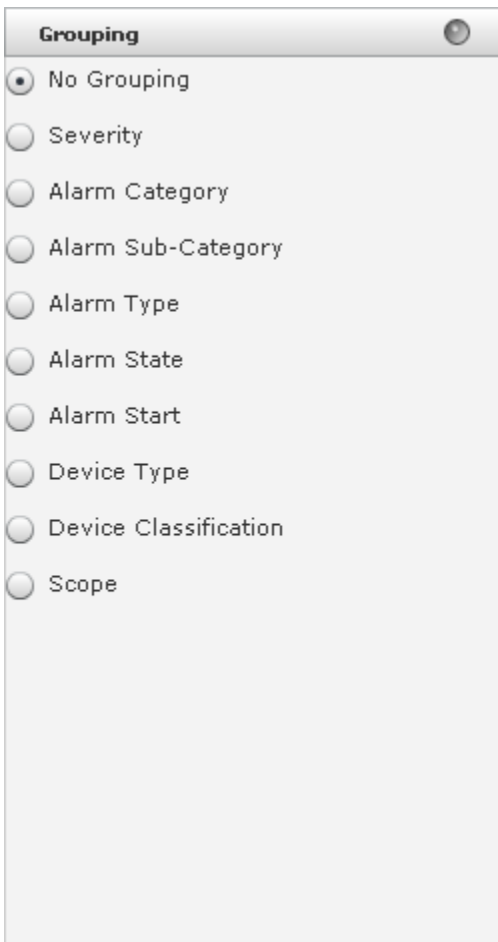
The indicator on the right of each filter turns green——when you change a filter from its original state. Click the green indicator to return a filter to its default state.

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 Severity—view alarms by severity.
- Alarm Type—view devices by alarm type.
- 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.

### Grouping Filter

The **Grouping** filter allows you to view alarms by grouping them using similar criteria.



The following views are available:

- No Grouping—Displays all alarms without grouping.

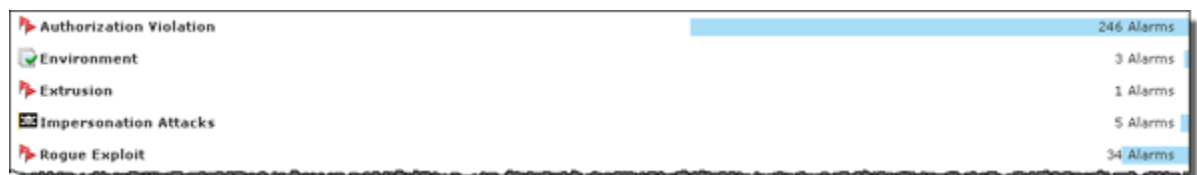
- Severity—Groups alarms into the different threat levels to your network. Threat levels that are not sensed are not shown.



- Alarm Category—Groups alarms into alarm categories.



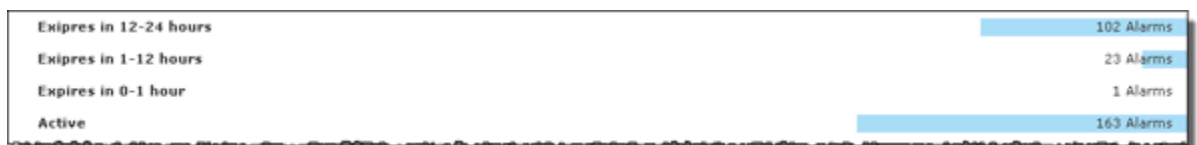
- Alarms Sub-Category—Groups alarms into alarm sub-categories.



- Alarm Type—Groups alarms by alarm type.



- Alarm State—Groups alarms by the state of the alarms.



- Alarm Start—Groups alarms by when they started.



- Device Type—Groups alarms by the device type.



- Device Classification—Groups alarms based on the device classification.



- Scope—Groups alarms based on where they are in the network. The highest network levels under the appliance level are displayed as the group.

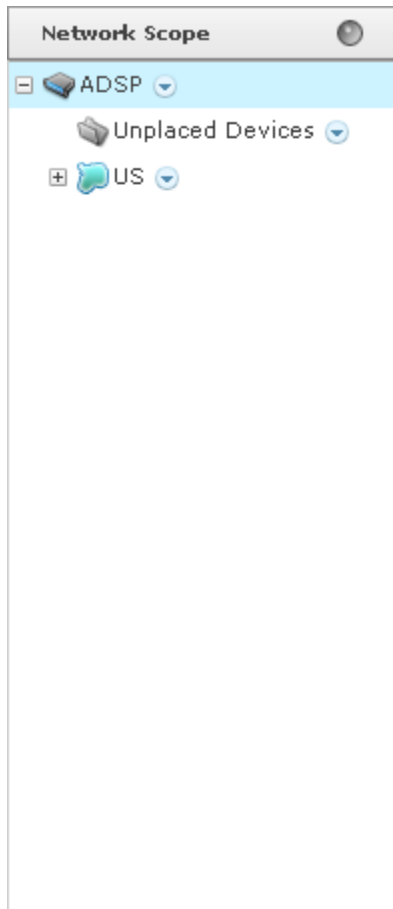


Clicking on a group will display the individual alarms in that group.



## Network Scope Filter

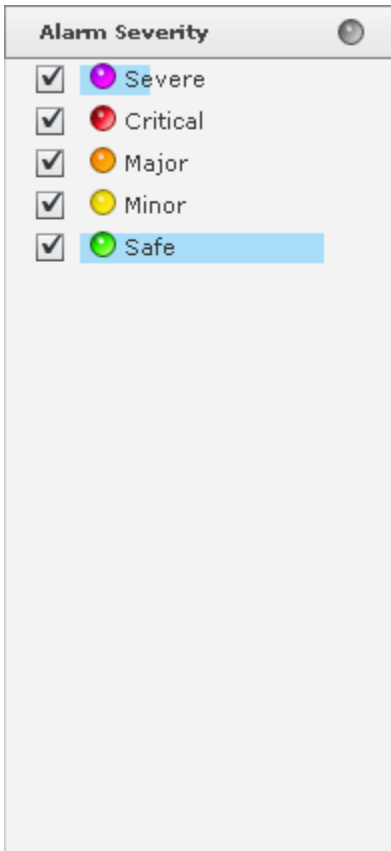
The **Network** Scope filter is used to view alarms according to where they are in the network tree. By selecting a network level, you limit the displayed alarms to only the ones under that particular network level.








If the appliance level is selected, all the alarms for that appliance are displayed. If a floor level is selected, only the alarms on that floor are displayed.

## Alarm Severity Filter

The **Alarm Severity** filter allows you to view devices by alarm severity.



The severities are:

- Severe——Displays only Severe alarms.
- Critical——Displays Critical and Severe alarms.
- Major——Displays Major, Critical, and Severe alarms.
- Minor——Displays Major, Critical, and Severe alarms.
- Safe——Displays alarms of all criticalities.

You can select the alarms that you want to view by checking the checkbox.

## Alarm Type Filter

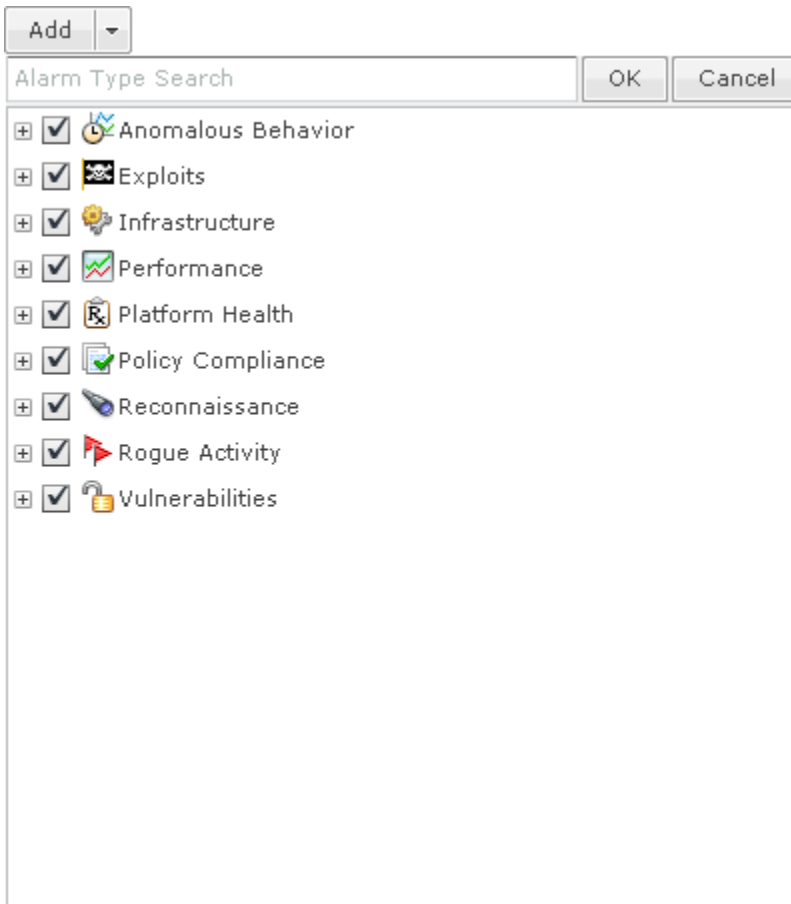
The **Alarm Type** filter allows you to view devices by alarm type.



You also have the option of displaying all alarm types or you may filter alarms by a specific type. The different alarm types are:

- Anomalous Behavior
- Exploits
- Infrastructure
- Performance
- Platform Health
- Policy Compliance
- Reconnaissance
- Rogue Activity
- Vulnerabilities.

The **Add** button is used to select the alarm types that you want to display.





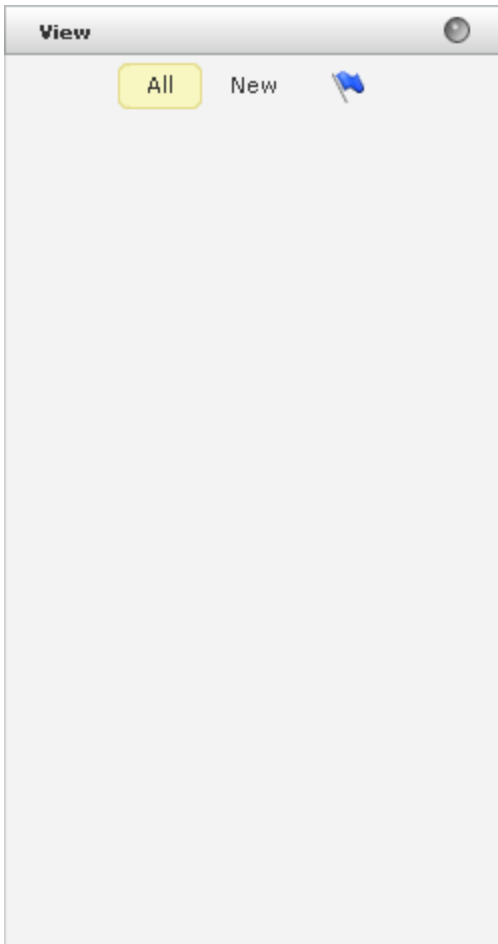
Click the **Add** button, select the alarm type(s), and then click **OK**. The following screen shots shows that you only want to display rogue alarms.




To remove an alarm type, select (highlight) the alarm type and click the **Remove** button.

## View Filter

The **View** filter gives you the option of viewing all alarms, new alarms, or flagged alarms.



To select an option, click **All**, **New**, or the blue flag—. The option you select will be highlighted.

## Device Filter

The **Device** filter is used to filter alarms by device classification, device type, and/or license status.

**Device**

**Device Classification**

- Sanctioned
- Unsanctioned
- Neighboring

**Device Type:**

- BSS
- Network Device
- Unknown Devices
- Wireless Client

**License Status**

- Licensed
- Unlicensed

Alarms can be displayed by the following device classifications:

- Neighboring—Display alarms for neighboring devices.
- Sanctioned—Display alarms for sanctioned devices. You may also choose to display any sanctioned device, inherited sanctioned devices, or overridden sanctioned devices.
- Unsanctioned—Display alarms for unsanctioned devices.

In addition to or instead of, alarms can be displayed by device type:

- BSS
- Network Device (includes APs, Sensors, Switches, and Wireless Managers)
- Unknown Device
- Wireless Client.

Also, alarms can be displayed by license status:

- Licensed
- Unlicensed

Select the checkbox(es) for the device classifications and/or device types that you want to display.

## Alarm Lifecycle Filter

The **Alarm Lifecycle** filter allows you to filter alarms over an alarm's lifecycle.

**Alarm Lifecycle**

**Alarm State**

- Active
- Expires in 0-1 hour
- Expires in 1-12 hours
- 12-24 hours
- Expires in 24-72 hours
- Expires in more than 72 hours

**Alarm started within prior**

- 0-1 hour
- 1-12 hours
- 12-24 hours
- 24-72 hours
- More than 72 hours

You can select alarm states and/or a time range when the alarms started. The alarm states include:

- Active Alarms
- Alarms that expire in 0 to 1 hour
- Alarms that expire in 1 to 12 hours
- Alarms that expire in 12 to 24 hours
- Alarms that expire in 24 to 72 hours
- Alarms that expire in more than 72 hours.

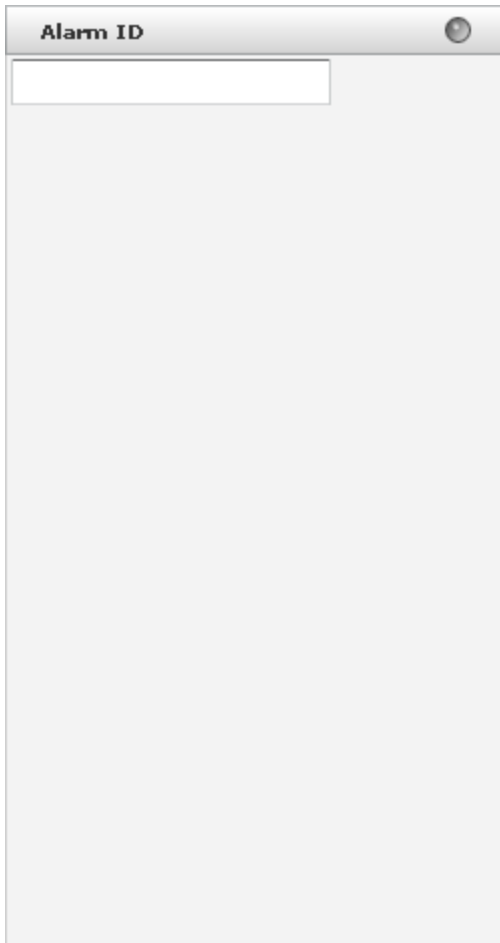
The time range when alarms started include:

- Alarms that started 0 to 1 hour ago
- Alarms that started 1 to 12 hours ago
- Alarms that started 12 to 24 hours ago
- Alarms that started 24 to 72 hours ago
- Alarms that started more than 72 hours ago.

Select the checkbox(es) for the alarm states and/or time ranges when the alarms started that you want to display.

### Alarm ID Filter

The **Alarm ID** filter is used to filter alarms using the alarm ID.

A screenshot of a web interface showing a window titled "Alarm ID". Inside the window, there is a single text input field at the top, which is currently empty. The rest of the window area is a light gray color, suggesting a list of results or a filter status area that is currently blank.

Normally, the alarm ID can be found in things such as:

- an email that was generated by an alarm.
- a SNMP notification generated by a Trap action defined in the Action Manager.
- a report generated by the Report system.

Type or paste an alarm ID in the **Alarm ID** field to filter alarms using that alarm ID. Only the alarm matching the ID will be displayed.

### Alarm Categories and Criticality

AirDefense Services Platform generates alarms when certain events or conditions occur in your wireless LAN that violate a policy or performance threshold.

To make alarms easy to identify, ADSP groups alarms into nine categories, and assigns a criticality to each alarm. Alarm notifications can also be delivered to the administrator via Email, SNMP, or Syslog.






## 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.

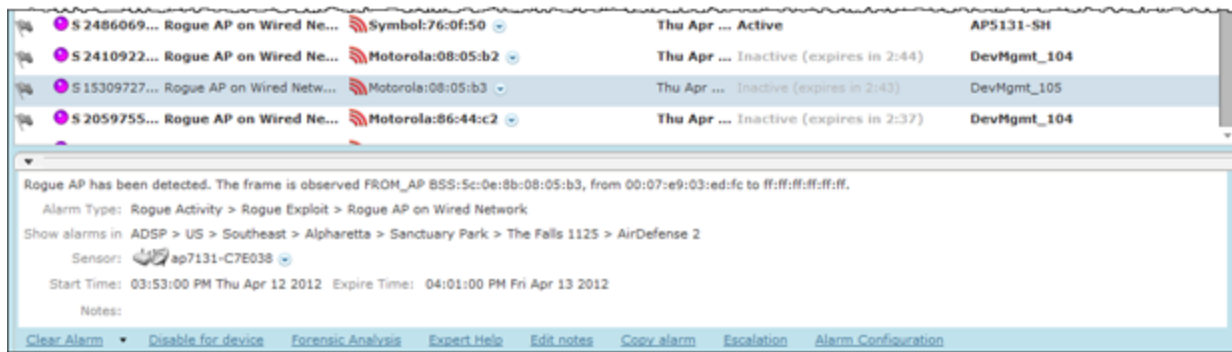
## Alarm Criticality

Alarms are assigned 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. Information about the alarm is displayed at the bottom of the **Alarms** tab.



If you do not see the alarm details, click the **Open** bar to display them.

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.

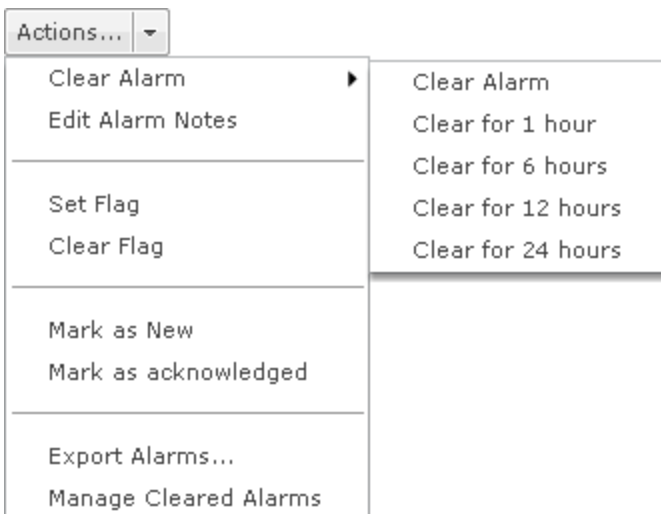
At the bottom of the detailed information are links that allow you to execute a function or provide more information.

Link	Description
Clear Alarm	Clear alarm works the same as <b>Clear Alarm</b> in the <b>Actions</b> 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"> <li>• Summary—displays a summary about the alarm type.</li> <li>• Description—displays detailed information about the alarm type.</li> <li>• Investigation—advises you on how to investigate the alarm type.</li> <li>• Mitigation—advises you on how to mitigate the alarm type.</li> </ul>
Edit notes	Allows you to edit or add notes for the alarm.

Link	Description
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 <b>Alarm Configuration</b> in the <b>Configuration</b> 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"> <li>• Clear Alarm (no time limit)</li> <li>• Clear for 1 hour</li> <li>• Clear for 6 hours</li> <li>• Clear for 12 hours</li> <li>• Clear for 24 hours.</li> </ul> <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.



Action	Description
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. You will be prompted for a name and a location to place the file.
Manage Cleared Alarms	Displays an overlay where you can manage cleared alarms. A list of alarms is displayed containing alarms that have been cleared and configured to remain cleared for a specified amount of time. You can remove alarms that have been configured to remain cleared for a time period by selecting (highlighting) the alarm(s) and clicking the <b>Remove Alarms</b> button. Click the <b>Close</b> —X button to exit the overlay.

---

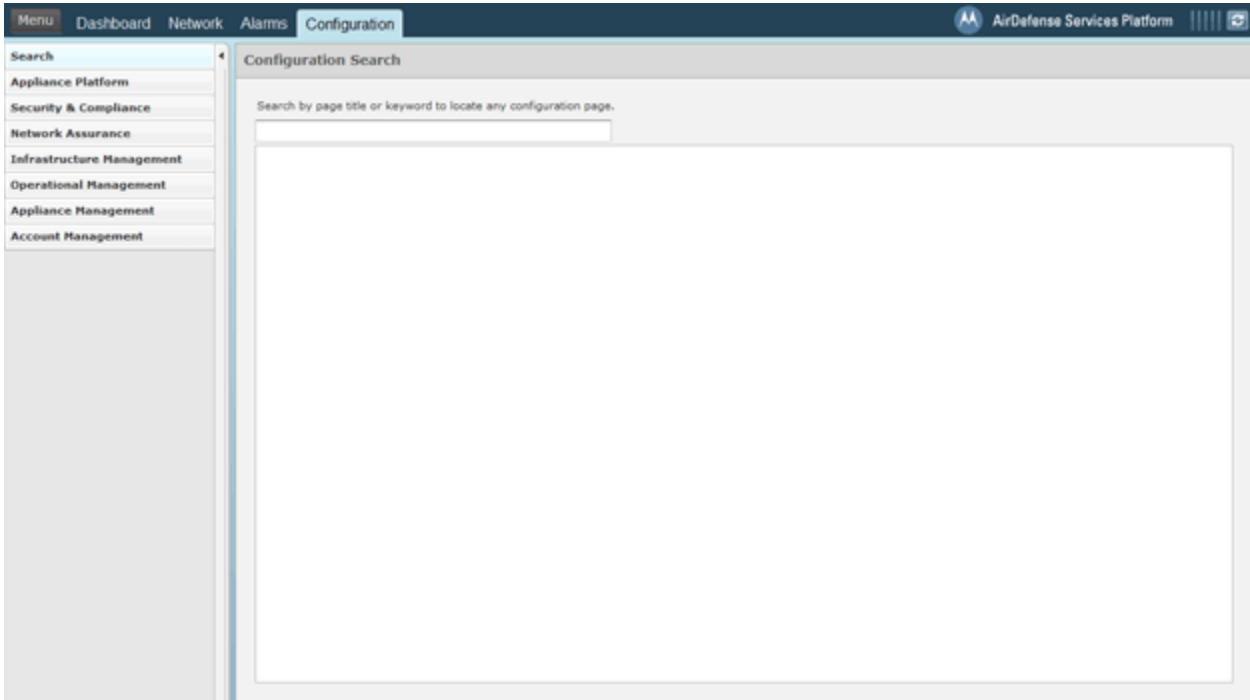
## Configuration

The **Configuration** tab allows you to initially set up ADSP, configure devices for management, and perform other administrative tasks such as user and Sensor administration. Once you configure your network with ADSP, you can administer and monitor your network from one central location.

The following configuration categories allow you fully set up and manage ADSP:

- 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.
- Appliance Management—configures the AirDefense Enterprise appliance.

- Account Management—creates and maintains user accounts.

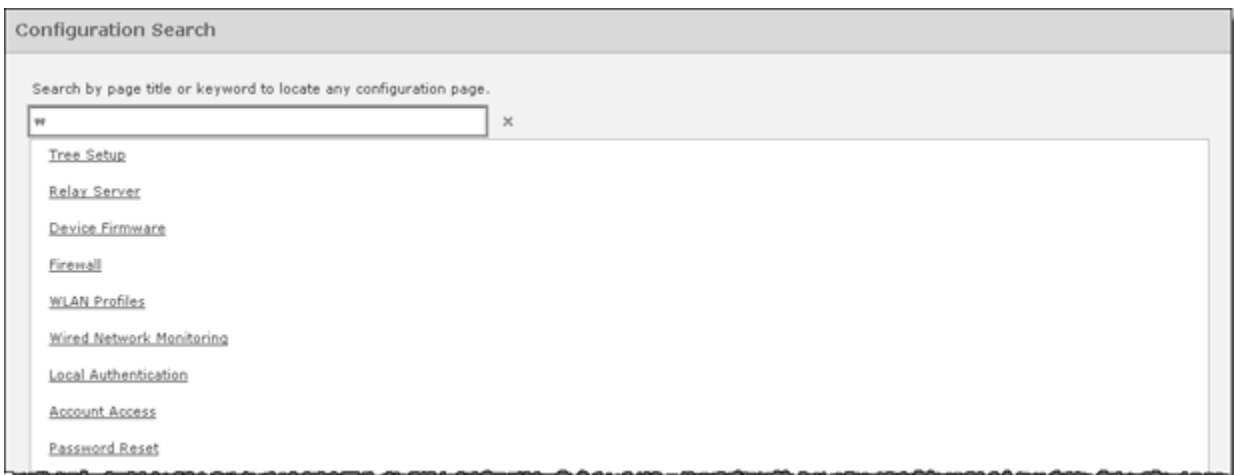


### Search

Searches the **Configuration** tab for quick location of a configuration feature.



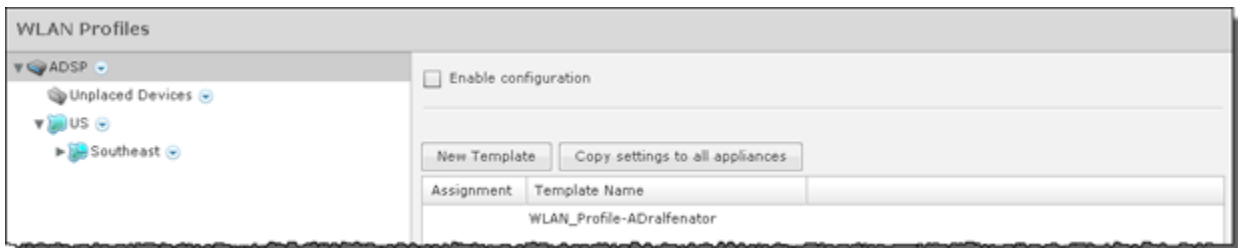
To conduct a search, just start typing.



Typing just 1 character will list available features related to that character. To narrow your search, type more text.



Click the link for the feature to navigate to it.



## Appliance Platform

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

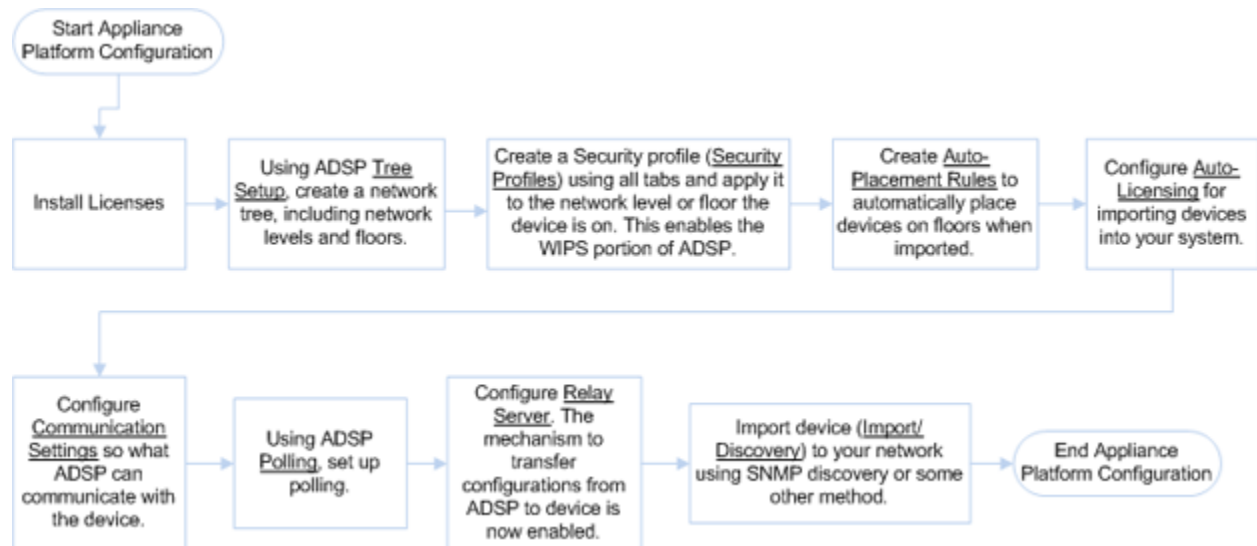
Search
<b>Appliance Platform</b>
01. Appliance Licensing
02. Tree Setup
03. Security Profiles
04. Auto-Placement Rules
05. Auto-Licensing
06. Communication Settings
07. Polling
08. Relay Server
09. Import / Discover Devices
<b>Security &amp; Compliance</b>
<b>Network Assurance</b>
<b>Infrastructure Management</b>
<b>Operational Management</b>
<b>Appliance Management</b>
<b>Account Management</b>

The Appliance 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. Auto-Licensing—Establish an import policy that controls how device licenses are applied 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.

The following flowchart shows the fundamental steps to initially configure ADSP.

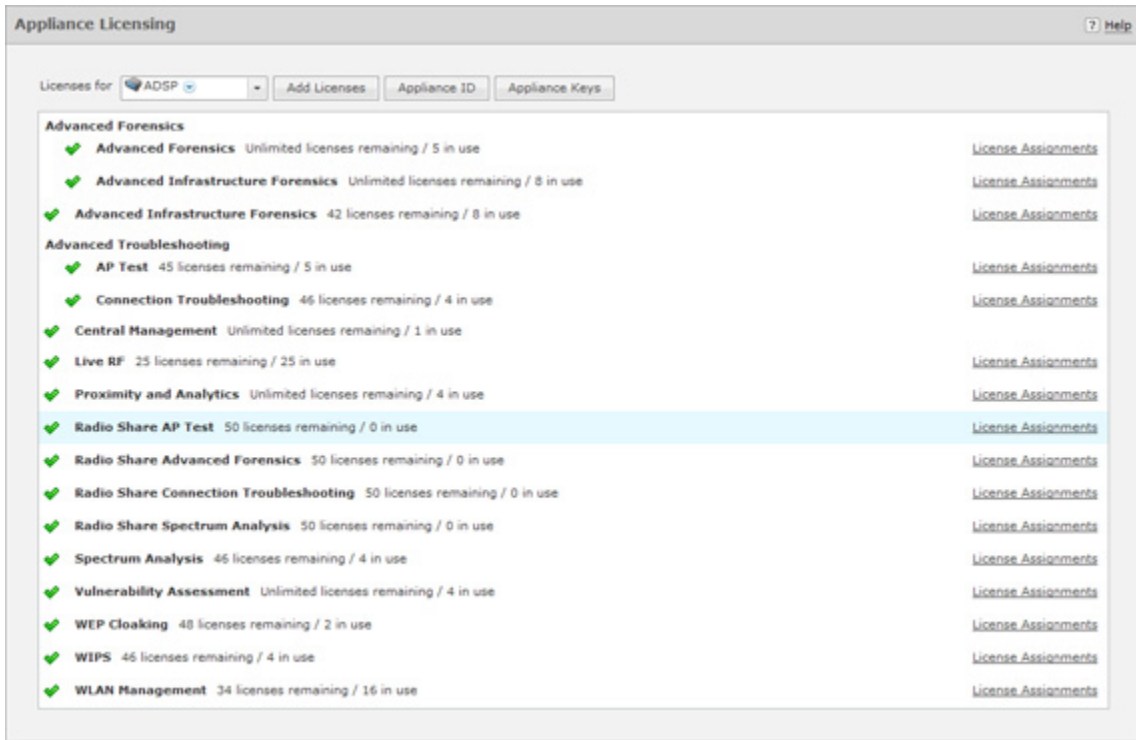


### Appliance Licensing

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 WIPS (base license) and the following add-on modules:



**NOTE** Modules are only displayed when they are installed.

- 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)
- Vulnerability Assessment
- WEP Cloaking
- WLAN Management

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.

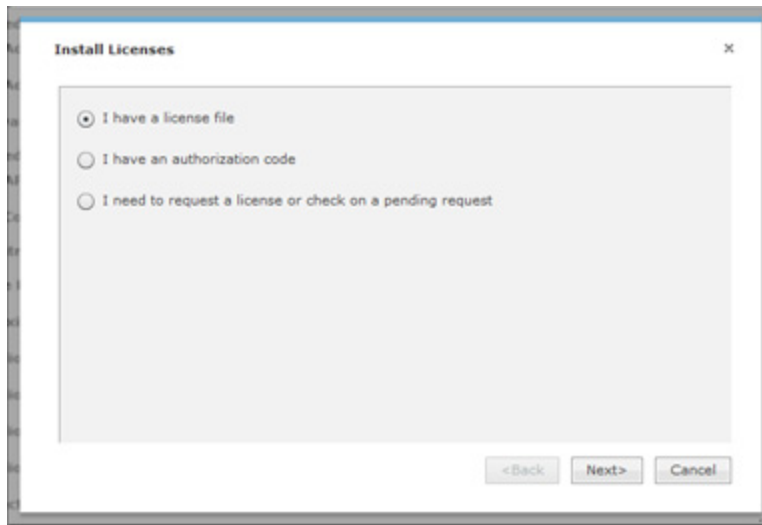
✔ **WIPS** - 46 licenses remaining / 4 in use  
 Order placed on 2019-06-04 (id=105472)  
 License count: 50 licenses  
 Valid from 2019-06-04 and does not expire  
 Maintenance from unspecified  
 Reassignments: 25 licenses / 25 licenses remaining

[License Assignments](#)

Field	Description
Order Date	Indicates the date the license was ordered and the license ID number.
License Count	Includes the following information: <ul style="list-style-type: none"> <li>• The number of units. The number of active units cannot exceed this number. Unit counts may be 0, a specific number, or unlimited.</li> <li>• 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.</li> <li>• A unit identifier. Units may be Sensors, APs, switch, etc.</li> <li>• A maximum value limiting the number of units.</li> <li>• A warning limit used to display an alarm that the unit count is being approached and that user should consider purchasing additional licenses.</li> </ul>
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.

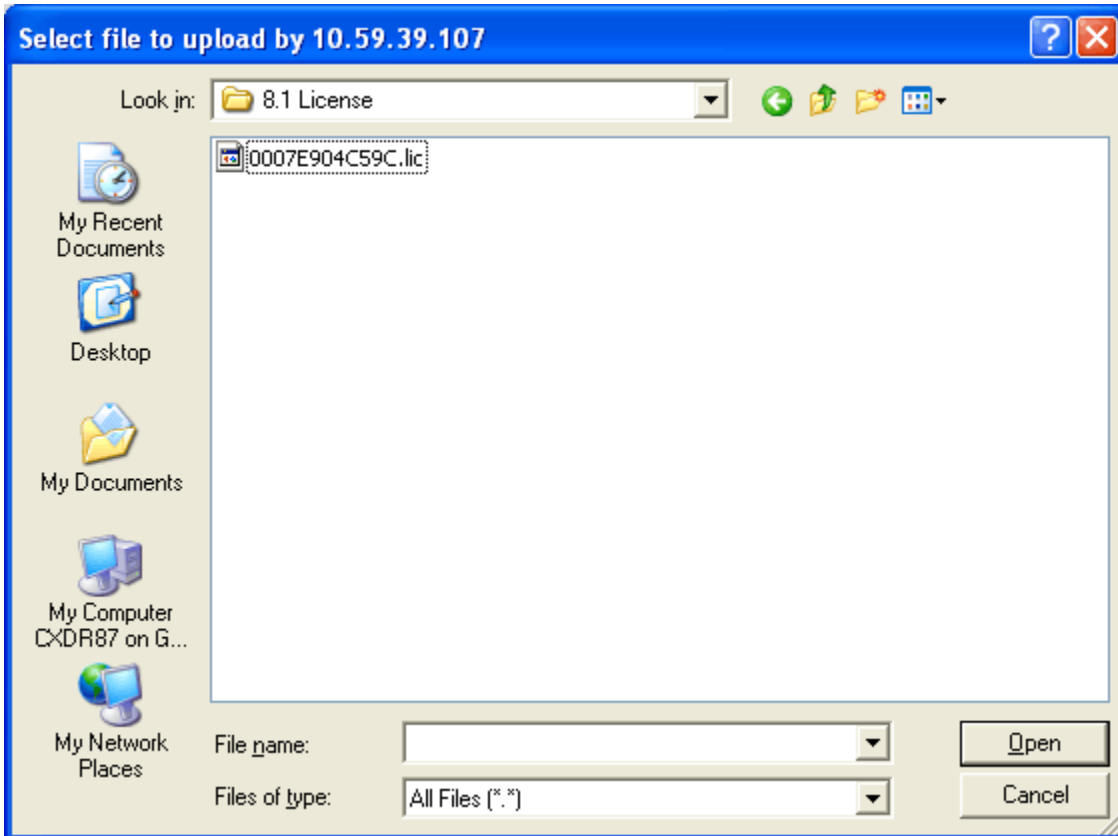


There are three ways to install a license:

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

### Using a License File

A license file contains information about your license. If you have a license file, select the **I have a license file** option and then click **Next**.

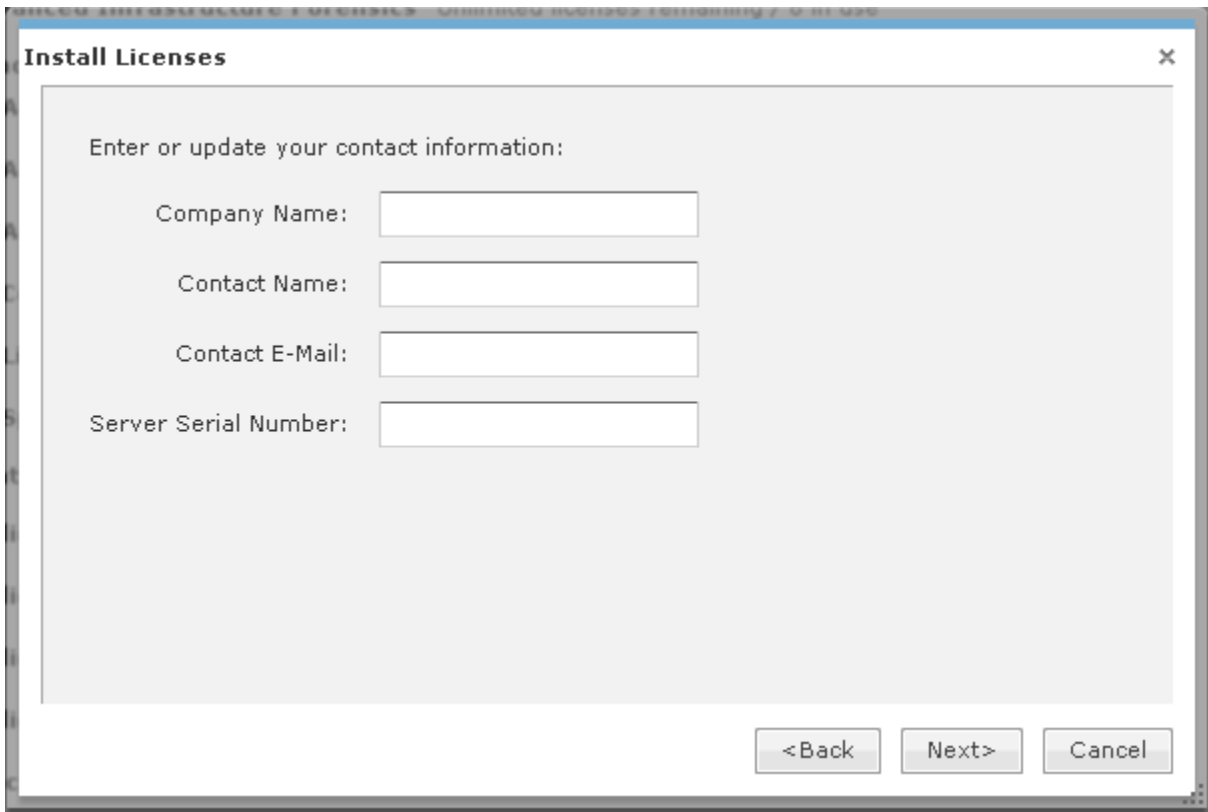


Navigate to the file and select it. Once you have selected the licensing file, click **Open**. The license information is updated.



**Using an Authorization Code**

If you have an authorization code, select the **I have an authorization code** option and then click **Next**.



The screenshot shows a dialog box titled "Install Licenses" with a close button (X) in the top right corner. The dialog contains the following text and input fields:

Enter or update your contact information:

Company Name:

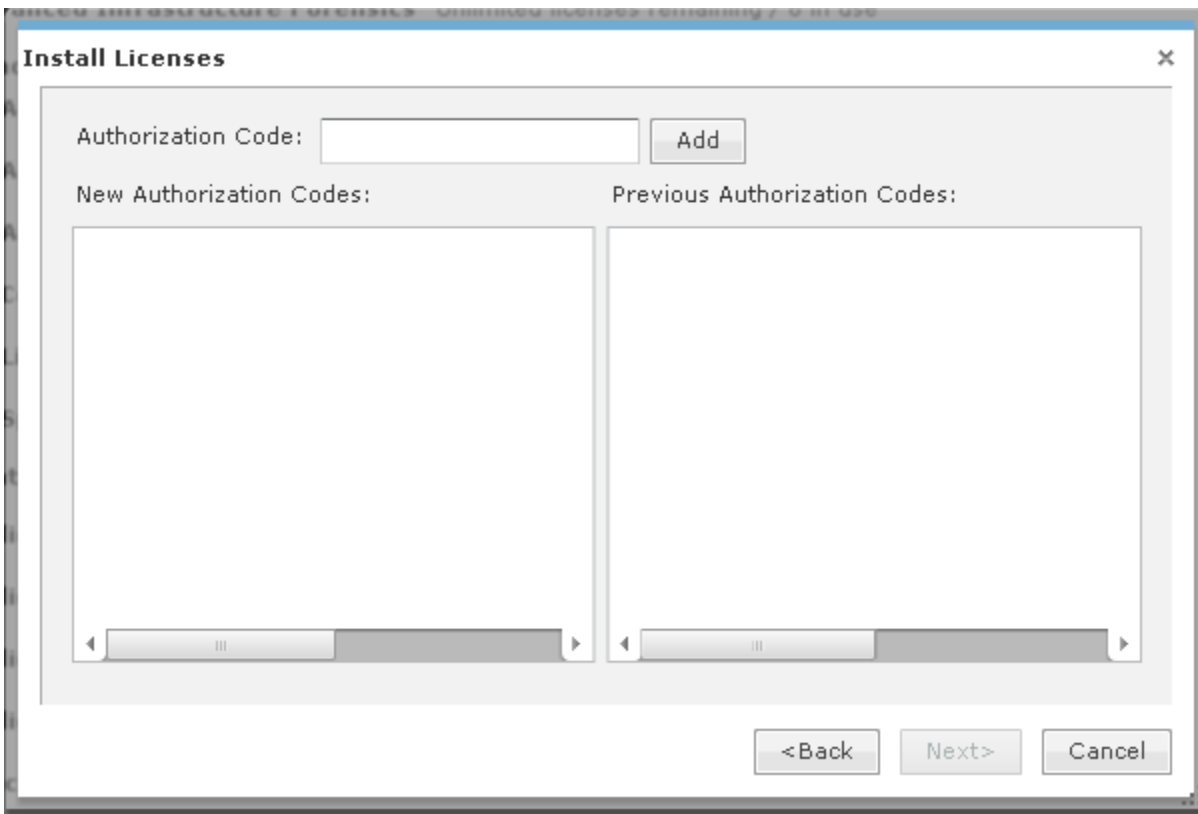
Contact Name:

Contact E-Mail:

Server Serial Number:

At the bottom right of the dialog, there are three buttons: "<Back", "Next>", and "Cancel".

Enter your company name, contact name, email address, and server serial number. Click **Next**.



Enter your authorization code and then click the **Add** button. The authorization code is added to the **New Authorization Codes** list. Click **Next** to continue. After the license is installed, the following message is displayed:

Licenses installed successfully

### **Requesting a License**

To request a license or to check if your requested license has been received:

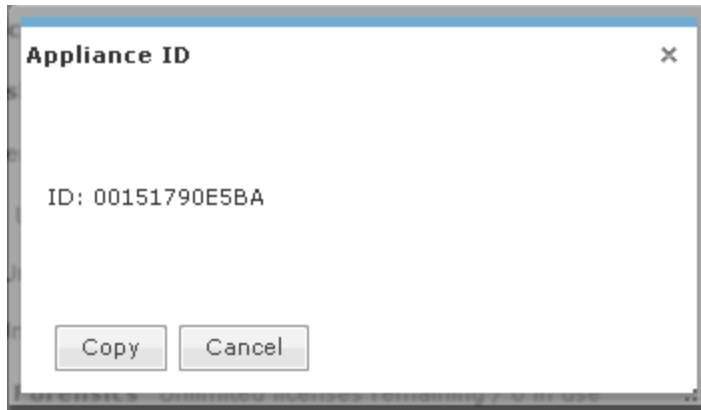
1. Select the I need to request a license or check on a pending request option and then click **Next**.
2. Enter your company name, contact name, email address, and server serial number.
3. Click **Next**. The system first checks to see if you have a pending license request. If a request has been made and the license has been received, it is installed. After installation, the following message is displayed:

Licenses installed successfully

4. If there are no pending request, follow the prompts to request a license.

### *Copy Appliance ID*

You can display the appliance's ID where you can copy it for later use. Click the **Appliance ID** button to display the ID.

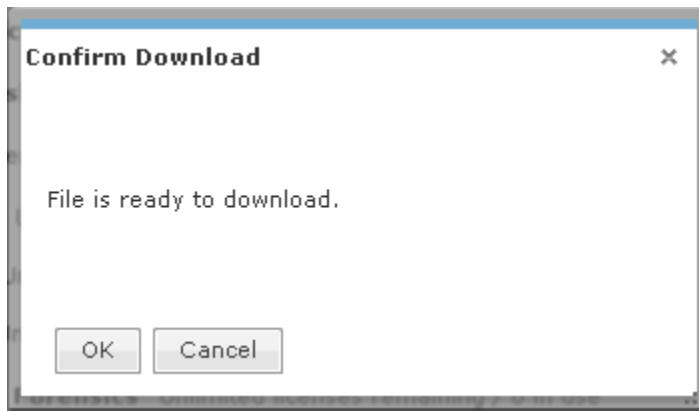


Once the ID is displayed, click the Copy button to copy the ID.

### *Download Appliance Keys*

You can download appliance keys to your workstation from the **Licenses** window. Follow these steps to download appliance keys:

1. Click the **Appliance Keys** button.



2. Click **OK**.
3. Navigate to the location where you want to save the appliance key file.
4. Click the **Save** button.

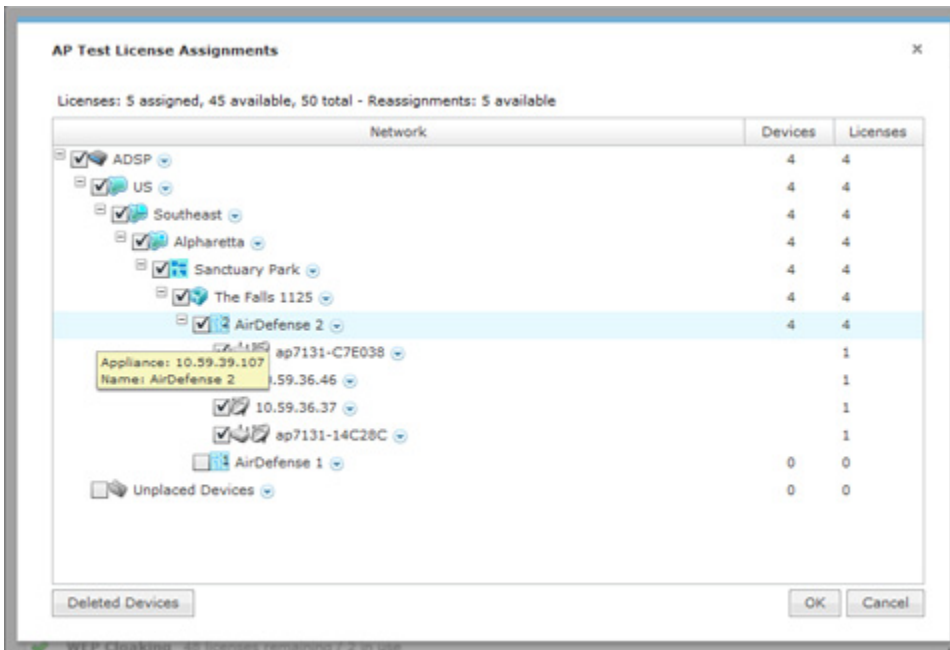
### *License Assignments*

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

✓ **NOTE** Once you assign a fixed license to a device, you cannot move it to another device.

### View License Assignments

To view license assignments, click the **License Assignments** link. The **License Assignments** window displays.




The following information is available:

- Total number of licenses
- Number of licenses assigned
- Number of licenses available
- Number of licenses available for reassignment
- List of licenses assigned to devices.

### Assigning a License to a Device

This feature only allows you to assign a fixed license to a device. To do so, follow these steps:

1. Select a fixed license by clicking on the license name.
2. Click the **License Assignments** link. The **License Assignments** window displays.
3. Use the **Open Tree**— icon to open tree levels until the device that you want to assign a license to is displayed.
4. Click the checkbox for the device to place a checkmark in the checkbox.
5. Click the **OK** button. The fixed license is assigned to the device.

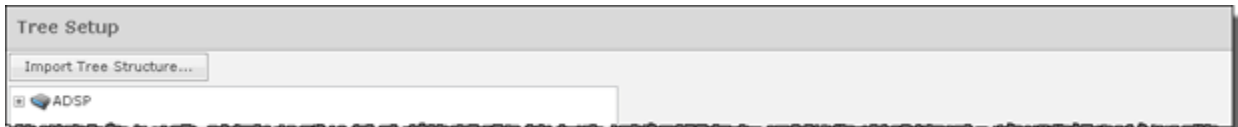
Open tree levels until the device that you want to assign a license to is displayed. Then, select the checkbox for the device.

## 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.


By default, your appliance is named ADSP. You add to your network tree starting at the appliance level. To begin defining your network tree, select (highlight) ADSP and then click the **add child** link on the right side of the highlighted area. A popup menu displays with a list of available network levels with the highest level at the top of the menu.



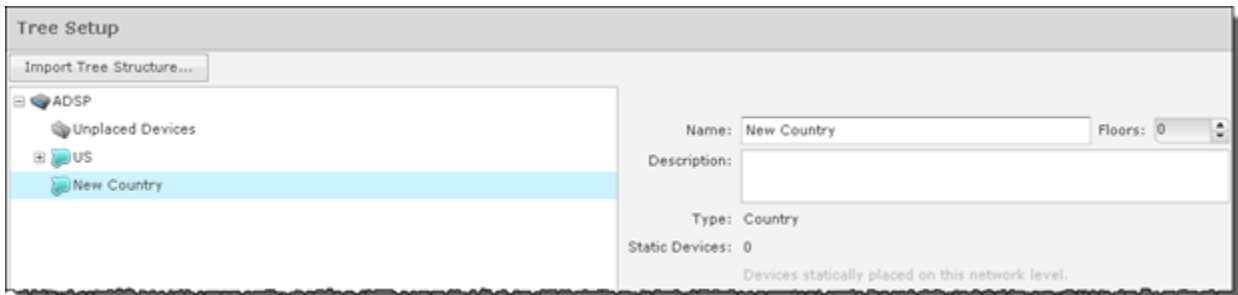
### Create Network Levels

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.

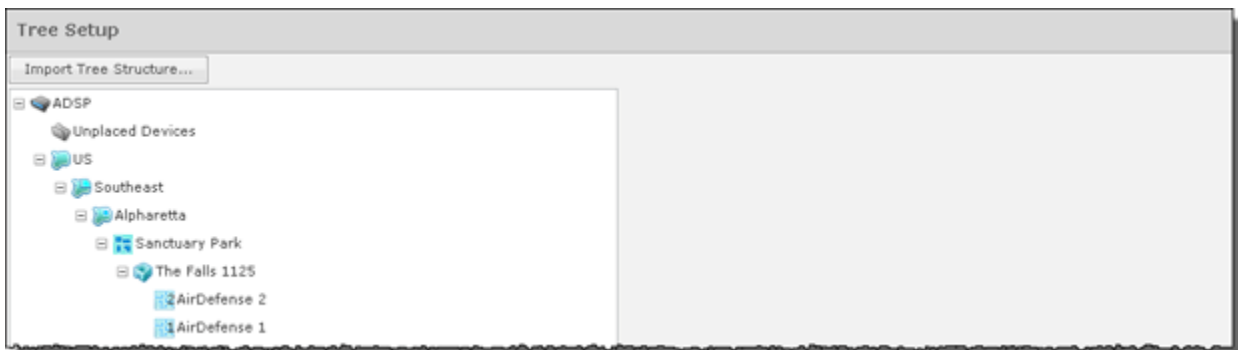
- ✓ **NOTE** The menu will only display the network level that is available at the selected level. You cannot add a network level that is higher up in the network tree.

Click the network level that you want to add. The new level will be hidden under the parent level. Click the **Expand-Collapse**  button next to the parent to reveal the new network level. Then, select the folder representing the new level.

- ✓ **NOTE** If the parent of the new level already contain Sensors, you cannot add a new level to it.



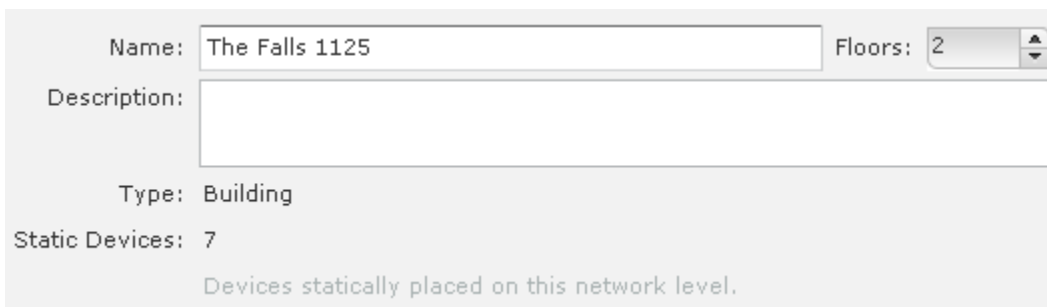
You can now name your new network level and give it a description. The name and description can be changed at any time. Repeat this process until you have defined your network tree.



You can delete a network level by selecting (highlighting) it and then clicking the **Delete**-X button on the right side of the highlighted area. A network level may not be deleted if contains static devices. Also, if the network level is the last level for an appliance, it may not be deleted.

### Add Floors

Notice in the previous screenshot there are two floors (AirDefense 1 and AirDefense 2) under the area (The Falls 1125). Floor numbers are displayed inside the Floor icon. You can add floors by selecting the building and then increasing the floor number using the **Floors** field.



You can delete a floor by decreasing the floor number. The last floor is always deleted first.

### *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.

You can edit existing tree structures using the **Import Tree Structure** button. Importing new CSV files does not replace an existing tree structure, instead the commands add or delete at the end of an import line can be used to incrementally add or remove scope levels from the existing tree structure.

The add and remove commands must be added to each line, separated by a comma, after the Path entry.

#### Example:

```
folder,localhost,The Falls 1125,,Building,,US/Southeast/Alpharetta/Sanctuary Part/The Falls 1125/Floor 2,add
folder,localhost,The Falls 1125,,Building,,US/Southeast/Alpharetta/Sanctuary Part/The Falls 1125/Floor 3,delete
```



**NOTE** The **add** command is assumed when neither **add** or **delete** is used in a comma delimited file, and **add** is included in the default exportable CSV file.

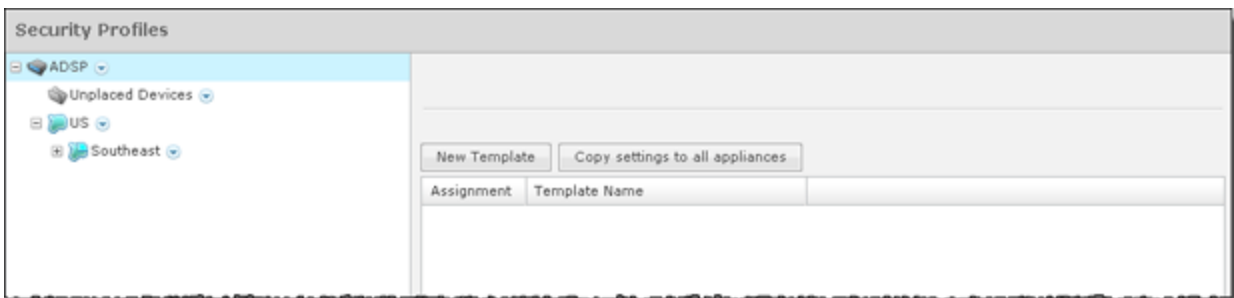
The path to the new folder must be present in the existing tree or be previously defined in the import file. For example, in the previous example, the path US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125 must already exist. Here is how you define that path:

```
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
```

Once you have finished building your network tree, click the **Apply** button to save your changes. This applies even when importing Auto-Placement Rules with the **Import Tree Structure** button. You may click the **Reset** button to revert back to your previous network tree configuration.

## Security Profiles

Security Profiles define the security configurations of sanctioned wireless clients on your wireless LAN.



When a Security Profile is applied to your system, if the security thresholds for that profile are exceeded, a security alarm is generated. This allows you to monitor network security issues and address them in a timely manner. If there are no Security Profiles applied to your system, no security alarms are generated.



Existing profiles are displayed in the window below the row of buttons.

New Template		Copy settings to all appliances
Assignment	Template Name	
<input type="checkbox"/>	Security-Corporate	
<input type="checkbox"/>	Security-Guest_MotorolaAD	
<input type="checkbox"/>	Security_Profile-ADralfenator	

You can edit, copy or delete any selected (highlighted) profile by clicking the appropriate link.

<input type="checkbox"/>	Security-Guest_MotorolaAD	( <a href="#">Edit</a>   <a href="#">Copy</a>   <a href="#">Delete</a> )
--------------------------	---------------------------	--

All profiles have three tabs that are used to set security threshold policies for your system.

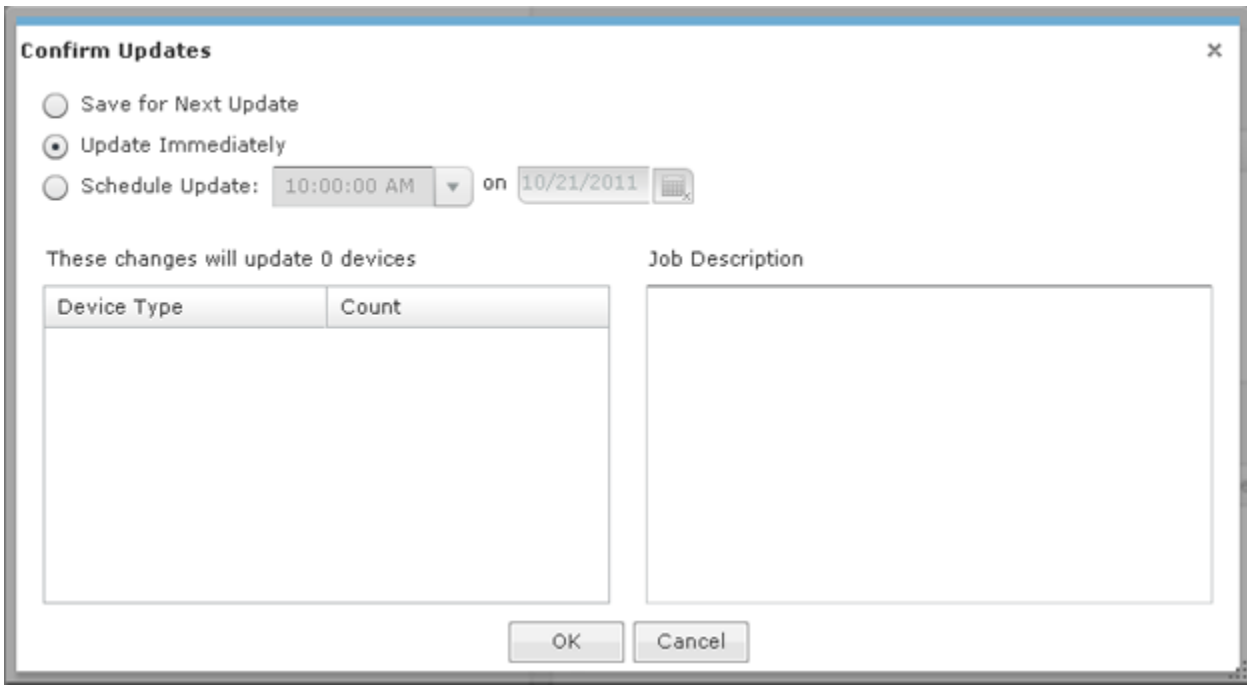
- General—Names your Security Profile and specifies whether or not you want to:
  - Allow unsanctioned wireless clients.
  - Allow SSID broadcast to be seen in the beacon.
  - Enable wireless client isolation.
- Privacy—Enables privacy monitoring for:
  - Base 802.11 authentication (Open or Shared)
  - 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.

To copy or edit a profile, select (highlight) the Security Profile, click the **Copy** or **Edit** link, and then make changes in any of the three tabs. Click **OK** to save your changes.

The **Copy settings to all appliances** button will copy the defined Security Profiles and all profile assignments to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your additions (changes). A confirmation overlay is displayed.



The image shows a 'Confirm Updates' dialog box with the following elements:

- Three radio buttons: 'Save for Next Update', 'Update Immediately' (selected), and 'Schedule Update: 10:00:00 AM on 10/21/2011'.
- A text label: 'These changes will update 0 devices'.
- A table with two columns: 'Device Type' and 'Count'.
- A text area labeled 'Job Description'.
- Two buttons at the bottom: 'OK' and 'Cancel'.

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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to Security Profiles are treated as jobs and are included in **Job Status** under **Device Monitoring**. The description supplied in the confirmation helps identify jobs.

Click the **Reset** button to discard any additions (changes).

### *Adding a New Profile*

Profiles are built using a template. Click the **New Template** button to add a new profile. Then, define your Security Profile using the **General**, **Privacy**, and **Rates** tabs. Once you have defined your Security Profile, click **OK** to save your profile or **Cancel** to exit without saving the profile.

### General Tab

The **General** tab is where you name your Security Profile and specify whether or not you want to use certain functions.

The screenshot shows a window titled "Security Profile" with three tabs: "General", "Privacy", and "Rates". The "General" tab is active. It contains the following fields and options:

- Name:** A text box containing "New\_Security\_Profile0.3816672405".
- Applies to SSID:** An empty text box.
- Preferences:**
  - Unsanctioned Wireless Clients:**
    - Do not allow access
    - Allow access
  - SSID Broadcast in Beacon:**
    - Do not allow broadcast
    - Allow broadcast
  - Wireless Clients:**
    - Enforce Isolation
    - Allow communication

At the bottom right, there are "Save" and "Cancel" buttons.

The **Name** field specifies the profile name. If you are adding or copying a Security Profile, ADSP gives the profile a default name beginning with `New_Security_Profile` and ending with a system generated number. You should change the default name to one that is more appropriate to its function. Once you save your profile, you cannot change the name.

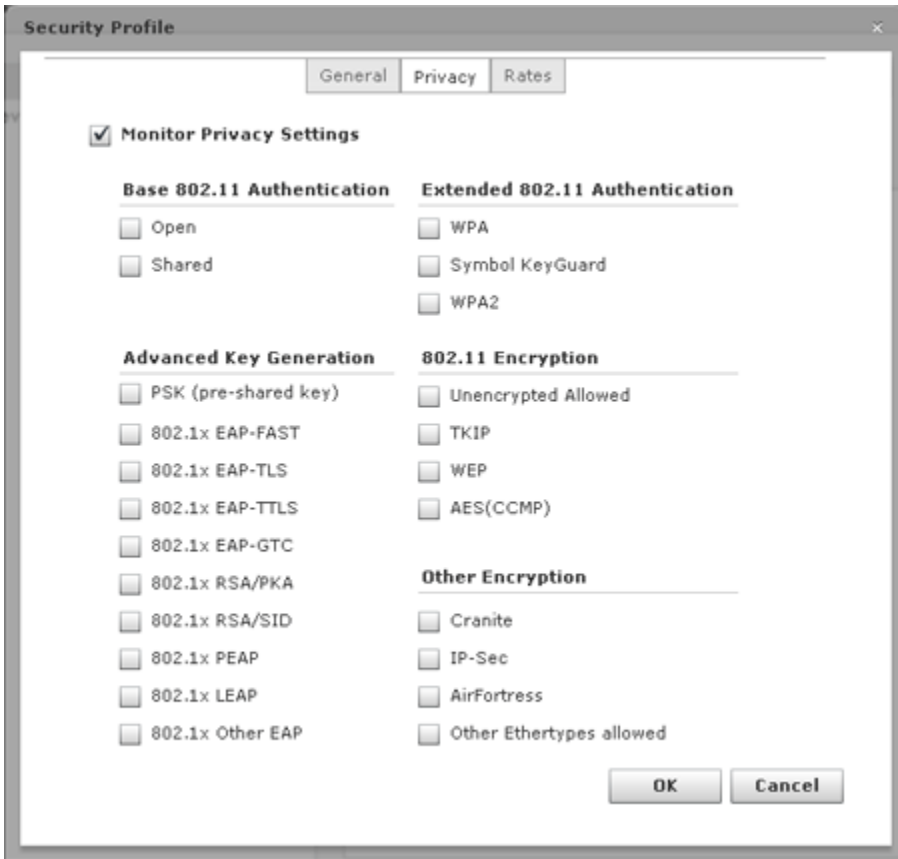
The **Applies to SSID** field specifies a SSID that the Security Profile applies to. This must be a valid SSID used in your system.

The **Preferences** are:

Preference	Description
Unsanctioned Wireless Clients	Choose to allow unsanctioned Wireless Clients or not to allow unsanctioned Wireless Clients in your system.
SSID Broadcast in Beacon	Choose to allow the BSS SSID to be broadcast in its beacon or not to allow the BSS SSID to be broadcast in its beacon. SSIDs are not passwords. Many BSSs allow their SSIDs to broadcast by default.
Wireless Clients	Choose to allow Wireless Clients to be isolated in your system or allow Wireless Clients to communicate in your system.

**Privacy Tab**

The **Privacy** tab contains options you can use to enter settings regarding transmission privacy.



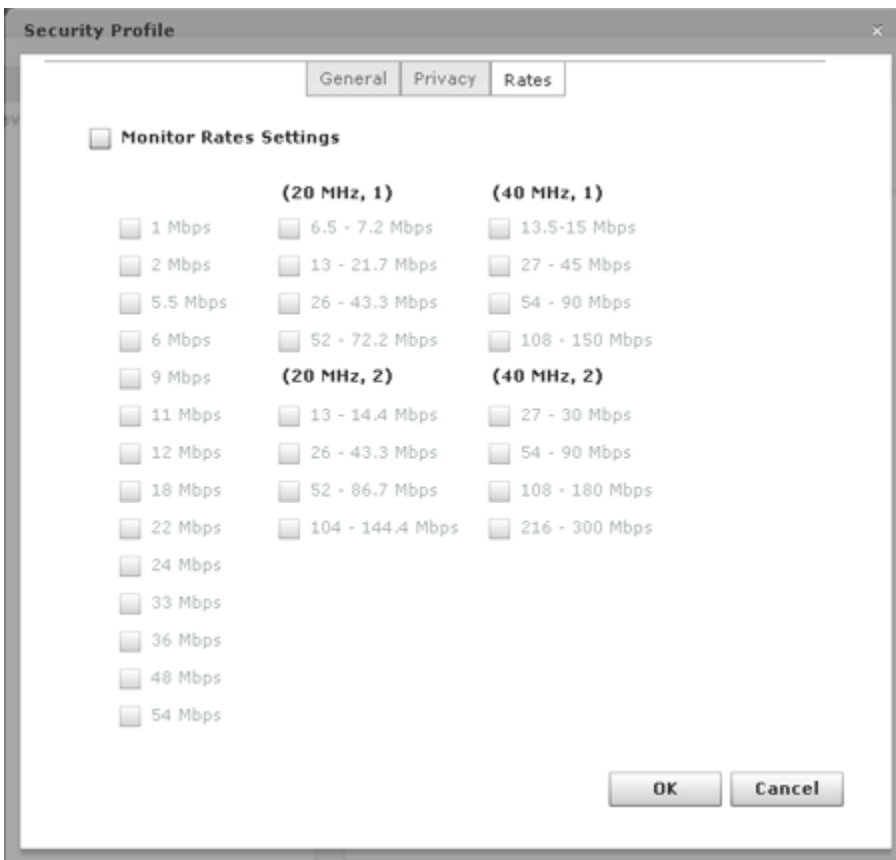
You must check the **Monitor Privacy Settings** checkbox to activate the functions. The functions are:

Function	Description
Base 802.11 Authentication	<p><b>Open</b>—When this checkbox is selected, open system authentication does not actually provide authentication; it only performs identity verification through the exchange of two messages between the initiator (Wireless Client) and the receiver (wireless access point).</p> <p><b>Shared</b>—When selected, shared key authentication provides authentication by verifying that an initiator has knowledge of a shared secret. Under the 802.11 standard, it is assumed that the shared secret is sent to the wireless access point over a secure channel that is independent of 802.11. In practice, the shared key authentication secret is manually distributed and typed.</p>
Extended 802.11 Authentication	<p><b>WPA</b>—Select to activate Wi-Fi Protected Access, which uses improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.</p> <p><b>WPA2</b>—Short for WiFi Protected Access 2, this checkbox enables the follow on security method to WPA for wireless networks that provide stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication.</p> <p><b>Symbol KeyGuard</b>—When this checkbox is selected, it activates Symbol KeyGuard authentication protocols, which is provided by Symbol.</p>
Advanced Key Generation	<p><b>PSK (preshared key)</b>—When selected, it activates the Pre-shared Key authentication.</p> <p><b>802.1x EAP-FAST</b>—When selected, it keys 802.1X EAP Flexible Authentication via Secure Tunneling.</p> <p><b>802.1x EAP-TLS</b>—When selected, it keys EAP Transport Level Security.</p> <p><b>802.1x EAP-TTLS</b>—When selected, it keys EAP Tunneled Transport Layer Security.</p> <p><b>802.1x EAP-GTC</b>—When selected, it keys EAP Generic Token Card.</p> <p><b>802.1x RSA/PKA</b>—When selected, it keys EAP RSA Public Key Authentication Protocol.</p> <p><b>802.1x RSA/SID</b>—When selected, it keys EAP RSA SecurID.</p> <p><b>802.1x PEAP</b>—When selected, it keys any 802.1X Protected Extensible Authentication Protocol (PEAP).</p> <p><b>802.1x LEAP</b>—When selected, it keys EAP Lightweight Extensible Authentication Protocol.</p> <p><b>802.1x Other EAP</b>—Keys any 802.1x EAP authentication/key distribution mechanism other than the types previously mentioned.</p>

Function	Description
802.11 Encryption	<p><b>Unencrypted Allowed</b>—Select this checkbox to allow no 802.11 encryption for wireless traffic.</p> <p><b>TKIP</b>—When selected, this enables the BSS to advertise support for Temporal Key Integrity Protocol (TKIP).</p> <p><b>WEP</b>—When selected, causes the BSS and Wireless Client to use WEP as their encryption policy.</p> <p><b>AES (CCMP)</b>—When selected, causes the BSS to advertise support for Advanced Encryption Standard (AES-CCMP).</p>
Other Encryption	<p><b>Cranite</b>—When selected, enables AP usage of Layer 3 Cranite encryption.</p> <p><b>AirFortress</b>—When selected enables AP usage of Layer 3 Airfortress encryption.</p> <p><b>IP-Sec</b>—When selected, enables AP usage of Layer 3 IP security protocol as encryption.</p> <p><b>Other Ethertypes allowed</b>—When selected, enables AP usage of other Layer 3 encryption mechanism which is not specified here.</p>

**Rates Tab**

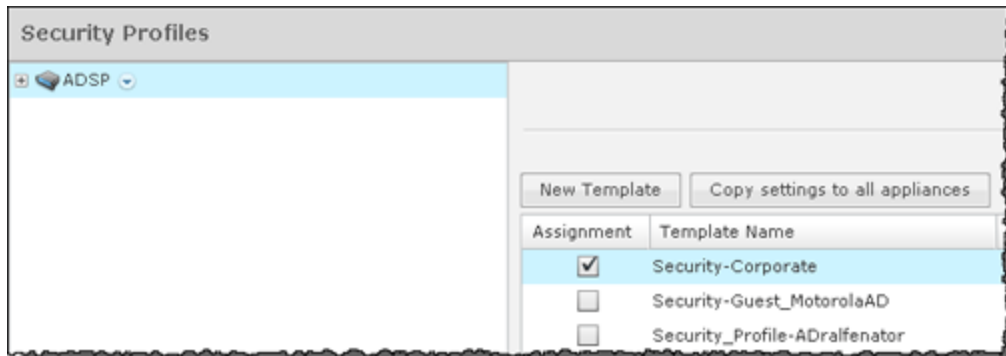
The **Rates** tab is where you can select transmit and receive data rates for BSSs to use.



You must check the **Monitor Privacy Settings** checkbox to activate the settings. Select the transmit and receive data rates you want BSSs to use.


### Applying an Existing Profile

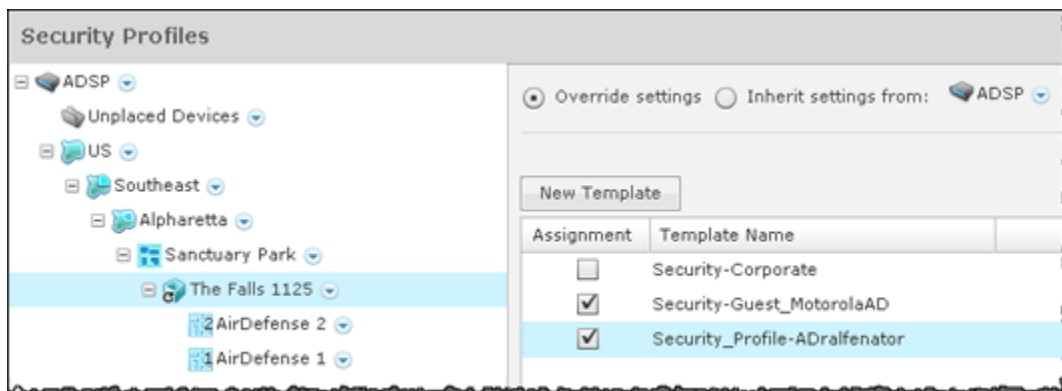
Once you have defined a Security Profile, to use it, you must apply it to your system.



✓ **NOTE** You may select multiple Security Profiles by checking more than one checkbox.

You should always apply a Security Profile at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Security Profile, you can apply that profile to that level. For example, in the above screen shot, the Security Profile for ADSP could be the **Security-Corporate** profile and then for a special case (in the following screen shot) you could override the Security Profile at the ADSP level and apply the **Security-Guest\_MotorolaAD** profile to the **The Falls 1125** network level.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

### 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.
- Adopted AP's discovered from a controller but without an applicable auto-placement rule should be placed in the same folder as the controller.
- 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.
  - 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.
  - 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.
  - 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.

Auto-Placement Rules

Auto-placement rules determine where devices will be placed in the network tree when they are imported.

Rules for: localhost

Buttons: Add, Delete, Move Up, Move Down, Import, Place Unplaced Devices

Sequence	Destination Folder
1	The Falls 1125 > AirDefense 2
2	The Falls 1125 > AirDefense 2
3	The Falls 1125 > AirDefense 1
4	The Falls 1125 > AirDefense 2
5	The Falls 1125 > AirDefense 2
6	The Falls 1125 > AirDefense 1
7	The Falls 1125 > AirDefense 2
8	The Falls 1125 > AirDefense 1

Place in Folder: localhost

Device Selection Rules:

Parameter	Value

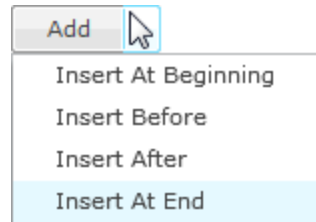
✓ **NOTE** Before you can define any Auto-Placement Rules, your network tree must already be configured.

Follow these steps to define a new auto-placement rule:



1. Click the **Add** button. The new rule is added to the list of rules and is automatically selected (highlighted).Add drop-down Menu

✓ **NOTE** You may optionally choose where you want the new rule to be placed by selecting a placement item from the drop-down menu. (**Inset At End** is the default.)



2. Using the **Place devices in scope** drop-down menu, select a scope to place devices when rule is applied.
3. Select one or more of the **Device Selection 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 ( <b>True</b> or <b>False</b> ). 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.

4. Click **Apply** to activate the new rule.

✓ **NOTE** You may click **Reset** to disregard any changes to the rules.

Auto-Placement Rules are applied in sequence. You should prioritize your rules so that the most important ones are applied first. Use the **Move Up** or **Move Down** buttons to arrange the list of rules.

You may delete a selected (highlighted) rule by clicking the **Delete** button.

Click the **Place Unplaced Devices** button to move unplaced devices to a network folder using the existing Auto-Placement Rules.

Click the **Apply** button to save any additions or changes. This applies even when importing Auto-Placement Rules with the **Import** button.

### ***Importing Auto-Placement Rules***

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:

```
autoplace ment_rule,server,Path,Network Address,IP Range,MAC Address,DNS Server,Uses DHCP,  
Device Name,Model Name,Firmware Version,Serial Number
```

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 *autoplace ment\_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).


### **Example:**

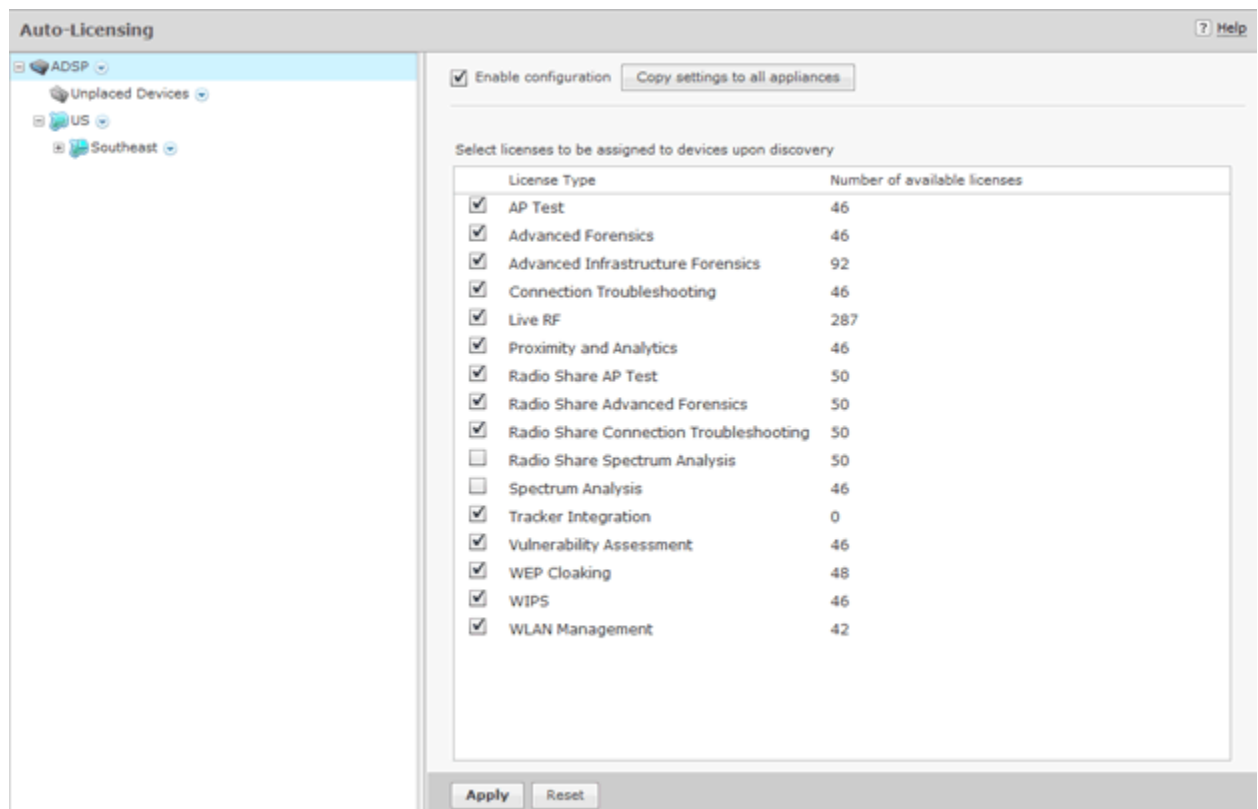
```
autoplace ment_rule,localhost,/USA/AutoPlacementTest/Floor 1,,172.17.17.0-172.17.17.19,,,,,6.0.196.0  
autoplace ment_rule,localhost,/USA/AutoPlacementTest/Floor 6,,172.17.15.0-172.17.15.200,,,,,6.0.196.0  
autoplace ment_rule,localhost,/USA/AutoPlacementTest/Floor 4,172.17.18.0/24,  
172.17.18.100-172.17.18.101,00:16:5d:20:47:60-00:16:5d:20:47:61,172.17.0.83,  
disable,BA-Sensor-240,M520,5.2.0.11.1234567890
```

## Auto-Licensing

Auto-Licensing allows you to define licensing rules for importing BSSs and Wireless Clients into your network system.

You may define Auto-Licensing at the appliance network level all the way down to the floor network level, but you should always define Auto-Licensing at the appliance level. Any network level below the appliance level will inherit the configuration. If you need to have a different configuration below the appliance level, use the **Override settings** option.

- ✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**  button to reveal the other levels.



The following rules apply:

- Only selected licenses (identified by a checkmark) are assigned.
- You can narrow the scope by selecting a network level from the network tree.
- A license will not be assigned if there are no available licenses.
- After a license assignment, the number of licenses are reduced accordingly.

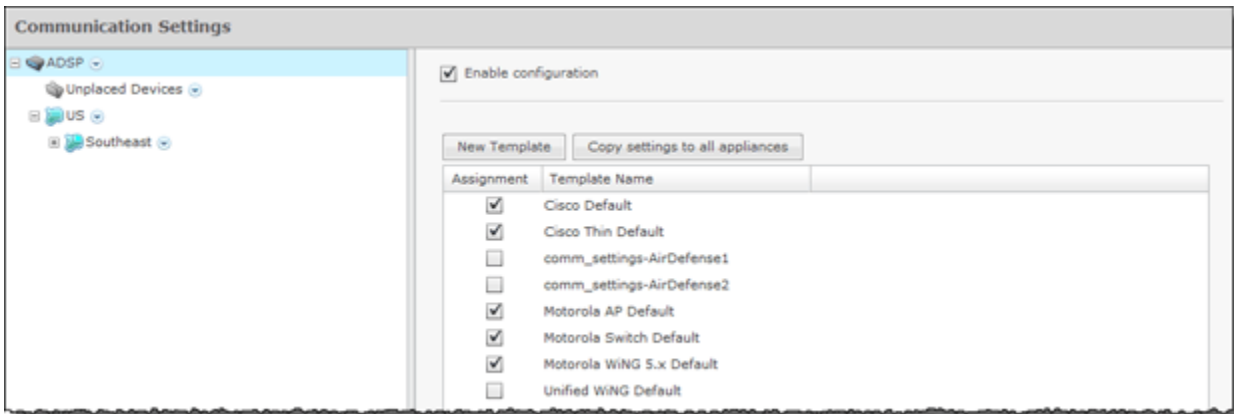
Click the **Apply** button to save your changes. A confirmation message **Successfully saved configuration** is displayed next to the **Reset** button. Click the **Reset** button to return rules as they were.

If there are multiple appliances in your system, once you have defined the device import rules, you can copy the configuration to all appliances in your system by clicking **Copy settings to all appliances**.

- ✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

## Communication Settings

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



Existing profiles are displayed in the window below the row of buttons. 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.

You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link. To copy or edit a profile, select (highlight) the Communication Settings Profile, click the **Copy** or **Edit** link, and then make your changes. Click **Save** to save your changes.

The **Copy settings to all appliances** button will copy Communication Settings to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

### *Adding a New Profile*

Click the New Template button to add a new profile using the Communication Settings Profile window. Then configure your communication settings using the following tabs:

- SNMP
- Console
- HTTP.

Once you have configured your communication settings, click **Save** to save your profile or **Cancel** to exit without saving the profile.

**SNMP Tab**

The **SNMP** tab is used to configure connectivity settings for SNMP devices.

The screenshot shows a dialog box titled "Communication Settings Profile" with a close button (X) in the top right corner. The "Profile Name" field contains "New\_comm\_settings\_pro". Below this are three tabs: "SNMP", "Console", and "HTTP", with "SNMP" selected. A checkbox labeled "Enable SNMP settings" is checked. The "Versions" dropdown menu is set to "V2". The "Read Community" and "Write Community" fields contain masked text (\*\*\*\*\*). A "Display Passwords" checkbox is unchecked. The "Port" field is set to "161", "Timeout in ms" is "300", and "Retries" is "3". The "User" field is empty. The "Auth Algorithm" dropdown is set to "MD5" and the "Privacy Algorithm" dropdown is set to "DES". Both have associated "Passphrase" fields that are currently empty. At the bottom are "Save" and "Cancel" buttons.

The following SNMP fields can be set:

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 <b>V2</b> or <b>V3</b> as the SNMP version used.
Read Community	Enter the Read Community string, which is used for the SNMP authentication. You also have an option to display passwords while typing them.
Write Community	Enter the Write Community string, which is used for the SNMP authentication.
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.

Field	Description
Auth Algorithm	The authentication algorithm is a SNMP V3 parameter that must match what is set on the device. The options are <b>MD5</b> , <b>SHA</b> and <b>None</b> . 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 <b>DES</b> , <b>3DES</b> , <b>AES128</b> , <b>AES192</b> , <b>AES256</b> and <b>None</b> . 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 screenshot shows a 'Communication Settings Profile' dialog box with the 'Console' tab selected. The 'Profile Name' is 'New\_comm\_settings\_pro'. There are three tabs: 'SNMP', 'Console', and 'HTTP'. Under the 'Console' tab, there is a checkbox for 'Enable Console settings' which is unchecked. Below this are three text input fields: 'User:', 'Password:', and 'Enable Password:'. To the right of the 'Password:' field is a checkbox for 'Display Passwords' which is also unchecked. Below these is a 'Protocol:' dropdown menu set to 'SSH' and a 'Port:' text input field set to '22'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

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. You also have an option to display passwords while typing them.
Enable Password	The enable password must be supplied in order to enter the enable mode.

Field	Description
Protocol	The protocol used to log into a device. The available options are <b>SSH</b> and <b>Telnet</b> .
Port	The port number that is used for communications. Port 22 is normally used but it may be another port number.

### **HTTP Tab**

The **HTTP** tab is used to supply login credentials for the devices that supply a web UI to interface with them.

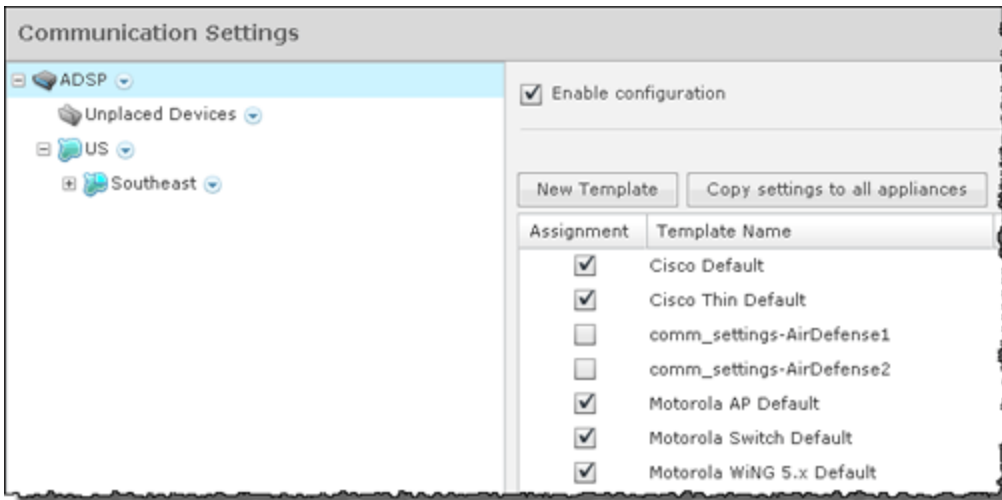
The screenshot shows a 'Communication Settings Profile' dialog box with the 'HTTP' tab selected. The 'Profile Name' is 'New\_comm\_settings\_pro'. There are three tabs: 'SNMP', 'Console', and 'HTTP'. Below the tabs, there is a checkbox for 'Enable HTTP settings' which is unchecked. Below that are fields for 'User:', 'Password:', 'Protocol:', and 'Port:'. The 'Protocol:' dropdown is set to 'HTTP' and the 'Port:' field contains '80'. There is also a 'Display Password' checkbox which is unchecked. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

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. You also have an option to display passwords while typing them.
Protocol	The protocol used to log into a device. The available options are <b>HTTP</b> and <b>HTTPS</b> .
Port	The port number that is used for communications. Port 80 is normally used but it may be another port number.

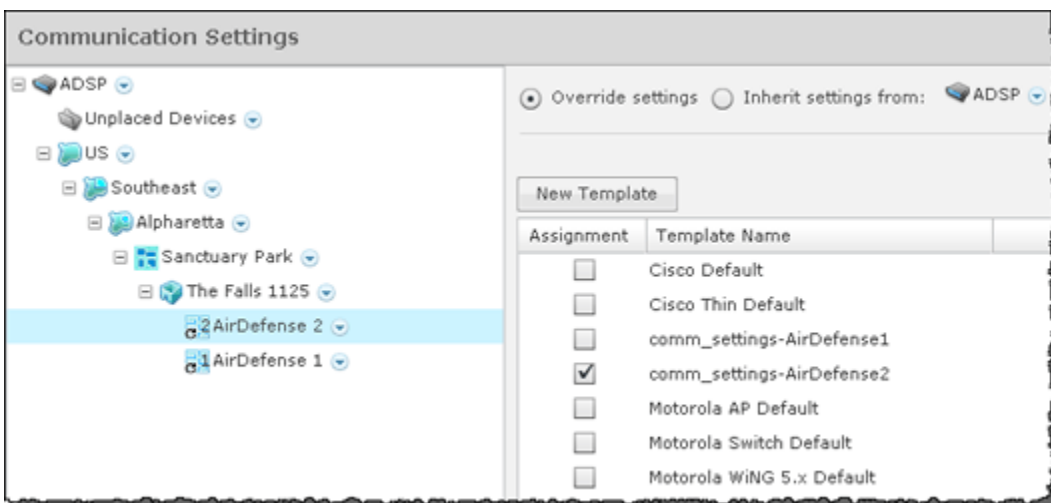
### Applying an Existing Profile

Once you have defined a Communication Settings Profile, to use it, you must apply it to your system. To configure Communication Settings, you must first select the **Enable configuration** checkbox to activate the settings.



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.

- ✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



- ✓ **NOTE** You may select multiple Communication Settings Profiles by checking more than one checkbox. If more than one profile is 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.

Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.



### ***Importing Communications Settings***

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

- Manually via **Menu > Import & Discovery** (see [Import and Discovery](#))
- Through a schedule via **Configuration > Appliance Platform > Import / Discover Devices** (see [Import / Discover Devices](#) to learn how to set up a schedule)
- Through your appliance CLI with the import command (see [Import / Discover Devices](#) for command syntax).

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 three 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)
- Profile name
- 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
```

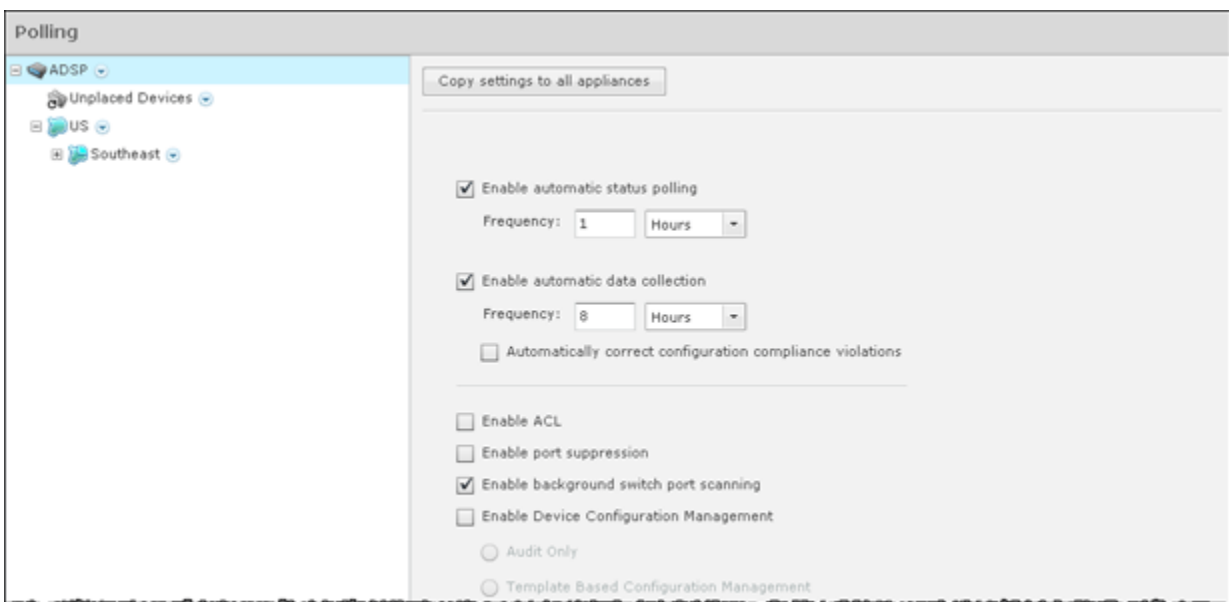
```
comm_settings_loc,ProfileName,/US/Southeast/AirDefense,folder
```



**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).

You may configure polling at the appliance network level all the way down to the floor network level, but you should always configure polling at the appliance level. Any network level below the appliance level will inherit the configuration. If you need to have a different configuration below the appliance level, use the **Override settings** option.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.

Select the **Enable automatic status polling** checkbox to enable polling for supported devices. When enabled, WMS automatically polls for device network status at an interval defined by the supplied **Frequency** value.

Each device model has an associated data collection profile which identifies the list of attributes collected periodically from the device. Select the **Enable automatic data collection** checkbox to collect these SNMP attributes at a **Frequency** defined by you. You can also select the **Automatically correct configuration compliance violations** checkbox to enable ADSP to correct configuration compliance violations by uploading the last approved configuration to the target device.

The following features can be enabled by selecting the appropriate checkbox:

- ACL
- Port suppression
- Background switch port scanning
- Device configuration management (must select Audit Only—configuration from device or Template Based Configuration Management—configuration from CLI profile).

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.


Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

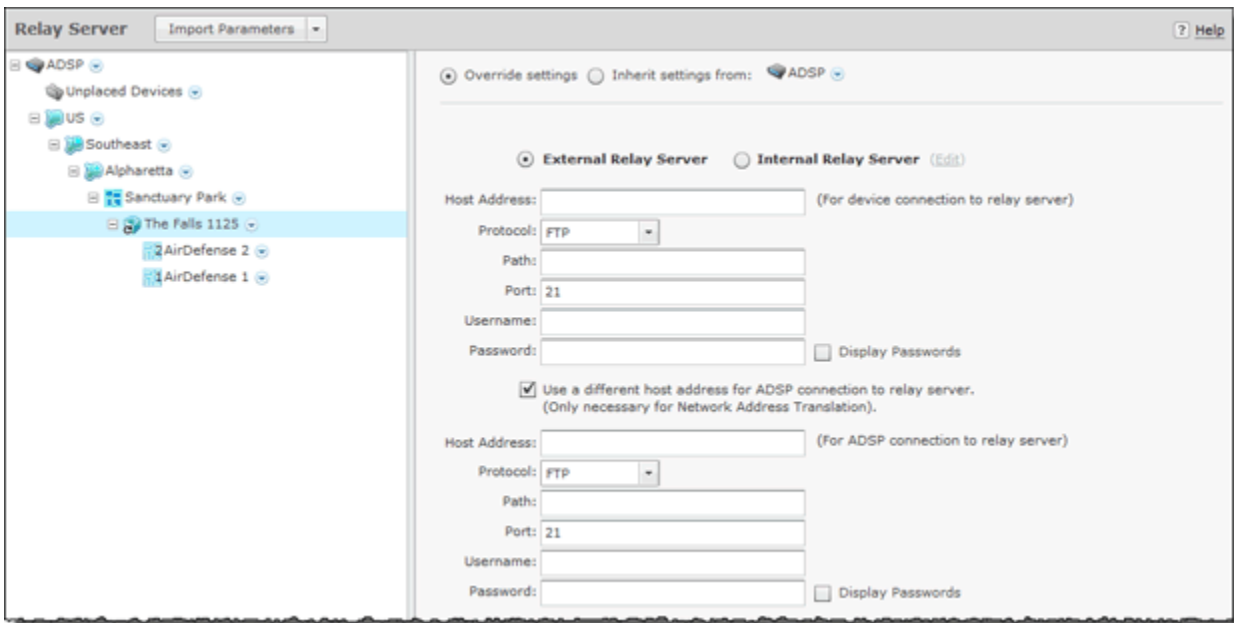
## Relay Server

✓ **NOTE** 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.

Define or update the Relay Servers used to access managed devices. Relay Servers are servers that devices access to fetch configuration, firmware, and provisioning information. Use the **Relay Server** screen to set the configurations of both the Device Relay and Appliance Relay Servers.

You may configure the Relay Servers at the appliance network level all the way down to the floor network level, but you should always configure the Relay Servers at the appliance level. Any network level below the appliance level will inherit the configuration. If you need to have a different configuration below the appliance level, use the **Override settings** option.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



Select **Enable configuration**. Then, decide if you want to use an internal or external relay server. For your convenience, ADSP has an internal relay server that you can use as your relay server (requires very little setup) or you can use your own external relay server where you will have to supply vital information for it to work with ADSP.

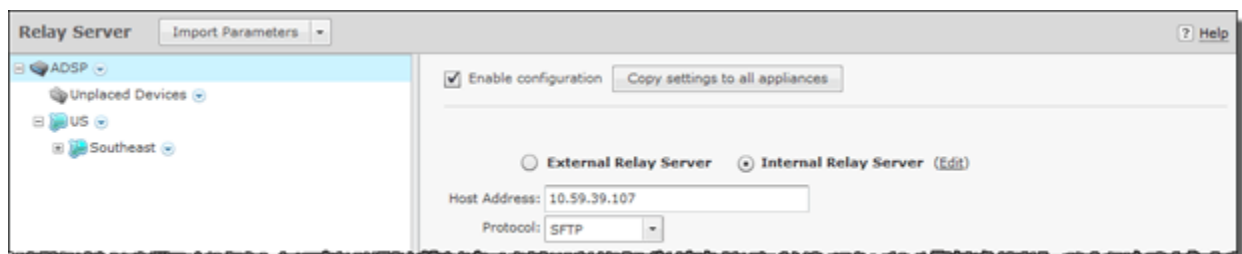
Click the **Apply** button to save any additions or changes. This applies even when importing Relay Server parameters with the **Import Parameters** button.

You can copy the Relay Server configuration to all your appliances by clicking the **Copy settings to all appliances** button.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

### ***Internal Relay Server***

Before ADSP can use the internal relay server, you must first enable the **Internal Relay Server** option.



You can edit the internal relay server initialization parameters by clicking the **Edit** link next to the **Internal Relay Server** radio button.

After selecting the **Enable configuration** checkbox, to use the internal relay server, select the **Internal Relay Server** radio button. Enter your host name or its IP address. Then, select a protocol to use (**FTP** or **SFTP**). Finally, click the **Apply** button.

### *External Relay Server*

After selecting the **Enable configuration** checkbox, to use an external relay server, select the radio button for the **External Relay Server**.

The default configuration uses the same credentials for downloading and uploading. Set the following values:

- 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.
- Select a protocol from the drop-down menu (**FTP**, **TFTP**, **SFTP**, **SCP**, **HTTP**, or **HTTPS**).
- Specify the **Path** ADSP uses to download information. You should either leave the path blank or use root (/).
- Specify the **Port** ADSP uses to connect to the External Relay Server.
- Enter the **Username** needed to update the External Relay Server used by ADSP.
- Enter the **Password** required to update the External Relay Server used by ADSP.

If you require a different upload relay server, select the **Use a different server for ADSP connection to relay server** checkbox. Another set of fields are displayed for the upload host. The fields are the same except you are supplying credentials for the upload host.

- ✓ **NOTE** The option to unsynchronized these configuration fields (download and upload) 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.

Enable configuration Copy settings to all appliances

External Relay Server  Internal Relay Server [\(Edit\)](#)

Host Address:  (For device connection to relay server)

Protocol:

Path:

Port:

Username:

Password:   Display Passwords

Use a different host address for ADSP connection to relay server.  
(Only necessary for Network Address Translation).

Host Address:  (For ADSP connection to relay server)

Protocol:

Path:

Port:

Username:

Password:   Display Passwords

Once you are finished, click the **Apply** button.

### ***Import Relay Server Information***

When using an external relay server, 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 two 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.

The **Import Parameters** button is a multifunction button. When the drop-down button is clicked, two other options are available: **Export Parameters** and **Get Template**. When one of these options is selected, it becomes the button. The **Export Parameters** button exports all the parameters to a file for you to use as an import file. The **Get Template** button displays a template that you can copy, paste the contents into an editor, and edit the contents to create an import file.

Things to Remember:

- Servers must be specified in pairs. You must specify a device connection and an ADSP connection in one entry.
- If the server information is the same, you still must enter information for both servers.
- 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
```

## 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.

Click the **Add** button to get started.

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 classified according to [Auto-Licensing](#).

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.

To set up a new import schedule, you must configure the settings and specify a schedule. Click **Apply** to save your device import schedule and add it to the device import list. Click **Reset** to discard any new changes/additions.

You can delete an scheduled import/discovery by selecting (highlighting) the schedule and then clicking the **Delete** button.

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 (also part of Appliance Platform) define the security configurations of sanctioned wireless clients on your wireless LAN. Refer to [Security Profiles](#) under Appliance Platform.

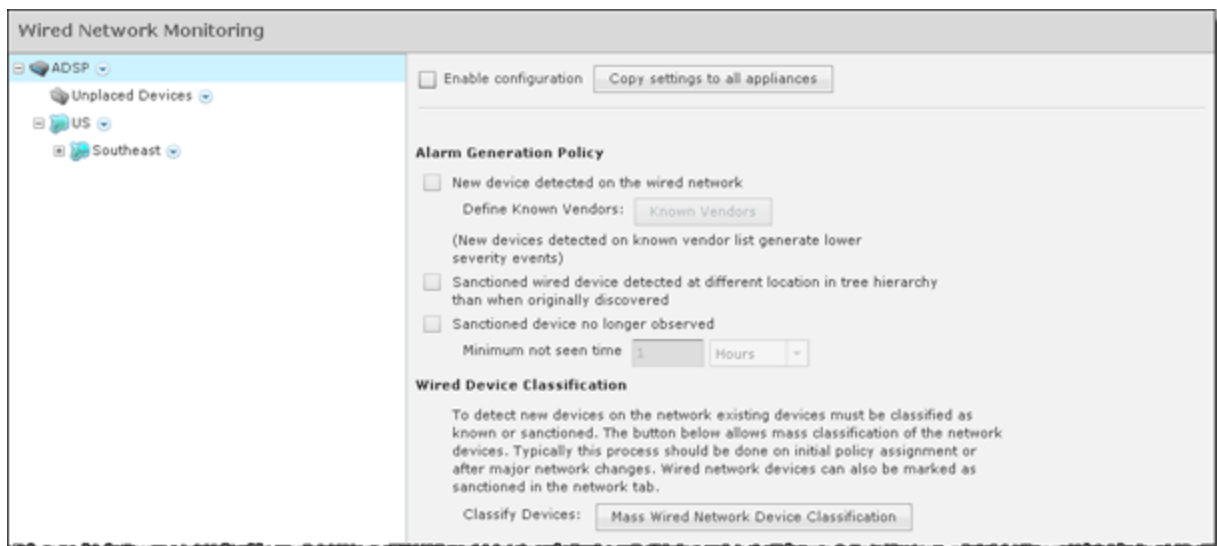
## Wired Network Monitoring

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

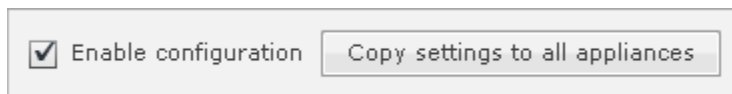
You can generate an alarm policy for your wired network by selecting any of the following conditions:

- 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.

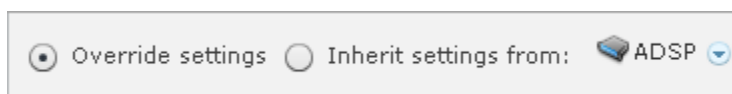
To detect new devices on your network, existing devices must be classified as sanctioned. The **Mass Wired Network Device Classification** button opens a dialog where you can sanction all or a selection of devices at one time. Typically, this process should be done when you initially configure policies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



To turn on **Wired Network Monitoring**, you should always enable it at the appliance level by selecting the **Enable configuration** checkbox. When you do, all the other network levels are also monitored.



Then, if you have a level that needs to be monitored using different settings, you can monitor that level by selecting the network level from the network tree, overriding the inherited Wired Network Monitoring (select **Override settings** radio button), and then defining different settings for Wired Network Monitoring.



**Generate Alarm Policy for New Devices**

It is a good practice, to have an alarm policy for new devices detected on your wired network. After enabling monitoring, select the New device detected on the wired network checkbox.

Enable configuration Copy settings to all appliances

---

**Alarm Generation Policy**

New device detected on the wired network  
 Define Known Vendors: Known Vendors

(New devices detected on known vendor list generate lower severity events)

To authorize all detected devices for the first time, or at any major infrastructure change, click on the **Mass Wired Network Device Classification** button.

Classify Devices: Mass Wired Network Device Classification

The **Sanction Devices** dialog opens.

**Sanction Devices**

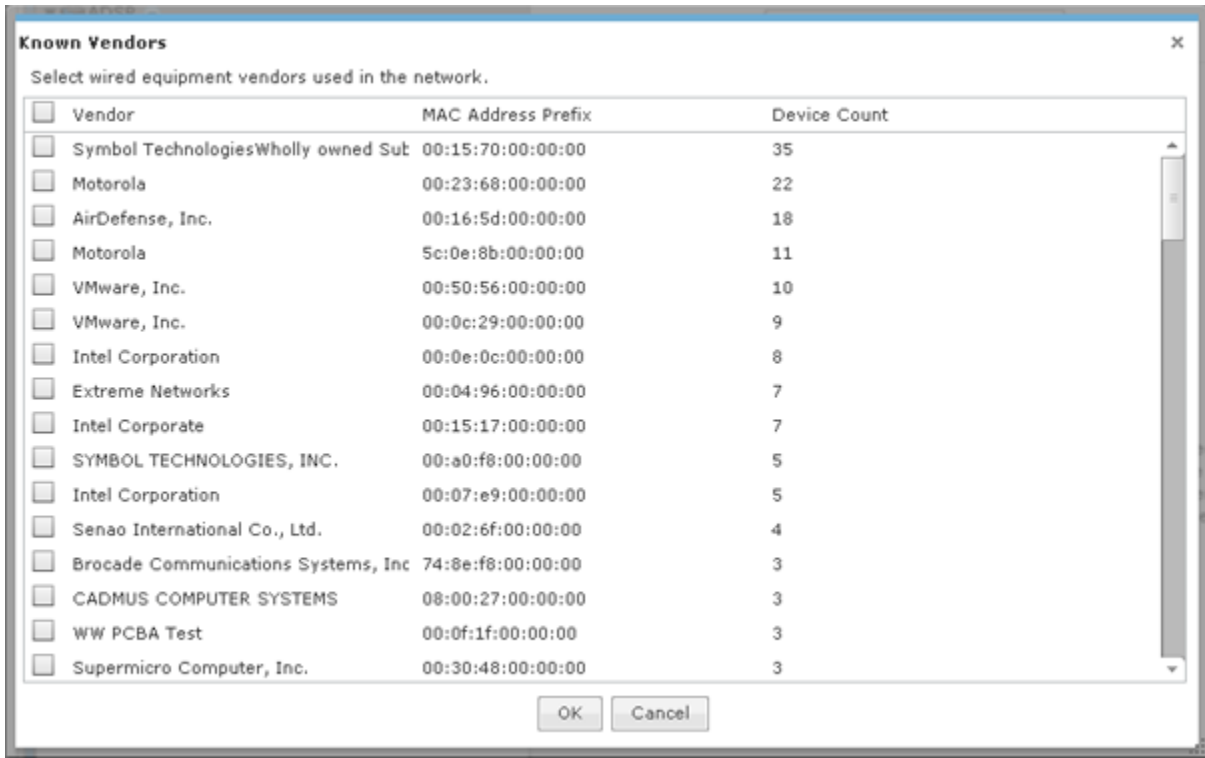
The selected devices will be sanctioned.

<input type="checkbox"/> Vendor	MAC Address Prefix	Device Count
<input type="checkbox"/> Symbol TechnologiesWholly owned Sub	00:15:70:00:00:00	35
<input type="checkbox"/> Motorola	00:23:68:00:00:00	23
<input type="checkbox"/> AirDefense, Inc.	00:16:5d:00:00:00	18
<input type="checkbox"/> Motorola	5c:0e:8b:00:00:00	11
<input type="checkbox"/> VMware, Inc.	00:50:56:00:00:00	10
<input type="checkbox"/> VMware, Inc.	00:0c:29:00:00:00	9
<input type="checkbox"/> Intel Corporation	00:0e:0c:00:00:00	8
<input type="checkbox"/> Extreme Networks	00:04:96:00:00:00	7
<input type="checkbox"/> Intel Corporate	00:15:17:00:00:00	7
<input type="checkbox"/> SYMBOL TECHNOLOGIES, INC.	00:a0:f8:00:00:00	5
<input type="checkbox"/> Intel Corporation	00:07:e9:00:00:00	5
<input type="checkbox"/> Senao International Co., Ltd.	00:02:6f:00:00:00	4
<input type="checkbox"/> APPLE COMPUTER INC.	08:00:07:00:00:00	3
<input type="checkbox"/> Brocade Communications Systems, Inc	74:8e:f8:00:00:00	3
<input type="checkbox"/> CADMUS COMPUTER SYSTEMS	08:00:27:00:00:00	3
<input type="checkbox"/> WW PCBA Test	00:0f:1f:00:00:00	3

OK Cancel

Select all the vendors you recognize as authorized and permanent for that site. (Help text is provided just above the **Mass Wired Network Device Classification** button.) Then, sanction devices detected at your site by clicking **OK**.

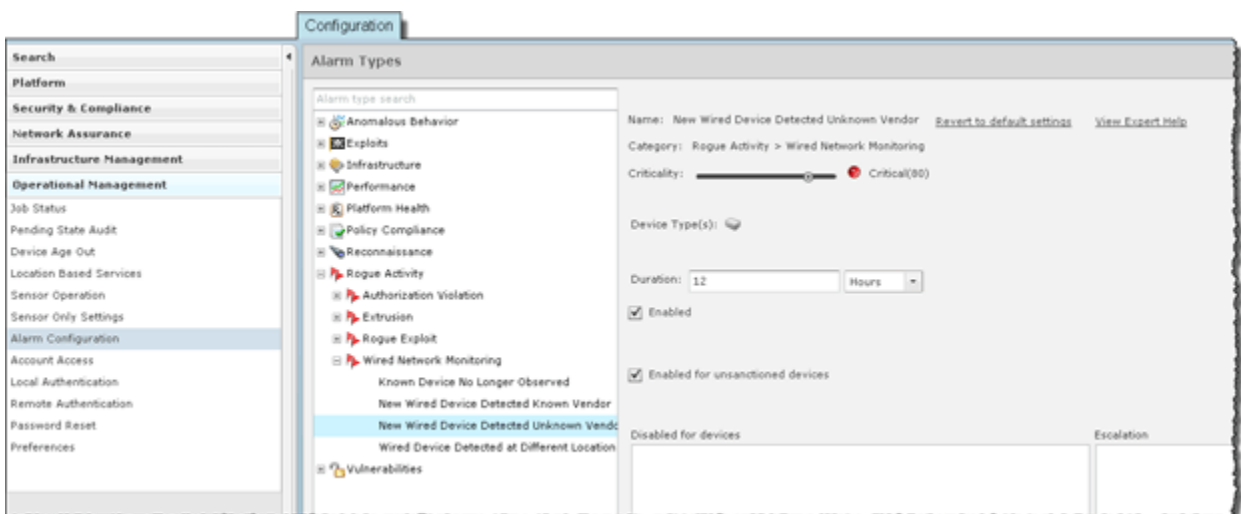
To have a finer control over alarms about new known vendor devices and new unknown vendor devices, you can utilize the Known Vendors classification tool. Click on the **Known Vendors** button to display a list of known vendors.



Select the approved vendors and click **OK**.

After configuring the Wired Network Monitoring options, click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

Once new devices are detected at your site, you will receive one of two alarms: New Wired Device Detected Known Vendor or New Wired Device Detected Unknown Vendor. Below is a screen shot of Alarm Configuration, where you can customize the criticality, duration, state and exception for each of the alarms.



## Network Assurance

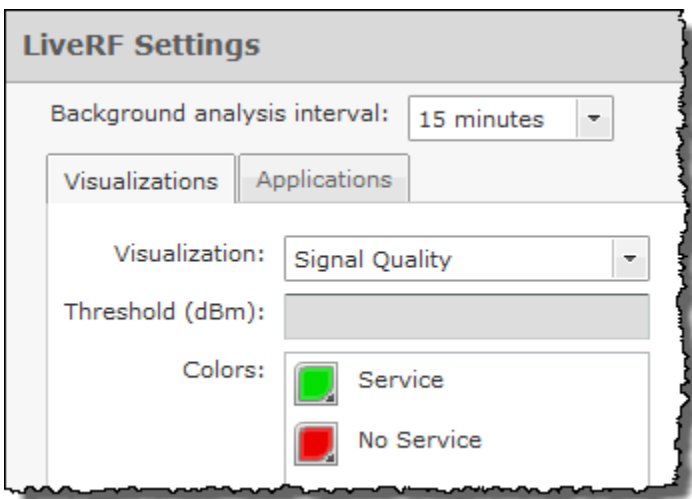
The Network Assurance category allows you to:

- 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.

### Live RF Settings

✓ **NOTE** A LiveRF license is required to access this feature.

Live RF provides a real-time snapshot of wireless coverage as well as performance. Live RF Settings are used to configure how Live RF is displayed and define Live RF applications.



The **Background analysis interval** drop-down allows you to set an interval for restarting background analysis. The options are:

- 1 minutes
- 15 minutes
- 60 minutes.

The **Visualizations** tab is used to change the visual aspects of LiveRF. The **Applications** tab is used to set options that allow you to determine if you have adequate coverage for your wireless network.























The **Check Synchronization** button is used to check all the appliances in your system to see if the Live RF Settings match. (The [Synchronize Accounts](#) topic has a good example of how the synchronization feature works.)





















✓ **NOTE** You must have a Central Management license in order to use the Check Synchronization feature.

Click the **Apply** button to save your additions (changes). Click the **Reset** button to discard any additions (changes).






















### Visualizations

Visualizations configure how Live RF heat maps are visually displayed. Each visualization contains items that are identified by a color. You can view the visualizations (shown below) by selecting one from the **Visualization** drop-down menu. While viewing a visualization, you can change the default color of an item by clicking on the color and then selecting a new color from the color chart. You may also change the threshold (if active) by typing in a new value.

Visualization	Default Colors
Signal Quality (Threshold inactive)	 Service  No Service
Coverage Hole (Threshold inactive)	 Service  No Service
Co-Channel Interference (default Threshold = -120)	 No Interference  Interference
Signal Coverage (Threshold inactive)	 Above -10 dBm  -20 to -10 dBm  -30 to -20 dBm  -40 to -30 dBm  -50 to -40 dBm  -60 to -50 dBm  -70 to -60 dBm  -80 to -70 dBm  Below -80 dBm
Signal To Interference (Threshold inactive)	 Above 30  25 to 30  20 to 25  15 to 20  10 to 15  5 to 10  Below 5

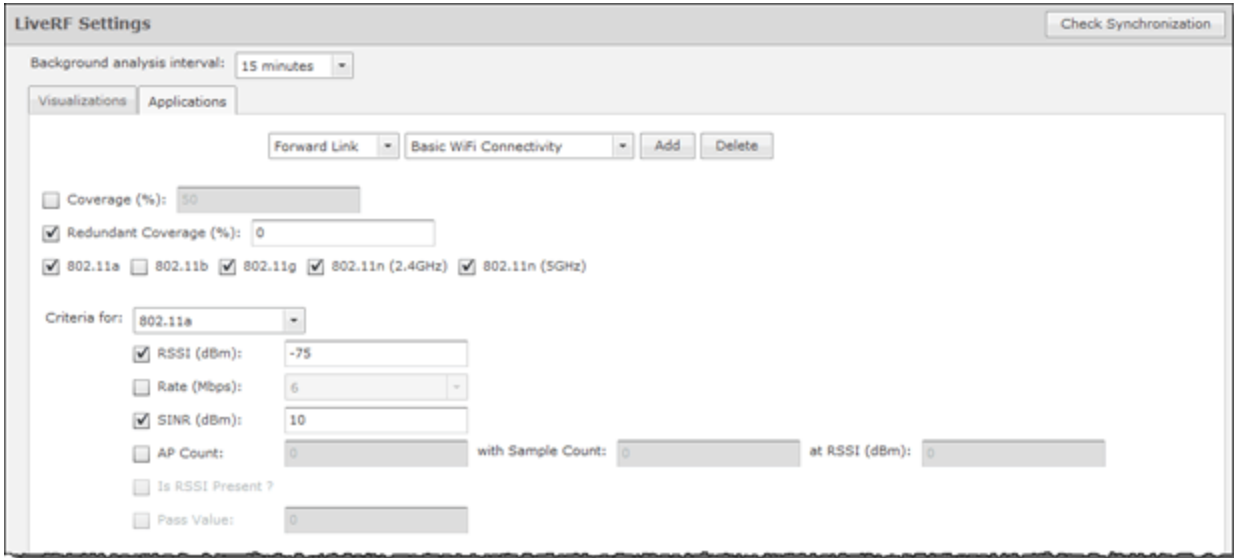
Visualization	Default Colors
Peak Data Rate (Threshold inactive)	<ul style="list-style-type: none"> <li> Above 100 Mbps</li> <li> 54 to 100 Mbps</li> <li> 48 to 54 Mbps</li> <li> 36 to 48 Mbps</li> <li> 25 to 36 Mbps</li> <li> 18 to 25 Mbps</li> <li> 12 to 18 Mbps</li> <li> 11 to 12 Mbps</li> <li> 9 to 11 Mbps</li> <li> 6 to 9 Mbps</li> <li> 5.5 to 6 Mbps</li> <li> 2 to 5.5 Mbps</li> <li> 1 to 2 Mbps</li> <li> Below 1 Mbps</li> </ul>
Noise (Threshold inactive)	<ul style="list-style-type: none"> <li> Above -50 dBm</li> <li> -60 to -50 dBm</li> <li> -70 to -60 dBm</li> <li> -80 to -70 dBm</li> <li> -90 to -80 dBm</li> <li> Below -90 dBm</li> </ul>



Visualization	Default Colors
Coverage Overlap (Threshold inactive)	 Good Overlap  Partial Overlap  Insufficient Overlap
Channel Coverage (Threshold inactive)	 Best coverage  2nd best coverage  3rd best coverage  4th best coverage  5th best coverage  6th best coverage  7th best coverage  8th best coverage  9th best coverage  10th best coverage  11th best coverage  12th best coverage  13th best coverage  14th best coverage
Service Counts (Threshold inactive)	 More than two devices  Two devices  One device  No devices

### *Applications*

Live RF uses applications to determine if you have adequate coverage for your wireless network. The applications have options that you can set to help you make this determination.



The screenshot displays the 'LiveRF Settings' window with the 'Applications' tab selected. At the top right, there is a 'Check Synchronization' button. Below the title bar, the 'Background analysis interval' is set to '15 minutes'. The 'Applications' section includes a 'Forward Link' dropdown menu, a 'Basic WiFi Connectivity' dropdown menu, and 'Add' and 'Delete' buttons. The 'Coverage (%)' is set to 50, and 'Redundant Coverage (%)' is set to 0. Underneath, several checkboxes are visible for different standards: 802.11a, 802.11b, 802.11g, 802.11n (2.4GHz), and 802.11n (5GHz). The 'Criteria for:' dropdown is set to '802.11a'. The criteria list includes: 'RSSI (dBm): -75' (checked), 'Rate (Mbps): 6' (unchecked), 'SINR (dBm): 10' (checked), 'AP Count: 0' (unchecked), 'Is RSSI Present?' (unchecked), and 'Pass Value: 0' (unchecked). There are also fields for 'with Sample Count: 0' and 'at RSSI (dBm): 0'.

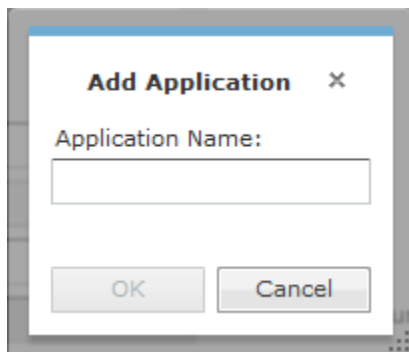
The default applications are:

- Basic WiFi Connectivity
- Mobile Handsets
- Video Surveillance
- Wireless VoIP Handsets
- Location Tracking.

To set the options for each application, select the application from the drop-down menu at the top of the **Applications** tab next to the **Add** button. When an application is selected, you can select the options that you want to use and set an values for the options. The options are:

Option	Description
Coverage (%)	Specifies the percentage of your wireless network that you consider your network is covered.
Redundant Coverage (%)	Specifies the percentage of your wireless network that you consider your network is covered redundantly.
Protocol used	<p>Specifies the protocols that you want to use to consider your network is covered. The choices are: <b>802.11a</b>, <b>802.11b</b>, <b>802.11g</b>, <b>802.11n (2.4 GHz)</b>, and <b>802.11n (5Ghz)</b>. For every protocol you select, that protocol is added to the <b>Criteria for</b> drop-down menu. You can then select a protocol from the drop-down menu and select the following options to use with that protocol:</p> <ul style="list-style-type: none"> <li>• <b>RSSI</b>—When selected, specify the RSSI value in dBm that you consider acceptable for the selected protocol.</li> <li>• <b>Rate</b>—When selected, specify the rate that you consider acceptable for the selected protocol.</li> <li>• <b>SINR</b>—When selected, specify the SINR value in dBm that you consider acceptable for the selected protocol.</li> <li>• <b>AP Count</b>—When selected, specify the number of APs that you consider acceptable for the selected protocol. Also, specify an acceptable RSSI value for the APs.</li> </ul>

You can add additional applications that you deem necessary by clicking the **Add** button. You will be prompted to enter an application name.

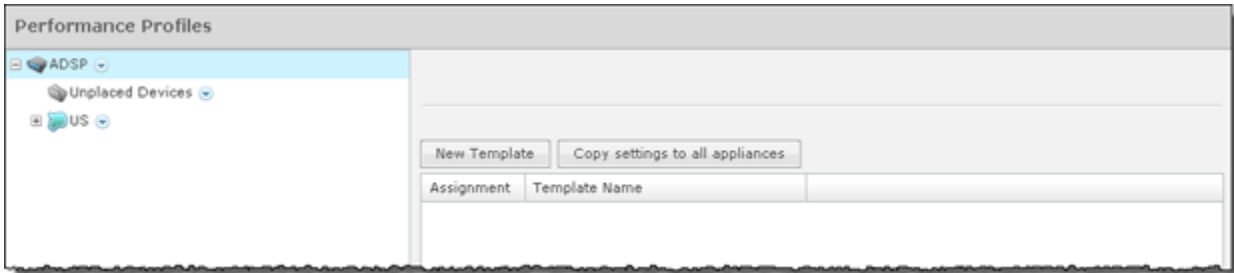


Enter an application name and click **OK** to add it to the drop-down menu. Then, specify the options for your application.

You can delete an application by selecting the application from the drop-down menu and clicking the **Delete** button.

## Performance Profiles

Performance Profiles are used to create and edit network performance threshold policies for BSSs and wireless clients on your wireless LAN.



When a Performance Profile is applied to your system, if the performance thresholds for that profile are exceeded, a performance alarm is generated. If there are no Performance Profiles applied to your system, no performance alarms are generated.

- ✓ **NOTE** You should monitor new ADSP deployments for several weeks to determine normal network activity before configuring Performance Profiles.

Existing profiles are displayed in the table below the row of buttons.

Assignment	Template Name	
<input type="checkbox"/>	New_Performance_Profile	( <a href="#">Edit</a>   <a href="#">Copy</a>   <a href="#">Delete</a> )

You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link.

All profiles have four tabs that are used to set performance threshold policies for your system.

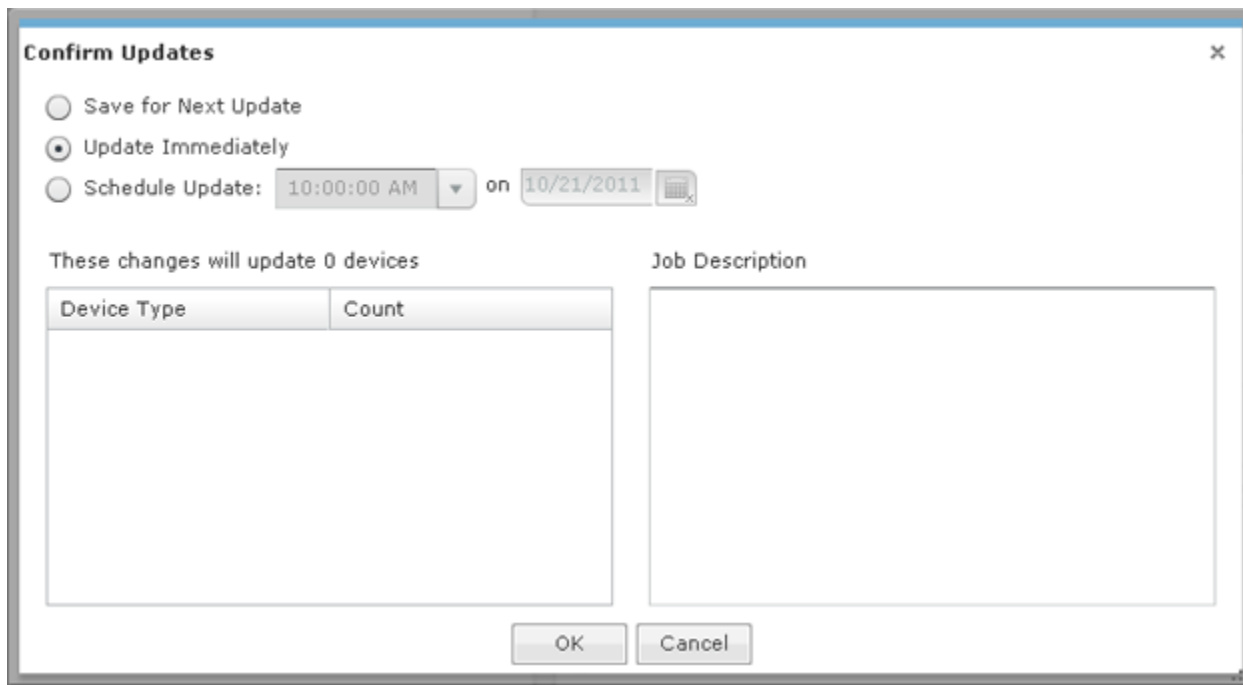
- General—Names your Performance Profile and specifies whether or not you want to:
  - Use a short time slot
  - Allow streaming traffic
  - Enable protection mode.
- Cumulative—Assigns thresholds to network characteristics for all wireless clients and traffic in the access point's BSS (Basic Service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

To copy or edit a profile, select (highlight) the Performance Profile, click the **Copy** or **Edit** link, and then make changes in any of the four tabs. Click **OK** to save your changes.

The **Copy settings to all appliances** button will copy the defined Performance Profiles and all profile assignments to all appliances in your system.

- ✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your additions (changes). A confirmation overlay is displayed.



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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to Performance Profiles are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.

Click the **Reset** button to discard any additions (changes).

### *Adding a New Profile*

Click the **New Profile** button to add a new profile. Then define your Performance Profile using the **General**, **Cumulative**, **Wireless Clients**, and **BSS** tabs. Once you have defined your Performance Profile, click **OK** to save your profile or **Cancel** to exit without saving the profile.

**General Tab**

The **General** tab is where you name your Performance Profile and specify whether or not you want to use certain functions.

The **Name** field specifies the profile name. If you are adding or copying a Performance Profile, ADSP gives the profile the default name `New_Performance_Profile`. You should change the default name to one that is more appropriate to its function. Once you save your profile, you cannot change the name.

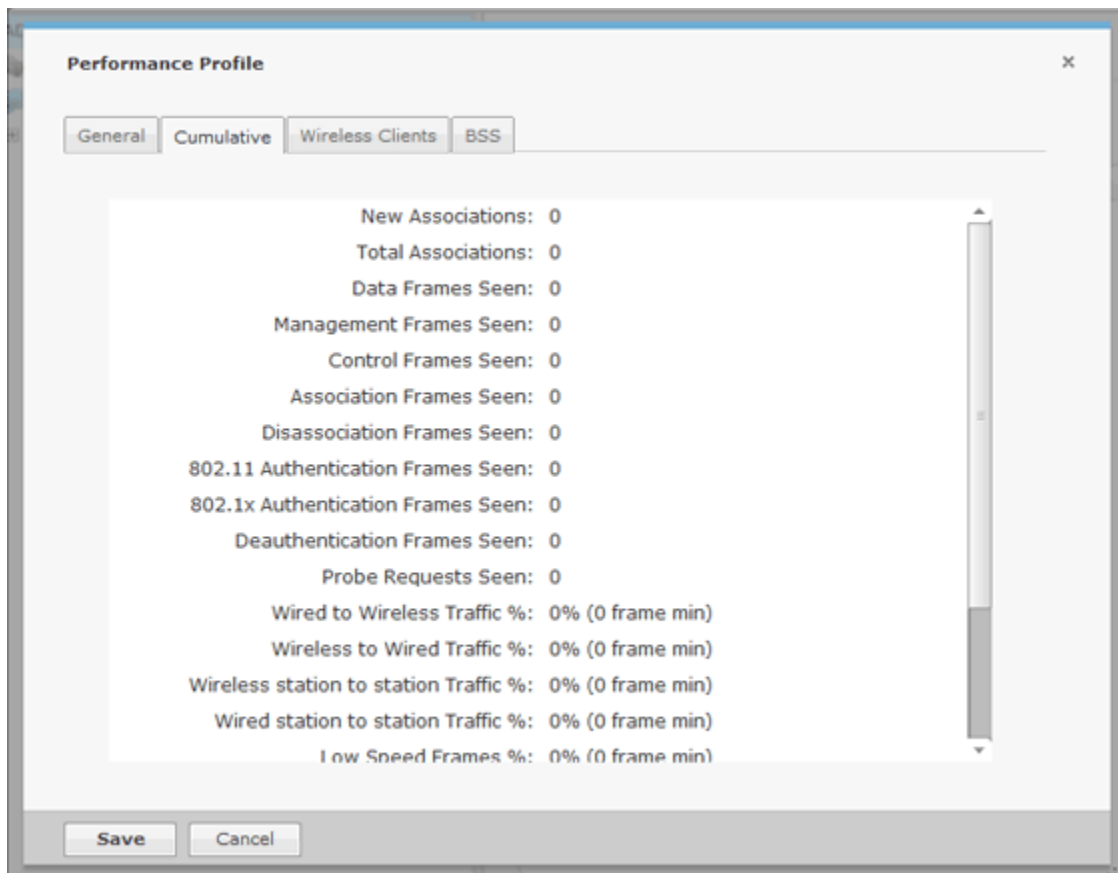
The functions are:

Function	Description
Short Time Slot Enabled	Choose <b>Yes</b> or <b>No</b> to allow short time slot capability as advertised in the Beacon, which when used on a pure 802.11g deployment, improves WLAN throughput by reducing wait time for transmitter to assure clear channel assessment.
Allow Streaming Traffic	Choose <b>Yes</b> or <b>No</b> to allow Streaming traffic in the wireless environment, such as video or audio traffic in wireless environment. It applies only to un-encrypted wireless traffic. <b>Warning:</b> Streaming traffic applications consume large bandwidth and can adversely impact all other Wireless Clients connected on the Wireless LAN.
Protection Mode Enabled	Choose <b>Yes</b> or <b>No</b> to allow Protection Mode operation to be advertised in Beacon or Probe response. Protection Mode operation is used to support mixed-mode operation of 802.11b/g protocols. <b>Note:</b> Use of Protection Mode in an 802.11g device can degrade the performance of the wireless network by introducing overhead to the network.

### Cumulative Tab

The Cumulative tab is where you assign thresholds to network characteristics for all Wireless Clients and traffic in the Access Point's BSS (Basic Service Set).

✓ **NOTE** Entering a 0 (zero) as a threshold disables alarm-generation for that threshold.



The thresholds are:

Threshold	Description
New Associations	<p>Enter the maximum number of new associations per minute ADSP will allow between a BSS and all Wireless Clients combined.</p> <p>Default = 20.</p> <p>Generally, this number should be low. Your Wireless Clients should associate with a BSS once in the morning when users log on, and rarely after that. In some cases, if the threshold value represents the actual number of Wireless Clients in a BSS, an alarm will be generated if the BSS goes off-line, forcing the Wireless Clients to re-associate with it. In no case should this value be greater than the actual number of Wireless Clients in a BSS.</p> <p>If the signal strength between a Wireless Client and a BSS is very low, the Wireless Client may repeatedly lose connectivity and then reconnect, increasing the number of associations per minute.</p>
Total Associations	<p>Enter the total number of Wireless Clients allowed to associate at any one time with a BSS. This number should reflect your actual number of Wireless Clients. ADSP generates an alarm if it detects a greater number, assuming that the extra associations are made by hackers.</p> <p>Default = 15.</p>
Data Frames Seen	<p>Enter the maximum number of data frames per minute allowed to be transmitted from all Wireless Clients combined. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Management Frames Seen	<p>Enter the maximum number of management frames per minute allowed to be transmitted from all Wireless Clients combined. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Control Frames Seen	<p>Enter the maximum number of control frames per minute allowed to be transmitted from all Wireless Clients combined. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Association Frames Seen	<p>Enter the maximum number of association frames allowed to be transmitted or received from all Wireless Clients. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Disassociation Frames Seen	<p>Enter the maximum number of disassociation frames allowed to be transmitted or received from all Wireless Clients. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
802.11 Authentication Frames Seen	<p>Enter the maximum number of 802.11 authentication frames allowed to be transmitted or received from all Wireless Clients. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>



Threshold	Description
802.1x Authentication Frames Seen	Enter the maximum number of 802.1x authentication frames allowed to be transmitted or received from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Deauthentication Frames Seen	Enter the maximum number of de-authentication frames allowed to be transmitted or received from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Probe Requests Seen	Enter the maximum number of probe requests allowed to be transmitted or received from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Wired to Wireless Traffic %	Enter the maximum percentage of data, per minute, allowed into a BSS from the wired portion of your network. If ADSP detects a greater number, it generates an alarm. Default = 60.
Wireless to Wired Traffic %	Enter the maximum percentage of data per minute allowed out of a BSS to a wired portion of your network. If ADSP detects a greater number, it generates an alarm. Default = 60.
Wireless station to station Traffic %	Enter the maximum percentage of data per minute allowed to be transmitted within the BSS from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 50.
Wired station to station Traffic %	Enter the maximum percentage of data per minute allowed to be transmitted from a wired portion of the network to another wired portion of the network, using an AP as a bridge. If ADSP detects a greater number, it generates an alarm. Default = 1.
Low Speed Frames %	802.11 protocols operate on a shared medium and use collision avoidance mechanism to access this medium. Excessive use of lower rates for transmitting frames is likely caused by stations which are either misconfigured to use lower rates or are too far from the APs to be able to support higher rates and cause alarms to be generated. Enter the maximum percentage of data per minute allowed for low speed frames to be transmitted or received from all stations. If ADSP detects a greater number, it generates an alarm. Default = 0.
Layer 3 Multicast Frames %	An alarm that is generated when the system has detected a high percentage of multicast traffic violating the policy thresholds. This may be a result of potential Layer 3 broadcast storm attacks on the network. Enter the maximum percentage of data per minute allowed for multicast frames to be transmitted or received within a BSS from all stations. If ADSP detects a greater number, it generates an alarm. Default = 0.

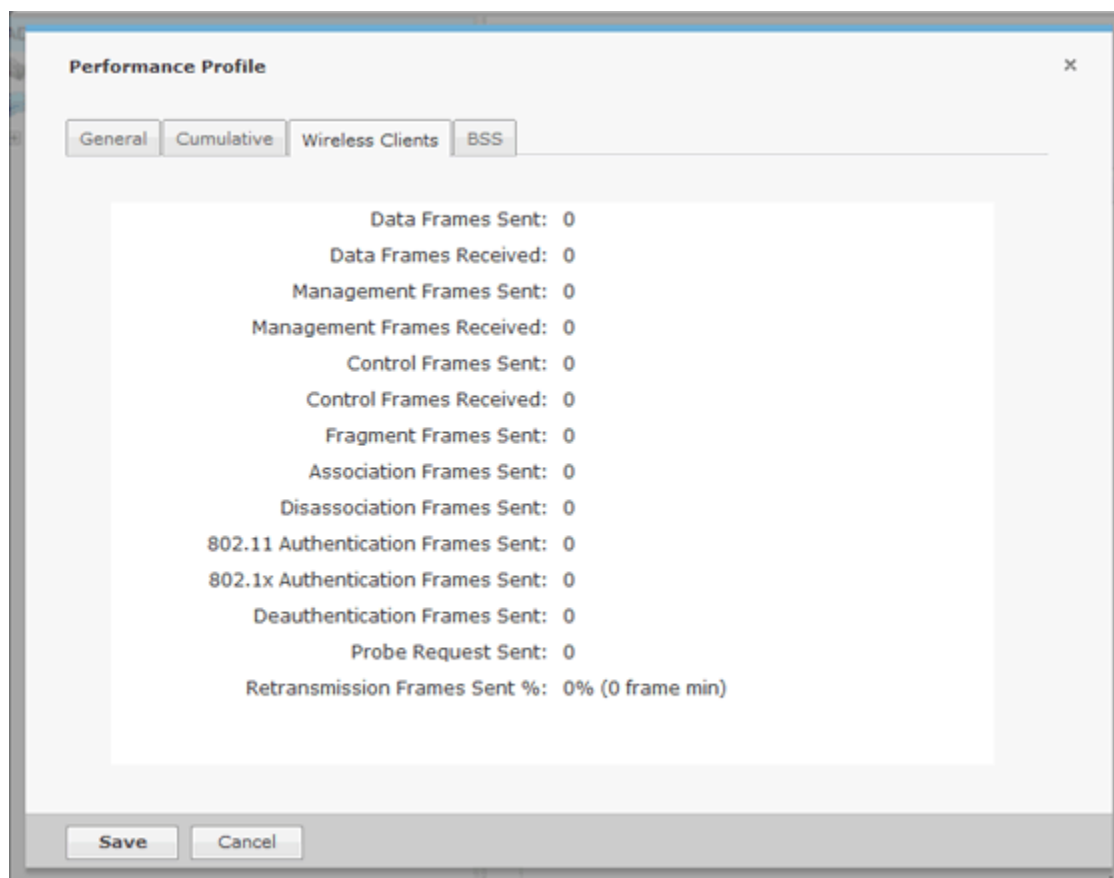
Threshold	Description
Layer 3 Broadcast Frames %	<p>An alarm that is generated when the system has detected a high percentage of broadcast traffic violating the policy thresholds. This may be a result of potential Layer 3 broadcast storm attacks on the network.</p> <p>Enter the maximum percentage of data per minute allowed for broadcast frames to be transmitted or received within a BSS from all stations. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Retransmission Frames %	<p>Enter the maximum percentage of retransmitted data frames allowed during a transmission of data within a BSS from all stations. If ADSP detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
PS Poll Frames Seen	<p>An alarm is generated by a DOS attack using an excessive number of PS-POLL frames have been detected.</p> <p>Enter the maximum number of PS Poll frames to be seen within a BSS. If ADSP detects a greater number, it generates an alarm. Default = 0.</p>

### **Wireless Clients Tab**

The Wireless Clients tab is where you assign 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.



**NOTE** Entering a 0 (zero) for any threshold-type disables that specific alarm.



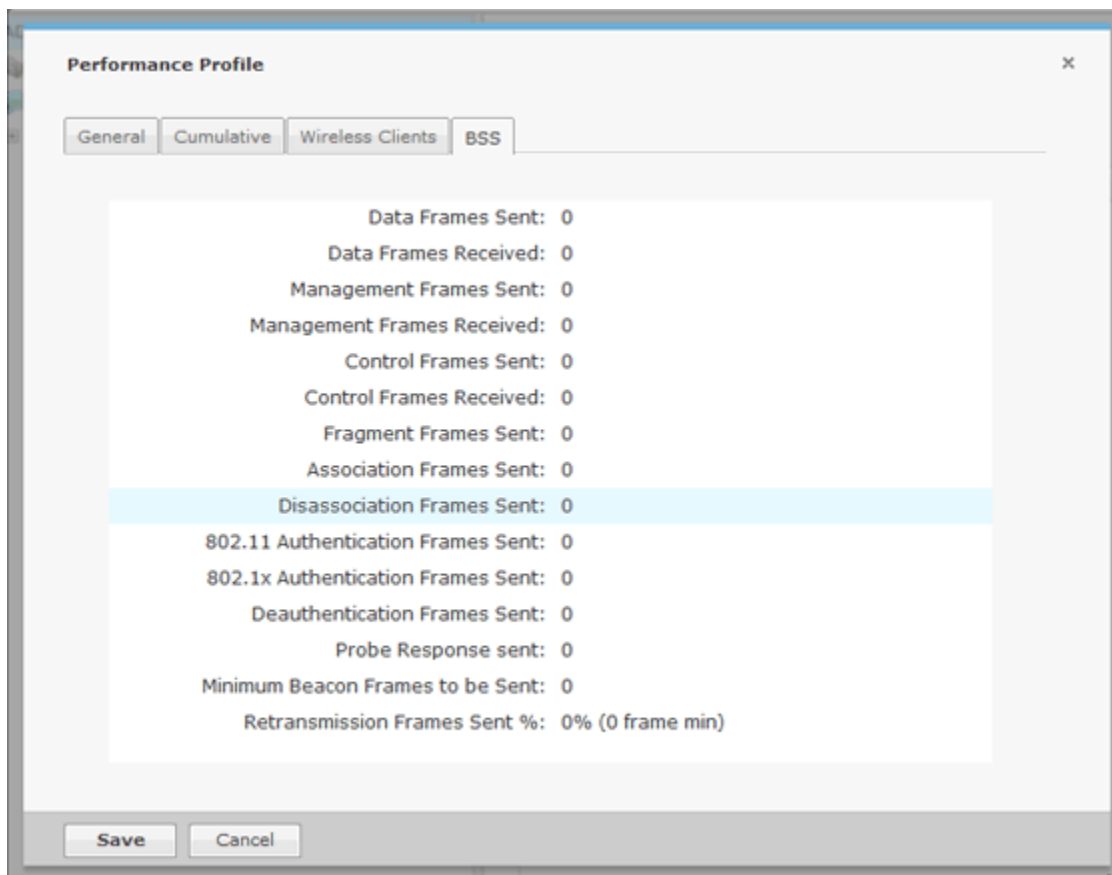
The thresholds are:

Threshold	Description
Traffic Sent %	Enter the maximum percentage of data per minute any Wireless Client is allowed to transmit. If ADSP detects a greater number, it generates an alarm. Default = 30.
Traffic Received %	Enter the maximum percentage of data per minute any Wireless Client is allowed to receive. If ADSP detects a greater number, it generates an alarm. Default = 30.
Data Frames Sent	Enter the maximum number of data frames per minute any Wireless Client is allowed to transmit. If ADSP detects a greater number, it generates an alarm. Default = 0.
Data Frames Received	Enter the maximum number of data frames per minute any Wireless Client is allowed to receive. If ADSP detects a greater number, it generates an alarm. Default = 0.
Management Frames Sent	Enter the maximum number of management frames per minute any Wireless Client is allowed to transmit. If ADSP detects a greater number, it generates an alarm. Default = 0. Management frames carry information related to negotiating network connections. If many more Management frames per minute than usual are detected, this could indicate a malicious disassociation or other form of Denial-of-Service attack.

Threshold	Description
Management Frames Received	Enter the maximum number of management frames per minute any Wireless Client is allowed to receive. If ADSP detects a greater number, it generates an alarm. Default = 0.
Control Frames Sent	Enter the maximum number of control frames per minute any Wireless Client is allowed to transmit. If ADSP detects a greater number, it generates an alarm. Default = 0.
Control Frames Received	Enter the maximum number of control frames per minute any Wireless Client is allowed to receive. If ADSP detects a greater number, an alarm is generated. Default = 0. Control frames carry information about negotiating the 802.11 protocol for getting data onto the airwaves, and are transmitted at only 1 Mbs. Unusually high numbers of Control frames may indicate bandwidth and network problems.
Fragment Frames Sent	Enter the maximum number of fragment frames per minute that are allowed from any Wireless Client. If ADSP detects a greater number, it generates an alarm. Default = 1.
Association Frames Sent	Enter the maximum number of association frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Disassociation Frames Sent	Enter the maximum number of disassociation frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
802.11 Authentication Frames Sent	Enter the maximum number of 802.11 authentication frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
802.1x Authentication Frames Sent	Enter the maximum number of 802.1x authentication frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Deauthentication Frames Sent	Enter the maximum number of de-authentication frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Probe Responses Sent	Enter the maximum number of probe requests allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Retransmission Frames Sent %	Enter the maximum percentage of data per minute that a station can retransmit as frames. If ADSP detects a greater number, it generates an alarm. Default = 0.

**BSS Tab**

The BSS tab is where you assign thresholds for transmitting data to/from BSSs.



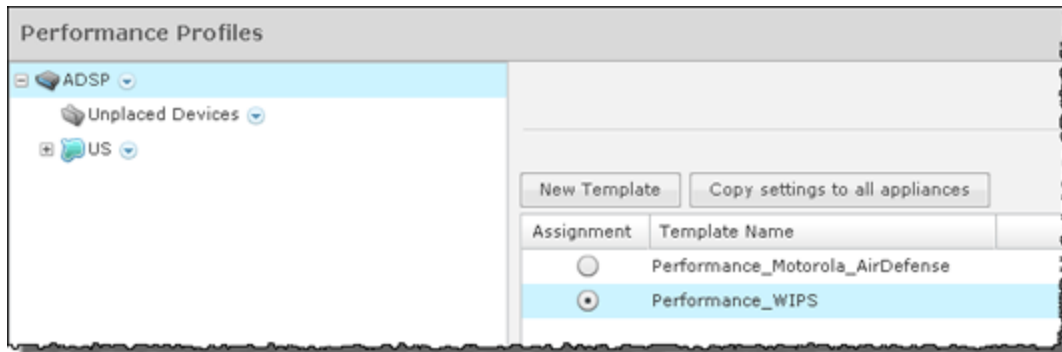
The thresholds are:

Threshold	Description
Traffic Sent %	Enter the maximum percentage of data per minute BSSs are allowed to transmit. If ADSP detects a greater number, it generates an alarm. Default = 60.
Traffic Received %	Enter the maximum percentage of data per minute BSSs are allowed to receive. If ADSP detects a greater number, it generates an alarm. Default = 60.
Data Frames Sent	Enter the maximum number of data frames per minute this BSS is allowed to transmit. If AirDefense detects a greater number, it generates an alarm. Default = 0.
Data Frames Received	Enter the maximum number of data frames per minute BSSs are allowed to receive. If ADSP detects a greater number, it generates an alarm. Default = 0.
Management Frames Sent	Enter the maximum number of management frames per minute BSSs are allowed to transmit. If ADSP detects a greater number, it generates an alarm. Default = 20,000.

Threshold	Description
Management Frames Received	Enter the maximum number of management frames per minute BSSs are allowed to receive. If ADSP detects a greater number, it generates an alarm. Default = 0.
Control Frames Sent	Enter the maximum number of control frames per minute BSSs are allowed to transmit. If ADSP detects a greater number, it generates an alarm. Default = 20,000.
Control Frames Received	Enter the maximum number of control frames per minute BSSs are allowed to receive. If ADSP detects a greater number, it generates an alarm. Default = 0.
Fragment Frames Sent	Enter the maximum number of fragment frames per minute BSSs may see before generating an alarm. Default = 1.
Association Frames Sent	Enter the maximum number of association frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Disassociation Frames Sent	Enter the maximum number of disassociation frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
802.11 Authentication Frames Sent	Enter the maximum number of 802.11 authentication frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
802.1x Authentication Frames Sent	Enter the maximum number of 802.1x authentication frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Deauthentication Frames Sent	Enter the maximum number of de-authentication frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Probe Responses Sent	Enter the maximum number of probe responses allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Minimum Beacon Frames to be Sent	Enter the minimal number of beacon frames allowed to be transmitted from all Wireless Clients. If ADSP detects a greater number it generates an alarm.
Retransmission Frames Sent %	Enter the maximum percentage of data per minute that a station can retransmit as frames. If ADSP detects a greater number, it generates an alarm. Default = 0.

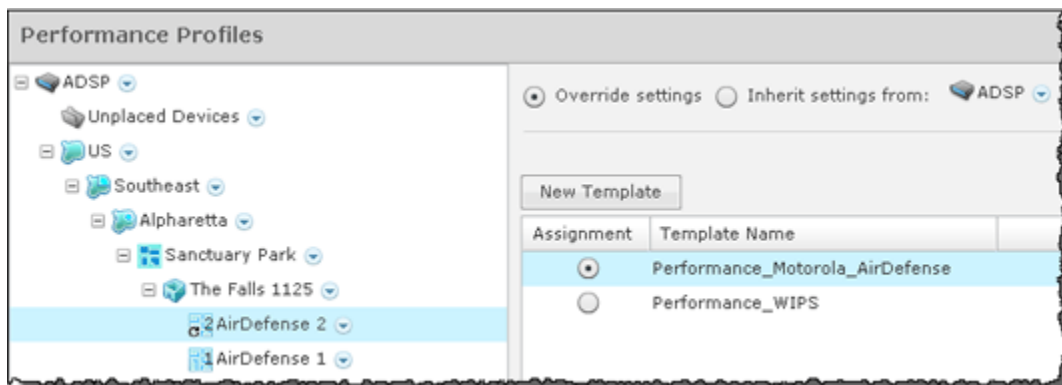
### Applying an Existing Profile

Once you have defined a Performance Profile, to use it, you must apply it to your system.



You should always apply a Performance Profile at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Performance Profile, you can apply that profile to that level. For example, in the above screen shot, the Performance Profile for ADSP could be the **Performance\_WIPS** profile and then for a special case (the following screen shot) you could override the Performance Profile at the ADSP level and apply the **Performance\_Motorola\_AirDefense** profile to the AirDefense 2 floor.

✓ **NOTE** The Override settings option is available when you select (highlight) a network level below the appliance level. Use the Expand–Expand button to reveal the other levels.

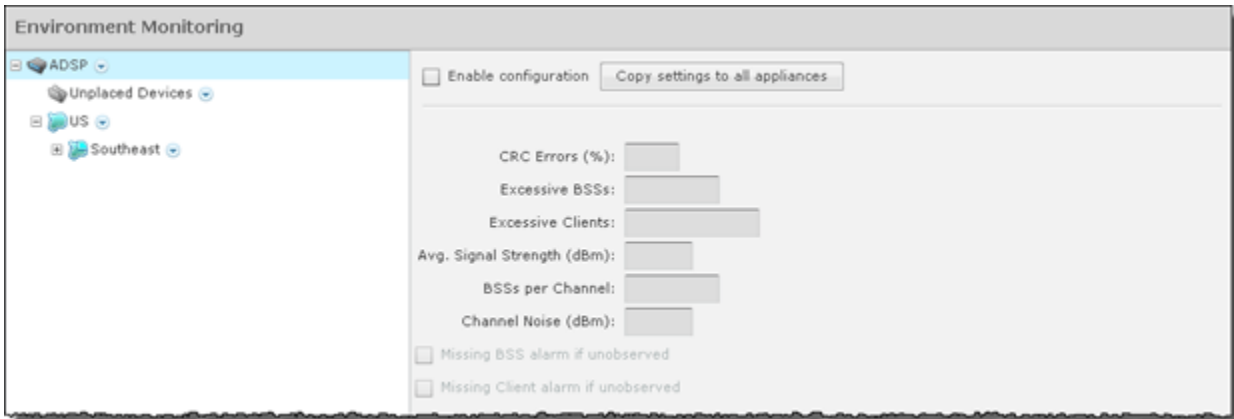


In this case, the **Performance\_WIPS** profile will be accessible to corporate-wide employees and guests while the **Performance\_Motorola\_AirDefense** profile will be available employees and guests on Floor 2 of the AirDefense facilities.

Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

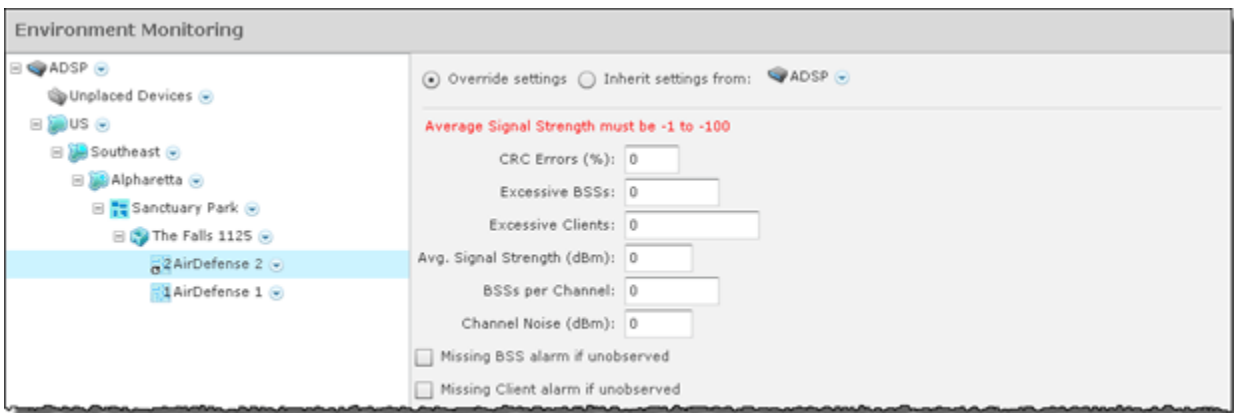
## Environment Monitoring

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.



To apply Environment Monitoring to your system, you must first select the **Enable configuration** checkbox.

You should always monitor your system at the appliance level. When you do, all the other levels are also monitored. Then, if you have a level that needs to be monitored using different settings, you can monitor that level by overriding the inherited Environment Monitoring and defining different settings for Environment Monitoring.



The following set of thresholds are monitored to see if any of value is exceeded. If a threshold value is exceeded, an alarm is generated.

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.



Threshold	Description
BSSs per Channel	The number of BSSs on any particular channel should not exceed the specified value.
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.

The Copy settings to all appliances button will copy the defined Environment Monitoring settings to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

## 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:

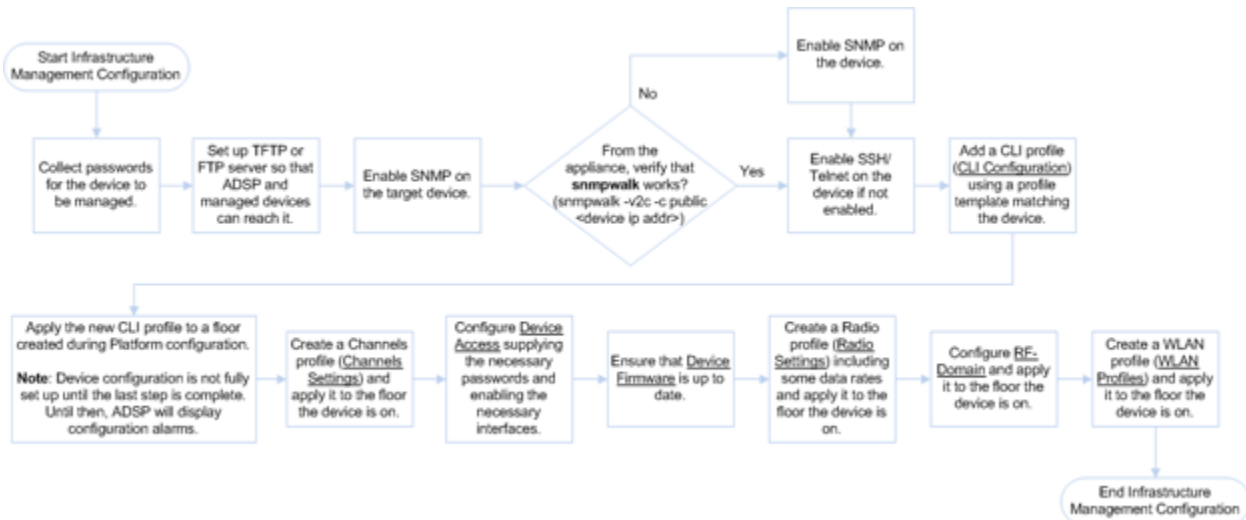
- Channel Settings
- Radio Settings
- WLAN Profiles
- CLI Configuration
- Command Run and Log
- Pending State Audit (added to the Operational Management category).

✓ **NOTE** You must configure the Platform before configuring Infrastructure Management.

You must configure all aspects of Infrastructure Management to integrate ADSP with your network, including:

- Create and update device configurations by revising the configuration files and their CLI command set.
- Specify the passwords to access devices and specify the interfaces that can be used to access devices.
- Update firmware on devices (if needed).
- Provide information to ADSP so that ADSP can apply the correct regulatory rules to the domain.
- Select power and channel settings for devices with B/N/G radios and/or A/N radios.
- Configure radios used in your network.
- Configure the WLAN settings for devices utilizing your network.

The following flowchart shows the fundamental steps to configure a device in your network using ADSP. Once you configure one device, adding others is much easier. This flowchart shows how to configure a device and apply the configuration to a floor. Ideally, you would set up ADSP to configure devices at the appliance level. Then, the configuration will be available on all network levels down to the floor level. If you have an exception, you would then override the configuration at a lower level.



Devices cannot be fully managed by ADSP until the configurations are applied.

## 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 **Configuration > Appliance Platform > Communication Settings**.

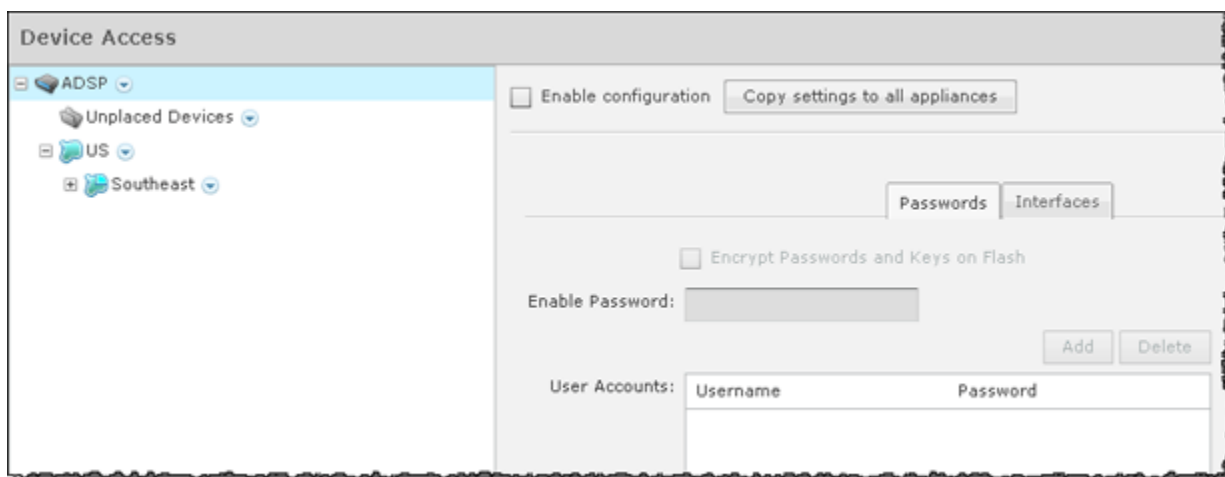
---

There are two tabs used to configure Device Access:

- Password
- Interfaces

You may configure Device Access at the appliance network level all the way down to the floor network level, but you should always configure Device Access at the appliance level. Any network level below the appliance level will inherit the configuration. If you need to have a different configuration below the appliance level, use the **Override settings** option.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.

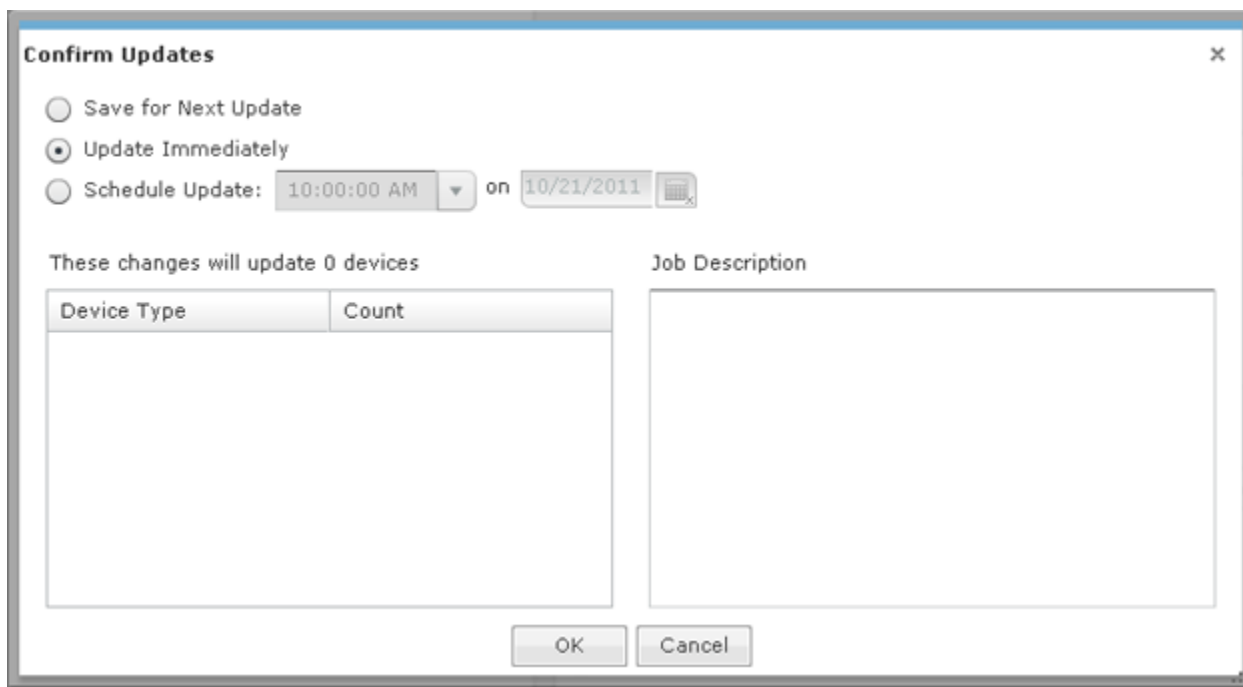


To configure Device Access, you must first select (highlight) ADSP from the tree and then enable configuration by selecting the **Enable configuration** checkbox. Then, use the **Passwords** and **Interfaces** tabs to configure Device Access.

The **Copy settings to all appliances** button will copy the defined Device Access to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your changes. A confirmation overlay is displayed.



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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to Device Access are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.

Click the **Reset** button to discard your changes.

### ***Passwords Tab***

The **Passwords** tab is used to specify the passwords to access devices.

The screenshot shows the 'Passwords' configuration page. At the top, there are two tabs: 'Passwords' (selected) and 'Interfaces'. Below the tabs, there is a checkbox for 'Encrypt Passwords and Keys on Flash'. Underneath, there is an 'Enable Password' text input field and a checkbox for 'Display Passwords'. To the right of these are 'Add' and 'Delete' buttons. Below these elements is a table labeled 'User Accounts' with two columns: 'Username' and 'Password'. The table is currently empty.

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 <b>Add</b> 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.

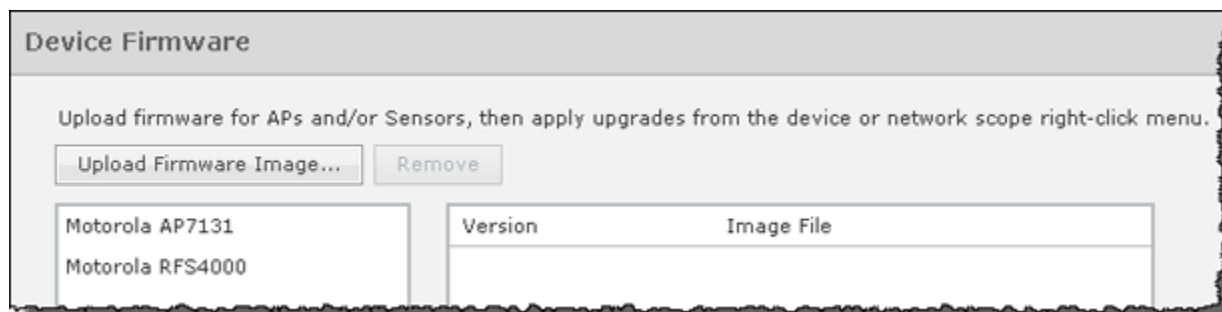
The screenshot shows the 'Interfaces' configuration page. At the top, there are two tabs: 'Passwords' and 'Interfaces' (selected). Below the tabs, there are five checkboxes for enabling different types of access: 'Telnet access enabled', 'SSH access enabled', 'HTTP access enabled', 'HTTPS access enabled', and 'SNMP access enabled'. Below these checkboxes are four text input fields: 'Read Community', 'Write Community', 'Trap Community', and 'Trap Destination'. To the right of these fields is a checkbox for 'Display Passwords'.

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"> <li>• Read Community</li> <li>• Write Community</li> <li>• Trap Community</li> <li>• Trap Destination.</li> </ul>

## Device Firmware

Device Firmware configuration allows you to upload new AP, Sensor, or Switch (Controller) firmware from a workstation to a network server. Once the firmware is uploaded, you can upgrade your APs, Sensors, or Switches using ADSP.

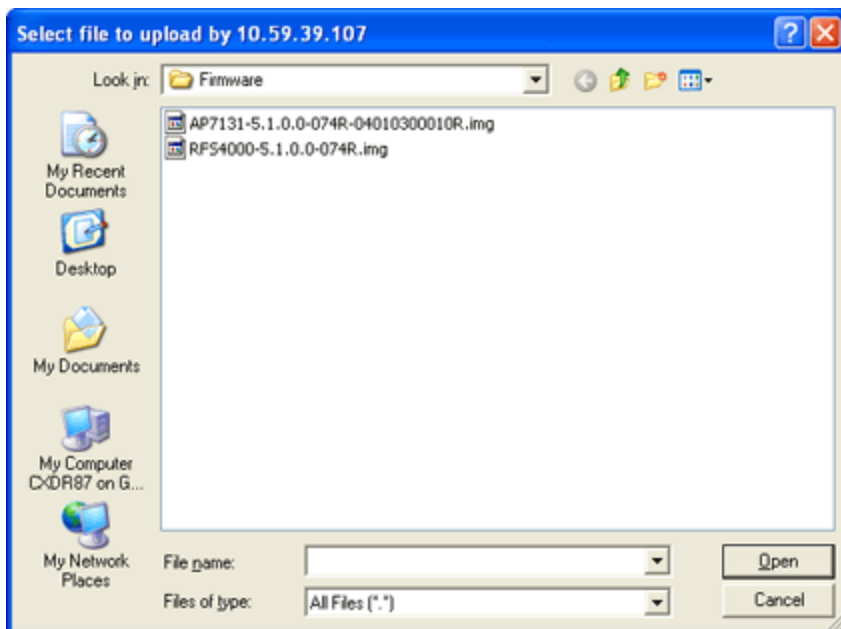


Uploaded firmware images are listed by device type, version number, and image file name. Just select (highlight) a device type to display the version number and image for that device.

Follow these steps to upload firmware:

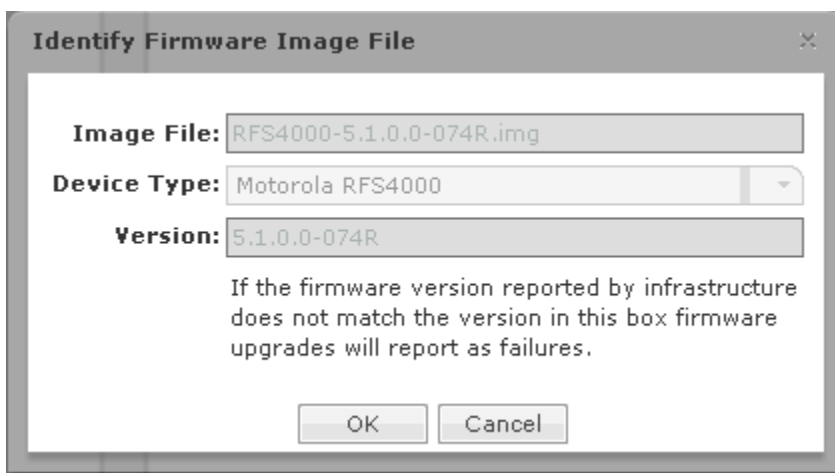
1. Click the **Upload Firmware Image** button. A browse window displays for you to select a firmware file.

2. Navigate to the directory (folder) where the firmware upgrade file resides.



✓ **NOTE** Firmware files have an IMG extension

3. Select (highlight) the upgrade file and then click **Open**. An **Identify Firmware Image File** window is displayed with the image file name identified.



4. Click **OK**. The firmware image is uploaded and now appears in the list of devices. It can now be used to upgrade APs or Sensors on your network.

✓ **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.

You can delete firmware from the list by selecting (highlighting) the device and then clicking the **Remove** button.


The **Check Synchronization** button is used to check all appliances in the network to ensure they have the same firmware. (The synchronization features works basically the same way wherever the feature is implemented. Synchronizing User Accounts has a good example of how the synchronization feature works.)

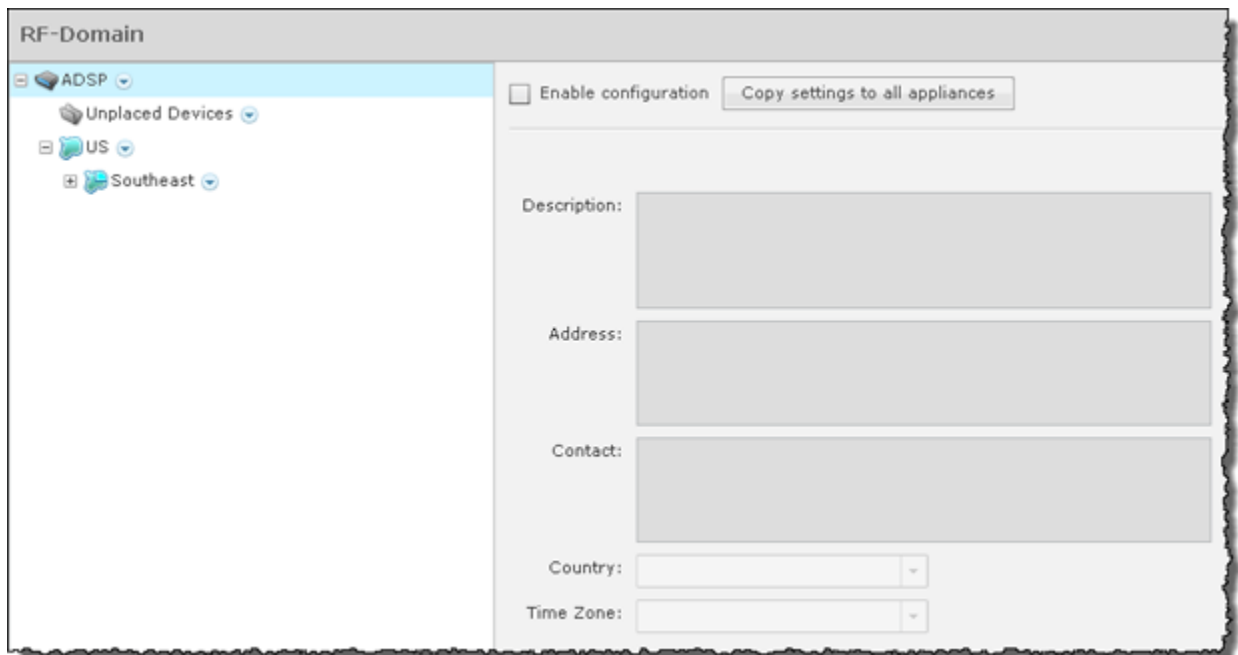
✓ **NOTE** You must have a Central Management license in order to use the Check Synchronization feature.

## 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.

You may configure RF-Domain at the appliance network level all the way down to the floor network level, but you should always configure RF-Domain at the appliance level. Any network level below the appliance level will inherit the configuration. If you need to have a different configuration below the appliance level, use the **Override settings** option.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



The screenshot shows the 'RF-Domain' configuration window. On the left, a tree view shows 'ADSP' selected, with sub-items 'Unplaced Devices', 'US', and 'Southeast'. The main area contains an 'Enable configuration' checkbox and a 'Copy settings to all appliances' button. Below these are five input fields: 'Description', 'Address', 'Contact', 'Country', and 'Time Zone'.

To configure RF-Domain, you must first select (highlight) ADSP from the tree and then enable configuration by selecting the **Enable configuration** checkbox. The configuration fields for each radio 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.
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.

The **Copy settings to all appliances** button will copy the defined RF-Domain to all appliances in your system.



**NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your changes. A confirmation overlay is displayed.

**Confirm Updates**

Save for Next Update  
 Update Immediately  
 Schedule Update: 10:00:00 AM on 10/21/2011

These changes will update 0 devices

Device Type	Count

Job Description

OK Cancel

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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to RF-Domain are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.


Click the **Reset** button to discard your changes.

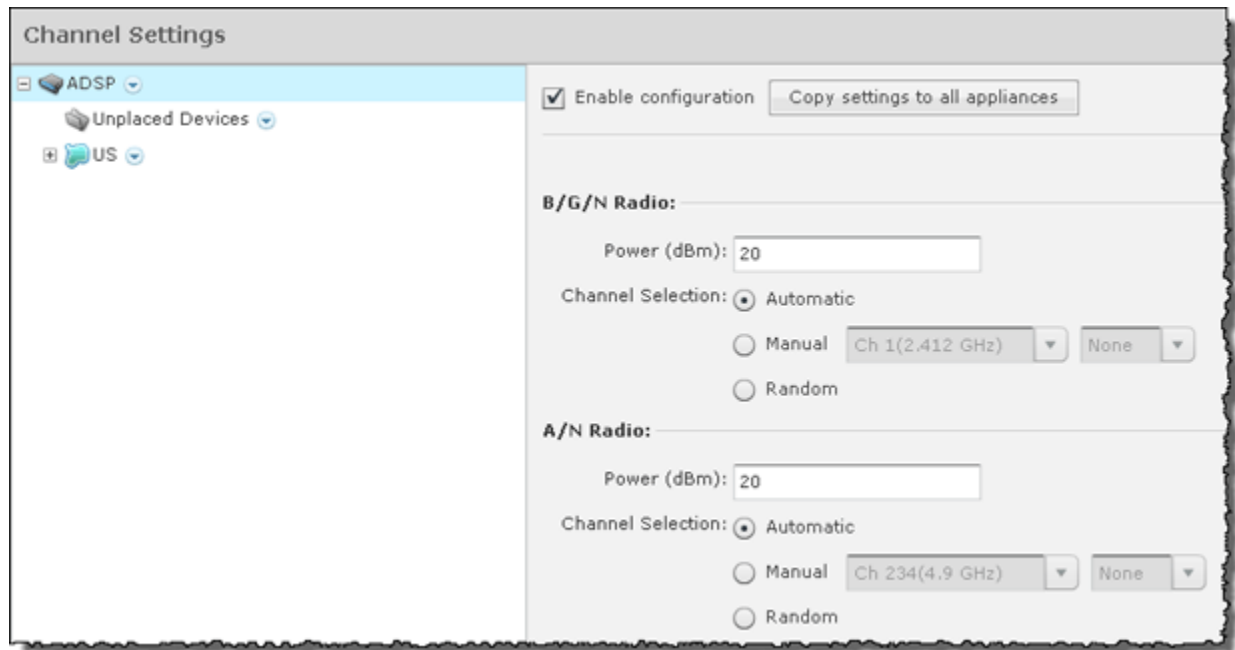
## Channel Settings

Channel Settings is used 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.



You may configure Channel Settings at the appliance network level all the way down to the floor network level, but you should always configure Channel Settings at the appliance level. Any network level below the appliance level will inherit the configuration. If you need to have a different configuration below the appliance level, use the Override settings option.

- ✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



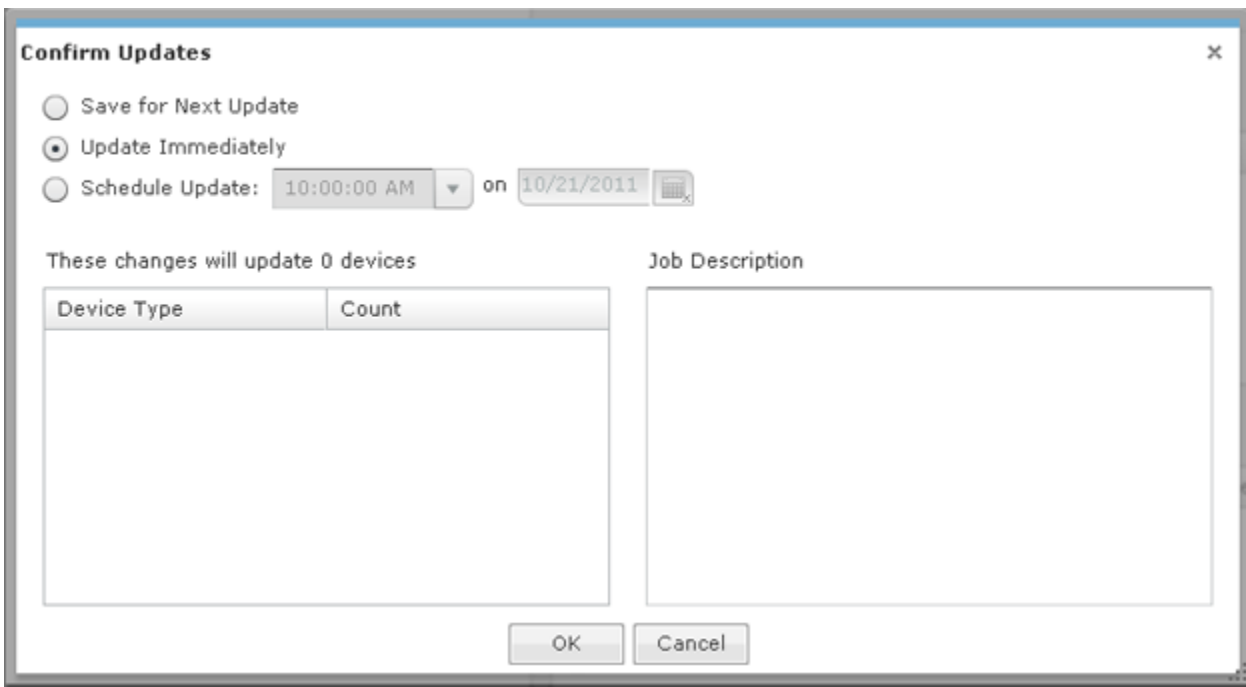
By default, Channel Settings are enabled, and are set for maximum power and automatic channel selection. The configuration fields for each radio are:

Field	Description
Power (dBm)	Enter the maximum power value (in dBm) that APs and wireless switches must have.
Channel Selection	Select one of three options: <ul style="list-style-type: none"> <li>Automatic—ADSP automatically sets which channel is used.</li> <li>Manual—Select a channel to use from the drop-down menu and then select the extension range (none, upper, or lower).</li> <li>Random—ADSP randomly sets the channel.</li> </ul>

The **Copy settings to all appliances** button will copy the defined Channel Settings to all appliances in your system.

- ✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your changes. A confirmation overlay is displayed.



The image shows a 'Confirm Updates' dialog box with the following elements:

- Three radio buttons: 'Save for Next Update', 'Update Immediately' (which is selected), and 'Schedule Update:'. The 'Schedule Update' option is followed by a time dropdown set to '10:00:00 AM' and a date field set to '10/21/2011'.
- A status message: 'These changes will update 0 devices'.
- A table with two columns: 'Device Type' and 'Count'. The table is currently empty.
- A text area labeled 'Job Description'.
- Two buttons at the bottom: 'OK' and 'Cancel'.

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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to Channel Settings are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.


Click the **Reset** button to discard your changes.

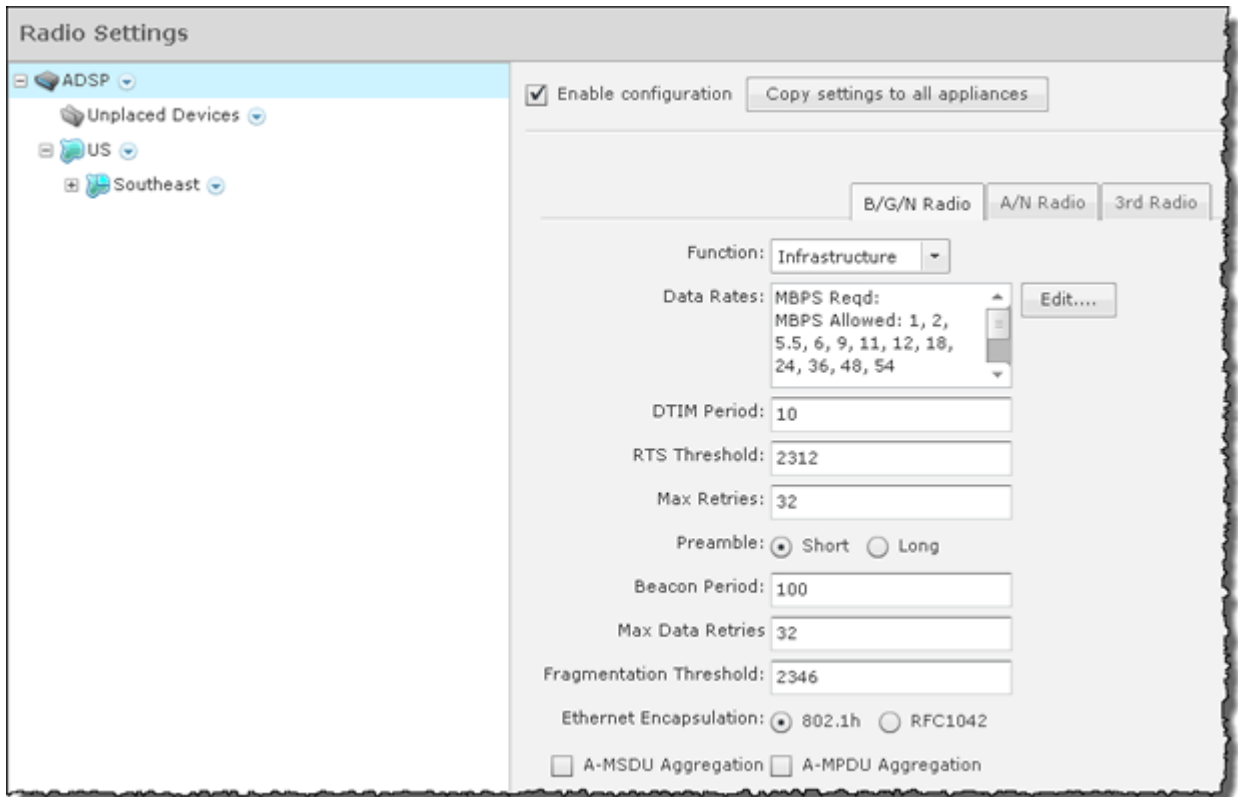
## Radio Settings

Radio Settings allow you to configure radios 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.

You may configure Radio Settings at the appliance network level all the way down to the floor network level, but you should always configure Radio Settings at the appliance level. Any network level below the appliance level will inherit the configuration. If you need to have a different configuration below the appliance level, use the **Override settings** option.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.

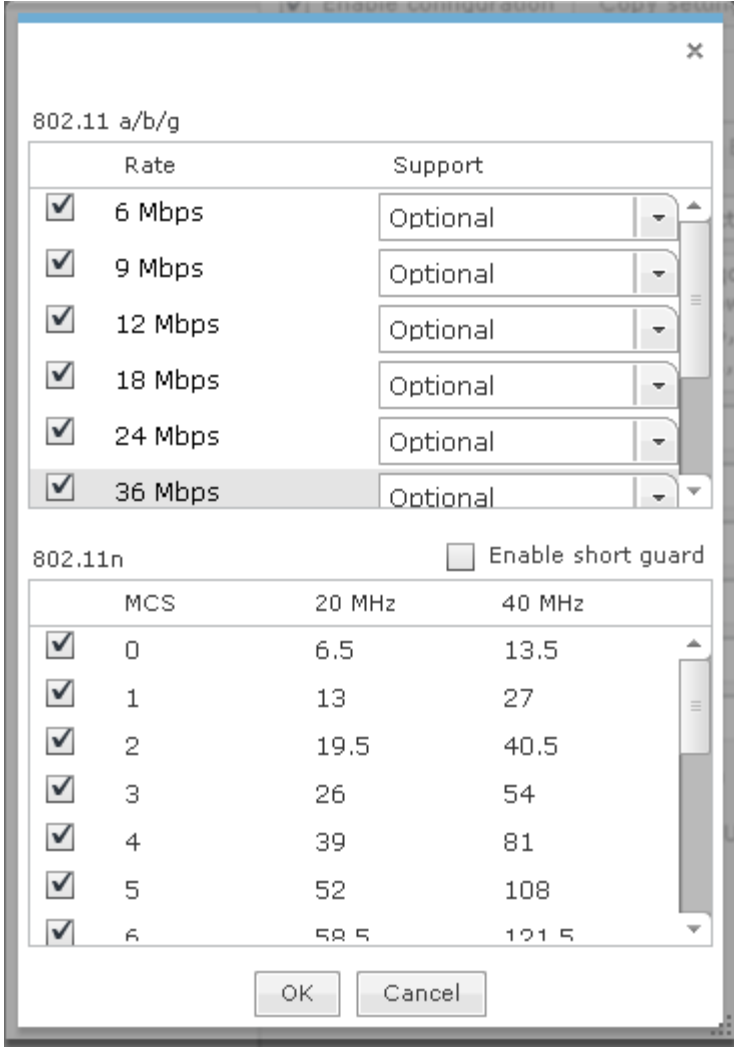


There are three possible radio configurations:

- 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. Select the function from the drop-down menu.
Data Rates	<p>Sets the data rates for the radios. Click the <b>Edit</b> button to set the rates.</p>  <p>By default, all data rates are selected.</p> <p>For 802.11 a/b/g, select the checkbox for each rate that you want to support. Then, specify if the rate is optional or mandatory.</p> <p>For 802.11n, select the MCSs that you want to support. Also, specify if you want to enable short guard.</p>
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.

Field	Description
Preamble	Specifies that the preamble is short or long. This field is not available for A/N radios.
Beacon Period	Specifies the supported beacon interval (period) in kilo-microseconds. 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.
A-MSDU Aggregation	Aggregation Enables Mac Service Data Unit (MSDU) aggregation.
A-MPDU Aggregation	Enables Message Protocol Data Unit (MPDU) aggregation.

There is only one field for the 3rd Radio: **Function**. You can either configure the 3rd Radio as a Sensor or disable it. Make your selection from the drop-down menu.

The **Copy settings to all appliances** button will copy the defined Radio Settings to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your changes. A confirmation overlay is displayed.

The screenshot shows a 'Confirm Updates' dialog box with the following elements:

- Three radio buttons: 'Save for Next Update', 'Update Immediately' (selected), and 'Schedule Update: 10:00:00 AM on 10/21/2011'.
- Text: 'These changes will update 0 devices'.
- Two empty text boxes: 'Device Type' and 'Count' (forming a table header).
- One empty text box: 'Job Description'.
- Buttons: 'OK' and 'Cancel'.

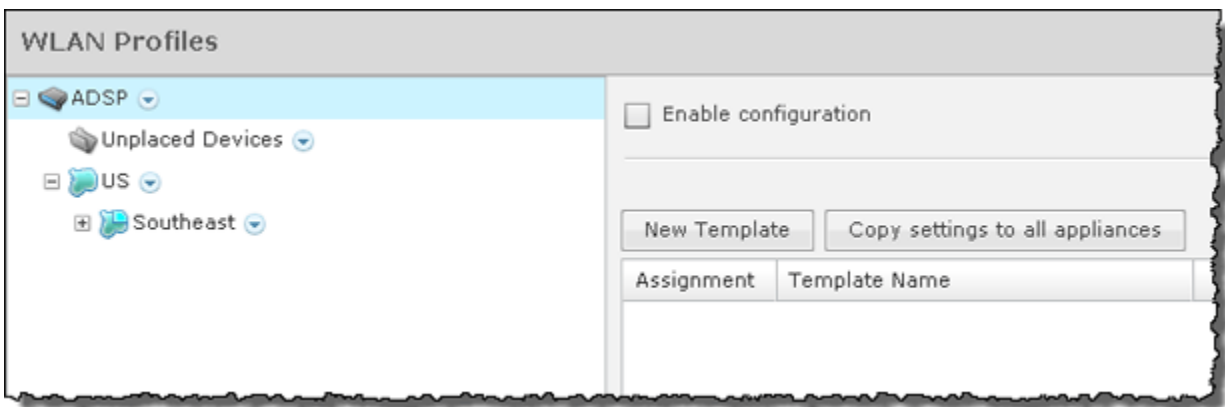
You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later. A list of device types along with the number of affected devices that will be updated is displayed. Also, if applicable, a list of unsupported settings is displayed. Click **OK** to apply changes or **Cancel** to abort.

Updates to Radio Settings are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.

Click the **Reset** button to discard your changes.

## WLAN Profiles

WLAN Profiles are used to configure the WLAN settings for devices utilizing your network.



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. Existing profiles are displayed in the table below the row of buttons.

Assignment	Template Name
	WLAN-Corporate
	WLAN-Guest_MotorolaAD
	WLAN_Profile-ADralfenator

You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link.

All profiles have two tabs that are used to set WLAN threshold policies for your system.

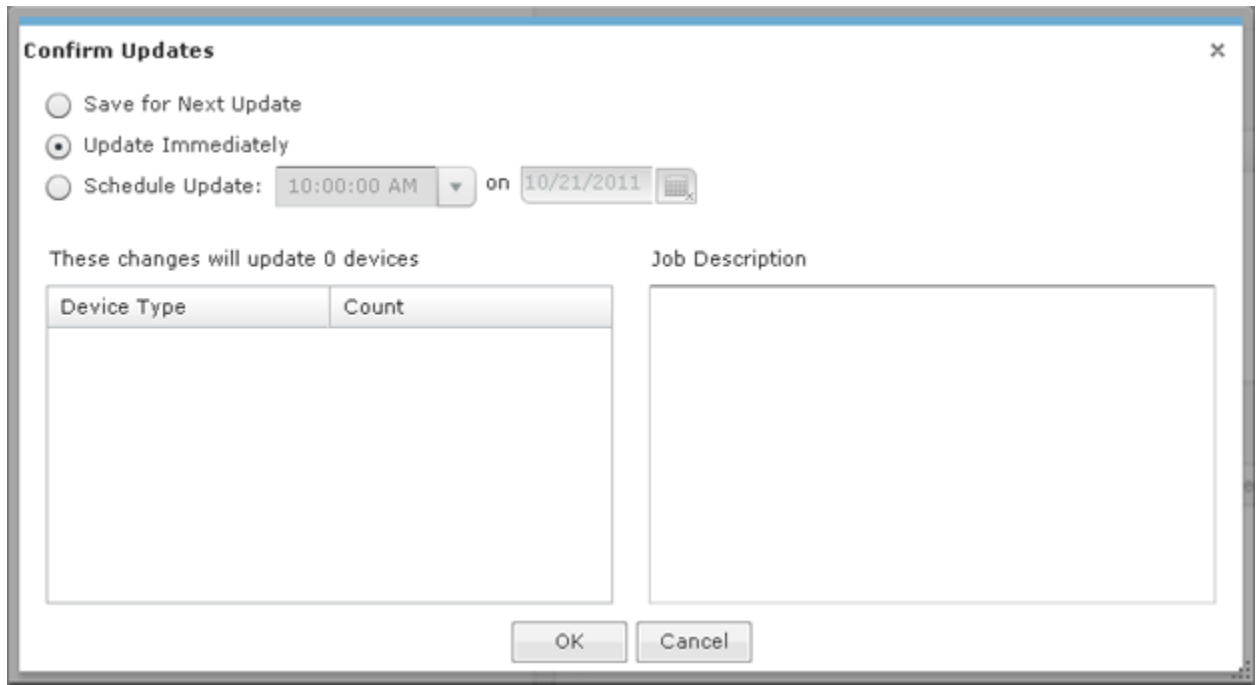
- General
- Security.

To copy or edit a profile, select (highlight) the WLAN Profile, click the **Copy** or **Edit** link, and then make changes in any of the two tabs. Click **OK** to save your changes.

The **Copy settings to all appliances** button will copy the defined WLAN Profiles and all profile assignments to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your additions (changes). A confirmation overlay is displayed.



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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to WLAN Profiles are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.

Click the **Reset** button to discard any additions (changes).

### ***Adding a New Profile***

Click the **New Template** button to add a new profile. Then define your WLAN Profile using the **General** and **Security** tabs. Once you have defined your WLAN Profile, click **OK** to save your profile or **Cancel** to exit without saving the profile.

**General Tab**

The **General** tab is where you name your WLAN Profile and specify the general settings not related to security.

The screenshot shows the 'WLAN Profiles Settings' dialog box with the 'General' tab selected. The 'Name' field contains 'New\_WLAN\_Profile'. The 'Description' and 'SSID' fields are empty. The 'Protocol' section has radio buttons for 'a', 'n (5 GHz)', 'b', 'n (2.4 GHz)', and 'g'. The 'WLAN Index' is set to '1', 'VLAN' is '1', and 'Association Limit' is '0'. The 'Station Timeout' is '10' with a dropdown menu set to 'Seconds'. Under 'Other Options', 'Broadcast SSID in Beacon' is checked, while 'Respond to all probe requests', 'Wireless Client Isolation', and 'Locally Bridged' are unchecked. A red error message at the bottom reads 'WLAN profile SSID is invalid'. 'Save' and 'Cancel' buttons are at the bottom right.

The available fields are:

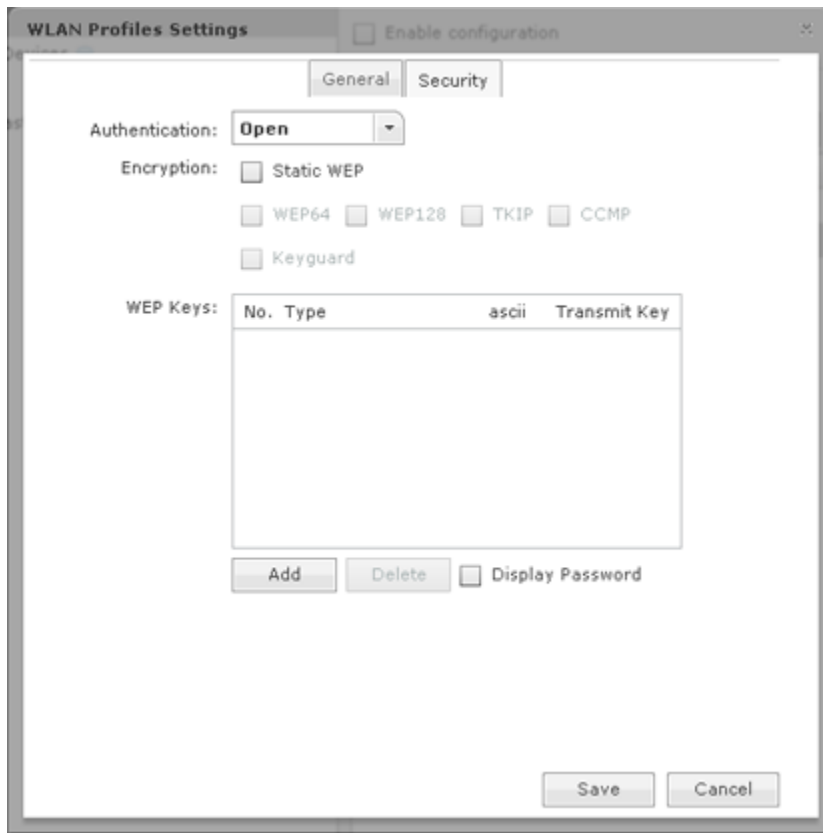
Field	Description
Name	Specifies the profile name.
Description	Allows you to specify a short description of the profile.
SSID	Specifies the Service Set Identifier (SSID) for devices.
Protocol	Specifies the protocol that the device can use [a, b, g, n (2.4 GHz), or n (5 GHz)].
WLAN Index	The order in which WLAN's will be assigned to a radio. For example, WLAN1 can have index 4, WLAN2 can have index 2, WLAN3 can have index 1, and WLAN4 can have index 3.
VLAN	Specifies the Virtual Local Area Network (VLAN) the device is authorized to use.



Field	Description
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"> <li>• Respond to all probe requests</li> <li>• Broadcast SSID in Beacon</li> <li>• Wireless Client Isolation</li> <li>• Locally Bridged.</li> </ul>

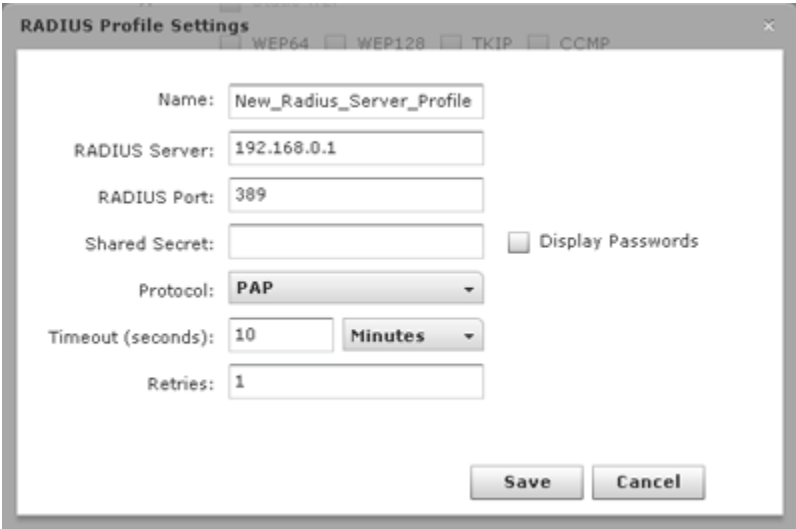
### Security Tab

The **Security** tab is where you define the security aspects of your WLAN Profile.



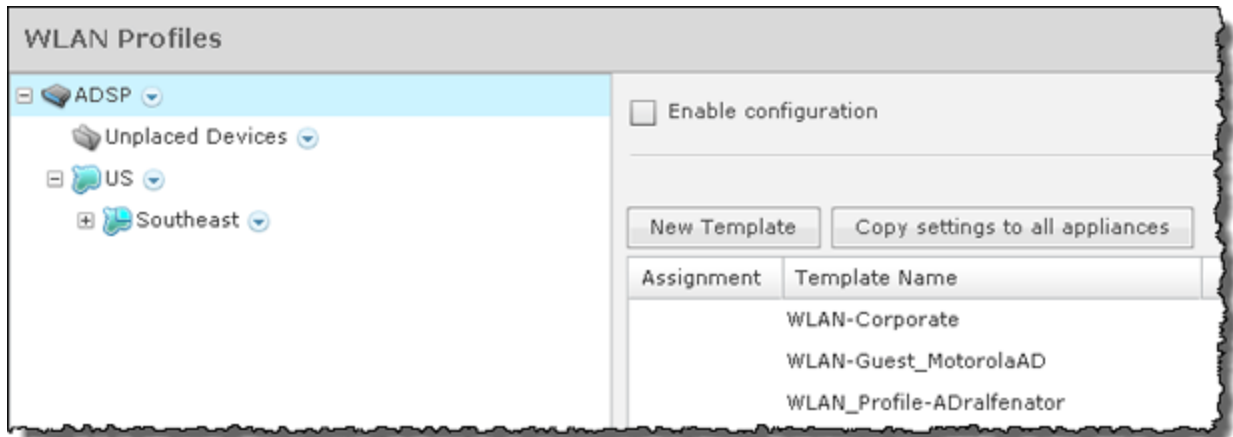
The available fields are:

Field	Description
Authentication	Specifies the type of authentication devices may use ( <b>Open</b> , <b>Shared</b> , <b>WPA</b> , <b>WPA PSK</b> , <b>WPA2</b> , <b>WPA2 PSK</b> , or <b>Legacy EAP</b> ).
Encryption	Specifies the type of encryption devices may use ( <b>Static WEP</b> , <b>WEP64</b> , <b>WEP128</b> , <b>TKIP</b> , <b>CCMP</b> , or <b>Keyguard</b> ). You may select one or more encryption types.

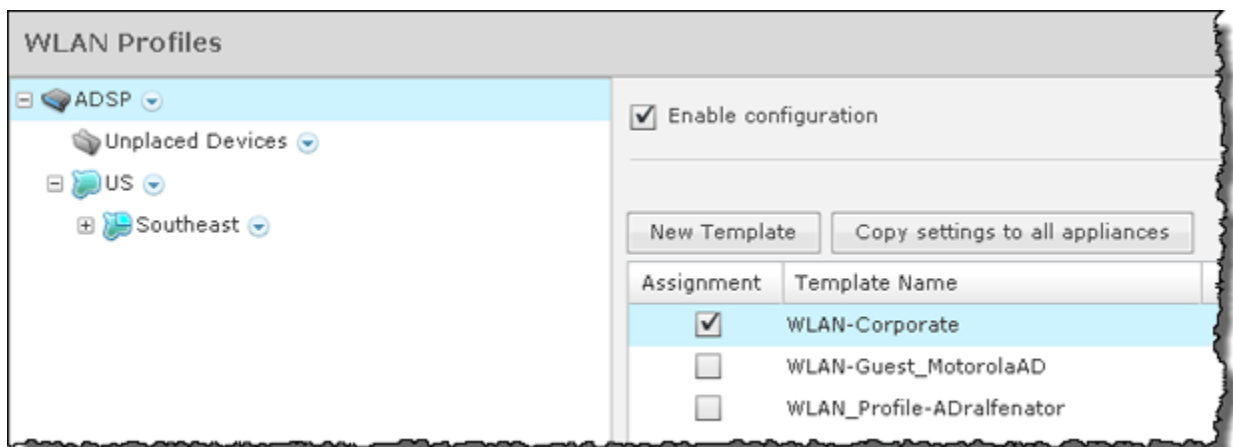
Field	Description
PSK	Specifies a pre-shared key (PSK) / password used by devices. The PSK may be ASCII or HEX.
WEP Keys	Specifies the WEP keys used to connect to the network. The WEP key may be ASCII or hexadecimal. You may also elect to transmit the WEP key. Check the <b>Display Passwords</b> checkbox to display the passwords in plain text. Use the <b>Add</b> button to add a new key or the <b>Delete</b> button to delete a key.
RADIUS Servers	<p><b>NOTE</b> 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 <b>New Server</b> button which displays the following overlay.</p>  <p>You must supply the following information:</p> <ul style="list-style-type: none"> <li>• A name for the RADIUS Server Profile.</li> <li>• The IP address or host name of the RADIUS server.</li> <li>• The RADIUS server port used for communications.</li> <li>• The shared password of the RADIUS server. Select the <b>Display Passwords</b> checkbox if you wish the password to be displayed while typing it.</li> <li>• A protocol selected from the drop-down menu (<b>PAP</b>, <b>CHAP</b>, <b>MSCHAP</b>, or <b>MSCHAPv2</b>).</li> <li>• A timeout value and a time interval selected from the drop-down menu (<b>Seconds</b> or <b>Minutes</b>).</li> <li>• The maximum number of retries to connect to the RADIUS server.</li> </ul> <p>Click <b>Save</b> to save the RADIUS server information.</p>

### Applying an Existing Profile


Once you have defined a WLAN Profile, to use it, you must apply it to your system.

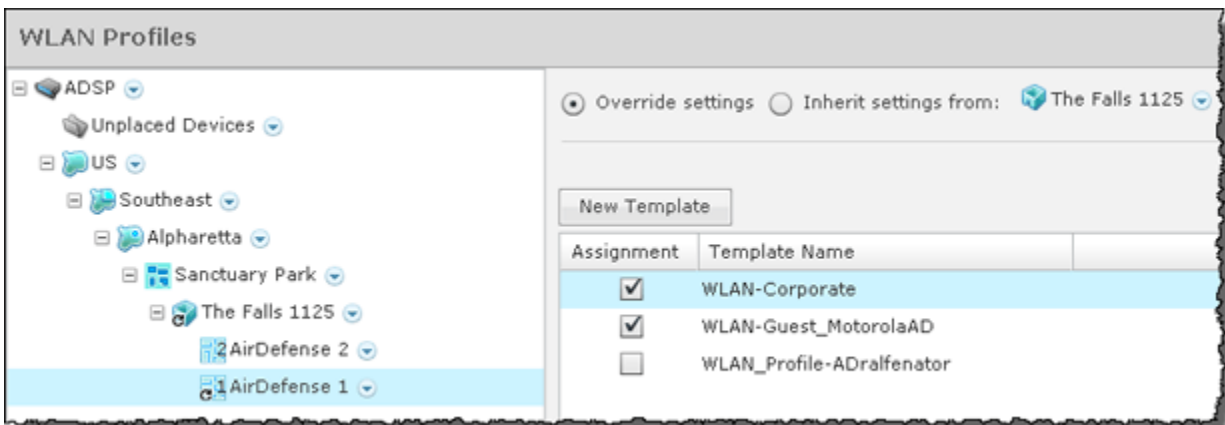


To apply WLAN Profiles to your system, you must first select the **Enable configuration** checkbox.



You should always apply a WLAN Profile at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different WLAN Profile, you can apply that profile to that level. For example, in the above screen shot, the WLAN Profile for the appliance could be the **WLAN-Corporate profile** and then for a special case you could override the WLAN Profile at the ADSP level and apply the **WLAN-Guest\_MotorolaAD** profile to the Motorola AirDefense network level.

- ✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



✓ **NOTE** You may select multiple WLAN Profiles by checking more than one checkbox.

In this case, the **WLAN-Corporate** profile will only be accessible to corporate employees that have the proper credentials while the **WLAN-Guest\_MotorolaAD** profile will be available to guests visiting the Motorola AirDefense facilities.

## 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.

With the AirDefense Services Platform, you can create and update device configurations by revising the configuration files and their CLI command set. CLI profiles (configuration templates) are provided that you can use as is or change to meet the configuration requirements of your devices. You can push the CLI profiles out to devices in your network to ensure all devices in your network conform to your company policies. Devices are typically Access Points and Switches. The following devices are currently supported:

- Alcatel AL v5.x
- Aruba Aruba600
- Brocade BR v5.x
- Brocade BR51X1
- Brocade BR71X1
- Brocade BRX000
- Cisco Airespace
- Cisco Autonomous 12x0/11x0
- 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 Wi-NG v5.x
- Motorola WS2000
- Motorola WS5100.

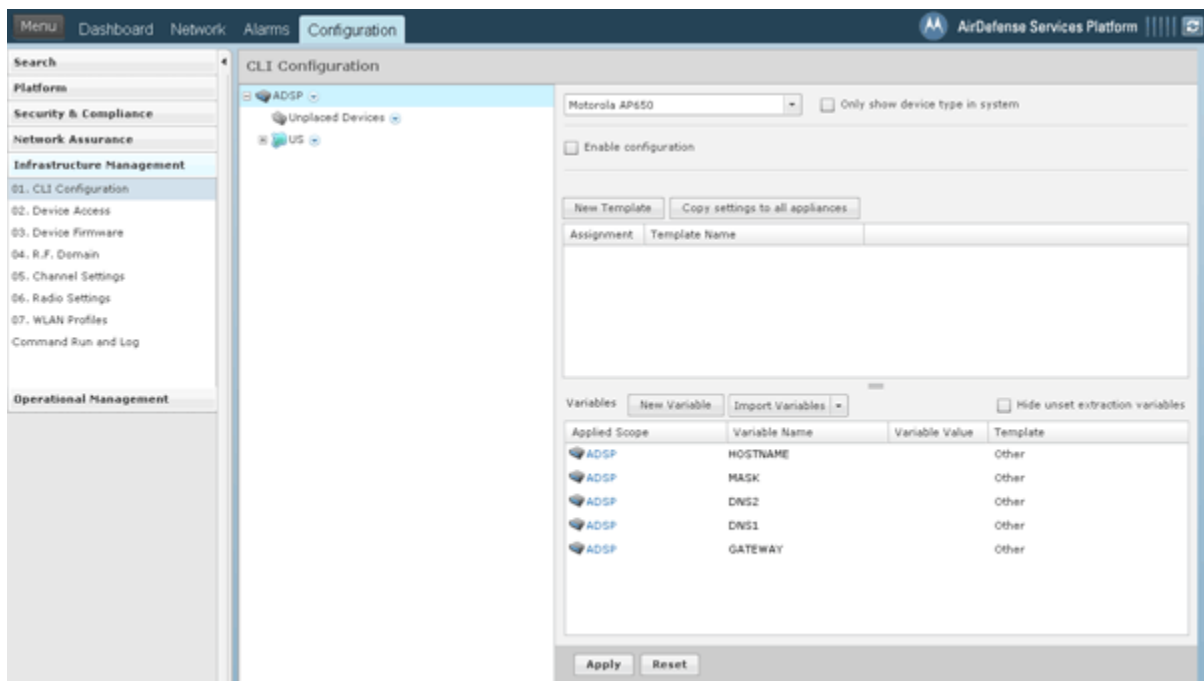
A device must be in a compliant state to receive a template. If you try to install a template on non-compliant (non-supported) devices, ADSP displays a warning message and prevents you from installing the template.

### *Adding a New Profile*

AirDefense Services Platform can create and update device configurations by revising the configuration files and their CLI command set. Configuration templates are provided that you can use as is or change to meet the configuration requirements of your devices. This allows you to apply profiles to any or all of the devices in your network. Devices are typically Access Points and Switches.

To create a new profile:

1. Select one of the supported CLI configurations from the CLI Configuration drop-down menu. The selected profile is accessed.



✓ **NOTE** The list of supported devices can be reduced to only the devices in your system by selecting **Only show device type in system** checkbox.

- If you want to add a new profile at the appliance level, select the appliance level and then select the **Enable configuration** checkbox. If you want to add a new profile at a lower network level, select the appropriate level and then select **Override settings** radio button.
- Click the **New Template** button. The template for the selected CLI Profile is displayed. In the following screen shot, the Motorola AP650 template is displayed.

**CLI Profile**

Name:

Device Type:

Reboot and write configuration updates to startup config (if available)  
 Do not reboot, instead write configuration updates to running config

```

!
version $[VERSION]
!
wlan-qos-policy default
qos trust wmm
!
radio-qos-policy default
!
firewall-policy default
!
mint-policy global-default
!
bridging-policy default
!
management-policy default
user admin password 1
e4a4b216f889b3e07be9a27af1946dad8fe68048o4b0fa31b29470e38cebdb8a role superuser access
all
!
!
$[WLAN_RADIO_CHANNEL_EXPANSION]
!
!
$[DEVICEACCESS_RFDOMAIN_EXPANSION]

```

Save Cancel

- Enter a name for the profile.
- Decide if you want to reboot the device and write configuration updates to the startup configuration, or not reboot and write configuration updates to the running configuration. Then, select the radio button reflecting your choice.
- Update the CLI commands to match your criteria (see [CLI Commands](#)).
- Click **Save**. The profile name is added to the list of profiles for that network level and that device type. Now, you can select it and apply it to a network level in your system.

Once you add a profile, you can copy, edit, or delete it by highlighting the profile and clicking the appropriate link (right side of profile). You can also copy the profile to all your other appliances using the **Copy settings to all appliances** button if you have a Central Management license and have added the appliance to your network (**Menu > Add Devices**).

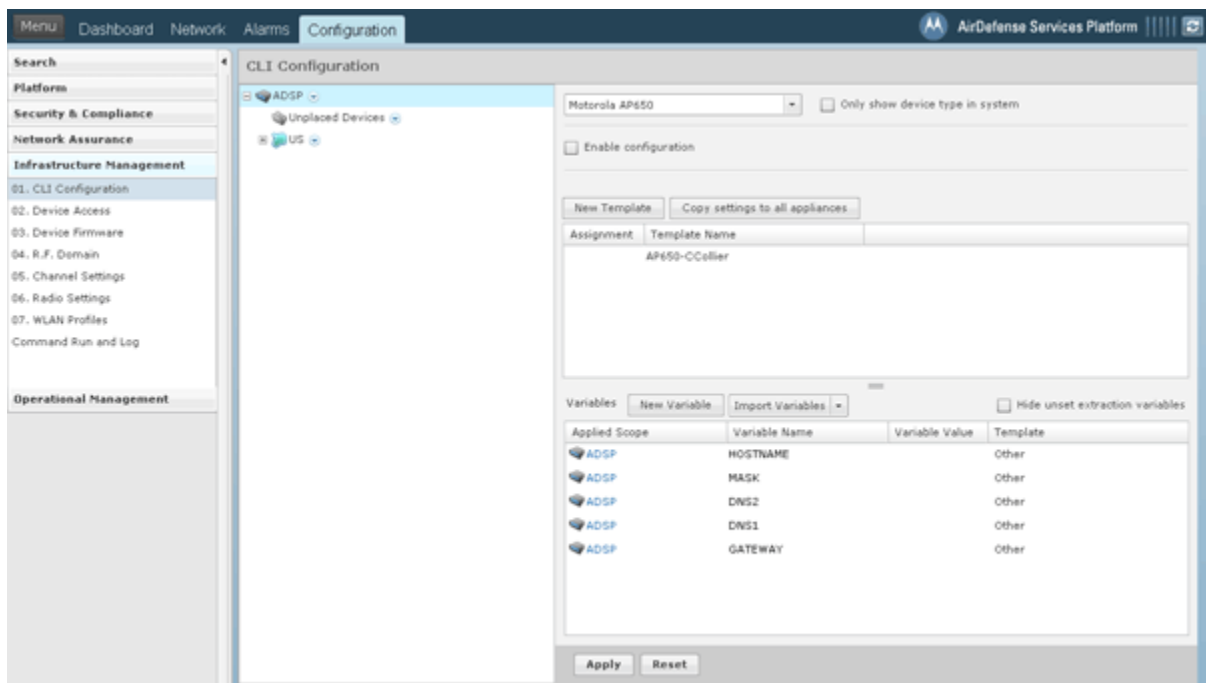
### Applying a Profile

Once you have defined a CLI profile for your device(s), you can now apply it to the device(s) in your network. A CLI profile can be applied to an appliance and all its network levels or it can be applied to a single network level. Any child network level automatically inherits the parent's CLI profile.

A good practice is to apply a CLI profile to the appliance level. This profile should be generic as possible to fit a wide range of devices in your network. Then, if you have any special considerations, apply CLI profiles to individual network levels that must meet your predefined special configurations.

To apply a CLI profile, follow these steps:

1. Select one of the supported CLI configurations from the **CLI Configuration** drop-down menu. Profiles for the selected device is displayed in the list of templates.



2. If you want to apply a profile at the appliance level, select the appliance level and then select **Enable configuration** checkbox. If you want to apply a profile at a lower network level, select the appropriate level and then select **Override settings** radio button.
3. Select the profile from the list of profiles.

Assignment	Template Name
<input checked="" type="radio"/>	AP650-CCollier

- Click **Apply** to save the configuration. A confirmation dialog is displayed.

✓ **NOTE** If you decide not to save the configuration, click **Reset** to discard any changes/updates and refresh the screen's display.

**Confirm Updates**

Save for Next Update  
 Update Immediately  
 Schedule Update: 10:00:00 AM on 10/21/2011

These changes will update 0 devices

Device Type	Count

Job Description

OK Cancel

The device type and the total count of affected devices are displayed.

- Decide if you want to save this update to be included in the next update, update immediately, or schedule the update for another time. Then, select your option.
- You may optionally enter a job description.
- Click **OK** to confirm. Click **Cancel** to exit without applying the update.

### **CLI Commands**

CLI commands are used to configure devices to your specification. Each device has its own set of CLI commands. You can edit the CLI commands for a defined profile using the **Edit** button.

✓ **NOTE** Only experienced administrators should edit the CLI commands for a device. If an invalid command is present and applied to devices in your network, they could be disabled.



```

!
version ${VERSION}
!
wlan-qos-policy default
  qos trust wmm
!
radio-qos-policy default
!
firewall-policy default
!
mint-security-policy the_policy
!
bridging-policy default
!
management-policy default
  user admin password 1
  e4a4b216f889b3e07be9a27af1946dad8fe68048c4b0fa31b29470e38cebdb8a role superuser access
  all
!
${WLAN_RADIO_CHANNEL_EXPANSION}
!
!
!
${DEVICEACCESS_RFDOMAIN_EXPANSION}

```

ADSP can update a new default configuration or an existing configuration of a device by manipulating the displayed configuration file and its CLI command set. This CLI command set represents a template that can be applied to other related devices or just a single access point. The template has placeholders for providing variable values for full or partial device configurations. The placeholders follow a syntax convention defined by ADSP. For example, there is a configuration command to define the WAN's IP address (ipadr 1 \${IP("1")}). The template file has a (ipadr 1 \${IP("1")}) value that can manually updated. The updated (ipadr 1 \${IP("1")}) variable is fed through a ADSP variance file and applied to a device (or groups of devices). Create these configuration variances as required to perform configuration updates to other supported devices through ADSP.

### 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.

Applied Scope	Variable Name	Variable Value	Template
ADSP	HOSTNAME		AP650-CCollier
ADSP	MASK		Other
ADSP	DNS2		Other
ADSP	DNS1		Other
ADSP	GATEWAY		AP650-CCollier
Unset Value	VERSION		AP650-CCollier
Unset Value	IP("vlan1")		AP650-CCollier

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 using the following format:

```
$_[VARIABLE_NAME]
```

Once a variable is added to the **CLI Commands** section, 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 \_

✓ **NOTE** If you create a new variable and its name already exist in a profile, you will not be able to remove it from the variable list. You can unset it so that it will not be used but it will still appear in the variable list.

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.

Clicking in the status area reveals a drop-down menu where you can change the status of a variable.

The **New Variable** button is used to add a new variable to the variables section. You will have to name the variable and place it in a profile to use it.

The multi-function button gives you access to the following three functions via the associated drop-down menu:

- The **Import Variables** function imports CLI variables. See [Import CLI Variables](#) for file format and examples.
- The **Export Variables** function exports CLI variables to a file for later use.
- The **Open Variable Template** function displays a template that you can copy, paste the contents into an editor, and edit the contents to create an import file.

The **Hide unset extraction variables** checkbox can be used to hide/reveal unset extraction variables displayed in the list of variables.

## Command Run and Log

Command Run and Log allows you to run CLI commands on devices that are in the Audit mode (not template based) and then store the results in a log file for viewing later.

- ✓ **NOTE** In order for **Command Run and Log** to work properly, a [Communication Settings](#) profile must exist for the affected devices.

The commands are applied to all devices in the selected scope. The scope may be any network level or floor. To select a scope, just select a scope from the **Scope** drop-down menu.

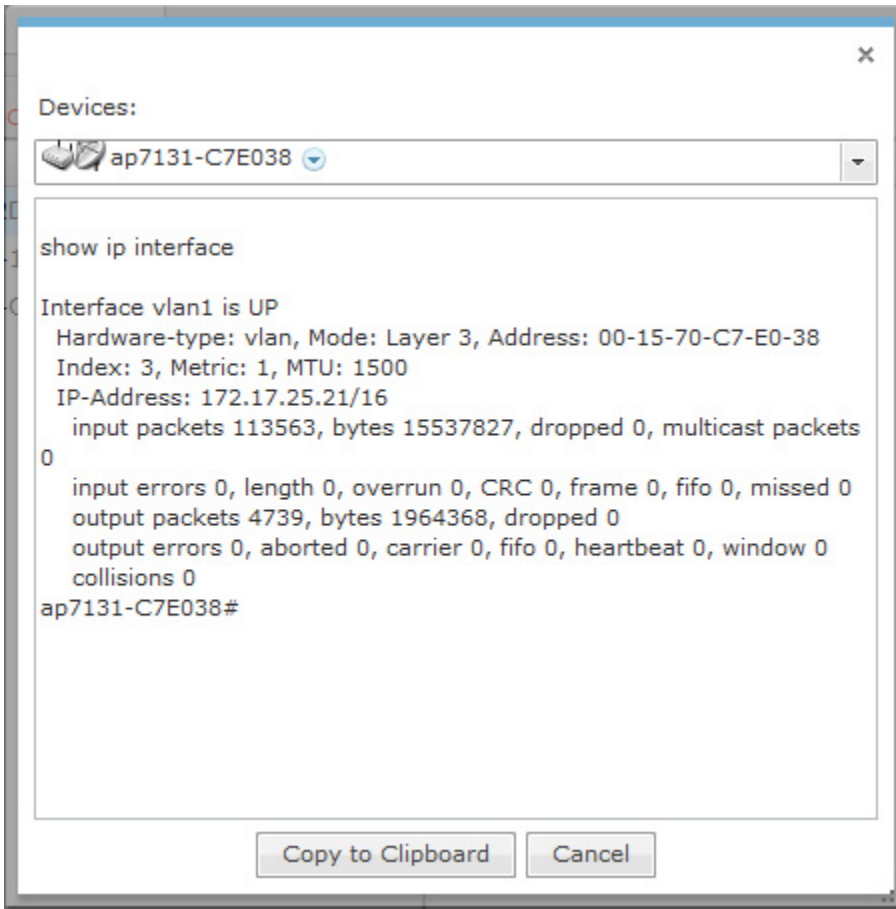
Each command must be on a line by itself. If a command requests a confirmation from a device, ADSP will respond Yes.

You may import an updated configuration from device(s) after a command has run successfully. Just select the **Import** checkbox.

The logs for the Command Run and Log are placed at: `/usr/local/smx/device-mgmt/jobs`. For each job, there is a job ID. The interaction with all devices for a job is placed in a sub-folder whose name is the job ID number.

After selecting a scope and entering your CLI commands, click **Apply** to run the commands. Clicking **Reset** returns Command Run and Log back to its original state.

You can check the job status by navigating to **Configuration > Operational Management > Job Status**. While viewing the job details, you can view the logs by selecting a device and then clicking the **View Log** link.



You can view the log of another device by selecting the device from **Devices** drop-down menu. The **Copy to Clipboard** button copies the log contents to the clipboard. The **Cancel** button exits the log.

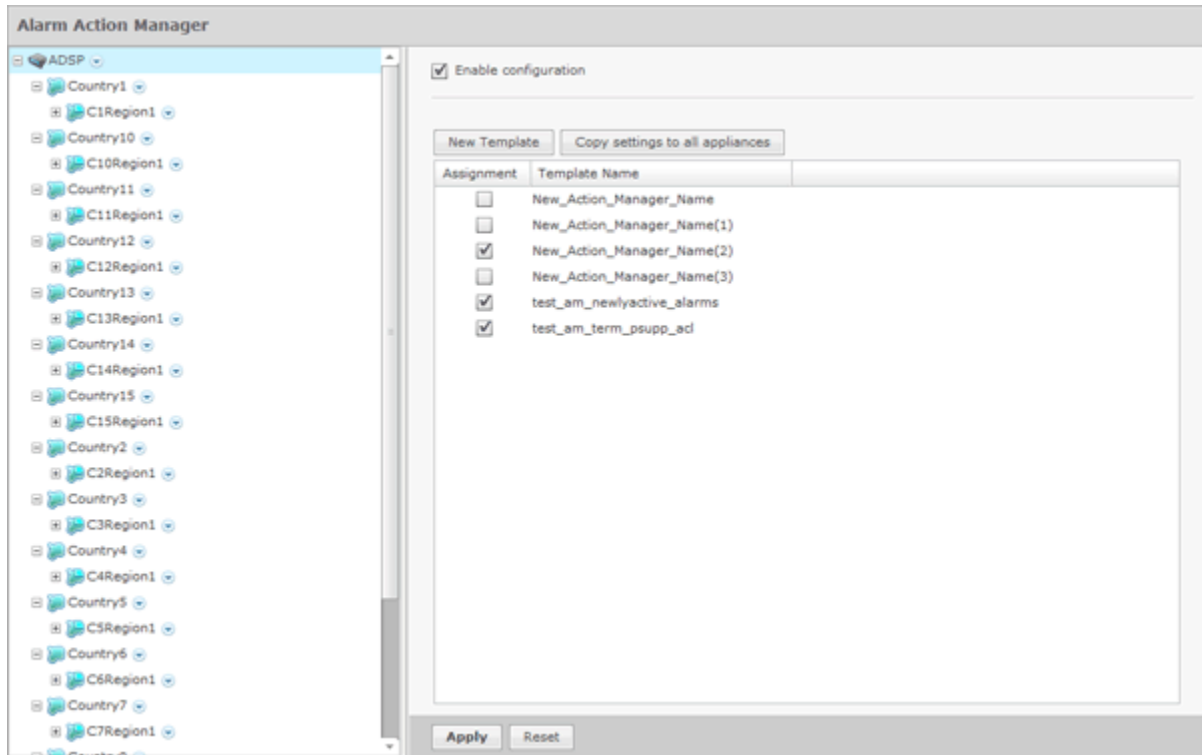
## Operational Management

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

- Automatically respond to alarms in your system with a predetermined action.
- 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 Action Manager

The Alarm Action Manager allows you to automatically respond to alarms in your system with a predetermined action called an Action Rule. By automating your response to certain alarms, you are free to concentrate on other administrative tasks; thus reducing management overhead. You may define as many Action Rules as you need to manage your network.



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

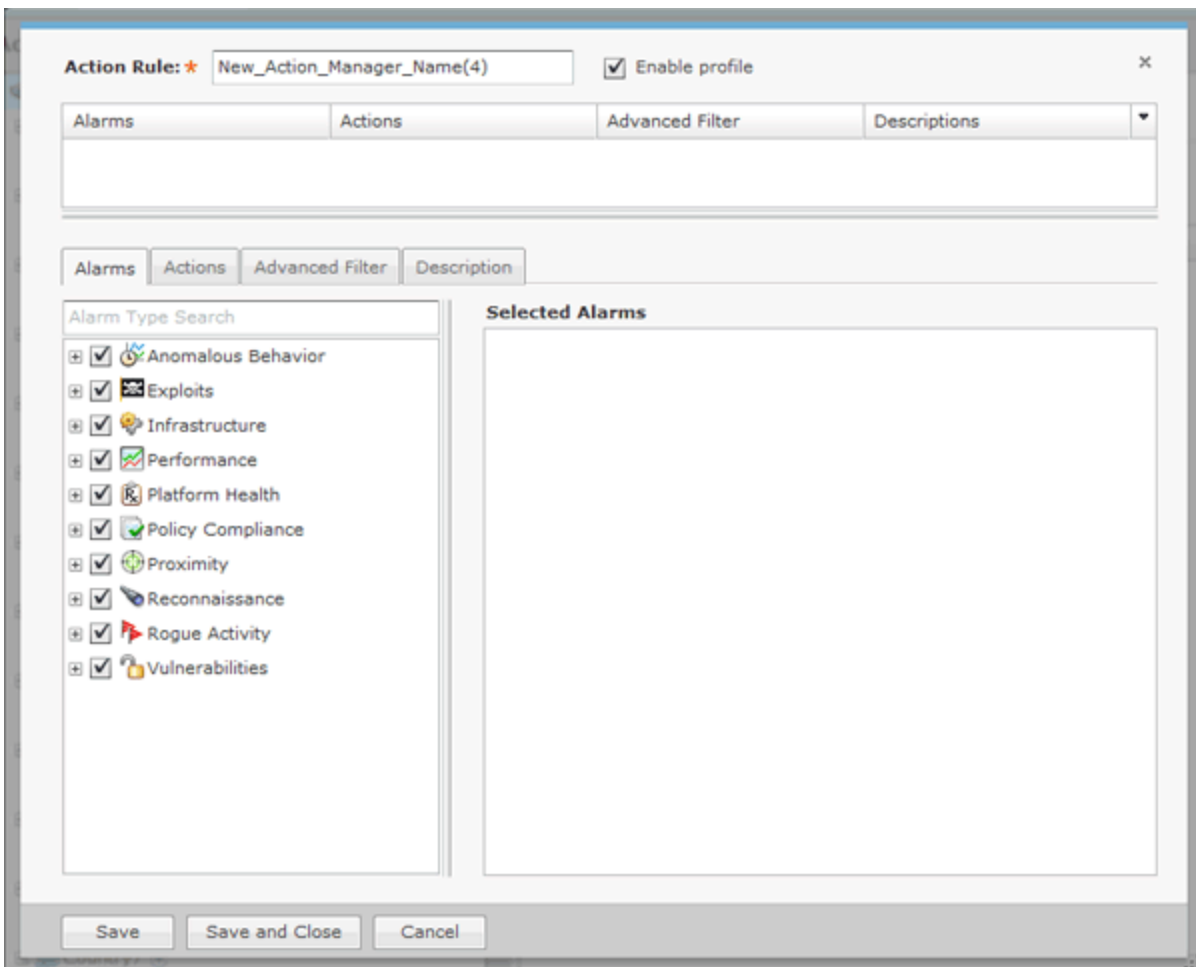
The Alarm Action Manager table displays one rule per row using the following columns:

Column	Description
Assignment	Specifies if a template defining an Action Rule is marked for use.
Template Name	The name of the template defining an Action Rule.

Once a template is added to the Alarm Action Manager, you can edit, copy, or delete it by selecting (highlighting) a template and then clicking on the appropriate link that appears to the right of the template.

### *Add/Edit Action Rule*

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



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

- Alarms
- Actions
- Advanced Filter
- Description.

### **Common Area**

The common area includes:

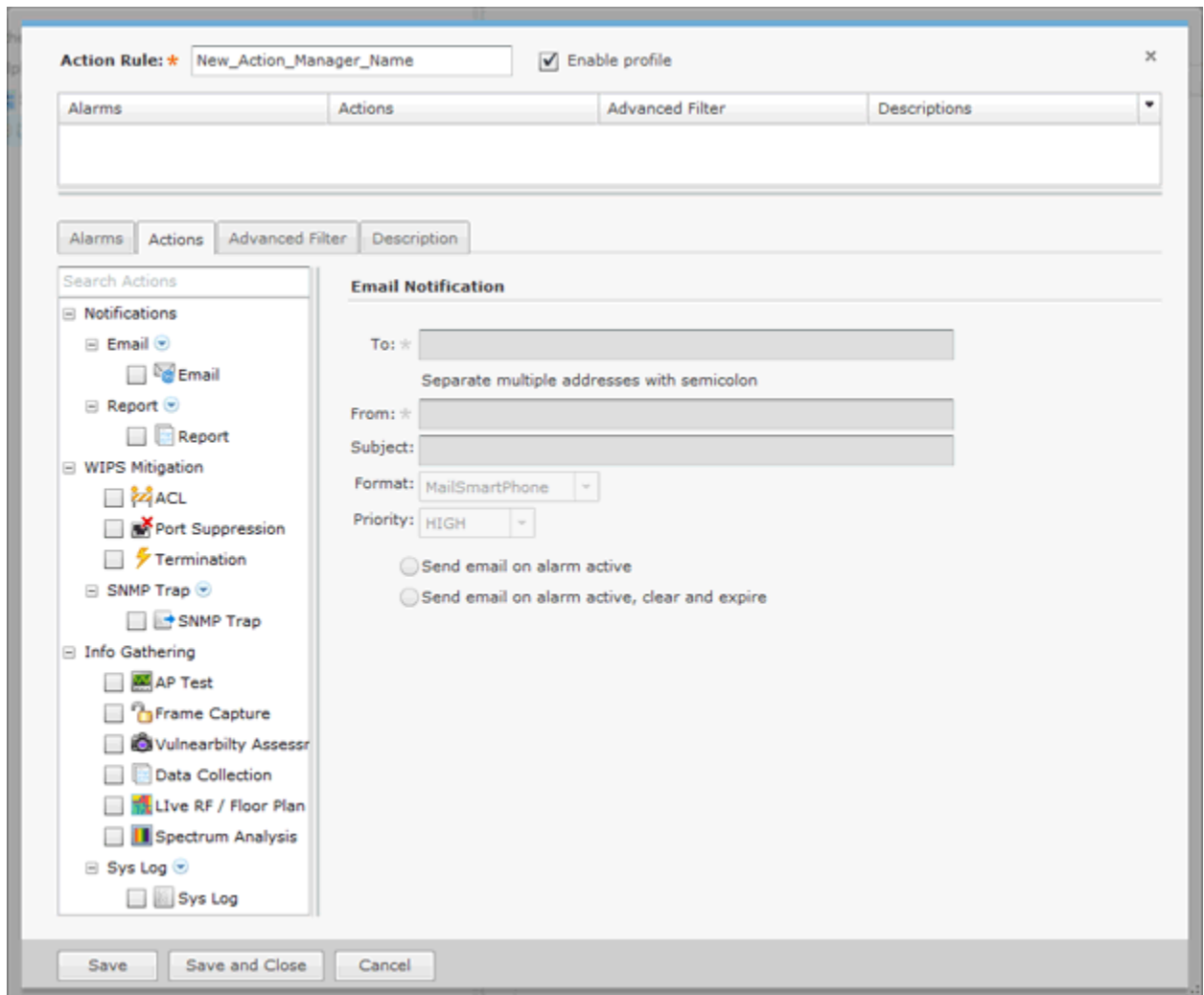
- An **Action Rule** field where you give your action rule a name.
- An **Enable profile** checkbox to enable the action rule.
- An action rule table that displays the values that you selected in the **Alarms**, **Actions**, **Advanced Filter**, and **Description** tabs.

### **Alarms Tab**

The **Alarms** tab is where you identify the alarms that you want to generate for your Action Rule. You may select one or more alarms to generate when the conditions in the filter are met.

## Actions Tab

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



Actions are divided into the following three categories:

- [Notifications](#)—Generates an email or a report if certain conditions are met.
- [WIPS Mitigation](#)—Mitigates a WIPS condition according to the selected action.
- [Info Gathering](#)—Executes one or more actions to gather information about your system.

Each category has actions specific to it. When an action is selected (highlighted), the information to execute the action is displayed on the right. Each action has its own set of fields/options that are used to execute the action.

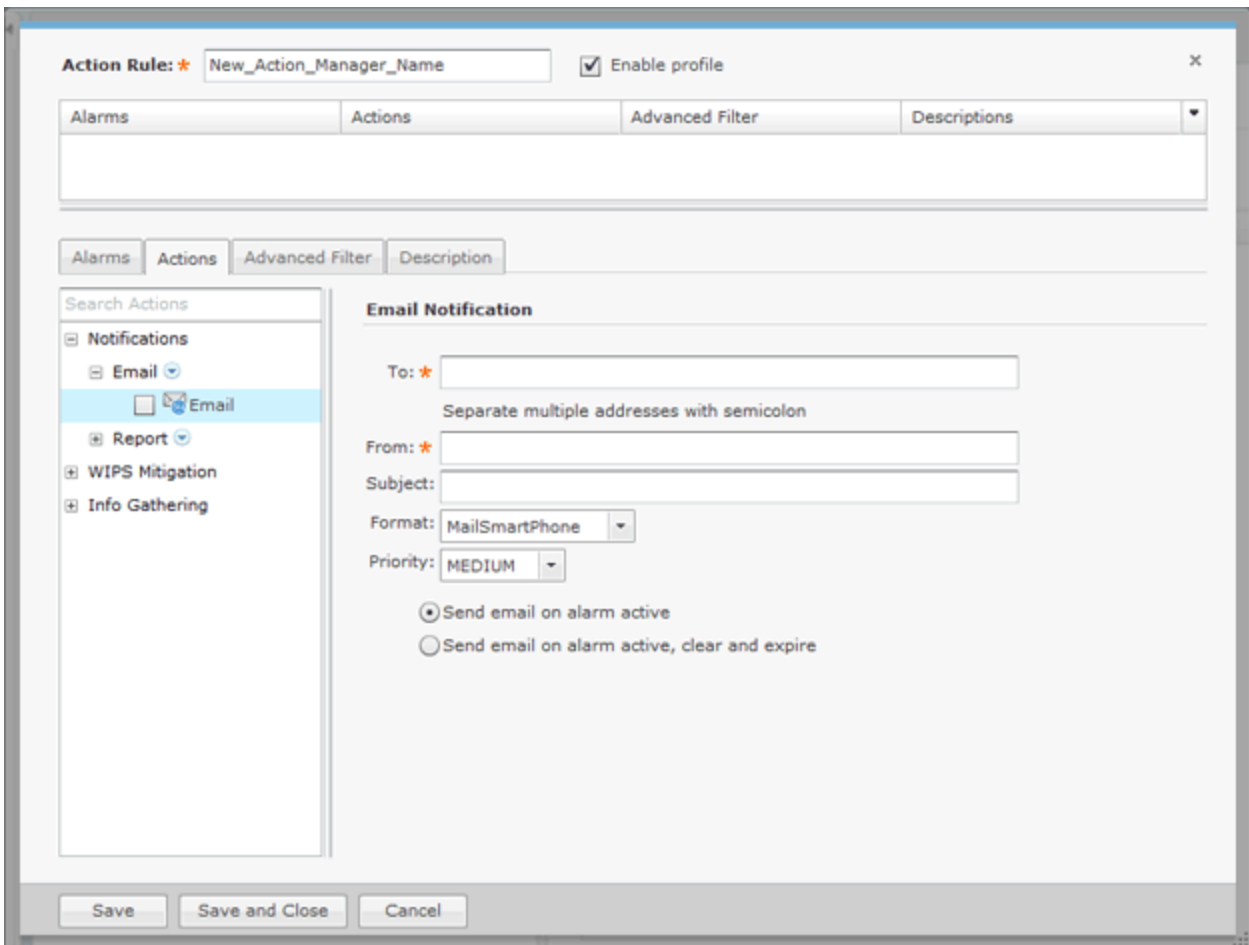
**Notifications**

The following actions are part of **Notifications**:

- [Email](#)
- [Report](#).

**Email**

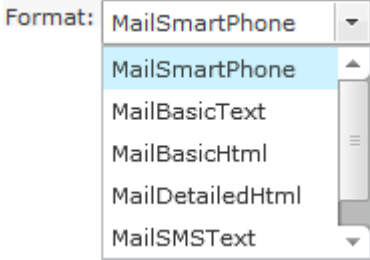
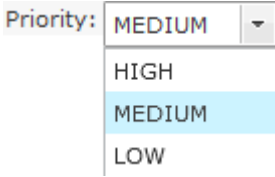
The Email action sends information about an alarm via email to a recipient if the conditions defined by the filter are met. To select the Email action, select **Notifications > Email** and then select **Email** from the **Search Actions**.



The following fields should be filled:

Field	Description
To	Specifies the email address of the recipient.
From	Specifies the email address of the sender.
Subject	Gives a short description of the email.



Field	Description
Format	<p>Specifies a format in which to send the email. Choose a format from the drop-down menu.</p> 
Priority	<p>Specifies a priority for the email. Choose a priority from the drop-down menu.</p> 
Send email options	<p>There are two options to send email:</p> <ul style="list-style-type: none"> <li>• Send email on alarm active—Send email on active alarms.</li> <li>• Send email on alarm active, clear and expire—Send email on active alarms, cleared alarms, and expired alarms.</li> </ul>

***Report***

The Report action runs a specific report if the conditions defined in the filter are met. To select the Report action, select **Notifications > Report** and then select **Report** from the **Search Actions**.

The following configuration fields are available:

Field	Description
Report Type	Specifies the type of report to run by selecting a report from the drop-down menu.
Scope Increase factor	Specifies the number of network levels to expand the scope. A value of 1 means only use the floor level. A value of 2 means use the floor and the floor's parent, and so forth.
Run immediate for previous	Executes the action immediately for the previous hours, days, or weeks.

Field	Description
Run on alarm clear / expire	Executes the action when a alarm clears or when a alarm expires. You have the option to execute for the duration of the alarm or for the previous hours, days, or weeks.
Publish	Specifies how to publish the report in Web Reporting: <b>SHARED</b> or <b>PRIVATE</b> . A shared report can be viewed by others. A private report can only be viewed by you. You should name the report to identify it.
E-mail	Specifies that you want to email the report when it runs. You have the option to email the report in one of the following formats: <b>HTML</b> , <b>PDF</b> , or <b>CSV</b> . You must furnish the email address of the person receiving the report.

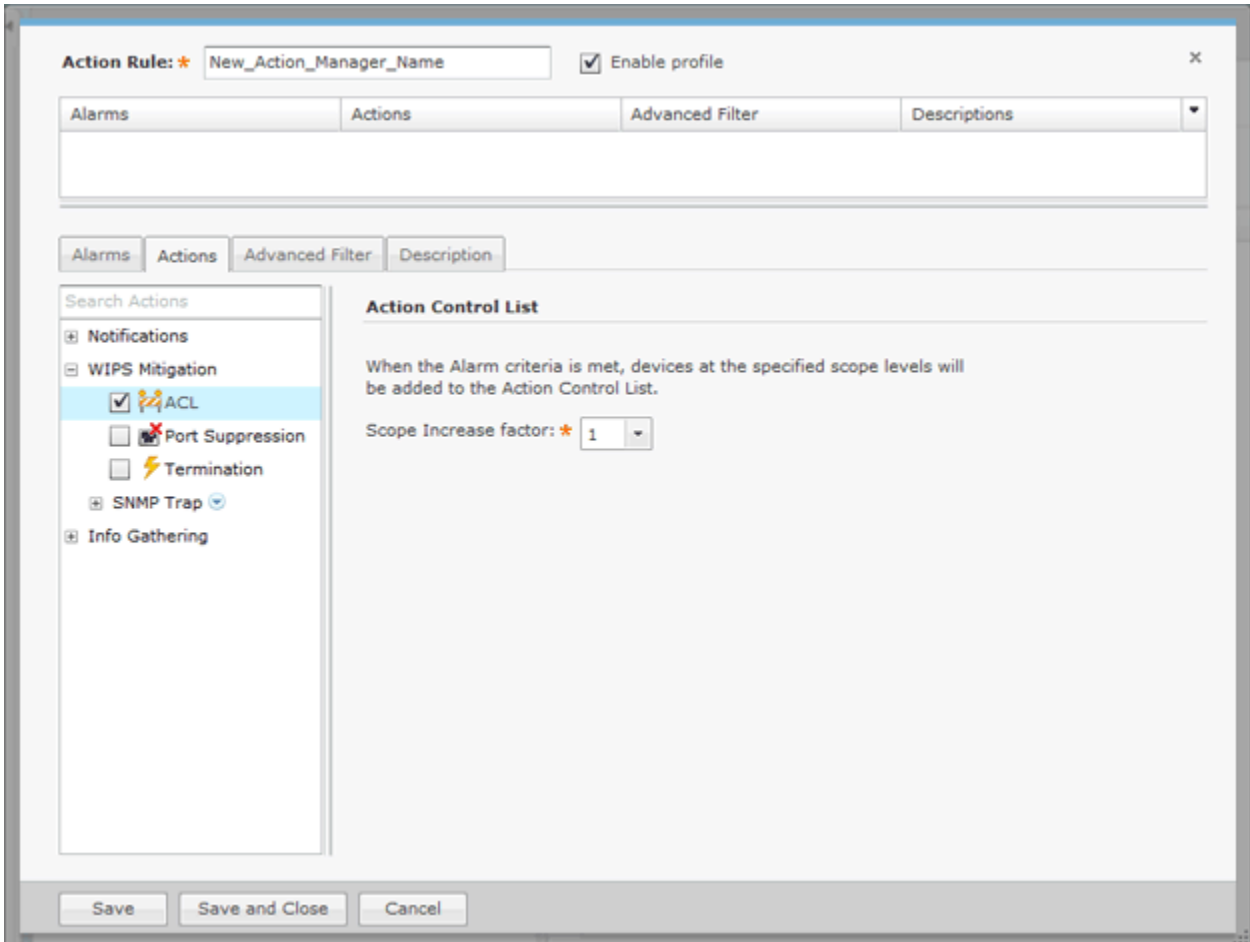
### WIPS Mitigation

The following actions are part of **WIPS Mitigation**:

- [ACL](#)
- [Port Suppression](#)
- [Termination](#)
- [SMNP Trap](#).

**ACL**

The ACL action enables the Access Control List on switches that meet the conditions defined in the filter. To select the ACL action, select **WIPS Mitigation > ACL** from the **Search Actions**.

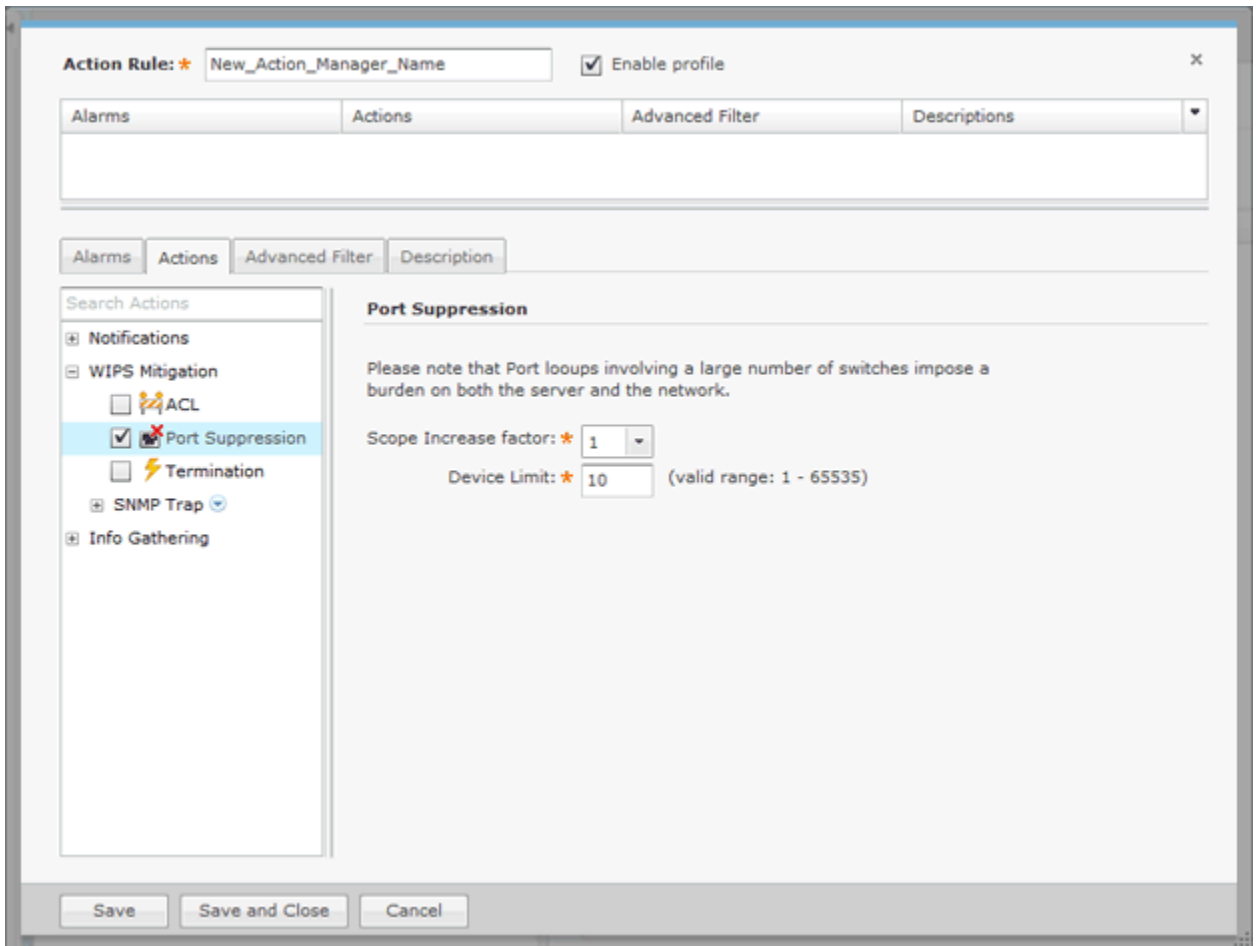


The **Scope Increase Factor** option specifies the number of network levels to expand the scope. A value of 1 means only use the floor level. A value of 2 means use the floor and the floor's parent, and so forth.

**Port Suppression**

The Port Suppression action is used to suppress communication between unauthorized devices and switches on your network. To select the Port Suppression action, select **WIPS Mitigation > Port Suppression** from the **Search Actions**.

- ✓ **NOTE** Before you can use Port Suppression, it must be enabled in **Configuration > Appliance Management > Appliance Settings**.



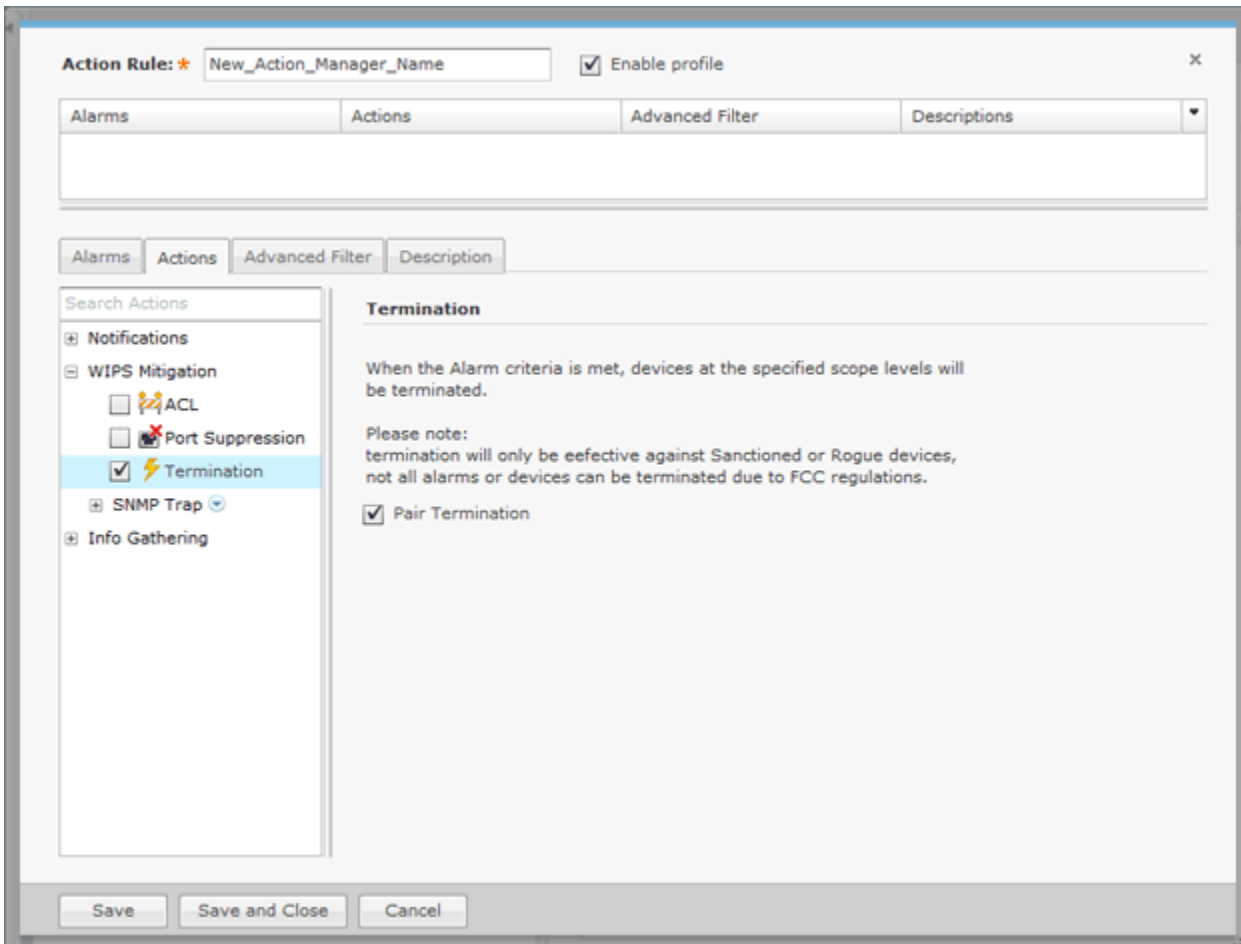
There are two options to configure: **Scope Increase Factor** and **Device Limit**.

The **Scope Increase Factor** option specifies the number of network levels to expand the scope. A value of 1 means only use the floor level. A value of 2 means use the floor and the floor's parent, and so forth.

The **Device Limit** option specifies a device limit. For instance, if you specify a device limit of 10 and more than 10 devices are connected to the port, the action will not be performed.

### ***Termination***

The Termination action is used to terminate devices that generate a certain alarm defined in the filter. To select the Termination action, select **WIPS Mitigation > Termination** from the **Search Actions**.



When **Pair Termination** is selected (the default state) and one of the following alarms is generated, the offending pair of devices are terminated:

- Ad-Hoc Connection between Sanctioned Stations
- Ad-Hoc Networking Extrusion Detected
- Sanctioned Client Association to Unsanctioned Virtual WiFi
- Unauthorized Roaming
- Unsanctioned Client Associated to Sanctioned Client running Virtual WiFi
- Wireless Client Accidental Association.

### GUI Configurations

Before you can use the Termination action, you must make the following GUI configurations:

1. Using the AirDefense GUI, go to **Configuration > Appliance Management > Appliance Settings**.



**NOTE** If you are not a user with read/write permission to the System Configuration functional area, the settings in **Appliance Management** will not appear, and you cannot edit the **Appliance Settings**.

2. Select the checkbox for **Air Termination system**.
3. Select the checkbox for **Policy-based Air Termination system**.
4. Click the **Apply** button.

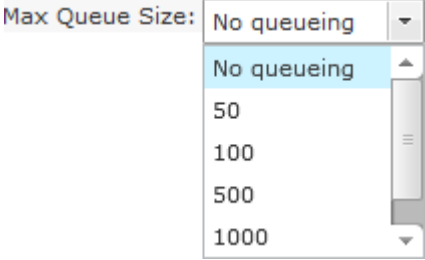
### SNMP Trap

The SNMP Trap action sends an SNMP notification to your SNMP server if the conditions defined in the filter are met. To select the SNMP Trap action, go to **WIPS Mitigation > SNMP Trap** and then select **SNMP Trap** from the **Search Actions**.

✓ **NOTE** Before you can use the SNMP Trap action, you must enable SNMP trap using [ADSPAdmin](#).

The following fields should be filled:

Field	Description
Server Address	Specifies the IP address of your SNMP server.
SNMP Port	Specifies the port you want to use for SNMP Notifications.
Community String	Specifies the community string for the receiving SNMP server. The string is a series of characters manipulated as a group, in this instance for SNMP.

Field	Description
Transport	<p>Specifies the desired transport protocol. Choices are:</p> <ul style="list-style-type: none"> <li>• UDP: User Datagram Protocol</li> <li>• TCP: Transmission Control Protocol.</li> </ul> <p><b>Hint:</b> Typically, UDP is the transport for SNMP traps. However, TCP can be useful for tunneling the traps over Secure Socket Layer (SSL).</p>
Max Queue Size	<p>Specifies the maximum queue size for the notification. Choose a size from the drop-down menu.</p> 
Send Time	<p>Specifies when to send the email by selecting one of the following conditions:</p> <ul style="list-style-type: none"> <li>• Send on alarm active</li> <li>• Send on alarm active, clear and expire</li> <li>• Send every x amount of minutes or hours.</li> </ul>

### Info Gathering

The following actions are part of **Info Gathering**:

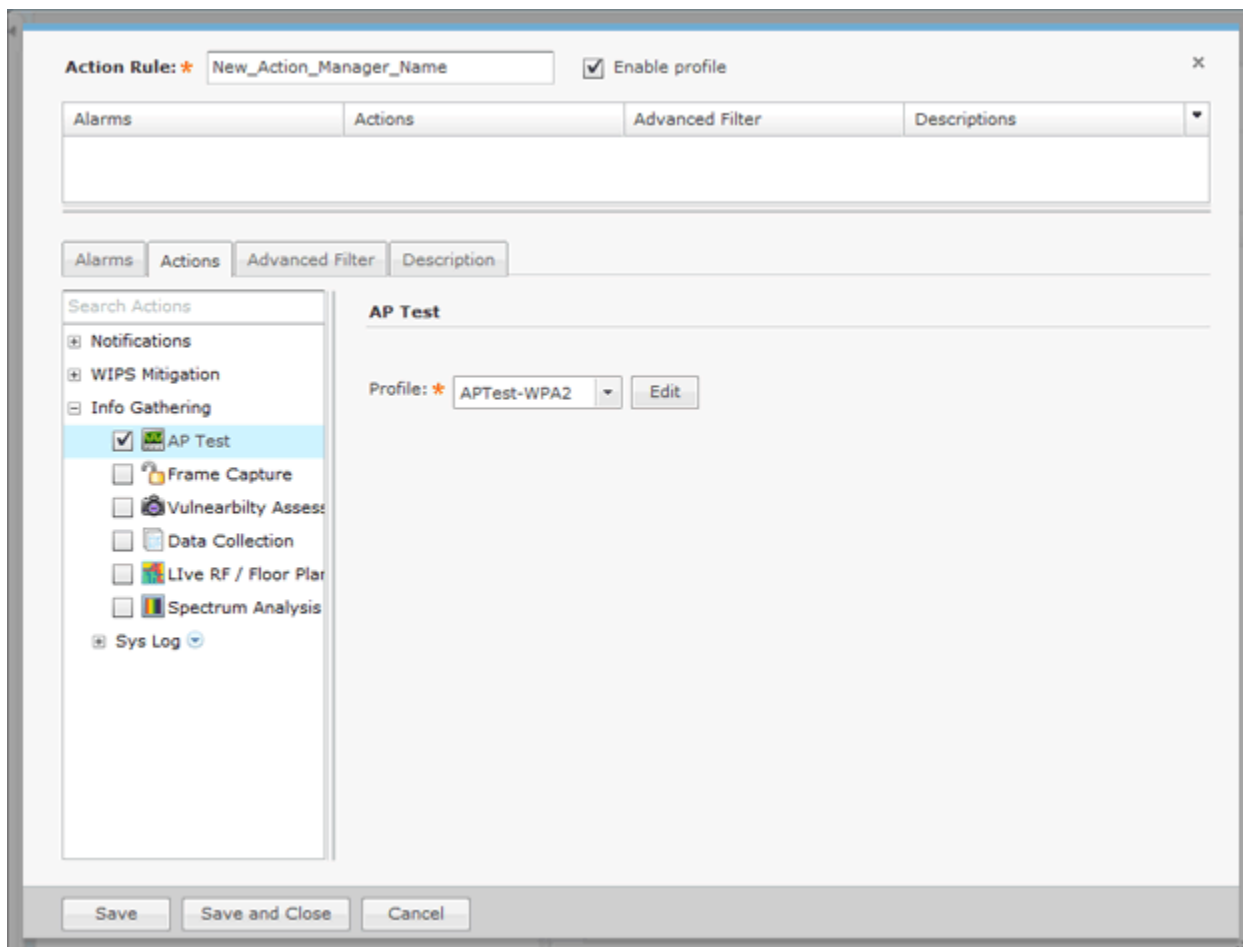
- [AP Test](#)
- [Frame Capture](#)
- [Vulnerability Assessment](#)
- [Data Collection](#)
- [Live RF / Floor Plan](#)
- [Spectrum Analysis](#)
- [Sys Log.](#)



***AP Test***

**NOTE** AP Test is part of the Advanced Troubleshooting module and requires an Advanced Troubleshooting license for access.

The AP Test action runs an AP Test using the specified profile if the conditions defined in the filter are met. To select the AP Test action, select **Info Gathering > AP Test** from the **Search Actions**.

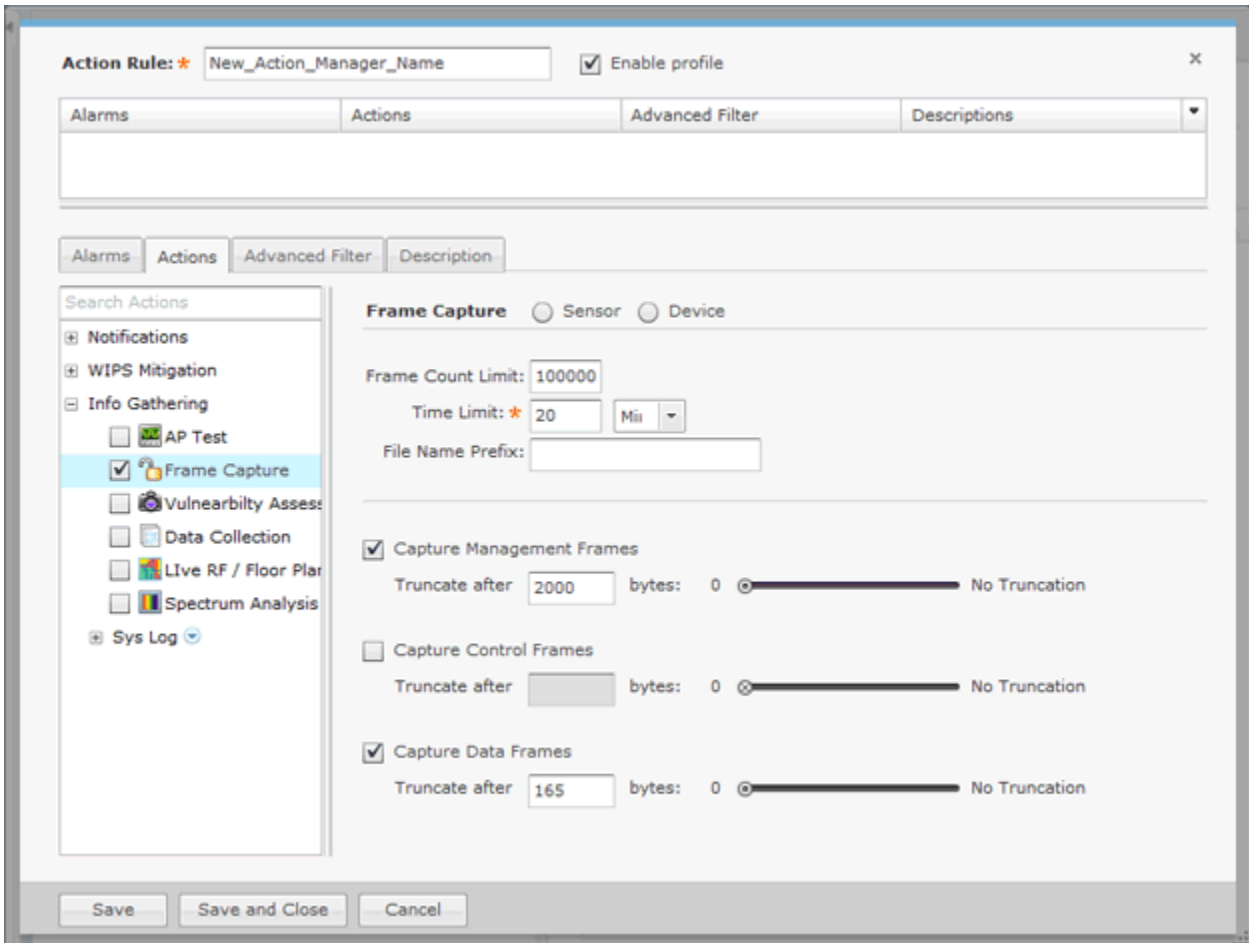


The following field is available:

Field	Description
Profile	Select a test profile from the drop-down menu. The <b>Edit</b> button can be used to modify the test profile. For more information on test profiles, refer to <a href="#">On-Demand Tests</a> for AP Test.

***Frame Capture***

The Frame Capture action 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 are met. To select the Frame Capture action, select **Info Gathering > Frame Capture** from the **Search Actions**.



The following configuration fields are available:

Field	Description
Frame Capture	Limits the scope of the frame capture to a Sensor or device.
Frame Count Limit	Limits the total amount of frames to capture.
Time Limit	Specifies a time duration for Frame Capture to run. You must enter x amount of minutes or hours.
File Name Prefix	Specifies a prefix for the file name. The prefix is added to a number sequence to make up the file name.
Capture Management Frames	Turns on capturing Management frames. Check the checkbox and slide the slider to specify when to stop capturing Management frames.
Capture Control Frames	Turns on capturing Control frames. Check the checkbox and slide the slider to specify when to stop capturing Control frames.
Capture Data Frames	Turns on capturing Data frames. Check the checkbox and slide the slider to specify when to stop capturing Data frames.

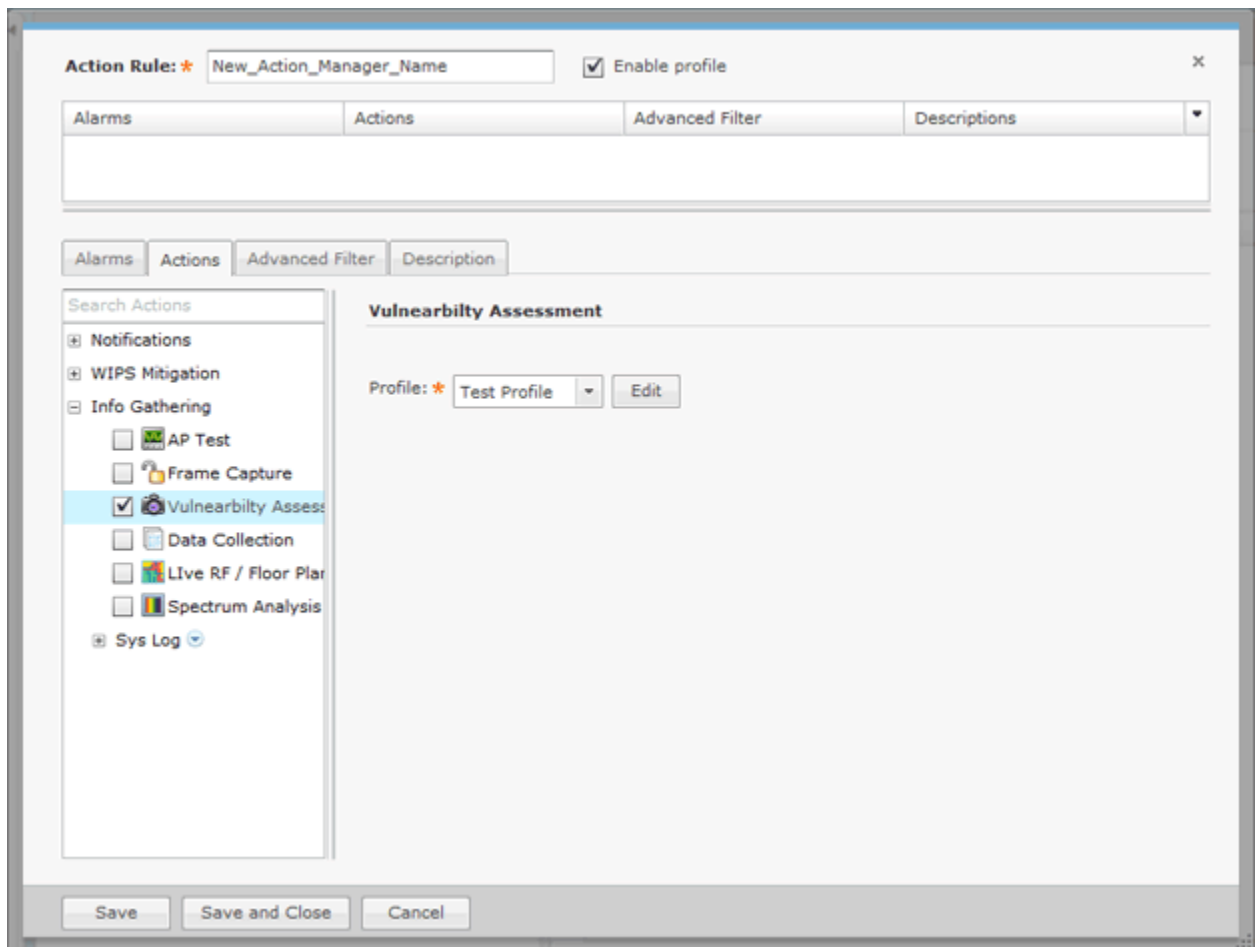
The captured file is stored in either—or, at times, both— of the following directories:

/usr/local/smx/pcaptures OR /usr/local/smx/pcaptures/saved.

### Vulnerability Assessment

✓ **NOTE** Vulnerability Assessment requires a Vulnerability Assessment license for access.

The Vulnerability Assessment action runs an vulnerability assessment using the specified profile if the conditions defined in the filter are met. To select the Vulnerability Assessment action, select **Info Gathering > Vulnerability Assessment** from **Search Actions**.



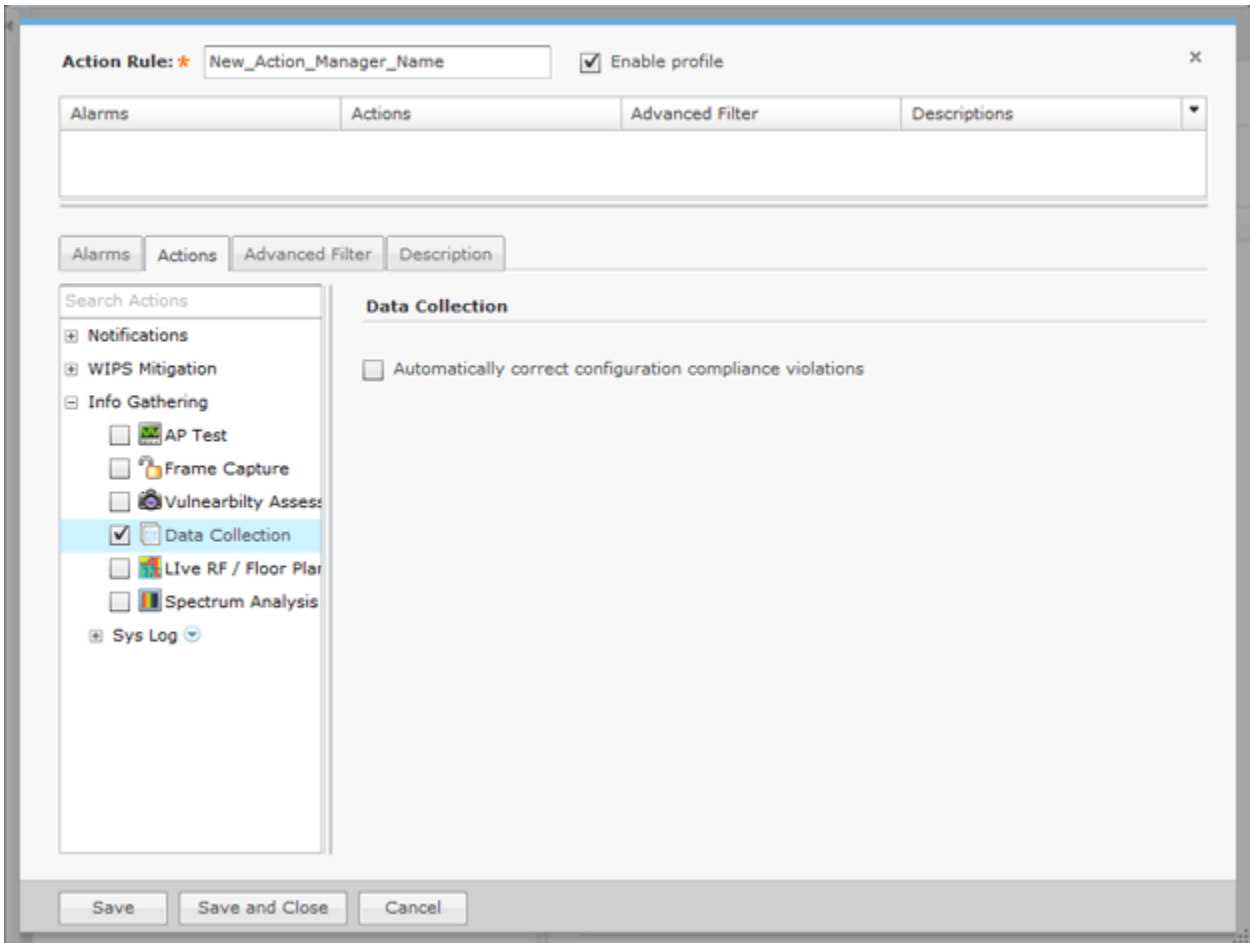
The following field is available:

Field	Description
Profile	Select an assessment profile from the drop-down menu. The <b>Edit</b> button can be used to modify the assessment profile. For more information on assessment profiles, refer to <a href="#">On-Demand Assessment</a> for Vulnerability Assessment.

Once you enable a Vulnerability Assessment action rule for BSSs, a vulnerability assessment will only start when ADSP detects a new alarm that was defined in the action rule. When the assessment is complete (after about 5 minutes), no other assessments will run until 10 minutes passes after the last vulnerability assessment was started. At that point, only another new alarm will trigger the Vulnerability Assessment action rule. No other assessments will run until a new alarm is detected. Once a new alarm is detected, the cycle repeats itself.

### Data Collection

The Data Collection action automatically corrects configuration compliance violations when the conditions defined in the filter are met. To select the Data Collection action, select **Info Gathering > Data Collection** from the **Search Actions**.

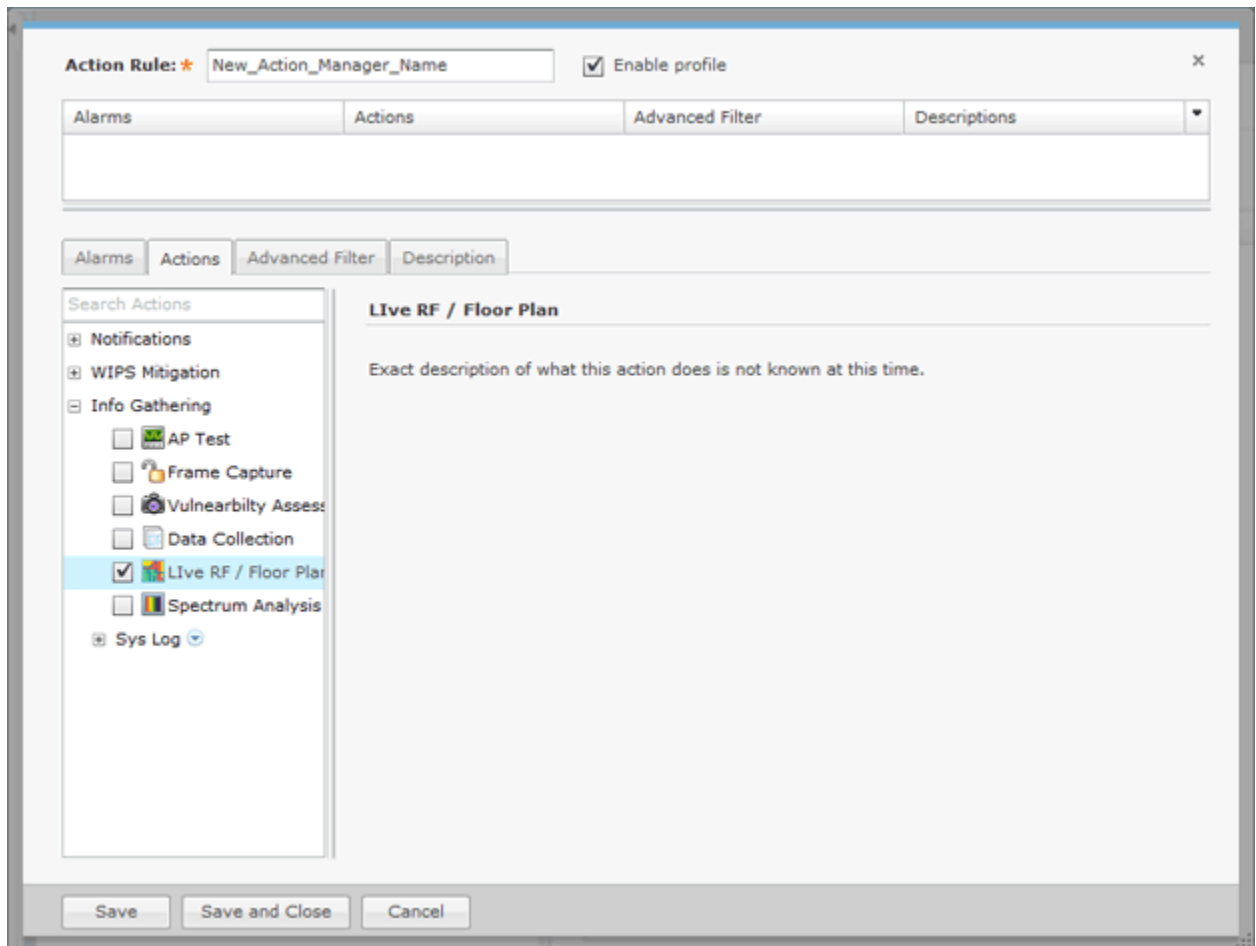


There is only one option: **Automatically correct configuration compliance violations**. When this option is selected and an alarm is generated by a device meeting the conditions specified in the filter, ADSP automatically uploads the last approved configuration to the device to correct any violations.

### Live RF / Floor Plan

✓ **NOTE** Live RF / Floor Plan requires a Live RF license for access.

The Live RF / Floor Plan action runs an infrastructure device poll to update the heat map predictions in Live RF if the conditions defined in the filter are met. The next time the user accesses Live RF / Floor Plan they'll see the latest updates, and will be able to see whether or not any APs or Sensors are offline. To select the Live RF / Floor Plan action, select **Info Gathering > Live RF / Floor Plan** from the **Search Options**.



There are no configuration options for Live RF / Floor Plan.

***Spectrum Analysis***

✓ **NOTE** Spectrum Analysis requires a Spectrum Analysis license for access.

The Spectrum Analysis action runs a regular Spectrum Analysis or an Advanced Spectrum Analysis using the specified profile if the conditions defined in the filter are met. To select the Spectrum Analysis action, select **Info Gathering > Spectrum Analysis** from the **Search Actions**.

The screenshot displays the configuration interface for the Spectrum Analysis action. At the top, the 'Action Rule' is 'New\_Action\_Manager\_Name' and the 'Enable profile' checkbox is checked. Below this is a table with columns for 'Alarms', 'Actions', 'Advanced Filter', and 'Descriptions'. A search bar is present above the table. The 'Search Actions' panel on the left shows a tree view with 'Info Gathering' expanded and 'Spectrum Analysis' selected. The main configuration area for 'Spectrum Analysis' includes:
 

- Time Limit:** 5 Minute(s)
- File Name Prefix:** SA\_
- Spectrum Settings / Advanced Spectrum Settings:** Two tabs are visible, with 'Spectrum Settings' selected.
- Scan Type:** Radio buttons for 'Full Scan' (selected) and 'Interference Scan'.
- Pulse Definition:**
  - Threshold:** -75 dBm
  - Width:** 250 microseconds

 At the bottom, there are 'Save', 'Save and Close', and 'Cancel' buttons.

The following fields are available:

Field	Description
Time Limit	Places a time limit on how long the Spectrum Analysis will run.
File Name Prefix	Defines a prefix for the Spectrum Analysis file. You may add to the prefix if you want to.
Spectrum Settings	Only used in regular Spectrum Analysis. These are the same <b>Spectrum Settings</b> described under <a href="#">Dedicated Analysis</a> .
Advanced Spectrum Settings	Only used in Advanced Spectrum Analysis. These are the <b>Dedicated Scan Settings</b> described under <a href="#">Advanced Spectrum Analysis</a> . The <b>In-Line Scan</b> options cannot be changed. The <b>Dedicated Scan</b> options can be adjusted as needed.

***Sys Log***

The Sys Log action sends an alarm notification to your Sys Log server if the conditions defined in the filter are met. To select the Sys Log action, select **Info Gathering > Sys Log > Sys Log** from the **Search Options**.

**Action Rule:** \*   Enable profile

Alarms    Actions    Advanced Filter    Descriptions

Alarms    Actions    Advanced Filter    Description

Search Actions

- Notifications
- WIPS Mitigation
- Info Gathering
  - AP Test
  - Frame Capture
  - Vulnerability Assessment
  - Data Collection
  - Live RF / Floor Plan
  - Spectrum Analysis
- Sys Log
  - Sys Log

**Sys Log**

Server Address: \*

Syslog Port: \*

Facility:

Format:

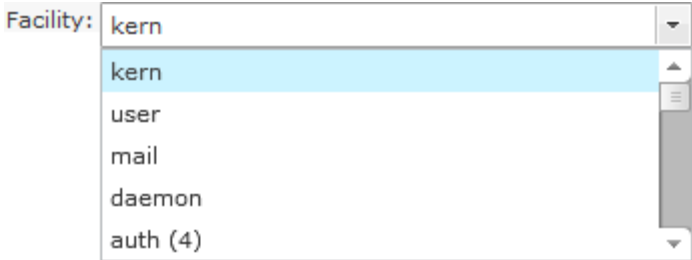
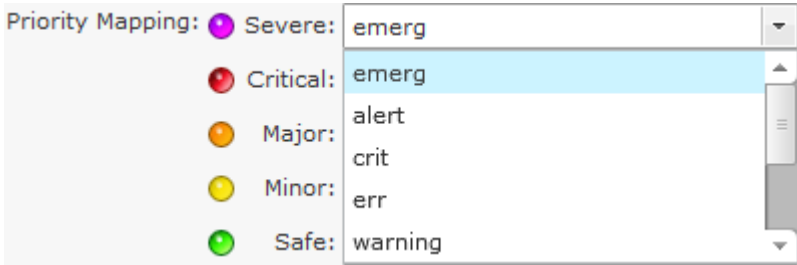
Email Send Time:

Priority Mapping:

- Severe:
- Critical:
- Major:
- Minor:
- Safe:

Save    Save and Close    Cancel

The following fields should be filled:

Field	Description
Server Address	Specifies the IP address of your Syslog server.
Syslog Port	Specifies the port you want to use for Syslog Notifications.
Facility	<p>Specifies a Syslog Facility which is an information field associated with a Syslog message. It is defined by the Syslog protocol. The intent of the facility is to provide an indication as to what part of the system the Syslog message originated.</p> <p>This facility can be very helpful to define rules that split messages, for example, to different log files based on the facility level.</p> <p>Choose a Syslog Facility from the drop-down menu.</p> 
Format	Specifies the format of the notification. At this time, the only option is <b>Syslog</b> .
Email Send Time	<p>Specifies when to send the email by selecting one of the following conditions:</p> <ul style="list-style-type: none"> <li>• On Alarm Activation</li> <li>• On Activation, clear or expire</li> <li>• Every x amount of minutes or hours.</li> </ul>
Priority Map	<p>The Priority Map enables you to change the name of the default priorities to an alternate selection. Click on the drop-down menu for the priority you would like to change and choose from the list. For example, if you want to change the priority for Severe, select an option from the <b>Severe</b> drop-down menu.</p> 



### Advanced Filter Tab

The **Advanced Filter** tab allows you to build a custom alarm filter or an expression to use as a alarm filter.

### **Filter List**

The Filter List lets you build an alarm filter from two or more conditions. To start a Filter List, click the **Filter List** radio button. Start off selecting when the filters (**When** statement) will be used. There are four options:

- All—All of the selected conditions must be met (logical “and” operation).
- Any—One or more selected conditions must be met (logical “or” operation).
- None (All)—None of the selected conditions are met (logical “and” operation).
- None (Any)—One or more selected conditions are not met (logical “or” operation).

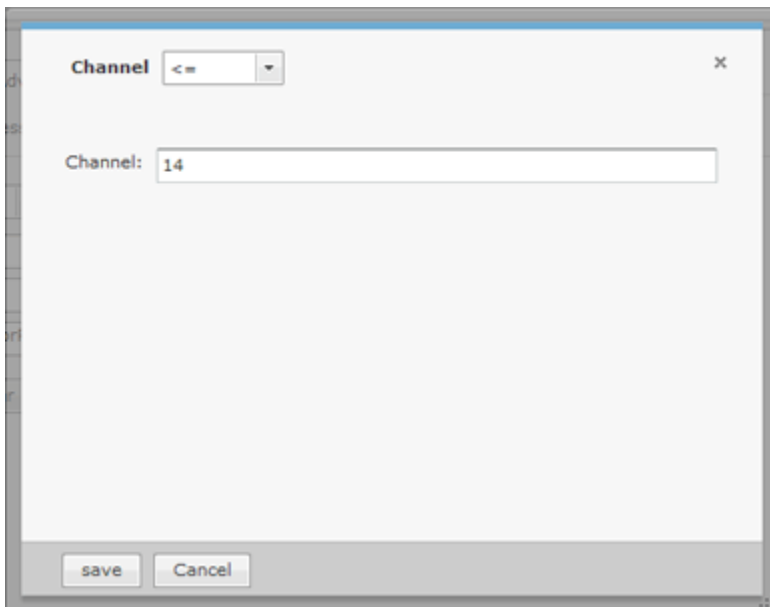
The **When** statement works together with an **If** statement matching a filter with a value. The available filters are:

- AdditionalInfo
- Adhoc
- Associated
- AssociatedBSSClassification
- AssociatedBSSIP

- AssociatedBSSMAC
- AssociatedBSSName
- AssociatedBSSVendorPrefix
- Channel
- ConnectedToWired
- Criticality
- Device802\_1XName
- DeviceAuditTime
- DeviceAuthentication
- DeviceCapabilities
- DeviceClassification
- DeviceClientType
- DeviceDHCP
- DeviceDNS
- DeviceEncryption
- DeviceFirmware
- DeviceFirstPolled
- DeviceFirstSeen
- DeviceIP
- DeviceLastAdoption
- DeviceLastDataPoll
- DeviceLastPolled
- DeviceLastSeen
- DeviceLastStatusPoll
- DeviceMAC
- DeviceManufacturer
- DeviceModel
- DeviceName
- DevicePolledID
- DevicePolledSSID
- DeviceProtocol
- DeviceSSID
- DeviceSensedID
- DeviceSensedSSID
- DeviceSerial

- DeviceType
- DeviceVendorPrefix
- SensorIP
- SensorMAC
- SensorName
- SignalStrength
- WatchList
- WiFiDirect.

When a filter is selected, an **Edit** button is displayed. Click the **Edit** button to select a mathematical comparison to indicate the relationship between the filter and a value that you specify.



Click the drop-down menu to select the type of comparison. This will vary according to the selected filter. The type of comparison may be:

- = Is equal to
- != Is not equal to
- < Is less than
- <= Is less than or equal to
- > Is greater than
- >= Is greater than or equal to
- LIKE Is similar to, matches some portion (Used for a partial match)
- ILIKE Case insensitive partial match
- IN Condition exists within the filter value (usually used when the filter combines two or more variables which must be compared in some way to create a trigger)

There will be one or more other fields to determine a value. This will vary according to the selected filter.

Click the **Save** button to save the comparison.

The following screen shot shows an example of a Filter List.

The screenshot displays the configuration for an Action Rule named "New\_Action\_Manager\_Name". At the top, there is a text input field for the rule name and a checked "Enable profile" checkbox. Below this is a horizontal menu with tabs for "Alarms", "Actions", "Advanced Filter", and "Descriptions". The "Advanced Filter" tab is selected, showing a "Filter List" configuration. Under "Filter List", there are radio buttons for "Filter List" (selected) and "Expression Editor". The configuration specifies "When All of these filters are met...". There are two filters listed: "If Channel" and "And DeviceMAC". Each filter has an "Edit" button and a close "x" button. At the bottom, there is an "Add Another" button with the text "(limit: 25 filters)".

You can have up to 10 filters. Just click the **Add Another** button to add additional filters.

You can remove a filter by clicking the **x** next to the filter.

### Expression Editor

The Expression Editor allows you to build a filter using expressions. An expression is made up of a field, operator (parentheses or quotation marks), and a value. The filters are the same as the ones used in the [Filter List](#).

The operators (parentheses and quotation marks) are:

- !
- (
- )
- AND
- OR
- =           Is equal to
- !=           Is not equal to
- <            Is less than
- <=           Is less than or equal to
- >            Is greater than
- >=           Is greater than or equal to

- LIKE Is similar to, matches some portion (Used for a partial match)
- ILIKE Case insensitive partial match
- IN Condition exists within the filter value (usually used when the filter combines two or more variables which must be compared in some way to create a trigger)
- " Wildcard matching any character
- NOT IN Opposite of IN. Condition does not exist within the filter value.

You can use AND/OR or parentheses to create complex expressions.

The filter is selected from a drop-down menu while the operators (parentheses and quotation marks) are selected by clicking on them. The filter values vary depending on the filter just like in the [Filter List](#).

You may type in part or all of the expression. If the expression is valid, a message "Parsing successful." is displayed at the bottom of the window. If the expression is invalid, an error message is displayed.

The screenshot shows a configuration window for an Action Rule. At the top, there is a field for 'Action Rule' with the value 'New\_Action\_Manager\_Name' and a checked 'Enable profile' checkbox. Below this is a table with columns for 'Alarms', 'Actions', 'Advanced Filter', and 'Descriptions'. The 'Alarms' column contains 'EAP Handshake Flood' and the 'Advanced Filter' column contains 'DeviceSSID LIKE ".\*abc.\*" AND Descriptions Tab content'. Below the table are tabs for 'Alarms', 'Actions', 'Advanced Filter', and 'Description'. The 'Expression Editor' tab is selected, showing a text area with the expression: 'DeviceSSID LIKE ".\*abc.\*" AND DeviceManufacturer ILIKE ".\*cisco" AND SensorMAC IN ("00:16:5d:.\*")'. A 'Parsing successful.' message is displayed in green at the bottom of the text area. At the bottom of the window are 'Save', 'Save and Close', and 'Cancel' buttons.

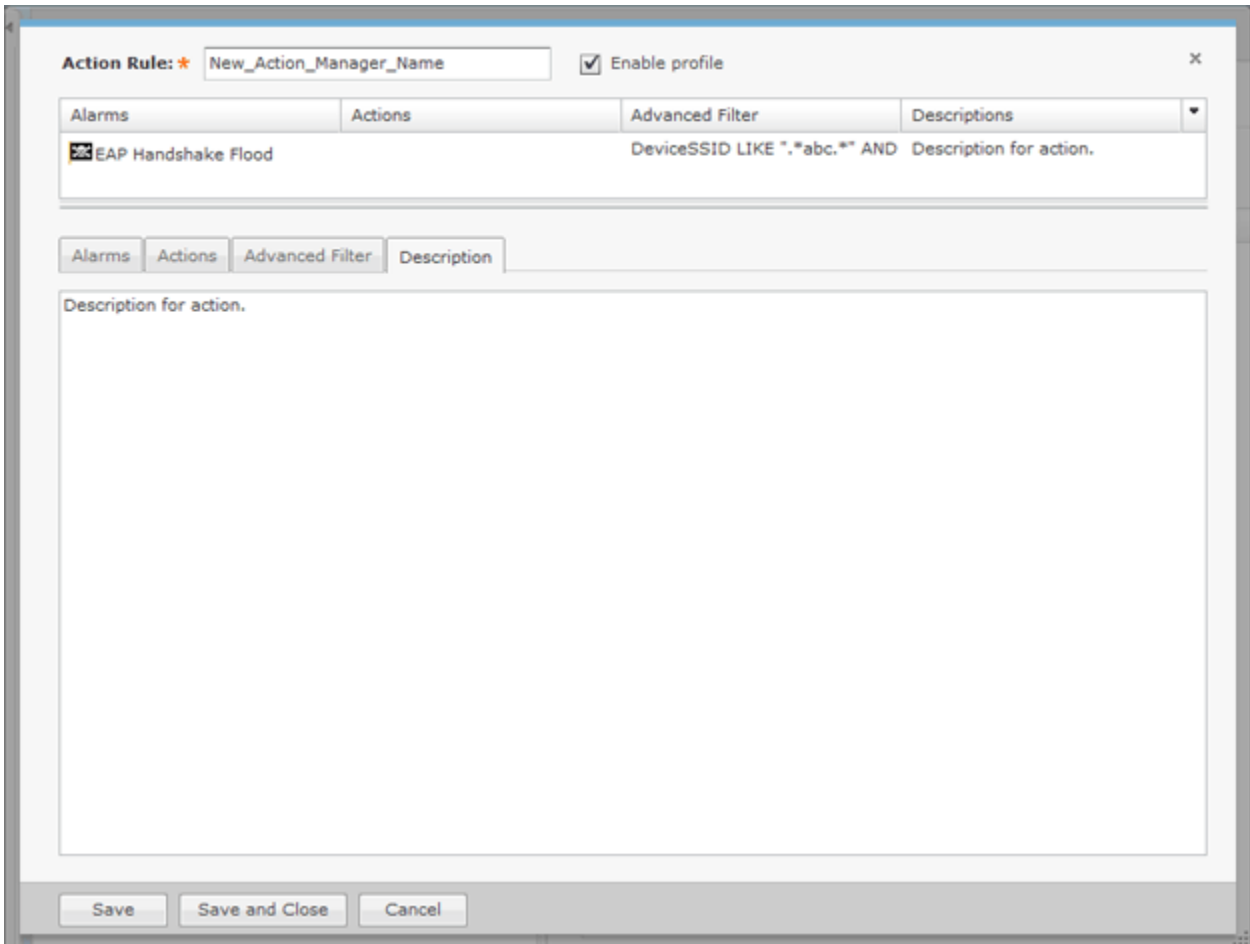
Notice the use of wildcards in the screen shot expression:

DeviceSSID LIKE ".\*abc.\*" AND DeviceManufacturer ILIKE ".\*cisco" AND SensorMAC IN ("00:16:5d:.\*")

Using wildcards with the operators LIKE, ILIKE, or IN, you must use .\* If you use just \*, the Action Rule will fail.

**Description Tab**

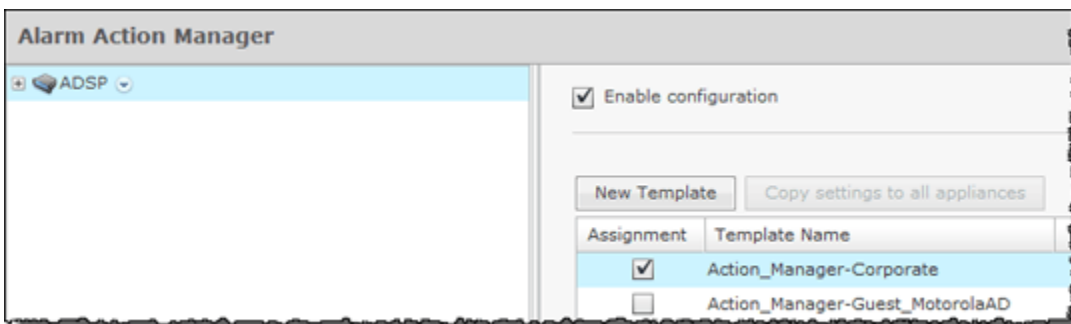
The **Description** tab is used to give your action a description.



Type a description and then click **Save** or **Save and Close**.


**Applying an Alarm Action Manager Template**

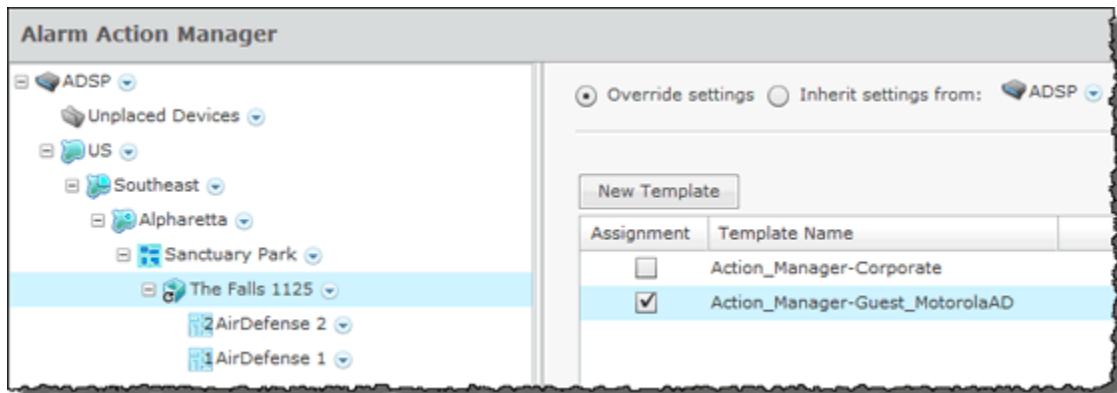
Once you have defined an Alarm Action Manager template, to use it, you must apply it to your system.



✓ **NOTE** You may select multiple Alarm Action Manager templates by checking more than one checkbox.

You should always apply an Alarm Action Manager template at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Alarm Action Manager template, you can apply that template to that level. For example, in the above screen shot, the Alarm Action Manager template for ADSP could be the **Action\_Manager-Corporate** template and then for a special case (in the following screen shot) you could override the Alarm Action Manager template at the ADSP level and apply the **Action\_Manager-Guest\_MotorolaAD** template to the **The Falls 1125** network level.

- ✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



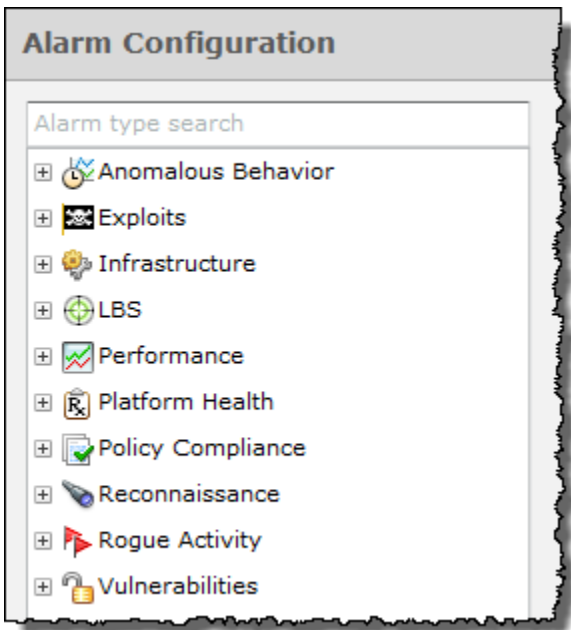
You can copy Alarm Action Manager templates to all your appliances by clicking the **Copy settings to all appliances** button.

- ✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

## 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. To access this feature, go to [Configuration > Operational Management > Alarm Configuration](#).



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

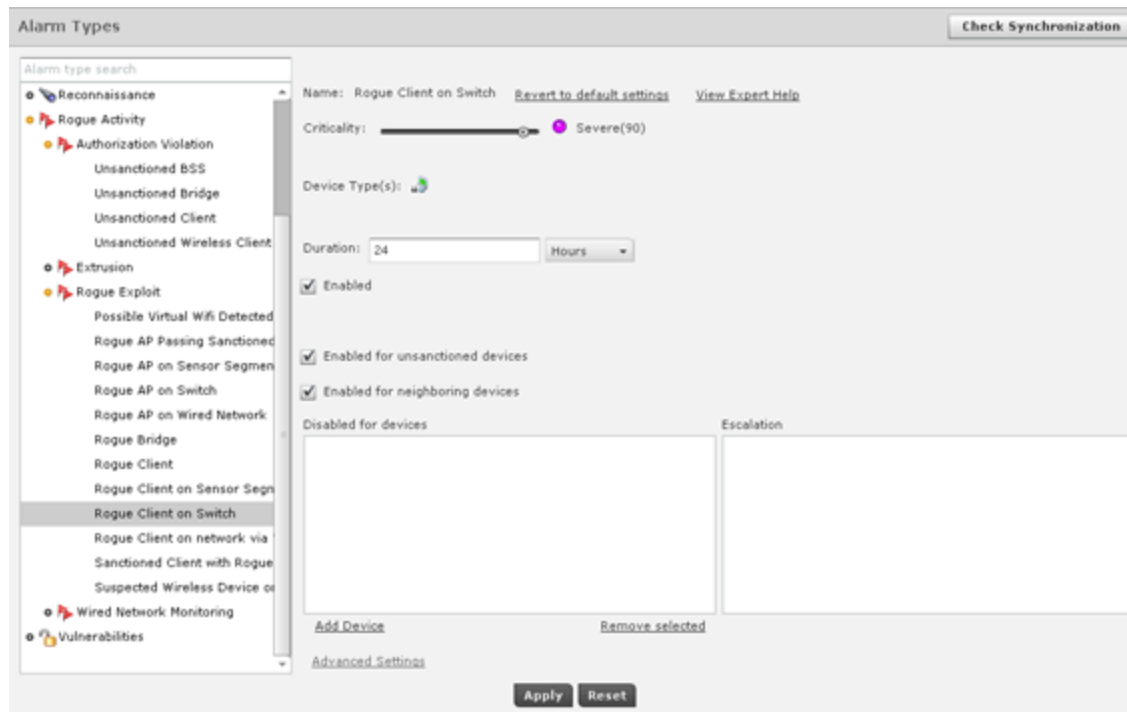
- Anomalous Behavior—Devices that operate outside of their normal behavior settings and generate events that could indicate anomalous or suspicious activity.
- Exploits—Events caused by a potentially malicious user actively interacting on your Wireless LAN using a laptop/PC as a wireless attack platform.
- Infrastructure—Events that are generated based on the SNMP traps received from the infrastructure devices.
- LBS—Events that are based on a Wireless Client's presence or events based on a Wireless Client's proximity to predefined virtual region.
- 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.

To configure an alarm, you must use the tree to drill down to the alarm and then make changes (see [Configuring Alarms](#)) or you can use Alarm type search. Just start typing related text until you see the alarm you are searching for.



## Configuring Alarms

Before you can configure an alarm, you must drill down to it using the alarm tree. First select an alarm type, then an alarm sub-type, and then click on the alarm to highlight it.



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.

Option	Description
Duration	<p>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.</p>
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 <b>Add Device</b> 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 <b>Advanced</b> link will display a <b>Device Search</b> dialog window. You can then search for a device using any combination of the following criteria:</p> <ul style="list-style-type: none"> <li>• Device name</li> <li>• MAC address</li> <li>• 802.1X name</li> <li>• DNS name</li> <li>• Vendor name</li> <li>• SSID</li> <li>• Protocol used.</li> </ul> <p>After selecting your search criteria, click the <b>Search</b> 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 <b>Close</b> when you are done.</p> <p>You can return to the original window by clicking the <b>Basic</b> link where you can enter only the MAC address.</p> <p>Clicking the <b>Remove selected</b> 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.

Click **Apply** to save your changes. You can revert back to the original settings by clicking the **Reset** link.

The **Check Synchronization** button is used to check all appliances in the network to ensure they are using the same alarm configuration. (The synchronization features works basically the same way wherever the feature is implemented. Synchronizing Accounts has a good example of how the synchronization feature works.)

✓ **NOTE** You must have a Central Management license in order to use the Check Synchronization feature.

### ***Anomalous Behavior Alarms***

Behavior Alarms track atypical device behavior based on a long term forensic baseline of devices at that site. ADSP utilizes the Forensic Datastore to monitor and store over 325 wireless statistics for each device on a minute-by-minute basis. Statistical analysis is performed over 2 weeks of this historical data to create a baseline of activity for devices. Events are generated when a device operates outside of its normal behavior to alert the administrator of anomalous or suspicious behavior.

For example, consider a user device that has a wireless usage behavior baseline of basic web and email access. A behavior event would be raised if this user then suddenly downloads significant amount of data after business hours, a time period when the station is not normally active. This anomalous behavior could be indicative of a stolen or spoofed identity, or disgruntled employee that may be downloading significant amounts of confidential and/or proprietary information.

#### **Behavior Alarm Sub-Types**

Behavior Alarms are broken down into the following two sub-types:

- BSS Abnormal Activity—Anomalous behavior events specific to BSSs.
- Wireless Client Abnormal Behavior—Anomalous behavior events specific to Wireless Clients.

#### **Alarm Library**

To view a list of Behavior Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Anomalous Behavior**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***Exploits Alarms***

Exploits are events in which a user is actively interacting with the wireless network or wireless medium. By exploiting wireless vulnerabilities a malicious user could cause wireless network disruptions or use the wireless medium to gain access to corporate resources and confidential data. The vulnerabilities may exist due to network configuration, corporate policy, or an inherent flaw in the 802.11 protocol. A malicious user with basic computer skills, a laptop, and a CD drive can obtain various sets of open source tool kits which will transform the laptop into a fully configured wireless attack platform.

As time has progressed these tools kits have become increasingly easier to use while offering an increasingly sophisticated toolset. The bottom line is the wireless attack tools have become accessible to a broader range of users. Because exploits involve active interaction with the wireless network, AirDefense recommends timely action to understand and mitigate the threat to minimize security exposure.

#### **Exploits Alarms Sub-Types**

Exploits Alarms are broken down into the following three sub-types:

- Active Attacks—Active attacks subcategory includes active malicious interaction with the wireless network. Active attacks are severe and present a high security risk and potential for significant exposure. Because these events are active in the wireless network, timely investigation is recommended to prevent the attack from continuing. These

events can be mitigated wirelessly to minimize and prevent continued exposure; mitigation can be initiated manually by the administrator or automatically if the system has been configured for policy-based termination.

- **DoS—Denial of Service (DoS)** events can cause significant disruption in the wireless networks by preventing a user from accessing a wireless resources. In wireless networks, DoS events can happen in two forms: the first form is a DoS attack directed at a specific device and the second form is a DoS attack directed at the wireless medium. Device level attacks will affect one or more devices depending on the attack setup; broadcast attacks for example can impact all stations associated to an Access Point, whereas a more directed attack will only impact a single station leaving other stations connected to the Access Point. In either case DoS attacks of this nature consume wireless bandwidth. The second type of attacks directed at the medium exploit inherent flaws in the 802.11 protocol impacting all devices on the channel by making the medium temporarily unusable. Denial of Service (DoS) attacks by themselves are of little use to a hacker or malicious user, but they may serve as the foundation for other more significant exploits.
- **Impersonation Attacks**—Many of the parameters in the 802.11 specification which are used to uniquely identify wireless networks and the wireless devices themselves are contained in clear unencrypted sections of the wireless traffic. Malicious users who listen to traffic in promiscuous mode are able to easily learn what these parameters are. Because the current 802.11 standard doesn't offer any validation of these parameters techniques called spoofing or identity theft have been developed to impersonate wireless devices to exploit wireless networks. Impersonation exploits are performed through the use of tools which craft wireless traffic substituting some of the learned parameters into the transmitted traffic. Because the wireless devices are unable to distinguish the impersonated traffic from the legitimate traffic, all traffic is processed as legitimate traffic including the malicious traffic. Impersonation is the foundation of a significant percentage of basic and advanced wireless exploits and may be the first sign of a sophisticated attack.

### **Alarm Library**

To view a list of Exploits Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Exploits**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***Infrastructure Alarms***

Infrastructure Alarms alert you to events that are generated based on the SNMP traps received from the infrastructure devices. Each infrastructure device is capable of forwarding SNMP traps to alert the ADSP of significant events related to the device. Examples of SNMP traps include ColdStart indicating that a device has recently rebooted or CPU Limit Exceeded indicating that the CPU on a device has reached a critical level for a period of time. The SNMP traps received from infrastructure devices are configurable on a per device basis. Each trap includes a message defining the significant event and optional varbinds that provide additional information related to the event. Each infrastructure device includes settings for enabling a specific trap or group of traps, where the trap(s) should be forwarded and what community string should be used to allow the management station to process the trap (similar to a password). Each infrastructure device must be configured to enable the proper traps, the trap receiver (IP address of the Wireless Services Platform) and community string before the notifications will be processed. By default, the community string "public" should be used when enabling traps on an infrastructure device.



**NOTE** To enable SNMP traps, you must use ADSPadmin. Details are included in the AirDefense Services Platform 9.0 User Guide.

### **Infrastructure Alarms Sub-Types**

Infrastructure Alarms are broken down into the following nine sub-types:

- **Device Operation**—Device operation events are based on operations-related SNMP trap notifications from infrastructure devices. The alarms in this category indicate that a standard process or service on an infrastructure

device has changed. Device operations can include a host of services from Dynamic Host Configuration Protocol (DHCP), cluster or redundancy control, Remote Authentication Dial-in User Service (RADIUS) server enablement or even Hotspot status changes. Events in this category assist in understanding if the proper services are running on an infrastructure device and if there may be any issues related to a specific service.

- **Device Status**—Device status events are based on operational status of an infrastructure device. The alarms in this category indicate whether a device is running, in what state a device may be operating, or if a device is currently offline. Device status events are not tied solely to the core infrastructure device such as a wireless controller, but also includes the adopted access point / port status. An access point may be denied adoption due to a wireless controller configuration option and an incorrect network setup.
- **Diagnostics**—Diagnostics events are based on hardware and software status notifications received in the form of SNMP traps for an infrastructure device. The alarms in this category trigger when hardware and software resource limits are reached.
- **MIB-II**—MIB-II events are based on standard Management Information Base (MIB) II SNMP traps for an infrastructure device. MIB-II traps are defined in RFC 1098 as traps supported by all devices that use the MIB-II standard. While most devices will use MIB-II to define these traps - some devices have ported these traps into their 'private' or 'proprietary' MIBs as defined by the hardware vendor.
- **Others**—All the unregistered SNMP traps from infrastructure devices.
- **Performance**—Performance events are based on the infrastructure device performance as related to the wireless network. Events in this category provide critical information about wireless station behavior (authentication and association), interference or congestion, and wireless utilization levels in the environment.
- **Platform Events**—Platform events are based on configuration-related internal notifications and configuration-related SNMP traps received from infrastructure devices. The alarms in this category indicate that a configuration event has occurred on an infrastructure device including a configuration change, a configuration is out of compliance or that a configuration update has failed. Device configurations are monitored for changes on a periodic basis to ensure that the device configuration matches the assigned profile for a device based upon the folder where a device is located. If the configuration on the infrastructure device does not match an alert will trigger a notification of the configuration change. SNMP trap notifications from devices can also indicate if a configuration has changed.
- **Security**—Security events are based on wireless network security SNMP traps received from infrastructure devices. The alarms in this category indicate that a security-related event has occurred as detected by an infrastructure device. Wireless controllers and access points that have been dedicated as 'detectors' periodically scan the wireless network for neighboring APs, possible rogue devices, wireless intrusions and active wireless attacks.
- **Statistics**—Statistics events are based on wireless network and service statistic SNMP traps received from infrastructure devices. Infrastructure devices measure network service performance (Hotspot status) and statistical thresholds as set in a device configuration. Statistical events are triggered when a specific statistical threshold has been exceeded. Examples of statistical thresholds include packets per second, throughput, average retries, and packets dropped. Setting statistical thresholds are useful for measuring network performance on a per infrastructure device basis.

### **Alarm Library**

To view a list of Infrastructure Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Infrastructure**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***LBS Alarms***

Location Based Services (LBS) alarms alert you to visitors with Wireless Clients entering or leaving your location.

### **LBS Alarm Sub-types**

LBS Alarms are broken down into the following two types:

- Presence—A Wireless Client has been detected in the environment or has left the environment.
- Region Presence—A Wireless Client has met one of the following conditions:
  - Entered a predefined virtual region
  - Exited a predefined virtual region.
  - Has been detected in a predefined virtual region for a specified amount of time.
  - Has been detected within a specified distance of a predefined virtual region.

To view a list of LBS Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, select **LBS**, and then select the alarm sub-type to see all the alarms associated with the sub-type.

### ***Performance Alarms***

Performance Alarms alert you to events that provide critical information about the service levels of the wireless network. In a wireless environment, Performance events can be an indication of problems related to configuration, compatibility, congestion, coverage, potential interference sources, and utilization levels. Because 802.11 operates in a shared and unlicensed frequency spectrum, it is possible that performance issues may be the result of non 802.11 devices such as microwaves and cordless phones, or could be a result of a conflict with other 802.11 devices, including both valid devices as well as neighboring devices transmitting into the monitored airspace.

### **Performance Alarms Sub-Types**

Performance Alarms are broken down into the following eight sub-types:

- AP Testing—AP Testing Events track network failures from an automated or manual AP connectivity test. The alarms in this category 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 which performs remote end to end network testing from a wireless perspective. The test is accomplished by using the deployed Sensors as a wireless station 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.
- Configuration/Compatibility—802.11 Wireless networks operate in unlicensed frequency ranges capable of operating in numerous different configurations. Monitoring the wireless devices operating configuration will ensure maximum compatibility and network performance.
- Congestion—802.11 Wireless network operate in a shared and uncontrolled medium; congestion is inevitable as the number of wireless devices and bandwidth demands increase. AirDefense Enterprise proactively monitors for congestion problems to ensure maximum performance on the wireless network.
- Coverage—802.11 Wireless networks operate in unlicensed frequencies; however the allowable power output by any single device has been regulated. This limits range and coverage capable by any single 802.11 capable wireless device. The main causes of coverage problems are related to deployments. AirDefense Enterprise provides detections of coverage problems to assist in troubleshooting specific areas of the wireless networks.
- LiveRF—LiveRF is a tool to that uses live data from sensors and WLAN infrastructure to provide real-time visualizations of the environment. The use of live data feeds ensures the visualizations accurately represent environmental changes and transient issues which may not have been captured in the plan or site survey. Visualizations provided allow administrators to troubleshoot wireless connectivity, throughput issues, capacity problems and identify RF interference sources for a floor or entire building. All of this is performed from a central

console, so troubleshooting can be performed without having to send administrators out to remote locations. LiveRF also allows runs in the background to automatically detect network problems based on thresholds defined by the administrator. The alarms in this category are a result of these proactive network problem detection capabilities.

- **Potential Interference Sources**—802.11 devices operate in unlicensed frequency ranges, 2.4GHz for b/g and 5GHz for a-channels and are subject to interference from other devices utilizing the same frequency. Common examples of these devices are: microwave ovens, Bluetooth devices, baby monitors, cordless telephones, Zigbee devices, non 802.11 wireless security cameras and wireless USB devices (wireless keyboard and mouse).
- **RF Spectrum Analysis**—802.11 Wireless networks operate in unlicensed frequencies. This includes any non 802.11 transmitters such as cordless phones, and Bluetooth share frequency spectrum with 802.11 wireless networks. A non 802.11 transmitter can impact the network by causing interference. Identifying the source is difficult with standard 802.11 hardware as these simply appear as noise. Spectrum Analysis can be used to identify the source of the interference and judge the impact the interferer will have on the wireless network.
- **Utilization**—802.11 Wireless networks operate in a medium where all devices share the available bandwidth. Any single device is capable of impacting performance by using all available wireless resources. AirDefense Enterprise monitors over 50 performance related utilization statistics for the authorized wireless devices, to ensure that utilization related performance problems are discovered before causing significant wireless network performance degradation.

### **Alarm Library**

To view a list of Performance Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Performance**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***Platform Health Alarms***

Platform Health Alarms alert you to events that provide information about the state of the AirDefense Services Platform and the Sensors which report back to the appliance.

### **Platform Health Alarm Sub-Types**

Platform Health Alarms are broken down into the following three sub-types:

- **License Manager**—License events provide information about the features and functionality in the ADSP that require a license to operate.
- **Platform**—Platform events provide operational and health information about the ADSP appliance.
- **Sensor**—Sensor events provide operation and health information about the Sensors that are reporting back to the ADSP appliance.

### **Alarm Library**

To view a list of Platform Health Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Platform Health**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***Policy Compliance Alarms***

Policy Compliance Alarms alert you to events that provide information about the observed operational configuration compared to the configured configuration. Policy discrepancies which are found allow configuration vulnerabilities to be corrected before they could be exploited. Sanctioned Access Point configuration problems account for a significant percentage of security vulnerabilities in any organization. Policy configuration problems typically result in significant security issues and should be addressed in a timely manner.

### **Policy Compliance Alarms Sub-Types**

Policy Compliance Alarms are broken down into the following eight sub-types:

- 802.11 Encryption—802.11 Wireless networks operate in a shared medium; all devices within the range of the transmission can passively hear the sender. Encryption is implemented in wireless networks to allow for secure transmission of data, and to prevent eavesdroppers from reading the contents. ADSP monitors the authorized Access Points to ensure that the defined encryption mechanisms are always used and the network operates in compliance with the enterprise policy.
- Advanced Key Generation—802.1x Authentication provides a mechanism to authenticate a user and/or computer against a network and generate the keys necessary to encrypt data; if required, the keys can be changed dynamically. ADSP monitors the authorized Access Points to ensure that the defined advanced key generation mechanisms are always used and the network operates in compliance with the enterprise policy.
- AirDefense Personal Policy Violation—AirDefense Personal is a client product designed to monitor the edge of the network. The edge of the network is defined by the mobile work force and their laptops that travel throughout the world to airports, hotspots, hotels, etc. As mobile workers travel they have confidential and proprietary corporate data to protect and can access the corporate network through a VPN (Virtual Private Network). User stations typically present the weakest security link to a malicious users. AirDefense Personal ensures that the enterprise policy is enforced any where, any time the client is using mobile resources, even when it is outside of the range of ADSP monitoring Sensors.
- Authentication—ADSP monitors 802.11 authentication as defined in the company policy against what has been observed in the air, allowing for notification of enterprise compliance policy violations.
- Environment—Environmental events allow for monitoring of generic operation wireless network activities. These events could have an impact on enterprise compliance, security and performance requirements.

ADSP Environment policy compliance now includes alarms that alert you to WiFi Direct devices that are violating your network compliance policy. WiFi Direct is peer-to-peer networking which may present issues with corporate networks controlling WiFi Direct devices. Being able to detect WiFi Direct gives corporate personnel a tool to investigate and determine if there is a threat to their network.

- Global—Global events are generic informative events about observed behavior in the wireless network.
- Incorrect BSS Configuration Observed—BSSs typically have static configuration set by the administrator. A BSS which changes its configuration or is not using the default configuration could prevent authorized access or allow unauthorized access. Incorrect configuration events monitor the BSS configuration as observed through the air against defined operational policies.
- Other Encryption—802.11 Wireless networks operate in a shared medium; all devices within the range of the transmission can passively hear the sender. Encryption is implemented in wireless networks to allow for secure transmission of data, and to prevent eavesdroppers from reading the contents. Other Encryption category allows for monitoring of 3rd party encryption that is not defined in the 802.11 specification, offering an additional level of security for the wireless network. ADSP monitors the authorized Access Points to ensure that the defined encryption mechanisms are always utilized and the network operates in compliance with the enterprise policy.

### **Alarm Library**

To view a list of Policy Compliance Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Policy Compliance**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***Reconnaissance Alarms***

Reconnaissance Alarms alert you to events that track devices which are actively attempting to locate wireless networks. 802.11 Wireless networking operates in a shared medium in which the wireless signals are not



constrained by the traditional physical boundaries. Signals may extend outside of building boundaries into parking lots or neighboring faculties enabling valid client devices, attackers or malicious users to receive the signals and discover available wireless networks. Wireless behavior from supplicants such as Windows XP zero configuration client (WZC) is an example of normal reconnaissance behavior where the client will continue to probe for all configured networks; this is normal reconnaissance activity that allows the clients to find networks which do not broadcast SSIDs.

Alternatively, Reconnaissance may be used by a malicious user as the first step in an attack on a wireless network. Open source reconnaissance tools, such as Wellenreiter, Netstumbler, and Dstumbler, can be used to discover wireless networks. Some reconnaissance tools use active methods to detect wireless networks and are easily detected by ADSP, while other tools such as Kismet have transitioned to a passive or "listen only" mode, and cannot be detected by any WIDS platform. For customers operating in no-wireless environments, reconnaissance events are of medium to high importance, and should be investigated. For deployments in urban multi-tenant areas reconnaissance events are of minor importance, because of the increasing prevalence of wireless networks combined with the increasing sophistication of newer reconnaissance tools that operate in passive mode and cannot be detected.

### **Reconnaissance Alarms Sub-Types**

Reconnaissance Alarms are broken down into the following three sub-types:

**Reconnaissance Tools**—Reconnaissance tools enable a user to discover available wireless devices in the vicinity of the user running the tool. While early versions of these tools use active methods to find available wireless resources, newer version are increasingly more sophisticated and have transitioned to passive or listen only mode and will go undetected.

**Typical Client Activity**—In wireless networking clients actively search for the wireless networks they have been configured to connect to, enabling the clients to find the wireless Access Points that are in the vicinity of the station. Once a client connects to an Access Point it will continue to search for other resources, which may include different networks or resources with a higher signal strength. Reconnaissance activity in environments with deployed wireless networks is considered typical and is expected behavior from devices.

**Weakness**—Access Points can be configured to make them more or less vulnerable to reconnaissance activity; some of these options include broadcasting the SSID in beacon, and options to respond to null probe requests. Configuring the Access Point to not respond to null probe requests and disable broadcasting the beacon in the SSID is a good security practice, which hides the wireless network identify from basic users, however it will do little to deter more advanced users attempting to discover the wireless network.

### **Alarm Library**

To view a list of Reconnaissance Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Reconnaissance**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***Rogue Activity Alarms***

Rogue Activity Alarms alert you to events of devices participating in unauthorized communication in your airspace. Examples of the type of event included in this category are detection of a wireless device operating in the airspace to detection of the most sever risks unsanctioned wireless device communicating with the wired network. AirDefense Services Platform makes a clear distinction between an unauthorized device, which may be a neighboring device transmitting into the monitored airspace, and a rogue device, a device which is communicating with a device on the sanctioned wired network. This distinction is critical to understand and appropriately respond to the threat posed by each individual device. This advanced threat assessment capabilities allows the administrator to safely ignore neighboring Access Points while focusing his attention to real threats.

### **Rogue Activity Alarm Sub-Types**

Rogue Activity Alarms are broken down into the following four sub-types:

- Authorization Violation—ADSP monitors the airspace for all wireless devices. The authorization violation subcategory defines devices which have not been acknowledged as sanctioned enterprise wireless devices, ignored transient or neighboring devices.
- Extrusion—Wireless technology increases the attack vectors that exist and present security challenges to an enterprise. Threats against infrastructure devices such as rogue APs, DoS attacks, and mis-configurations are some of the most well known and the primary focus to secure and protect against. Often overlooked are lesser known and more prevalent threats that exist against endpoints or wireless stations. The very nature of how these endpoints search for available wireless networks to connect and inability to validate authenticity of the network they are connecting to makes them vulnerable to forming unsanctioned connections. This process of a sanctioned wireless station connecting to an external unsanctioned network is known as an Extrusion. A successful Extrusion may take several forms but will always have the same effect of a sanctioned device forming L2 and L3 connection and should be considered a similar threat to a hacker connection directly to a laptop with a crossover cable.

ADSP Rogue Extrusion now includes alarms that alert you to WiFi Direct devices on your network. WiFi Direct is peer-to-peer networking which may present issues with corporate networks controlling WiFi Direct devices. Being able to detect WiFi Direct gives corporate personnel a tool to investigate and determine if there is a threat to their network.

- Rogue Exploit—Rogue Exploit sub-type contains alarms to detect true rogue activities by any unsanctioned wireless device communicating with the devices on the wired infrastructure. Examples include unauthorized Access Point physically attached to the wired network (Rogue AP) or an unauthorized station on the wireless network connected to an authorized AP (Rogue Wireless Client).
- Wired Network Monitoring—Rogue Activity includes events for devices participating in unauthorized communication in your airspace. Examples of the type of event included in this category are detection of a wireless device operating in the airspace to detection of the most severe risks unsanctioned wireless device communicating with the wired network. AirDefense Enterprise makes a clear distinction between an unauthorized device, which may be a neighboring device transmitting into the monitored airspace, and a rogue device, a device which is communicating with a device on the sanctioned wired network. This distinction is critical to understand and appropriately respond to the threat posed by each individual device. This advanced threat assessment capabilities allows the administrator to safely ignore neighboring Access Points while focusing his attention to real threats.

### **Alarm Library**

To view a list of Rogue Activity Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Rogue Activity**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

### ***Vulnerabilities Alarms***

Vulnerabilities Alarms alert you to weaknesses that are not actively exploited, but have been detected in the airspace. Weaknesses can potentially be exploited by both active and passive methods. For example, unencrypted wired side traffic leakage can be exploited passively by discovering wired-side device information, while rogue Access Points can be actively exploited by a station associating to it. Vulnerabilities provide an inherent security risk to the enterprise and should be carefully evaluated to understand the potential exposure that could occur if a vulnerability was exploited. Once a vulnerability is discovered options should be considered to remediate the vulnerability to prevent it from being exploited.

### **Vulnerability Alarm Sub-types**

Vulnerability Alarms are broken down into the following five sub-types:

- **Fuzzing**—An active attacking technique that is used to find vulnerabilities and flaws in vendor's wireless drivers. When a fuzzing attack occurs, a malicious user will generate valid 802.11 frames but will randomly change information in the frames in an attempt to discover vulnerabilities in the wireless driver. A successful fuzzing attack can have various outcomes, depending on the specifics of the attack and the vulnerability in the wireless driver. Possible outcomes include full root access of the attacked system, remote code execution, DoS attack, or kernel crash. In general, fuzzing attacks present significant risk to the enterprise. Because wireless drivers receive and process broadcast traffic, fuzzing attacks may not require a physical connection but just physical proximity to the attacker to execute a successfully attack.
- **Predictive Problems**—Through passive wireless monitoring AirDefense will provide events indicating potential wireless security issues. Issues may be related to network or client configuration and may not currently be actively exploited, however the danger exists that they could be exploited. Predictive problem detection allows an administrator to take proactive measures to resolve security issues before a malicious user has the potential to exploit it.
- **Suspect Activity**—Suspect Activity captures wireless events or activity, though not a direct attack on the wireless network, suggest the potential for an exploit. Suspect activity events should be reviewed as they generate, often suspect activity would be accompanied by an other exploit events as it may be only one facet of malicious activity.
- **Vulnerability Assessment**—ADSP actively tests the security posture of the wireless infrastructure to determine if there are weaknesses that could allow a wireless user to access sensitive systems on the wired side. This is accomplished by allowing the user to perform scheduled or on-demand tests that allow the sensor to emulate a station (laptop or other wireless device), associate to one or more access points, and test different paths of access to the wired side. The alarms in this category indicate that a vulnerability has been found in the security posture and should be considered a high priority event, and could relate to the exposure of sensitive information such as cardholder information. This vulnerability may be the result of a firewall or wireless switch misconfiguration, or some other weakness in the layered defenses. A subsequent vulnerability report can be created based on these alarms. In addition, the Action Manager can be used to automatically disable an Access Point until the vulnerability has been remediated.
- **Wired Leakage**—In wireless networks unencrypted wired side traffic leakage into the air is a result of basic Access Point functionality. The Access Point at its most simplistic form is a bridge between the wired medium and the wireless medium, allowing wireless devices to communicate with devices on the bounded wired network. An Access Point typically works the same for traffic in the reverse direction, traffic from the wired network can be transmitted into the air, to specific devices as well as broadcast addresses. The security concern entails the broadcast or multi-cast wired traffic which the Access Point bridges into the air in clear text. All devices within range of the AP can passively listen to this traffic and gain information about network configuration, routing, and the devices on the wired network. This is problem is compounded when the Access Point is placed on a VLAN which has user systems NetBios traffic that can reveal a great deal about the networked devices. It is best practice to place the Access Points on a dedicated subnet which will limit the broadcast domain of the network to minimize wired side leakage.

### **Alarm Library**

To view a list of Vulnerability Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Vulnerabilities**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

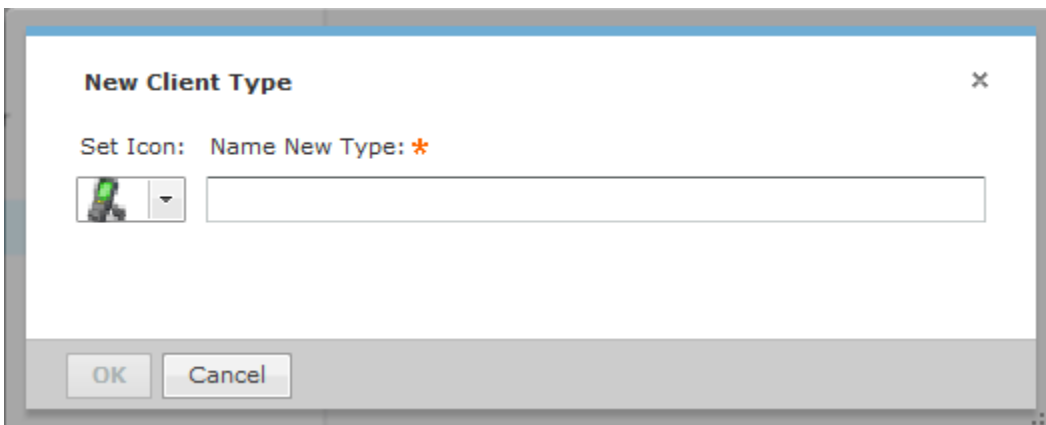
### **Client Types**

Client Types gives you the ability to:

- Add new client types to your system.
- Edit existing client types to change the icon or name.
- Remove existing client types from your system.



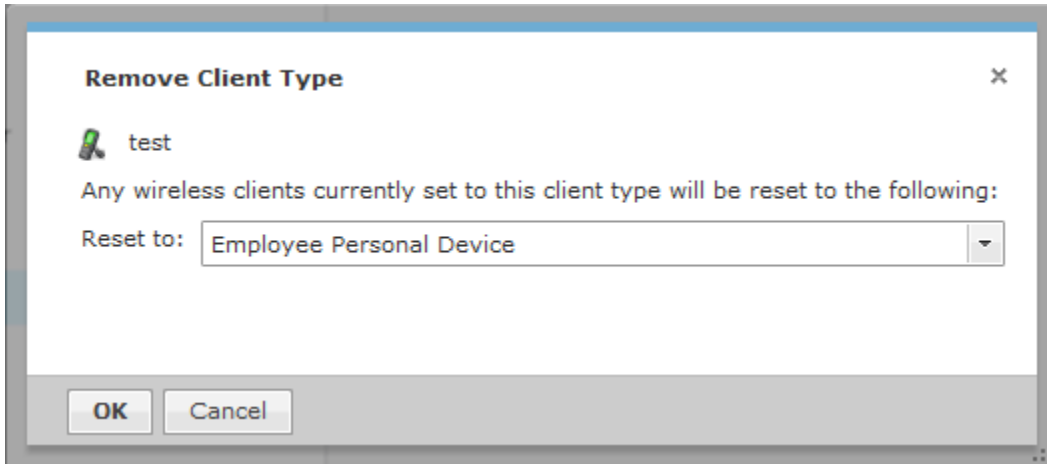
Click the **New** button to add a new client type.



Select an icon by choosing an icon from the **Set Icon** drop-down menu, type in a new name in the **Name New Type** field, and then click **OK**.

To edit a client type select (highlight) the client type and then click the **Edit** button. You can change the icon or the client type name.

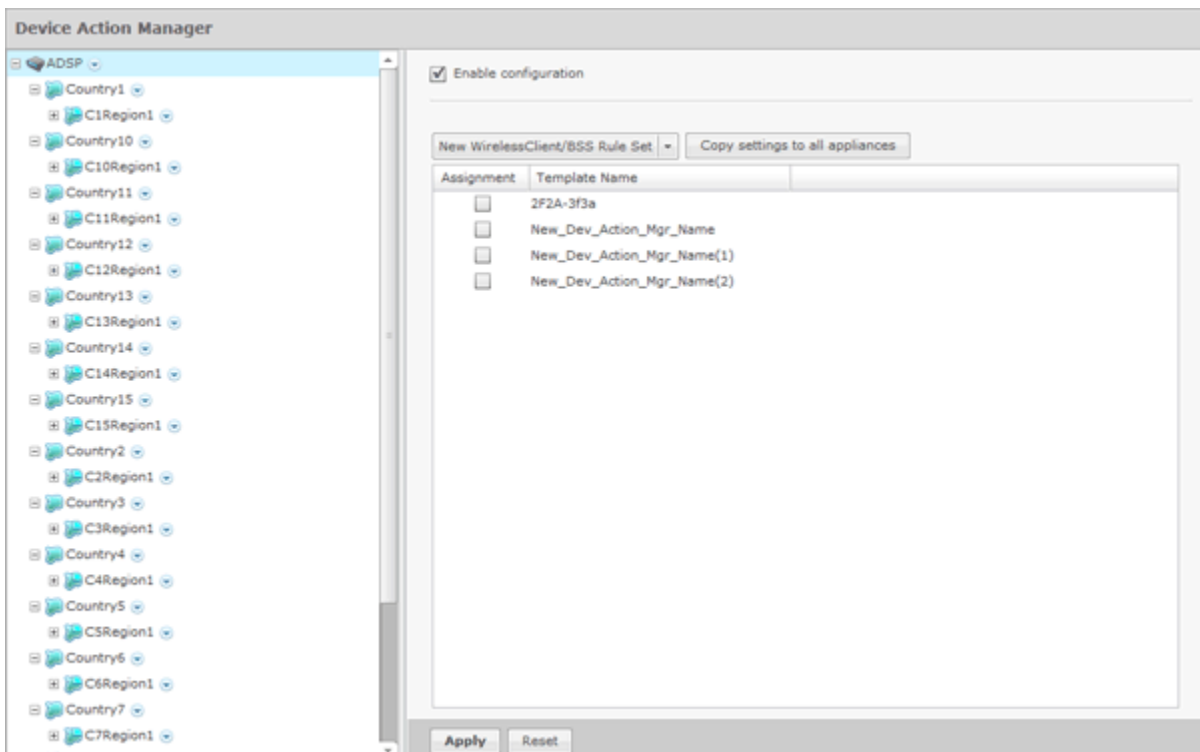
To remove a client type, select (highlight) the client type and then click the **Remove** button.



Click **OK** to remove the client type.

## Device Action Manager

The Device Action Manager allows you to automatically apply rules to devices in your system. By automating your response to certain predefined conditions, you are free to concentrate on other administrative tasks; thus reducing management overhead. You may define as many rules as you need to manage your network.



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

Column	Description
Assignment	Specifies if a template defining a rule is marked for use.
Template Name	The name of the template defining a rule.

Once a template is added to the Device Action Manager, you can edit, copy, or delete it by selecting (highlighting) a template and then clicking on the appropriate link that appears to the right of the template.

The Device Action Manager supports two types of rule sets: one for Wireless Clients/BSSs and one for Infrastructure devices. ADSP uses a dual purpose button to access the rule sets:

- New Wireless Client/BSS Rule Set
- New Infrastructure Device Rule Set.

Clicking the drop-down menu button displays a menu where you can select one of the rule sets. The last option that you select becomes the button.

### *Adding a Wireless Client/BSS Rule Set*

The **Wireless Client / BSS / Unknown Devices Rule Set** window is where you add a Wireless Client/BSS Rule Set or edit an existing Wireless Client/BSS Rule Set.

There are three things that you must do to define a Wireless Client / BSS / Unknown Devices Rule Set:

1. Name the rule set.
2. Select and define at least one filter. You may have up to ten filter. Click the **Add Another** button to add additional filters. Each added filter adds an “and” statement.
3. Select and define at least one action. You may have up to five actions. Click the **Add Another** button to add additional actions.

A rule set may have one or more rules. Each rule must have a least one filter and one action. Click the **Add Another Rule** button to add additional rules.

#### **Filters**

Filters are built using a **When** statement and an **If** statement. Start off selecting when the filters (**When** statement) will be used. There are four options:

- All—All of the selected conditions must be met (logical “and” operation).
- Any—One or more selected conditions must be met (logical “or” operation).
- None (All)—None of the selected conditions are met (logical “and” operation).

- None (Any)—One or more selected conditions are not met (logical “or” operation).

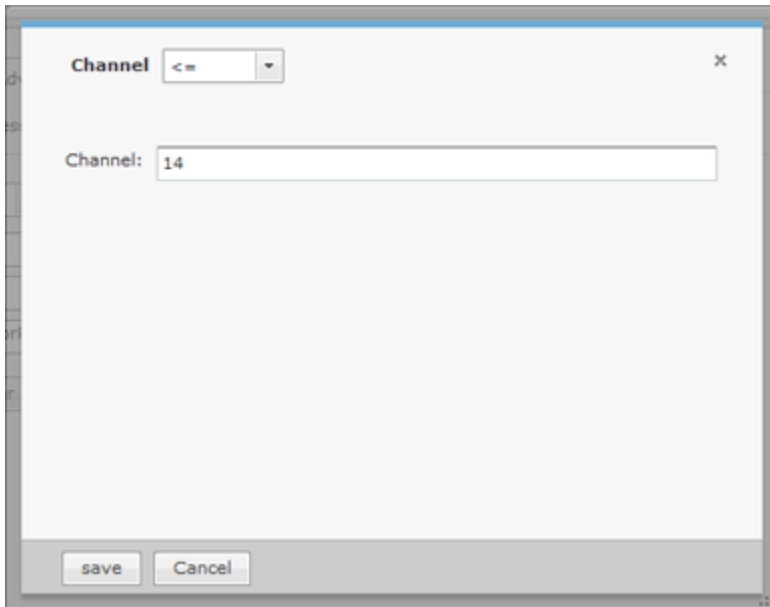
The **When** statement works together with an **If** statement matching a filter with a value. The available filters are:

- Adhoc
- Associated
- AssociatedBSSClassification
- AssociatedBSSIP
- AssociatedBSSMAC
- AssociatedBSSName
- AssociatedBSSVendorPrefix
- Channel
- ConnectedToWired
- Device802\_1XName
- DeviceAuthentication
- DeviceClassification
- DeviceClassificationInherit
- DeviceClientType
- DeviceEncryption
- DeviceFirstPolled
- DeviceFirstSeen
- DeviceIP
- DeviceLastPolled
- DeviceLastSeen
- DeviceMAC
- DeviceManufacturer
- DeviceName
- DevicePolledID
- DevicePolledSSID
- DeviceProtocol
- DeviceSSID
- DeviceSensedID
- DeviceSensedSSID
- DeviceType
- DeviceVendorPrefix
- SensorIP



- SensorMAC
- SensorName
- SignalStrength
- WatchList
- WiFiDirect.

When a filter is selected, an **Edit** button is displayed. Click the **Edit** button to select a mathematical comparison to indicate the relationship between the filter and a value that you specify.



Click the drop-down menu to select the type of comparison. This will vary according to the selected filter. The type of comparison may be:

- = Is equal to
- != Is not equal to
- < Is less than
- <= Is less than or equal to
- > Is greater than
- >= Is greater than or equal to
- LIKE Is similar to, matches some portion (Used for a partial match)
- ILIKE Case insensitive partial match
- IN Condition exists within the filter value (usually used when the filter combines two or more variables which must be compared in some way to create a trigger)

There will be one or more other fields to determine a value. This will vary according to the selected filter.

Click the **Save** button to save the comparison.

The following screen shot shows an example of a filter within a rule.

You can remove a statement by clicking the **x** next to the statement.

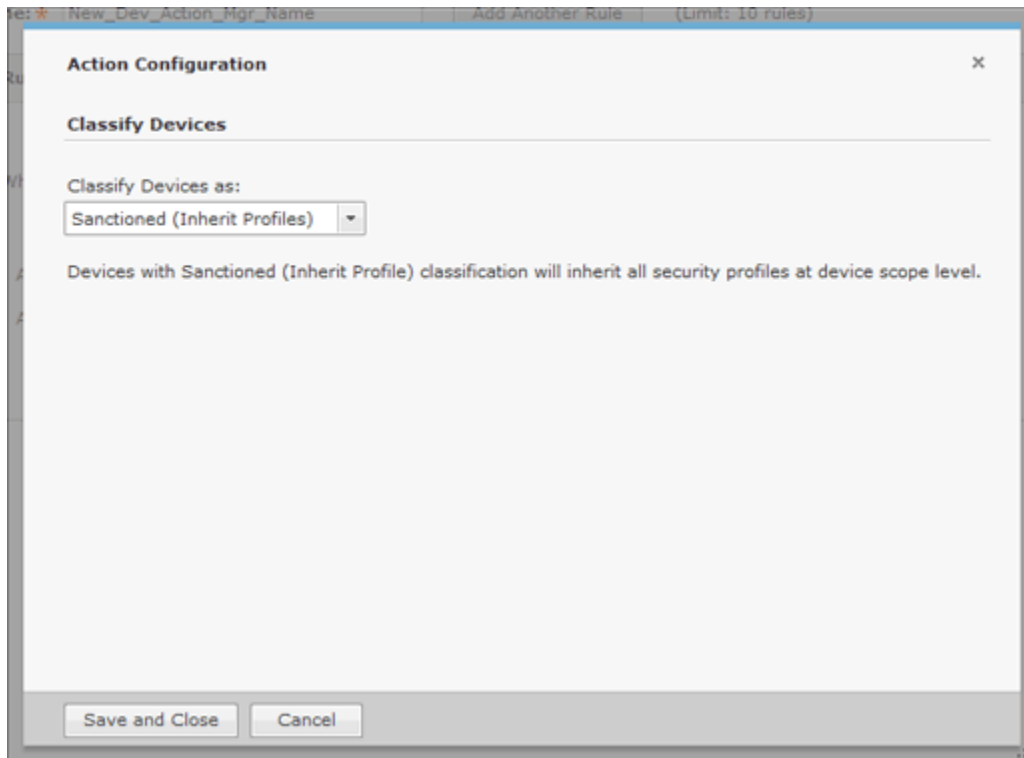
### **Actions**

You may specify one or more actions to run when certain conditions are met as defined by the filter(s). Valid actions are:

- Classify Devices—Classifies devices using the filter(s) to determine which devices are to be classified.
- Clear active alarm for active devices—Clears any active alarm if the conditions defined in the filter(s) are met.
- Set Client Type—Sets the Client Type for Wireless Clients as defined in the filter(s).
- ACL—Enables the Access Control List on switches that meet the conditions defined in the filter(s).
- Port Suppression—Suppresses communication between unauthorized devices and switches on your network as defined in the filter(s).
- Termination—Terminates devices that meet the conditions defined in the filter(s).
- AP Test—Runs an AP Test using the specified profile if the conditions defined in the filter(s) 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(s) are met.

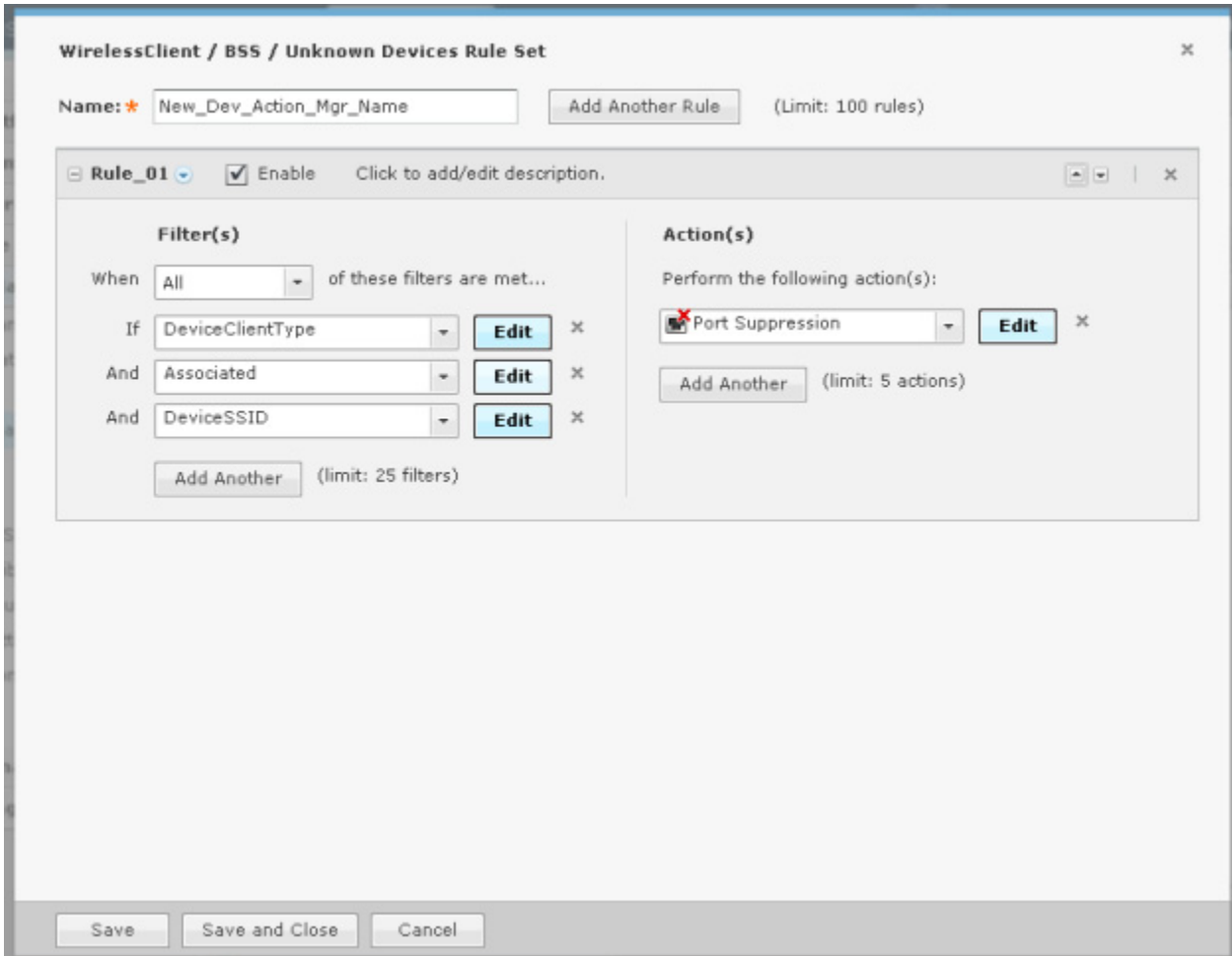
- Vulnerability Assessment—Runs a vulnerability assessment using the specified profile if the conditions defined in the filter(s) are met.
- Delete Device—Deletes any device from your system that meets the criteria defined in the filter(s).

When an action is selected, an **Edit** button is displayed. Click the **Edit** button to configure the action. Configuration will be different for each type of action. For example, selecting **Classify Devices** as your action displays the following dialog window.



Classify Devices allows you to classify devices as: **Sanction (Inherit Profiles)**, **Unsanctioned**, **Neighboring**, or **Sanction (Assign Profiles)**. Click the **Save and Close** button to save the configuration and exit the dialog window.

The following screen shot shows an example of a fully defined filter and action.



You can remove an action by clicking the **x** next to the action.

Click the **Save and Close** button to save the rule set and exit the window.

### *Adding a Infrastructure Device Rule Set*

The **Infrastructure Device Rule Set** window is where you add an Infrastructure Device Rule Set or edit an existing Infrastructure Device Rule Set.

The screenshot shows the 'Infrastructure Device Rule Set' configuration window. At the top, there is a 'Name' field containing 'New\_Dev\_Action\_Mgr\_Name' and an 'Add Another Rule' button. Below this is a section for 'Rule\_01' which is checked as 'Enable'. The 'Filter(s)' section includes a 'When' dropdown set to 'All' and an 'If' dropdown set to 'Select Filter...'. The 'Action(s)' section includes a 'Perform the following action(s):' dropdown set to 'Select action...'. Both sections have 'Add Another' buttons with limits of 25 filters and 5 actions respectively. At the bottom are 'Save', 'Save and Close', and 'Cancel' buttons.

Basically, the **Infrastructure Device Rule Set** works the same as the **Wireless Client / BSS / Unknown Devices Rule Set** with differences in the filters and actions.

#### **Filters**

The available filters for the **Infrastructure Device Rule Set** are:

- DeviceCapabilities
- DeviceDHCP
- DeviceDNS
- DeviceFirmware
- DeviceFirstSeen
- DeviceIP
- DeviceLastDataPoll
- DeviceLastSeen
- DeviceLastStatusPoll

- DeviceMAC
- DeviceManufacturer
- DeviceModel
- DeviceName
- DevicePolledIP
- DeviceSensedIP
- DeviceSerial
- DeviceVendorPrefix.

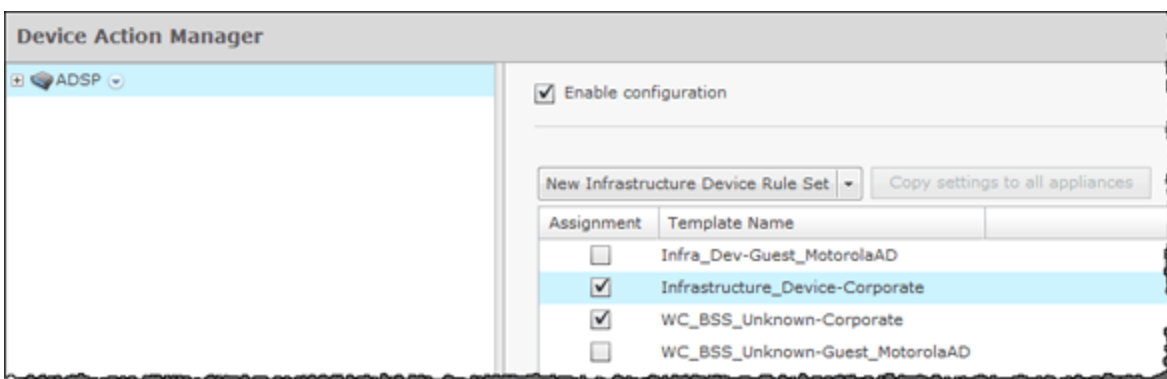
### **Actions**

The available actions for the **Infrastructure Device Rule Set** are:

- Clear active alarm for active devices—Clears any active alarm if the conditions defined in the filter(s) 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(s) are met.
- Data Collection—Corrects configuration compliance violations when the conditions defined in the filter(s) are met.
- Live RF / Floor Plan—Runs an infrastructure device poll to update the heat map predictions in Live RF if the conditions defined in the filter(s) are met.
- ACL—Enables the Access Control List on switches that meet the conditions defined in the filter(s).
- Port Suppression—Suppresses communication between unauthorized devices and switches on your network as defined in the filter(s).
- SNMP Trap—Sends an SNMP notification to your SNMP server if the conditions defined in the filter(s) are met.
- Spectrum Analysis—Runs a regular Spectrum Analysis or an Advanced Spectrum Analysis using the specified profile if the conditions defined in the filter(s) are met.
- Delete Device—Deletes any device from your system that meets the criteria defined in the filter(s).

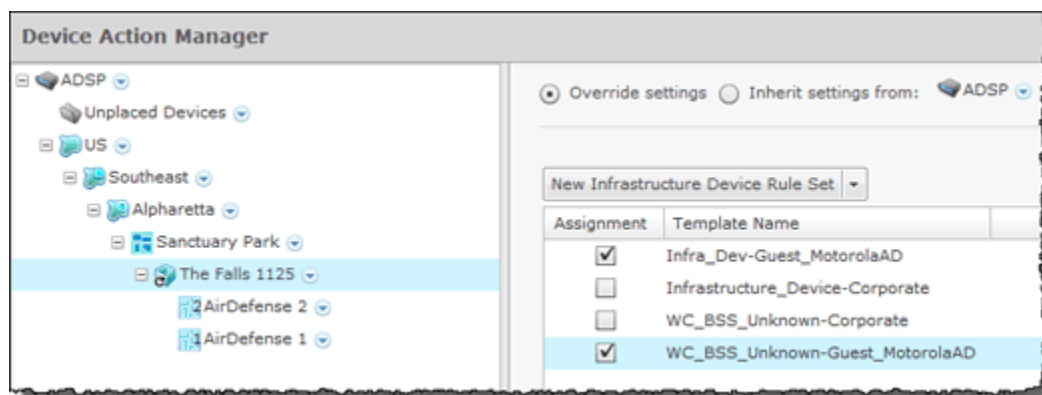
### ***Applying a Device Action Manager Template***


Once you have defined Device Action Manager templates, to use them, you must apply them to your system.



✓ **NOTE** You may select multiple Device Action Manager templates by checking more than one checkbox.

You should always apply a Device Action Manager template at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Device Action Manager template, you can apply that template to that level. For example, in the above screen shot, the Device Action Manager templates for ADSP could be the **WC\_BSS\_Unknown-Corporate** and **Infrastructure\_Device-Corporate** templates; then for a special case (in the following screen shot) you could override the Device Action Manager templates at the ADSP level and apply the **WC\_BSS\_Unknown-Guest\_MotorolaAD** and **Infra\_Dev-Guest\_MotorolaAD** templates to the The Falls 1125 network level.



- ✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the Expand— button to reveal the other levels.

You can copy Device Action Manager templates to all your appliances by clicking the **Copy settings to all appliances** button.

- ✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

### 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.

## 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.

Sensed devices last seen observations					Age out settings	
<b>BSSs</b>					You may enter a value between 1 hour and 7 days.	
	Sub Totals	Last 24 Hrs	Last 1-7 Days	Over 7 Days	Unsanctioned BSSs	<input type="text" value="3"/> Day(s) ▾
Sanctioned	9	9	0	0	Ad-Hoc BSS	<input type="text" value="4"/> Hours ▾
Unsanctioned	954	829	125	0	Unsanctioned Wireless Clients	<input type="text" value="3"/> Day(s) ▾
Neighbor	0	0	0	0	Unsanctioned Unknown	<input type="text" value="2"/> Day(s) ▾
Sub Totals	963	838	125	0		
<b>Wireless Clients</b>						
	Sub Totals	Last 24 Hrs	Last 1-7 Days	Over 7 Days		
Sanctioned	0	0	0	0		
Unsanctioned	251	190	61	0		
Neighbor	0	0	0	0		
Sub Totals	251	190	61	0		
<b>Unknown</b>						
	Sub Totals	Last 24 Hrs	Last 1-7 Days	Over 7 Days		
Sanctioned	0	0	0	0		
Unsanctioned	775	648	127	0		
Sub Totals	775	648	127	0		
<b>All Devices</b>	<b>1,989</b>	<b>1,676</b>	<b>313</b>	<b>0</b>		

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

- Unsanctioned BSSs
- Ad-Hoc BSSs
- Unsanctioned 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.

Click the **Apply** button to apply any changes. Click the **Reset** button to discard any changes and revert back to the previous settings.

## 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



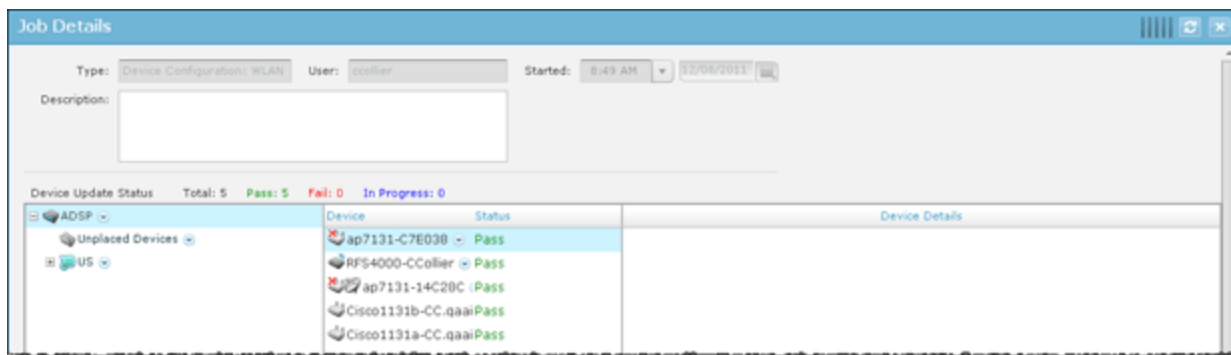
Job statuses are displayed in table format with seven columns.

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. Jobs may be canceled by selecting (highlighting) the job and clicking the **Cancel** button. Jobs may be removed from the Job Status list by selecting (highlighting) the job and clicking the **Remove** button.

You can export a job's status by selecting (highlighting) the job and clicking the **Export Status** button. A window displays where you can name the file and specify where to save it.

You can view job details by clicking the **View Details** button.



The Job Details overlay displays all the information displayed in Job Status plus some additional details such as:

- 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 using the **Export Status** button.
- Cancel the job using the **Cancel Job** button.
- Save any changes such as changing the job description using the **Save Changes** button.

Close the **Job Details** overlay by clicking the **Close (X)** button.

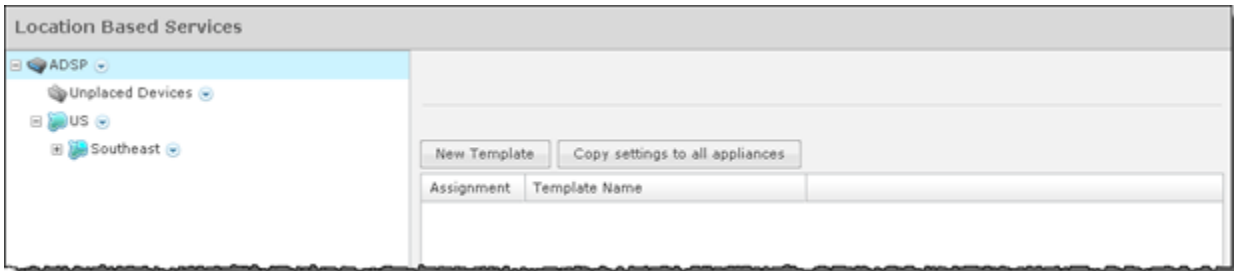
## Location Based Services

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

Use Location Based Services (LBS) to customize how frequently devices within specific locations are performing RF scans. For example, you may want to use a short frequency such as seconds to track high priority client devices, but use a lower frequency for tracking APs.

## LBS Profiles

ADSP uses the information in the LBS profile to track devices by location.



Follow these steps to assign a template to a device.

Assignment	Template Name	
<input type="checkbox"/>	New_LBS_Profile	( <a href="#">Edit</a>   <a href="#">Copy</a>   <a href="#">Delete</a> )

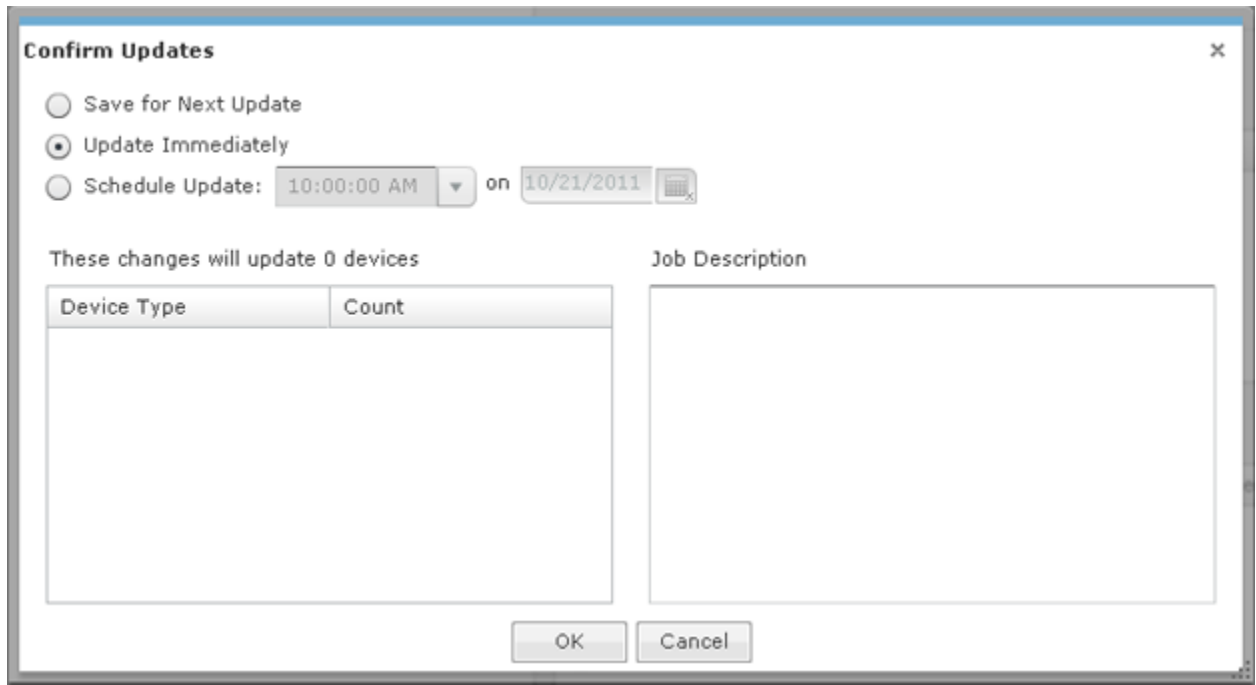
You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link.

To copy or edit a profile, select (highlight) the LBS profile, click the **Copy** or **Edit** link, and then make your changes. Click **Save** to save your changes.

The **Copy settings to all appliances** button will copy the defined LBS profile and all profile assignments to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your additions (changes). A confirmation overlay is displayed.



The image shows a 'Confirm Updates' dialog box with the following elements:

- Three radio buttons: 'Save for Next Update', 'Update Immediately' (selected), and 'Schedule Update:'. The 'Schedule Update' option is followed by a time dropdown set to '10:00:00 AM' and a date field set to '10/21/2011'.
- A status message: 'These changes will update 0 devices'.
- A table with two columns: 'Device Type' and 'Count'. The table is currently empty.
- A text area labeled 'Job Description'.
- 'OK' and 'Cancel' buttons at the bottom.

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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to LBS profiles are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.

Click the **Reset** button to discard any additions (changes).

### Adding a New LBS Profile

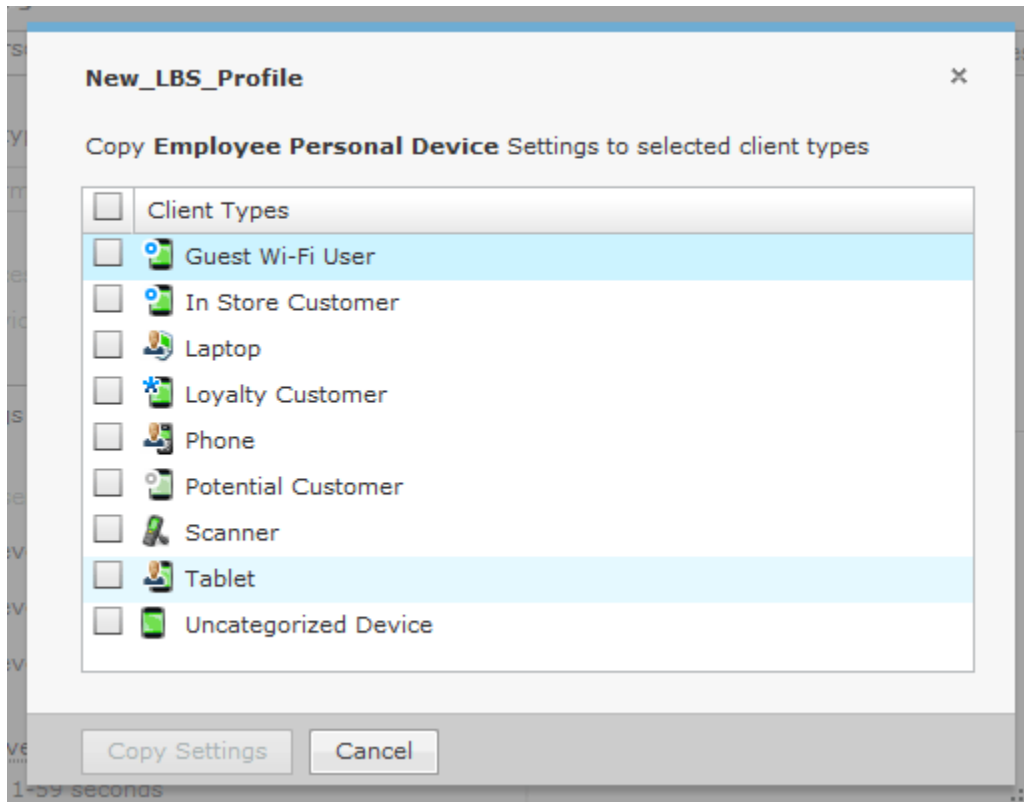
Click the **New Template** button to add a new profile.

There are two types of settings: one that is client based and the other is for global LBS settings.

Define your LBS profile using the following common fields:

Field	Description
Location Based Services Profile	Specifies the configuration profile name.
Client type configuration	Sets the valid device types for you system. Options must be specified for each device type.
Enable client type	Enables the client type chosen in the <b>Client type configuration</b> field. All other fields are inactive until you enable a client type. You must also select a priority: <b>Critical</b> , <b>High</b> , <b>Normal</b> or <b>Low</b> .
Only track devices connected to authorized BSSs	Track only the devices that are connected to an authorized BSS.

You can copy the settings for the selected client type by clicking the **Copy settings** button.



You must select the checkbox of the client type you want to copy to. Selecting the checkbox at the top of the list selects all client types. When finished, click the **Copy Settings** button to copy the settings and return to the previous dialog box.

You can set all client type priorities by clicking the **Set all client type priorities** button.

<input type="checkbox"/>	Client Types	Priority
<input type="checkbox"/>	Employee Personal Device	Normal
<input type="checkbox"/>	Guest Wi-Fi User	Normal
<input type="checkbox"/>	In Store Customer	Normal
<input type="checkbox"/>	Laptop	Normal
<input type="checkbox"/>	Loyalty Customer	Normal
<input type="checkbox"/>	Phone	Normal
<input type="checkbox"/>	Potential Customer	Normal
<input type="checkbox"/>	Scanner	Normal
<input type="checkbox"/>	Tablet	Normal
<input type="checkbox"/>	Uncategorized Device	Normal

Buttons: Set Priorities, Reset, Cancel

You must select the checkbox for each client type and then select the priority. Selecting the checkbox at the top of the list selects all client types. When finished, click the **Set Priorities** button to set your selected priorities and return to the previous dialog box.

### **Client Based Settings**

Define the Client Based Settings for your Location Based Services profile using the following fields found in the **Presence Settings** tab:

Field	Description
Enable all Presence enter events	Enables the enter events that alerts ADSP that a device has entered the premises. Three enter events are available. Each enter event includes a RSSI threshold (in dBms) in which the device would have to exceed before triggering the presence event.
API preset event frequency	Enables the API preset event frequency. Set frequency between 1- 120 minutes or 1 - 59 seconds.
Presence age out	Sets the time span that a device's location is aged out of the system. Valid entries are 1 - 120 minutes.
Enable Presence exit events	Enables the exit events that alerts ADSP that a device has left the premises.

Define the Client Based Settings for your Location Based Services profile using the following fields found in the **Location Tracking Settings** tab:

Field	Description
Select all Sources	Select the type of source to use ( <b>Wi-Fi Zones</b> or <b>Wi-Fi Positioning</b> ).
Enable all Virtual Region Events	Identifies which of the available virtual region events the given device can trigger: <b>Enter, Exit, Proximity, and/or Contained</b> .
Location Refresh Rate	Sets the rate at which the device type is to have its location updated by ADSP.
Confidence Limit	Sets the confidence level for seeing a tracked device in your network.
Location 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 - 120 minutes or 2 - 59 seconds. Location Age Out must be greater than the Location Refresh Rate.

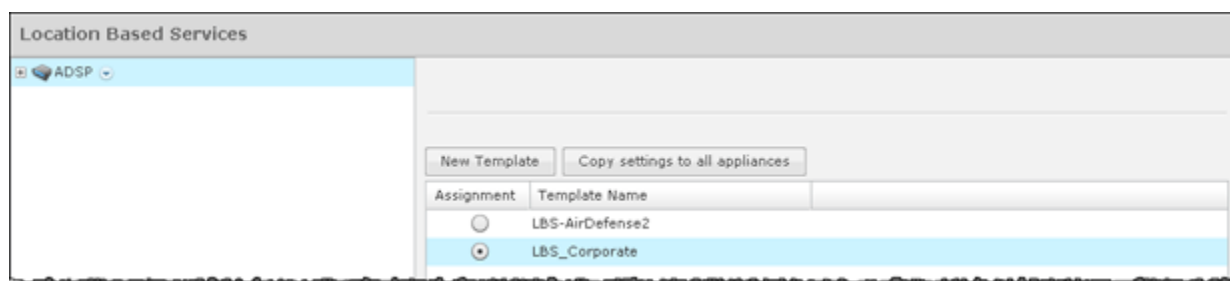
### Global LBS Settings

Define the Global LBS Settings for your Location Based Services profile as follows:


Field	Description
Enable tracking non-associated wireless clients	Track wireless clients that are not associated to any wireless network.
Wi-Fi zone threshold	Wi-Fi zone location tracking will place a client on the sensor reporting the highest signal strength above the zone threshold. The threshold is specified as an RSSI value in dBm.

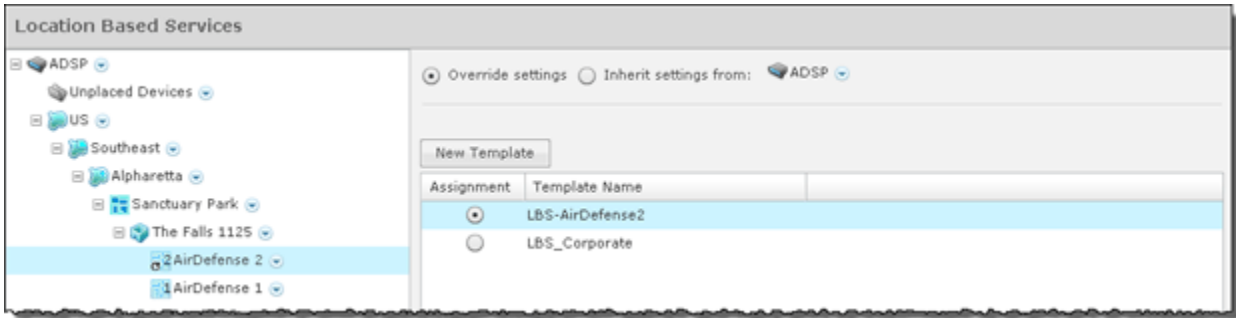
### *Applying an Existing Profile*

Once you have defined a Location Based Services profile, to use it, you must apply it to your system.



You should always apply a Location Based Services profile at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Location Based Services profile, you can apply that profile to that level. For example, in the above screen shot, the Location Based Services profile for ADSP could be the **LBS\_Corporate** profile and then for a special case (the following screen shot) you could override the Location Based Services profile at the ADSP level and apply the **LBS-AirDefense2** profile to the AirDefense 2 floor.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.

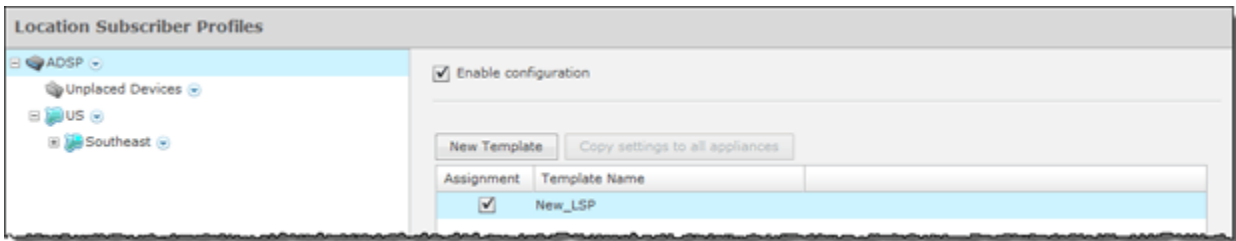


In this case, the **LBS\_Corporate** profile will be accessible to corporate-wide employees and guest while the **LBS-AirDefense2** profile will be specific to employees and guests on Floor 2 of the AirDefense facilities.

Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

### Location Subscriber Profiles

Location Subscriber Profiles are used to define subscriber profiles used in Proximity and Analytics. The profile specifies information for connecting to a third party application.



Existing profiles are displayed in the table below the row of buttons.

Assignment	Template Name
<input checked="" type="checkbox"/>	New_LSP

You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link.

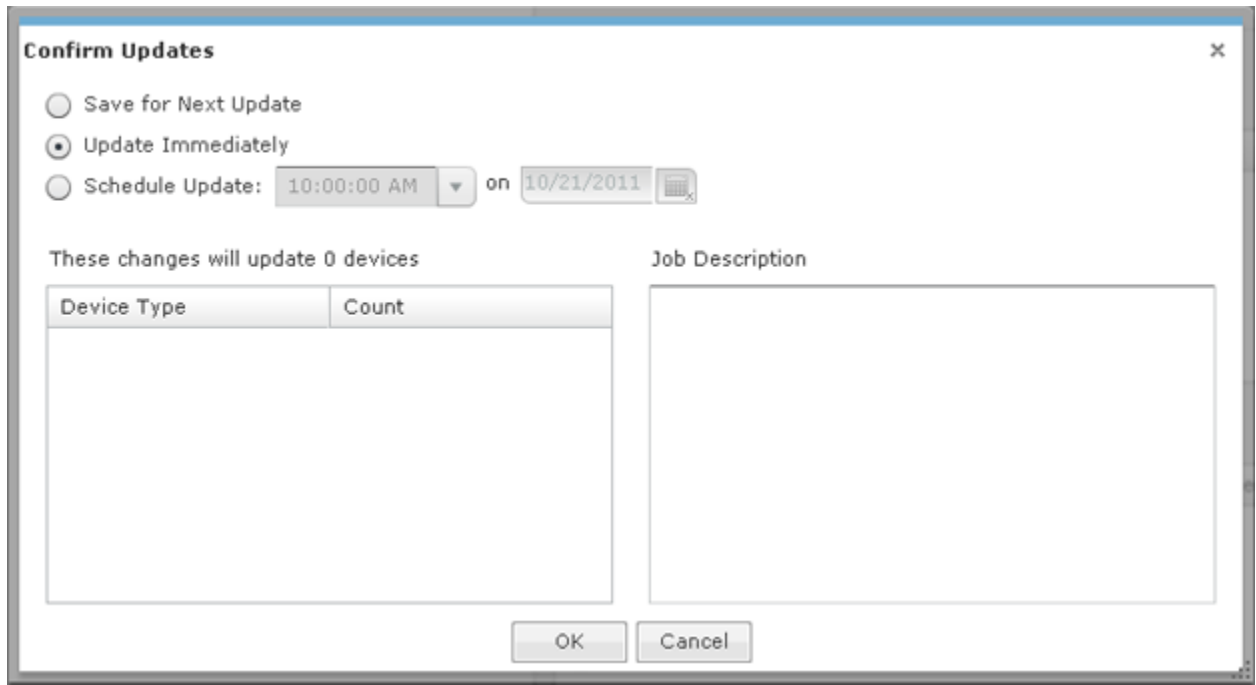
To copy or edit a profile, select (highlight) the LBS profile, click the **Copy** or **Edit** link, and then make your changes. Click **Save** to save your changes.

The **Copy settings to all appliances** button will copy the defined LBS profiles and all profile assignments to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.



Click the **Apply** button to save your additions (changes). A confirmation overlay is displayed.



The image shows a 'Confirm Updates' dialog box with the following elements:

- Three radio buttons for update options:
  - Save for Next Update
  - Update Immediately
  - Schedule Update: 10:00:00 AM on 10/21/2011
- A summary line: 'These changes will update 0 devices'
- A table with two columns: 'Device Type' and 'Count'. The table is currently empty.
- A text area labeled 'Job Description' which is also empty.
- Two buttons at the bottom: 'OK' and 'Cancel'.

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. 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. Click **OK** to apply changes or **Cancel** to abort.

Updates to Location Subscriber Profiles are treated as jobs and are included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.

Click the **Reset** button to discard any additions (changes).

### *Adding a New Profile*

Click the New Template button to add a new profile.

**Location Subscriber Profile**

**Subscriber Name:** \* New\_LBS\_Subscriber\_Name

Connection Settings | Location & Region Events | Presence Events | RSSI Data

**Subscriber Push URL:** \*

https://

Single IP: 192.168.1.1:1234  
FQDN: example.com:1234

Format:  Binary  JSON

Timeout: \* 2000 milliseconds

Retry Limit: \* 3

Username: \*

Password: \*

Display Password

Test Connection

Enable Proxy Settings

Host: \*

Port: \*

Username: \*

Password: \*

Display Password

Save Save and Close Cancel

Name your Location Subscriber Profile in the **Subscriber Name** field and use the following tabs to define the profile:

- Connection Settings
- Location & Region Events
- Presence Events
- RSSI Data.

After defining the profile, click **Save and Close** to save the profile and exit the profile. Clicking **Save** will save the profile and leave it open. Clicking **Cancel** will cancel any changes that are not saved and exit the profile.

## Connection Settings

The **Connection Settings** tab allows you to set up a secured connection to a third party application.

The **Connection Settings** tab is divided into two parts: subscriber information (required) and proxy settings (optional).

The subscriber information supplies the information needed to make the connection to the third party application. Subscriber information includes the following fields:

Field	Description
Subscriber Push URL	Supplies the IP address (192.168.1.1:1234) or domain name (example.com:1234) used to connect to a third party application.
Format	Specifies the data exchange format ( <b>Binary</b> or <b>JSON</b> ).
Timeout	Specifies a timeout value for the connection to complete.
Retry Limit	Indicates the number of attempts to retry making a connection.
Username	Supplies the username used to authenticate the connection.
Password	Specifies the password of the user making a connection. You may select the <b>Display Password</b> checkbox to reveal the password.

You can test the connection to see if it is working by clicking the **Test Connection** button.

Proxy settings allow you to configure a proxy if you are required to do so to access the Internet. Proxy settings include the following fields:

Field	Description
Enable Proxy Settings	Select the checkbox if users must use a proxy to access the third party application.
Host	The IP address of the proxy server.

Field	Description
Port	The port number used to communicate with the proxy server.
Username	A valid username used to authenticate a user to the proxy.
Password	The password of the user used for authentication. You may select the <b>Display Password</b> checkbox to reveal the password.

### Location & Region Events

The **Location & Region Events** tab is used to stream location and region events to a third party application.

Field	Description
Enable location event stream	Select checkbox to turn on streaming location events to a third party application.
Enable region event stream	Select checkbox to turn on streaming regional events to a third party application.
Select all Sources	Select the type of source to use: <b>Wi-Fi Zones</b> (zone tracking) or <b>Wi-Fi Positioning Zones</b> (position tracking.) You can select both, but position tracking will take precedence.  To see all the devices that have been placed on a sensor, select the 3 <sup>rd</sup> button on the right side of the left pane. All the devices will be displayed. To move a zone-tracked device to the top of the stack, click on the device in the left hand pane.
Select all Events	Filters streaming by events. The event triggers are <b>Enter</b> , <b>Exit</b> , <b>Proximity</b> , and/or <b>Contained</b> . You may select all the triggers by selecting Filter by Event Type, or you may select one or more events separately. When filtering by events and a trigger occurs, location and region event information is sent to the third party application.

Field	Description
Select all Client Types	Filters streaming by client types. You may select all client types by selecting <b>Select all Client Types</b> , or you may select one or more client types separately. When a client type is detected, location and region event information for that particular client type is sent to the third party application.
Filter by Wireless Clients	Filter streaming using the MAC address of one or more Wireless Clients. When a specified Wireless Client is detected, location and event information for that Wireless Client is sent to the third party application. Typing part of a MAC address displays Wireless Clients matching the partial address.
Filter by Region	Filters streaming by regions. When a region is detected, such as specific section of a store, location and region event information for the third party application is limited to the specified area(s). Typing part of a region name displays regions matching the partial name.

### Presence Events

The **Presence Events** tab is used to stream presence events to a third party application.

Field	Description
Enable presence event stream	Select checkbox to turn on streaming presence events to a third party application.
Select all Events	Filters streaming by events. The event triggers are <b>Enter 1</b> , <b>Enter 2</b> , <b>Enter 3</b> , <b>Exit</b> , and/or <b>Contained</b> . You may select all the triggers by selecting <b>Select all Event</b> , or you may select one or more events separately. When filtering by events, when a trigger occurs, presence event information is sent to the third party application.

Field	Description
Select all Client Types	Filters streaming by client types. You may select all client types by selecting <b>Select all Client Types</b> , or you may select one or more client types separately. When a client type is detected, presence event information for that particular client type is sent to the third party application.
Filter by Wireless Client	Filter streaming using the MAC address of one or more Wireless Clients. When a specified Wireless Client is detected, presence event information for that Wireless Client is sent to the third party application. Typing part of a MAC address displays Wireless Clients matching the partial address.

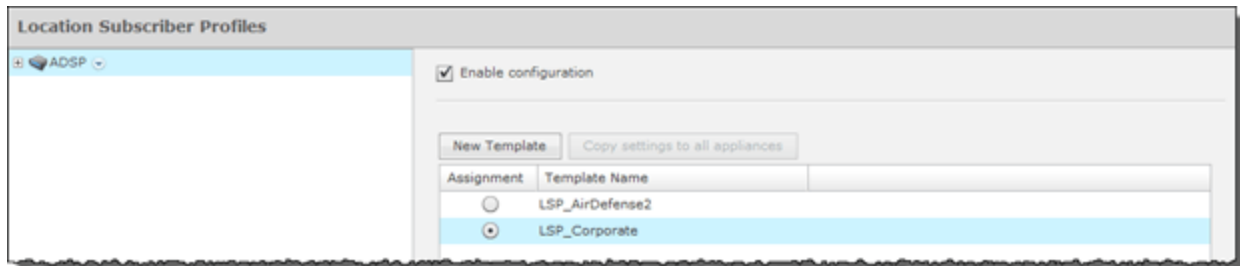
### **RSSI Data**

The **RSSI Data** tab is used to stream RSSI data to a third party application.


Field	Description
Enable RSSI data stream	Select checkbox to turn on streaming RSSI data to a third party application.
Select all Client Types	Filters streaming by client types. You may select all client types by selecting <b>Select all Client Types</b> , or you may select one or more client types separately. When a client type is detected, RSSI data for that particular client type is sent to the third party application.
Filter by Wireless Client	Filter streaming using the MAC address of one or more Wireless Clients. When a specified Wireless Client is detected, RSSI data for that Wireless Client is sent to the third party application. Typing part of a MAC address displays Wireless Clients matching the partial address.

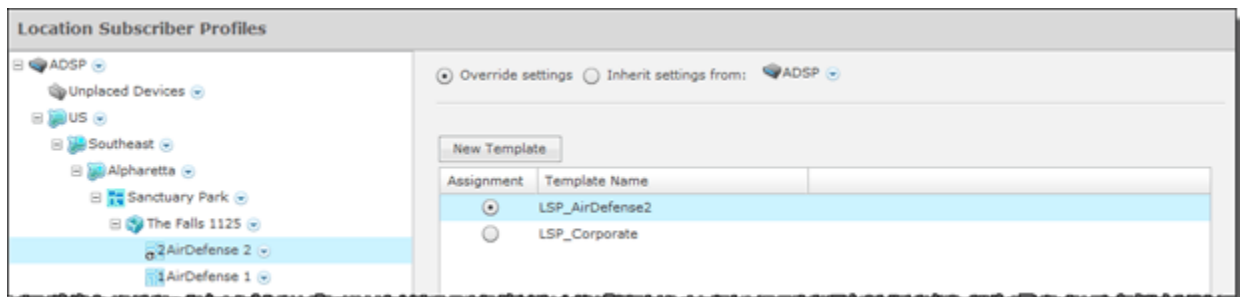
### Applying an Existing Profile

Once you have defined a Location Subscriber Profile, to use it, you must apply it to your system.



You should always apply a Location Subscriber Profile at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Location Subscriber Profile, you can apply that profile to that level. For example, in the above screen shot, the Location Subscriber Profile for ADSP could be the **LSP\_Corporate** profile and then for a special case (the following screen shot) you could override the Location Subscriber Profile at the ADSP level and apply the **LSP\_AirDefense2** profile to the AirDefense 2 floor.

✓ **NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



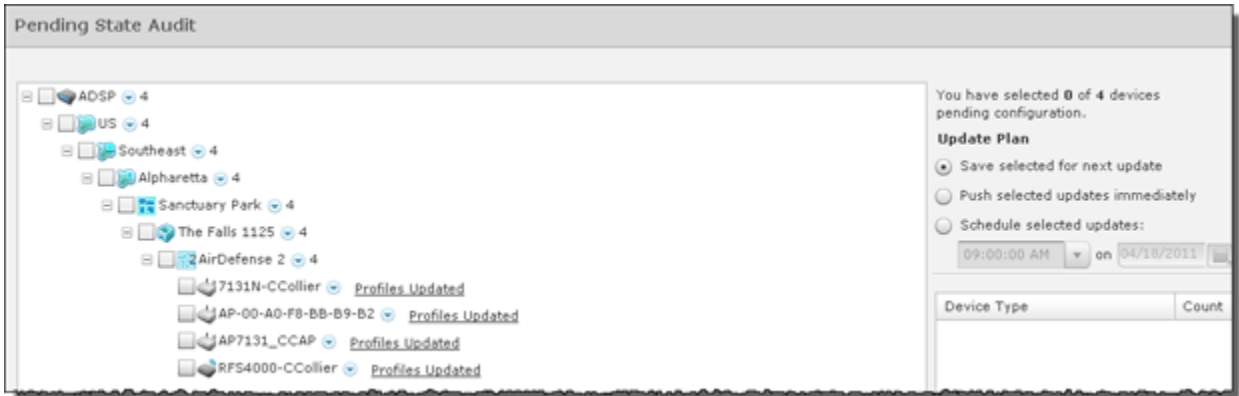
In this case, the **LSP\_Corporate** profile will be accessible to corporate-wide employees and guest while the **LSP\_AirDefense2** profile will be specific to employees and guests on Floor 2 of the AirDefense facilities.

Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

### Pending State Audit

✓ **NOTE** A WLAN Management license is required to access 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.



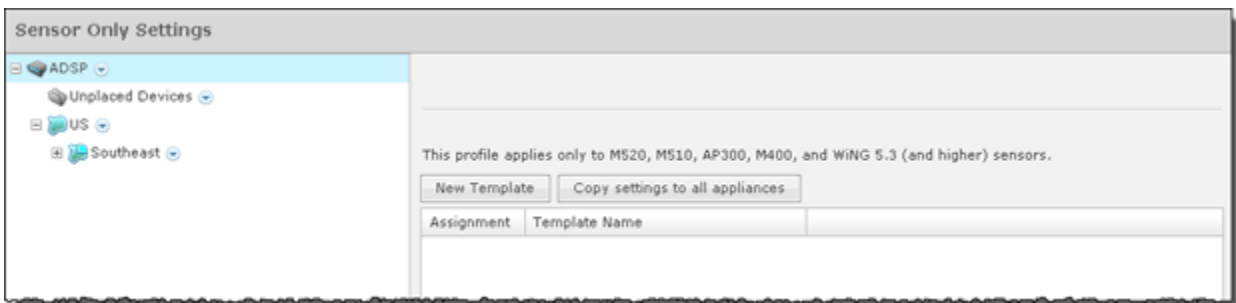
Folders with a checkmark identify that folder as having devices that in a pending state. Devices with a checkmark identify that device as a device that are in a pending state.

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 **Operation Management**. 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. Click **OK** to apply changes or **Cancel** to abort.

Click the **Apply** button to update the selected devices. A confirmation overlay is displayed.

### 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.



Existing profiles are displayed in the table below the row of buttons.

Assignment	Template Name
<input type="checkbox"/>	New_sensor_settings_pro ( <a href="#">Edit</a>   <a href="#">Copy</a>   <a href="#">Delete</a> )

You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link.

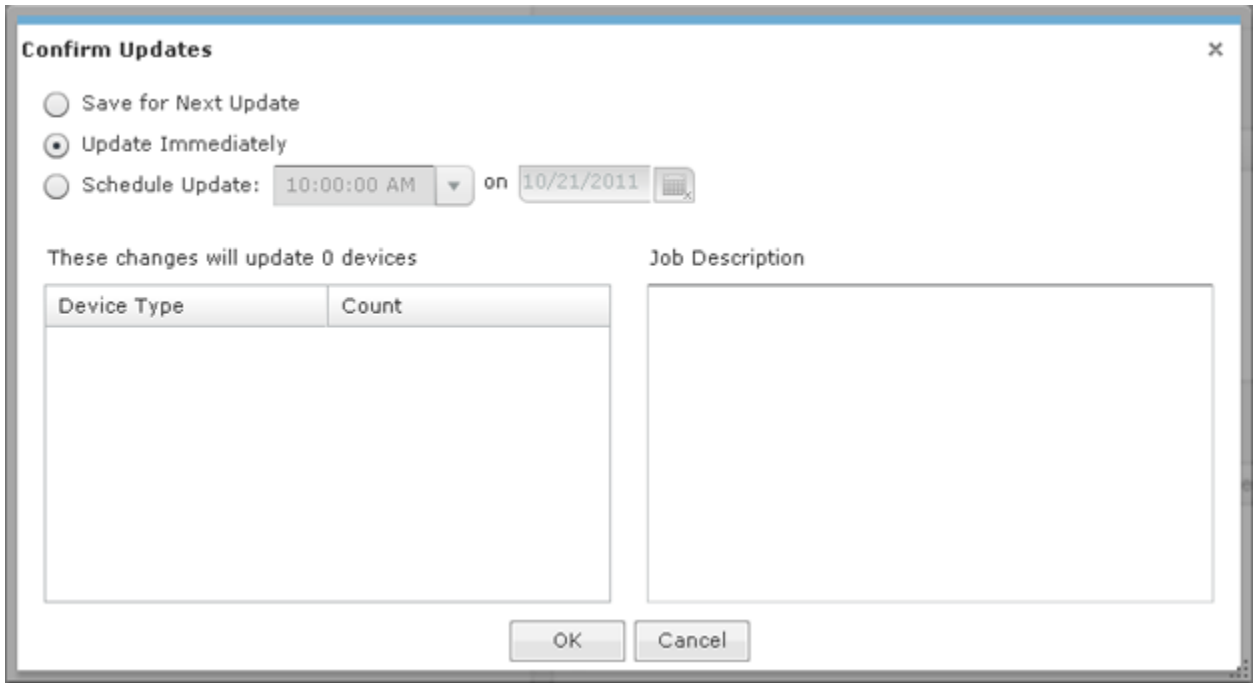


To copy or edit a profile, select (highlight) the Sensor Only Settings profile, click the **Copy** or **Edit** link, and then make your changes. Click **Save** to save your changes.

The **Copy settings to all appliances** button will copy the defined Sensor Only Settings profiles and all profile assignments to all appliances in your system.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

Click the **Apply** button to save your additions (changes). A confirmation overlay is displayed.



The image shows a 'Confirm Updates' dialog box with the following elements:

- Three radio buttons for update options:
  - Save for Next Update
  - Update Immediately
  - Schedule Update: 10:00:00 AM on 10/21/2011
- A status message: 'These changes will update 0 devices'
- A table with two columns: 'Device Type' and 'Count'. The table is currently empty.
- A text area labeled 'Job Description' which is also empty.
- Two buttons at the bottom: 'OK' and 'Cancel'.

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. 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. Click **OK** to apply changes or **Cancel** to abort.

Click the **Reset** button to discard any additions (changes).

### Adding a New Profile

Click the **New Template** button to add a new profile.

Define your Sensor Settings profile using the following fields are:

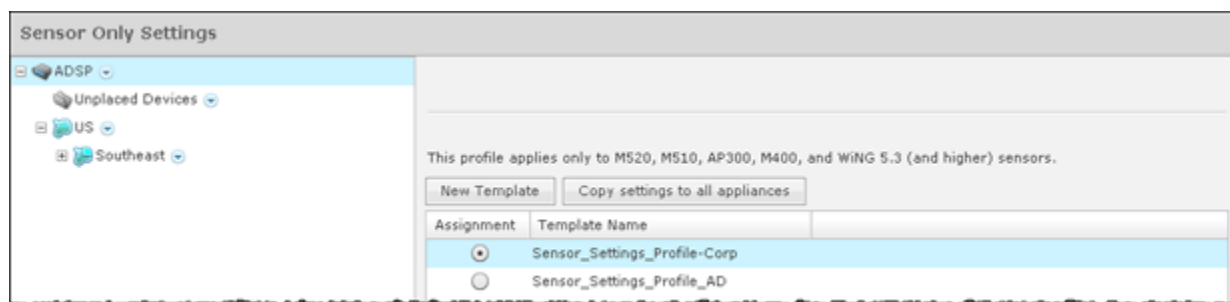
Field	Description
Primary Appliance	Specifies the IP address of the primary appliance.
Secondary Appliance	Specifies the IP address of the secondary appliance.
Sensor Admin Password	Specifies the admin password for your Sensors. Supplying this password is mandatory.
Sensor Monitor Password	Specifies 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.

Once you have defined your Sensor Settings profile, click **Save** to save your profile or **Cancel** to exit without saving the profile.


### *Applying an Existing Profile*

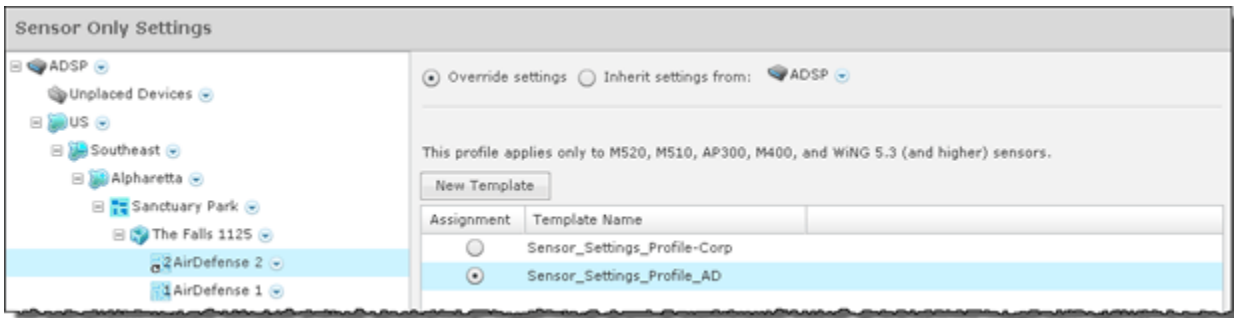
Once you have defined a Sensor Settings profile for your Sensors, you can now apply it to the Sensors in your network. A Sensor Settings profile can be applied to an appliance and all its network levels or it can be applied to a single network level. Any child network level automatically inherits the parent's Sensor Settings profile. A good practice is to apply a Sensor Settings profile to the appliance level. This profile should be generic as possible to fit a wide range of devices in your network. Then, if you have any special considerations, apply Sensor Settings profiles to individual network levels that must meet your predefined special configurations.



You should always apply a Sensor Only Settings Profile at the appliance level. When you do, the profile is inherited for all the other network levels. Then, if you have a level that needs a different Sensor Only Settings Profile, you can apply that profile to that level. For example, in the above screen shot, the Sensor Only Settings Profile for ADSP could be the **Sensor\_Settings\_Profile-Corp** profile and then for a special case (in the following screen shot) you could override the Sensor Only Settings Profile at the ADSP level and apply the **Sensor\_Settings\_Profile\_AD** profile to the AirDefense 2 floor.



**NOTE** The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**— button to reveal the other levels.



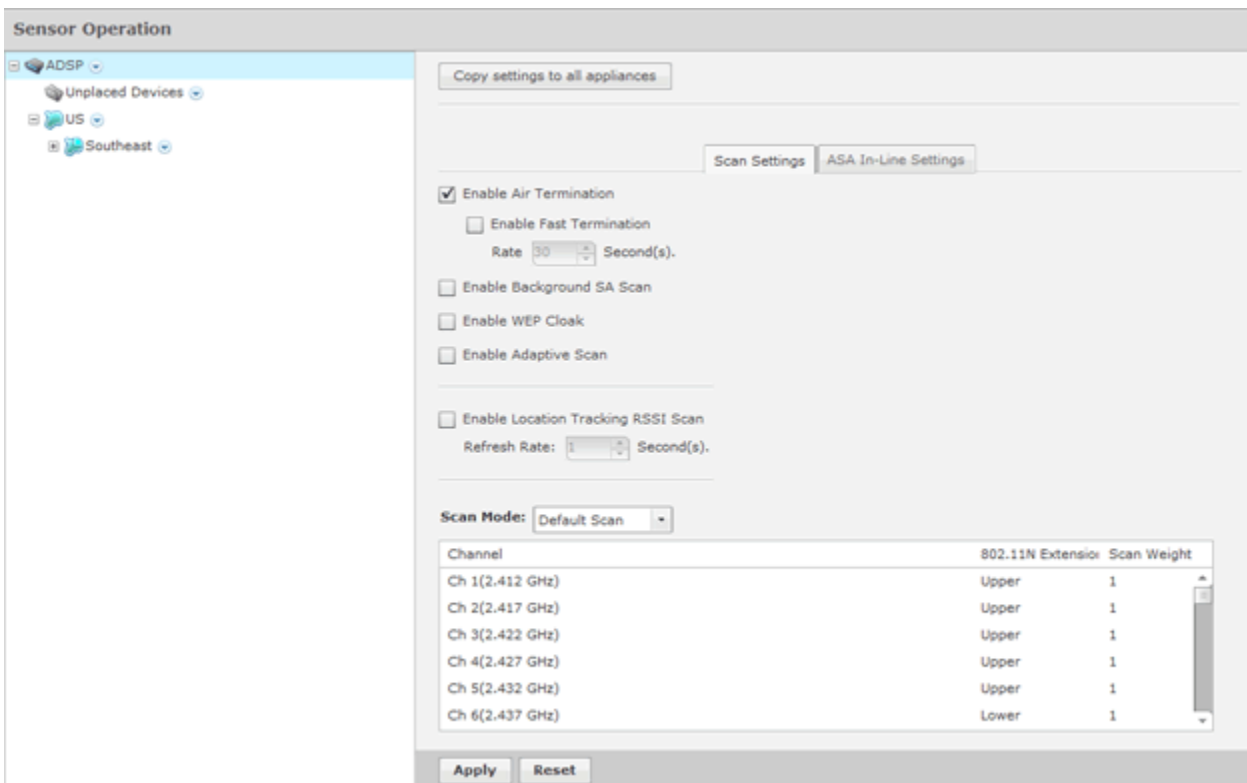
Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

## Sensor Operation

Sensor Operation settings allow you to:

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

To access the Sensor Operation settings, go to **Configuration > Operational Management > Sensor Operation**.



Use the **Scan Settings** and **ASA In-Line Settings** tabs to configure Sensor Operation. You can copy Sensor Operation configurations to all your appliances by clicking the **Copy settings to all appliances** button.

✓ **NOTE** You must have a Central Management license in order to copy settings to all appliances.

To save any configuration changes, click the **Apply** button. Clicking the **Reset** button resets all options back to their original settings.

### Scan Settings

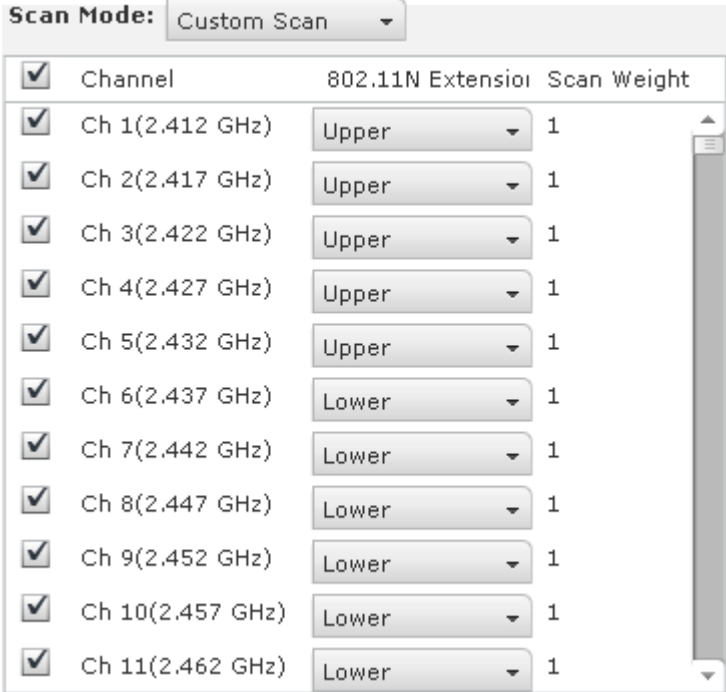
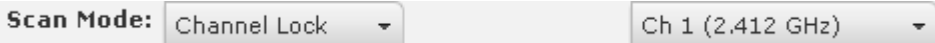
The **Scan Settings** tab is used to enable Sensor-level options and configure the Sensor scan pattern. Scan settings are configured at the appliance level of the network tree and inherited by all lower levels.

Channel	802.11N Extension	Scan Weight
Ch 1(2.412 GHz)	Upper	1
Ch 2(2.417 GHz)	Upper	1
Ch 3(2.422 GHz)	Upper	1
Ch 4(2.427 GHz)	Upper	1
Ch 5(2.432 GHz)	Upper	1
Ch 6(2.437 GHz)	Lower	1

The appliance level can be expanded to show the lower levels. If a lower level is selected from the tree, its scan settings are displayed on the right. If the scan settings are inherited from a parent level, the options are read only and grayed-out. If the scan settings are overridden, the options have read/write permission and can be edited. All tree levels that do not inherit the same settings as the selected node are displayed with gray text. The following options are available:

Feature/Function	Description
Enable 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.
Enable Background SA Scan	Spectrum Analysis has the capability to run background scans. By default, background scans are disabled.
Enable 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.
Enable 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.

<b>Feature/Function</b>	<b>Description</b>
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 Proximity and Analytics license before this option is visible.)

Feature/Function	Description
Scan Mode	<p>You can choose channels to monitor by selecting one of the following scan modes:</p> <ul style="list-style-type: none"> <li>• Default Scan—the table displays the channels that will be scanned and is not editable.</li> <li>• Extended Channel Scan—the table displays all standard channels plus the extended channels that will be scanned.</li> <li>• Extended and Emergency Channel Scan—the table displays all channels including emergency channels that will be scanned.</li> <li>• 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.</li> </ul>  <p>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.</p> <ul style="list-style-type: none"> <li>• Channel Lock—used to lock a Sensor on a specific channel for scanning. A drop-down menu is displayed where you can select a channel.</li> </ul>  <p><b>Note:</b> All channels in the 2.4 and 5 GHz bands are grouped together.</p>

### *ASA In-Line Settings*

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

Setting	Value
ASA 2.4 GHz Threshold (dBm):	-105
ASA 2.4 Duty Cycle (dBm):	-90
ASA 5 GHz Threshold (dBm):	-105
ASA 5 GHz Duty Cycle (dBm):	-90

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.

## **Appliance Management**

Topics under the Appliance Management category describe how to configure the AirDefense Enterprise appliance. Go to **Configuration > Appliance Management**.

The Appliance Management category allows you to:

- Back up, clear, or restore system configuration
- View, create, and install security certificates for the ADSP appliance
- Select the level of security for your certificates
- Specify information needed by your appliance and enable key system features
- Specify the language to be used on your appliance
- Synchronize the configuration on your primary and secondary servers
- Back up forensic information
- Download configuration backup and/or system log files to your workstation
- Validate certificates, and add or remove public keys
- View status of any backup or restore that was initiated
- Add customized banners to be shown each time users log into the system.



## Appliance Settings

Use the **Appliance Settings** window to specify information needed by your appliance and to enable key system features.

---

**IMPORTANT** You must be a user with read/write access to the System Configuration functional area to use this feature.

---

To access this window, go to **Configuration > Appliance Management > Appliance Settings**.

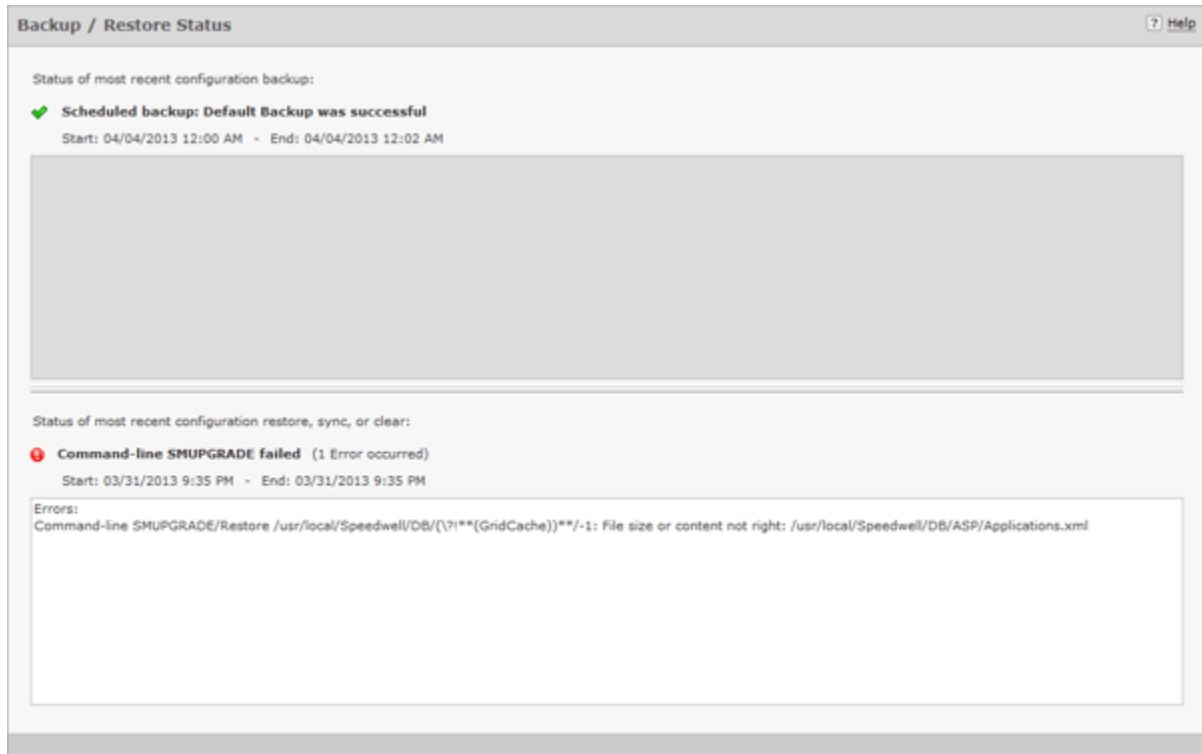
### Options

Function	Description
Port	Set the UI Port. This setting configures the system port for access to ADSP. Choose the system port from a port indicator/selector. Choices are port 1024 through 65000. <b>Hint:</b> ADSP will not allow you to choose a port already in use.
Mail Relay Server	Define the mail relay host. Enter an IP address or a fully-qualified host name.
Max Connections	Specify the maximum number of application server connections that can occur simultaneously.
User Session Limit	Limit the number of login sessions that one user can have at any one time.
Air Termination System	Air Termination enables you to terminate the connection between your wireless LAN and any associated authorized or unauthorized Access Point or Wireless Client. <b>Yes:</b> Click this radio button to enable AirTermination at the system level. Once enabled, the AirTermination setting for individual Sensors can also be enabled (See Sensor.) <b>No:</b> (Default). Click this radio button to disable AirTermination. <b>Hint:</b> If you are not an Admin level user, this setting will not be visible.

Function	Description
Policy-based Air Termination System Enabled	<p>Policy-based Air Termination is an automated version of Air Termination. This feature enables you to formulate an Action Plan to automatically terminate the connection between your wireless LAN and any associated authorized or unauthorized Access Point or Wireless Client, based on alarms.</p> <p><b>Yes:</b> Click this radio button to enable Policy-based Termination at the system level.</p> <p><b>No:</b> (Default). Click this radio button to disable Policy-based Termination.</p> <p><b>Hint:</b> If you are not an Admin level user, this setting will not be visible.</p>
Port Suppression System	<p>Port Suppression enables you to turn off the port on the network switch through which a device is communicating. You can suppress the communications port for any network device, effectively shutting down the communication port for the device.</p> <p><b>Yes:</b> Click this radio button to enable Port Suppression at the system level. See the Note, below.</p> <p><b>No:</b> (Default). Click this radio button to disable Port Suppression.</p> <p><b>Note:</b> You must have added SNMP Managed Switches and have full read and write privileges (see Adding/Importing Switches).</p>
Auto-Logout Enabled	<p>Use this feature to enable/disable the automatic logout feature, which logs a user out of ADSP after a specified amount of time.</p> <p><b>Yes:</b> Click this radio button to use Auto-Logout and activate the Auto-Logout Timeout scroll list.</p> <p><b>No:</b> Click this radio button to disable the Auto Logout and deactivate the Auto-Logout Timeout drop down list.</p> <p><b>Note:</b> You must log off ADSP and then log back in before changes take effect.</p>
Auto-Logout Timeout (Minutes)	<p>This scroll list is activated when the Auto-Logout Enabled option is selected. Use the scroll button to set the number of minutes for the automatic logout feature to log users out of the system.</p> <p><b>Note:</b> You must log off ADSP and then log back in before changes take effect.</p>
Spectrum Scan Timeout	<p>This drop-down menu allows you to set the timeout value for scanning during dedicated Spectrum Analysis. The values can be 1 - 120.</p>
Sensor Cloaking Limit	<p>The number amount of Sensors that can be cloaked at any one time.</p>



## Backup / Restore Status

Backup / Restore Status allows you to view the status of your configuration backups and restores.



The top section displays status information about backups. The bottom section displays status information about configuration restores, synchronization, clear information, and upgrade information.

The following status information is displayed:

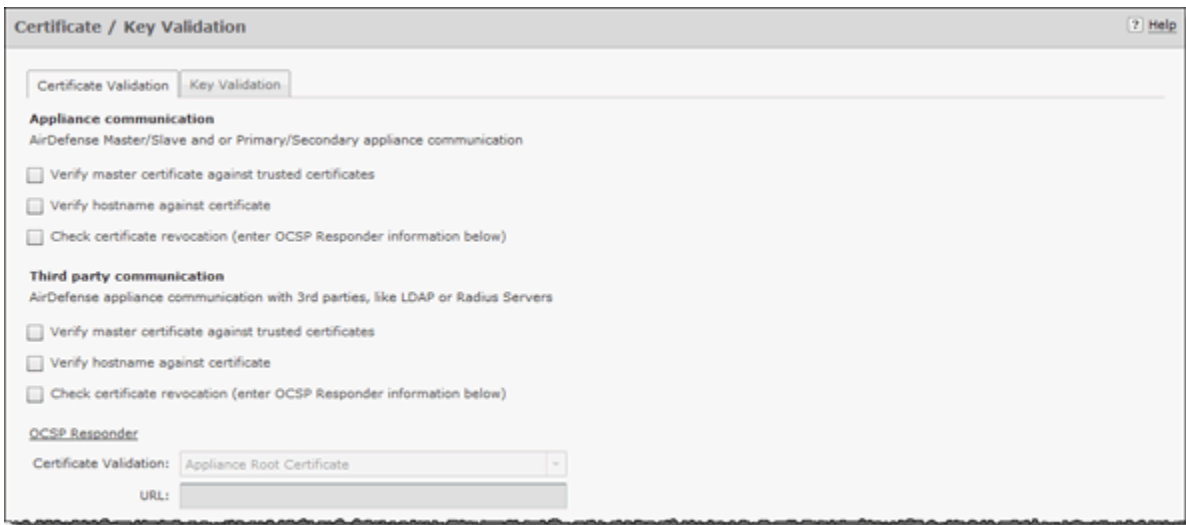
- A green checkmark—  indicates that the backup/restore was successful.
- A red circle containing an exclamation mark—  indicates that the backup/restore was unsuccessful.
- A start and end time is displayed to show you when the backup/restore started and when it ended.
- Any errors are displayed in the error window for each section.

### Certificate / Key Validation

Certificate / Key Validation is where you validate certificates, and add or remove public keys.

#### *Certificate Validation*

The Certificate Validation tab allows you to validate certificate communications for your appliance and/or for any third party servers.



The screenshot shows the 'Certificate / Key Validation' web interface. At the top, there are two tabs: 'Certificate Validation' (selected) and 'Key Validation'. Below the tabs, there are two main sections: 'Appliance communication' and 'Third party communication'. Each section contains three checkboxes: 'Verify master certificate against trusted certificates', 'Verify hostname against certificate', and 'Check certificate revocation (enter OCSP Responder information below)'. Below these sections, there is an 'OCSP Responder' section with a 'Certificate Validation' dropdown menu (set to 'Appliance Root Certificate') and a 'URL' text input field.

There are three types of verifications for either appliance communications or third party communications. They are:

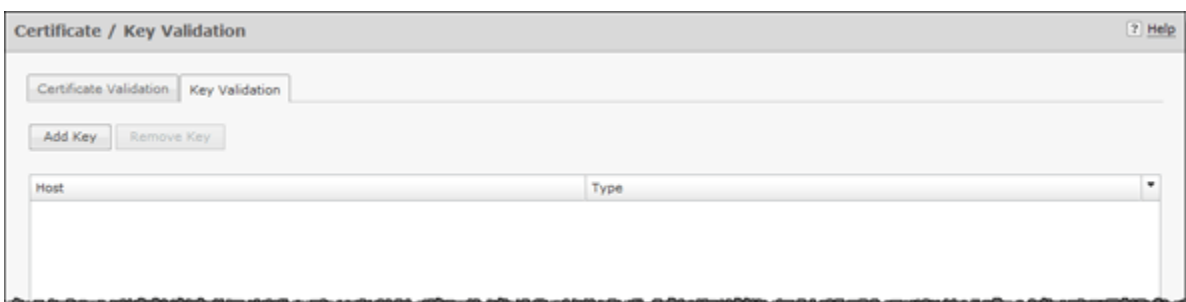
- Verify master certificate against trusted certificates
- Verify hostname against certificate
- Check certificate revocation.

Select the appropriate checkbox for each type of verification that you want to check. If the **Check certificate revocation** checkbox is selected, the OCSP Responder fields are activated. When activated, you must select the certificate type and enter its URL.

Clicking **Apply** validates your selections.

#### *Key Validation*

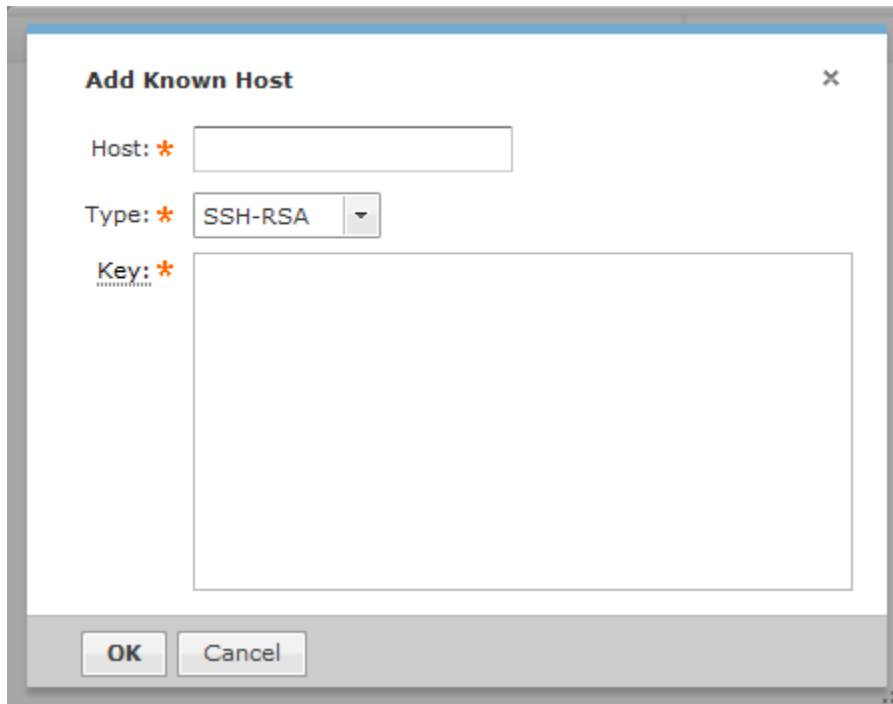
The **Key Validation** tab allows you to add and remove public keys for other servers.



The screenshot shows the 'Certificate / Key Validation' web interface with the 'Key Validation' tab selected. At the top, there are two tabs: 'Certificate Validation' and 'Key Validation' (selected). Below the tabs, there are two buttons: 'Add Key' and 'Remove Key'. Below these buttons, there is a table with two columns: 'Host' and 'Type'. The table is currently empty.

To add a public key:

1. Click the **Add Key** button.



2. Type in the name of the other server.
3. Select the type of public key that you want to add (**SSH-RSA** or **SSH-DSS**).
4. Paste the public key into the **Key** field.

For example, if you possess the following public key:

```
---- BEGIN SSH2 PUBLIC KEY ----
```

Comment: ""

```
AAAAB3NzaC1yc2EAAAABJQAAAIBrxx+YqQARTVMHfyjisoQvBZoxvBMxf9CbXoo
VpWHBezQbm3anaav+4rEPlylcfFrIR/9o3/ldXT+arnXlrZ+7v3kBVx9SRWr5GY1
BtPFEIVQi1PJz/tXTP3erWyoZ4mwsb0kmoFAPc9LBrwrLtSlkrXezZrKZMa4VzB9
yK6dAQ==
```

```
---- END SSH2 PUBLIC KEY ----
```

copy the actual key part and paste it into the **Key** field.

```
AAAAB3NzaC1yc2EAAAABJQAAAIBrxx+YqQARTVMHfyjisoQvBZoxvBMxf9CbXoo
VpWHBezQbm3anaav+4rEPlylcfFrIR/9o3/ldXT+arnXlrZ+7v3kBVx9SRWr5GY1
BtPFEIVQi1PJz/tXTP3erWyoZ4mwsb0kmoFAPc9LBrwrLtSlkrXezZrKZMa4VzB9
yK6dAQ==
```

5. Click **OK**.

To remove a public key, select (highlight) the key and then click the **Remove Key** button.

## Certificate Manager

Certificates verify the authenticity of the ADSP appliance. They 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 browser.

---

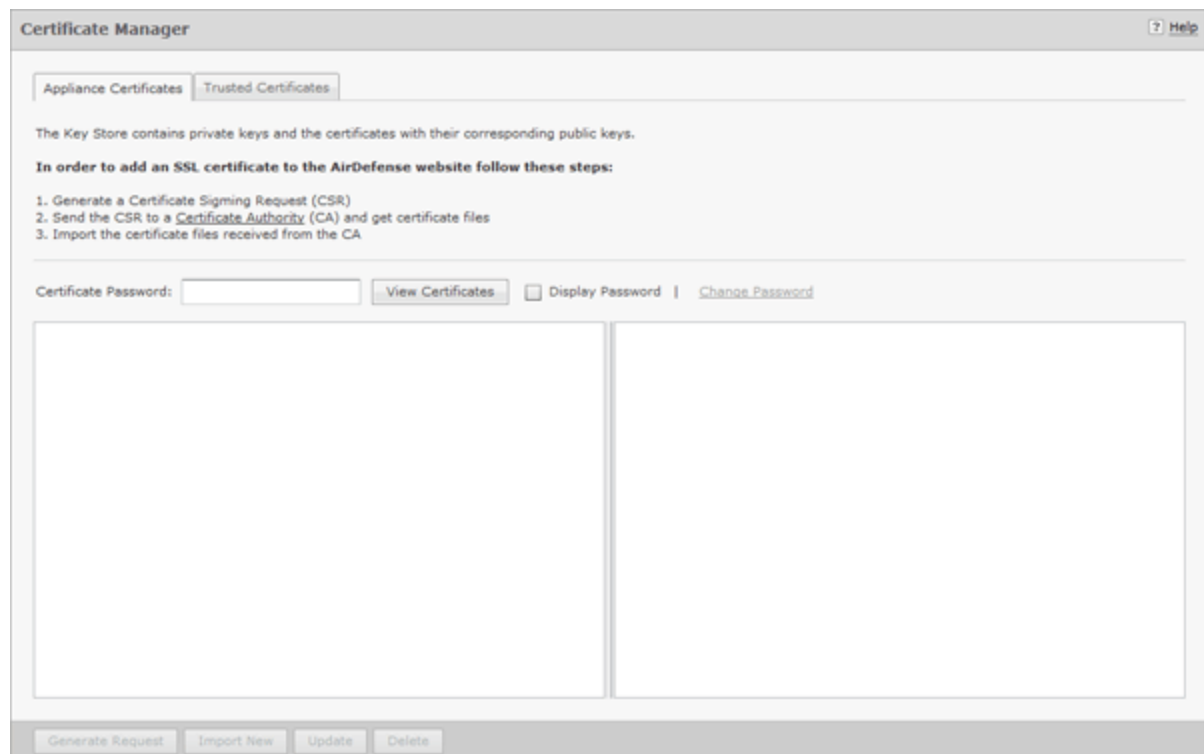
**IMPORTANT** Motorola AirDefense recommends using a security certificate for every ADSP appliance in your network. Furthermore, we recommend that you replace the pre-installed security certificate from Motorola AirDefense with either a self-signed certificate or a root-signed certificate.

---

Motorola AirDefense supports the X.509 ITU-T (ITU Telecommunication Standardization Sector) standard for certificates. The supported encryption key lengths are 2048, 4096, and 8192. More information about the X.509 ITU-T standard can be found by searching the Internet.

Use the Certificate feature to view and create security certificates for the ADSP appliance, and to perform other certificate-related tasks, such as installing certificates. You must be a user with the role of Admin to use this feature. You can access the Certificates feature by following these steps:

1. Navigate to **Configuration > Appliance Management > Certificate Manager**.



2. Enter your certificate password.

✓ **NOTE** The first time you access Certificates use the default password (security). Afterwards, change the default password to one that is more secure.

3. Click the **View Certificates** button.

### *Certificate Types*

Every ADSP appliance comes with an Motorola AirDefense certificate. However, there are three other certificates available; each represents a different level of security.

- Self-signed certificate
- Root-signed certificate
- SSL certificate.

The following table describes each of the certificate types:

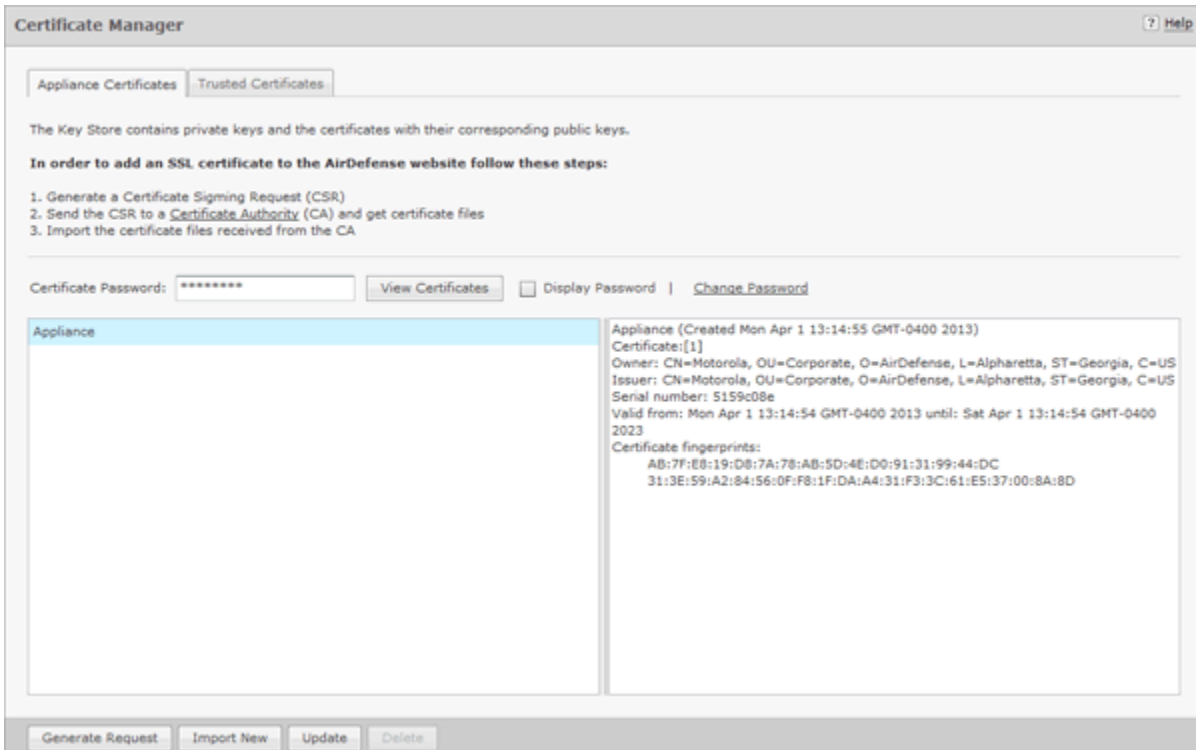
Certificate	Description
AirDefense Certificate	<p><b>The AirDefense certificate represents a minimal level of security.</b></p> <p>Motorola AirDefense ships the ADSP appliance with a pre-installed security certificate. It is a working certificate that provides TLS encryption, but has not been verified 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.</p> <p>Unless the certificate meets all required criteria, you will receive one or more alert screens when you open a session with ADSP.</p>
Self-Signed Certificate	<p><b>A self-signed certificate represents an intermediate level of security.</b></p> <p>A self-signed certificate (also called "Tomcat Certificate") is a certificate that you must generate. In this certificate, you specify the host name of the AirDefense Server, but do not have the certificate verified and digitally signed by a root Certificate Authority.</p> <p>Unless the certificate meets all required criteria, you will receive one or more alert screens when you open a session with AirDefense.</p>
Root-Signed Certificate	<p><b>A root-signed certificate represents a high level of security.</b></p> <p>A root-signed certificate is a public certificate that is verified by a root Certificate Authority (CA). This is a digitally-signed certificate that ensures the authenticity of the AirDefense Server.</p>
SSL Certificate	<p><b>A SSL certificate represents the highest level of security.</b></p> <p>SSL certificates create a secure connection between a client and a server. The client is usually a web browser transmitting private information over the Internet. The URL for SSL connections start with https:// instead of http://.</p>

### *Viewing Certificates*

There are two panels in the Certificates window. The left panel lists your current certificates. When you select (highlight) a certificate by clicking on it, information for that certificate is displayed in the right panel. The following information is available:

- Alias name
- Creation date

- Certificate details that include:
  - Certificate number
  - Owner information
  - Issuer information
  - Serial number
  - Validation period stating when the certificate became valid and when it ends
  - Certificate fingerprints.



### ***Sharing Certificates***

ADSP has a Central Management feature that allows you to monitor more than one appliance. In this situation, there will be a master appliance and a slave appliance. In order for this scenario to take place, you will need to share certificates between the master and the slave appliance.

There are two scenarios to sharing certificates after adding a slave appliance:

- Certificates on either the master appliance or slave appliance are in the default state.
- Certificates have been modified, changed, or imported on either appliance, and have been signed by a Certificate Authority (CA).

### **Sharing Certificates in Default State**

Sharing certificates in the default state is the easiest way to share certificates between a master appliance and a slave appliance. The following conditions must be met:

- The slave appliance must first be added using **Add Devices** under the **Menu**
- Both servers must be able to successfully ping each other
- Both master and slave must be running the same build



- The certificates have not been modified or changed, or imported to either of the servers, and have not been signed by a CA
- The user name and passwords are entered correctly in Share certificate window, and the **Alias** field has the slave appliance IP address.

The procedure to sharing certificates in the default state is:

1. Access the Certificate Manager.
2. Select the slave appliance in the **Appliance** field.
3. Type in the certificate password and then click **View Certificates**.
4. Click the **Share Appliance Certificate** button.

✓ **NOTE** The **Share Appliance Certificate** button is only visible after adding the slave appliance with **Add Devices**.

5. Fill in the above dialog window with the following information:

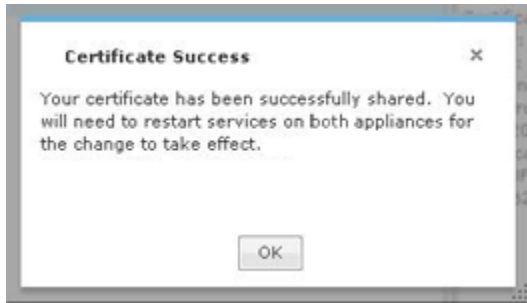
For the slave appliance:

- The user name and password used to access the GUI
- The appliance certificate password
- The trusted certificate password.

For the master appliance:

- The appliance certificate password
- The trusted certificate password.
- An alias that will show up in the trusted certificates on the slave. The default is the slave appliance IP address. This field is for identification purposes. You can change it to whatever you want it to be.

6. Click the **Share** button.



7. Click **OK**.
8. Restart the master appliance and slave appliance.
9. Check the master appliance to see that the slave appliance is now online.

### **Sharing Certificates not in Default State**

Sharing certificates not in the default state involves some extra steps. The following conditions must be met:

- The slave appliance must first be added using **Add Devices** under the **Menu**
- Both servers must be able to successfully ping each other
- Both master and slave must be running the same build
- The user name and passwords are entered correctly in Share certificate window, and the **Alias** field has the slave appliance IP address.

The procedure to sharing certificates in the default state is:

- ✓ **NOTE** This procedure assumes that you have added a certificate using the procedures under [Adding Certificates](#).

1. Access the Certificate Manager.
2. In the **Appliance** field, select the slave appliance.
3. Type in the certificate password and then click **View Certificates**.
4. Click the **Share Appliance Certificate** button.

- ✓ **NOTE** The **Share Appliance Certificate** button is only visible after adding the slave appliance with **Add Devices**.

- Fill in the above dialog window with the following information:

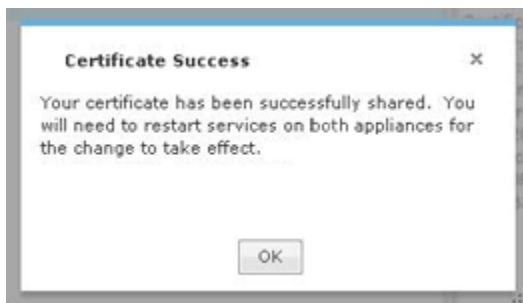
For the slave appliance:

- The user name and password used to access the GUI
- The appliance certificate password
- The trusted certificate password.

For the master appliance:

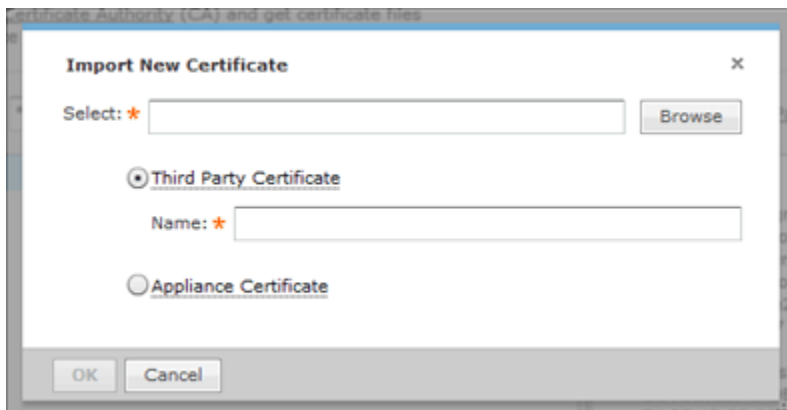
- The appliance certificate password
- The trusted certificate password.
- An alias that will show up in the trusted certificates on the slave. The default is the slave appliance IP address. This field is for identification purposes. You can change it to whatever you want it to be.

- Click the **Share** button.



- Click **OK**.
- On the master appliance, access the **Trusted Certificate** tab.
- In the **Appliance** field, select the master appliance.
- Type in the certificate password and then click **View Certificates**.

11. Click the **Import New** button.



12. Browse to CA certificate and select it.
13. Click **OK**.
14. Restart the master appliance.
15. On the slave appliance, access the **Trusted Certificate** tab and then repeat Steps 9 through 12.
16. Restart the slave appliance.
17. Check the master appliance to see that the slave appliance is now online.

### ***Adding Certificates***

There are two types of certificates that you can add:

- Appliance Certificate
- Trusted Certificate.

Installation instructions for each type are included in their respective topics.

### **Appliance Certificates**

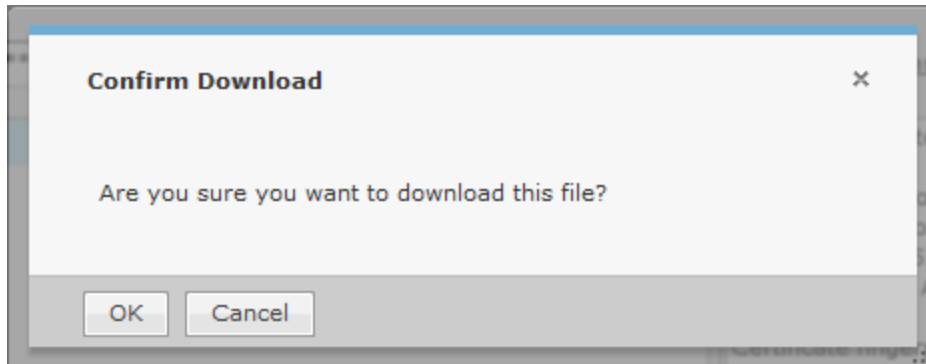
The Appliance Certificates store private keys and the certificates with their corresponding public keys. There are three main steps to adding an appliance certificate. They are:

1. Generate a Certificate Signing Request (CSR).
2. Send the CSR to a Certificate Authority (CA) and get certificate files.
3. Import the certificate files received from the CA.

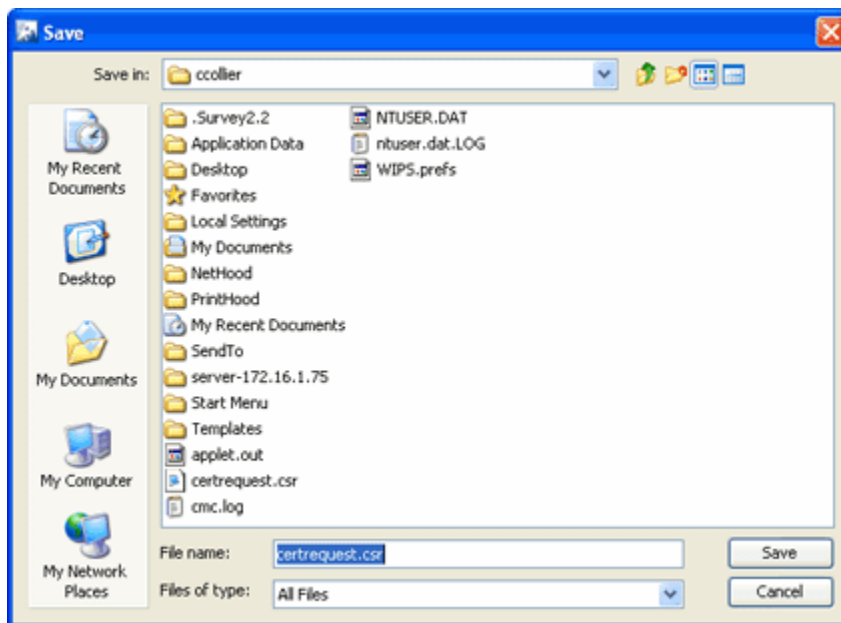
Each of these steps are discussed in the following sub-topics.

### Generate a CSR

1. Click the **Generate Request** button. A window opens for you to confirm that you want to download the CSR.



2. Click **OK**. A window opens for you to save your request.



3. Navigate to in a convenient place such as your Desktop to save the CSR. The default name is *certrequest.csr*. You can use this name or change it.
4. Click the **Save** button.

### Send CSR to a CA and Get Certificate Files

There is no set procedure on how to send a CSR to a CA and get the certificate files. This is dependent on the CA and their procedures.

The file save in Generate a CSR has the information that a CA needs to issue certificate files. You will have to present this information to the CA in some way.

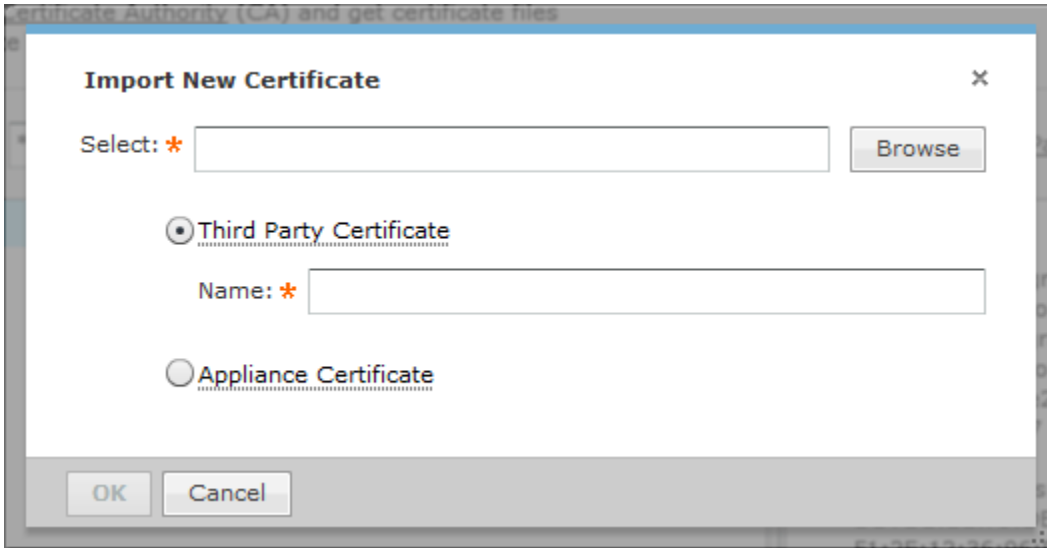
Once you give the CA the information from the generated file, they will give you instructions on how to proceed, probably an email message. You will have to save the certificate files somewhere on your workstation such as your Desktop. There should be three certificates:

- Intermediate

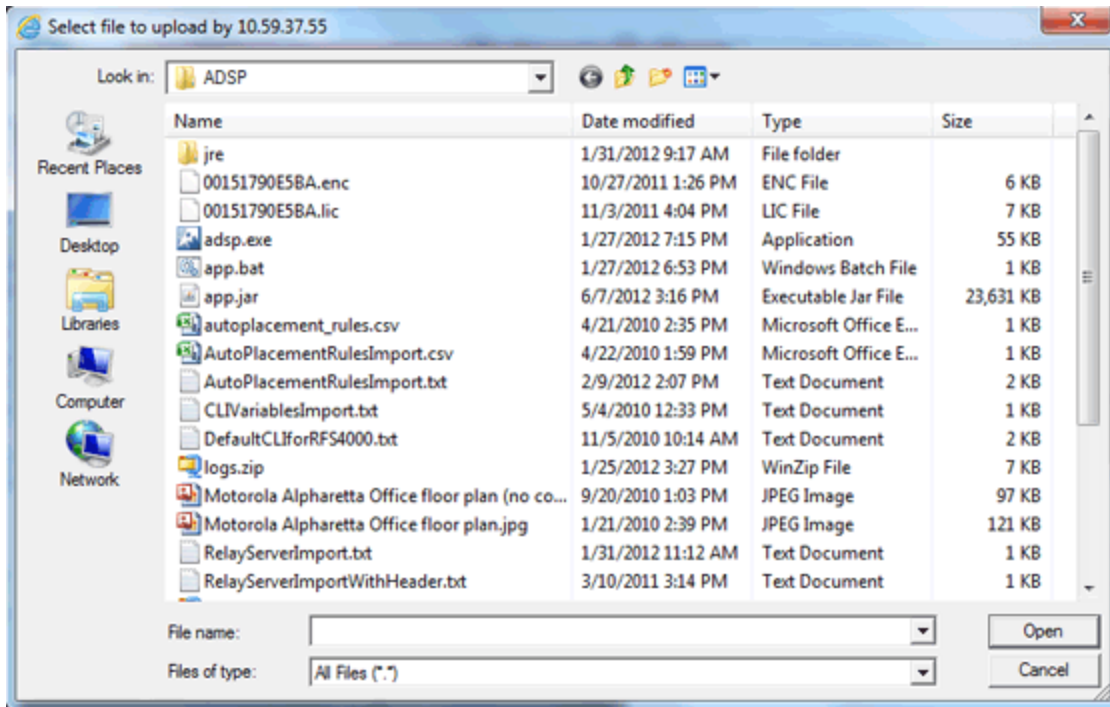
- Root
- SSL which is the tomcat certificate.

**Import the Certificate Files**

1. Click the **Import New** button. The **Import New Certificate** window displays.



2. Click the **Browse** button to open the **Select file to upload** window.



✓ **NOTE** This is the procedure for a third party certificate. You also have the option of selecting an appliance certificate which includes private keys for the appliance, and is either self-signed or signed by a CA. Appliance certificates are always named Appliance.

3. Navigate to the Intermediate certificate, select (highlight) it, and then click the **Open** button. The file name should now display in the **Select** field.

4. Type in a name for the certificate.
5. Click **OK**.
6. Repeat Steps 1 to 5 to import the Root certificate.
7. Repeat Steps 1 to 5 to import the SSL certificate.

✓ **NOTE** The name for the SSL certificate defaults to tomcat. You cannot change this name.

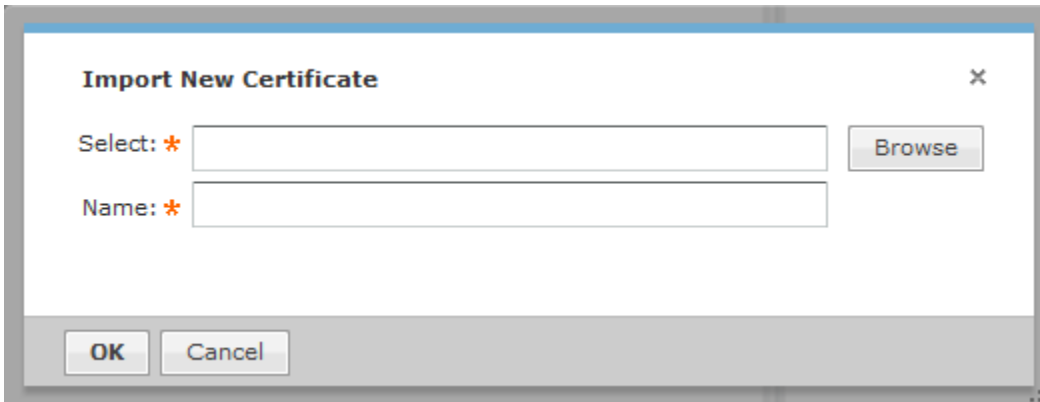
8. Click **OK**.

✓ **NOTE** You will have to restart tomcat services before the certificates are activated. The tomcat services are located on your ADSP appliance.

### Trusted Certificates

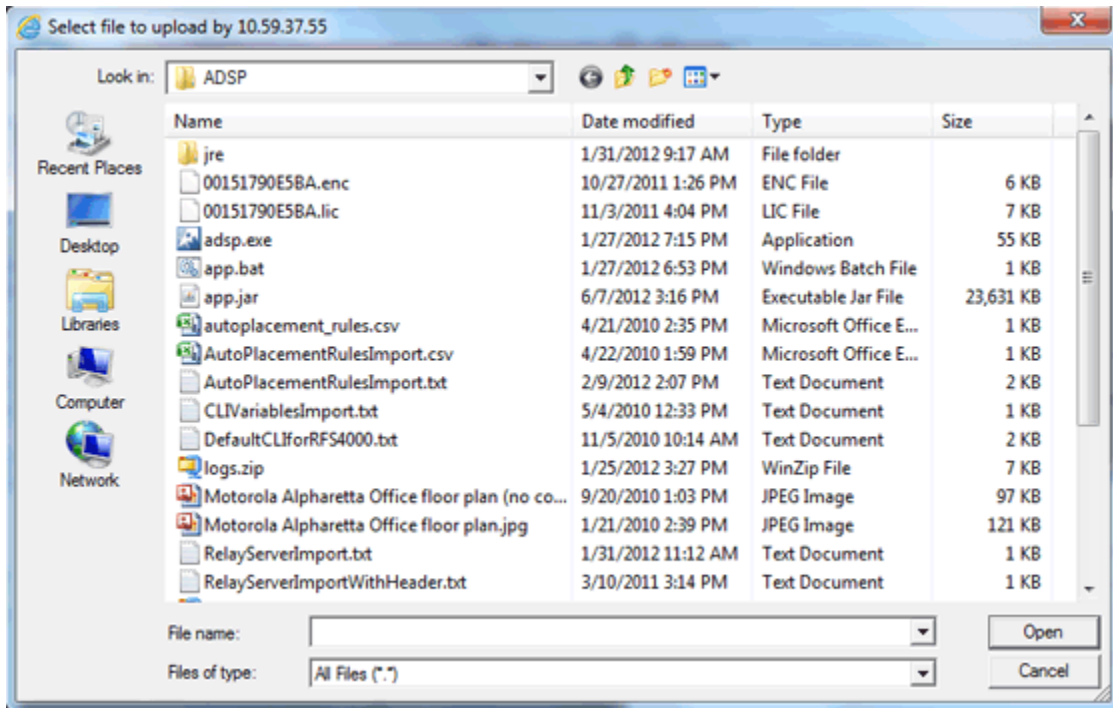
The Trusted Certificates store contains certificates from other parties (like ADSP Appliances, LDAP or Radius Servers) that you expect to communicate with, or from Certificate Authorities that you trust to identify other parties. Follow these steps to install a trusted certificate:

1. Click the **Import New** button. The **Import New Certificate** window displays.



The screenshot shows a dialog box titled "Import New Certificate" with a close button (X) in the top right corner. The dialog contains two text input fields: "Select: \*" and "Name: \*". To the right of the "Select" field is a "Browse" button. At the bottom of the dialog are "OK" and "Cancel" buttons.

- Click the **Browse** button to open the **Select file to upload** window.



- Navigate to the trusted certificate, select (highlight) it, and then click the **Open** button. The file name should now display in the **Select** field.
- Type in a name for the certificate.
- Click **OK**.

### ***Updating Default Certificate Information***

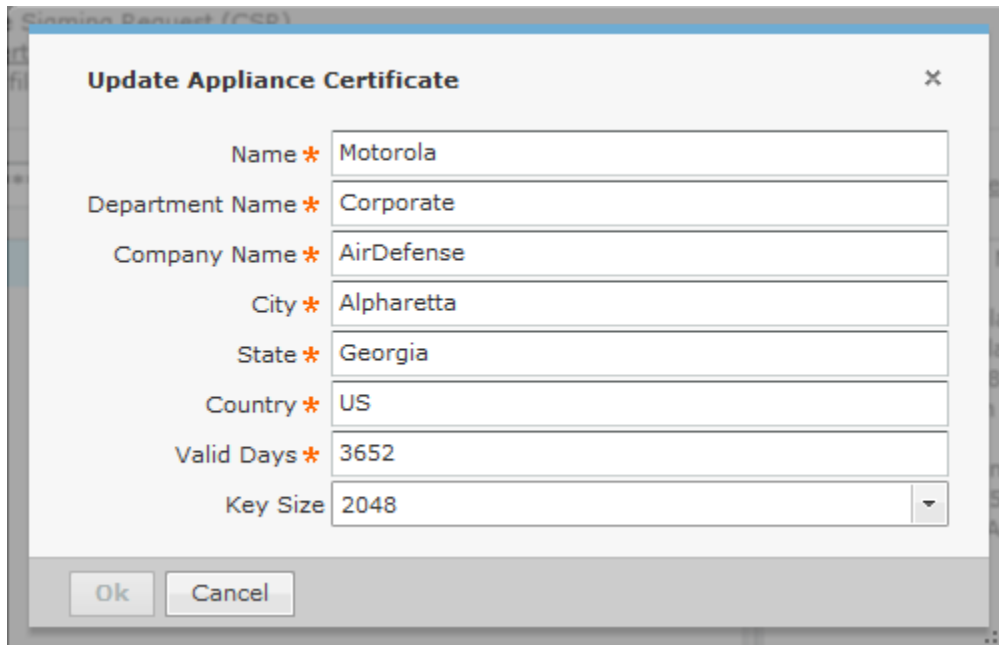
The Motorola AirDefense default information is included with each certificate that you add. You may change this information if you feel it is necessary. The following information may be changed:

Field	Description
Name	The hostname you assigned the ADSP appliance.
Department Name	The department in which the ADSP administrator is a member.
Company Name	The name of your company.
City	The city in which your company is located.
State	The State (full name—not abbreviated) in which the company is located.
Country	The two-character country code for the country in which the company is located.
Valid Days	The number of days a certificate is valid once you add it.
Key Size	The certificate encryption key length. Supported encryption key lengths are 2048, 4096, and 8192.

To change the default information, follow these steps:



1. Click the **Update** button to display the **Update Appliance Certificate** window.



**Update Appliance Certificate**

Name \* Motorola

Department Name \* Corporate

Company Name \* AirDefense

City \* Alpharetta

State \* Georgia

Country \* US

Valid Days \* 3652

Key Size 2048

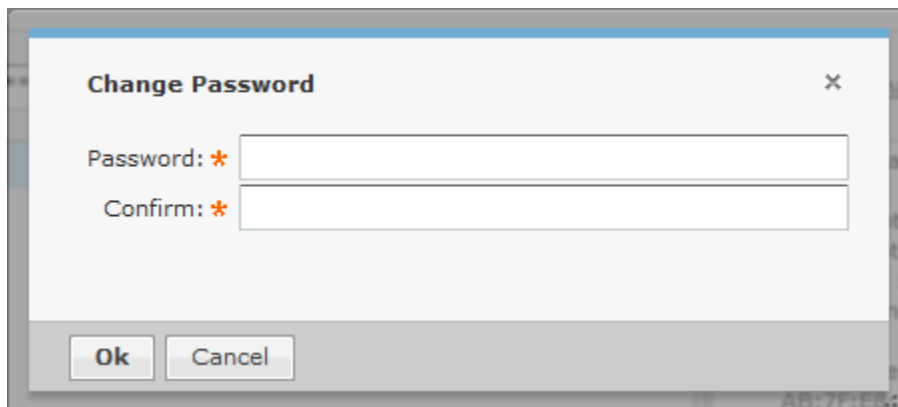
Ok Cancel

2. Change any of the information using the previous table as a guideline.
3. Click the **OK** button.

### *Changing Certificate Password*

The **Certificates** window has a default password (security). You should change this password to a more secure password. To change the password:

1. Click the **Change Password** link.



**Change Password**

Password: \*

Confirm: \*

Ok Cancel

2. Type the new password in the **Password** field.
3. Type the new password again in the **Again** field.
4. Click the **OK** button.

### *Exporting Certificates*


Exporting a certificate allows you to store a copy of the certificate, the certificate trust list, and the certificate revocation list on a computer disk.

✓ **NOTE** This information is required for Managed Services Provider (MSP) integration.


Depending on your browser, follow one of these procedures:

✓ **NOTE** Procedures for Internet Explorer and Firefox are included here. Other browsers will have similar buttons/links that allow you to export a certificate.

#### **For Internet Explorer**

1. Click **Certificate Error**—  near the top of Internet Explorer.
2. Click the **View Certificates** link.
3. Access the **Details** tab.
4. Click the **Copy to File** button. The **Certificate Export Wizard** displays.
5. Click **Next**.
6. Select a file format for the certificate and then click **Next**.
7. Click the **Browse** button. Then, select a location and specify a file name.
8. Click **Save**. The path and file name is displayed in the **File Name** field.
9. Click **Finish**.

#### **For Firefox**

1. Click the area with the Motorola logo and appliance ID—  near the top of Firefox.
2. Click the **More Information** button.
3. Click the **View Certificate** button.
4. Access the **Details** tab.
5. Click the **Export** button.
6. Select a location and specify a file name.
7. Click **Save**.

## Configuration Backup

Configuration Backup allow you to backup up your appliance configuration to your workstation or to your appliance. There are two methods to accomplish this:

- Manual Backups
- Automatic Backups.

The screenshot shows the 'Configuration Backup' interface. At the top, there are buttons for 'Backup Now', 'Enable Configuration Backup Scheduling' (checked), 'Add New Schedule', and 'Delete'. Below this is a table with two columns: 'Name' and 'Schedule'. The table contains one entry: 'Default Backup' with a schedule of 'Default Backup - Daily: Every 1 day at 12:00 AM'. Below the table are two sections: 'Settings' and 'Schedule'. The 'Settings' section includes fields for 'Job Name', 'Destination' (Local selected, Remote unselected), 'Host', 'Port', 'Protocol' (SCP), 'Path', 'User', 'Password' (with a 'Display Password' checkbox), and 'Retries' (set to 1, max 5). The 'Schedule' section includes 'Frequency' (One Time Schedule), 'Time' (12:00 AM), and 'Date' (04/03/2013). At the bottom are 'Apply' and 'Reset' buttons.

### 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 looks like: `Backup_8.1.0-10_ECRT236.am.mot.com_20101018000011.zip.enc`. The name always includes the release, the server 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.

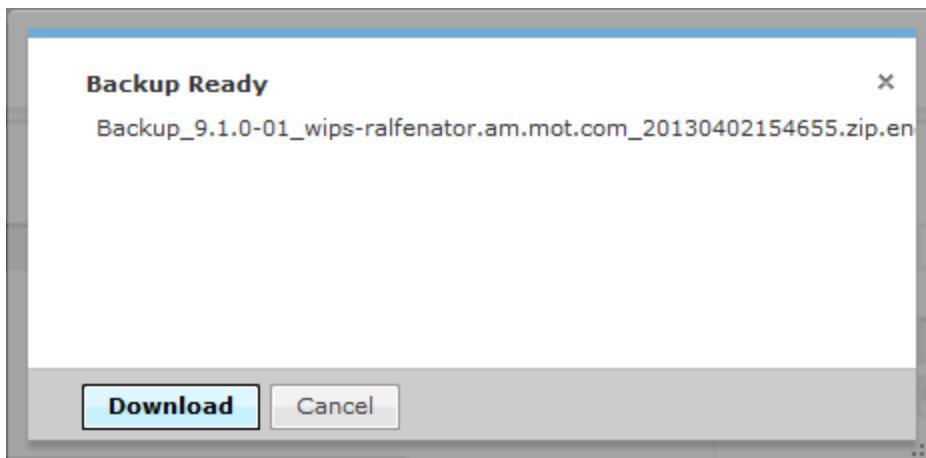
### ***Backup Recommendations***

- As a minimum, schedule a daily backup internal during non-peak hours.
- If there is an external server to backup to, schedule an external backup at least once a week and NOT at the same time as a local backup.
- NEVER direct a backup to /usr/local/smx/backups on a standby server. This will prevent synchronization from working properly.

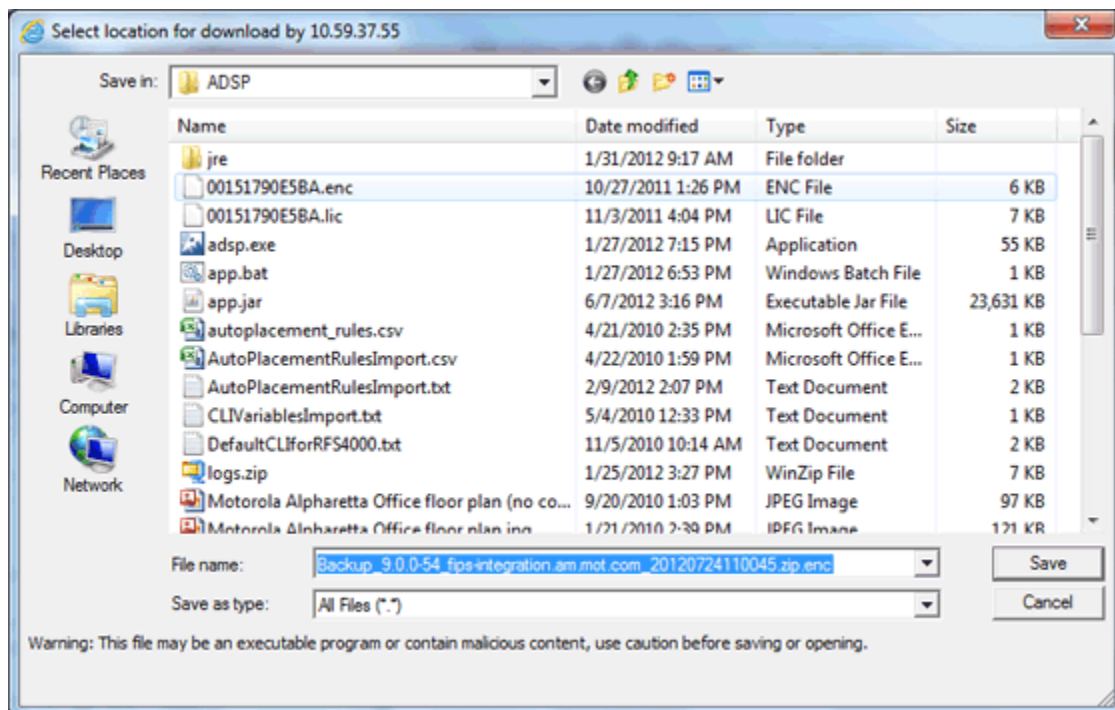
### ***Manual Backups***

You can manually back up your server configuration to your workstation by following these steps:

1. Click the **Backup Now** button to display the **Backup Ready** window.



2. Click the **Download** button to open a window where you can select your destination directory (folder).



3. Navigate to the directory where you want to back up your server configuration.
4. Click **Save** to save the backup file in the selected directory.

### *Automatic Backups*

Automatic Backups backs up your system configuration to your ADSP appliance.



**CAUTION** Do not configure the automatic backup time and the automatic synchronization time with the same values.

To schedule automatic backups, follow these steps:

1. Enable automatic backups by clicking the **Enable Configuration Backup Scheduling** checkbox to place a checkmark in the box.
2. Type in a name for the backup (**Job Name** field).
3. 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 drop-down menu.
4. 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 <b>Time</b> drop-down menu. Then, select a day for the backup by clicking the <b>Calendar</b> button in the <b>Date</b> 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.

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

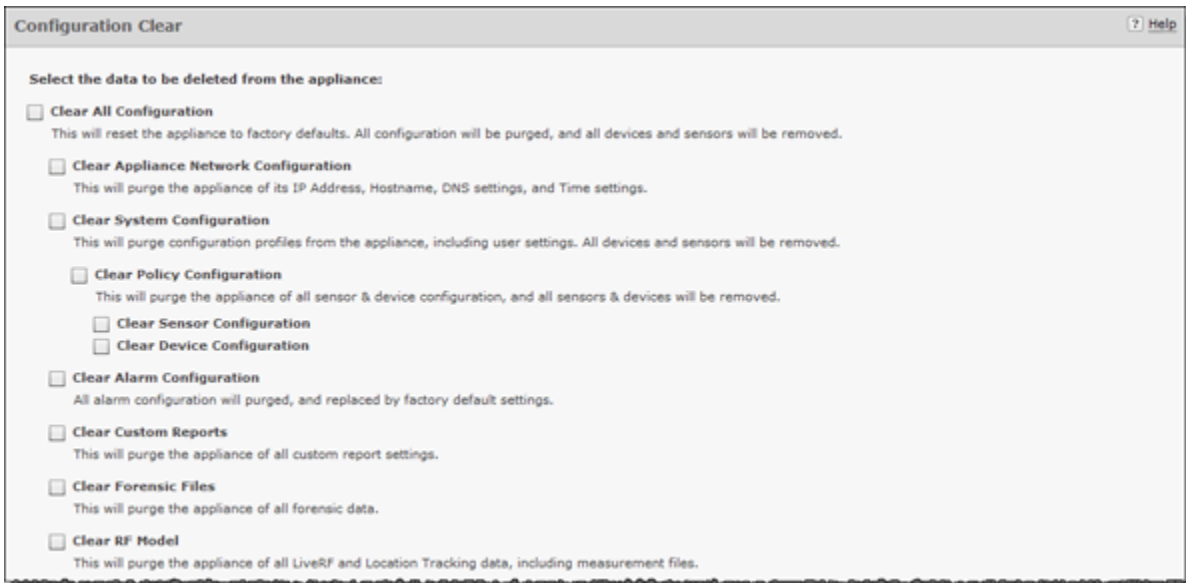
During an automatic backup you can also send the backup configuration to another AirDefense Enterprise server. Click the **Remote** checkbox to place a checkmark in the box and fill in the following fields:

Field	Description
Host	The name of the server where you want to back up the configuration. This can be an IP address or a DNS name defined by your DNS server.
Port	The port number to use during the backup.
Protocol	The file transfer protocol to use for backing up the configuration ( <b>SCP</b> , <b>SFTP</b> , or <b>HTTPS</b> ).
Path	The directory (folder) where to place the backup on the destination server.
User	The username used to log in on the destination server.

Field	Description
Password	The password used to log in on the destination server.
Verify Server Certificate/Key	Verifies that the server certificate (HTTPS connections) or server key (SCP and SFTP connections) is valid.
Retries	The number of times to retry the backup if a failure occurs. The maximum number is 5.

## Configuration Clear

You can clear configuration data and set it back to its default state when your system was delivered.



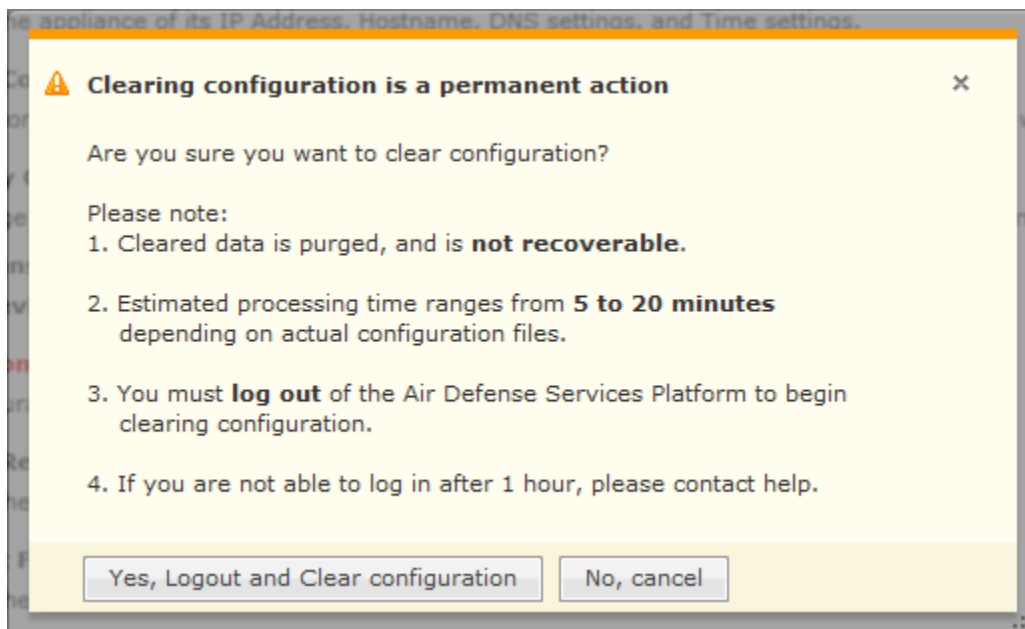
You can clear all your configuration data and reset the system as it was first delivered or you can clear specific configuration data. The options are:

Option	Description
Clear All Configuration	Clears all configuration data, setting your server back to its original default state.
Clear Appliance Network Configuration	Clears the configuration for the appliance network. All network configuration is set back to default.
Clear System Configuration	Clears all system configuration data. This encompasses everything except what is covered by the other options. There are three other options associated with this option. <ul style="list-style-type: none"> <li>Clear Policy Configuration—Clears all policy configurations that you have changed. If you select this option, the Sensor and Device configurations will be automatically selected.</li> <li>Clear Sensor Configuration—Clears all Sensor configurations that you customized.</li> <li>Clear Device Configuration—Clears all device configurations that you customized.</li> </ul>
Clear Alarm Configuration	Clears any configuration dealing with alarms and sets alarm configuration data back to default.

Option	Description
Clear Custom Reports	Clears any custom reports that you have created.
Clear Forensic Files	Clears (removes) any forensic data files that exists.
Clear RF Model	Clears the RF data used by Live RF and Location Tracking in the Floor Plan.

To clear configuration data, follow these steps:

1. Select one or more options by placing a checkmark in the checkbox.
2. After selecting your options, click the **Next** button. A confirmation window is displayed.



3. Select the **Yes, Logout and Clear configuration** button to confirm that you want to logout and clear the configuration data.

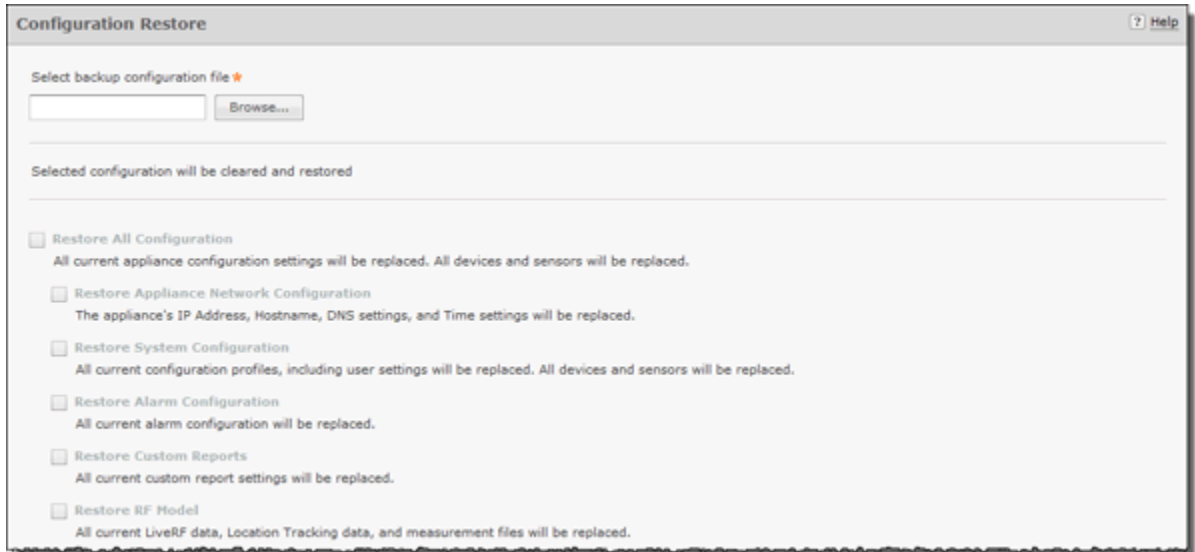


**NOTE** Clicking the **No, cancel** button will cancel the clear operation.

## Configuration Restore

You can restore a backup configuration that you backed up to your workstation. To do so, follow these steps:

1. Navigate to **Configuration > Appliance Management > Configuration Restore**.



2. Click **Replace** button to open a window where you can select the directory (folder) where your configuration was backed up.
3. Navigate to the directory where your configuration was backed up and select the backup file.
4. Click **Open** to select the file. The directory path with file name displays in the **Select backup configuration file** field and the options become active.
5. Select the options that you want to restore using the following table:

Option	Description
Restore All Configuration	Restores all configuration data from the backup file.
Restore Appliance Network Configuration	Restores the configuration for the appliance network.
Restore System Configuration	Restores all system configuration data. All Sensors and devices are replaced.
Restore Alarm Configuration	Restores any configuration dealing with alarms.
Restore Custom Reports	Restores any custom reports that you backed up.
Restore RF Model	Restores the RF data used by Live RF and Location Tracking in the Floor Plan.

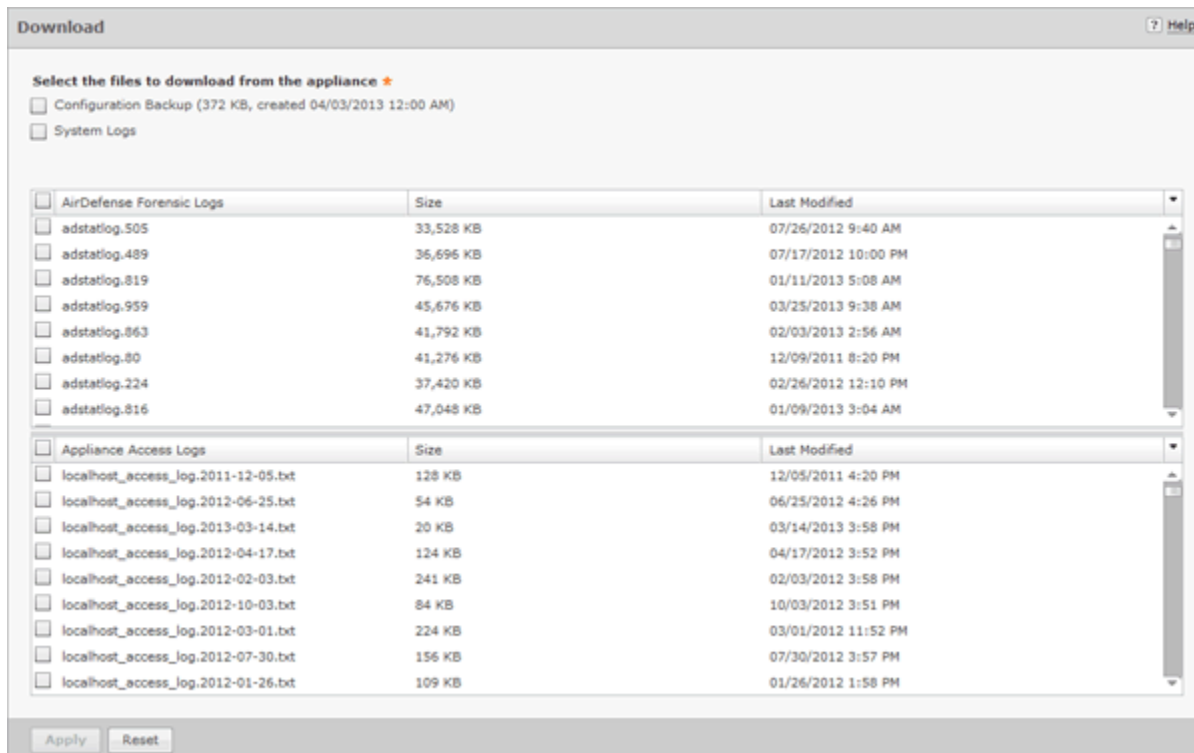
6. Click **Apply**. The configuration is restored to your ADSP server.

If you want to restore a configuration that was automatically backed up to your ADSP server, you can download it to your workstation (see [Download Logs](#)).



## Download Logs

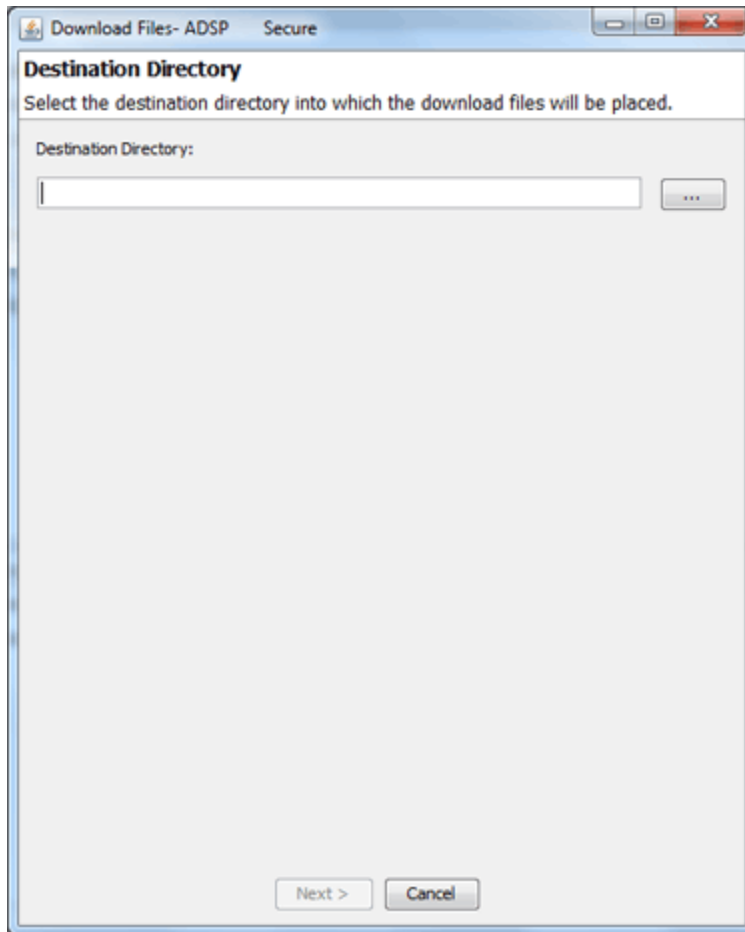
You can download configuration files that were automatically backed up to your ADSP server to your workstation. Once the backed up configuration is on your workstation, you can restore it. See [Configuration Restore](#).



To download a configuration, follow these steps:

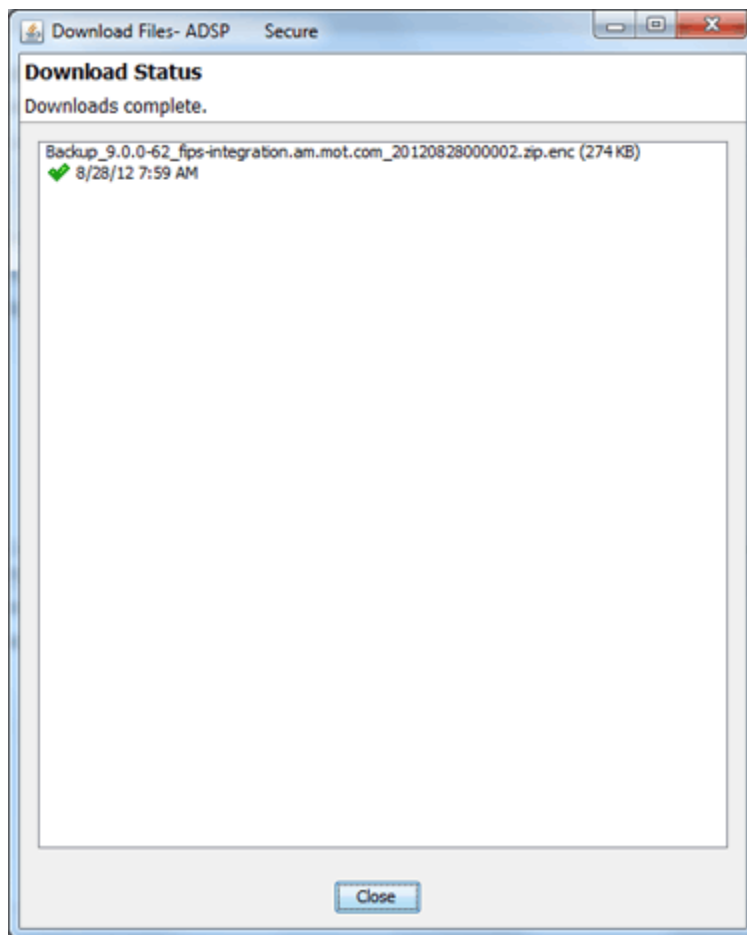
1. Navigate to **Configuration > Appliance Management > Download Logs**.
2. Select if you want to download a backup that exists on your appliance and/or the system logs.
3. You can download all forensic logs or all appliance access logs. Alternatively, you can pick and choose the forensic logs or appliance access logs that you want to download.

4. Click **Apply**. A destination directory window is displayed.



5. Click the **Browse** button to open a window where you can select your destination directory (folder).
6. Navigate to the directory where you want to download your server configuration.
7. Click **Select** to select the destination. The destination path displays in the **Destination Directory** field.

- Click **Next**. The configuration is downloaded to the selected directory and a status window is displayed confirming the download.



- Click **Close**.

## Forensic and Log Backup

You can automatically back up Forensics data and log files by navigating to **Configuration > Appliance Management > Forensic and Log Backup**.

To enable this automatic forensics backup, click the **Enable Automatic Forensics Backup** checkbox to place a checkmark in the checkbox. To enable this automatic log backup, click the **Enable Automatic Log Backup** checkbox to place a checkmark in the checkbox. Fill in the fields described in the table below. Fields for both types of backups are the same. Now, whenever a forensics file or a log file is created, it is automatically backed up on the host specified in the **Host** field.

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

Field	Description
Host	The name of the server where you want to back up forensics or log files. This can be an IP address or a DNS name defined by your DNS server.
Port	The port number to use during the backup.
Protocol	The file transfer protocol to use for backing up forensics or log files.
Path	The directory (folder) where to place the backup on the destination server.
User	The username used to log in on the destination server.
Password	The password used to log in on the destination server.
Verify Server Certificate/Key	Verifies that the server certificate (HTTPS connections) or server key (SCP and SFTP connections) is valid.
Retries	The number of times to retry the forensic backup if a failure occurs. The maximum number is 5.

You can schedule the backups for system and access logs. Select an interval and then 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 <b>Time</b> drop-down menu. Then, select a day for the backup by clicking the <b>Calendar</b> button in the <b>Date</b> 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.

## Language

ADSP allows you to select English, Chinese, Japanese, Korean, Portuguese, or Spanish as the language to use with your appliance.



Changing the language requires you to restart your appliance from ADSPadmin in the appliance CLI. Click **Apply** to switch languages.

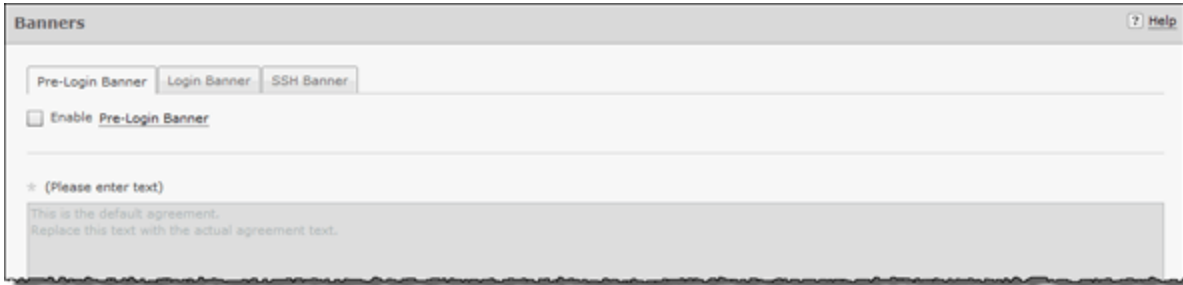
## Login / SSH Banners

The Banners window 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. Navigate to **Configuration > Appliance Management > Login / SSH Banners**.

Pre-Login banners are created in the **Pre-Login Banner** tab. Login banners are created in the **Login Banner** tab. SSH banners are created/edited in the **SSH Banner** tab.

### *Pre-Login Banner*

The **Pre-Login Banner** tab is provided for ADSP users who wish to display their own customized banner before logging into ADSP.



To activate, select **Enable Pre-Login Banner** checkbox.

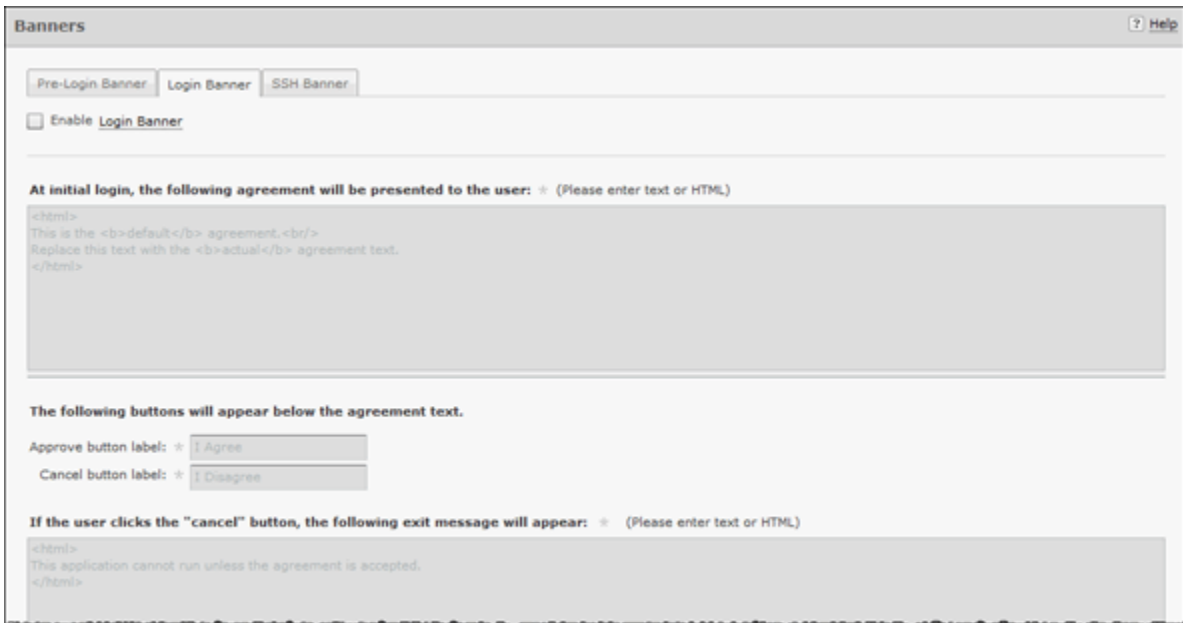
### Settings

The \* **(Please enter text)** field is available to enter text that users will see before logging into ADSP. Text can be entered in HTML or text format.

Click **Apply** to save the pre-login banner.

### *Login Banner*

The **Login Banner** tab 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.



To activate, select **Enable Login Banner** field.

**Features**

Function	Description
At initial login...	Enter the actual startup agreement text in this area; this text is what will appear when the ADSP application is first opened. <b>Note:</b> This text can be entered in HTML or text format.
Approve button label	Enter the actual text that will appear for the approve button on the <b>Startup Agreement</b> window. Default = <b>I Agree</b>
Cancel button label	Enter the actual text that will appear for the cancel button on the Startup Agreement window. Default = <b>I Disagree</b>
If the user clicks the...	Enter the actual text that will appear as a message dialog window when you choose to cancel the Startup Agreement. <b>Note:</b> This text can be entered in HTML or text format.

Click **Apply** to save the Login banner.

**SSH Banner**

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



To activate, select **Enable SSH Banner** field.

**Settings**

The **At initial login...** field is available to enter text that users will see when accessing the ADSP appliance through SSH. Text can be entered in HTML or text format.

Click **Apply** to save the SSH banner.

**Redundant Appliance Sync**

ADSP provides a feature that allows you to synchronize the configuration on your primary and secondary servers. There are two methods to accomplish this:

- Manual Synchronization
- Automatic Synchronization.

The proper way to synchronize servers is to configure your primary server first and then synchronize your secondary server with your primary server. All configuration settings are copied from your primary server to

your secondary server so that the two servers have the same configuration. Configuration settings from the primary server will override any configuration settings on the secondary server.

### *How Synchronization Works*

- Synchronization will not work if there is no backup file or if there is a backup in progress.
- On the standby server, during either scheduled or on-demand synchronization, the standby server pulls the current backup from `/usr/local/smx/backups` on the primary server.
- NEVER schedule a synchronization or perform an on-demand synchronization at the same time a backup is occurring on the primary server.
- NEVER start an on-demand backup while synchronizing servers.
- 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 server.
  - **NEVER** direct a backup from the primary server to `/usr/local/smx/backups` on a standby server. This will prevent synchronization from working properly.
- NEVER back up to the desktop from the standby server, because that process overwrites the existing file in `/usr/local/smx/backups`. See [How Backups Work](#).
- As the second part of synchronization, the standby server 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 server.

### *Synchronization Rules*

- You should only back up the primary server. NEVER schedule or perform a backup on the standby server.
- Synchronization should only be done from the standby server. NEVER schedule or perform a synchronization on the primary server.
- Always schedule or perform a backup on the primary server one hour before scheduling a synchronization or performing an on-demand synchronization on the standby server. Backups require more time as the primary server 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.

### *Manual Synchronization*

Follow these steps to manually synchronize your primary and secondary ADSP appliances:

1. On the secondary server, select the **Designate this as a Secondary (redundant) appliance** checkbox. The synchronization options activate.
2. Enter the IP address or DNS name of the primary server you want to synchronize with in the **Address** field.
  - ✓ **NOTE** If using a DNS name, it must be defined by your DNS server.
3. Enter the port number of the primary server in the **Port** field.



4. Enter the username in the **Username** field that allows you to log in on the primary server you are synchronizing with.



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

5. Enter the password in the **Password** field that allows you to log in on the primary server you are synchronizing with.
6. Select whether you want to synchronize appliance name and/or synchronize mail relay.
7. Click the **Sync Now** button. Configuration files are downloaded to the secondary server.

### *Automatic Synchronization*

Follow these steps to set up automatic synchronization of your primary and secondary ADSP appliances:



**CAUTION** Do not configure the automatic backup time and the automatic synchronization time with the same values.

1. Enable automatic synchronization by selecting the **Designate this as a Secondary (redundant) appliance** checkbox to place a checkmark in the box.
2. Enter the address, port, username, and password as described for manual synchronization.
3. Select whether you want to synchronize appliance name and/or synchronize mail relay.
4. 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 drop-down menu.
5. 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 <b>Time</b> drop-down menu. Then, select a day for the synchronization by clicking the <b>Calendar</b> button in the <b>Date</b> 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 the 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 synchronization. Last, specify a time of day.

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

### Appliance Replacement Considerations

Replacing an appliance should be done in such a way that no data is lost during the transition. Following these recommendations will help prevent data loss:

- 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.
- Hold onto the old appliance until you have retrieved all important data from the appliance's hard drive. Forensic data and other important data need to be backed up from the old appliance especially if you need the data for auditing purposes.
- You should install the new appliance on a lab network not connected to the LAN/WAN. Do not place the appliance on the WAN until you have restored the backed up configuration. The Sensors will connect to the appliance and your network tree will not be set up. Once connected to a lab network, you can either restore the primary's configuration file, or restore the configuration from a secondary appliance to the primary appliance. If the configuration is restored from the secondary appliance, you should then change the IP address of the new appliance to the one for the old appliance, reboot, and install the new appliance on the network.
- Once the new appliance is on the network, back up forensic data from the secondary appliance as required.
- ADSP restores the configuration long before the screen indicates that the process is complete. Executing a ping to the appliance will let you know exactly when the system is up. Once you receive a response, you can then log back in.

### 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.

Use the Account Access feature to:

- View current user information
- Add new users (**New User Account** button)
- Add new group accounts (**New Group Account** button)
- Edit user accounts (**Edit** link)
- Delete user accounts (**Delete** link)

- Synchronize user accounts (**Check Synchronization** button).

You must be a user with Admin privileges to use the Account Access feature. To access this feature, go to **Configuration > Operational Management > Account Access**.

The screenshot displays the 'Account Access' interface. At the top, there is a 'New Group Account' dropdown menu and a 'Check Synchronization' button. Below this is the 'Group Accounts' section, which includes 'More Up' and 'More Down' buttons. A table lists two group accounts:

Order	Group Name	Description	Group Permissions
1	Documentation	Document Development	Admin
2	Operations	Operation Center Members	Operation Center

Below the group accounts table are 'Apply' and 'Reset' buttons. The 'User Accounts' section is located below a horizontal separator. It contains a table with the following data:

User Name	Description	User Permissions
jjopalan (admin)	Development	Admin
FDeltrop (Ralf Deltrop)		Admin
nyuen (Admin)	Development	Admin
manager (Manager)	Development	Admin
cmeyer (Adcm Mayer)	Development	Admin
thight (Todd Nightingale)	Development	Admin
chill (Admin)	Development	Admin
jjosgue (admin)	Development	Admin
mcote (Admin)	Development	Admin
nyengati (admin)	Development	Admin

Information available is:

- Group account name (Group Name).
- User account name (User Name). The user's full name is displayed in parenthesis.
- Description of the account (Description).
- Role of the user in ADSP (User Permissions).

### ***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.



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

### ***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***

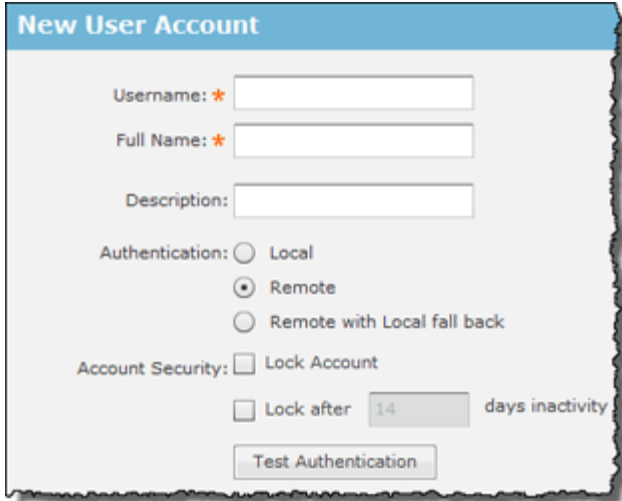
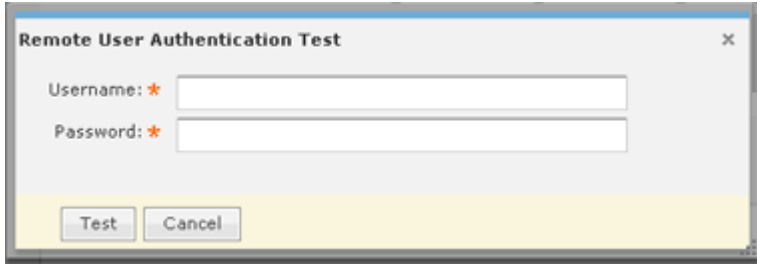
ADSP makes it easy to balance easy access to the system with a high level of system security and the ability to track the actions of users. Admin users can create numerous user accounts with varying levels of platform (system) access.

Click the **New User Account** button to access the **New User Account** overlay.

- ✓ **NOTE** The New User Account button is part of a multi-purpose button. Clicking the drop-down menu button displays a menu where you can select **New User Account** or **New Group Account**. The last option that you select becomes the button.

Use the following table to configure the user account:

Field	Description
Username	The account name of the user.
Full Name	Enter a formal name of the user, if desired.
Description	Enter a description of the user account, if desired.

Field	Description
Authentication	<p>Select <b>Local</b> if the user will use Local Authentication. Select <b>Remote</b> if the user will use Remote Authentication. Select <b>Remote with local fall back</b> if the user will use Remote Authentication with local fall back.</p> <p><b>Note:</b> At least one Administrator should be set to Local Authentication to avoid getting locked out of the system if a WLAN link is disconnected.</p> <p>When adding a remote user, <a href="#">Remote Authentication</a> must be set up first. Once Remote Authentication is set up, select the <b>Remote</b> radio button.</p>  <p>You can test remote user authentication using <b>Test Authentication</b> button.</p>  <p>Enter a user's username and password. Then, click the <b>Test</b> button. If the credentials are valid, you will receive a pass message. If the credentials are invalid, you will receive a failed message.</p>
New Password	<p>Enter a new password for the user.</p> <p><b>Note:</b> Password must include lowercase letters and uppercase letters. Password must be 6-32 characters in length. Password may not contain spaces or tabs.</p>
Verify Password	<p>Enter the new password again, to verify the password.</p>
Lock Account	<p>Check this checkbox if you want to lock the account.</p>
Lock after x days inactivity	<p>Check this checkbox if you want to lock the account after x amount of days of no use. Select the <b>Show Passwords</b> checkbox to reveal passwords.</p>
Change password at next logon	<p>Check this checkbox if you want to force the user to change password at the next logon. Select the <b>Show Passwords</b> checkbox to reveal passwords.</p>



Field	Description
Feature Permissions	<p>Limits users to specific functions within ADSP. Functional areas include:</p> <ul style="list-style-type: none"> <li>• Device Tuning</li> <li>• Alarm Management</li> <li>• Appliance Management</li> <li>• Alarm Criticality</li> <li>• Network Management</li> <li>• Threat Mitigation</li> <li>• System Configuration</li> <li>• Reporting</li> <li>• Analysis Tools</li> <li>• AP Test</li> <li>• Vulnerability Assessment</li> <li>• Connection Troubleshooting.</li> </ul> <p>You can apply a template or you can select individual functions for users to access. The following templates are available:</p> <ul style="list-style-type: none"> <li>• Admin—Gives users read/write permission to all functional areas.</li> <li>• Guest—Gives users read permission to Alarm Management, Reporting, Analysis Tools, and Connection Troubleshooting. No access is provided for the other functional areas.</li> <li>• Helpdesk—Gives users read/write permission to Connection Troubleshooting. No access is provided for all other function areas.</li> <li>• 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.</li> </ul>
Functional Roles	<p>Gives access to the following Functional Roles:</p> <ul style="list-style-type: none"> <li>• Security—Manage security alarms</li> <li>• Platform Monitoring—Manage the alarms that monitor the platform (system)</li> <li>• Locationing—Manage the alarms triggered by Location Based Services</li> <li>• Performance Monitoring and Troubleshooting—Manage the alarms that monitor platform (system) performance and alarms generated by troubleshooting features such as AP Test</li> <li>• Infrastructure Management—Manage the alarms dealing with infrastructure management</li> </ul> <p>Select the appropriate checkbox(es).</p>
Scope Permissions	<p>Limits user operations to a specific scope within the network with the highest level being the entire system. You can drill down to the lowest level and limit user operations to a specific floor within the network or anywhere in-between.</p>

Once you have configured the user options, click the **Save** button to save the user account. A message **The new User Account is created Successfully** is briefly displayed (top-right area of overlay) to confirm the account addition. ADSP will alert you to any errors. You can display more information about the error by clicking on the error message.

Click the **X** next to the **Save** button to close the **New User Account** overlay panel.

### **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***

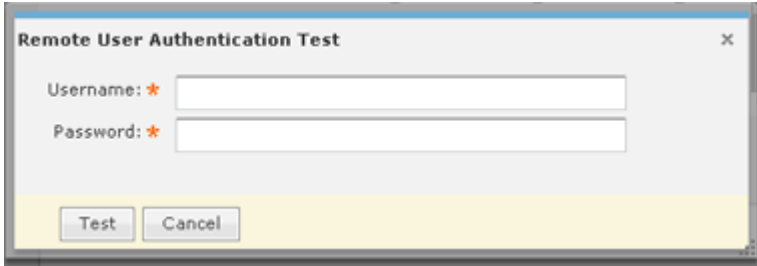
Group accounts involve a group of users set up through remote authentication (either LDAP or RADIUS). When a user attempts to log into ADSP that is a member of a group, ADSP first uses local authentication to log in the user. If the user is not part of local authentication, remote authentication is used. 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.

Click the **New Group Account** button to access the **New Group Account** overlay.



**NOTE** The **New Group Account** button is part of a multi-purpose button. Clicking the drop-down menu button displays a menu where you can select **New User Account** or **New Group Account**. The last option that you select becomes the button.

Use the following table to configure the user account:

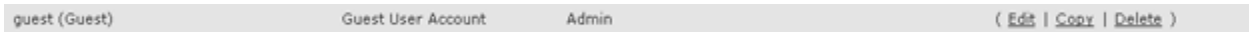
Field	Description
Group Name	Enter the name of the group account.
Description	Enter a description of the group account, if desired.
Disable group login	Disable the current login group.
Test Authentication	<p>Test remote user authentication using LDAP or RADIUS.</p>  <p>Enter a user's username and password. Then, click the <b>Test</b> button. If the credentials are valid, you will receive a pass message. If the credentials are invalid, you will receive a failed message.</p>
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.

Once you have configured the group options, click the Save button to save the group account. A message **The new Group Account is created Successfully** is briefly displayed (top-right area if overlay) to confirm the account addition. ADSP will alert you to any errors. You can display more information about the error by clicking on the error message.

Click the **X** in the top-right corner to close the **New Group Account** overlay panel.

**Copy, Delete, or Edit Accounts**

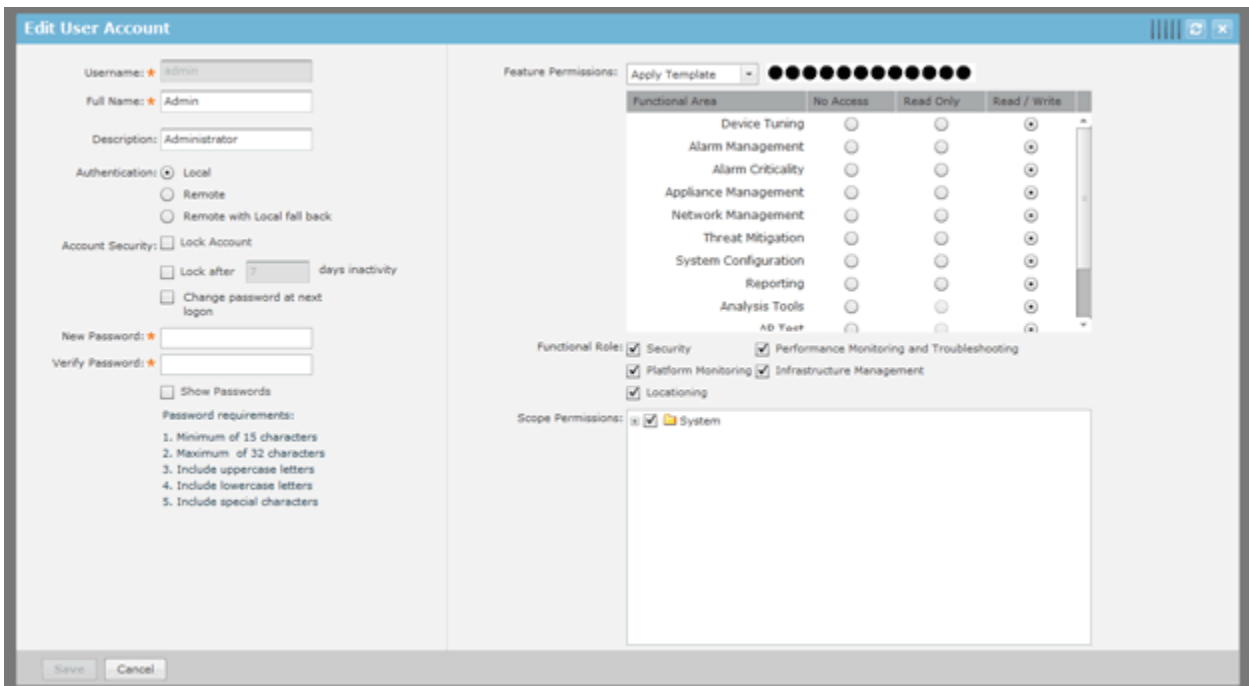
Roll over the account and click the copy link (shown below) to copy an account. Account information from the copied account is supplied when you copy an account.



To delete a group or user account, select (highlight) the account and then click the **Delete** link.

Click the **Edit** link to edit an account or double-click on the account. Account information is already supplied when you edit an account.

The screen shot shows the **Edit User Account** overlay. If the account is a group account, the **Edit Group Account** overlay will display. The fields are the same as when you create a new account.



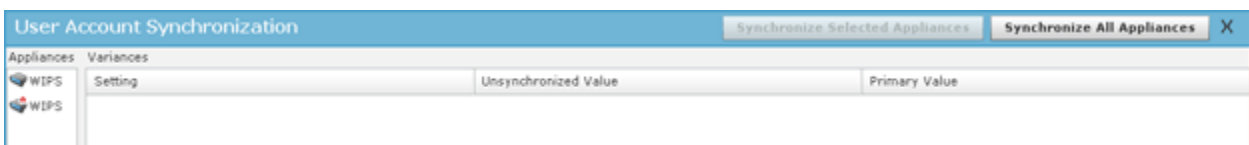
Once you have configured the user or group options, click the **Save** button to save the user/group account. ADSP will alert you to any errors. You can display more information about the error by clicking on the error message.

Click the **X** in the top-right corner to close the overlay panel.

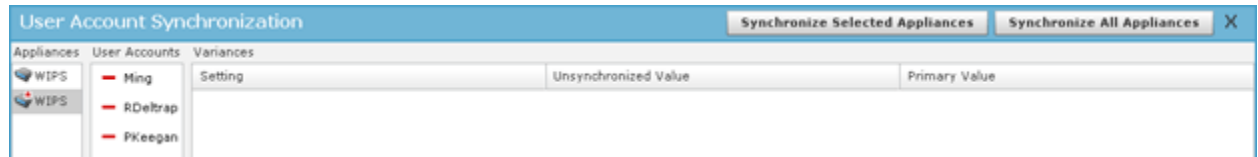
**Synchronize Accounts**

The **Check Synchronization** button is used to see if all accounts on all appliances in your system are in sync.

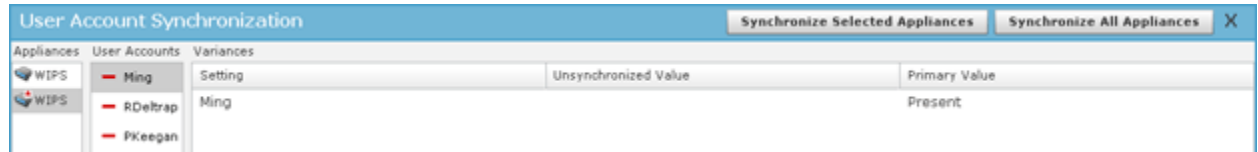
✓ **NOTE** You must have a Central Management license in order to use the Check Synchronization feature.



If an appliance is out of sync with the primary appliance, a red asterisk (\*) is displayed on the out of sync appliance. If you select (highlight) the out of sync appliance, a list of accounts are displayed that are out of sync on the selected appliance.



If you select (highlight) one of the user account, you will see the out of sync values.



Click the **Synchronize All Appliances** button to add the missing accounts to all appliances in your system. Click the **Synchronize Selected Appliances** to add the missing accounts to the selected appliance(s).

Click the **X** in the top, right corner to exit the **User Account Synchronization** overlay.

## Local Authentication

Local Authentication is used to authenticate users on the local appliance. It also allows you to manage password aging, password complexity, and account lockout criteria. To access this window, go to **Configuration > Operational Management > Local Authentication**.

Field	Description
Max Login Attempts	The maximum amount of login attempts before a user is locked out of an account. You must also specify if the account is locked within a time limit or no time limit.
Password must be changed after x days	The number of days a password can be used before it expires. Once expired, users are required to change passwords.
High complexity password required	If checked, users are required to use a highly complex password when creating passwords.

After setting up the Local Authentication, click the **Apply** button to save the configuration. Click the **Reset** button to discard any changes and revert back to the previous settings.

The **Check Synchronization** button is used to check all appliances in the network to ensure they are using the same Local Authentication. (The synchronization features works basically the same way wherever the feature is implemented. Synchronizing Accounts has a good example of how the synchronization feature works.)

✓ **NOTE** You must have a Central Management license in order to use the Check Synchronization feature.

Click the **X** in the top, right corner to exit the **Local Authentication Synchronization** overlay.

## Password Reset

Password Reset is used to change the password of the current user. To change the information for other users, you must access **Account Access** under **Configuration > Operational Management**. You must be a user with the role of Admin to edit User Accounts. To access **Password Reset**, go to **Configuration > Operational Management > Password Reset**.

The screenshot shows a web form titled "Password Reset". It contains three text input fields stacked vertically. The first field is labeled "Old Password:", the second is labeled "New Password:", and the third is labeled "Verify Password:". Each field is a simple rectangular box with a light gray border.

Field	Description
Old Password	Enter your current password here.
New Password	Enter your new user password here.
Verify Password	Enter your new password here again.

After entering your password information, click the **Apply** button to save your changes. Click the **Reset** button to discard any changes.

## Remote Authentication

Remote Authentication is used to authenticate users by using the password stored on a RADIUS or LDAP server. This reduces the cost of managing different passwords across different systems and avoids replication of password data throughout multiple databases. To access this feature, go to **Configuration > Operational Management > Remote Authentication**.

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.

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

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

To get started, click the **New** button. Remote Authentication fields are displayed so that you can set up Remote Authentication.

**Remote Authentication** [New] [Move Up] [Move Down] [Delete]

New\_Auth\_Source

Name:

Type:

LDAP  LDAPS

LDAP Server:

LDAP Port:

User Prefix:  (Example: "CN=")

User Suffix:  (Example: "DN=mycompany, DC=com")

Use LDAP for external group based authentication

? **LDAP basics**

Contact your LDAP administrator - be sure to follow your organization's protocol.

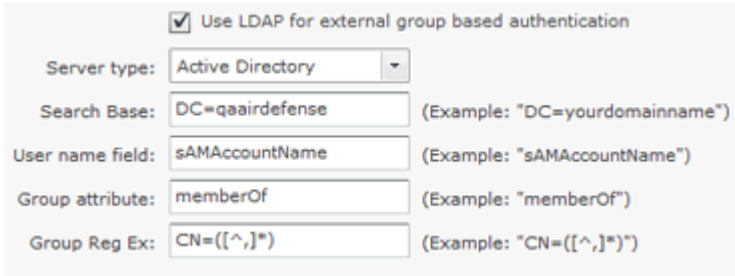
**Prefix** is added to the username to form the user distinguished name (DN).

**Suffix** is a DN that identifies the top entry in a locally held directory hierarchy. There is no requirement that you use a suffix.

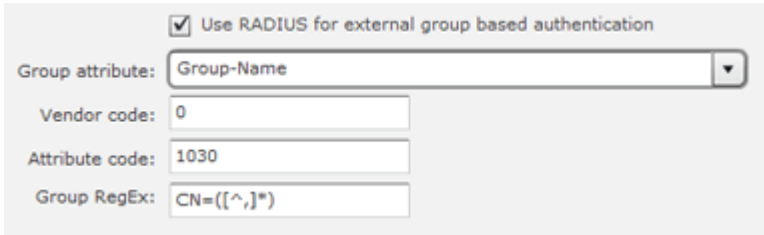
✓ **NOTE** If you encounter problems, contact your LDAP administrator. He/she can advise you on how to fill in the fields. If you can, use an LDAP browser (<http://www.ldapadministrator.com/download.htm>) to login and browse. This will allow you to test your settings to see if they are right. There should also be errors in the LDAP server log that give more details on the problem.

Use the following table to enter data into the fields:

Field	Description
Name	Enter a configuration name.
Type	Select a server type from the drop-down menu: LDAP or RADIUS.
Protocol	Select a protocol type by clicking the appropriate radio button: <b>LDAP</b> or <b>LDAPS</b> . If the using a RADIUS server, the protocol type is selected from a drop-down menu. The options are <b>PAP</b> , <b>CHAP</b> , <b>MSCHAP</b> , or <b>MSCHAPv2</b> .
LDAP Server	Enter the IP Address of the LDAP server. This option only displays for LDAP servers.
RADIUS Server	Enter the IP Address of the RADIUS server. This option only displays for RADIUS servers.
LDAP Port	Enter the authorization server port number. This option only displays for LDAP servers.
RADIUS Port	Enter the authorization server port number. This option only displays for RADIUS servers.
Shared Secret	Enter the shared secret password for the RADIUS server. You can make passwords viewable by selecting the <b>Display Passwords</b> checkbox. This option only displays for RADIUS servers.
Timeout	Enter a timeout value for authentication. This option only displays for RADIUS servers.

Field	Description
Retries	Enter the number of times to retry authentication. This option only displays for RADIUS servers.
User Prefix	Enter the name of the windows domain for the server (e.g., qaairdefense\). <b>User Prefix</b> is optional. You can leave this field blank or you can supply a prefix ending in a backslash (\) or a double backslash (\\). You may have to experiment to see which option is valid for you.
User Suffix	Enter the Internet domain name for the server (e.g., motorola.com). <b>User Suffix</b> is optional. You can leave this field blank or you can supply a suffix.
Use LDAP for ...	<p>This field is displayed if <b>LDAP</b> is chosen for the <b>Type</b> field. Select this checkbox if you are using external group based authentication. If checked, more fields are displayed.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Search Base—Enter a string to find your domain name in the directory. Normally, the string is DC=yourdomainname. The <b>Search Base</b> field should be the same as the <b>User Prefix</b> field without any backslashes.</li> <li>• User field name—Enter a string to find your user name in the directory. Normally, the string is sAMAccountName.</li> <li>• Group attribute—Enter a string to find your group name in the directory. Normally, the string is memberOf.</li> <li>• 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=[^,]*).</li> </ul> <p>If the LDAP administrator changes any of the strings from what is normally used, he/she must inform you of the string to use.</p> <p>Example:</p>  <p>The screenshot shows a configuration window with the following fields and values:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Use LDAP for external group based authentication</li> <li>Server type: Active Directory (dropdown menu)</li> <li>Search Base: DC=qaairdefense (Example: "DC=yourdomainname")</li> <li>User name field: sAMAccountName (Example: "sAMAccountName")</li> <li>Group attribute: memberOf (Example: "memberOf")</li> <li>Group Reg Ex: CN=[^,]* (Example: "CN=[^,]*")</li> </ul>



Field	Description
Use RADIUS for ...	<p>This field is displayed if <b>RADIUS</b> is chosen for the <b>Type</b> field. Select this checkbox if you are using external group based authentication. If checked, more options are displayed.</p> <ul style="list-style-type: none"> <li>Group attribute—Displays a list of attributes to identify a group to ADSP. When an attribute is selected, values are inserted into the <b>Vendor code</b>, <b>Attribute code</b> and <b>Group RegEx</b> fields for ADSP to use in group identification. You should not change any of the inserted values.</li> </ul> <p>Example:</p> 

After the entering the Remote Authentication data, click the **Apply** button to save the configuration. The configuration name is now displayed in the list on your left. If you highlight (click) a name in the list you can edit the fields for that configuration. You may also delete any highlighted configuration by clicking the **Delete** button. You can change the order of configuration preference using the **Move Up** or **Move Down** button.

You can test your Remote Authentication configuration using the **Test Authentication** button for user accounts or group accounts. For help using this button, see [Creating and Changing User Accounts](#) or [Creating and Changing Group Accounts](#).

The **Check Synchronization** button is used to check all appliances in the network to ensure they are using the same Remote Authentication. (The synchronization features works basically the same way wherever the feature is implemented. [Synchronize Accounts](#) has a good example of how the synchronization feature works.)



**NOTE** You must have a Central Management license in order to use the Check Synchronization feature.

Click the **X** in the top, right corner to exit the **Remote Authentication Synchronization** overlay.

## 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**.

After defining your preferences, click the **Apply** button to save your changes. Click the **Reset** button to discard any changes.

### Default View

Select the default view when logging into ADSP. The following views are available:

- Dashboard tab
- Network tab
- Alarms tab
- Configuration tab.

### 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 deselected.

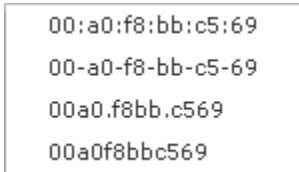
When viewing devices in the **Network** tab, the row of any device that is considered inactive will have lighter text than active devices.

### ***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 server. Select the **Use a proxy to access the server** checkbox, then enter the IP address and port number of the server. If authentication is required to access the server, select the **Proxy requires authentication** checkbox, then supply the **Username** and **Password**.

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 username and password.

### *Network New Column Preferences*

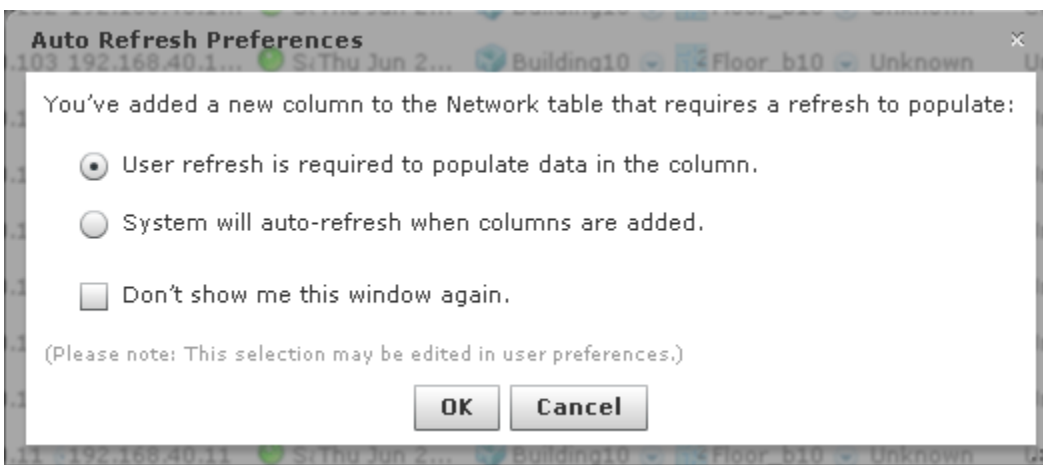


**NOTE** This feature operates only on columns affected by a system refresh (the **Sensor, AP, Associated Clients, Associated BSS, Adopted APs, Severity, Floor, and Scope** columns). Columns displaying only device information that does not change are not affected.

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.

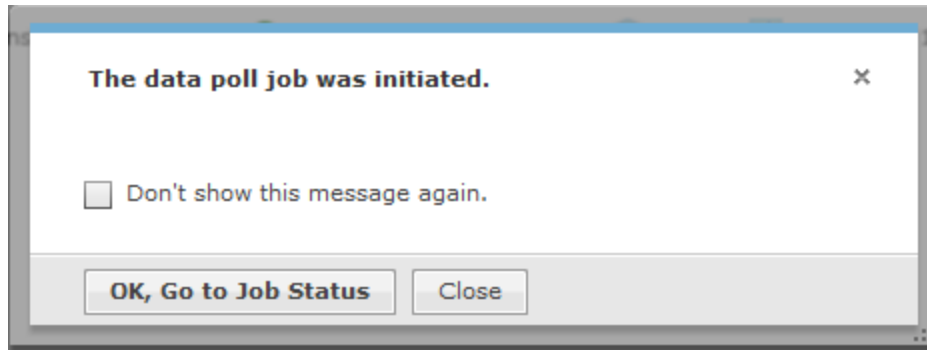


Click **OK** to save your changes.

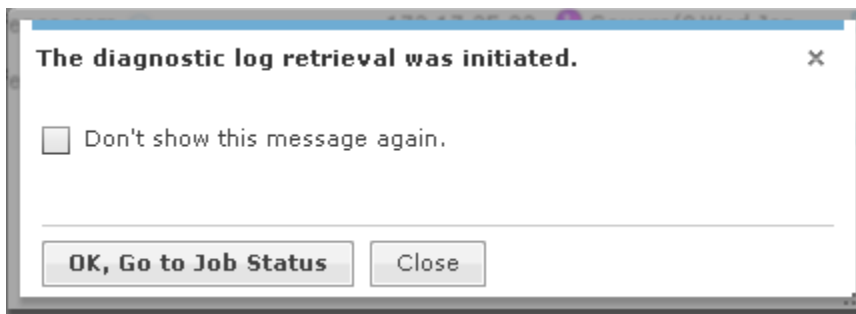
### *Show Job Initiation Message Dialogs*

You have option of displaying a message dialog when initiating certain jobs. The different options are:

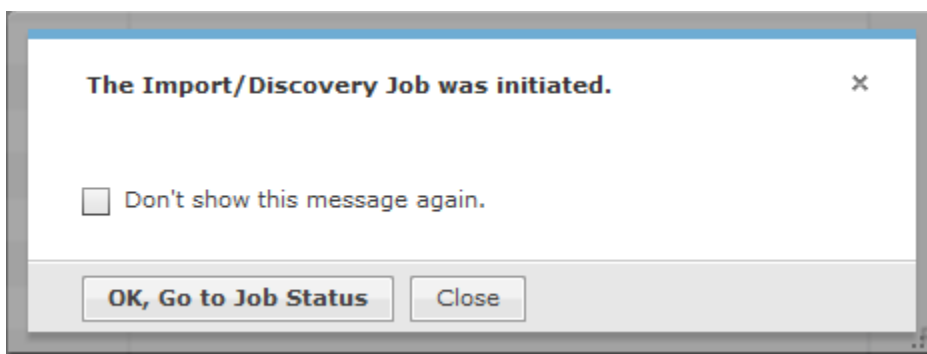
- Show Data Poll Job Initiation Message Dialog—Displays the following dialog window when a data poll is manually initiated:



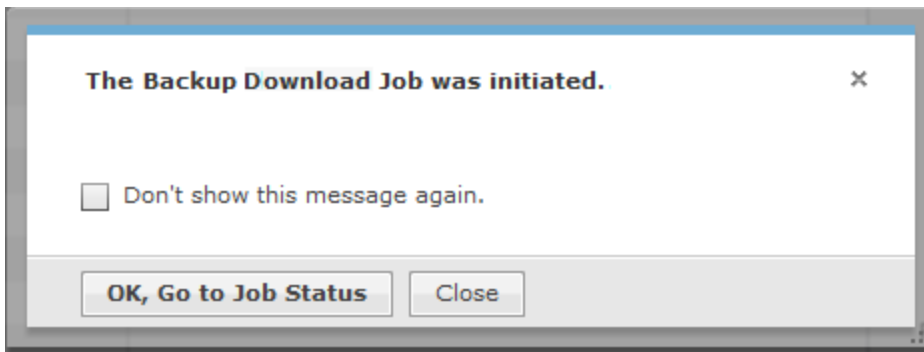
- Show Diagnostic Logs Job Initiation Message Dialog—Displays the following dialog window when manually retrieving the diagnostic log:



- Show Import/Discovery Job Initiation Message Dialog—Displays the following dialog window when an import/discover device is manually initiated:



- Show Backup Download Job Initiation Message Dialog—Displays the following dialog window when a backup download job is manually initiated:



In all four cases, you are given the option of not showing the message again. You can also view the job status by clicking the **OK, Go to Job Status** button, or by navigating to **Configuration > Operational Management > Job Status** if you wish to view the job status later.

Type	Description	User	Status	Start Time	Finish Time	Progress
Data Poll	On Demand Data Poll	ccollier	Polled 1 devices	Tue May 15 2012 02...	Tue May 15 2012 02...	1/1
Device Configuration	On Demand Log Retri...	ccollier	Complete: successful	Tue May 15 2012 10...	Tue May 15 2012 10...	1/1
Data Poll	On Demand Data Poll	ccollier	Polled 1 devices	Tue May 15 2012 10...	Tue May 15 2012 10...	1/1
SNMP Discovery	New Scheduled Impor	ccollier	Polled 3 devices	Mon May 14 2012 0...	Mon May 14 2012 0...	3/3

## Automatic Configuration of WLAN Infrastructure Devices

ADSP provides two methods of automatically configuring WLAN infrastructure devices:

- Auto-Connect—Used with APs installed with WiNG 5.3 firmware or later. This is the preferred method.
- Zero Touch—Used with devices installed with firmware older than WiNG 5.3.

### Auto-Connect Feature

- ✓ **NOTE** The Auto-Connect feature only works with AP devices. Switches with radios are **NOT** supported.

The Auto-Connect feature is specifically designed to get un-configured APs into ADSP as Sensors. After a successful DNS lookup, the un-configured AP attaches to ADSP. ADSP must then have the correct RF-domain setting for the final placement location of the newly added AP and a Sensor-only policy configured before it will automatically re-configure the AP device to work as a Sensor.

There are three conditions that must be met before auto-connection will start:

- The AP must have the default password set
- The AP must have the radio set to the default setting
- The AP can not be adopted to any controller.

If these conditions are met, Auto-Connect will start a DNS lookup for airdefense1 or airdefense2 after five minutes from booting up into a running state. It goes with out saying that for this feature to work the network that the AP is connected to must have DHCP and a DNS server with at least the airdefense1 name configured.

## Zero Touch WLAN Infrastructure Deployment

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_contrack_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:  Hours

Enable automatic data collection  
Frequency:  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**

Encrypt Passwords and Keys on Flash

Enable Password:   Display Passwords

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**

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.

### Configuration Examples

Examples are provided to demonstrate:

- How to configure an AP-7131 which can be used to configure other Motorola devices and initially set up the WIPS portion of ADSP.
- How to configure a CISCO device.
- How variables are affected if you set up a CLI profile and then make changes to the CLI in a device's properties.
- How custom CLI variables affect a Custom CLI.

#### AP-7131 Example

- ✓ **NOTE** You must configure the Appliance Platform before configuring Infrastructure Management.

For this example, a Motorola AP-7131 and a static IP address are used.

1. Collect all the passwords for the AP-7131 to be managed.
2. Enable SSH/Telnet if it is not enabled on the AP-7131.
3. Make sure that you have a supported TFTP or FTP server set up so that both the ADSP and the managed AP-7131 can reach it. ADSP recommends FTP:IIS Win2k and TFTP 3C Daemon. Both methods have to allow for overwriting the configuration file because when a configuration is changed, the server creates a new file with the same name and will again push it to the relay server.
4. Enable SNMP on the device and verify that you can execute **snmpwalk** from the server. You will need the IP address and community string for the AP-7131. To verify SNMP connectivity, from the server, run the following command against your target device: **snmpwalk -v2c -c <community string> <IP Addr>**.
5. Add a CLI profile using the default Motorola AP7131 device type (or other device type) as a template and apply the profile to the floor the device is located on.
  - a. Go to **Configuration** -> **Infrastructure Management** -> **CLI Configuration**.
  - b. Select **Motorola WiNG v5.x** from the **CLI Configuration** drop-down menu.
  - c. Select a floor for the device.
    - ✓ **NOTE** The floor should already exist. If it does not, use tree setup to create it (**Configuration** > **Appliance Platform** > **Tree Setup**).
  - d. Select **Override settings**.
  - e. Select your newly created profile by clicking its radio button.

- ✓ **NOTE** If your profile is the only available profile, it will be selected automatically.

- f. Click **Apply**.

Since the profile is incomplete right now, the system will not apply it. Only complete profiles are delivered to the device. So, in this example, the full set of profiles will not be applied until the very last step. When Device Access and Communication Settings are configured and have a valid relay server set up and running, the profile will be applied. The *device-mgmt.log* file in */usr/local/smx/log* can be used to verify what is going on.

6. Create a Channels profile and apply it to the floor the AP-7131 is placed on as follows:

✓ **NOTE** ADSP automatically sets up a default Channels profile. Only follow these steps, if you want to use your own settings.

- a. Go to **Configuration > Infrastructure Management > Channel Settings**.
- b. Select the floor.
- c. Select **Override settings**.
- d. Select the proper settings.
- e. Click **Apply**.

7. Configure Device Access as follows:

- a. Go to **Configuration > Infrastructure Management > Device Access**.
- b. Select the floor.
- c. Select **Override settings**.
- d. Enter the User ID and Password.
- e. Go to the **Interfaces** tab.
- f. Enable SSH.
- g. Enable SNMP and enter passwords for the Read/Write community. Then, enter password for a Trap Destination including your server IP address.

✓ **NOTE** You must also add the Trap Community and destination to get traps on your server. This can be done from the server CLI: **ADSPadmin > Config > SNMP – Enable**.

- h. Click **Apply**.

8. Ensure that the device firmware is current. (**Configuration > Infrastructure Management > Device Firmware**). If firmware is not current, update it.

9. Create a Radio Settings configuration for the AP-7131 and apply it to the floor the device is placed. You must include some data rates.

✓ **NOTE** ADSP automatically sets up a default Radio Settings profile. Only follow these steps, if you want to use your own settings.

- a. Go to **Configuration > Infrastructure Management > Radio Settings**.
- b. Select the floor.
- c. Select **Override settings**.
- d. Select the proper settings.
- e. Click **Apply**.

10. Configure RF-Domain and apply to Access Point by selecting the scope where the floor the AP-7131 is placed as follows:

- a. Go to **Configuration > Infrastructure Management > RF-Domain**.
  - b. Select the floor.
  - c. Select **Override settings**.
  - d. Enter RF-Domain information.
  - e. Click **Apply**.
11. Create WLAN profile and apply it by associating the profile with the location that contains the managed device.
- a. Go to **Configuration > Infrastructure Management > WLAN Profiles**.
  - b. Click **New Profile**.
  - c. Enter information for the WLAN Profile in the **General** and **Security** tabs.
  - d. Click **OK**.
  - e. Ensure that the appliance is selected in the network tree and select **Enable configuration**.
  - f. Select the floor.
  - g. Select **Override settings**.
  - h. Select the WLAN Profile.
  - i. Click **Apply**.

The profile is now complete but ADSP cannot communicate with the AP-7131.

12. If you have not already done so during the Platform configuration, import the AP-7131 into your network using SNMP discovery using a single IP address. This can be done with **Configuration > Appliance Platform > Import/Discover Devices**.

✓ **NOTE** Select SNMP discovery with a target folder of a floor created in the Appliance Platform configuration. You can use the Device Import Rules or manually select the floor.

13. Set automatic status polling and automatic data collection for 3 minutes, and turn on automatic configuration correction (**Configuration > Appliance Platform > Polling**).
14. If necessary, configure the Communication Settings so that ADSP can communicate with the AP-7131. HTTP is only used for Airwave and WLSE devices so this is not needed for the AP-7131. In the **General** tab, enable data collection and enable configuration. For **SNMP**, set version to v2c with proper read/write community information. Under **Console** tab, add the same user you have for device access and enable password information so that ADSP can talk to the Access Point. Now ADSP can communicate with the AP-7131.
- a. Go to **Configuration > Appliance Platform > Communication Settings**.
  - b. Select the floor.
  - c. Select **Override settings**.
  - d. Enter SNMP information.
  - e. Enter Console information.
  - f. Click **Apply**.

15. Verify that changes made to your applicable profiles are now being pushed out to the AP-7131. The relay server should have a copy of the rendered profile and it should match what is on the AP-7131.
- A simple test to verify changes are being pushed to the AP-7131 is to change the WLAN profile that is applied to the AP. This change will be immediately pushed if everything is working.
  - A console connection can be used to watch the profile being pushed to the AP-7131.
  - Checking the relay server ftp/tftp root directory will allow you to look at the configuration that is rendered and pushed to the AP-7131.
  - Looking at the in /usr/local/smx/log/device-mgmt.log, you can watch as the server configures the AP-7131.
  - Alarms will be present if the configuration is incomplete.
  - Alarms will be present if the Relay server cannot be reached.

Changes are pushed immediately to the AP-7131 in the following circumstances:

- The Access Point is managed already and something in its profile changes.
- The Access Point is moved to another location that is configured.

Changes are **NOT** pushed when a device is discovered; this will happen during polling.

### CISCO Device Example

✓ **NOTE** You must configure the Appliance Platform before configuring Infrastructure Management.

For this example, a CISCO device and a static IP address are used.

1. This is critical for Cisco AP ADSP Management. Validate supported firmware: Cisco 1230 Thick AP – 12.3.8-JEC2(ED) or Cisco 1130 Thick AP – 12.4-10b(JDA).
2. Collect all the passwords on the device to be managed. For example, for a Cisco device, you need the enable password and a login.
3. Enable SSH/Telnet if it is not enabled on the Cisco device.
4. Make sure that Cisco devices have at least a RSA modulus of 768 bits or higher or your server will not talk to it via SSH.
5. Make sure that you have a supported TFTP or FTP server set up so that both the ADSP and the managed device can reach it. ADSP recommends FTP:IIS Win2k and TFTP 3C Daemon. Both methods have to allow for overwriting the configuration file because when a configuration is changed, the server creates a new file with the same name and will again push it to the relay server.
6. Enable SNMP on the device and verify that you can execute **snmpwalk** from the server. You will need the IP address and community string for the device. To verify SNMP connectivity, from the server, run the following command against your target device: **snmpwalk -v2c -c <community string> <IP Addr>**.
7. ADD a CLI profile using the default Cisco Autonomous 12x0/11x0 device type (or other device type) as a template.
  - a. Go to **Configuration -> Infrastructure Management -> CLI Configuration**.
  - b. Select **Cisco Autonomous 12x01/11x0** from the **CLI Configuration** drop-down menu.
  - c. Click the **New Profile** button.
  - d. Enter a name for your profile.
  - e. Update the CLI commands, if necessary.
  - f. Click **OK**. Your newly created profile should now be available in the list of profiles.

- g. Select a floor for the device.

✓ **NOTE** The floor should already exist. If it does not, use tree setup to create it (**Configuration > Appliance Platform > Tree Setup**).

- h. Select **Override settings**.

- i. Select your newly created profile by clicking its radio button.

✓ **NOTE** If your profile is the only available profile, it will be selected automatically.

- j. Click **Apply**.

Since the profile is incomplete right now, the system will not apply it. Only complete profiles are delivered to the device. So, in this example, the full set of profiles will not be applied until the very last step. When Device Access and Communication Settings are configured and have a valid relay server set up and running, the profile will be applied. The *device-mgmt.log* file in */usr/local/smx/log* can be used to verify what is going on.

- 8. Create a Channels profile and apply it to the floor the device is placed as follows:

- a. Go to **Configuration > Infrastructure Management > Channel Settings**.
- b. Select the floor.
- c. Select **Override settings**.
- d. Select the proper settings.
- e. Click **Apply**.

- 9. Configure Device Access as follows:

- a. Go to **Configuration > Infrastructure Management > Device Access**.
- b. Select the floor.
- c. Select **Override settings**.
- d. Enter the enable password for Cisco (Cisco).
- e. Enter the User ID (Cisco) and Password (Cisco).
- f. Go to the **Interfaces** tab.
- g. Enable SSH.
- h. Enable SNMP and enter passwords for the Read/Write community. Then, enter password for a Trap Destination including your server IP address.

✓ **NOTE** You must also add the Trap Community and destination to get traps on your server. This can be done from the server CLI: **ADSPadmin > Config > SNMP – Enable**.

- i. Click **Apply**.

- 10. Ensure that the device firmware is current. (**Configuration > Infrastructure Management > Device Firmware**). If firmware is not current, update it.

- 11. Create a Radio Settings configuration for the device and apply it to the floor the device is placed. You must include some data rates.

- a. Go to **Configuration > Infrastructure Management > Radio Settings**.
- b. Select the floor.
- c. Select **Override settings**.



- d. Select the proper settings.
  - e. Click **Apply**.
12. Configure RF-Domain and apply to Access Point by selecting the scope where the floor the Access Point is placed on as follows:
- a. Go to **Configuration > Infrastructure Management > RF-Domain**.
  - b. Select the floor.
  - c. Select **Override settings**.
  - d. Enter RF-Domain information.
  - e. Click **Apply**.
13. Create WLAN profile and apply it by associating the profile with the location that contains the managed device.
- a. Go to **Configuration > Infrastructure Management > WLAN Profiles**.
  - b. Click **New Profile**.
  - c. Enter information for the WLAN Profile in the **General** and **Security** tabs.
  - d. Click **OK**.
  - e. Ensure that the appliance is selected in the network tree and select **Enable configuration**.
  - f. Select the floor.
  - g. Select **Override settings**.
  - h. Select the WLAN Profile.
  - i. Click **Apply**.

The profile is now complete but ADSP cannot communicate with the Cisco device.

14. If you have not already done so during the Appliance Platform configuration, import the device into your network using SNMP discovery using a single IP address. This can be done with **Configuration > Appliance Platform > Import/Discover Devices**.

✓ **NOTE** Select SNMP discovery with a target folder of a floor created in the Appliance Platform configuration. You can use the Device Import Rules or manually select the floor.

15. Set automatic status polling and automatic data collection for 3 minutes, and turn on automatic configuration correction (**Configuration > Appliance Platform > Polling**).
16. If necessary, configure the Communication Settings so what ADSP can communicate with the device. HTTP is only used for Airwave and WLSE devices so this is not needed for Cisco devices. On the **General** tab, enable data collection and enable configuration. For **SNMP**, set version to v2c with proper read/write community information. Under **Console** tab, add the same user you have for device access and enable password information so that ADSP can talk to the Access Point. Now ADSP can communicate with the Access Point.
- a. Go to **Configuration > Appliance Platform > Communication Settings**.
  - b. Select the floor.
  - c. Select **Override settings**.
  - d. Enter SNMP information.
  - e. Enter Console information.
  - f. Click **Apply**.

17. Verify that changes made to your applicable profiles are now being pushed out to the Cisco device. The relay server should have a copy of the rendered profile and it should match what is on the Cisco device.
  - A simple test to verify changes are being pushed to the Access Point is to change the WLAN profile that is applied to the AP. This change will be immediately pushed if everything is working.
  - A console connection can be used to watch the profile being pushed to the AP.
  - Checking the relay server ftp/tftp root directory will allow you to look at the configuration that is rendered and pushed to the device.
  - Looking at `/usr/local/smx/log/device-mgmt.log`, you can watch as the server configures the device.
  - Alarms will be present if the configuration is incomplete.
  - Alarms will be present if the Relay server cannot be reached.

Changes are pushed immediately to the device in the following circumstances:

- The device is managed already and something in its profile changes.
- The device is moved to another location that is configured.

Changes are **NOT** pushed when a device is discovered; this will happen during polling.

### CLI Variable Scenarios

When making changes to CLI on a device the following occurs:

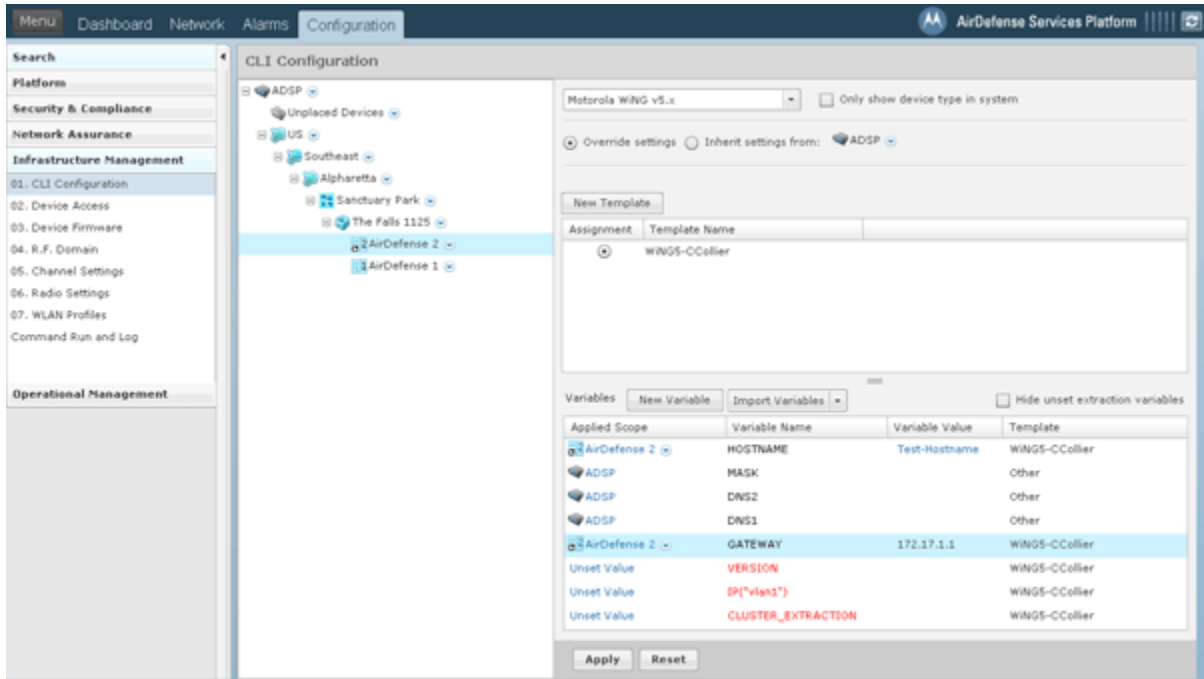
- If the value for the variable is an empty string (no spaces, new lines, tabs, text, anything), then the variable is not saved for the CLI Variable Profile.
- If the variable value is populated, it will be saved.

When sending variables to the device or displaying variables in the GUI, the CLI Profile variables and CLIVars Profile variables are merged (with CLIVars Profile variables taking precedence).

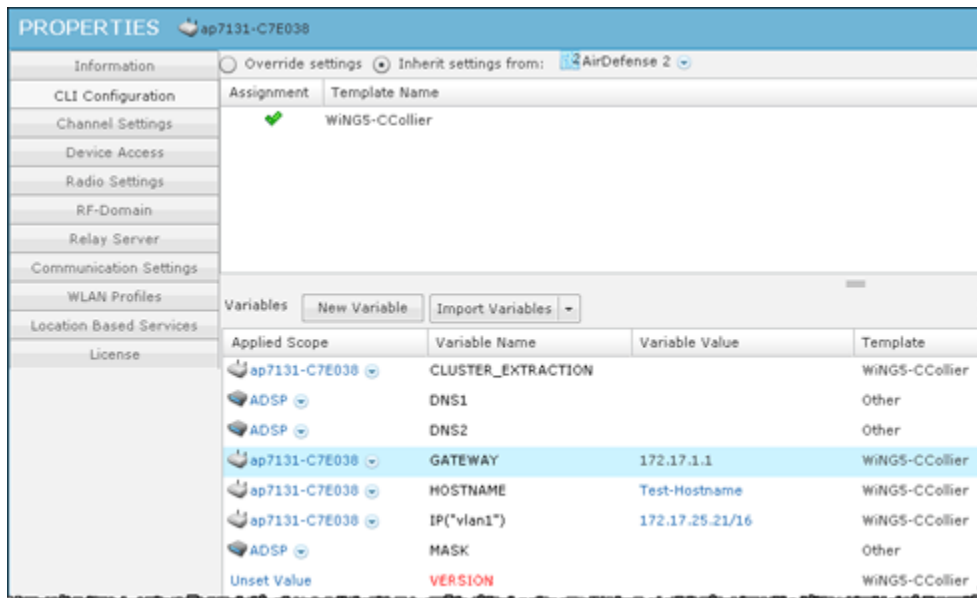
*Scenario A*

ProfileX is defined at the folder level as follows:

1. HOSTNAME=Test-Hostname
2. GATEWAY=172.17.1.1



If the properties page of a device that inherits this folder level is accessed, the defined variables are displayed from the folder level. In this case, the CLI profile (ProfileX) is not merged with the CLIVars Profile since there is no CLIVars.



The result of this scenario is that these settings are defined at the CLI Profile level and inherited straight from their definition at the folder level.

**Scenario B**

ProfileX is defined at the folder level but modified at the device level (override a named profile) or (inherit profile but edit variables) as follows:

1. Information is inherited from ProfileX.
  - a. HOSTNAME=Test-Hostname
  - b. GATEWAY=172.17.1.1
2. Make some changes.
  - a. HOSTNAME=TestDevice
  - b. GATEWAY is cleared to null

Applied Scope	Variable Name	Variable Value	Template
ap7131-C7E038	CLUSTER_EXTRACTION		WINGS-CCollier
ADSP	DNS1		Other
ADSP	DNS2		Other
ap7131-C7E038	GATEWAY	TestDevice	WINGS-CCollier
ap7131-C7E038	HOSTNAME	TestDevice	WINGS-CCollier
ap7131-C7E038	IP("vlan1")	172.17.25.21/16	WINGS-CCollier
ADSP	MASK		Other
Unset Value	VERSION		WINGS-CCollier

After the modification, the variables that are not null (empty string) are saved and applied at the device level. In this case, the CLI Profile (ProfileX) is merged with the CLIVars which yields the following results:

- a. a.HOSTNAME=TestDevice

## b. GATEWAY=172.17.1.1

Applied Scope	Variable Name	Variable Value	Template
ap7131-C7E038	CLUSTER_EXTRACTION		WINGS-CCollier
ADSP	DNS1		Other
ADSP	DNS2		Other
ap7131-C7E038	GATEWAY	172.17.1.1	WINGS-CCollier
ap7131-C7E038	HOSTNAME	TestDevice	WINGS-CCollier
ap7131-C7E038	IP("vlan1")	172.17.25.21/16	WINGS-CCollier
ADSP	MASK		Other
Unset Value	VERSION		WINGS-CCollier

The result of this combination will result in the HOSTNAME coming from the CLIVars and the GATEWAY coming from the CLI Profile (ProfileX)

### Scenario C

ProfileX and ProfileY are defined at the folder level but modified at the device level (override a named profile) or (inherit profile but edit variables) as follows:

1. Information is inherited from ProfileX.
  - a. HOSTNAME=Test-Hostname
  - b. GATEWAY=172.17.1.1
2. Set override and make some changes.
  - a. HOSTNAME=TestB-Hostname

## b. GATEWAY is cleared to null

The screenshot shows the 'PROPERTIES' page for device 'ap7131-C7E038'. The 'Override settings' radio button is selected, and the 'Variables' table is displayed below. The 'GATEWAY' variable is highlighted in blue and has the value 'Unset Value'.

Applied Scope	Variable Name	Variable Value	Template
ap7131-C7E038	CLUSTER_EXTRACTION		WINGS-CCollier
ADSP	DNS1		Other
ADSP	DNS2		Other
ap7131-C7E038	GATEWAY	Unset Value	WINGS-CCollier
ap7131-C7E038	HOSTNAME	TestB-Hostname	WINGS-CCollier
ap7131-C7E038	IP("vlan1")	172.17.25.21/16	WINGS-CCollier
ADSP	MASK		Other
Unset Value	VERSION		WINGS-CCollier

3. Save changes.

4. Now set back to inherit either ProfileX or ProfileY (any other profile).

The screenshot shows the 'PROPERTIES' page for device 'ap7131-C7E038'. The 'Inherit settings from' radio button is selected, and the 'Variables' table is displayed below. The 'GATEWAY' variable is highlighted in blue and has the value '172.17.1.1'.

Applied Scope	Variable Name	Variable Value	Template
ap7131-C7E038	CLUSTER_EXTRACTION		WINGS-CCollier
ADSP	DNS1		Other
ADSP	DNS2		Other
ap7131-C7E038	GATEWAY	172.17.1.1	WINGS-CCollier
ap7131-C7E038	HOSTNAME	TestB-Hostname	WINGS-CCollier
ap7131-C7E038	IP("vlan1")	172.17.25.21/16	WINGS-CCollier
ADSP	MASK		Other
Unset Value	VERSION		WINGS-CCollier

In this case (as in Scenario B), these values were set at the device level. Override was removed and the device was set to inherit again. You might expect Step 2 of this example to be reset to Step 1. This is not the case. You would have to clear the settings in the variables section for this to happen; otherwise, the variables section would always change to the values of the inherited profile (X or Y).

## Custom CLI Example

This example shows how to use custom CLI variables.

- ✓ **NOTE** Customization of device values from ADSP requires expert knowledge of what each configuration parameter does and how making changes to those values will affect the device being modified.

The following conditions are assumed:

- A non-default CISCO VLAN configuration is used.
- A Cisco 1230 AP is managed and connected to a licensed ADSP server and the user accessing the configuration has all required permissions. It also implies that the user has a good working understanding of how device configuration is achieved in ADSP.
- VLAN configuration for a Cisco 1230 CLI profile can be modified using a variable defined by the user. ADSP provides for this action through custom variable notation for use inside a CLI profile. The variable notation is in the format that follows: \${variablename}.

The following steps lead you through the basic steps required:

1. First you must create a custom variable and use it in a CLI profile. For this example, define the variable \${CustomVLAN}.
2. By inserting this variable into a CLI profile, you are able to match the non-default setting in the WLAN Profile.

The screenshot shows the 'WLAN Profiles Settings' dialog box with the 'General' tab selected. The 'Name' field contains '1230Only', 'Description' is empty, and 'SSID' is 'Cisco1230\_VLAN'. Under 'Protocol', 'a n (2.4 GHz)' and 'g' are checked. The 'VLAN' field contains the number '7' and is circled in red. A red arrow points from the text 'The VLAN variable must match the value set here.' to the 'VLAN' field. Other fields include 'Association Limit' (3), 'Station Timeout' (10 seconds), and several 'Other Options' checkboxes: 'Respond to all probe requests' (checked), 'Broadcast SSID in Beacon' (unchecked), 'Wireless Client Isolation' (checked), and 'Locally Bridged' (unchecked). 'Save' and 'Cancel' buttons are at the bottom.

3. The following screen shot shows how it is used:
  - a. The variable \${CustomVLAN} is inserted directly into the CLI profile that is applied to a device.

- b. When `#[CustomVLAN]` is first entered into the profile, it becomes available for use in the **Variables** section as CustomVLAN. This is where you enter the custom VLAN value.

CLI Profile: Cisco Autonomous 12x0/11x0

Name: Cisco1230-Custom

Device Type: Autonomous 12x0/11x0

Reboot and write configuration updates to startup config (if available)

Do not reboot, instead write configuration updates to running config

```
bridge irb
${DEVICEACCESS_RFDOMAIN_EXPANSION}
${WLAN_RADIO_CHANNEL_EXPANSION}
interface Dot11Radio0.#[CustomVLAN]
encapsulation dot1Q #[CustomVLAN] native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
```

Assigned Profile

- Cisco1130-CCollier
- Cisco1230-Custom

Variables defined for AirDefense 2

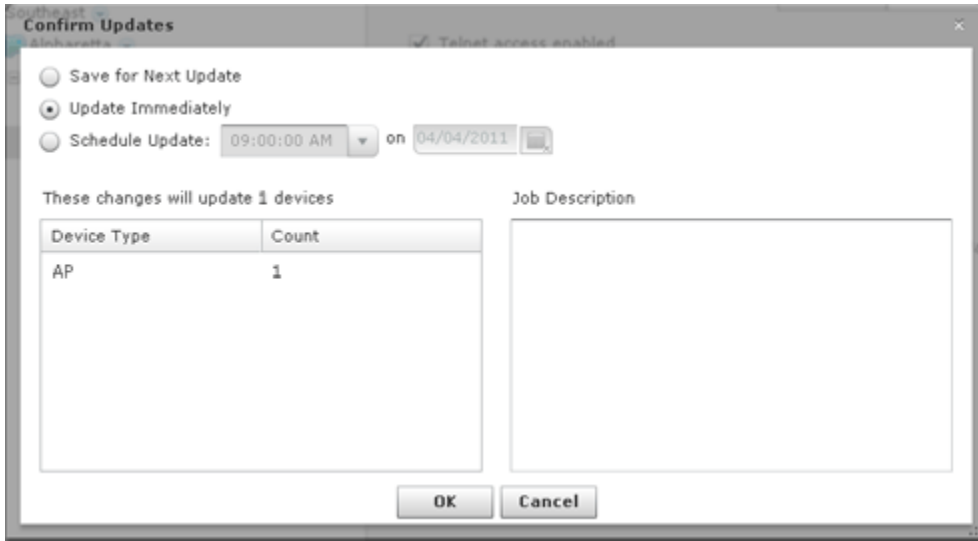
Status	Name	Default Value
ADSP	MASK	
ADSP	DNS2	
ADSP	DNS1	
ADSP	GATEWAY	
Removed	VERSION	
Removed	DOMAINNAME	
Overridden	CustomVLAN	7

After the variable is added directly into the profile, it displays as a variable that can have values. For this example, the VLAN variable is 7.

- c. To complete this VLAN customization example for the Cisco 1230 AP, the following modifications need to be made:
- interface Dot11Radio0.#[CustomVLAN]
  - encapsulation dot1Q #[CustomVLAN] native
  - interface Dot11Radio1.#[CustomVLAN]
  - encapsulation dot1Q #[CustomVLAN] native
  - interface FastEthernet0.#[CustomVLAN]
  - encapsulation dot1Q #[CustomVLAN] native



- When you apply the values in the custom CLI configuration, they are applied to the configured device.




- As with all customizations, you should test it in a lab environment before putting it into production.

### Configuration Notes

WS2000 Upgrades

ADSP 9.x WS2000 upgrade will only occur if the relay server is accessible from subnet1.

## Drop-down Menus


Drop-down menus are conveniently accessible for devices and network levels throughout AirDefense Services Platform. They provide functions that users can access by clicking the drop-down menu button——associated with a device or network level. The functions operated on a single device or group of devices in the network level.

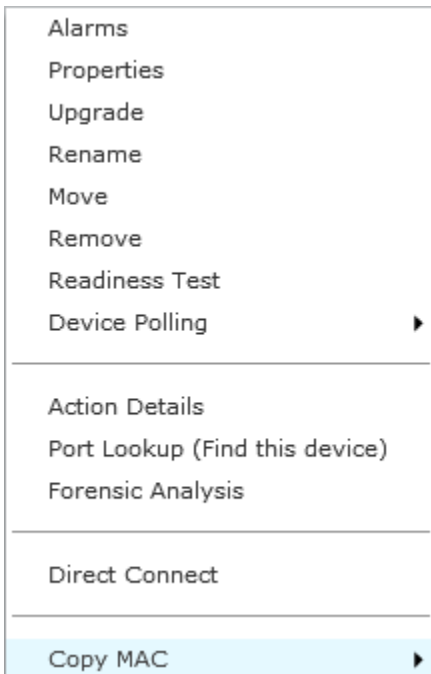
### Devices

Drop-down menus for devices contain functions that operate on a single device or multiple devices. These drop-down menus are available throughout AirDefense Service Platform. The devices are:

- Access Points
- BSS
- Wireless Client
- Sensors
- Wireless Switch
- Wired Switch
- Unknown Devices
- WLSE
- AirWave.

### Access Point


The Access Points drop-down menu contains functions that you can apply to the selected Access Point. Click the drop-down menu button——next to the Access Point name to display the drop-down menu.

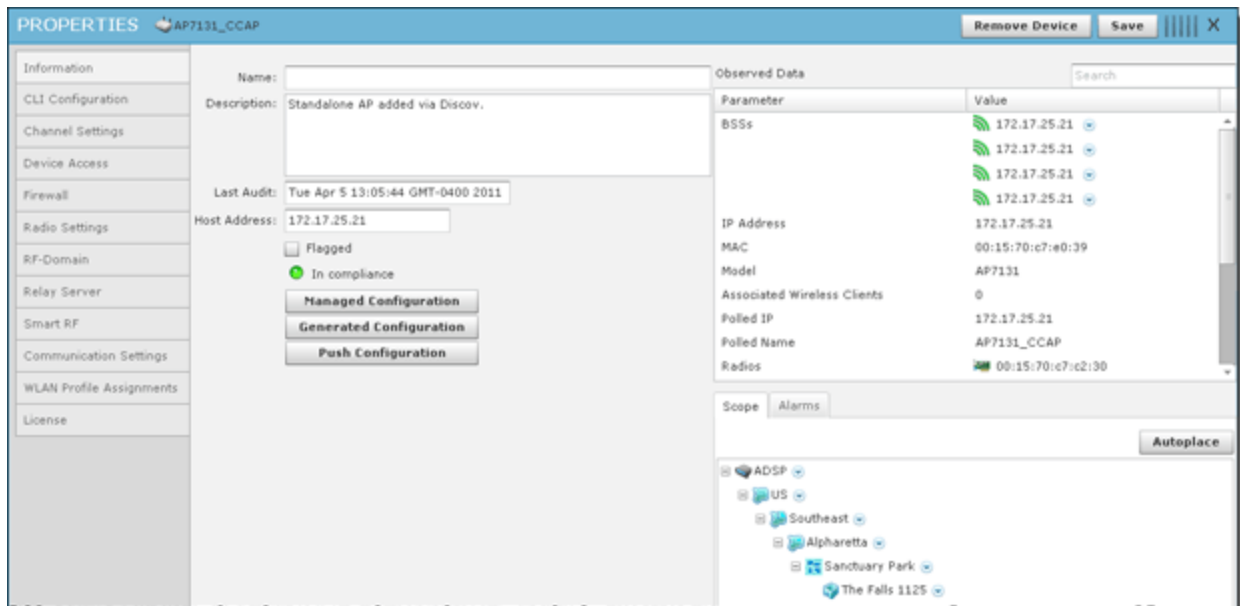


The drop-down menu for Access Points contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Access Point.
Properties	Opens the <b>Properties</b> overlay for the selected Access Point.
Upgrade	Upgrades the firmware for the selected Access Point. (See <a href="#">Upgrade Devices</a> for more information.)
Rename	Opens a dialog window to rename the selected Access Point.
Move	Moves the selected Access Point to another network level (floor). (See <a href="#">Move Devices</a> for more information.)
Remove	Removes the selected Access Point from your network. (See <a href="#">Remove Devices</a> for more information.)
Readiness Test	Validates that the AP is management ready (that is, it can be managed through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected Access Point. (See <a href="#">Audit Devices</a> for more information.)
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 <a href="#">Forensic Analysis</a> 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.

### Properties

You can view the properties of an Access Point by clicking the drop-down menu button——and clicking **Properties**.



The screenshot displays the 'PROPERTIES' window for an Access Point (AP7131\_CCAP). The window is divided into several sections:

- Left Panel:** A vertical list of configuration categories including Information, CLI Configuration, Channel Settings, Device Access, Firewall, Radio Settings, RF-Domain, Relay Server, Smart RF, Communication Settings, WLAN Profile Assignments, and License.
- Central Form:** Contains fields for Name, Description (Standalone AP added via Discov.), Last Audit (Tue Apr 5 13:05:44 GMT-0400 2011), and Host Address (172.17.25.21). It also includes a 'Flagged' checkbox and a green 'In compliance' indicator. Below these are buttons for 'Managed Configuration', 'Generated Configuration', and 'Push Configuration'.
- Observed Data Table:** A table with columns for Parameter and Value. It lists:
  - BSSs: 172.17.25.21 (repeated four times)
  - IP Address: 172.17.25.21
  - MAC: 00:15:70:c7:e0:39
  - Model: AP7131
  - Associated Wireless Clients: 0
  - Polled IP: 172.17.25.21
  - Polled Name: AP7131\_CCAP
  - Radios: 00:15:70:c7:c2:30
- Bottom Panel:** A network tree view showing a hierarchy: ADSP > US > Southeast > Alpharetta > Sanctuary Park > The Falls 1125. An 'Autoplace' button is visible.

The following information is displayed:

Field	Description
Name	The name of the Access Point.
Description	A description of the Access Point.
Last Audit	The date and time of the last audit.
Host Address	IP address of the Access Point.
Flagged	Flag an Access Point that you want to bring attention to.
In compliance / Not in compliance	Status of the last compliance audit. Click the <b>Managed Configuration</b> button to display the Access Point configuration. Click the <b>Generated Configuration</b> button to display a generated configuration for a device. The generated configuration is the same configuration sent to a relay server to configure a device. Click the <b>Push Configuration</b> button to push the existing configuration out to the Access Point.
Observed Data	Data that AirDefense Services Platform observed about the Access Point. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the Access Point is shown under the **Scope** tab. The **Autoplace** button can be used to place the Access Point in a network folder using Auto-Placement Rules.

Alarms related to the Access Point are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

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

- [CLI Configuration](#)
- [Channel Settings](#)
- [Device Access](#)
- [Radio Settings](#)
- [RF-Domain](#)
- [Relay Server](#)
- [Communication Settings](#)
- [WLAN Profiles](#) Assignments
- License—Display valid licenses for Access Point.


These configuration settings (or profiles) are all located in the [Configuration](#) tab.

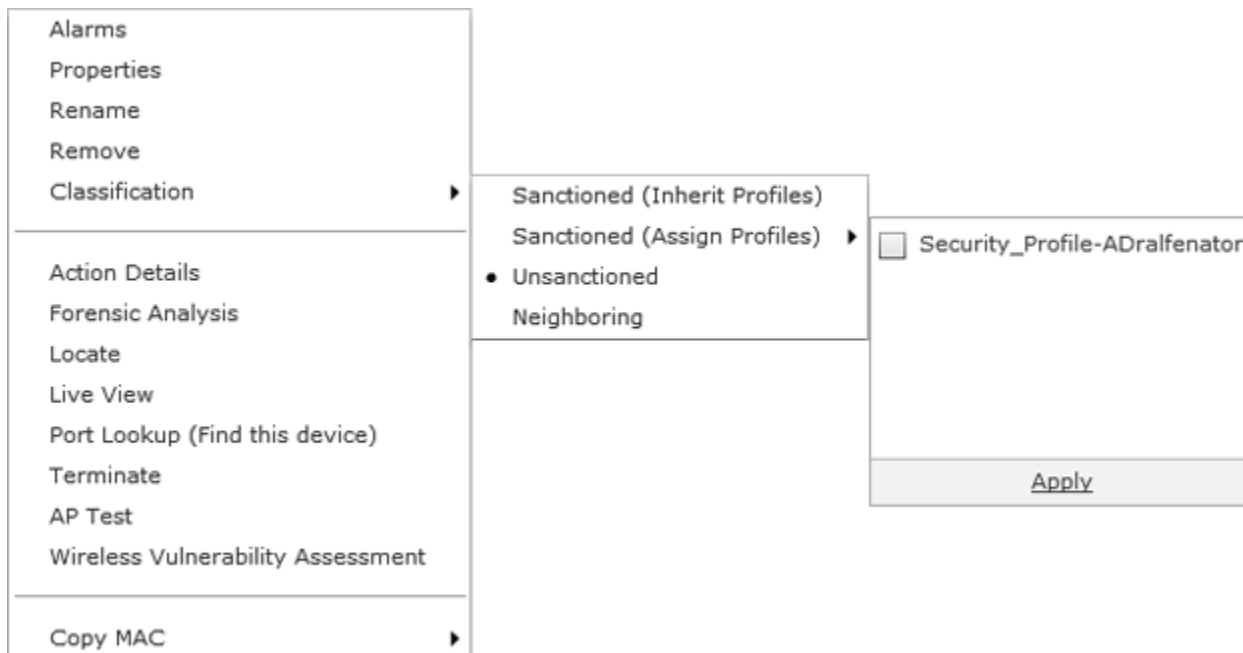
If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to remove a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

## BSS

The BSS drop-down menu contains functions that you can apply to the selected BSS. Click the drop-down menu button— next to the BSS name to display the drop-down menu.




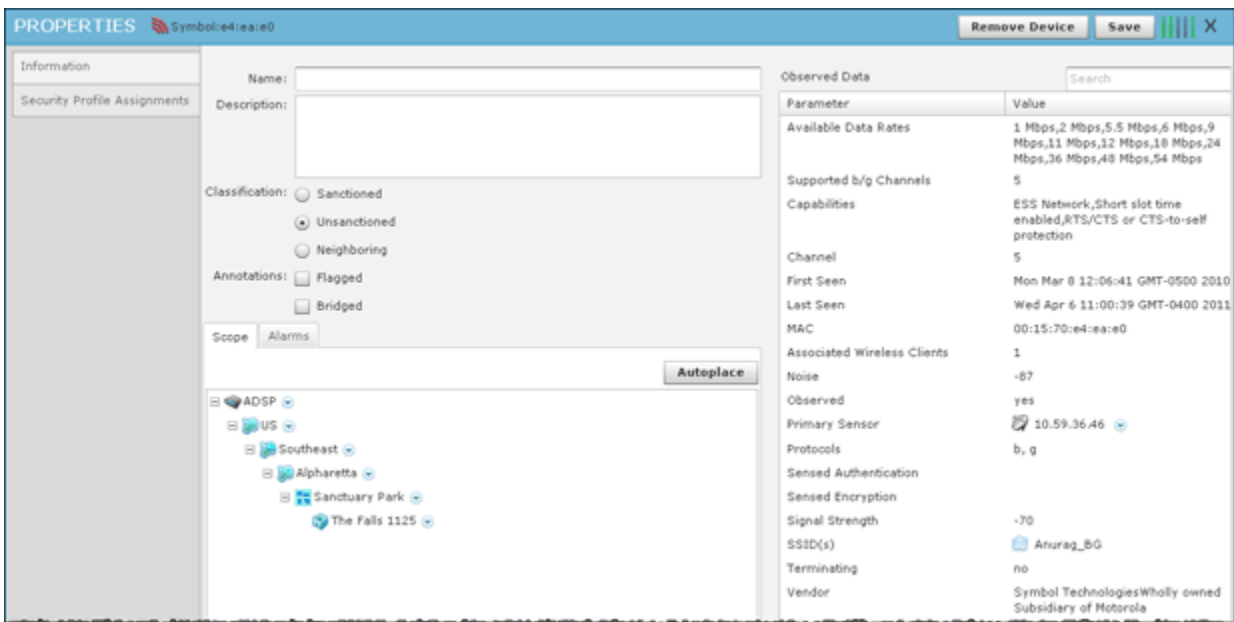
The drop-down menu for BSSs contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected BSS.
Properties	Opens the <b>Properties</b> overlay for the selected BSS.
Rename	Opens a dialog window to rename the selected BSS.
Remove	Removes the selected BSS from your network. (See <a href="#">Remove Devices</a> for more information.)
Classification	Classifies the BSS using one of the following classifications: <ul style="list-style-type: none"> <li>Sanctioned (inherit)—Classify the selected BSS as a sanctioned device that inherits its traits from wherever its location in the network tree.</li> <li>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 <b>Apply</b> link.</li> <li>Unsanctioned—Classify the selected BSS as unsanctioned.</li> <li>Neighboring—Classify the selected BSS as a neighboring device.</li> </ul>
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Forensic Analysis	Opens the <a href="#">Forensic Analysis</a> window for the specified BSS.

Function	Description
Locate	Opens the device Location tracking window so that you can quickly locate the selected BSS.
Live View	Opens the <a href="#">Live View</a> 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. (See <a href="#">Scheduled AP Test</a> for more information.)
Wireless Vulnerability Assessment	Opens the Vulnerability Assessment window so that you can scan your wireless network for vulnerabilities. (See <a href="#">On-Demand Assessment</a> for more information.)
Copy MAC	Copies the MAC address of the selected BSS for later use.

### Properties

You can view the properties of a BSS by clicking the drop-down menu button— and clicking **Properties**.



Parameter	Value
Available Data Rates	1 Mbps,2 Mbps,5.5 Mbps,6 Mbps,9 Mbps,11 Mbps,12 Mbps,18 Mbps,24 Mbps,36 Mbps,48 Mbps,54 Mbps
Supported b/g Channels	5
Capabilities	ESS Network,Short slot time enabled,RTS/CTS or CTS-to-self protection
Channel	5
First Seen	Mon Mar 8 12:06:41 GMT-0500 2010
Last Seen	Wed Apr 6 11:00:39 GMT-0400 2011
MAC	00:15:70:e4:ea:e0
Associated Wireless Clients	1
Noise	-87
Observed	yes
Primary Sensor	10.59.36.46
Protocols	b, g
Sensed Authentication	
Sensed Encryption	
Signal Strength	-70
SSID(s)	Anuraq_BG
Terminating	no
Vendor	Symbol Technologies Wholly owned Subsidiary of Motorola

The following information is displayed:

Field	Description
Name	The name of the BSS.
Description	A description of the BSS.

Field	Description
Classification	The classification of the BSS: <b>Sanctioned</b> , <b>Unsanctioned</b> , or <b>Neighboring</b> .
Annotations	The annotations specified for the BSS: <b>Flagged</b> or <b>Bridged</b> .
Observed Data	Data that AirDefense Services Platform observed about the BSS. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the BSS is shown under the **Scope** tab. The **Autoplace** button can be used to place the BSS in a network folder using Auto-Placement Rules.

Alarms related to the BSS are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

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

- [Security Profiles](#) Assignments.


This configuration profile is located in the [Configuration](#) tab.

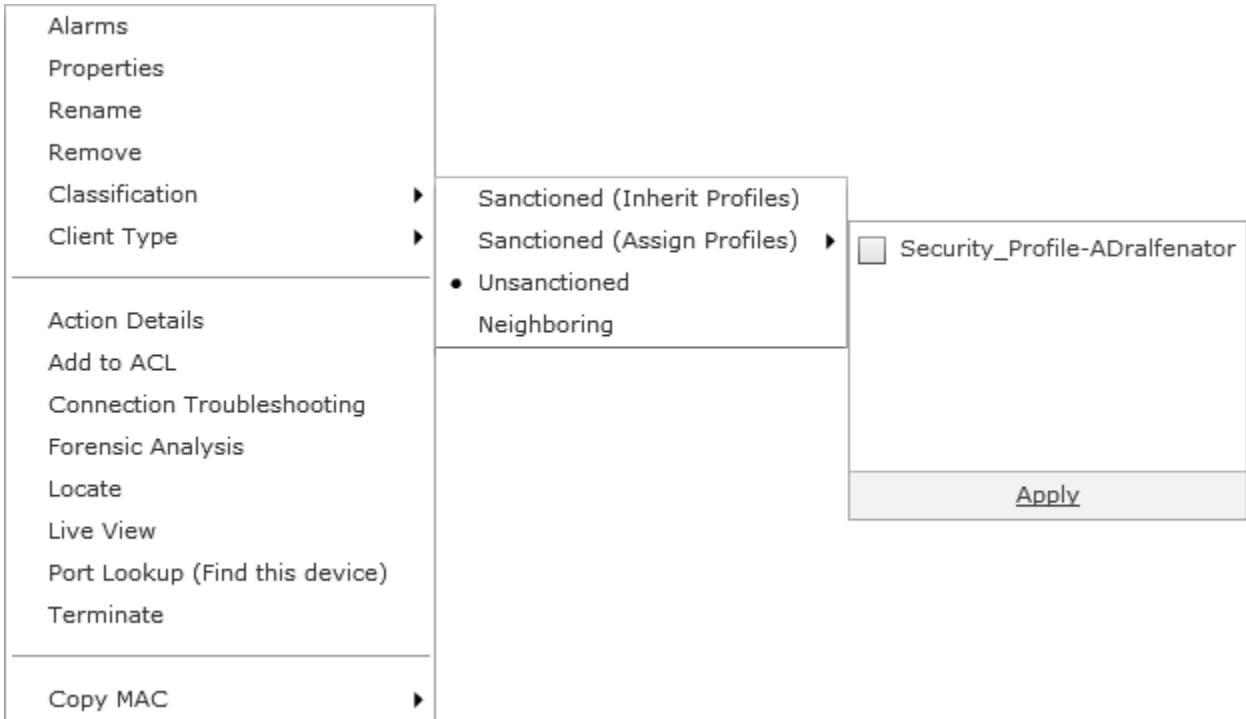
If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

## Wireless Clients











The Wireless Client drop-down menu contains functions that you can apply to the selected Wireless Client. Click the drop-down menu button——next to the Wireless Client name to display the drop-down menu.



The drop-down menu for Wireless Clients contains the following functions:


Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Wireless Client.
Properties	Opens the <b>Properties</b> 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"> <li>Sanctioned (inherit)—Classify the selected Wireless Client as a sanctioned device that inherits its traits from wherever its location in the network tree.</li> <li>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 <b>Apply</b> link.</li> <li>Unsanctioned—Classify the selected Wireless Client as unsanctioned.</li> <li>Neighboring—Classify the selected Wireless Client as a neighboring device.</li> </ul>

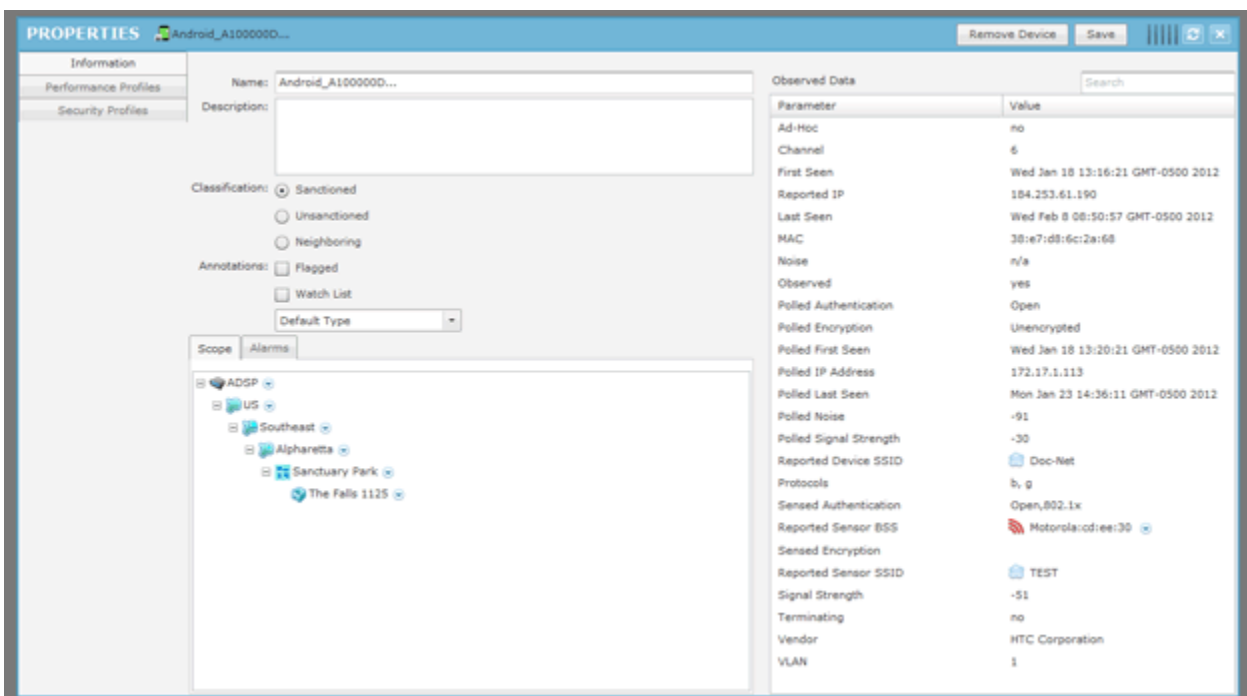


Function	Description
Client Type	<p>Client Type appears in the menu only when a Wireless Client is sanctioned. As default, Wireless Clients are assumed to be laptops, displaying a laptop icon. This menu item allows you to differentiate phones and handheld devices from laptops in ADSP.</p> <ul style="list-style-type: none"> <li>• Employee Personal Device—</li> <li>• Guest Wi-Fi User—</li> <li>• In Store Customer—</li> <li>• Laptop—</li> <li>• Loyalty Customer—</li> <li>• Phone—</li> <li>• Potential Customer—</li> <li>• Scanner—</li> <li>• Tablet—</li> <li>• Uncategorized Device—</li> </ul> <div data-bbox="511 1045 1334 1470" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Client Type ▸</p> <ul style="list-style-type: none"> <li>Employee Personal Device</li> <li>Guest Wi-Fi User</li> <li>In Store Customer</li> <li>Laptop</li> <li>Loyalty Customer</li> <li>Phone</li> <li>Potential Customer</li> <li>Scanner</li> <li>Tablet</li> <li>• Uncategorized Device</li> </ul> </div> <ul style="list-style-type: none"> <li>• Select the appropriate device to represent a Wireless Client and use its icon for the selected Wireless Client throughout the GUI.</li> </ul>
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).
Connection Troubleshooting	Opens <a href="#">Connection Troubleshooting</a> so that you can troubleshoots a Wireless Client's ability to connect to your wireless network.
Forensic Analysis	Opens the <a href="#">Forensic Analysis</a> window for the specified Wireless Client.
Locate	Opens the Floor Plan and adds the Wireless Client to the Location Tracking list so that you can quickly locate the selected Wireless Client.

Function	Description
Live View	Opens the <a href="#">Live View</a> 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. (See <a href="#">Terminate</a> for more information.)
Copy MAC	Copies the MAC address of the selected Wireless Client for later use.

### Properties

You can view the properties of a Wireless Client by clicking the drop-down menu button— and clicking **Properties**.



The following information is displayed:

Field	Description
Name	The name of the Wireless Client.
Description	A description of the Wireless Client.
Classification	The classification of the Wireless Client: <b>Sanctioned</b> , <b>Unsanctioned</b> , or <b>Neighboring</b> .
Annotations	The annotations specified for the Wireless Client: <b>Flagged</b> or <b>Watch List</b> . If the Wireless Client is a sanctioned device, a drop-down menu is added where you can designate the Wireless Client as one of the Client Types discussed previously.
Observed Data	Data that AirDefense Services Platform observed about the Wireless Client. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the Wireless Client is shown under the **Scope** tab.

Alarms related to the Wireless Client are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

You can view and/or override a Wireless Client's configuration by selecting:

- [Performance Profiles](#)
- [Security Profiles.](#)


These configuration settings (or profiles) are all located in the [Configuration](#) tab.

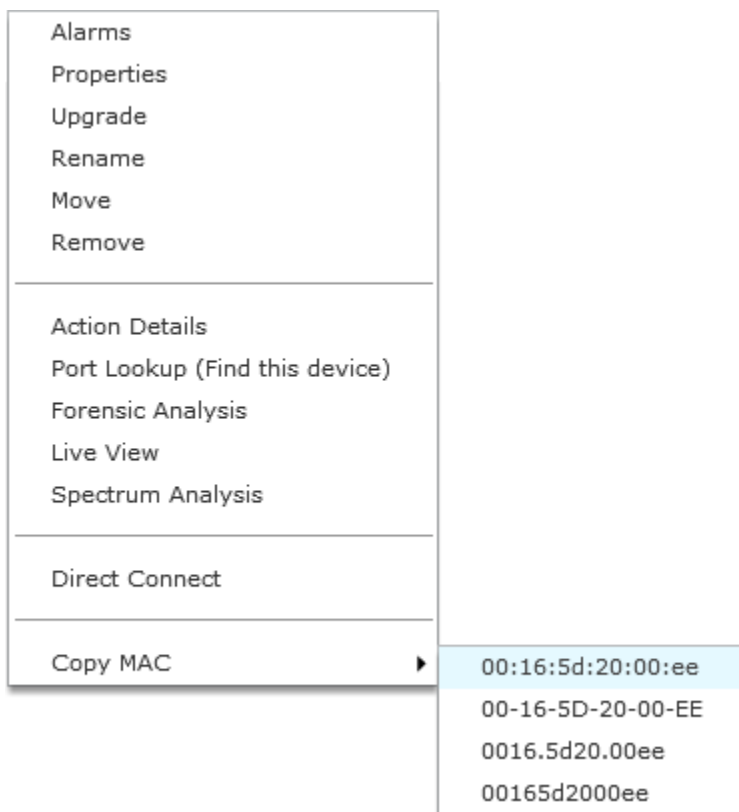
If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

## Sensor

The Sensors drop-down menu contains functions that you can apply to the selected Sensor. Click the drop-down menu button— next to the Sensor name to display the drop-down menu.




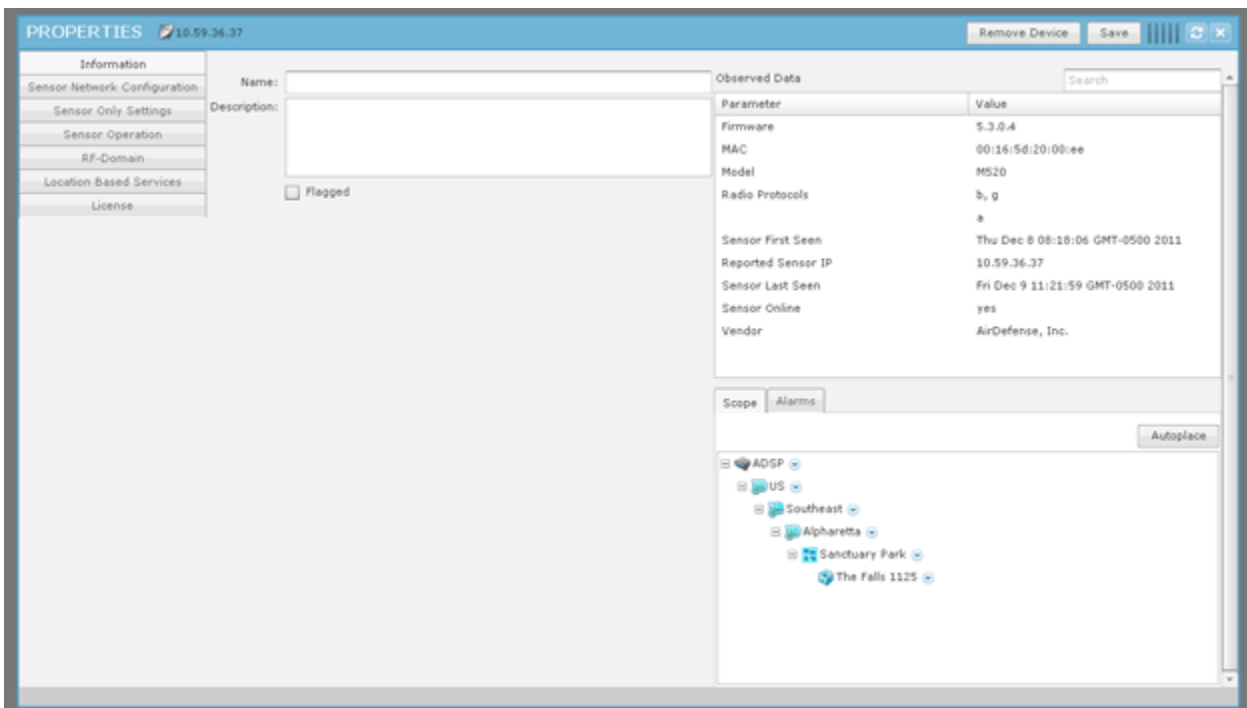
The drop-down menu for Sensors contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Sensor.
Properties	Opens the <b>Properties</b> overlay for the selected Sensor.
Upgrade	Upgrades the firmware for the selected Sensor. (See <a href="#">Upgrade Devices</a> for more information.)

Function	Description
Rename	Opens a dialog window to rename the selected Sensor.
Move	Moves the selected Sensor to another network level (floor). (See <a href="#">Move Devices</a> for more information.)
Remove	Removes the selected Sensor from your network. (See <a href="#">Remove Devices</a> for more information.)
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 <a href="#">Forensic Analysis</a> window for the specified Sensor.
Live View	Opens the <a href="#">Live View</a> window for the selected Sensor; allows you to analyze current WLAN activity on the device.
Spectrum Analysis	Accesses Spectrum View to identify and locate interference sources on your wireless network. (See <a href="#">Spectrum Analysis</a> for more information.)
Direct Connect	Accesses the user interface (UI) for the selected Sensor.
Copy MAC	Copies the MAC address of the selected Sensor for later use.

### Properties

You can view the properties of a Sensor by clicking the drop-down menu button— and clicking **Properties**.



The following information is displayed:

Field	Description
Name	The name of the Sensor.
Description	A description of the Sensor.
Host Address	The IP address of the host.
Flagged	Flag a Sensor that you want to bring attention to.
Observed Data	Data that AirDefense Services Platform observed about the Sensor. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the Sensor is shown under the **Scope** tab. The **Autoplace** button can be used to place the Sensor in a network folder using Auto-Placement Rules.

Alarms related to the Sensor are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

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

- [Sensor Network Configuration](#)
- [Sensor Only Settings](#)
- [Sensor Operation](#)
- [RF-Domain](#)
- [Location Based Services](#)
- License—Display valid licenses for Sensor.

These configuration settings (or profiles), except Sensor Network Configuration, are all located in the [Configuration](#) tab.

If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

### **Sensor Network Configuration**

Sensor Network Configuration is used to configure network settings for Sensors that are connected to your AirDefense Services Platform appliance.

There are three configurable sections:

- IPv4
- IPv6
- DNS.

#### IPv4

Field	Description
Use DHCP	Select the checkbox to enable DHCP, short for Dynamic Host Configuration Protocol, which is a protocol for assigning dynamic IP addresses to devices in a network.
IP Address	Manually enter a static IP address for the Sensor.
Net Mask	Manually enter the subnet to which the Sensor belongs.
Gateway	Manually assign a valid Gateway IP address to the Sensor.

#### IPv6


Select the **IPv6** checkbox to activate the IPv6 options.

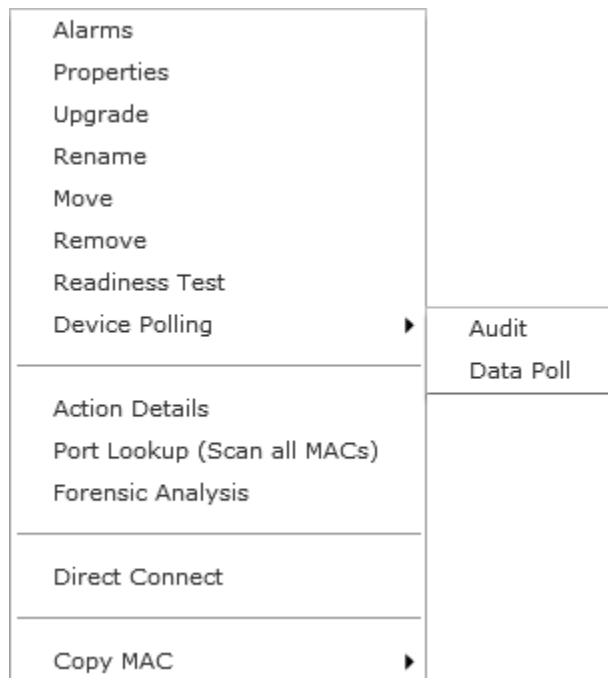
Field	Description
Use DHCP	Select the checkbox to enable DHCP.
IP Address	Manually enter a static IP address for the Sensor.
Prefix Length	Specify the static prefix length as a decimal value.
Gateway	Manually assign a valid static Gateway IP address to the Sensor.

## DNS

Field	Description
Obtain DNS Automatically	Select the checkbox automatically obtain DNS information.
Primary DNS	Manually enter an IP address for the primary DNS server.
Secondary DNS	Manually enter an IP address for the secondary DNS server.
Domain Name	Manually enter a domain name for your DNS server.

## Wireless Switch

The Wireless Switch drop-down menu contains functions that you can apply to the selected Wireless Switch. Click the drop-down menu button——next to the Wireless Switch name to display the drop-down menu.




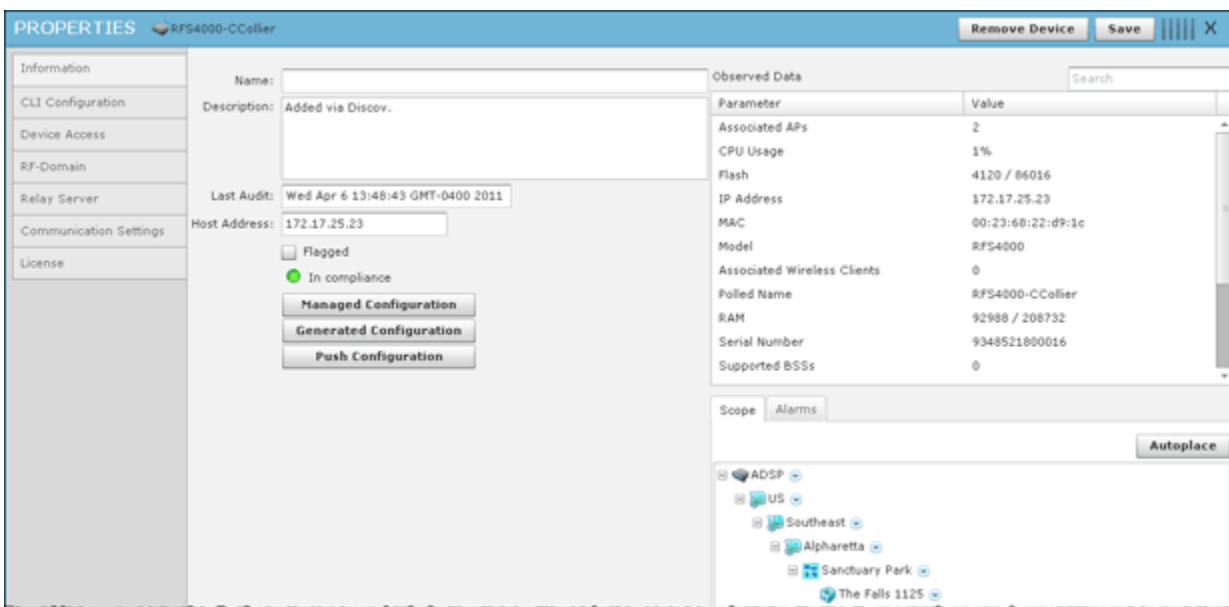
The drop-down menu for Wireless Switches contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Wireless Switch.
Properties	Opens the <b>Properties</b> overlay for the selected Wireless Switch.
Upgrade	Upgrades the firmware for the selected Wireless Switch. (See <a href="#">Upgrade Devices</a> for more information.)
Rename	Opens a dialog window to rename the selected Wireless Switch.
Move	Moves the selected Wireless Switch to another network level (floor). (See <a href="#">Move Devices</a> for more information.)
Remove	Removes the selected Wireless Switch from your network. (See <a href="#">Remove Devices</a> for more information.)

Function	Description
Readiness Test	Validates that the Wireless Switch is management ready (that is, it can be managed through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected Wireless Switch. (See <a href="#">Audit Devices</a> for more information.)
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup	Scans MAC Addresses to view a list of switch ports.
Forensic Analysis	Opens the <a href="#">Forensic Analysis</a> 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.

### Properties

You can view the properties of a Wireless Switch by clicking the drop-down menu button— and clicking **Properties**.



The screenshot shows the 'PROPERTIES' window for a Wireless Switch named 'RFS4000-CCollier'. The window is divided into several sections:

- Information:** Name, Description (Added via Discov.), Last Audit (Wed Apr 6 13:48:43 GMT-0400 2011), Host Address (172.17.25.23), and compliance status (In compliance).
- Observed Data:** A table listing parameters and their values:
 

Parameter	Value
Associated APs	2
CPU Usage	1%
Flash	4120 / 86016
IP Address	172.17.25.23
MAC	00:23:68:22:d9:1c
Model	RFS4000
Associated Wireless Clients	0
Polled Name	RFS4000-CCollier
RAH	92988 / 208732
Serial Number	9348521800016
Supported BSSs	0
- Scope:** A tree view showing the device's location within the network hierarchy: ADSP > US > Southeast > Alpharetta > Sanctuary Park > The Falls 1125.

The following information is displayed:

Field	Description
Name	The name of the Wireless Switch.
Description	A description of the Wireless Switch.
Last Audit	The date and time of the last audit.
Host Address	The IP address of the Wireless Switch.



Field	Description
Flagged	Flag a Wireless Switch that you want to bring attention to.
In compliance / Not in compliance	<p>Status of the last compliance audit.</p> <p>Click the <b>Managed Configuration</b> button to display the Wireless Switch configuration.</p> <p>Click the <b>Generated Configuration</b> button to display a generated configuration for a Wireless Switch. The generated configuration is the same configuration sent to a relay server to configure a Wireless Switch.</p> <p>Click the <b>Push Configuration</b> button to push the existing configuration out to the Wireless Switch.</p>
Observed Data	Data that AirDefense Services Platform observed about the Wireless Switch. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the Wireless Switch is shown under the Scope tab. The Autoplace button can be used to place the Wireless Switch in a network folder using Auto-Placement Rules.

Alarms related to the Wireless Switch are shown in the Alarms tab. The Actions button can be used to perform one of the listed functions on a selected (highlighted) alarm.

You can view and/or override a Wireless Switch's configuration by selecting:

- [CLI Configuration](#)
- [Device Access](#)
- [RF-Domain](#)
- [Relay Server](#)
- [Communication Settings](#)
- License—Display valid licenses for Wireless Switch.


These configuration settings are all located in the [Configuration](#) tab.

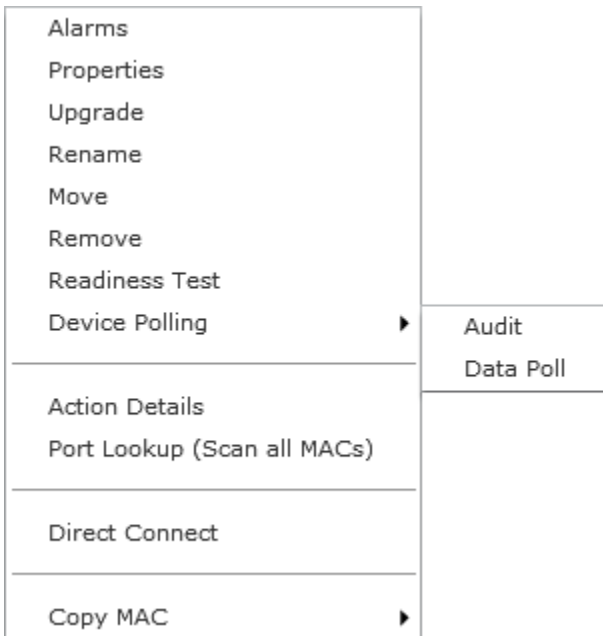
If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

## Wired Switch


The Wired Switch drop-down menu contains functions that you can apply to the selected Wired Switch. Click the drop-down menu button— next to the Wired Switch name to display the drop-down menu.

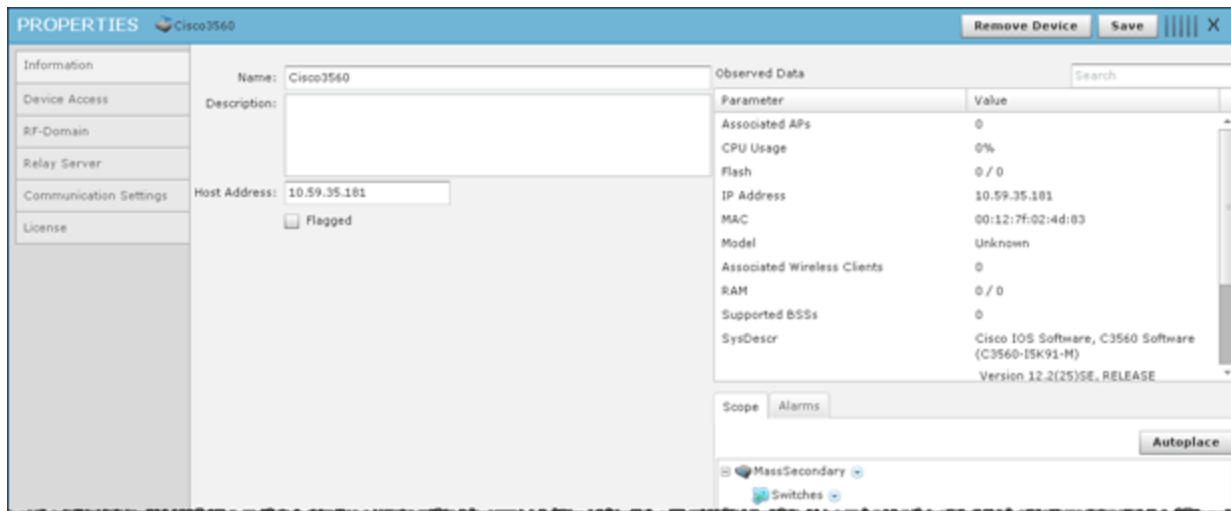


The drop-down menu for Wired Switches contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Wired Switch.
Properties	Opens the <b>Properties</b> overlay for the selected Wired Switch.
Upgrade	Upgrades the firmware for the selected Wired Switch. (See <a href="#">Upgrade Devices</a> for more information.)
Rename	Opens a dialog window to rename the selected Wired Switch.
Move	Moves the selected Wired Switch to another network level (floor). (See <a href="#">Move Devices</a> for more information.)
Remove	Removes the selected Wired Switch from your network. (See <a href="#">Remove Devices</a> for more information.)
Readiness Test	Validates that the Wired Switch is management ready (that is, it can be manage through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected Wired Switch. (See <a href="#">Audit Devices</a> for more information.)
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup (Scan all MACs)	Scans MAC Addresses to view a list of switch ports.
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.

## Properties

You can view the properties of a Wired Switch by clicking the drop-down menu button——and clicking **Properties**.



The following information is displayed:

Field	Description
Name	The name of the Wired Switch.
Description	A description of the Wired Switch.
Host Address	The IP address of the Wired Switch.
Flagged	Flag a Wired Switch that you want to bring attention to.
Observed Data	Data that AirDefense Services Platform observed about the Wired Switch. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the Wired Switch is shown under the Scope tab. The Autoplace button can be used to place the Wired Switch in a network folder using Auto-Placement Rules.

Alarms related to the Wired Switch are shown in the Alarms tab. The Actions button can be used to perform one of the listed functions on a selected (highlighted) alarm.

You can view and/or override a Wired Switch's configuration by selecting.

- [Device Access](#)
- [RF-Domain](#)
- [Relay Server](#)
- [Communication Settings](#)
- License—Display valid licenses for Wired Switch.


These configuration settings are all located in the [Configuration](#) tab.

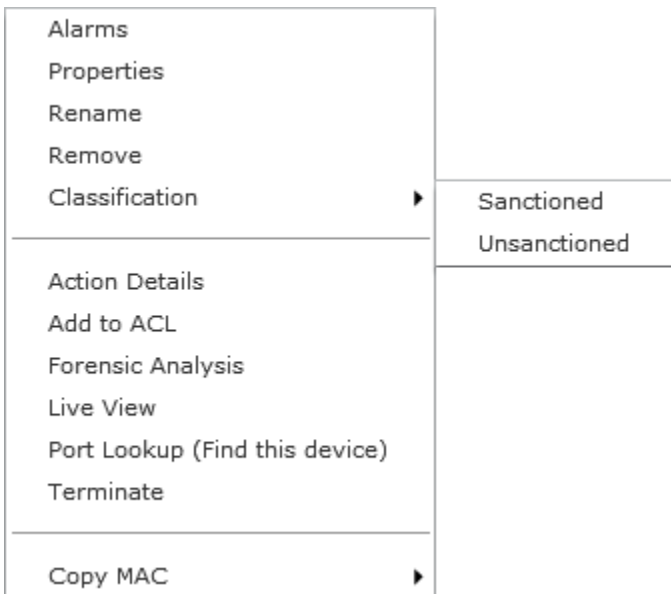
If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

## Unknown Devices


The Unknown Devices drop-down menu contains functions that you can apply to the selected Unknown Device. Click the drop-down menu button— next to the Unknown Device name to display the drop-down menu.

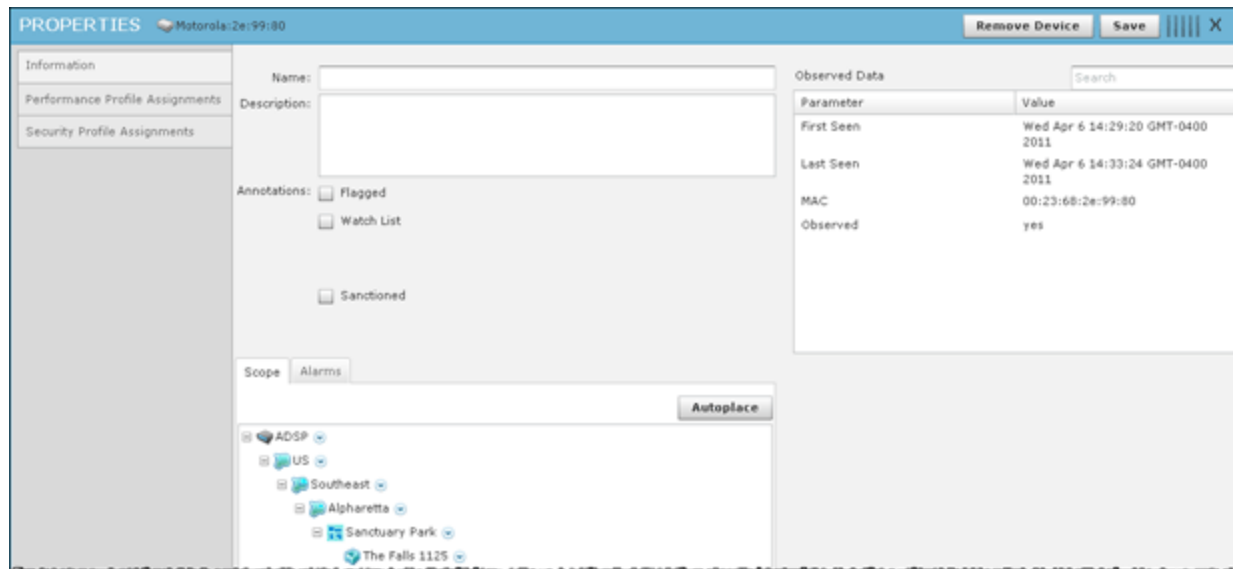


The drop-down menu for unknown devices contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected unknown device.
Properties	Opens the <b>Properties</b> 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. (See <a href="#">Remove Devices</a> for more information.)
Classification	Classifies the unknown device as <b>Sanctioned</b> or <b>Unsanctioned</b> .
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 <a href="#">Forensic Analysis</a> window for the specified unknown device.
Live View	Opens the <a href="#">Live View</a> window for the selected unknown device; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the <a href="#">Port Lookup</a> window where you can locate the physical port where the Unknown Device is accessing your network.
Terminate	Accesses the <a href="#">Terminate</a> 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.

## Properties

You can view the properties of an Unknown Device by clicking the drop-down menu button— and clicking **Properties**.



The following information is displayed:

Field	Description
Name	The name of the Unknown Device.
Description	A description of the Unknown Device.
Annotations	The annotations specified for the Unknown Device: <b>Flagged</b> , <b>Watch List</b> , or <b>Sanctioned</b> .
Observed Data	Data that AirDefense Services Platform observed about the Unknown Device. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the Unknown Device is shown under the **Scope** tab. The **Autoplace** button can be used to place the Unknown Device in a network folder using Auto-Placement Rules.

Alarms related to the Unknown Device are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

You can view and/or override a Unknown Device's configuration by selecting:

- [Performance Profiles](#) Assignments
- [Security Profiles](#) Assignments.


These configuration settings (or profiles) are all located in the [Configuration](#) tab.

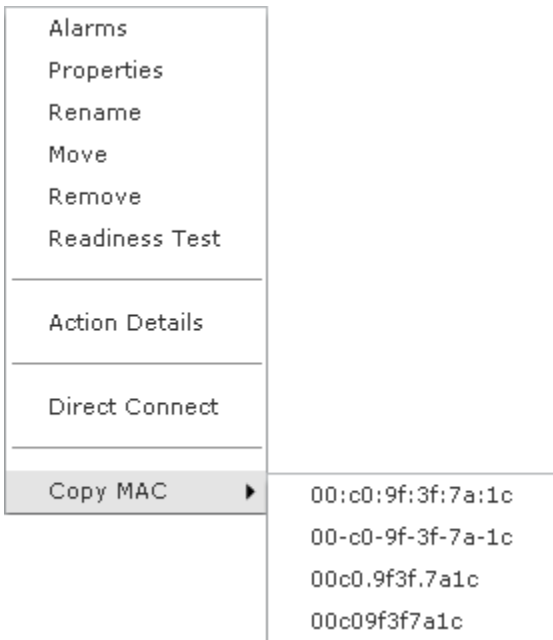
If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

## WLSE


The WLSE drop-down menu contains functions that you can apply to the selected WLSE. Click the drop-down menu button— next to the WLSE name to display the drop-down menu.

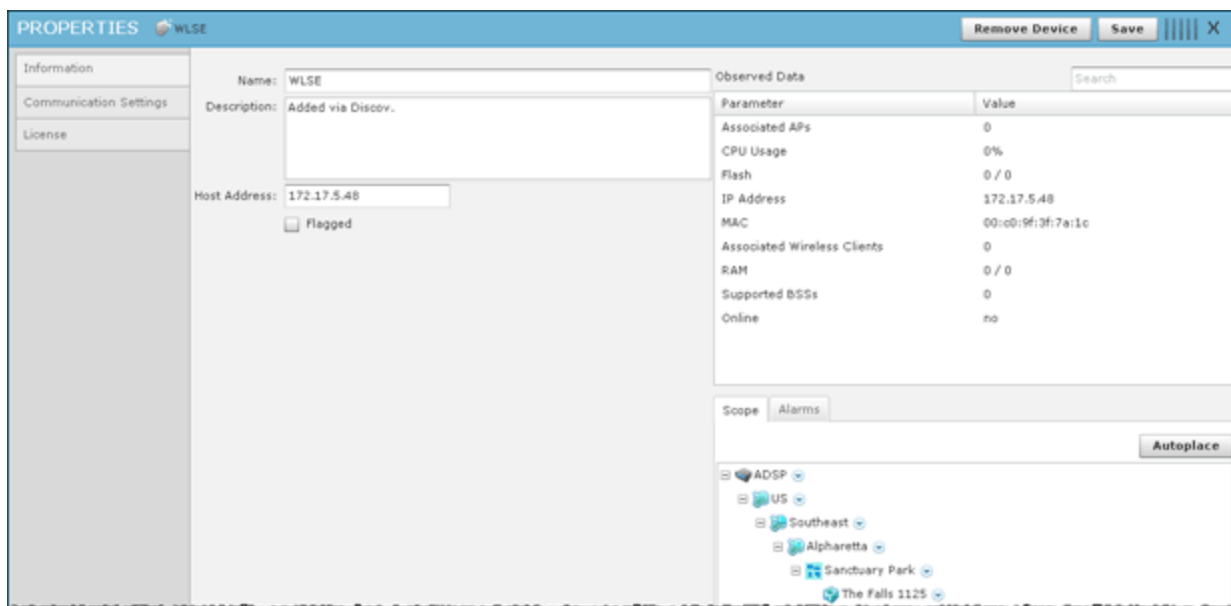


The drop-down menu for WLSE devices contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected WLSE device.
Properties	Opens the <b>Properties</b> overlay for the selected WLSE device.
Rename	Opens a dialog window to rename the selected WLSE device.
Move	Moves the selected WLSE device to another network level (floor). (See <a href="#">Move Devices</a> for more information.)
Remove	Removes the selected WLSE device from your network. (See <a href="#">Remove Devices</a> for more information.)
Readiness Test	Validates that the WLSE device is management ready (that is, it can be managed through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)
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.

## Properties

You can view the properties of a WLSE by clicking the drop-down menu button— and clicking **Properties**.



The following information is displayed:

Field	Description
Name	The name of the WLSE.
Description	A description of the WLSE.
Host Address	The IP address of the WLSE.
Flagged	Flag a WLSE that you want to bring attention to.
Observed Data	Data that AirDefense Services Platform observed about the WLSE. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the WLSE is shown under the **Scope** tab. The **Autoplace** button can be used to place the WLSE in a network folder using Auto-Placement Rules.

Alarms related to the WLSE are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

You can view and/or override an WLSE's configuration by selecting **Communication Settings**. Communication Settings configuration settings are located in the **Configuration** tab.


You can display valid licenses for a WLSE by selecting **License**.

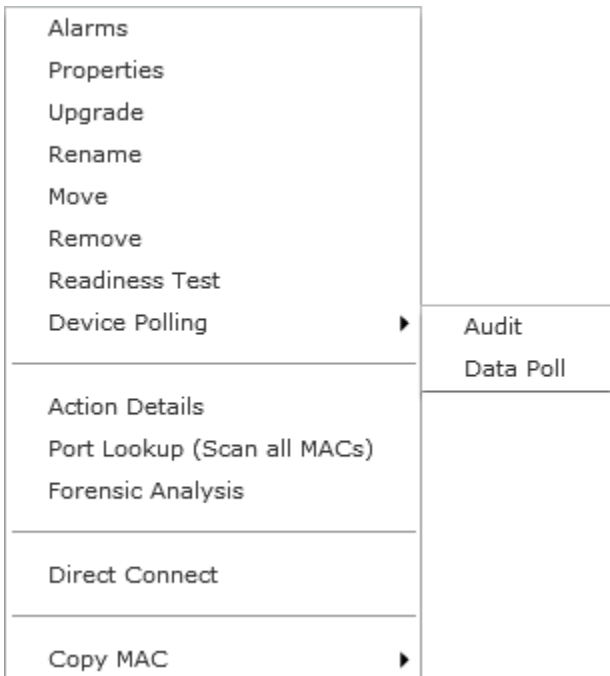
If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

## AirWave

The AirWave switch drop-down menu contains functions that you can apply to the selected AirWave switch. Click the drop-down menu button— next to the AirWave switch name to display the drop-down menu.




The drop-down menu for AirWave devices contains the following functions:

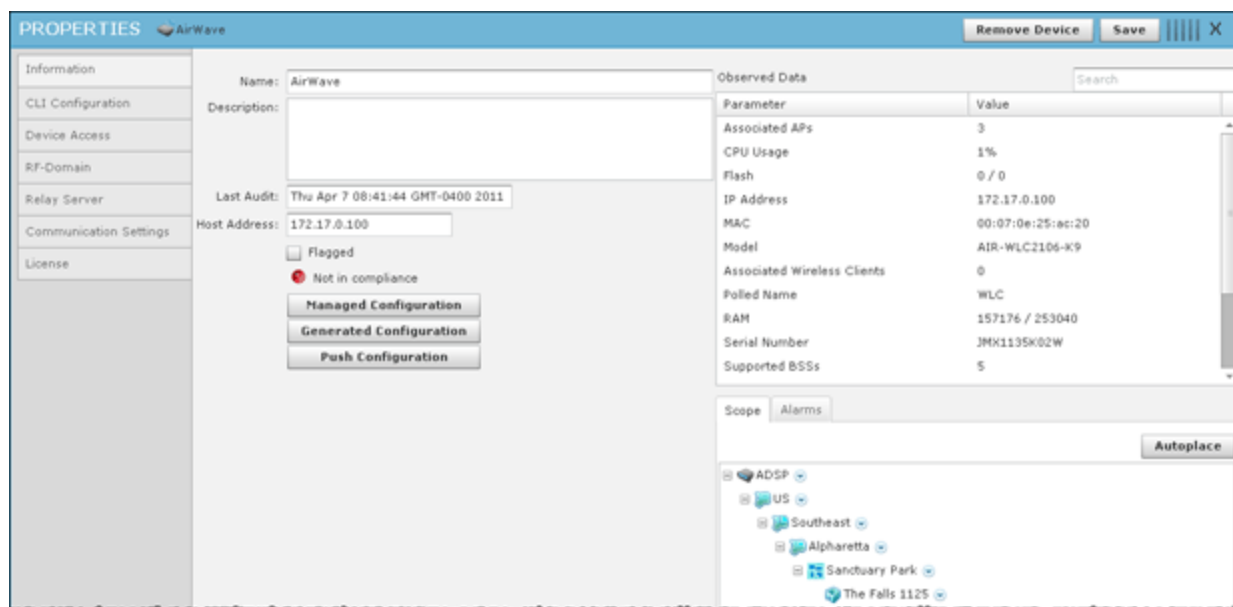
Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected AirWave device.
Properties	Opens the <b>Properties</b> overlay for the selected AirWave device.
Upgrade	Upgrade the firmware for the selected AirWave switch. (See <a href="#">Upgrade Devices</a> for more information.)
Rename	Opens a dialog window to rename the selected AirWave device.
Move	Moves the selected AirWave device to another network level (floor). (See <a href="#">Move Devices</a> for more information.)
Remove	Removes the selected AirWave device from your network. (See <a href="#">Remove Devices</a> for more information.)
Readiness Test	Validates that the AirWave device is management ready (that is, it can be managed through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)
Device Polling	Conduct a compliance audit on the selected AirWave switch. (See <a href="#">Audit Devices</a> for more information.)
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup (Scan all MACs)	Scan MAC addresses to view a list of switch ports.



Function	Description
Forensic Analysis	Opens the <a href="#">Forensic Analysis</a> 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.

### Properties

You can view the properties of a AirWave switch by clicking the drop-down menu button— and clicking [Properties](#).



The following information is displayed:

Field	Description
Name	The name of the AirWave Switch.
Description	A description of the AirWave Switch.
Last Audit	The date and time of the last audit.
Host Address	The IP address of the AirWave Switch.
Flagged	Flag a AirWave Switch that you want to bring attention to.
In compliance / Not in compliance	Status of the last compliance audit. Click the <b>Managed Configuration</b> button to display the AirWave Switch configuration. Click the <b>Generated Configuration</b> button to display a generated configuration for a AirWave Switch. The generated configuration is the same configuration sent to a relay server to configure a AirWave Switch. Click the <b>Push Configuration</b> button to push the existing configuration out to the AirWave Switch.
Observed Data	Data that AirDefense Services Platform observed about the AirWave Switch. You can filter the observed data by entering significant text in the <b>Search</b> field.

The scope of the AirWave Switch is shown under the **Scope** tab. The **Autoplace** button can be used to place the AirWave Switch in a network folder using Auto-Placement Rules.

Alarms related to the AirWave Switch are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

You can view and/or override a AirWave Switch's configuration by selecting:

- [CLI Configuration](#)
- [Device Access](#)
- [RF-Domain](#)
- [Relay Server](#)
- [Communication Settings](#)
- License—Display valid licenses for AirWave switch.

These configuration settings are all located in the [Configuration](#) tab.

If you make changes, click the **Save** button to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button—X to close the **Properties** overlay.

### **Device Functions Requiring More Explanation**

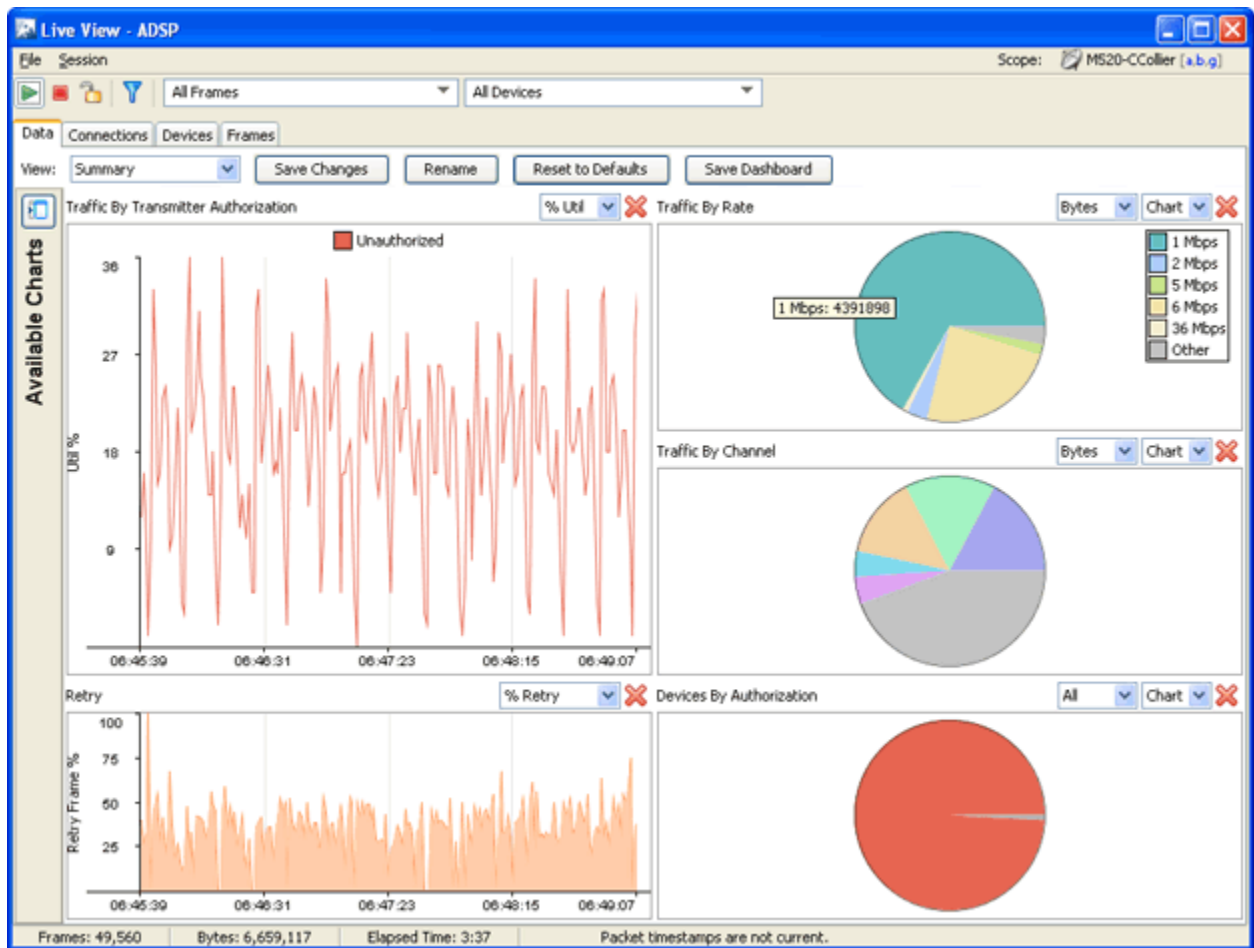
The device functions discussed here are drop-down menu functions that operate on devices and require more details on how to use them. Depending on the device, these functions may or may not appear in the drop-down menu. They are:

- Live View
- Locate
- Port Lookup
- Readiness Test
- Spectrum Analysis
- Terminate.

#### ***Live View***

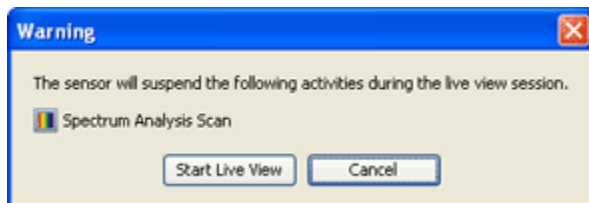
ADSP gives you a Live View of the devices operating in your wireless LAN. Live View capability exists throughout the GUI, wherever a device icon appears. You access Live View by clicking on the drop-down menu

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, the following warning displays.



You can either start the monitoring session and suspend the Spectrum Analysis, or cancel the Live View session.

Live View consists of four main categories of information:

- Data
- Connections
- Devices
- Frames.

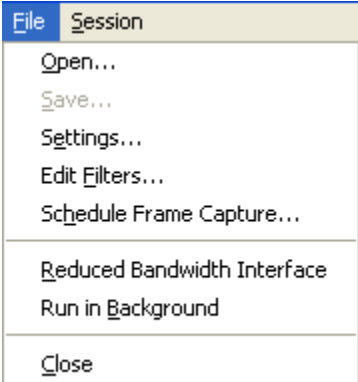
### **Common Area**


The common area holds the menus and buttons that are common to the **Live View** window. It is located at the top of the window.







## Overview

Menus

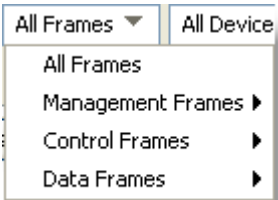
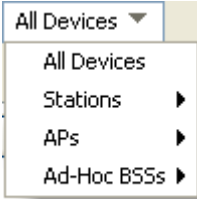
Menu	Option	Description
	Open	Opens a captured frame file for viewing. (See <a href="#">Frame Capture Analysis</a> for more information.)
	Save	Opens the <b>Save Frame Capture</b> popup window where you can save the temporary capture file to a permanent file on the server or to a file on your workstation. (See <a href="#">Frame Capture</a> for more information.)
	Settings	Opens the <b>Live View Settings</b> popup window where you can set options for your Live View sessions. (See <a href="#">Live View Settings</a> for more information.)
	Edit Filters	Opens the Live View Filter popup window where you can set options to filter data. (See <a href="#">Live View Filter</a> for more information.)
	Schedule Frame Capture	Schedule a Frame Capture session using the scheduler. (See <a href="#">Schedule Frame Capture</a> for more information.)
	Reduced Bandwidth Interface	Shrinks the <b>Frame Capture</b> window and conserves bandwidth while running Live View. <div data-bbox="959 1142 1484 1367" data-label="Image"> </div> <ul style="list-style-type: none"> <li>While in the reduced bandwidth state, you can:               <ul style="list-style-type: none"> <li>Return to the original <b>Live View</b> window by clicking <b>Live View</b>.</li> <li>Run live view in the background by clicking <b>Run in Background</b>.</li> <li>Stop capturing Live View frames and exit Live View by clicking <b>Stop Capture</b>.</li> </ul> </li> </ul>
	Run in Background	Exits <b>Live View</b> window and runs Live View in the background.
	Close	Exits the Live View session and closes the <b>Live View</b> window.

Menu	Option	Description
	Start	Starts a Live View session.
	Stop	Stops a Live View session.
	Freeze	Freezes a Live View session. The data in the window freezes but Live View keeps collecting data to display later after you unfreeze the session.

***Buttons***

Button	Description
	Starts a Live View session.
	Stops a Live View session.
	Freezes a Live View session. The data in the window freezes but Live View keeps collecting data to display later after you unfreeze the session. Click the <b>Freeze</b> button again to unfreeze the session.
	Opens the <b>Live View Filter</b> popup window, where you can set options to filter data. (See <a href="#">Live View Filter</a> for more information.)

***drop-down Menus***

drop-down Menu	Description
	Acts as a quick filter to display only frames for the selected frame type. To view all types, select <b>All Frames</b> .
	Acts as a quick filter to display only frames for the selected device. To view all devices, select <b>All Devices</b> .

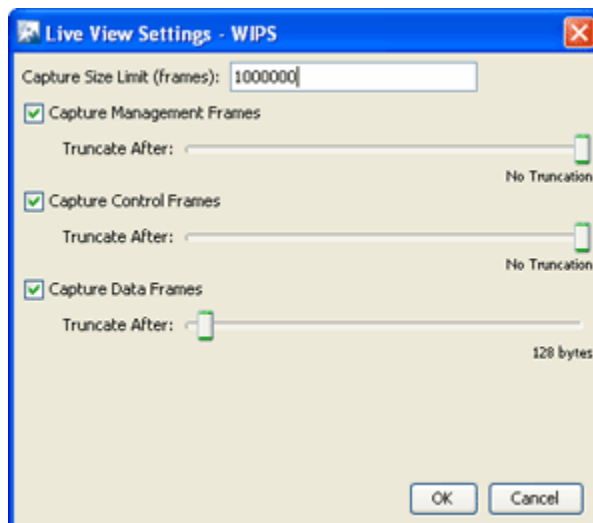
## Live View Settings

Live View has four user adjustable settings. They are:

Setting	Description
Capture Size Limit	Sets the maximum amount of frames that can be captured during any one session.
Capture Management Frames	Sets the Live Monitoring sessions to capture management frames. If selected, you can also truncate management frames to a specific number of bytes or have no truncation.
Capture Control Frames	Sets the Live Monitoring sessions to capture control frames. If selected, you can also truncate control frames to a specific number of bytes or have no truncation.
Capture Data Frames	Sets the Live Monitoring sessions to capture data frames. If selected, you can also truncate data frames to a specific number of bytes or have no truncation.

To change the settings:

1. Select **File > Settings** to display the **Live View Settings** popup window.



2. Make your adjustments.
3. Click **OK**.


### Live View Filter

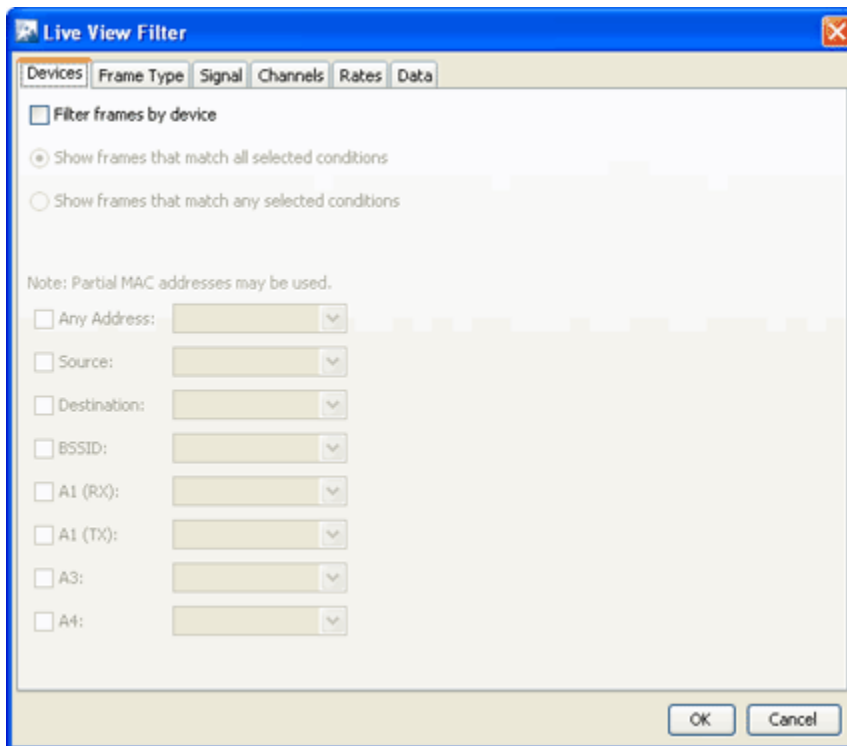
You can limit what you see in Live View through the use of filters. Frames may be filtered by any of the following methods:

Method	Description
Devices	<p>Filters Live View frames by devices. To filter by devices, go to the <b>Devices</b> tab, select <b>Filter frames by device</b>, and select any of the following conditions along:</p> <ul style="list-style-type: none"> <li>• Any Address</li> <li>• Source</li> <li>• Destination</li> <li>• BSSID</li> <li>• A1 (RX)</li> <li>• A1 (TX)</li> <li>• A3</li> <li>• A4</li> </ul> <p>For every condition that you select, you must specify a MAC address. You have the option of displaying frames that match all of the selected conditions or displaying frames that match any of the selected conditions.</p>
Frame Type	<p>Filters Live View frames by 802.11 frame type. To filter by frame types, go to the <b>Frame Type</b> tab, select <b>Filter frames by frame type</b>, and de-select any frame type that you do not want to display. You may filter out a whole category (Control, Management, or Data) or any of the sub-categories.</p>
Signal Filters	<p>Live View frames by signal strength. To filter by signal strength, go to the <b>Signal</b> tab, select <b>Filter frames by signal strength</b>, and enter the minimum signal strength in dBm and the maximum signal strength in dBm. Only signals within the specified range will display in Live View.</p>
Channel Filters	<p>Live View frames by channels. To filter by channels, go to the <b>Channels</b> tab, select <b>Filter frames by channel</b>, and deselect the channels that you do not want to display. You may filter out a whole category (b/g or a) of channels or individual channels.</p>
Rates Filters	<p>Live View frames by transmission rate. To filter by transmission rate, go to the <b>Rates</b> tab, select <b>Filter frames by rate</b>, and deselect any rate that you do not want to display.</p>
Data Filters	<p>Live View frames by data type. To filter by data type, go to the <b>Data</b> tab, select <b>Filter frames by data</b>, de-select any of the encryption types that you do not want to display, and de-select any of the Ether types that you do not want to display.</p>

To filter Live View frames:



1. Select **File > Edit Filters** or click the **Filter-**  button to display the **Live View Filter** popup window.



2. Set your filter criteria by clicking on the appropriate tab.
3. Click **OK**.

## Data Tab

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

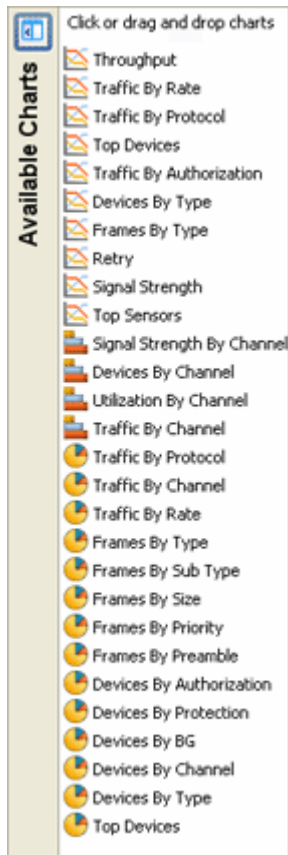


The **Data** tab focus can be changed by changing the view. Depending on the view that is selected different charts are displayed. There are four available views:

View	Description
Summary	Provides a summary of frame data using the following charts: <ul style="list-style-type: none"> <li>Traffic By Transmitter Authorization</li> <li>Retry</li> <li>Traffic By Rate</li> <li>Traffic By Channel</li> <li>Devices By Authorization.</li> </ul> This is the default view.
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.


Each view is customizable. You can add more charts to a view, rearrange the view, or remove charts from a view.

To add a chart to a view, click the **View Available Charts**— button to reveal the Available Charts.




Once the Available Charts are revealed, you can drag and drop a chart to the display area. You can display up to nine charts. To view a chart temporarily, click on the chart name. It will display superimposed over the current charts.

drop-down menus are available to customize the view of the charts.

To hide Available Charts, click the **Hide Available Charts**— button.

To rearrange a view, you can drag and drop charts to another location.

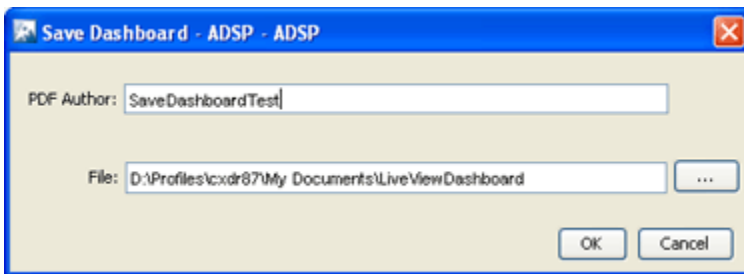
To remove a chart, click the **Remove**— button associated with the chart.

Once you have customized the display to fit your needs, click the **Save Changes** button to save your arrangement. The customized view is saved on your ADSP server. Now, whenever you access Live View, you can access your customized arrangement. This is true even if you are accessing the GUI on another workstation.

You can change the name of a view by clicking the **Rename** button. Just type in the new name and click **OK**. This allows you to give a view a more descriptive name if you changed the view significantly.

To return a view to the original factory default, click the **Reset to Defaults** button.

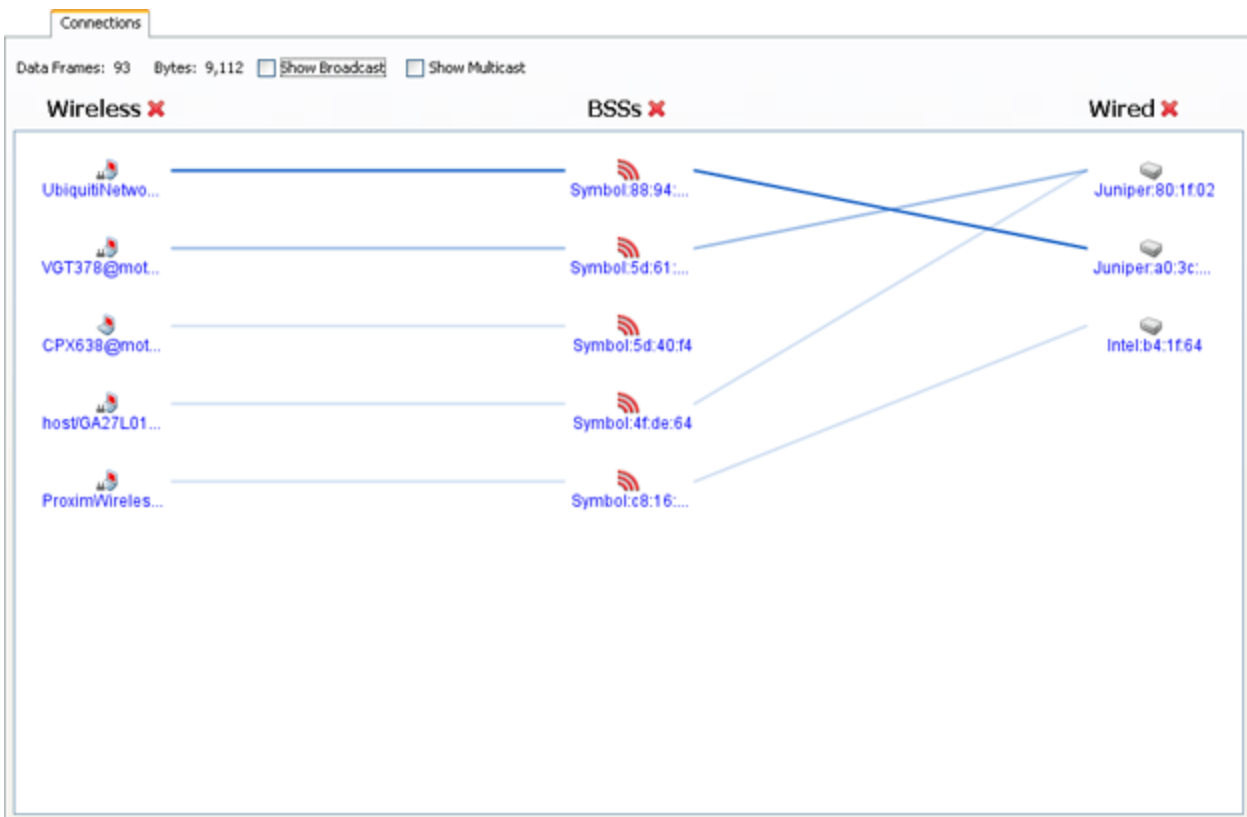
You can save a PDF file with a snapshot of the data charts by clicking the **Dashboard** button. A dialog window opens where you can name the PDF file and specify an author's name.



After supplying author's name and file name, click **OK**.

### **Connections Tab**

The **Connections** tab displays 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. Just select the checkbox for the option you want.

The **Data Frames** and **Bytes** fields display the count of data frames and bytes.

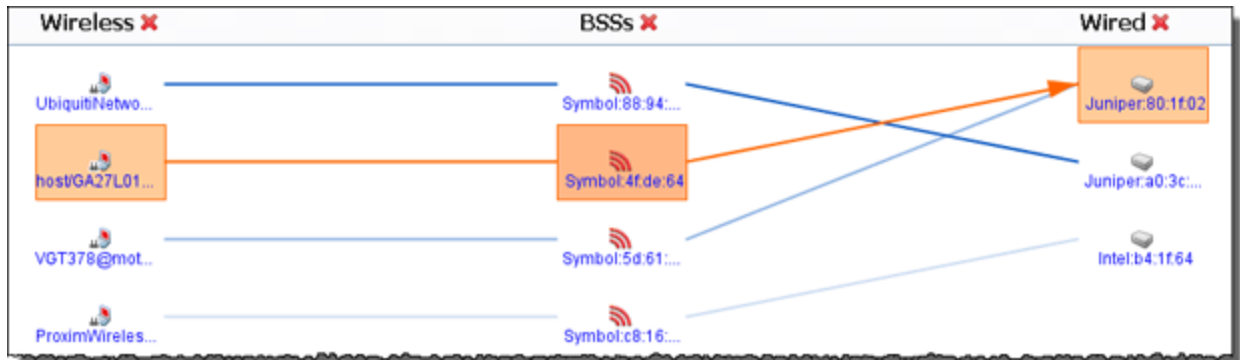
If more than 50,000 frames have been captured during the Live View session, only the most recent 50,000 frames are displayed.

Devices are listed in three columns: Wireless (wireless devices), Access Points and Wired (wired devices). Device columns may be disabled or re-enabled by using the hide ( **X** )/show ( **+** ) button next to the column name. For example, if the Access Points column is hidden, then connections will be shown directly from the source to the destination without the BSS in the middle.

A connection is defined as a set of devices referenced by a single data frame. Typically, a connection will involve three devices (source, destination, and BSS); but, in some cases may involve four devices (wireless bridging).

A line is defined as a link between two devices. Each connection is made up of multiple lines and each line may be part of multiple connections. The intensity and Z-order (whether a line is on top or bottom) of a line is based on the number of frames between the two devices.

Clicking on a device selects a connection involving that device. The devices and lines involved in the connection will be highlighted.



If you continue clicking on the device, the graph will cycle through the connections involving the selected device. Buttons are also provided to cycle through the connections.

Showing connection 1 of 2 including Cisco:35:37:a0  

The **Data Frames** and **Bytes** fields will only show the data corresponding to the selected connection.

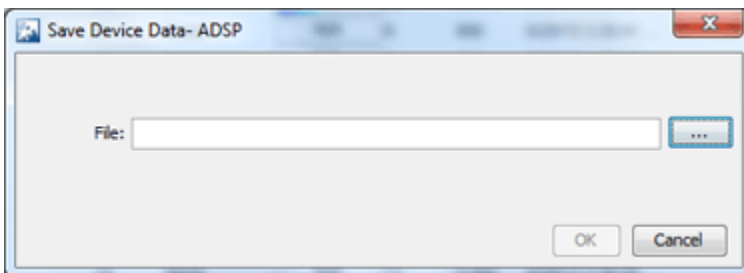
## Devices Tab

The **Devices** tab displays the devices that have been seen during a Live Monitoring session in tabular form.

Device	SSID	Chan...	Channel E...	Signal (dBm)	Frames	Bytes	Last Seen	Authentica...	Encryption
Motorola:20:a9:50	chad-test	36	None	-83	39	8,658	5/29/13 2:46:05 ...		
Motorola:20:b3:70	DevMgmt_101	11	None	-57	55	11,605	5/29/13 2:46:05 ...		None
Motorola:20:b3:71	DevMgmt_102	11	None	-56	57	12,427	5/29/13 2:46:03 ...		None
Motorola:20:b3:72	DevMgmt_103	11	None	-57	60	12,915	5/29/13 2:46:07 ...		None
Motorola:20:b3:73	DevMgmt_104	11	None	-57	59	12,926	5/29/13 2:46:07 ...		TKIP
5c:0e:8b:20:b7:30	chad-test	1	None	-91	1	219	5/29/13 2:45:12 ...		
Motorola:20:ba:f0	DevMgmt_101	161	None	-59	80	10,070	5/29/13 2:46:03 ...		None
Motorola:20:ba:f1	DevMgmt_102	161	None	-59	81	9,379	5/29/13 2:46:03 ...		None
Motorola:20:ba:f2	DevMgmt_103	161	None	-60	82	10,808	5/29/13 2:46:03 ...		None
Motorola:20:ba:f3	DevMgmt_104	161	None	-59	89	11,820	5/29/13 2:46:03 ...		TKIP
Motorola:23:7a:50	AP6532-Service	36	None	-72	44	9,685	5/29/13 2:46:05 ...		
Motorola:24:44:90	RFS4K-WAN4	11	None	-67	3	720	5/29/13 2:45:28 ...	WPA2 - PSK	CCMP
Motorola:24:73:80	RFS4K-WAN4	48	Lower	-72	52	11,667	5/29/13 2:46:06 ...	WPA2 - PSK	CCMP
Motorola:25:34:00	AP6532-Service	1	None	-79	14	3,150	5/29/13 2:45:51 ...		
Motorola:25:34:20	AP6532-Service	161	None	-69	34	7,752	5/29/13 2:46:03 ...		
Motorola:33:f7:d8		5	None	N/A	5	1,680	5/29/13 2:45:48 ...		
Motorola:49:bb:44		5	None	N/A	0	0	5/29/13 2:30:34 ...		
Motorola:4a:e6:70	AP7161-47BB44...	1	None	-69	20	4,631	5/29/13 2:45:27 ...		
Motorola:4a:e6:71	ap7161_net1_j	1	None	-70	37	8,436	5/29/13 2:46:06 ...		
Motorola:4a:fe:50	DevMgmt_ZERO	149	Upper	-60	129	23,265	5/29/13 2:46:03 ...		
Motorola:4a:fe:51	DevMgmt_102	149	Upper	-60	72	13,978	5/29/13 2:46:03 ...		
Motorola:4a:fe:52	DevMgmt_103	149	Upper	-60	84	16,452	5/29/13 2:46:03 ...		
Motorola:4a:fe:53	DevMgmt_104	149	Upper	-60	75	14,652	5/29/13 2:46:03 ...		
Motorola:4a:fe:54	DevMgmt_105	149	Upper	-59	81	15,978	5/29/13 2:46:03 ...		
Motorola:4a:fe:55	DevMgmt_106	149	Upper	-60	80	15,746	5/29/13 2:46:03 ...		
Motorola:4a:fe:56	DevMgmt_107	149	Upper	-60	80	16,768	5/29/13 2:46:03 ...		

Options are provided to show all devices, only BSSs, Wireless Clients, or Wired 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 **Export** button can be used to export device data to a CSV file.



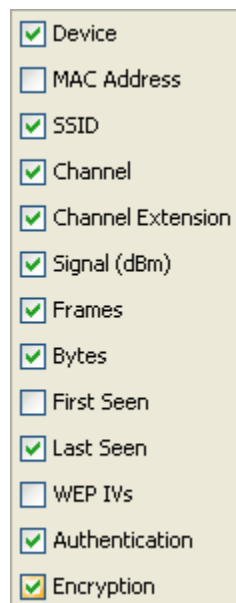
Just browse to a folder (directory) to save the file in, type in a name, and click the **Select** button. The name of the file is displayed in the **File** field. Now, click **OK** to save the file in the selected folder (directory).

The Devices 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.
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.

Column display and arrangement can be customized as follows:

- Hide or un-hide a category by right-clicking in the column heading area, and uncheck or checking the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

## Frames Tab

The **Frames** tab displays the frames that were captured during a Live Monitoring session.

Time	Source	Destination	BSSID	Observe...	Channel...	Rate	Signal (d...	Size	Protocol
15:51:08.1...	Motorola:48:83:6f	Intel:a1:b3:2c	Motorola:48:83:6f44		None	6 Mbps	-67	213	Probe response
15:51:08.1...	Symbol:c8:46:30	Broadcast	Symbol:c8:46:3044		None	6 Mbps	-70	230	Beacon
15:51:08.1...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f044		None	6 Mbps	-83	160	Beacon
15:51:08.1...	Symbol:c8:46:31	Broadcast	Symbol:c8:46:3144		None	6 Mbps	-70	196	Beacon
15:51:08.1...	Symbol:e4:ea:70	Broadcast	Symbol:e4:ea:7044		None	6 Mbps	-76	97	Beacon
15:51:08.1...	Motorola:48:83:6f	Broadcast	Motorola:48:83:6f44		None	6 Mbps	-67	202	Beacon
15:51:08.1...	Symbol:c8:46:32	Broadcast	Symbol:c8:46:3244		None	6 Mbps	-71	205	Beacon
15:51:08.1...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f044		None	6 Mbps	-83	160	Beacon
15:51:08.2...	Symbol:c8:46:30	Broadcast	Symbol:c8:46:3044		None	6 Mbps	-70	230	Beacon
15:51:08.2...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f044		None	6 Mbps	-83	160	Beacon
15:51:08.2...	Motorola:43:cb:3c	Broadcast	Motorola:43:cb:3c13		None	1 Mbps	-74	212	Beacon
15:51:08.2...	Symbol:c8:46:31	Broadcast	Symbol:c8:46:3144		None	6 Mbps	-70	196	Beacon
15:51:08.2...	Symbol:e4:ea:70	Broadcast	Symbol:e4:ea:7044		None	6 Mbps	-76	97	Beacon
15:51:08.2...	Motorola:48:83:6f	Broadcast	Motorola:48:83:6f44		None	6 Mbps	-67	202	Beacon
15:51:08.2...	Motorola:43:cb:31	Broadcast	Motorola:43:cb:3113		None	1 Mbps	-75	232	Beacon
15:51:08.2...	Symbol:c8:46:32	Broadcast	Symbol:c8:46:3244		None	6 Mbps	-70	205	Beacon
15:51:08.2...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f044		None	6 Mbps	-83	160	Beacon
15:51:09.3...	Motorola:43:db:1f	Broadcast	Motorola:43:db:1f1		None	1 Mbps	-72	148	Beacon
15:51:09.3...	Cisco:df:3d:a0	Broadcast	Cisco:df:3d:a01		None	1 Mbps	-83	195	Beacon
15:51:09.3...	Symbol:c8:3c:21	Broadcast	Symbol:c8:3c:211		None	1 Mbps	-82	207	Beacon
15:51:09.3...	Cisco:0c:fc:8e	Broadcast	Cisco:0c:fc:8e1		None	1 Mbps	-80	148	Beacon


  

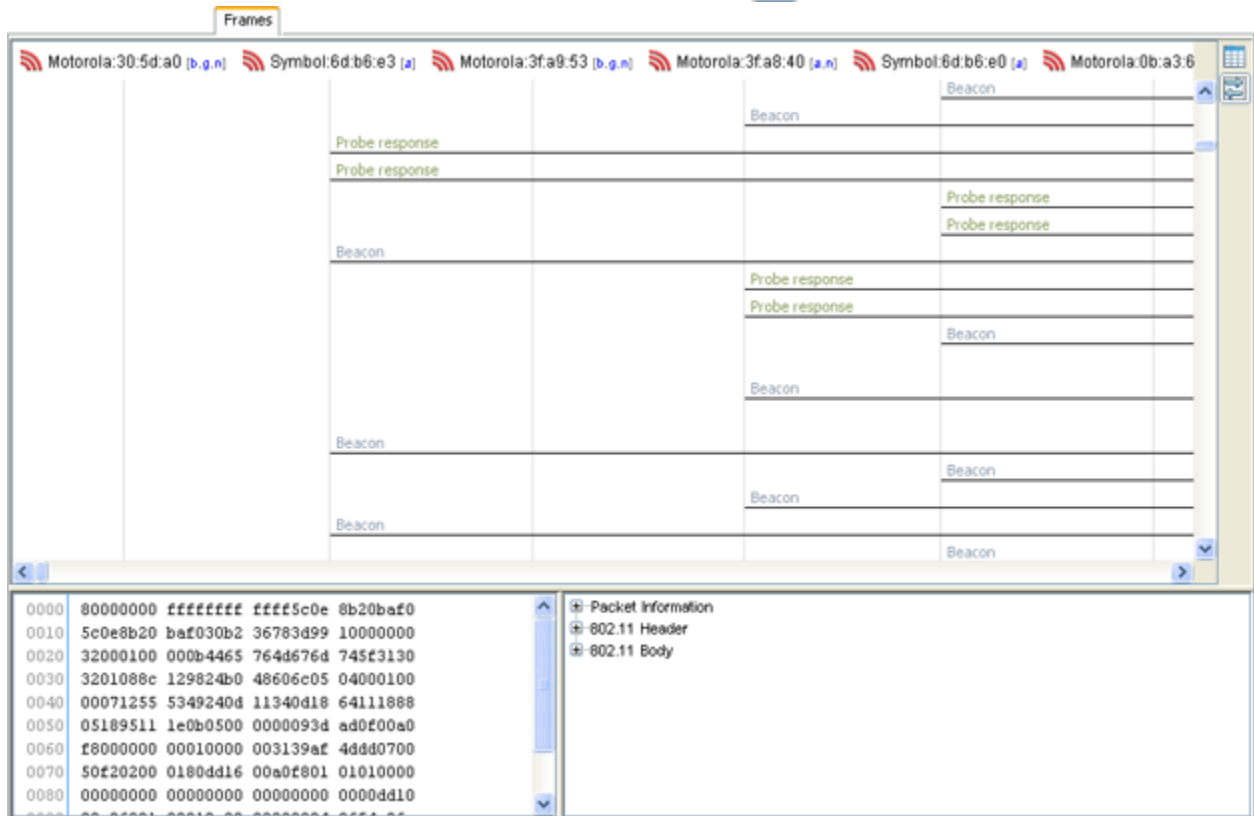
0000	80000000	fffffff	ffff5c0e	8b20baf0					
0010	5c0e8b20	baf030b2	36783d99	10000000					
0020	32000100	000b4465	764d676d	745f3130					
0030	3201088e	129824b0	48606c05	04000100					
0040	00071255	5349240d	11340d18	64111888					
0050	05189511	1e0b0500	0000093d	ad0f00a0					
0060	f8000000	00010000	003139af	4ddd0700					
0070	50f20200	0180dd16	00a0f801	01010000					
0080	00000000	00000000	00000000	0000dd10					


The captured file is stored in either—or, at times, both— of the following directories:

/usr/local/smx/pcaptures OR /usr/local/smx/pcaptures/saved.



You can switch to the frames view by clicking the Frames View— button.



Click the Data Table— button to switch back to the table view.

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).

### Table View

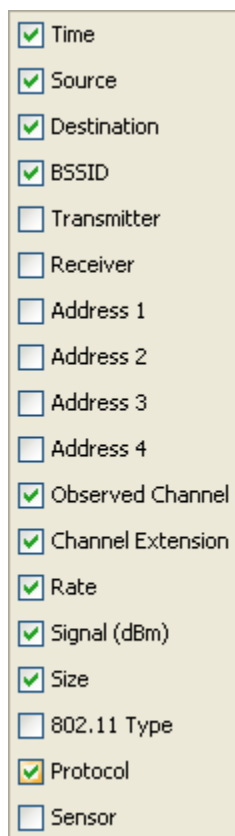
The frame table can be customized to display the following information:

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.

Column	Description
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.
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.

Column display and arrangement can be customized as follows:

- Hide or un-hide a category by right-clicking in the column heading area, and uncheck or checking the checkbox for a category (see below).



- Rearrange columns by clicking on a column heading and dragging it to a new position.

When a frame is selected (highlighted), the frame data is shown in the hex values and decodes areas.

The decodes area shows the 802.11 interpretation of the frame data in a tree structure. The hex values area and decodes area are linked so that selections in one area will follow the selections in the other.

### Frames View

The devices from which the frames were captured are displayed across the top of the tab. A frame is selected by clicking anywhere on the line under the frame name. When selected, the frame is highlighted in blue.

When a frame is selected (highlighted), the frame data is shown in the hex values and decodes areas.

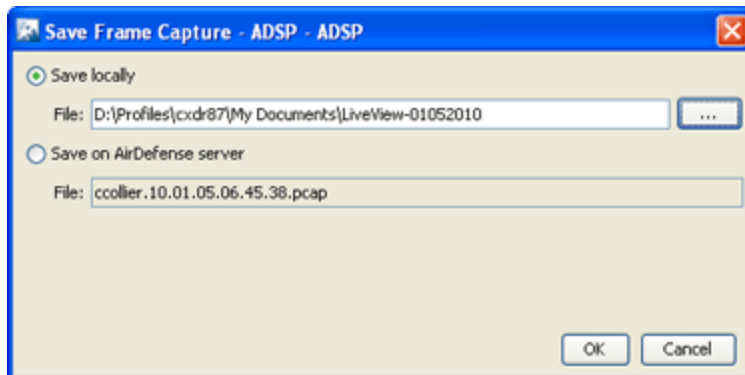
The decodes area shows the 802.11 interpretation of the frame data in a tree structure. The hex values area and decodes area are linked so that selections in one area will follow the selections in the other.

### Frame Capture

There are two ways to capture frames from Live View: manually or automatically using the scheduler.

#### Manual Frame Captures

Live View automatically saves session frame data in a temporary file on your ADSP server. You can save the temporary file to a permanent file on the server or to a file on your workstation. To save a file, first stop the session (click **Stop** button or select **Session > Stop**) and then select **File > Save** to display the **Save Frame Capture** popup window.



To save the file on your workstation:

1. Select the **Save locally** radio button.
2. Click the **Select Destination**— button.
3. Navigate to the folder (directory) where you want to save the file.
4. Type a filename and then click **OK**. The file name along with the path displays in the **File** field.
5. Click **OK**.

To save the file on your ADSP server:

1. Select the **Save on AirDefense server** radio button.

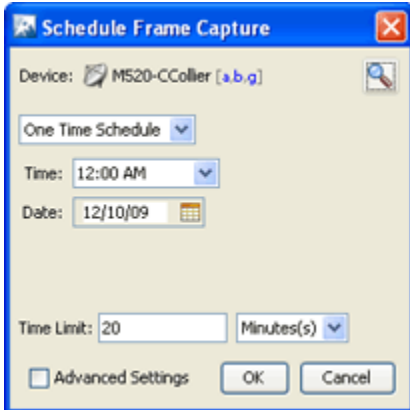
✓ **NOTE** The file name is selected automatically. You cannot change it.

2. Click **OK**.

Once the file is saved, you can view it using [Frame Capture Analysis](#). You can access this feature by selecting **Menu > Frame Capture Analysis**.

### Automatic Frame Captures

You can run automatic frame captures using the AirDefense Services Platform scheduler. Open the Schedule Frame Capture window by selecting **File > Schedule Frame Capture** from the **Live View** window.



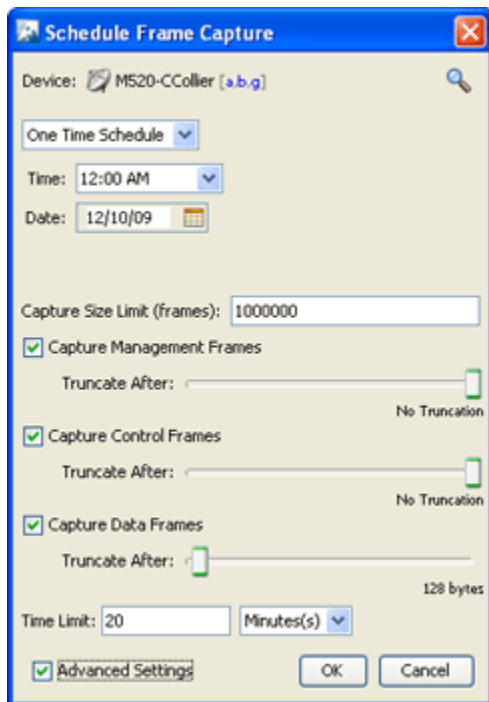
To schedule automatic frame captures, follow these steps:

1. Decide how often you want to run the frame capture by selecting **One Time Schedule**, **Intra-Day Schedule**, **Daily Schedule**, **Weekly Schedule**, or **Monthly Schedule** from the drop-down menu.
2. 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 <b>Time</b> drop-down menu. Then, select a day for the frame capture by clicking the <b>Calendar</b> button in the <b>Date</b> field and selecting a date.
Intra-Day Schedule	Select a time to begin the frame capture. 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 frame capture 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 frame capture 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 frame capture. Last, specify a time of day.

3. Place a time limit on the frame capture by entering the time in the **Time Limit** field; then, select **Minute(s)** or **Hour(s)**.
4. Click **OK** to set the automatic frame capture schedule.

The **Advanced Settings** field adds additional fields to run your frame capture. Just select the **Advanced Settings** checkbox.



There are four additional fields in the **Advance Schedule Frame Capture** window. The steps to set a schedule are the same except you need to set the additional fields. There is a **Capture Size Limit (frames)** field where you can set a limit on how large the captured frame file can grow.

The three other fields are used to truncate the captured frame file for captured:

- Capture Management Frames
- Capture Control Frames
- Capture Data Frames.

If you want to truncate any of the above frames, place a checkmark in the checkbox next to field that you want to truncate. Then, move the sidebar to make your adjustment. Moving the slider to the left reduces amount of bytes to capture. Moving the slider all the way to the right sets the field to no truncation.

If you remove the checkmark from the **Advanced Settings** checkbox, you are returned to the original **Schedule Frame Capture** window.

### ***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.

✓ **NOTE** Location Tracking is not intended to be used on devices that are being terminated.

✓ **NOTE** In order to locate a device, a floor plan must already exist. (See Floor Plan.)

- ✓ **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.

**Importing Maps**

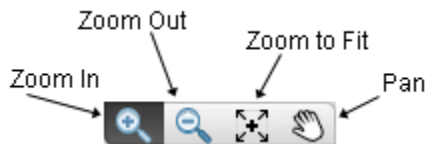
To use the built-in Location Tracking feature, you will need to import a map first and place the sensors at their specific locations.

- ✓ **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. 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.


---

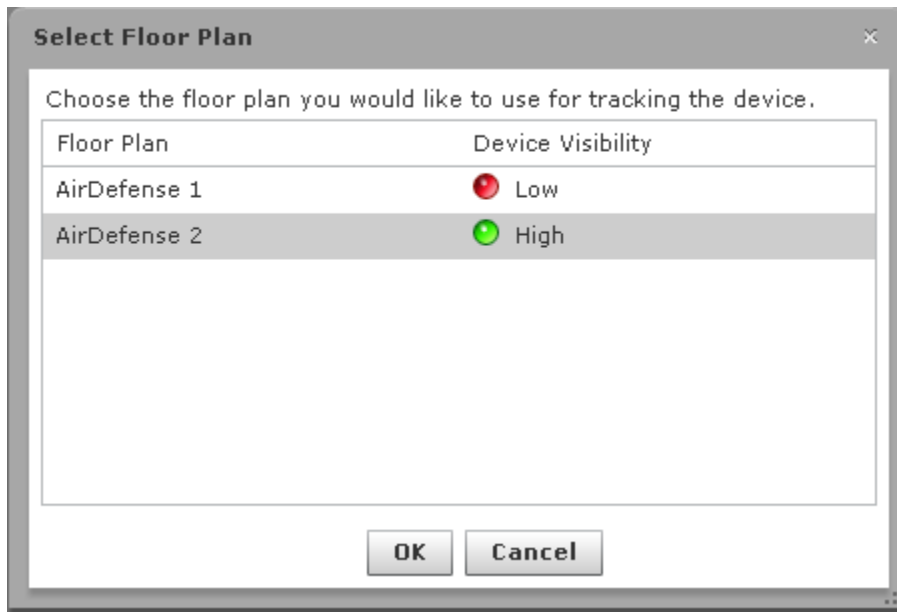
**IMPORTANT**The Floor Plan single dimension limit (width or height) is 8192 pixels while the total pixel count (width x height) limit is 8,000,000 pixels. If the appliance has at least 2GB of memory, the total pixel count may be as high as 16,777,215 pixels but the single dimension limit is still 8192 pixels.

---

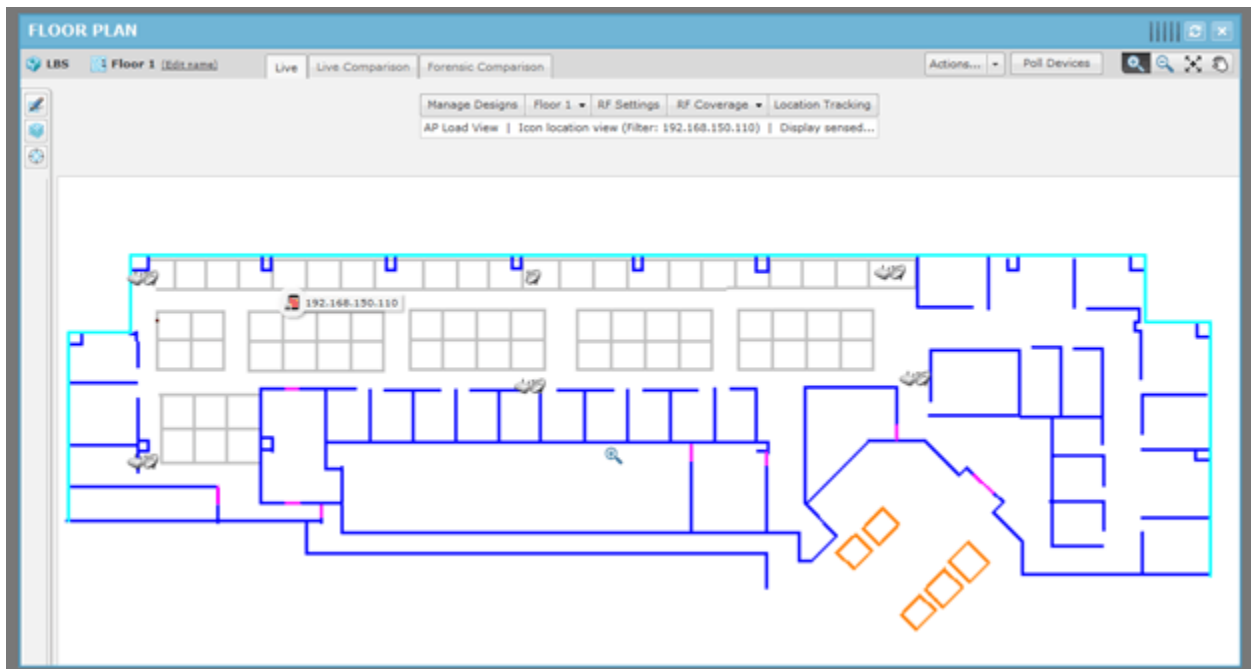
One or more maps or floor plans of the tracking coverage area are needed for this to work. You can obtain floor plans from any source, including producing your own by using drawing tools. Most applications will require multiple maps, for example, if you are setting up multiple buildings. You must supply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

### 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 drop-down menu button—. To track a device, the floor plan (map) must be loaded and sensors positioned on the map).



Select the Floor Plan with the highest visibility and then click **OK**. The Floor Plan displays showing the device being tracked.



Clicking the **Refresh** button will refresh the Floor Plan. If the device has moved, you will see its new position in the Floor Plan.

The Floor Plan is also refreshed automatically (unless turned off) using **Menu > Auto Refresh**. The available refresh rates are:

- 30 seconds
- 1 minute
- 5 minutes.

You can place your cursor over the tracked device to display statistics and information about the device.

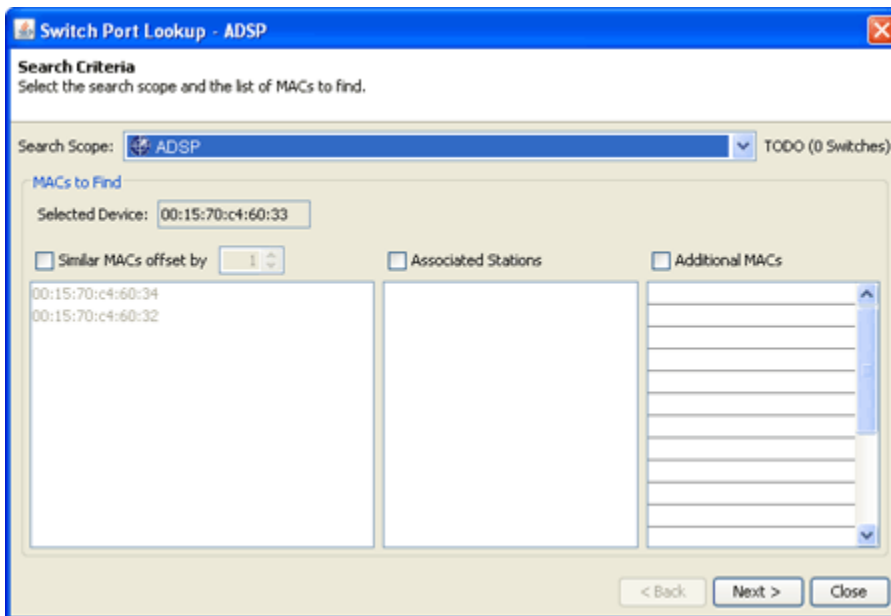
### ***Port Lookup***

Port Lookup allows you to quickly locate the physical port that an authorized/unauthorized device is using to connect to your network. If it is determined that a rogue wireless device is connected to the network, the wired-side port can be shut off to contain the rogue device threat.

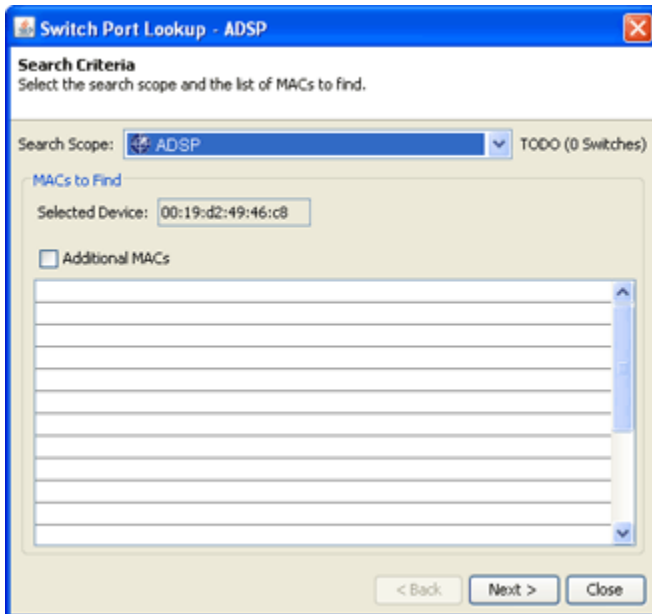
✓ **NOTE** To use this feature, you will need to configure your system with all known managed SNMP switches.



Port Lookup is accessed from a device's drop-down menu and displays the **Switch Port Lookup** window. If the device you select is a BSS, the following window displays:



If the device you select is a Wireless Client, the following window displays:



The following table provides detail on the **Switch Port Lookup** window's functions and features.

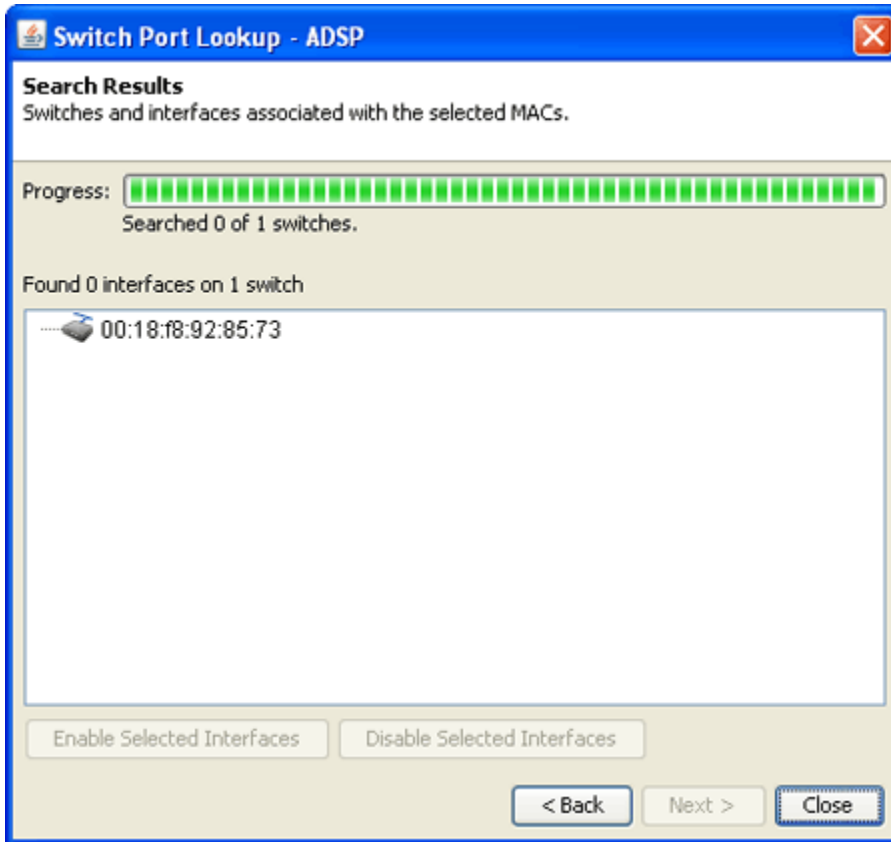
Function/Feature	Description
Search Scope	A drop-down menu that allows you to limit the scope of your search.
Selected Device	A read-only field that displays the MAC address of the selected device.

Function/Feature	Description
Similar MACs offset by	<p>This function appears only if selected device is a BSS. If checked, the search includes other BSSs with a MAC address similar to the selected station. The other stations are listed in the sub-window.</p> <p>Use this function to search for a range of MAC addresses. The range is set by the offset value that you select. For example, suppose you are performing Port Lookup for a device whose last 2 characters are :04, when you select 3 for Add MACs In Range, 3 tiers of MAC Addresses above and below the 04 address appear: 07, 06, 05 -- 04 -- 03, 02, 01.</p> <p>The default offset value is 1.</p>
Associated Wireless Clients	<p>This function appears only if selected device is a BSS. If checked, the search includes Wireless Clients that are connected to the AP. Any connected Wireless Clients are displayed in the sub-window.</p>
Additional MACs	<p>If checked, the search includes any additional MAC addresses that you specify.</p>

### **Performing a Port Lookup**

1. Click the drop-down menu button—drop-down menu button for the suspect device and then select Port Lookup from the menu. The **Switch Port Lookup** window displays.
2. Select the search scope from the **Search Scope** drop-down menu.
3. If the suspect device is a BSS, decide if you want to include a range of similar MAC addresses and/or if you want to include Wireless Clients in your search, and check the appropriate checkbox(es).
4. If you want to include additional MACs in your search, check the **Additional MACs** checkbox and type in the MAC addresses that you want to include.

5. Click **Next**. The following window showing the search results displays.



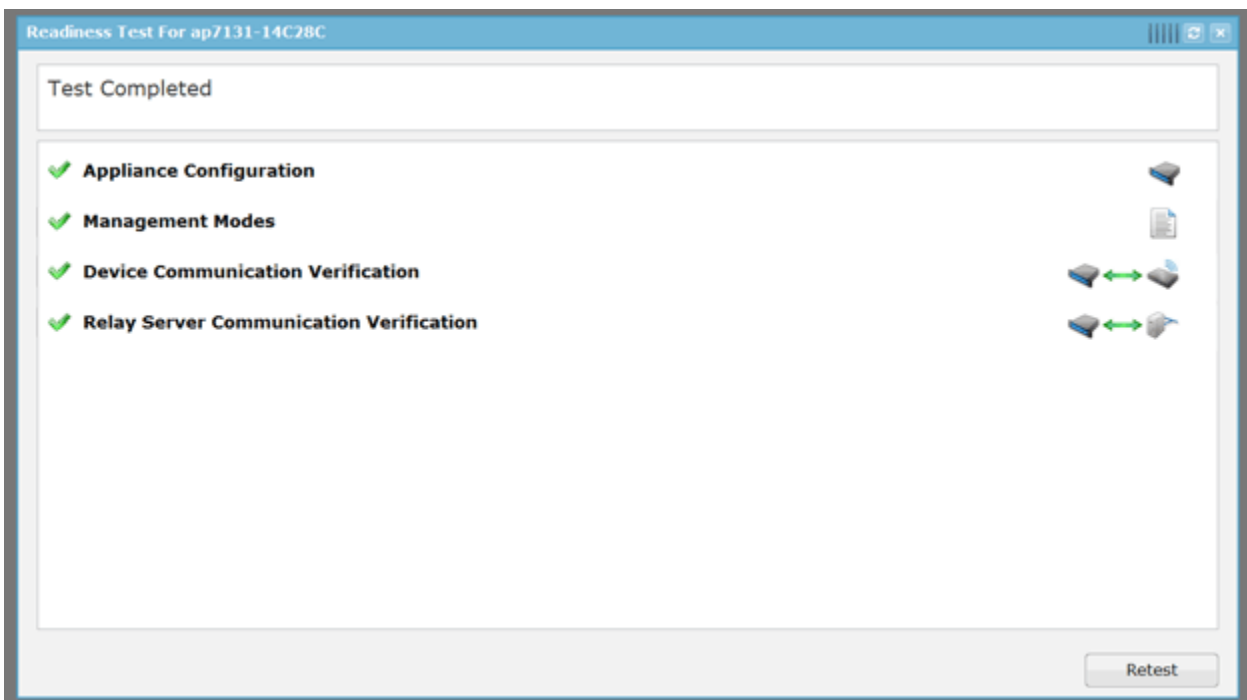
From this window, you can disable or enable a selected (highlighted) interface by clicking the appropriate button.

6. Click **Close** to exit.




### ***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.

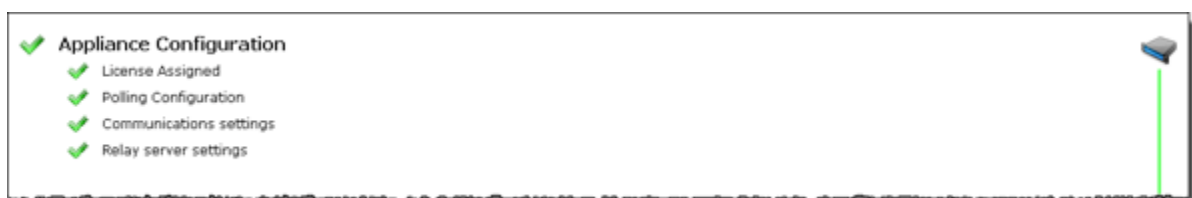
To access the Readiness Test, click **Readiness Test** from the drop-down menu of an AP, a Sensor, a Switch, or a network folder (level). A series of test are run and displayed in a **Readiness Test** overlay.



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. You can click on any category to display the tests for that category. If a test is marked as a problem or caution area, you can click on the test to navigate to the problem area and take action to correct the problem.

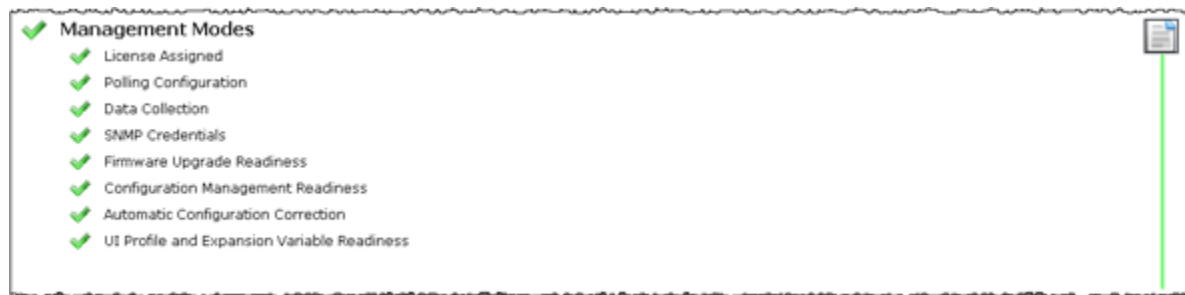
- Appliance Configuration



There are four tests for Appliance Configuration:

- License Assigned—validates that the number of licenses do not exceed the number of configured devices.
- Polling Configuration—validates that the folder or device selected inherits a configured polling profile.
- Communications settings—validates that the folder or device selected inherits a configured communication settings profile.
- Relay server settings—validates that the folder or device selected inherits a configured relay server profile.

- Management Modes



There are eight tests for Management Modes:

- License Assigned—validates that the number of licenses do not exceed the number of configured devices.
- Polling Configuration—validates that the folder or device selected inherits a configured polling profile.
- Data Collection—validates that data collection is enabled when polling.
- SNMP Credentials—validates that the SNMP credentials are supplied for the communications settings.
- Firmware Upgrade Readiness—validates that firmware upgrades are in place and ready to be applied.
- Configuration Management Readiness—validates that device configuration management is enabled for the communications settings.

✓ **NOTE** A WS5100 running 2.1.4.0-001R is limited to discovery and upgrade. If you run the Readiness Test on this device, you will get a false result indicating the device has passed Configuration Management Readiness. This is also true for WiNG 5.0 and 5.1.x devices.

- Automatic Configuration Correction—validates that configuration compliance violations are automatically corrected when polling.
  - UI Profile and Expansion Variable Readiness—validates that the folder or device selected inherits UI profiles and that the expansion variables exists for the profiles. UI profiles include Channel Settings, Device Access, Radio Settings, RF-Domain, WLAN Profiles.
- Device Communication Verification



There are three tests for Device Communication Verification:

- SNMP Connection—validates that the folder or device selected inherits credentials for SNMP access to the device(s). Test is successful only if valid data can be returned.
- CLI Connection—validates that ADSP can communicate with the selected device via the CLI.
- HTTP Connection—validates that ADSP can communicate with the selected device via HTTP.

- Relay Server Communication Verification



There are five tests for Relay Server Communication Verification:

- Relay server settings—validates that the folder or device selected inherits a configured relay server profile.
- Relay Server Connection Test—validates that the relay server can be reached.
- Relay Server Upload Test—validates that the relay server can upload CLI profiles.
- Relay Server Download Test—validates that the relay server can download CLI profiles.
- Relay Server Delete Test—validates that the relay server can delete CLI profiles.

### ***Spectrum Analysis***

- ✓ **NOTE** A Spectrum Analysis license is required to access this feature.

Spectrum Analysis gives you a tool to identify and locate interference sources on your wireless network. You must possess a valid Spectrum Analysis license from Motorola AirDefense for each Sensor that you wish to conduct an analysis from.

Spectrum Analysis supports two modes of operation:

- Background Analysis
- Dedicated Analysis.

### **Background Analysis**

When enabled, background analysis continually scans for interference sources as part of the normal scan pattern. An alarm is generated when interference is detected.

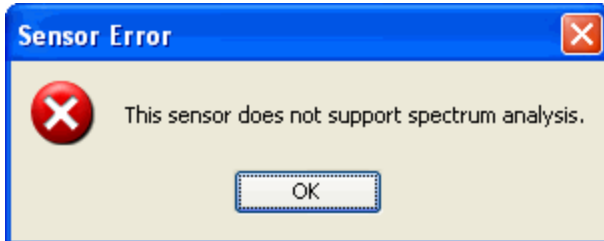
There are two ways to turn on background analysis:

- When a Spectrum Analysis license is applied to a Sensor, you are given an option to enable background scanning.
- In the **Sensor Operation** settings of the **Sensor Monitoring** category under the **Configuration** tab, there is an option to enable background scanning.

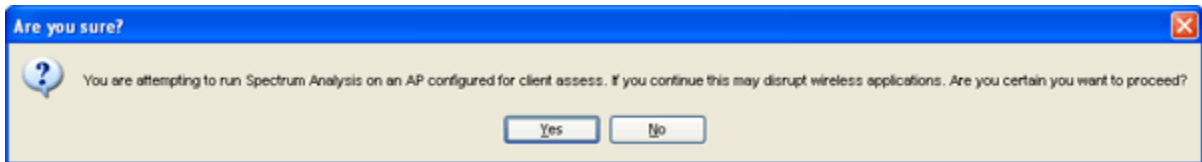
### Dedicated Analysis

Dedicated analysis disables the normal scan pattern for a Sensor. Then, it conducts a detailed spectrum scan and displays the results in the **Spectrum View** window.


The **Spectrum View** window can only be accessed if the selected Sensor is licensed for Spectrum Analysis. If the Sensor does not support Spectrum Analysis, the following error popup is displayed:

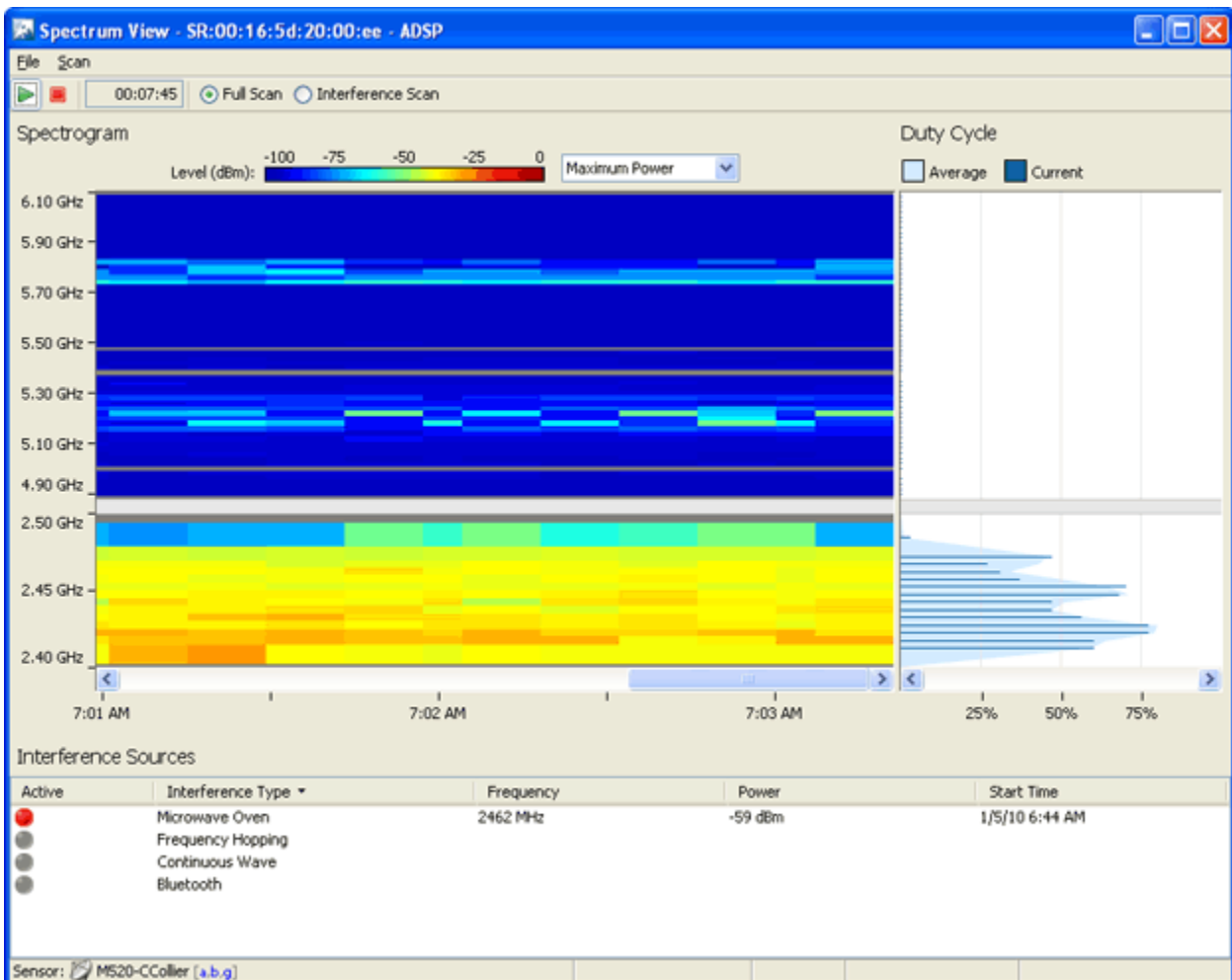


In addition, if you attempt to run Spectrum Analysis on an AP configured for client access (device configured as AP and Sensor), the following error popup may display:



This usually will happen if you only have one radio turned on. If you continue, your wireless application may be disrupted but Spectrum Analysis will run.

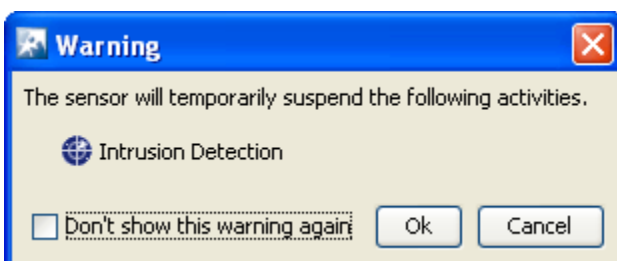
To access the **Spectrum View** window, click the drop-down menu button— for a Sensor and then select **Spectrum Analysis** from the drop-down menu.



Select **File > Close** to exit the **Spectrum View** window. You will be prompted to save the scan to an ADSP file. An ADSP file can be opened by navigating to **Menu > Open > Spectrum Analysis**.

### Scanning

A dedicated scan starts automatically when the **Spectrum View** window is opened. You are given a warning to alert you that running a dedicated scan will temporarily suspend Intrusion Detection.



You must click **OK** to continue. You can turn the warning off by selecting the checkbox next to **Don't show this warning again**.

There are three conditions that may prevent a scan from starting. They are:

- The Sensor is already running a dedicated RF scan for any user

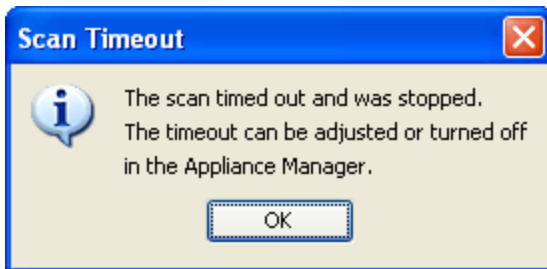


- Another user is running Live View on the Sensor
- Ten scans are already running (maximum supported).

You can stop a scan by clicking the **Stop Scan**— button or selecting **Scan > Stop Scan**. A scan can be restarted by clicking the **Start Scan**— button or selecting **Scan > Start Scan**.

A counter is displayed next to the **Stop Scan** button to show how long the scan has been running.

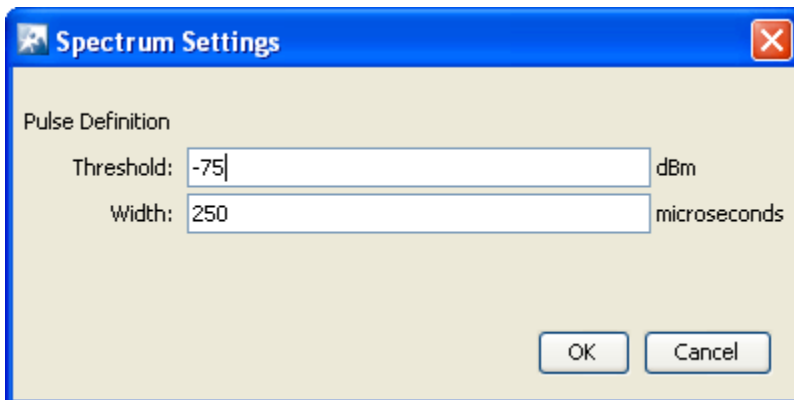
The default scanning time is 10 minutes. Scanning time can be adjusted by selecting **Configuration > Appliance Management > Appliance Settings**. If a timeout occurs, the following **Scan Timeout** popup is displayed:



Click **OK** to close the popup.

### Spectrum Settings

Spectrum View lets you adjust the pulse definition via the **Spectrum Settings** window. To access the Spectrum Settings, select **File > Settings**.



As you can see, there are two fields for pulse definition: **Threshold** and **Width**. You can adjust the pulse threshold by typing in a new value in dBm. You can adjust the pulse width by typing in a new value in microseconds. Click **OK** to set the new values and close the window.

### Scanning Modes

There are two scanning modes: Full Scan and Interference Scan. The Full Scan scans the entire 2.5GHz bandwidth (in 5MHz steps) and 5GHz bandwidth (in 20MHz steps) with a short dwell time (around 50 ms). Full Scan supports limited classification of interference sources. The Interference Scan scans three frequencies in the 2.5GHz band and three frequencies in the 5GHz band with a longer dwell time (around 500 ms). Interference Scan supports classification for all interference sources. To select a mode, select the appropriate radio button or select a mode from the **Scan** menu.

### Spectrogram

The spectrogram shows the average power level measured at each of the frequencies in the scan settings over a period of time. The graph is cleared when a scan starts and updates regularly as data becomes available during the scan.

When a scan starts, data starts showing in the right side of the graph. As new data is scanned, the older data moves to the left. Once the graph is full, a horizontal scrollbar becomes visible.

You can display the frequency and power value by moving the cursor over points in the graph.

The Duty Cycle chart shows the duty cycle values for the most recent time slice and an average of the duty cycles across all time slices. When the cursor is placed over the Duty Cycle chart, the frequency and duty value is highlighted and displayed. Also, the status bar displays the frequency, duty value, average power, and average pulse power.

You can adjust the size of the **Spectrogram** and **Duty Cycle** chart by clicking and dragging the divider (left or right) between them. The size of the charts may be adjusted along the X axis by dragging a divider which is shown between the spectrogram and the duty cycle chart.

### Interference Sources

The Interference Sources table lists:

- Whether the interference source is active (red ball) at the moment or not (gray ball)

✓ **NOTE** An alarm is generated whenever an interference source is detected.

- The name of the interference source:
  - Microwave Oven
  - Frequency Hopping
  - Continuous Wave
  - Bluetooth
- The frequency of the interference source
- The power of the interference source
- The time when the interference source was first detected.


Each time a scan is started, the table clears and is updated when data becomes available.

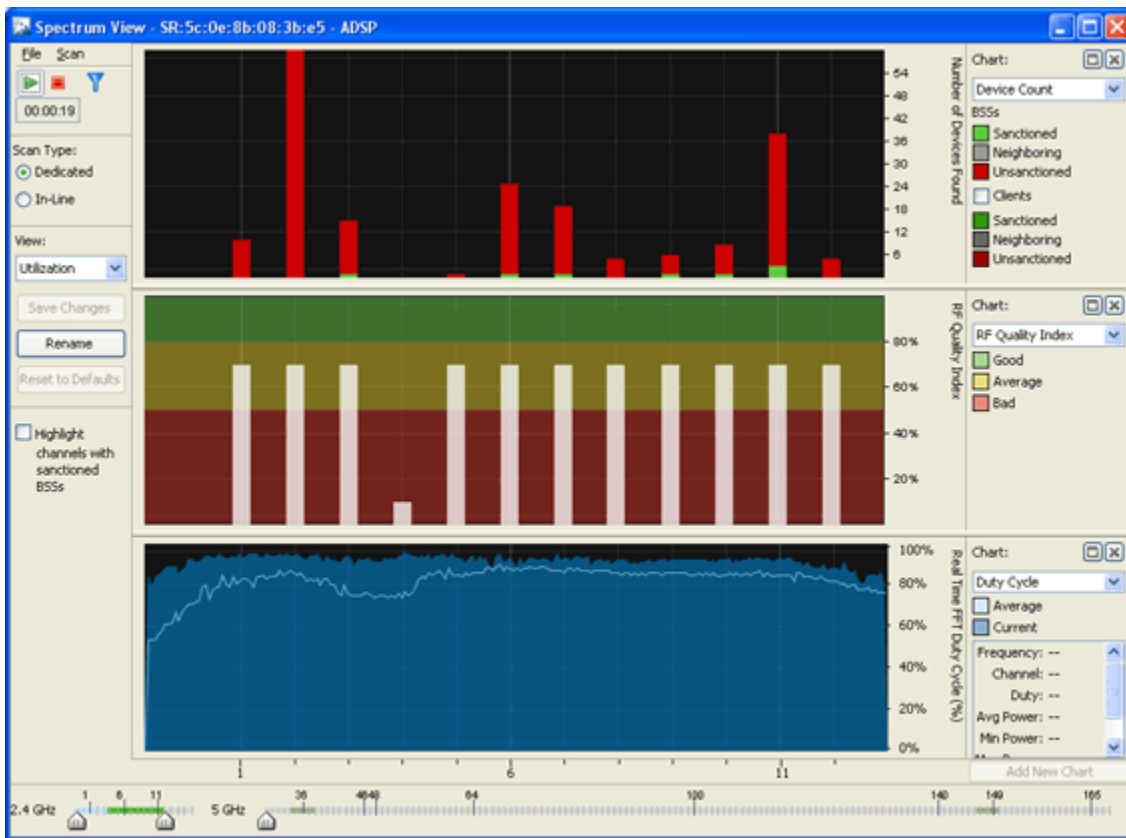
### Advanced Spectrum Analysis

✓ **NOTE** A Spectrum Analysis license is required to access this feature.

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. Currently, only the Motorola AP621, AP622, AP6511, AP6521, AP6522, and AP8132 can run this enhanced version of Spectrum Analysis.

✓ **NOTE** If an AP6521 is configured in the AP/radioshare mode, Advanced Spectrum Analysis will only run if the **Scan Type** is **In-Line**.

The new version of Spectrum Analysis is accessed the same way. Just click the drop-down menu button—  for a Sensor and then select **Spectrum Analysis** from the drop-down menu.



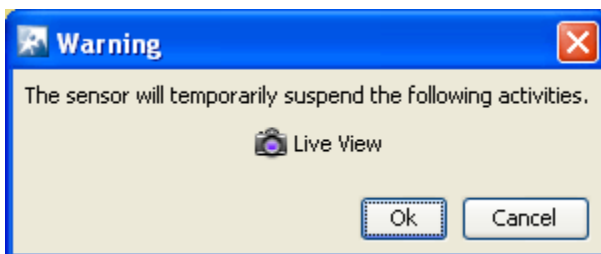
Select **File > Close** to exit the **Spectrum View** window. You will be prompted to save the scan to an ADSP file. An ADSP file can be opened by navigating to **Menu > Open > Spectrum Analysis**.

### Scanning



A dedicated scan starts automatically when the **Spectrum View** window is opened. There are three conditions that may prevent a scan from starting. They are:

- The Sensor is already running a dedicated RF scan for any user
- Another user is running Live View on the Sensor
- Ten scans are already running (maximum supported).

If one of these conditions exists, a warning similar to this is displayed:

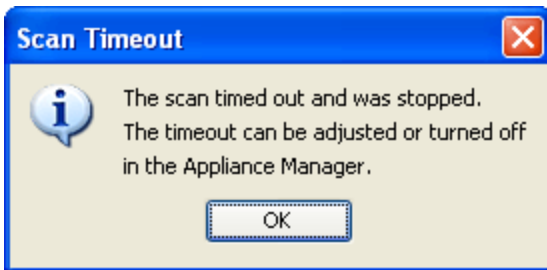


To continue, you will have to click **OK** to suspend the activity. Clicking **Cancel** will stop Advanced Spectrum Analysis from running.

You can stop a scan by clicking the **Stop Scan**— button or selecting **Scan > Stop Scan**. A new scan can be started by clicking the **Start Scan**— button or selecting **Scan > Start Scan**.

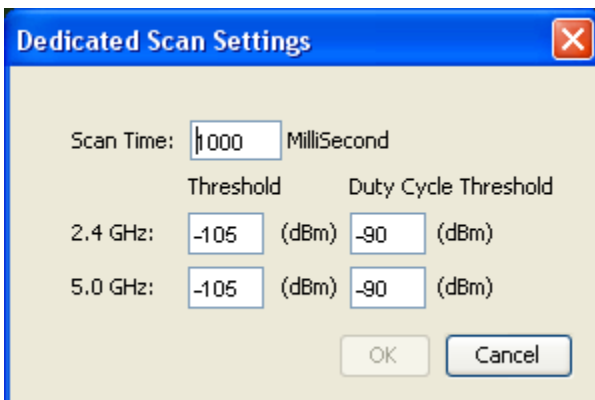
A counter is displayed next to the **Stop Scan** button to show how long the scan has been running.

The default scanning time is 10 minutes. Scanning time can be adjusted by selecting **Configuration > Appliance Management > Appliance Settings**. If a timeout occurs, the following **Scan Timeout** popup is displayed:



Click **OK** to close the popup.

You can change the scan time, threshold, or duty cycle for dedicated scans by navigating to **File > Dedicated Scan Settings**.



The scan time (default 1000) should be entered in milliseconds. The threshold (default -105 for 2.4 and 5 GHz) and duty cycle (default -90 for 2.4 and 5 GHz) should be entered in dBm. After making changes, click **OK** to confirm the changes or click **Cancel** to discard any changes.

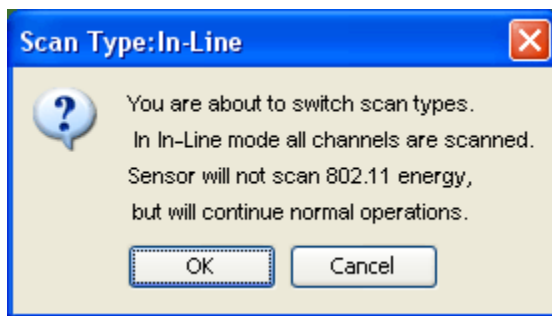
### Scan Type

Advanced Spectrum Analysis supports two types of scans:

- Dedicated Scan—Conducts a full detailed spectrum scan (default).
- In-Line Scan—Conducts a spectrum scan of all channels minus 802.11 details.

✓ **NOTE** To conduct an In-Line Scan, you must enable location tracking RSSI scan under **Configuration > Operational Management > Sensor Operation** and set the refresh rate to 1 second.

You can change the scan type by selecting the appropriate radio button. When the scan type is changed, a warning is displayed.



Click **OK** to confirm the scan type change.

### Views

Advanced Spectrum Analysis has the following four views that display default charts for each view:

- Utilization—Displays charts that show 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 that show interference sources in your network. The default charts are:
  - Interference
  - Spectral Density.
- Spectrum Detail—Displays charts that show the spectrum details of your network. The default charts are:
  - Spectrogram
  - Real Time FFT (Fast Fourier Transform)
  - Spectral Density.

You can change which charts are displayed for each view using the **Charts** drop-down menu. Once you have changed charts and you want to save the changes, click the **Save Changes** button.

You can change the name of a view by clicking the **Rename** button. This allows you to name the views according to your needs. If for any reason you want to retrieve the default views, you can do so by clicking the **Reset to Defaults** button.



Selecting the **Highlight channels with sanctioned BSSs** checkbox highlights the channels with sanctioned BSSs in all the charts.


### Chart Manipulation

The following chart manipulations are available:

You can display a maximum of 3 charts. If only one or two charts are displayed, click the **Add New Chart** button to add another chart. If three charts are displayed the **Add New Chart** button is inactive.

You can change a chart's height, by dragging the bar between the charts up or down.

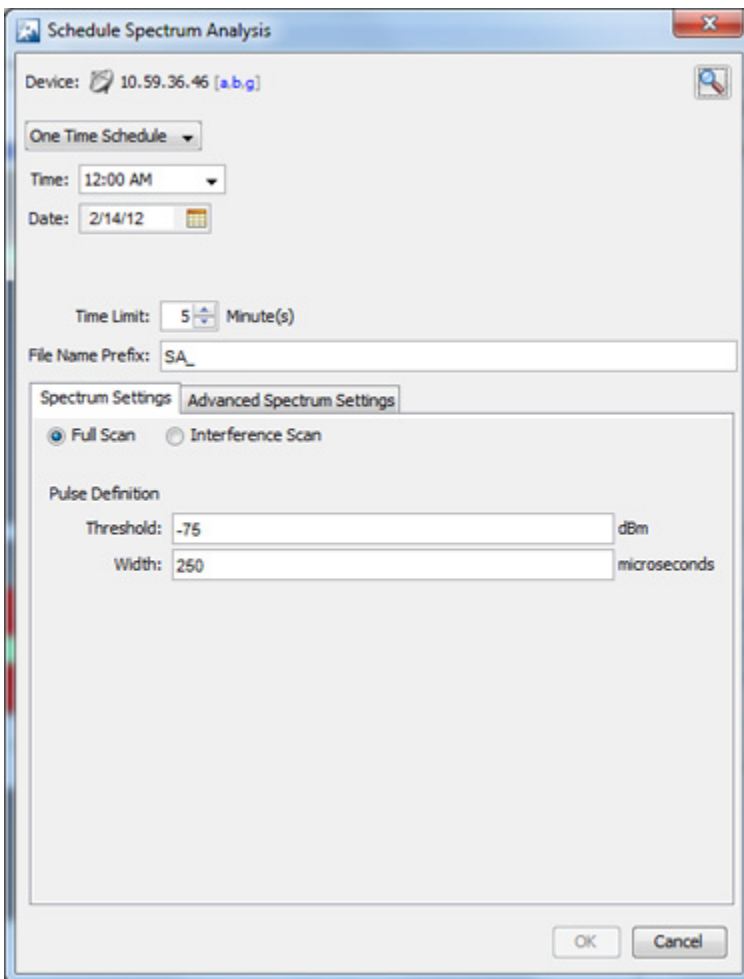
You can expand a chart to fill the entire chart area by clicking the **Expand**— button. Click the **Restore**— button to restore a chart to its original size.

You can remove a chart from the chart area by clicking the **Close**— button.

The 2.4 and 5 GHz channel views are controlled by the sliders at the bottom of the window. The entire 2.4 GHz range is selected by default. By default, no channels in the 5 GHz range are selected.

### **Schedule Spectrum Analysis**

You can schedule Spectrum Analysis for regular Spectrum Analysis or Advanced Spectrum Analysis by selecting **File > Schedule Spectrum Analysis**.



The fields used to schedule a Spectrum Analysis are:

Field	Description
Schedule	<p>There are five options to schedule an assessment. Depending on the option you select, you must fill in the related fields as follows:</p> <ul style="list-style-type: none"> <li>• One Time Schedule—Choose a time for the assessment by selecting a time from the <b>Time</b> drop-down menu. Then, select a day for the assessment by clicking the Calendar button in the Date field and selecting a date.</li> <li>• Intra-Day Schedule—Select a time to begin the assessment. Then, select a frequency in hours.</li> <li>• Daily Schedule—Select a frequency in day, weekdays only, or weekends only. Then, select a time of day.</li> <li>• Weekly Schedule—Choose a frequency in days. Then, select a day or multiple days to conduct the assessment by clicking the checkbox next to the day to place a checkmark in the box.</li> <li>• Monthly Schedule—Choose the months that you want to run a assessment 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 assessment. Last, specify a time of day.</li> </ul>
Time Limit	Places a time limit on how long the Spectrum Analysis will run.
File Name Prefix	Defines a prefix for the Spectrum Analysis (ADSA) file that is saved when the Spectrum Analysis is complete. You may add to the prefix if you want to. The saved file can be opened by selecting <b>Menu &gt; Open &gt; Spectrum Analysis</b> .
Spectrum Settings	Only used in regular Spectrum Analysis. These are the same <b>Spectrum Settings</b> described under <a href="#">Dedicated Analysis</a> .
Advanced Spectrum Settings	Only used in Advanced Spectrum Analysis. These are the <b>Dedicated Scan Settings</b> described under <a href="#">Advanced Spectrum Analysis</a> .

You can switch devices by clicking **Search** button.

Device Search- ADSP

Scope: ADSP

Criteria

MAC Address: [dropdown]

Name: [text box]

IP Address: [text box]

802.1x Username: [text box]

Vendor: [text box]

DNS Name: [text box]

SSID: [text box]

Supports 802.11a:  Yes  No  Either

Supports 802.11b:  Yes  No  Either

Supports 802.11g:  Yes  No  Either

Supports 802.11n:  Yes  No  Either

Search Now

New Search

Results:

Close

When searching, you can supply additional information such as:

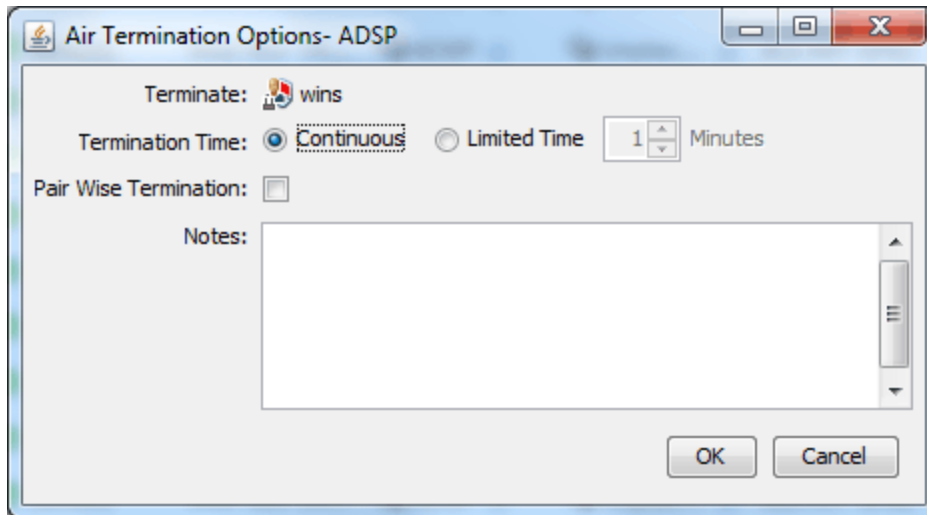
- Select the scope from the network tree
- The MAC address of the device
- The name of the device
- The IP address of the device
- The 802.1x username used for authentication
- The vendor name of the device
- The DNS name used by the device
- The SSID of the device
- Select whether or not the device supports the 802.11a, b, g, or n protocols.

Once you have entered the search criteria, click the **Search Now** button. The results are displayed in the **Results** area. Select the device that you want to run Spectrum Analysis on and then click **Close**.



### *Terminate*

The AirDefense Services Platform lets you terminate the connection between your wireless LAN and any BSS or Wireless Client associated with it. In the case of BSSs, all Wireless Clients associated to the BSS are de-authenticated.




## Network Levels

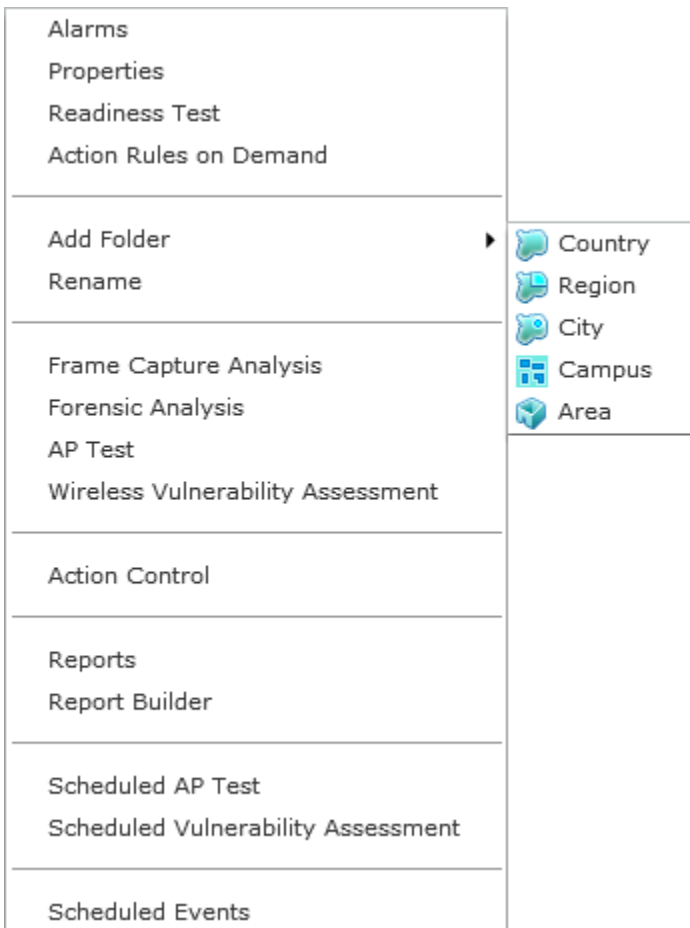
Network Level drop-down menus contain functions that operate on the selected network level. These drop-down menus are available throughout AirDefense Service Platform. The network levels are:

- Appliance
- Country
- Region
- City
- Campus
- Building
- Floor.

The Appliance network level displays by default. The other network levels must be defined in **Configuration > Appliance Platform > Tree Setup**.

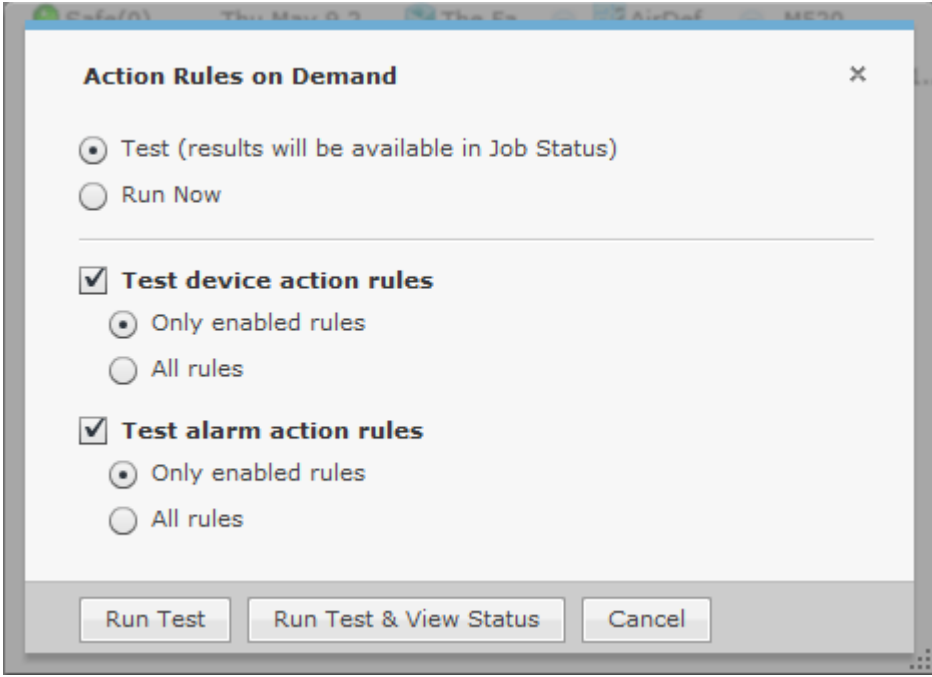
## Appliance

The Appliance drop-down menu contains functions that you can apply to the selected Appliance as well as the standalone features included in the Menu. Click the drop-down menu button— next to the Appliance name to display the drop-down menu.




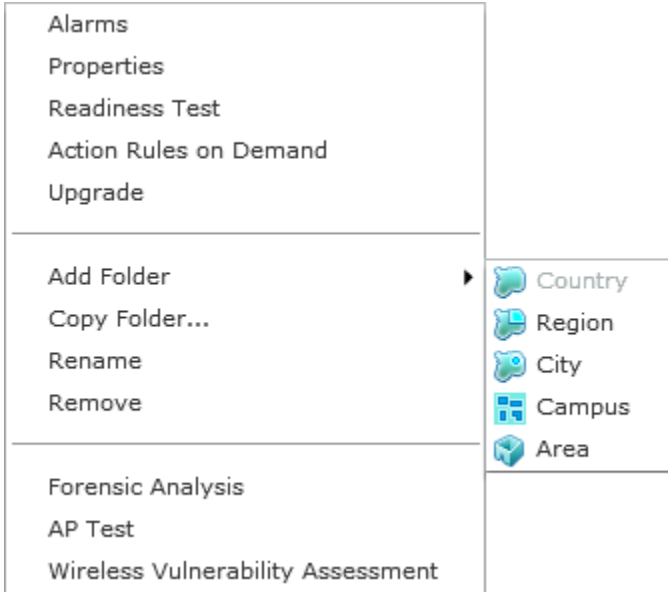
The drop-down menu for appliances contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Appliance.
Properties	Opens the <b>Properties</b> 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. (See <a href="#">Readiness Test</a> for more information.)

Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in <a href="#">Job Status</a>, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> <li>• Only enabled rules—run test on the enabled rules.</li> <li>• All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.</li> </ul>
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 <a href="#">Frame Capture Analysis</a> .
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
AP Test	Accesses <a href="#">Scheduled AP Test</a> .
Wireless Vulnerability Assessment	Accesses <a href="#">Scheduled Vulnerability Assessment</a> .
Action Control	Accesses <a href="#">Action Control</a> .
Reports	Accesses Reports ( <a href="#">Using Web Reporting</a> ).
Report Builder	Accesses the Report Builder ( <a href="#">Using the Report Builder</a> ).
Scheduled AP Test	Accesses <a href="#">Scheduled AP Test</a> .
Scheduled Vulnerability Assessment	Accesses <a href="#">Scheduled Vulnerability Assessment</a> .
Scheduled Events	Accesses <a href="#">Scheduled Events</a> .

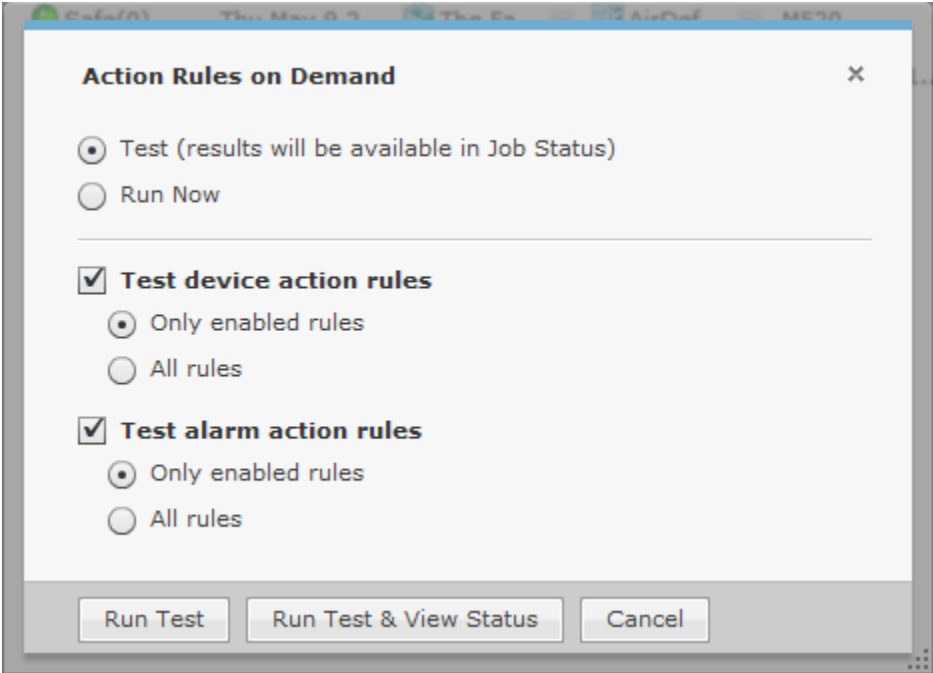
## Country

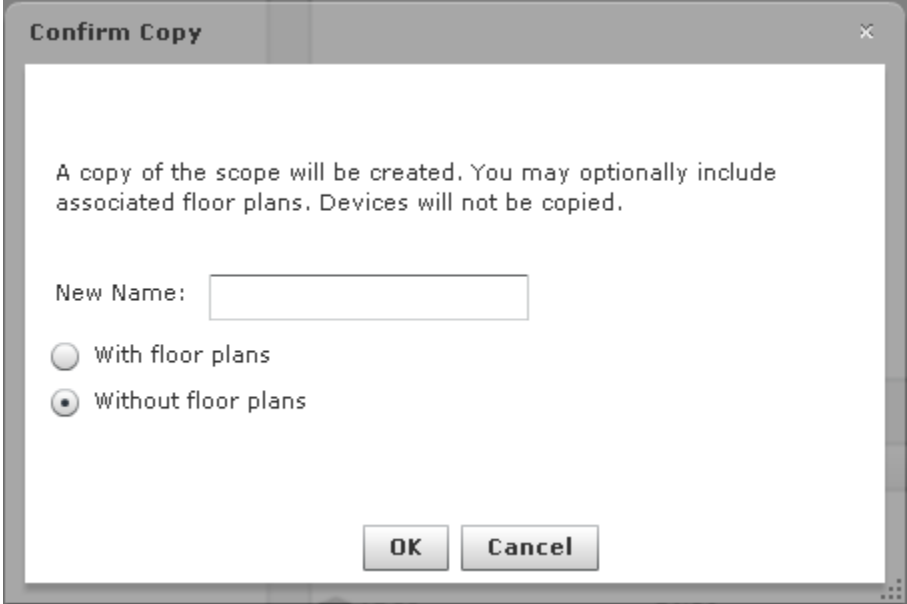
The Country level drop-down menu contains functions that you can apply to the selected Country level. Click the drop-down menu button— next to the Country name to display the drop-down menu.




The drop-down menu for countries contains the following functions:

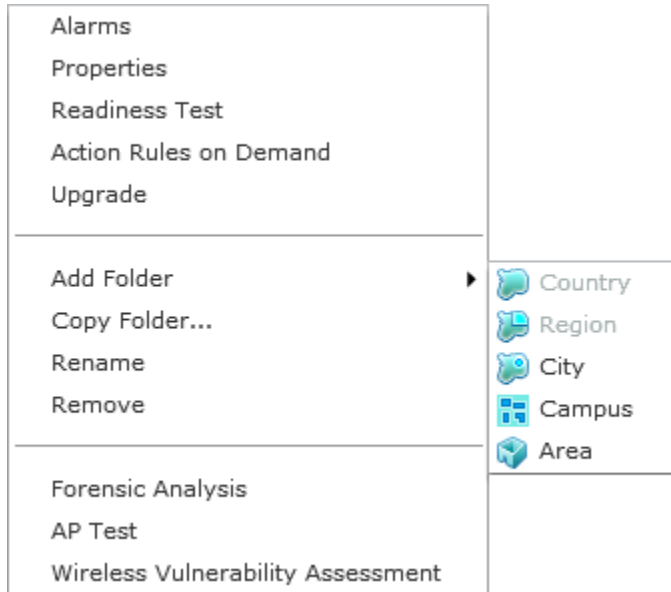
Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Country.
Properties	Opens the Properties overlay for the selected Country.
Readiness Test	Validates that devices in the country scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas. You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)

Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in <a href="#">Job Status</a>, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> <li>• Only enabled rules—run test on the enabled rules.</li> <li>• All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.</li> </ul>
Upgrade	Upgrades the firmware for devices in the selected Country. (See <a href="#">Upgrade Devices</a> for more information.)
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.

Function	Description
Copy Folder	<p>Copies the network scope of a Country.</p>  <p>Enter a name for the country, select if you want the to include the floor plans or not, and click <b>OK</b>.</p>
Rename	Opens a dialog window to rename the selected Country.
Remove	Removes the selected Country from your network. (See <a href="#">Remove Devices</a> for more information.)
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
AP Test	Accesses AP Test. ( <a href="#">Scheduled AP Test</a> )
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment. ( <a href="#">Scheduled Vulnerability Assessment</a> )

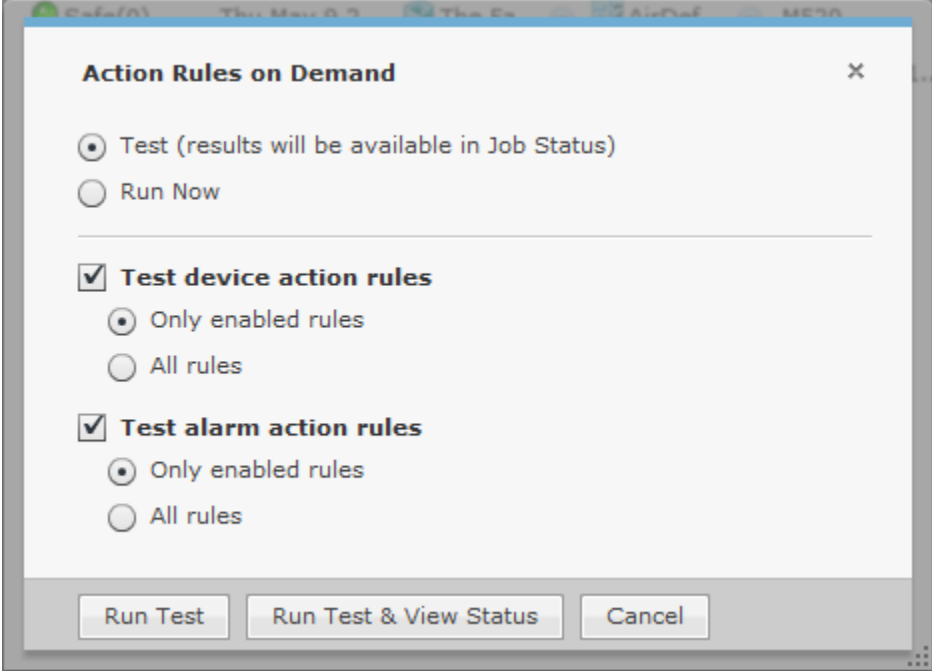
## Region

The Region level drop-down menu contains functions that you can apply to the selected Region level. Click the drop-down menu button— next to the Region name to display the drop-down menu.

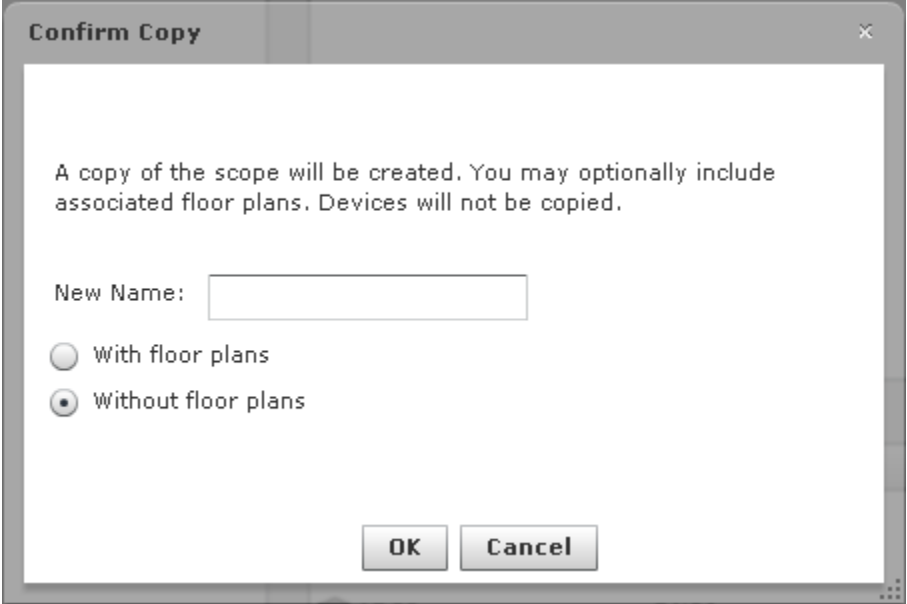


The drop-down menu for regions contains the following functions:


Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Region.
Properties	Opens the <b>Properties</b> 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. You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)

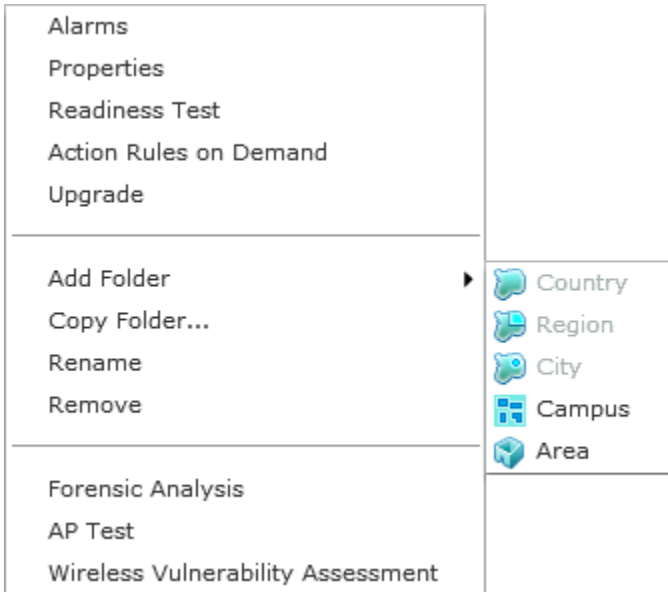
Function	Description
<p>Action Rules on Demand</p>	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in <a href="#">Job Status</a>, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> <li>• Only enabled rules—run test on the enabled rules.</li> <li>• All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.</li> </ul>
<p>Upgrade</p>	<p>Upgrades the firmware for devices in the selected Region. (See <a href="#">Upgrade Devices</a> for more information.)</p>
<p>Add Folder</p>	<p>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.</p>



Function	Description
Copy Folder	<p>Copies the network scope of a Region.</p>  <p>Enter a name for the region, select if you want the to include the floor plans or not, and click <b>OK</b>.</p>
Rename	Opens a dialog window to rename the selected Region.
Remove	Removes the selected Region from your network. (See <a href="#">Remove Devices</a> for more information.)
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
AP Test	Accesses AP Test ( <a href="#">Scheduled AP Test</a> ).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment ( <a href="#">Scheduled Vulnerability Assessment</a> ).

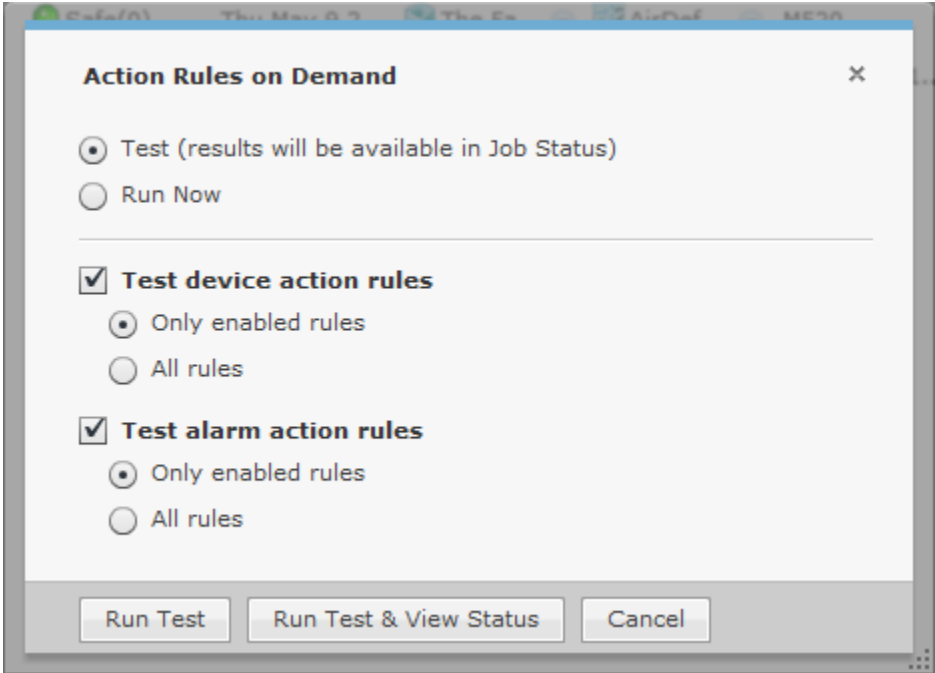
## City

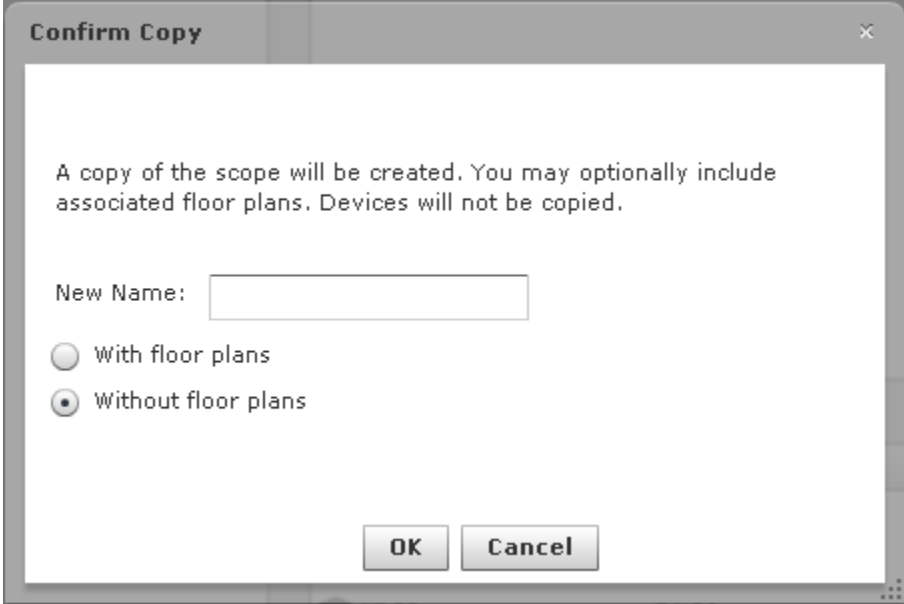
The City level drop-down menu contains functions that you can apply to the selected City level. Click the drop-down menu button— next to the City name to display the drop-down menu.




The drop-down menu for cities contains the following functions:

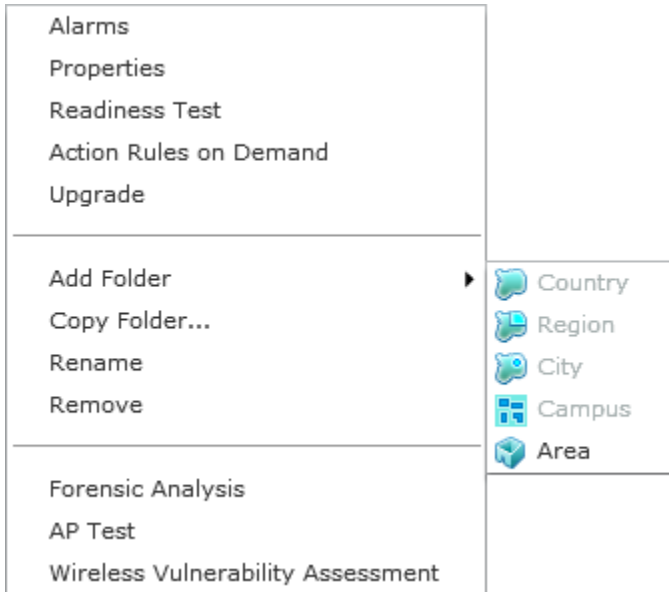
Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected City.
Properties	Opens the <b>Properties</b> overlay for the selected City.
Readiness Test	Validates that devices in the city scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)

Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in <a href="#">Job Status</a>, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> <li>• Only enabled rules—run test on the enabled rules.</li> <li>• All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.</li> </ul>
Upgrade	Upgrades the firmware for devices in the selected City. (See <a href="#">Upgrade Devices</a> for more information.)
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.

Function	Description
Copy Folder	<p>Copies the network scope of a City.</p>  <p>Enter a name for the city, select if you want the to include the floor plans or not, and click <b>OK</b>.</p>
Rename	Opens a dialog window to rename the selected City.
Remove	Removes the selected City from your network. (See <a href="#">Remove Devices</a> for more information.)
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
AP Test	Accesses AP Test ( <a href="#">Scheduled AP Test</a> ).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment ( <a href="#">Scheduled Vulnerability Assessment</a> ).

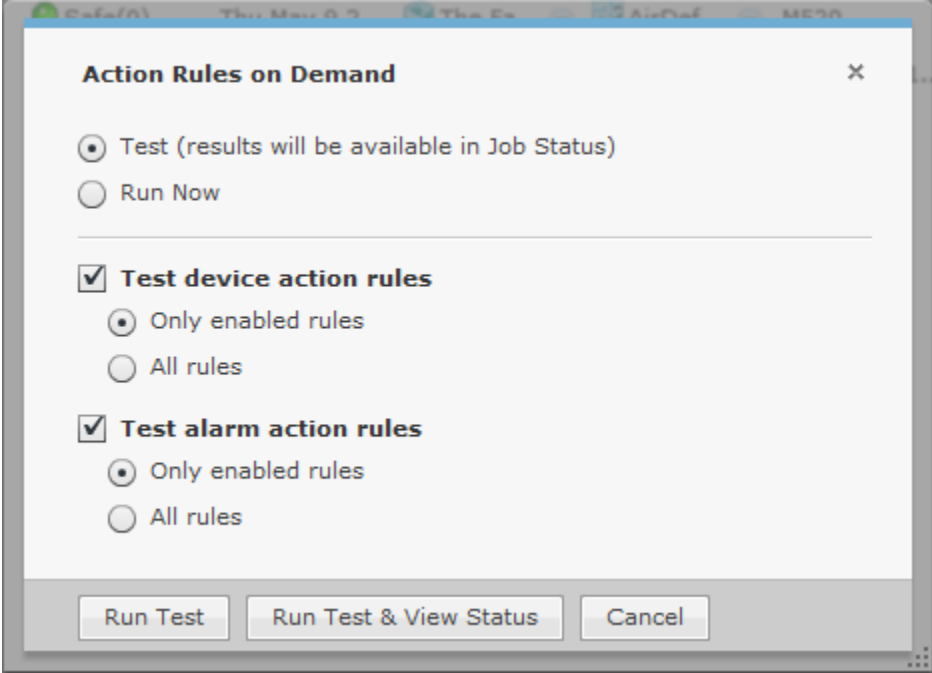
## Campus

The Campus level drop-down menu contains functions that you can apply to the selected Campus level. Click the drop-down menu button— next to the Campus name to display the drop-down menu.




The drop-down menu for campuses contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Campus.
Properties	Opens the <b>Properties</b> overlay for the selected Campus.
Readiness Test	Validates that devices in the campus scope are management ready (that is, devices can be managed through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)

Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in <a href="#">Job Status</a>, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> <li>• Only enabled rules—run test on the enabled rules.</li> <li>• All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.</li> </ul>
Upgrade	Upgrades the firmware for devices in the selected Campus. (See <a href="#">Upgrade Devices</a> for more information.)
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.

Function	Description
Copy Folder	<p data-bbox="537 300 992 327">Copies the network scope of a Campus.</p> <div data-bbox="537 346 1438 947" style="border: 1px solid gray; padding: 10px;"> <p data-bbox="565 365 737 392"><b>Confirm Copy</b> <span style="float: right;">✕</span></p> <p data-bbox="591 506 1308 562">A copy of the scope will be created. You may optionally include associated floor plans. Devices will not be copied.</p> <p data-bbox="591 625 721 653">New Name: <input data-bbox="745 619 1062 663" type="text"/></p> <p data-bbox="591 684 805 711"><input type="radio"/> With floor plans</p> <p data-bbox="591 730 841 758"><input checked="" type="radio"/> Without floor plans</p> <p data-bbox="899 869 1133 911" style="text-align: right;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div> <p data-bbox="537 957 1487 1014">Enter a name for the campus, select if you want the to include the floor plans or not, and click <b>OK</b>.</p>
Rename	Opens a dialog window to rename the selected Campus.
Remove	Removes the selected Campus from your network.
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
AP Test	Accesses AP Test ( <a href="#">Scheduled AP Test</a> ).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment ( <a href="#">Scheduled Vulnerability Assessment</a> ).

### Area

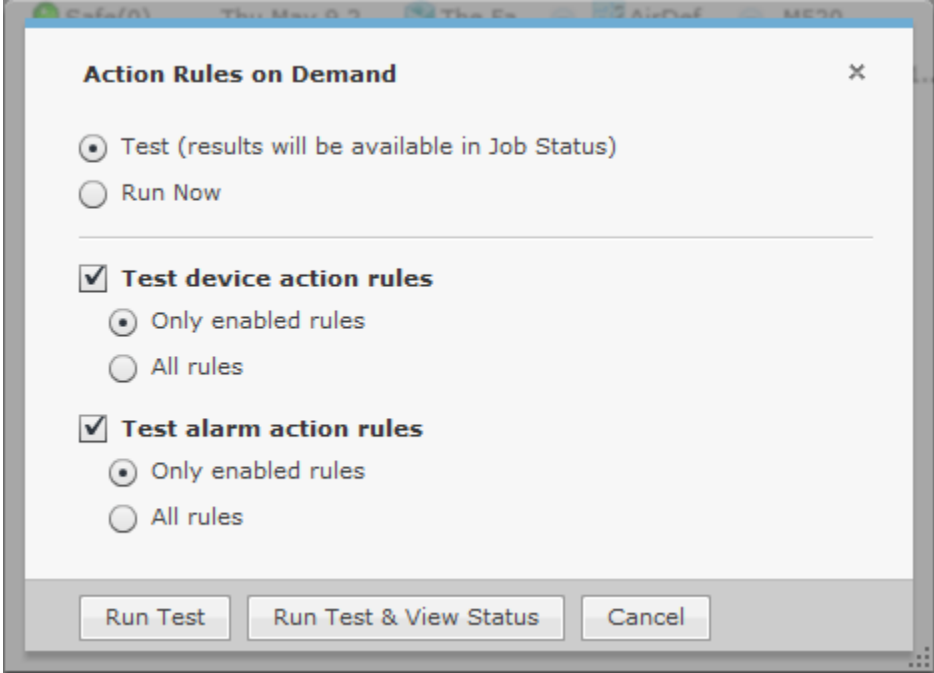
The Area (Building) level drop-down menu contains functions that you can apply to the selected Area level. Click the drop-down menu button— next to the Area name to display the drop-down menu.

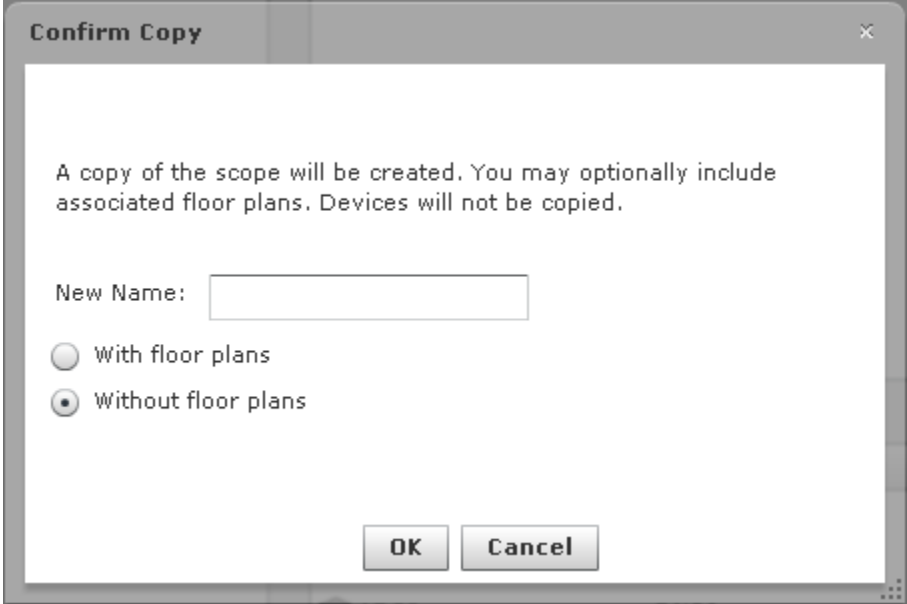


The drop-down menu for buildings contain the following functions:


Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Area.
Properties	Opens the <b>Properties</b> overlay for the selected Area.
Readiness Test	Validates that devices in the area scope are management ready (that is, devices can be manage through ASDP). You are alerted of problem areas. (See <a href="#">Readiness Test</a> for more information.)

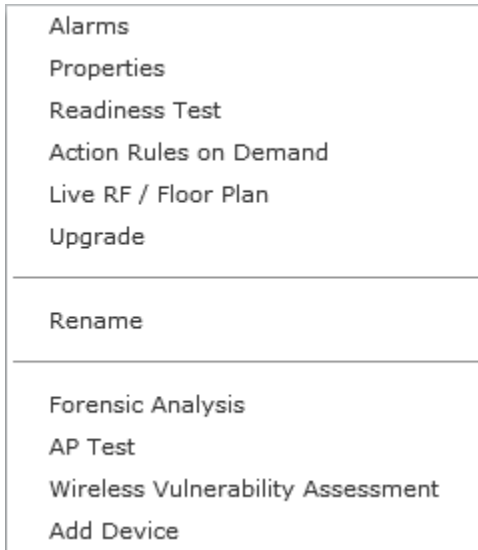


Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in <a href="#">Job Status</a>, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> <li>• Only enabled rules—run test on the enabled rules.</li> <li>• All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.</li> </ul>
Live RF / Floor Plan	Views the floor plan for a area where you can manipulate the floor plan, add devices, and track devices.
Upgrade	Upgrades the firmware for devices in the selected Area. (See <a href="#">Upgrade Devices</a> for more information.)

Function	Description
Copy Folder	<p>Copies the network scope of a Area.</p>  <p>Enter a name for the building, select if you want the to include the floor plans or not, and click <b>OK</b>.</p>
Rename	Opens a dialog window to rename the selected Area.
Remove	Removes the selected Area from your network.
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
AP Test	Accesses AP Test ( <a href="#">Scheduled AP Test</a> ).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment ( <a href="#">Scheduled Vulnerability Assessment</a> ).

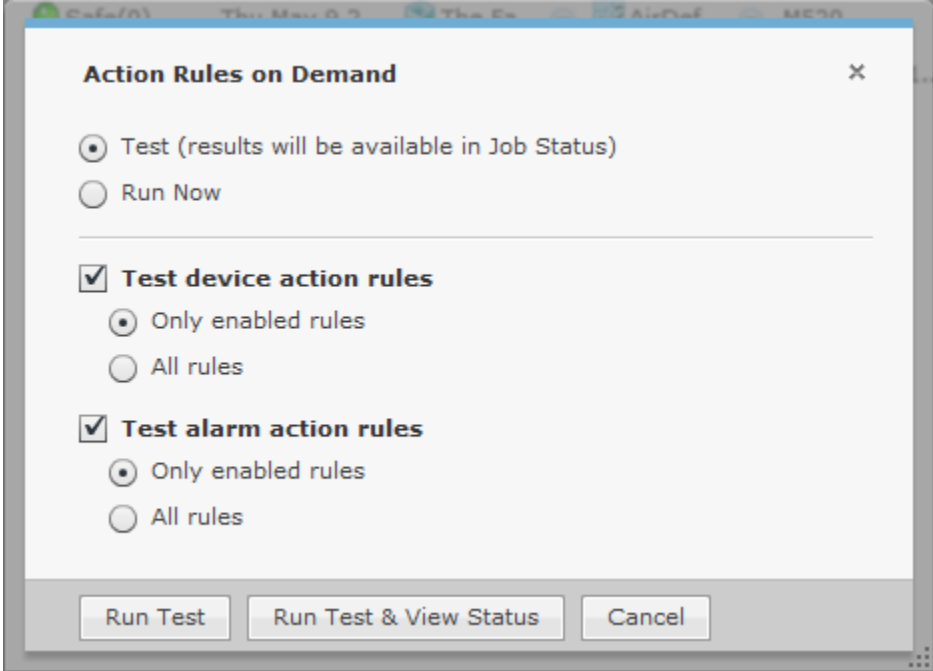
## Live RF / Floor Plan

The Live RF / Floor Plan level drop-down menu contains functions that you can apply to the selected floor level. Click the drop-down menu button— next to the Floor name to display the drop-down menu.



The drop-down menu for floors contain the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Floor.
Properties	Opens the <b>Properties</b> 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. (See <a href="#">Readiness Test</a> for more information.)

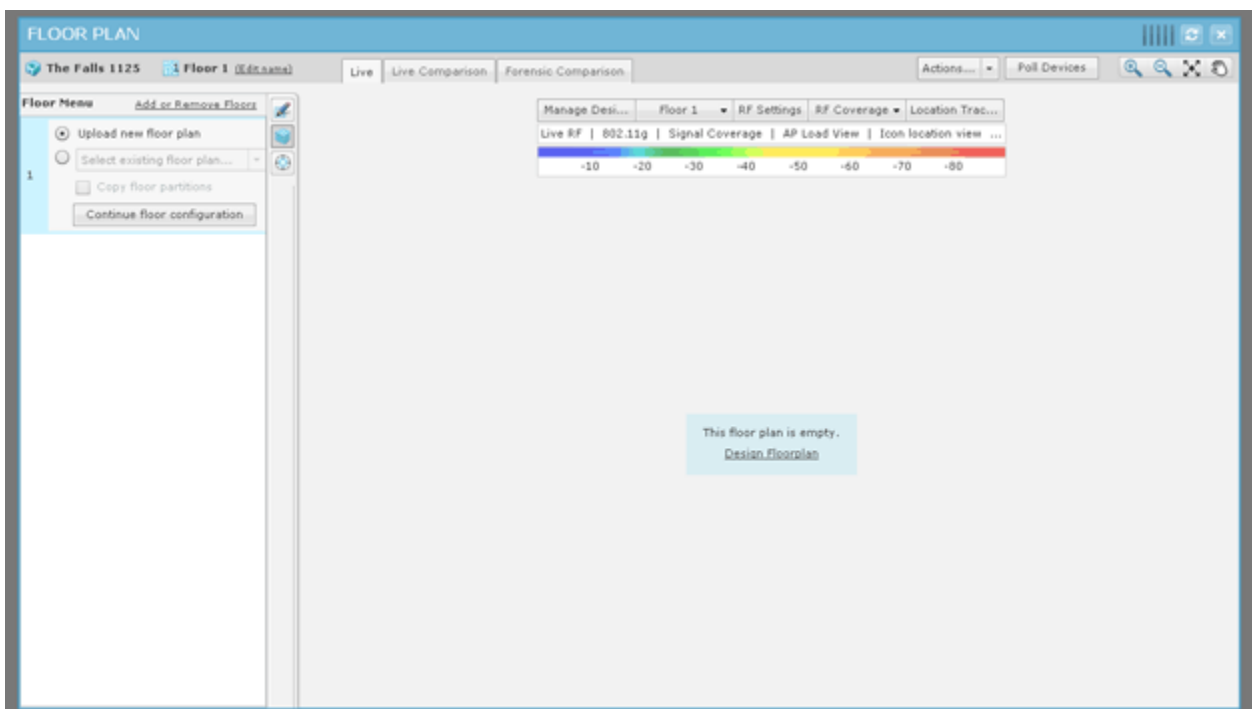
Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in <a href="#">Job Status</a>, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> <li>• Only enabled rules—run test on the enabled rules.</li> <li>• All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.</li> </ul>
Live RF / 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. (See <a href="#">Upgrade Devices</a> for more information.)
Rename	Opens a dialog window to rename the selected Floor.
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
AP Test	Accesses AP Test ( <a href="#">Scheduled AP Test</a> ).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment ( <a href="#">Scheduled Vulnerability Assessment</a> ).
Add Device	Adds devices to the AirDefense Services Platform. Add devices to the AirDefense Services Platform. (See <a href="#">Add Devices</a> .)

## ***Floor Plan***

You can use the Floor Plan to:

- Lay out floors in a building
- View Live RF data
- Locate devices
- Add additional floors to a building
- Plan where to place devices on a floor for maximum coverage.

The first time that you access Floor Plan, you will need to upload a background image for your first floor (see [Upload Image](#)).



If you are accessing Floor Plan from an area (building), the first floor is selected. If you are accessing Floor Plan from a floor, that floor is selected.

Click the **Close** button—X to save and close the Floor Plan. The Floor Plan can now be viewed throughout ADSP, and can be used to locate devices in your network and display Live RF data.

## **Creating Floor Plans**

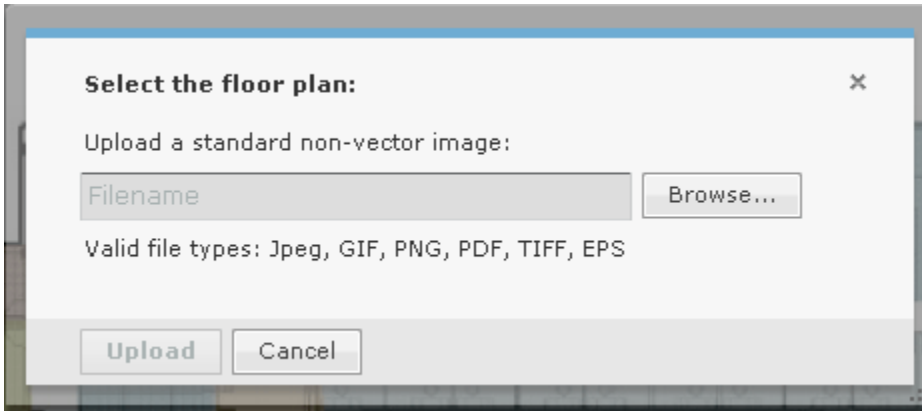
To create a floor plan:

- Upload an background image to use as a guide to insert walls, cubicles, doors, elevators, etc.
- Add additional floors if your building contains two or more floors.
- Use the editing tools to insert walls, cubicles, doors, elevators, etc.

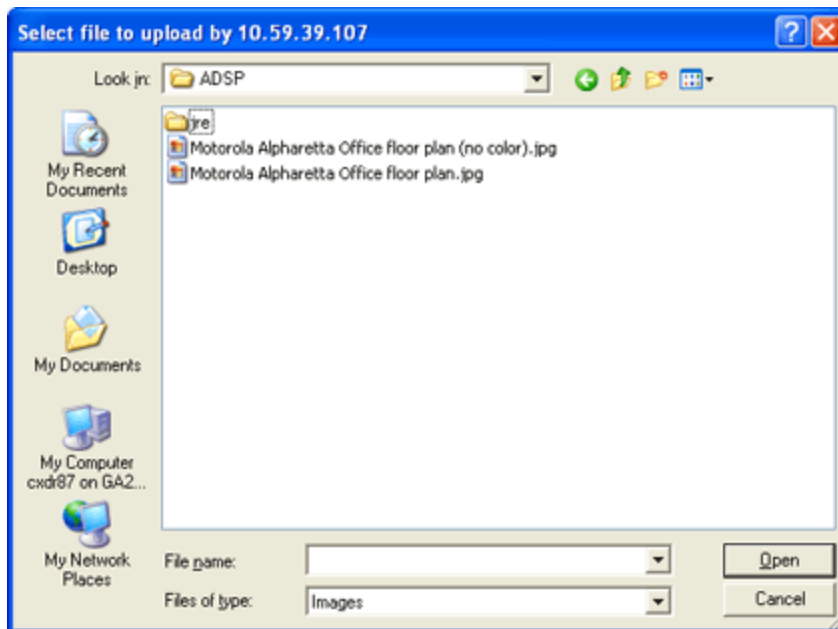
### Upload Image

The easiest way to create a floor plan is to upload a background image. Click the **Continue floor configuration** button or the **Design Floorplan** link to get started.

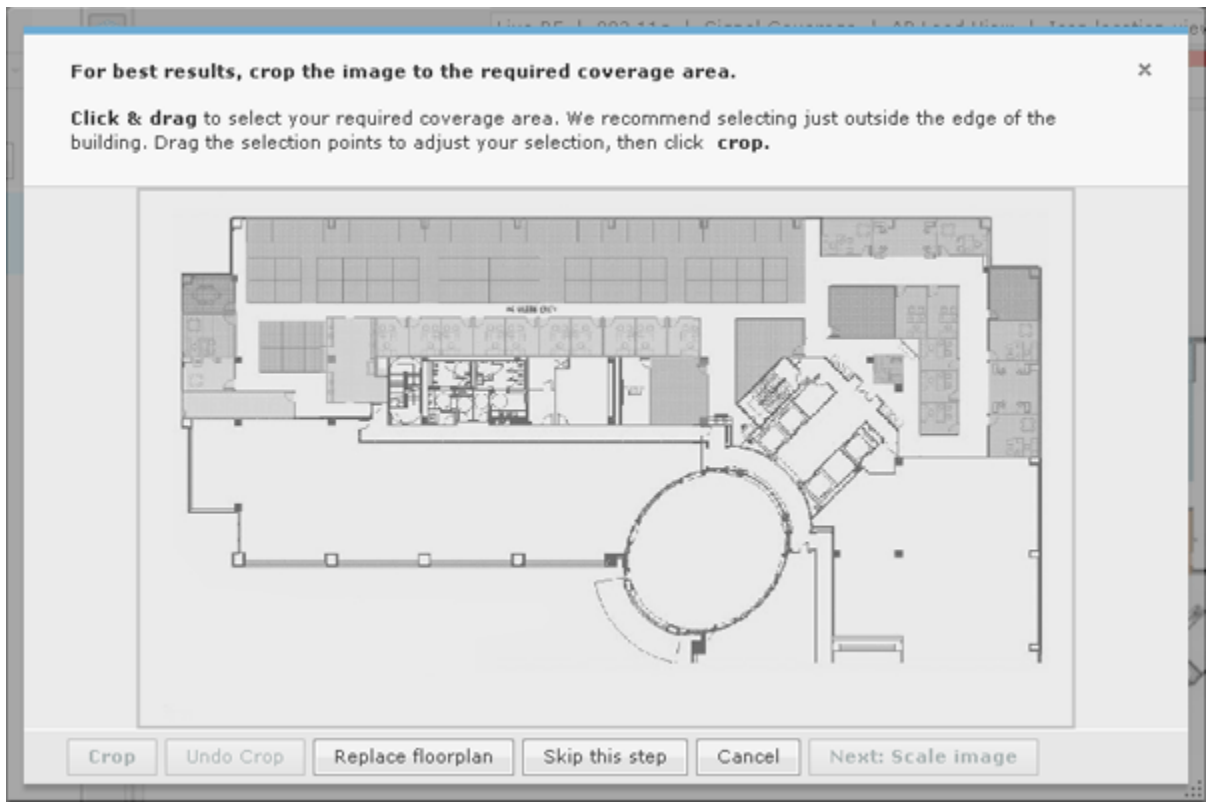
- ✓ **NOTE** The Floor Plan single dimension limit (width or height) is 8192 pixels while the total pixel count (width x height) limit is 8,000,000 pixels. If the appliance has at least 2GB of memory, the total pixel count may be as high as 16,777,215 pixels but the single dimension limit is still 8192 pixels.



1. Click the **Browse** button.



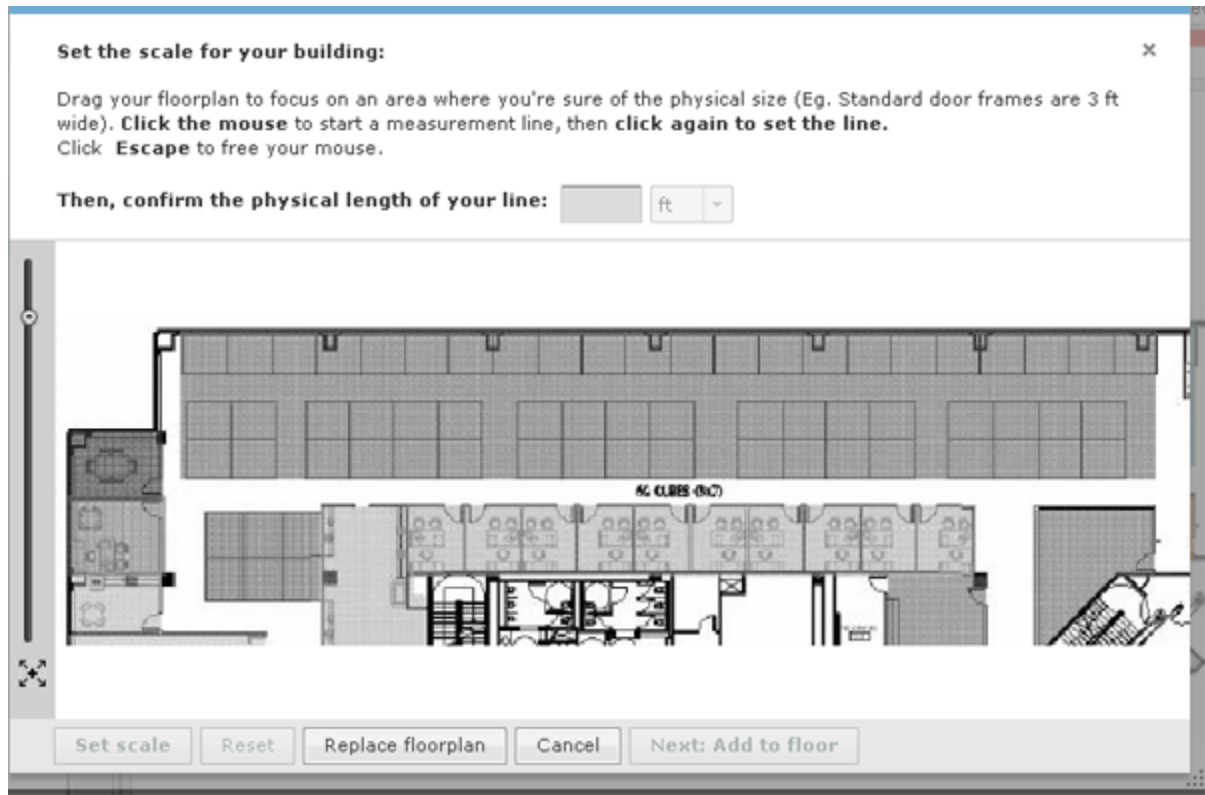
2. Browse to the location of the image, select it (usually a BMP, GIF, or JPG file), and then click **Open**. The **Upload** button is now active. Click it.



This is the Floor Plan wizard. You can use it to guide you through adding a floor to your Floor Plan.

3. You can crop the image to only show the area you are concerned with. Draw a rectangle around the area you want to crop by:
  - a. Clicking on a point in the image.
  - b. Dragging your mouse to draw the rectangle.
  - c. Clicking the end point of the rectangle.
4. Click the **Crop** button to complete cropping the image.

5. Click the **Next: Scale Image** button.

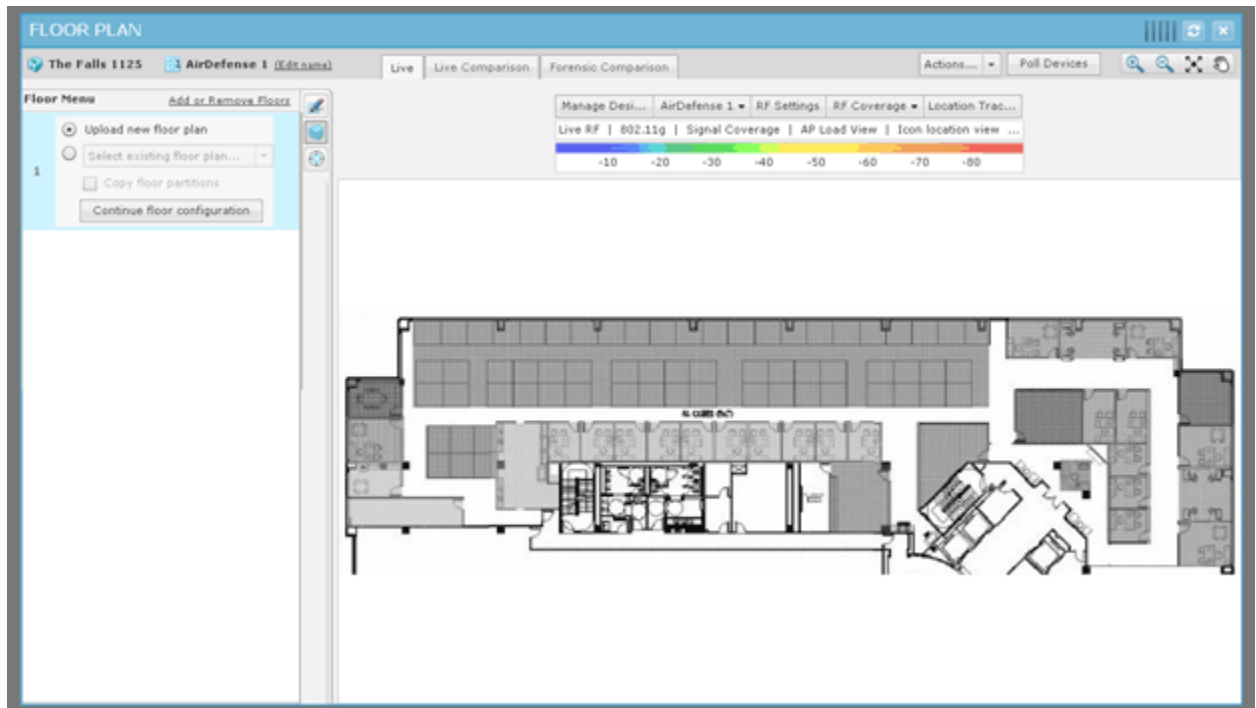


6. Scale your image by clicking on a point in the image, draw a line, and then click an end point. Enter the distance of the line which represents the actual length of the physical space in feet or meters. The **Set scale** button is activated. Click it to complete scaling.
7. The **Next: Add to floor** button is activated. Click it to add the floor to your floor plan.

✓ **NOTE** You can undo any changes by clicking the **Cancel** button. You can remove an image by clicking the **Replace floorplan** button.



Your uploaded floor plan will look similar to the following one:



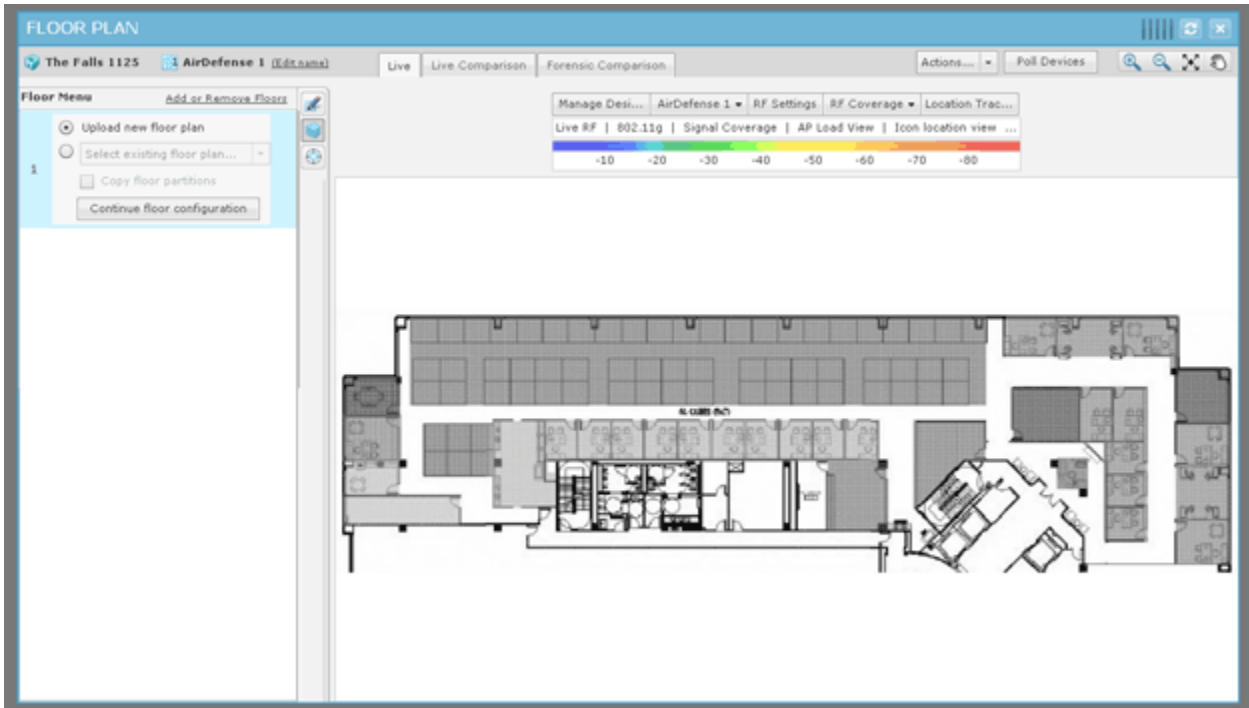
You can now use the editing tools to add walls, cubicles, doors, elevators, etc. This allows you to account for building obstacles when ADSP does calculations to locate devices and/or to display Live RF data.

### Add Additional Floors

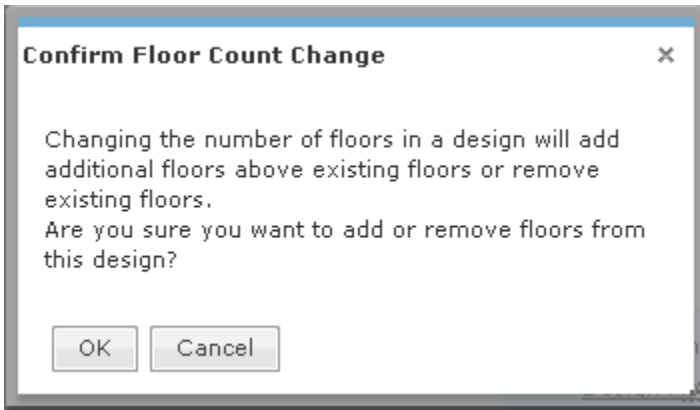
To add an additional floor to your building, first reveal the existing floors by clicking anywhere on the **Floor Plan Toolbar**.



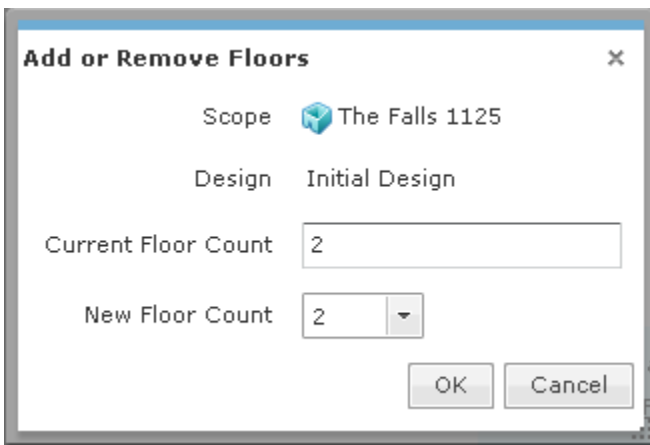
✓ **NOTE** Clicking the **Floor Plan Toolbar** also removes floor selection from view.



Click the **Add or Remove Floors** link. The following dialog is displayed:

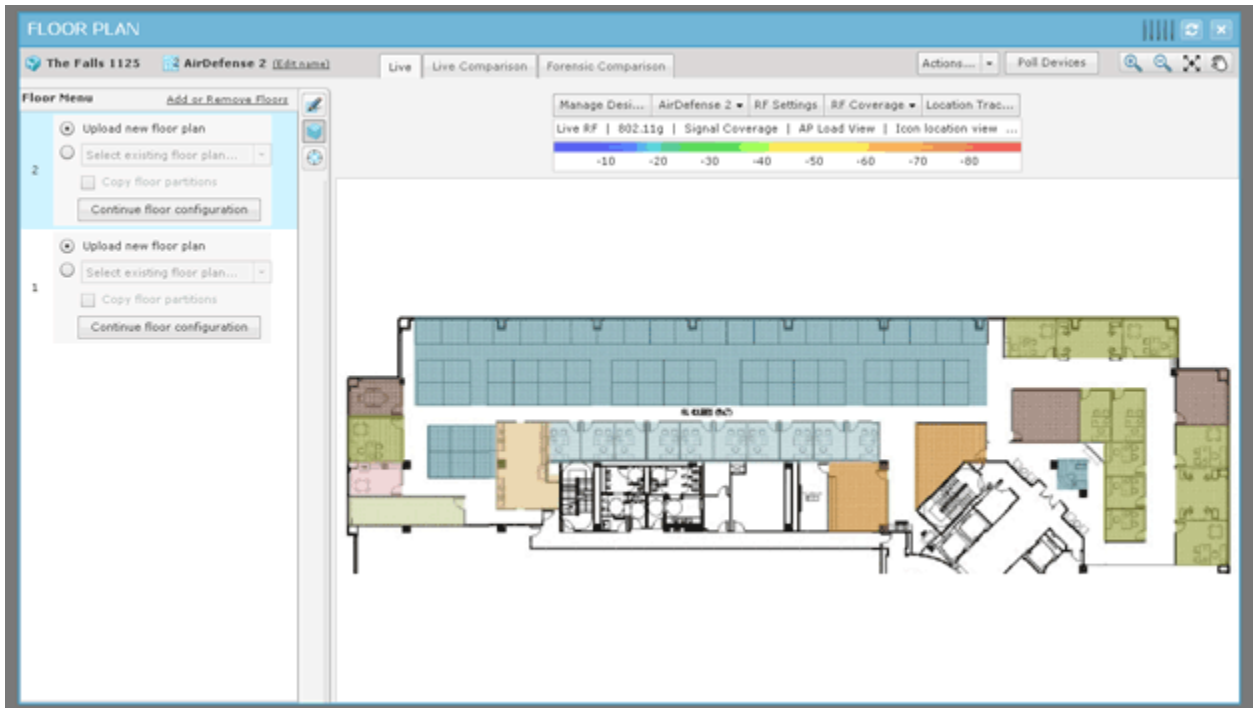


Click **OK** to continue to the following dialog:



Click the **New Floor Count** drop-down and select a floor number. If you increase the floor count, floors are added accordingly. You can have as many as 100 floors in a building. If you decrease the floor count, floors are removed starting at the top floor. Click **OK** to make the change.

After you add a floor, you will need to upload a background image for your floor or design a new floor plan. The following floor plan shows a building with two floors:




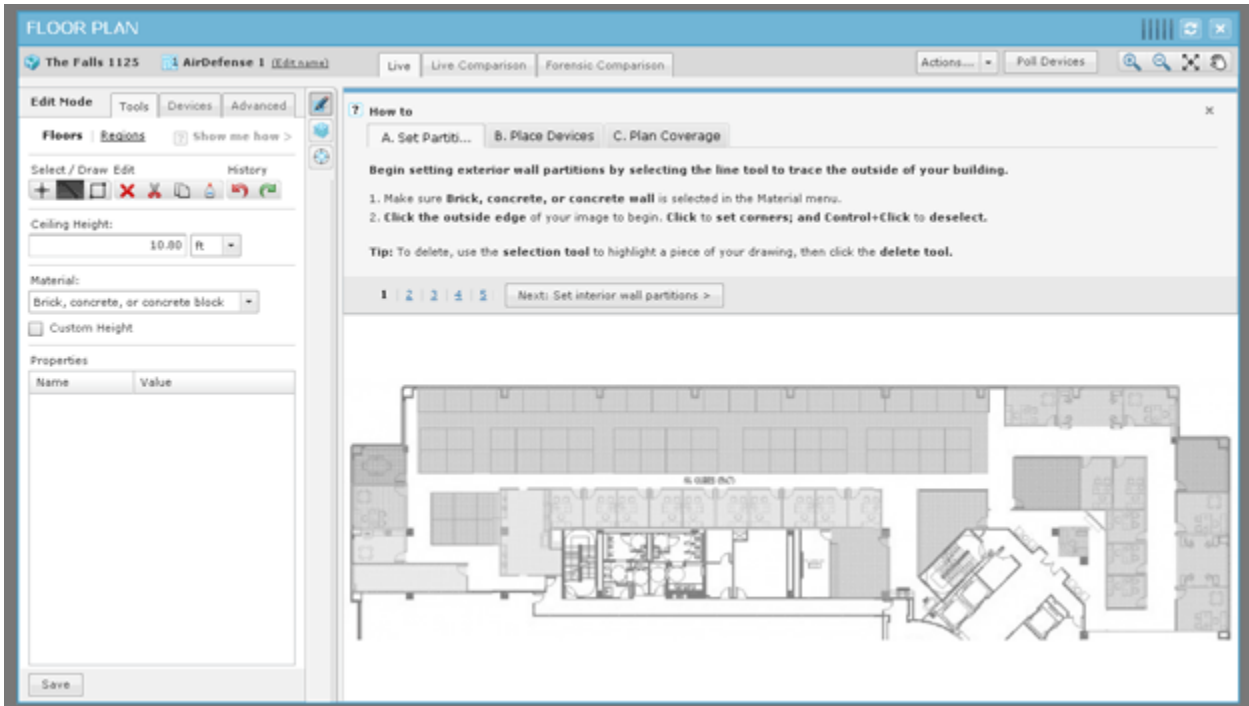
To access the different floors within a building, click the thumbnail image for the floor located in the left pane.

### Editing Floor Plans

Editing a floor plan involves:

- Using the tools to design (draw) or alter the floor plan.
- Adding devices to your floor plan to view Live RF data and locate devices.
- Using the advanced controls to enhance the floor plan.

Click the **Edit Mode**— button (part of the Floor Plan toolbar) to edit a floor plan.



The first time you enter the **Edit Mode** the **How to** wizard is accessed. The **How to** wizard guides you step-by-step through the editing process to set up your Floor Plan. You can hide the **How to** wizard by clicking its **Close**—x button and edit your Floor Plan as you like using the **Tools**, **Devices**, and **Advanced** tabs. If the **How to** wizard is hidden, you can access it by clicking the **Show me how** link.

While editing a floor plan, in addition to the editing tools, you have access to the [Context Label](#) and the [Actions](#).

✓ **NOTE** The **Context Label** is only visible when you hide the **How to** wizard.

You can switch between Floor Plan views using the following tabs:

Links	Description
Live	Displays a single floor with the Live RF heat map. This is where you edit your Floor Plan.
Live Comparison	Displays two views of the floor plan side-by-side so that you can make a comparison.
Forensic Comparison	Displays two heat maps for comparison: one with Live RF data and one with forensic RF data.

The **Save** button saves any changes.

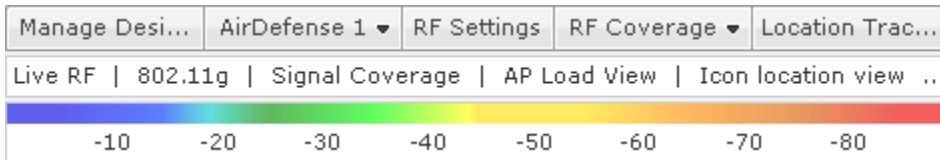
### **Global Tools**

Global tools are tools that are available on all Floor Plan pages. They are:

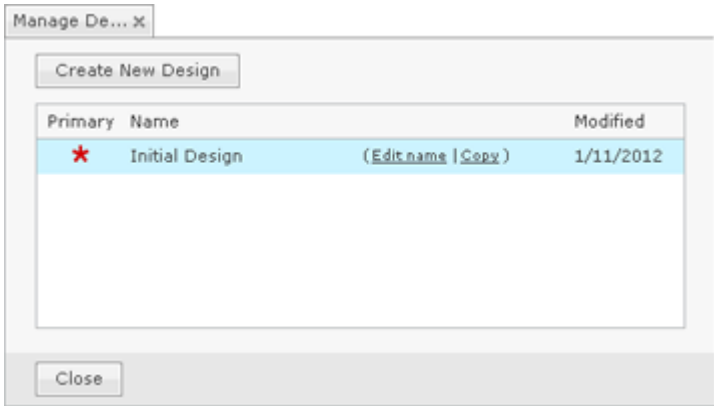

- Context Label
- Actions
- Floor manipulation.

## Context Label

The **Context Label**, located near the top-center of the Floor Plan, controls the context of the Floor Plan.



The **Context Label** shows you the following information:

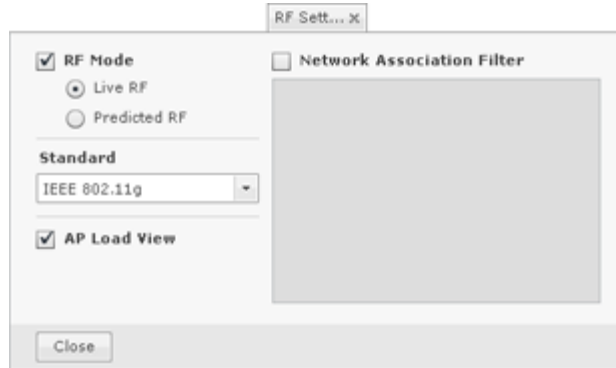
Field	Description
Manage Designs	<p>When this field is clicked, a list of existing designs is displayed:</p>  <p>You can edit or add to the list using the following actions:</p> <ul style="list-style-type: none"> <li>Click the <b>Primary</b> field for a design to make it the primary design.</li> <li>Click on the <b>Edit name</b> link to change the name.</li> <li>Click the <b>Copy</b> button to create a new design identical to the selected design. A name for the new design is auto-generated and can be changed using the <b>Edit name</b> link.</li> <li>Click the <b>Remove</b>-X button (last column of a design) to remove a design. You cannot remove the primary design. An undo remove link is displayed when a design is removed in case you change your mind.</li> <li>Click the <b>Create New Design</b> button to create a new design. A name for the new design is auto-generated and can be changed using the <b>Edit name</b> link.</li> </ul> <p>Click <b>Close</b> to exit the design manager.</p>
Floor Selection	<p>This field shows the selected floor. If you click the field, you can select another floor to view.</p> 

Field	Description
-------	-------------

RF Settings

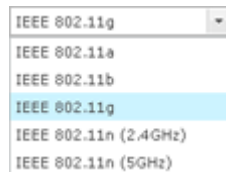
RF Settings includes:

- The RF Mode setting
- The Protocol setting
- The AP Load View setting
- The Network Association Filter.



The RF Mode setting determines if your heat maps display no RF data (deselected), Live RF data (selected), or Predicted RF data (selected).

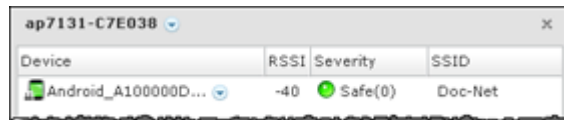
The Protocol setting allows you to filter RF data according to the selected protocol.



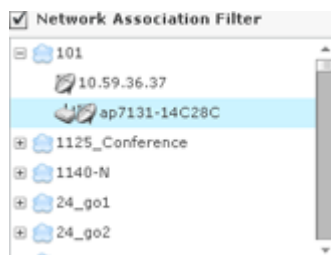
The **AP Load View** setting, when selected, displays a circle around any AP that has Wireless Clients associated with it. Layered on the circle is a smaller circle displaying the number of associated Wireless Clients.




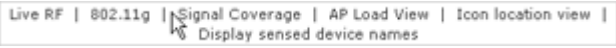

Clicking on the smaller circle displays all the associated Wireless Clients in a table.



The **Network Association Filter** is where the network device association is shown in a network tree. You may select an entire SSID or individual devices.

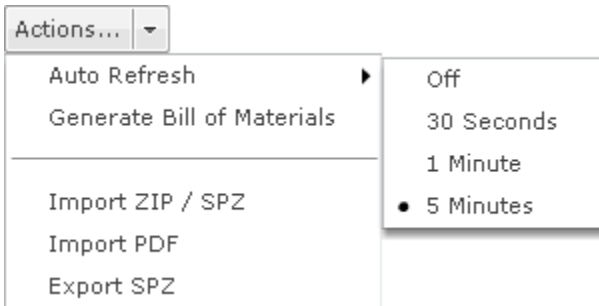


Field	Description
RF Coverage	<p>This field lets you select the coverage visualization or application coverage for your heat maps. If you click the field, you can select another visualization or application.</p>  <p>Visualizations and applications are configured in <a href="#">Configuration &gt; Network Assurance &gt; Live RF Settings</a>.</p>
Location Tracking	<p>This field displays a list of devices being tracked grouped by device type.</p>  <p>If a device in the list is selected (highlighted) it is highlighted in the floor plan map. Location Tracking has two views: <b>Icon location view</b> and <b>Heat map display</b>. The <b>Icon location view</b> displays the most likely location for selected devices as an icon for each device. The <b>Heat map display</b> displays the most likely locations for the selected device as a color gradient ranging from red (most likely) to blue (least likely) locations.</p> <p>The <a href="#">Track</a> topic gives more details on how to track devices.</p>

Field	Description
Current Settings	<p>This field gives you a quick view of the settings that have been set via the <b>Context Label</b>.</p>  <p>Three dots (...) at the end of the <b>Current Settings</b> indicate there are more settings that have been configured. Moving your mouse over the <b>Current Settings</b> will reveal the additional settings.</p> 
Color Chart	<p>The color chart is a legend representing the signals displayed as RF data in the Floor Plan. Each color represents a signal strength (in dBm).</p> 

**Actions**

The Floor Plan Actions contains a set of tools for generating a bill of materials and importing/exporting floor plan data.



**Auto Refresh**

**Auto Refresh** works on both Live RF and location tracking. For Live RF, auto refresh uses the latest data (radio, power, channel, live status, etc.) ADSP has about devices to refresh RF data. For location tracking, it refreshes the current position of the devices being tracked. There are four options for Auto Refresh:

- Off
- 30 seconds
- 1 Minute
- 5 Minutes (default).



***Generate Bill of Materials***

**Generate Bill of Materials** creates a bill of materials for the selected design and places the output in a PDF file.

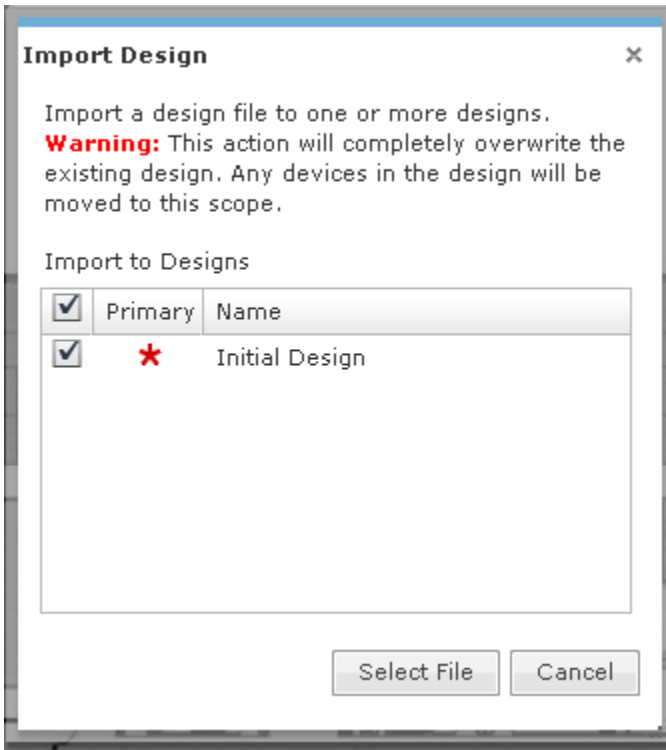
The following fields are available:

Field	Description
Design	Selects the design to use when generating the bill of materials.
Floors	Selects the floors of the design to use when generating the bill of materials. A checkmark selects the floors. The top checkbox, when checked, will select or deselect all of the floors.
Add changelist from	When selected, the output contains images for the selected design and an additional design that you select from the drop-down menu. The output will also contain device tables that show the differences between the two designs (devices added, removed, and/or changed).
Format	Selects a letter or legal page format, and whether you want portrait or landscape format.

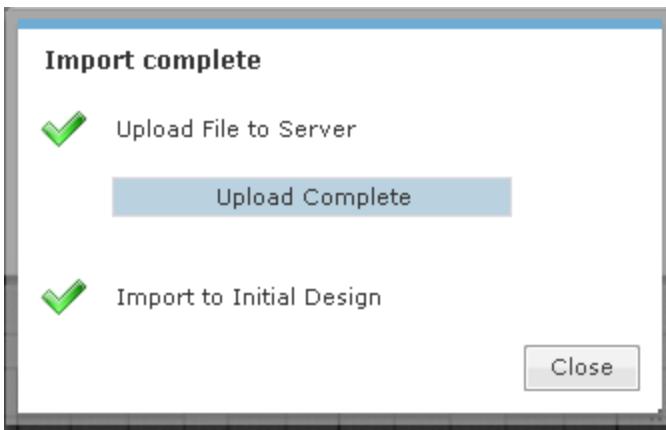
Click **Start** to begin the process. A checklist is generated to indicate success or not. Click the link, [Click to choose where to save the PDF file.](#), to specify where to place the generated PDF file and then click **Save** to save the file. If an error occurs, an error message is generated.

***Import ZIP / SPZ***

**Import ZIP / SPZ** imports a LAN Planner design that was exported to a ZIP or a speedwell ZIP (SPZ) file.



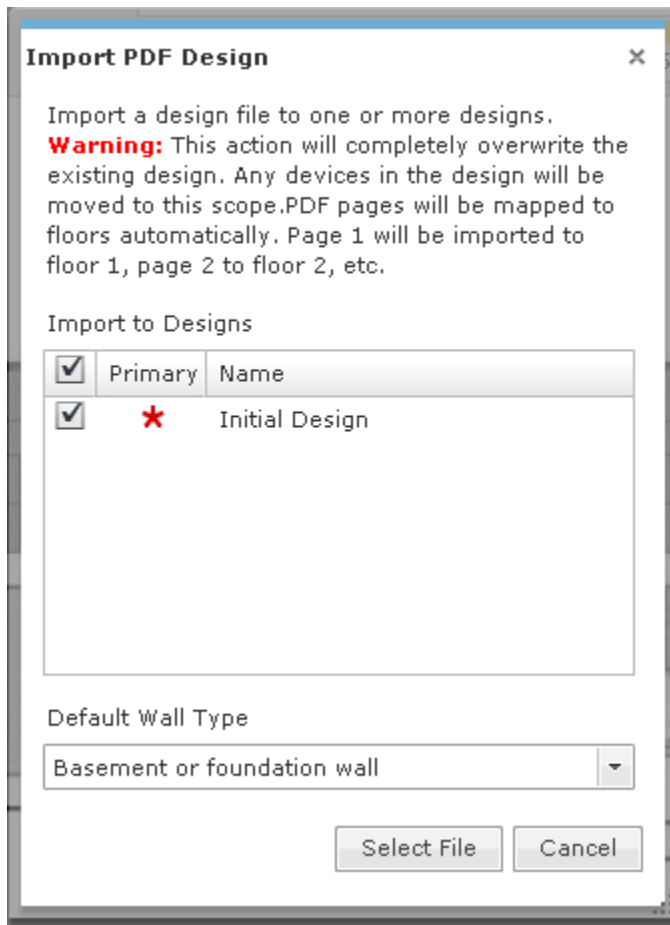
First select the design you want to replace (indicate with a checkmark) and then click the **Select File** button. Next, navigate to the file, select it, and then click **Open**. When the import is complete, a confirmation is displayed.



Click the **Close** button to return to the Floor Plan.

***Import PDF***

**Import PDF** imports a design created in AutoCAD and exported to a PDF file.



Basically, **Import PDF** works like **Import ZIP / SPZ** with the following exceptions:

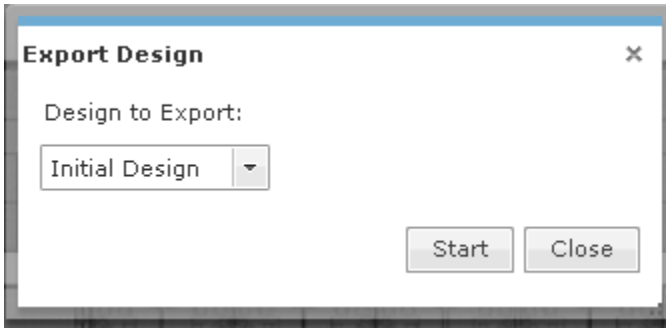
- You can choose the default wall type with Import PDF as follow: Basement or foundation wall
- Brick, concrete, or concrete block
- Cubicle wall
- Drywall or sheetrock
- Elevator or metallic obstacle
- Glass door or window, no tint
- Metallic rack
- Wooden door.

Imported PDF pages are automatically mapped to existing floors. Page 1 is imported to floor 1, page 2 is imported to floor2, and so on.

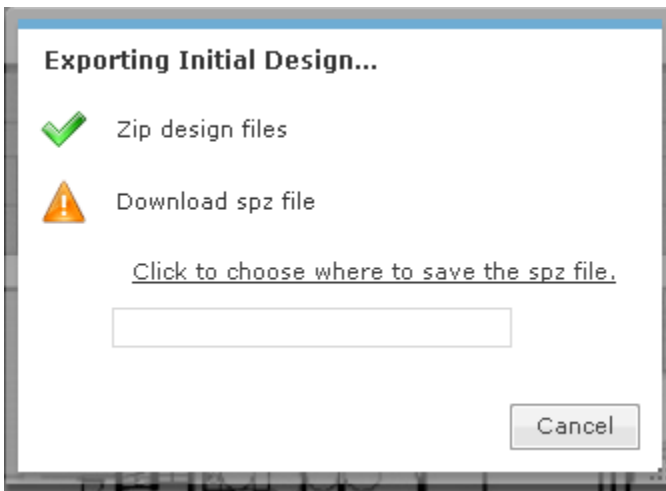
### ***Export ZIP***

- ✓ **NOTE** Before exporting a floor plan design for a newly created or edited floor plan, you **must** leave the Editing page first. If you do not, DWG files will not export correctly.

**Export ZIP** exports the selected floor plan design to a ZIP file that can be imported into LAN Planner.



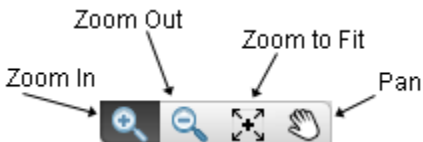
To begin, select a design from the drop-down menu and then click **Start**. A checklist is generated to indicate success or not.







Click the link, [Click to choose where to save the ZIP file.](#), to specify where to place the generated ZIP file and then click **Save** to save the file. If an error occurs, an error message is generated.

### **Floor Manipulation**

The floor manipulation tools (located near the top-right side of the Floor Plan) allow you to adjust the size of the floor plan image with a single click and/or move the floor plan image by dragging it to a new position.



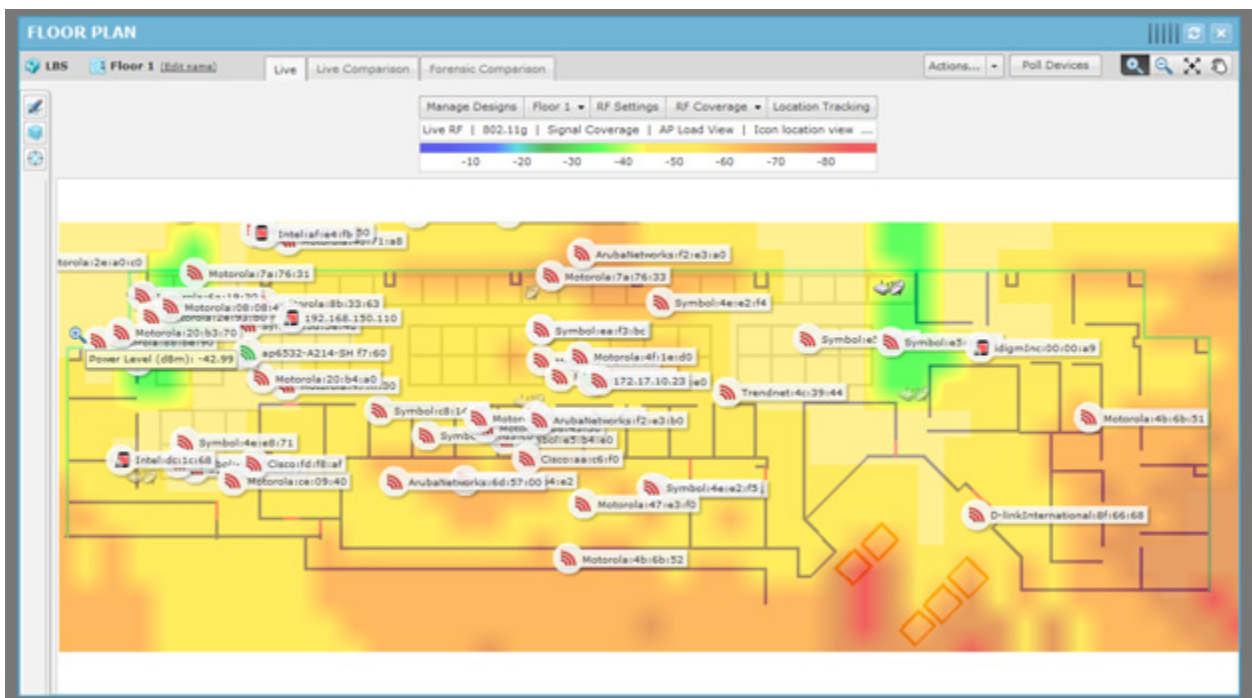
The following tools are available:

Tool	Description
	Click this tool to zoom in (enlarge the size) a floor plan image. Each click will zoom into another level.
	Click this tool to zoom out (reduce the size) a floor plan image. Each click will zoom out to another level.
	Click this tool to fill 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.
	Click this tool to move/re-position the floor plan image. After clicking the tool, use the hand (click and hold) to move/re-position the image.

### Live Tab

✓ **NOTE** A Live RF license is required to access this feature.

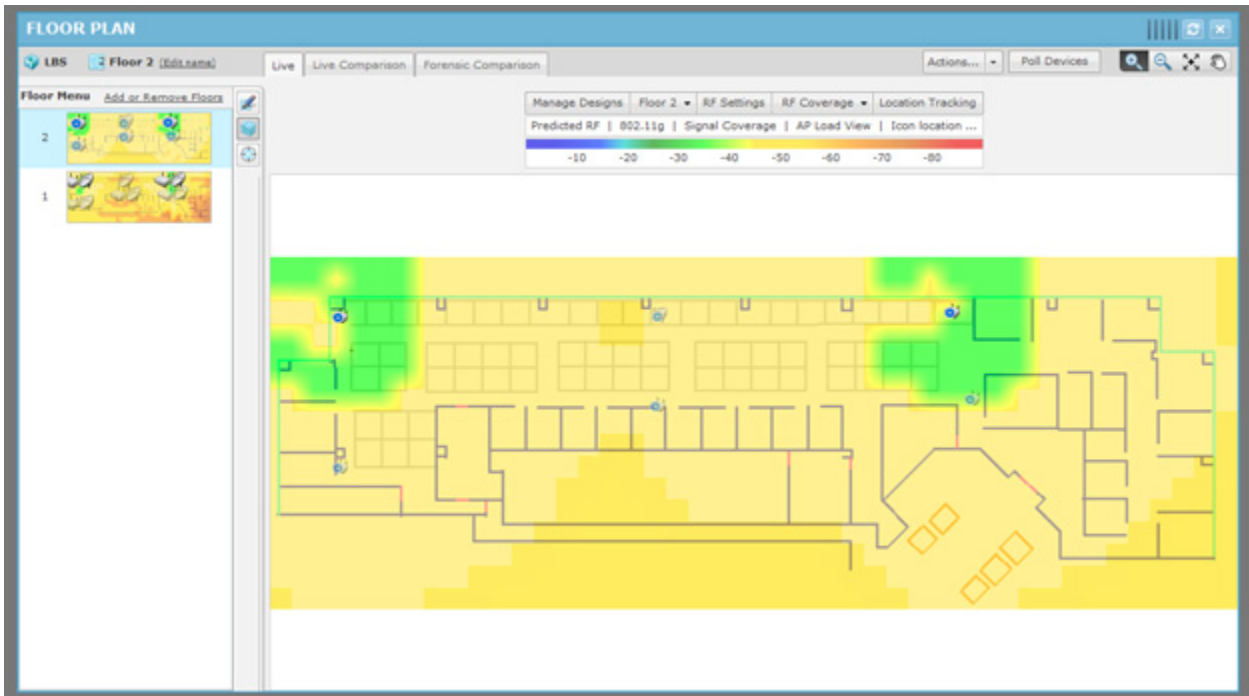
The **Live** tab displays a heat map that represents signal coverage for APs placed on a Floor Plan. When the Floor Plan is accessed, if devices are in place, Live RF starts and a heat map is displayed.



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.

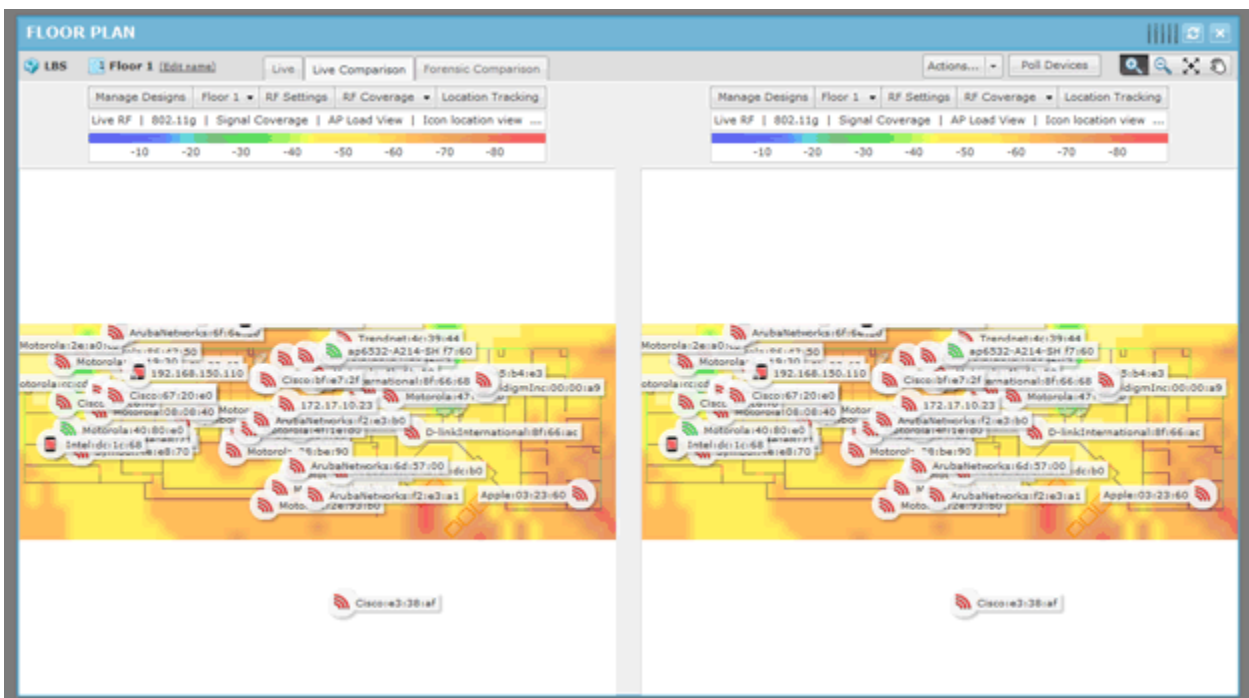
### Predictive RF

The Floor Plan also displays a Predictive RF heat map that represents predicted coverage for planned devices placed on a Floor Plan. You must first place planned devices on the Floor Plan using the **Devices** tab of the **Edit Mode**. Once you have the planned devices in place, click the RF selection drop-down menu (top, right of the **Context Label**) and select **Predictive RF**.



### Live Comparison Tab

The **Live Comparison** tab displays two views of the floor plan side-by-side so that you can make a comparison.

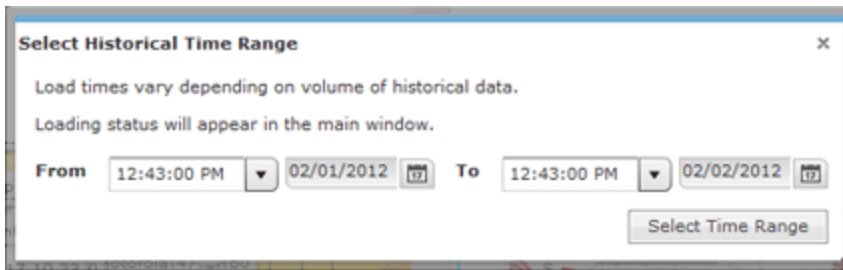


You have access to the **Context Label** where you can manipulate one or both of the images.

The floor manipulation tools are available so that you can zoom in/out or pan the images.

### **Forensic Comparison Tab**

The **Forensic RF** tab visualizes forensic data to display coverage over a specific time range. Click the **Forensic RF** tab to display a historical heat map for signal coverage.



Specify a beginning time and date, specify an end time and date, and then click **Select Time Range** button.



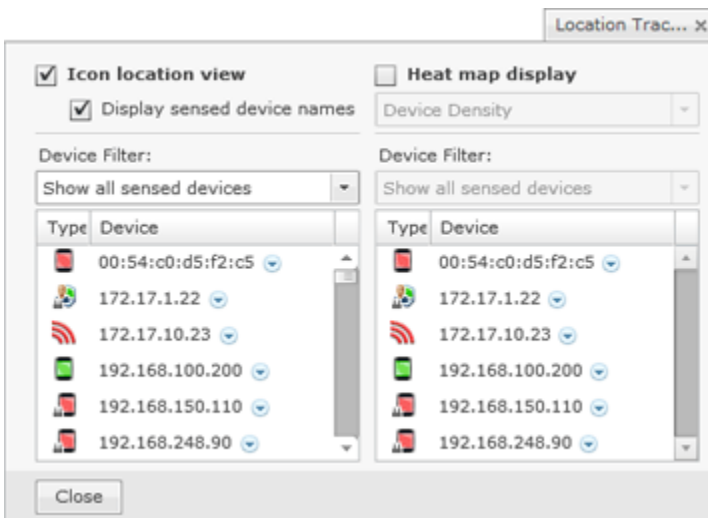
Two heat maps are displayed: one displaying Live RF for the current date and time, and one displaying Forensic RF for the specified time range. You can change the time range by clicking the **Edit** link and entering a new range. You can adjust the time range up or down within the specified range using the slider. Data points are displayed under the time line to indicate when changes occur. Move the slider to a data point to display the change in forensic data.

**Track**

Tracking enables you to locate and track rogue devices that may be threatening your wireless LAN. In order for **Tracking** to open and function properly, you must have three (minimum) Sensors for each floor map loaded.

- ✓ **NOTE** Tracking is not intended to be used on devices that are being terminated.
- ✓ **NOTE** In order to track a device, a floor plan must already exist.

To start tracking a device, click the **Location Tracking** button in the **Context Label**.



All sensed devices are displayed when Location Tracking (in the list of devices and the floor plan) is first accessed. You can group devices by type by selecting **Filter by device type** from the drop-down menu. You can search for devices by selecting **Search for devices** from the drop-down menu.

There are two views for Location Tracking:

- **Icon location view** displays the devices on the map by its icon and device name.
- **Heat map display** displays the likely location for a tracked device as a color gradient ranging from red (most likely) to blue (least likely) locations. The device icon is displayed on the map at the most likely location for the device. You can view **Heat map display** by **Device Density** or by **Single Device Probability**.



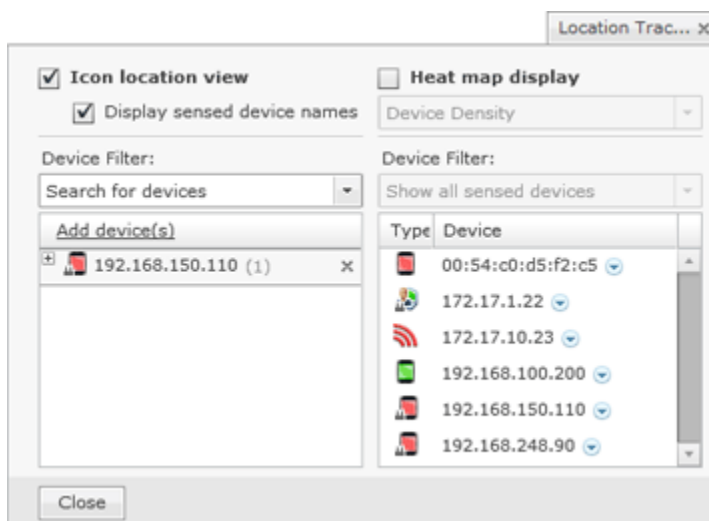
For either view, you can search for a device by selecting **Search for devices** and then clicking the **Add Device** button. A dialog opens where you can type in a MAC address.



Type in a partially or whole MAC address.

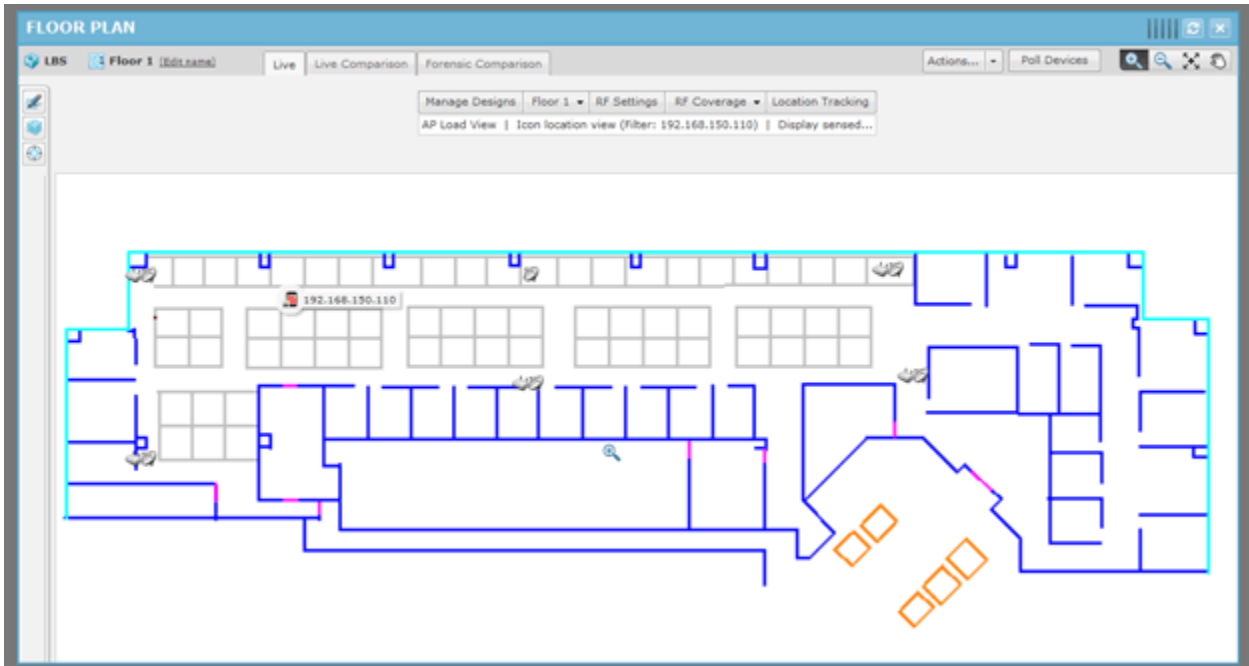
✓ **NOTE** The **Advanced** link is used to open a search dialog that gives you more options to find devices.

When you see the device listed, click on it and then click **Track Device**. The device is displayed in the tracked device list.



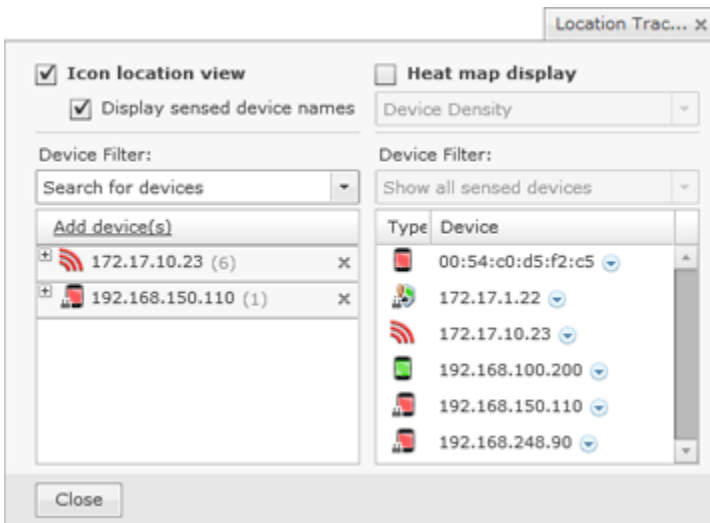
✓ **NOTE** You may select more than one device using the **<Shift>** key or the **<Ctrl>** key.

Click the **Close** button or anywhere outside the Location Tracking dialog to display the device in the Floor Plan.

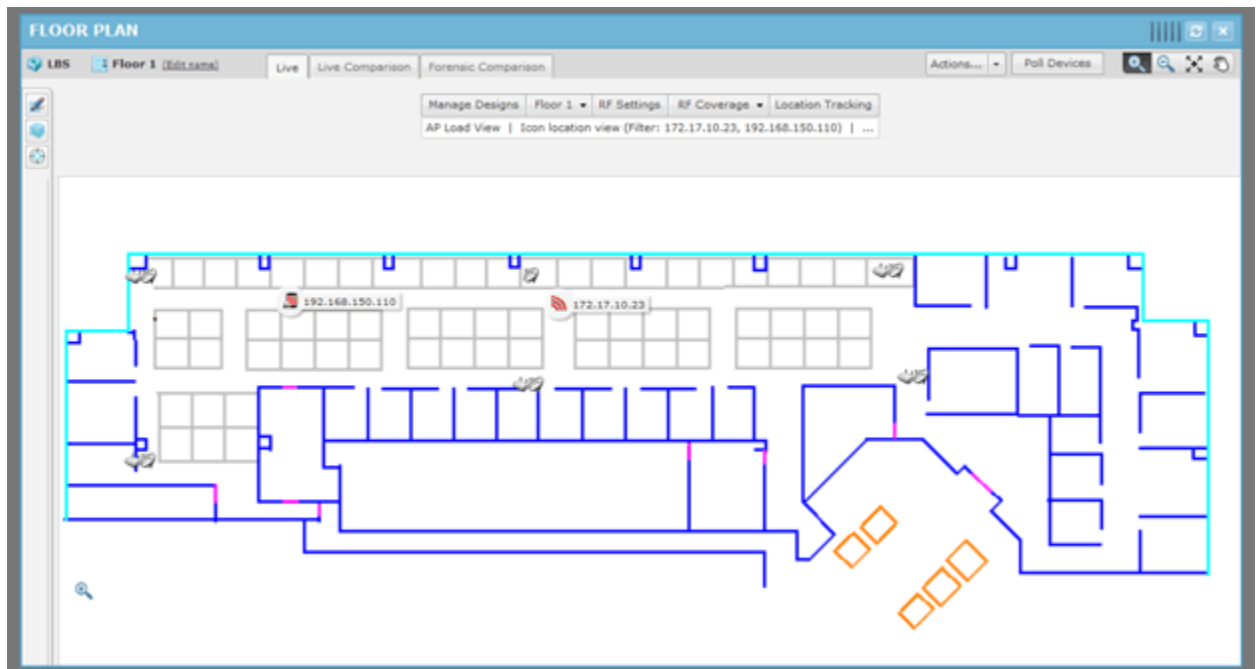


The Floor Plan shows the device being tracked. Clicking the Refresh button will refresh the image. If the device has moved, you will see its current position in the floor plan.

You can track more than one device by adding them as described above. Each time you add a device it is displayed in a list of tracked devices.



Click the **Close** button or anywhere outside the Location Tracking dialog to display the devices in the Floor Plan.



### AP Assisted Tracking

In order to get AP assisted location tracking working with the Motorola RFS4000, RFS6000 and RFS7000 controllers, the WiOS controller must be enabled so that RSSI data can be passed to ADSP. There is a procedure for BSSs and Wireless Clients (refer to [BSS Tracking](#) and [Client Tracking](#)).

- ✓ **NOTE** This is only for the Motorola based controller infrastructure. The 4.x version of standalone APs do not require this sort of configuration. The Cisco WLC does not require configuration to enable AP assisted location tracking.

### BSS Tracking

For BSS tracking, the Enhanced Beacon table on the RFSX000 controller must be enabled.

1. Log into the RFSX000.
2. Navigate to **Security > Enhanced Probe/Beacon Table > Beacon Table**.
3. Select the **Enable Enhanced Beacon Table** checkbox.
4. In the **Channel Set** fields, enable the channels for each radio that you want to scan.
5. Leave the default values for **Scan Interval**, **Scan Time**, and **Maximum number of APs**.
6. Click **Apply**.
7. Navigate to **Network > Access Port Radios**.
8. Double-click on the B/G radio of the AP650.
9. Select the **Enable Enhanced Beacon Table** checkbox.
10. Click **Apply**.
11. Repeat steps 9 and 10 for the A radio.

12. Save the configuration.
13. Restart the controller. (If you are going to enable the enhanced probe table, follow the directions provided below before restarting the switch.)

To verify Location Tracking with this setup:


1. Navigate to **Security > Enhanced Probe/Beacon Table > Beacon Table**.
2. Click the **Beacon Found** tab.
3. Verify that this page is being populated with rogue AP and signal strength data.
4. In the **Portal MAC** column, verify that the radio MAC of your AP650 appears in this column.
5. The column next to the **Portal MAC** column is the Rogue AP detected by the portal MAC.
6. Copy one the Rogue AP MAC addresses detected by the AP650 radio (A or B/G).
7. In ADSP, drag the AP650 to a floor plan with 2 other sensors.
8. Attempt to track the device that matches the previously recorded MAC address.
9. If the target device is detected by the other 2 sensors, location tracking should work.

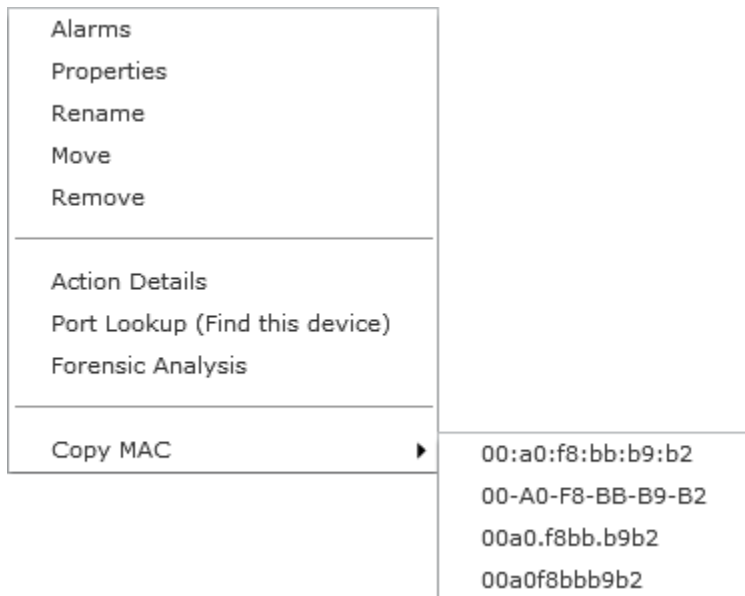
### Client Tracking

For Wireless Client tracking, the Enhanced Probe table must be enabled on the RFSX000 controller to permit an AP to forward MU probe request data to the controller. Each Wireless Client's MAC address that the user wishes to track must be manually entered into the RFSX000's preferred Wireless Client (MU) list. Thus, if you want to track multiple rogue Wireless Clients, you have to input the MAC of each Wireless Client (MU) into the switch, then wait until it is pushed into ADSP.

1. Log into the RFSX000.
2. Navigate to **Security > Enhanced Probe/Beacon Table > Probe Table**.
3. Select the **Enable Enhanced Probe Table** checkbox.
4. In the **Preferred MUs** section, click the **Add** button.
5. Enter the MAC address of the MU (Wireless Client) that you want to populate the **Probe Request** table with data.
6. Click **OK**.
7. Click **Apply**.
8. Navigate to **Network > Access Port Radios**.
9. Double-click on the B/G radio of the AP650.
10. Select the **Enable Enhanced Probe Table** checkbox.
11. Click **Apply**.
12. Repeat steps 9 – 11 for the A radio.
13. Restart the controller.

## Unplaced Devices

The Unplaced Devices level drop-down menu contains functions that you can apply to the selected Unplaced Device level. Click the drop-down menu button— next to the Unplaced Devices name to display the drop-down menu.



The drop-down menu for unplaced devices contains the following functions:

Function	Description
Alarms	Accesses the <b>Alarms</b> tab where you can view the alarms for the selected Unplaced Devices level.
Properties	Opens the <b>Properties</b> overlay for the selected Unplaced Devices level.
Rename	Opens a dialog window to rename the selected unplaced device.
Move	Moves the selected unplaced device to another network level (floor). (See <a href="#">Move Devices</a> for more information.)
Remove	Removes the selected unplaced device from your network. (See <a href="#">Remove Devices</a> for more information.)
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup (Find this device)	Opens the <a href="#">Port Lookup</a> window where you can locate the physical port where the unknown device is accessing your network.
Forensic Analysis	Accesses <a href="#">Forensic Analysis</a> .
Copy MAC	Copies the MAC address of the selected unplaced device for later use.

## Network Level Properties

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

### *Appliance Level*

The screenshot shows a window titled 'PROPERTIES' for an 'ADSP' appliance. On the left is a sidebar with the following 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 contains the following fields and buttons:

- Name: ADSP
- Host: localhost
- Port: 0
- Status: OK
- Buttons: Autoplace, Push Configuration

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.

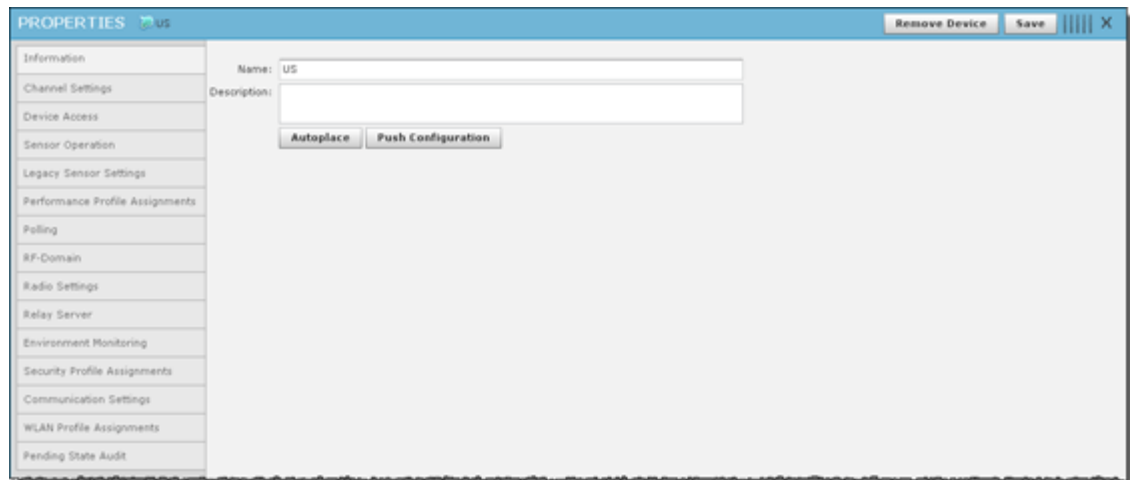
You can view and/or override an appliance's configuration by selecting:

- [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 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.

For configuration instructions, see the [Device Firmware](#) topic under *The GUI*.

### 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.

For configuration instructions, see the [Channel Settings](#) topic under *The GUI*.

### 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.

For configuration instructions, see the [Radio Settings](#) topic under *The GUI*.

### 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](#).

For configuration instructions, see the [WLAN Profiles](#) topic under *The GUI*.

### CLI Configuration

The Command Line Interface (CLI) for devices is a powerful tool that gives you direct access to access points and switches. 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.

For configuration instructions, see the [CLI Configuration](#) topic under *The GUI*.

---

## 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 [Operation Management](#). 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.

For configuration instructions, see the [Relay Server](#) topic under *The GUI*.



# CHAPTER 4 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.

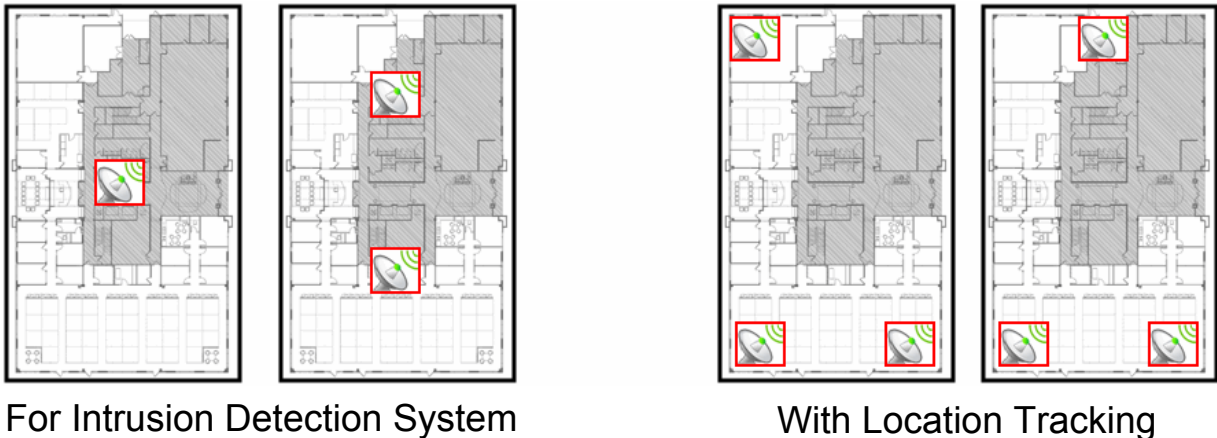
### Considerations

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.



#### 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 floor plan 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).

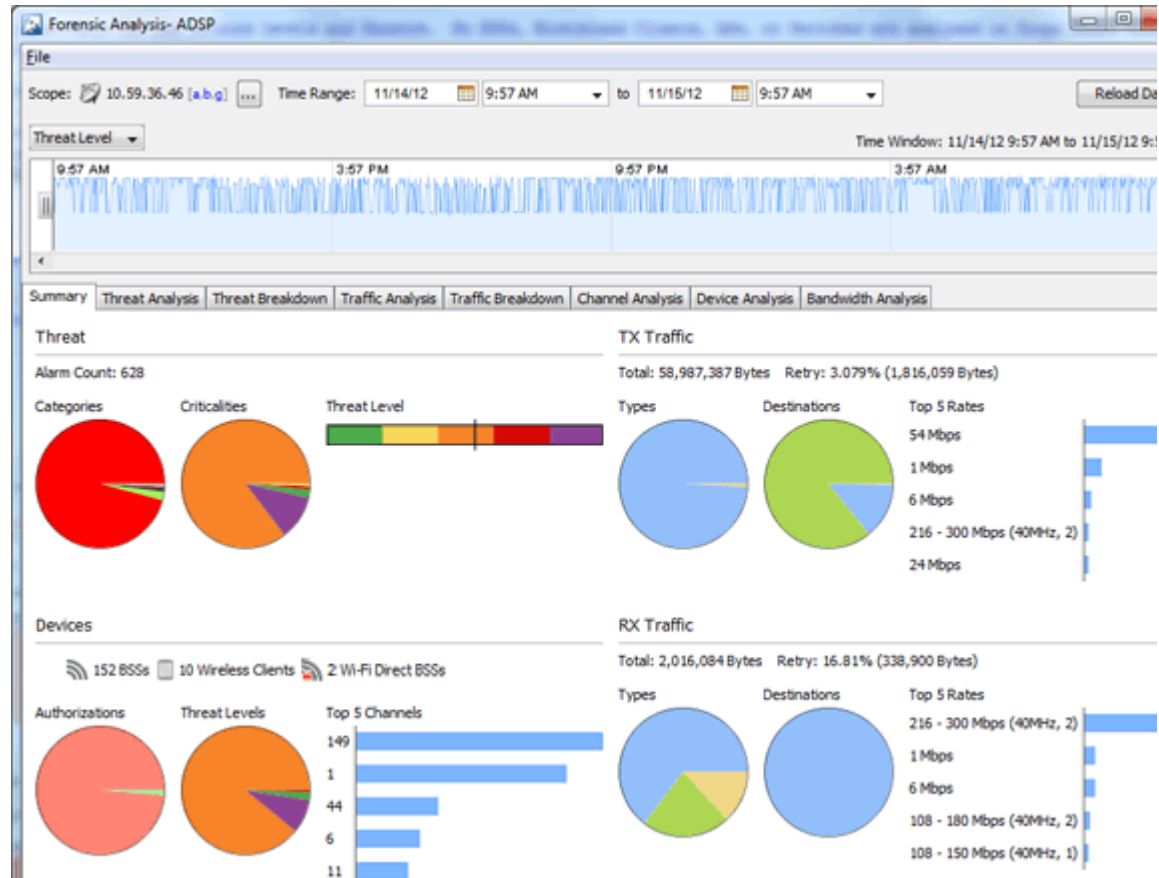
Administrators can view the activity of a suspect device over a period of months and drill down to minute-by-minute detail of wireless activity. Records are kept over a long period of time so that administrators can review events months later to improve network security posture, assist in forensic investigations, 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 [Advanced Forensic Analysis](#) for details on how to use Advanced Forensic Analysis.

## Scope Based Forensic Analysis

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

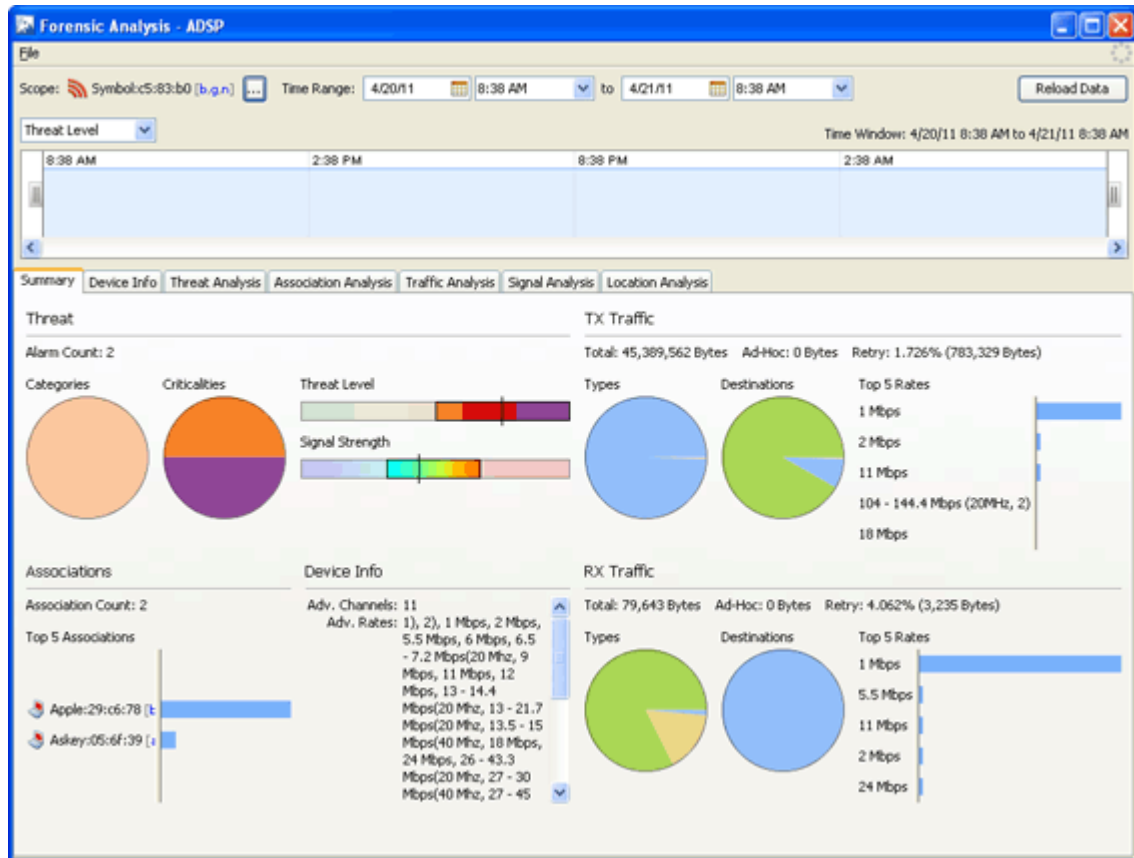


The following forensic data is included with Scope Based Forensic Analysis:

- 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.



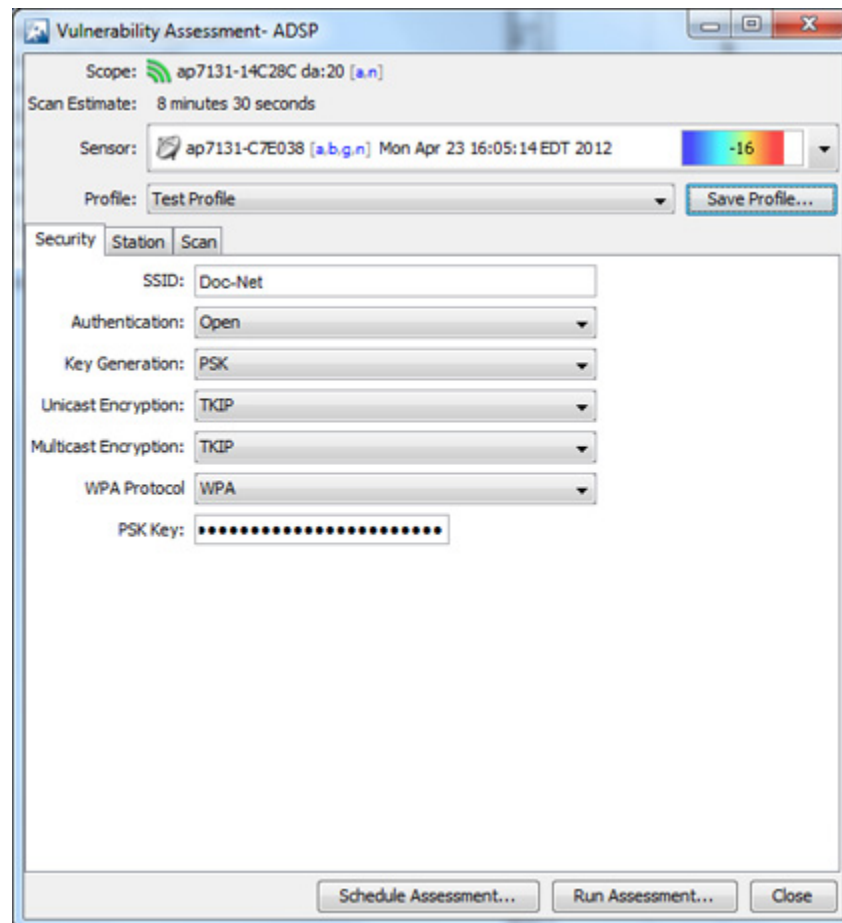
The assessment is accomplished by using deployed sensors as a wireless client to connect to an AP and scan network resources. Vulnerability Assessment can be run automatically or manually, providing proactive notification that network resources may be compromised.

- ✓ **NOTE** For ADSP 9.1.0, 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.

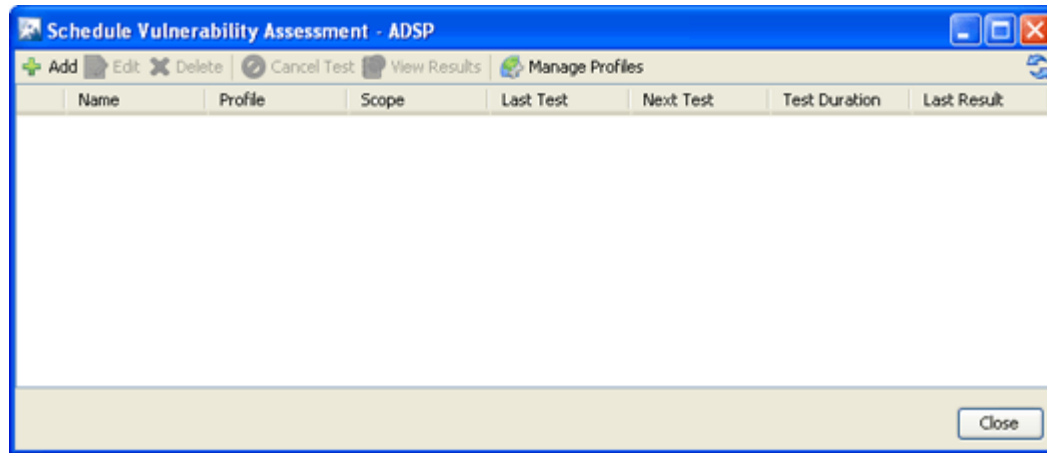


The **Vulnerability Assessment** window allows you to configure and run the assessment. After you have configured an assessment, you can save it as a profile. A profile can be selected later to run test on a similar scope.

See the [On-Demand Assessment](#) 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 [Scheduled Assessment](#) 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.

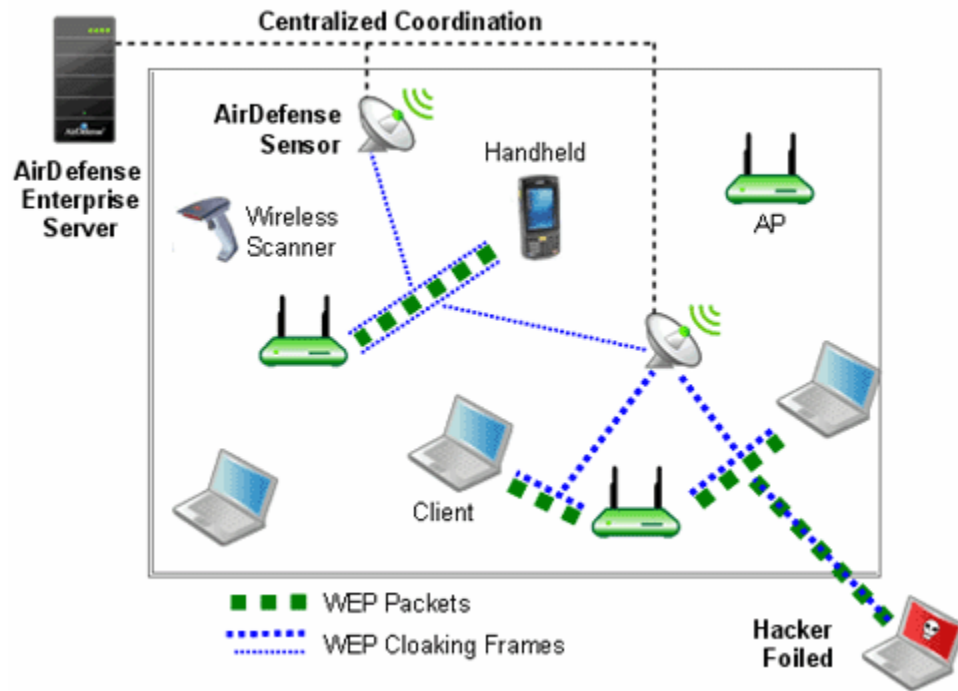
- ✓ **NOTE** By default, the sensor is a passive wireless monitoring device and does not transmit (provided termination has not been enabled). Enabling the sensors for WEP Cloaking will cause the sensors to actively transmit on the channels of the access points it is protecting.

### 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 IUs)

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 IUs. Usually, 104-bit WEP
  can be cracked with about one million IUs, 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 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.

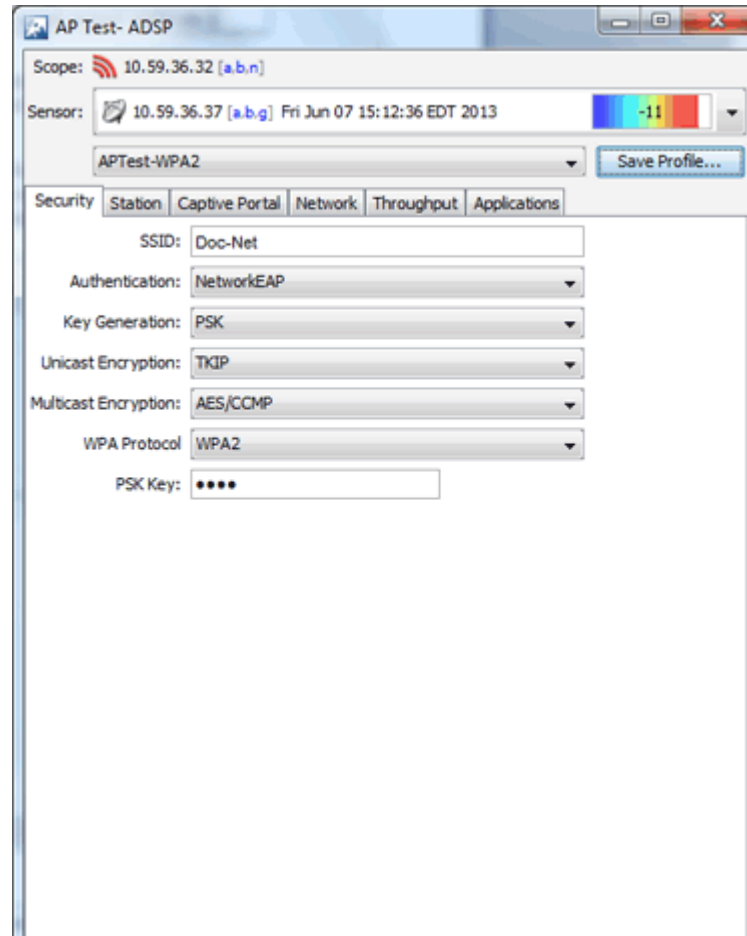


**NOTE** For ADSP 9.1.0, AP testing is supported on the M510 and M520 sensors with firmware version 5.3 or higher installed, and on APs configured as sensors with WiNG version 5.1 or higher installed.

## 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.

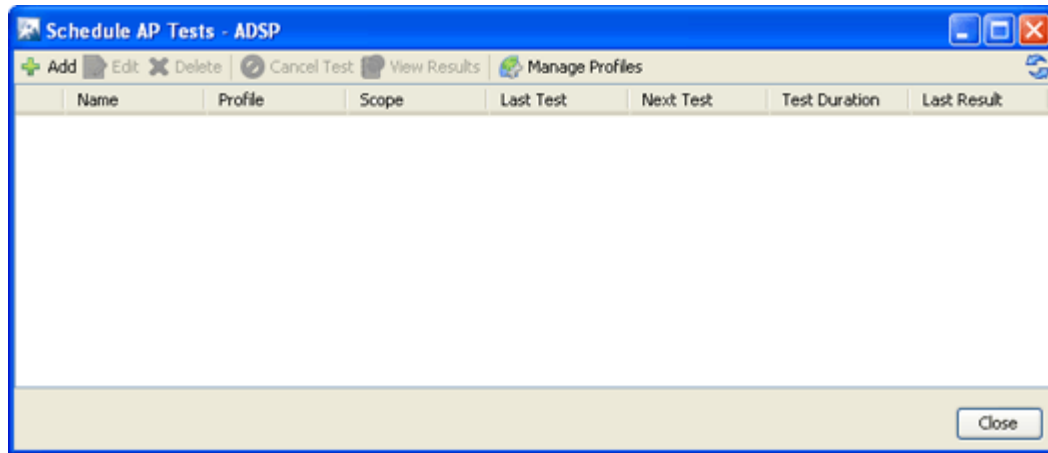


The **AP Test** window allows you to configure and run the AP Test with the click of a button. You must configure AP Test using the **Security**, **Station**, **Network**, and **Throughput** folders. After you have configured an AP Test, you can save it as a profile. A profile can be selected later to run test on a similar access point.

See the [On-Demand Tests](#) topic under *The GUI* 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:

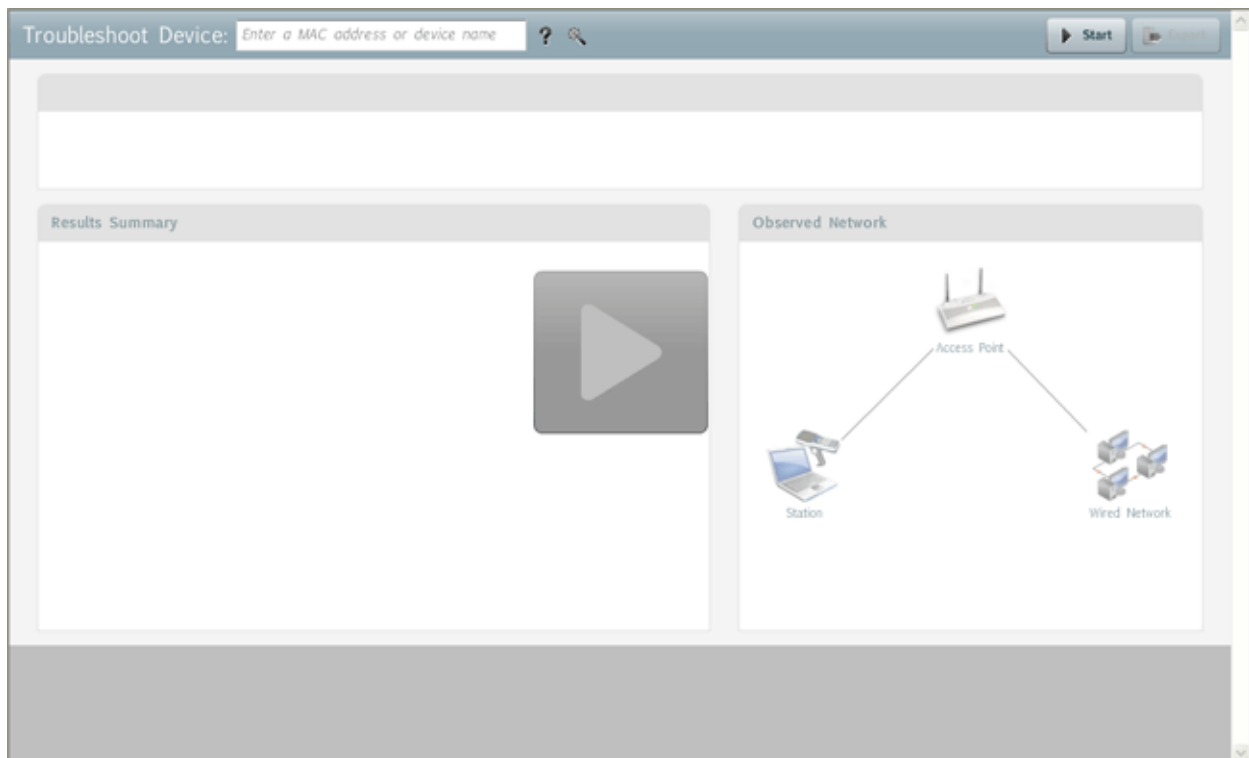
- Add, edit, delete, and cancel tests
- View detail test results
- Manage the profiles that are used to run tests on similar access points.

See the [Scheduled Tests](#) topic under *The GUI* 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.

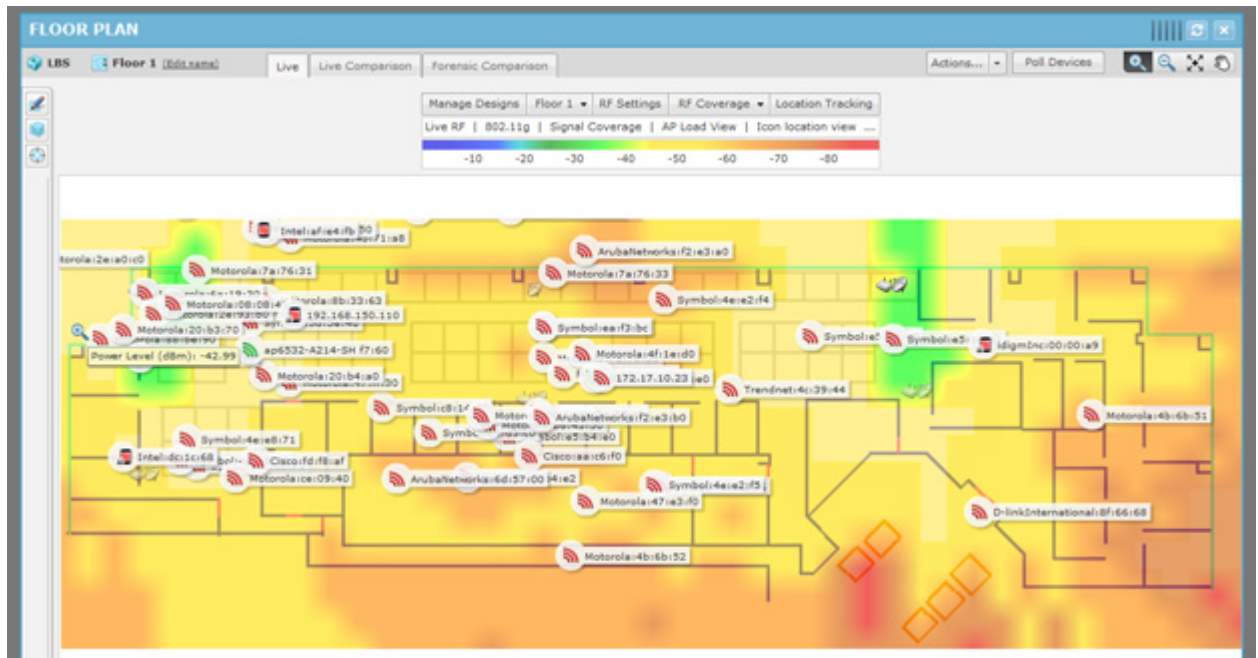


The [Connection Troubleshooting](#) topic under *The GUI* fully explains how to use the Connection Troubleshooting tool.



## 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 > Live RF 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.

The [Live Tab](#) topic under *The GUI* fully explains how to use Live RF.

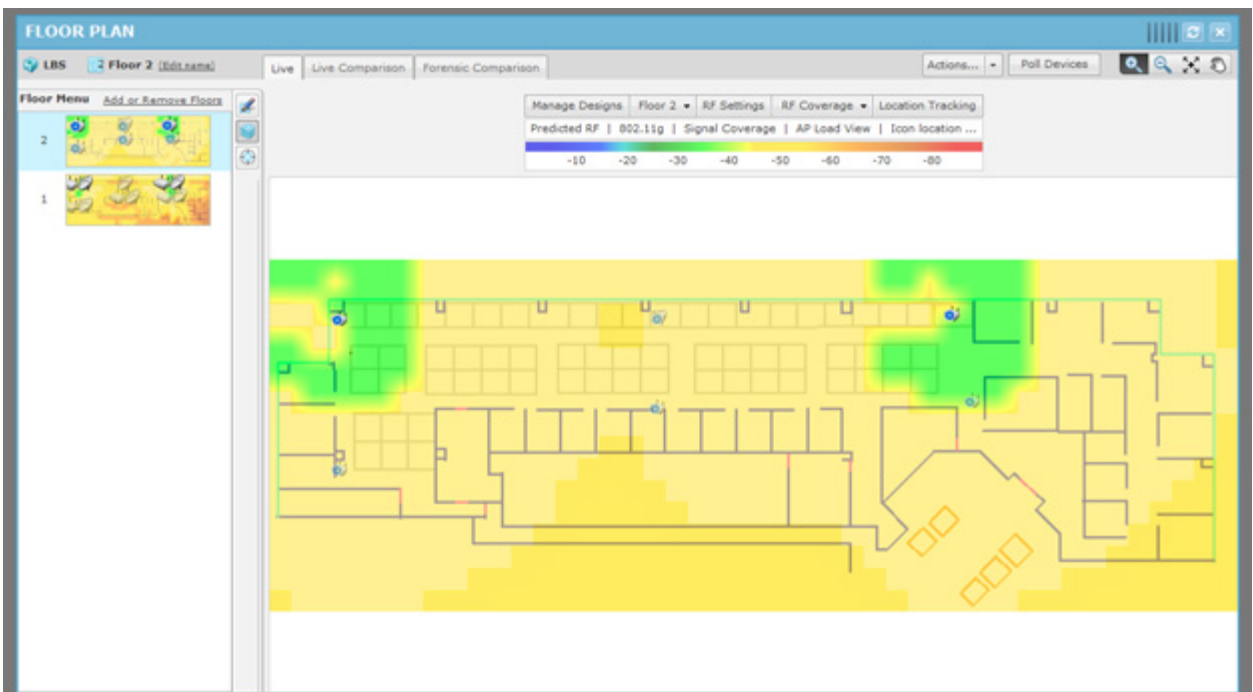
## Forensic RF

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.



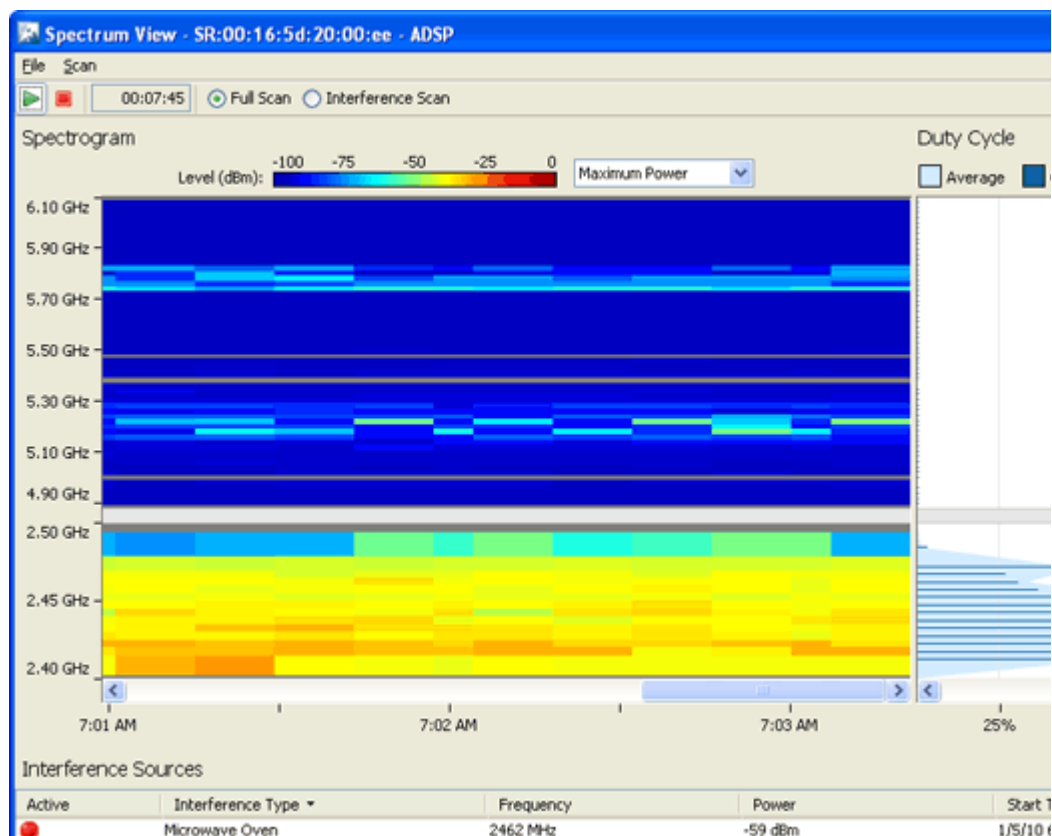
There must be enough unassigned LiveRF licenses to cover the number of planned devices in the floor plan.

## 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:

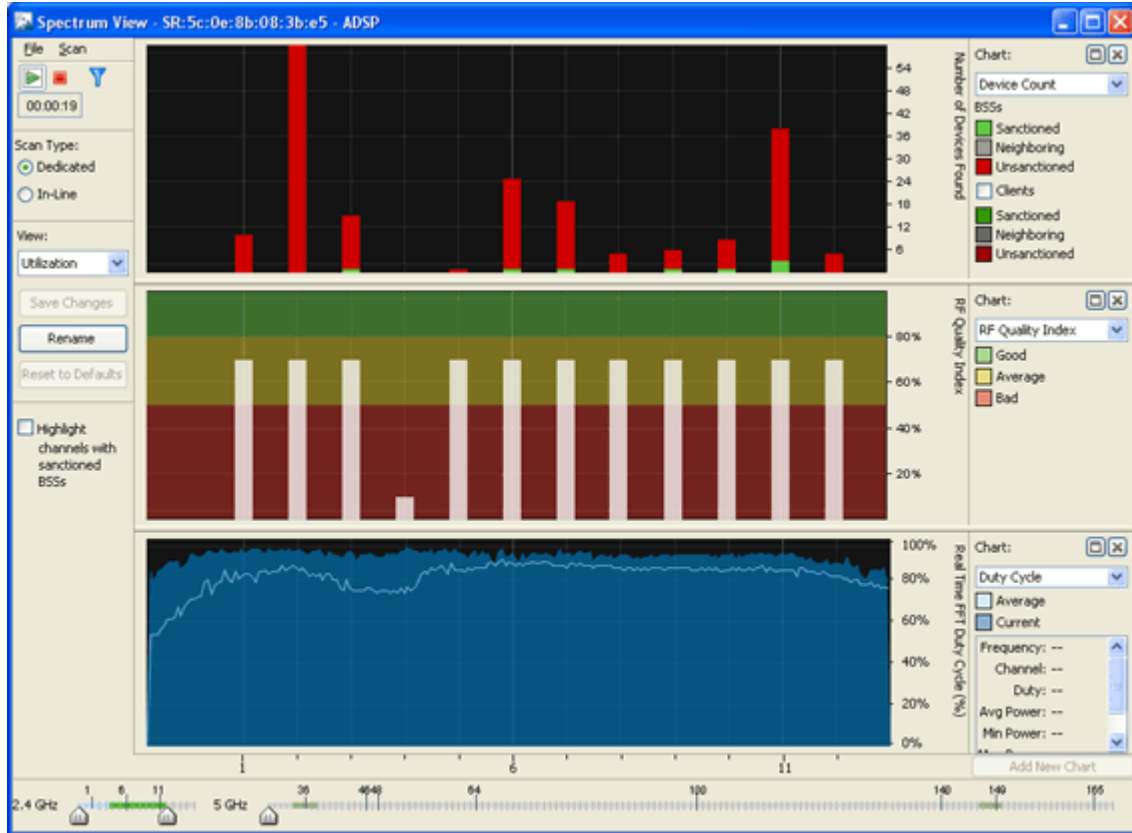
- Background Scanning
  - Part-time scanning of power spectral density (Layer 1), while sensor continues to scan for WIPS (Layer 2).
  - Generate 'RF Spectrum Analysis' alerts (BlueTooth, Microwave, Frequency Hopper, Continuous Wave)
- Dedicated Spectrum View
  - Sensor temporarily dedicated to Spectrum 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)



The [Spectrum Analysis](#) topic under *The GUI* fully explains how to use Spectrum Analysis.

## 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.

The [Advanced Spectrum Analysis](#) topic under *The GUI* fully explains how to use Advanced Spectrum Analysis.

---

## 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 under *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 shaing. 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 (LBS) 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.

LBS 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 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"><li>• Default Type</li><li>• Employee Device</li><li>• Employee Laptop</li><li>• Employee Phone</li><li>• High Priority Visitor Device</li><li>• Laptop</li><li>• Low Priority Visitor Device</li><li>• MCD</li><li>• Visitor Device</li><li>• VoIP Phone.</li></ul>
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: <b>Enter</b> , <b>Exit</b> , <b>Proximity</b> , and/or <b>Contained</b> .
Presence Base Event	Identifies which of the available presence based events the given device can trigger: <b>On Detect</b> and/or <b>On Exit</b> . 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 to the accuracy of location tracking.

---

## RSSI Scan Data

Devices can report RSSI scan data to ADSP. Sensor Operation settings (found under **Configuration > Operational Management**) has an option (**Enable Location Tracking RSSI Scan**) that allows you to use the RSSI scan 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.

---

## Reference Material

A good source of information is the *Proximity and Analytics — Location Based Services Design and Configuration Guide*. 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 *Proximity and Analytics — Location Based Services Design and Configuration Guide*, go to the Motorola Solutions support website for product manuals at the following URL <http://support.symbol.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.

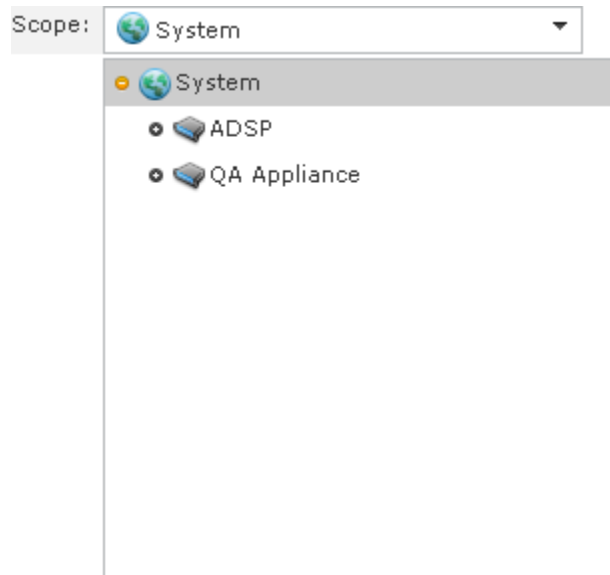
Once a Central Management license is installed, you must add the other appliances by navigating to [Menu > Add Devices](#). Select [Appliance](#) as your device type.

When you add an appliance, here are some things to remember:

- Ensure that the user accounts with the same username and password exist on both appliances (master and slave.)
- Ensure that the appliances have the same GUI software version.
- Ensure that you have all the licenses installed on the master appliance, not on the slave appliances. For example, you must have a Spectrum Analysis license on the master appliance to use it on the slave appliance.
- Before adding appliances, ensure that the Ping (ICMP) option is enabled in ADSPadmin. This allows the system to establish connections between appliances.

## Effects on the Dashboard

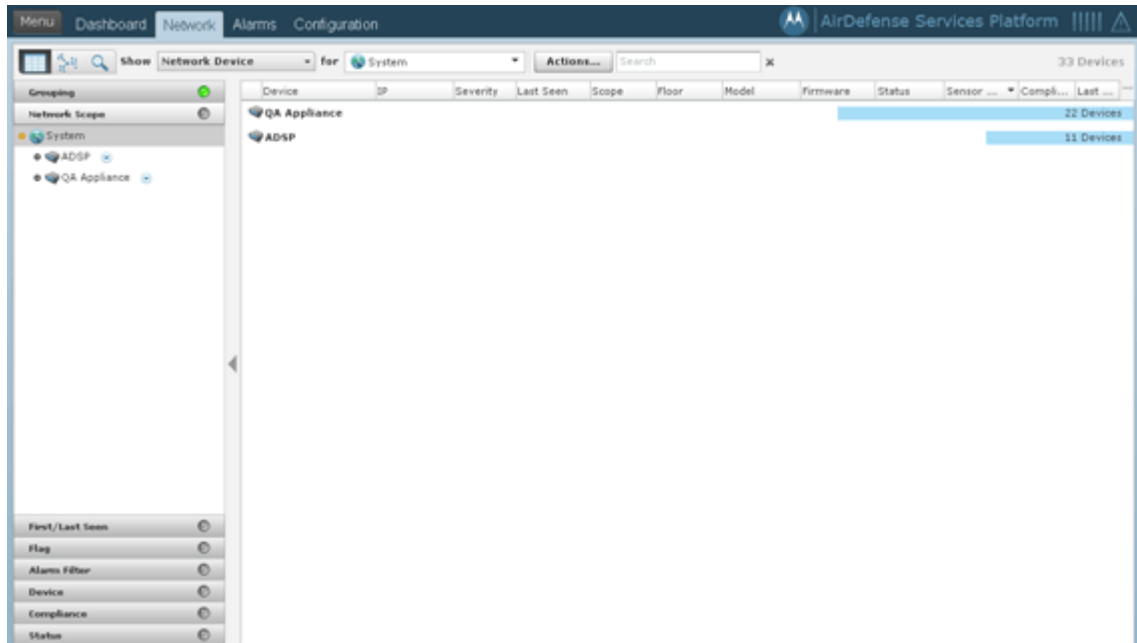
With a Central Management license, your Dashboard becomes a monitor of all appliances along with their associated devices. You can monitor your entire system at once or each individual appliance by selecting the appropriate scope all the way down to the floor level.



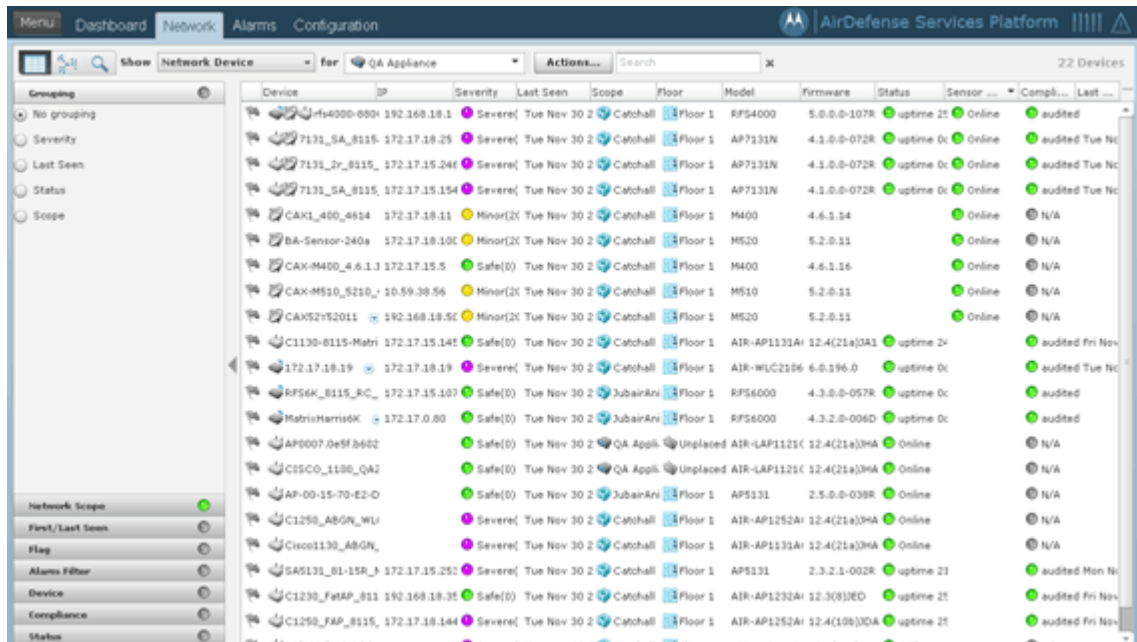
Selecting [System](#) as the scope displays a combination of all appliances being managed. Selecting an appliance or a network level of the appliance only displays that appliance or that network level and below.

## Effects on the Network Tab

A Central Management license allows you to display devices from any managed appliance in the [Network](#) tab. If displaying devices on a system level, on the device totals for the appliances are shown.



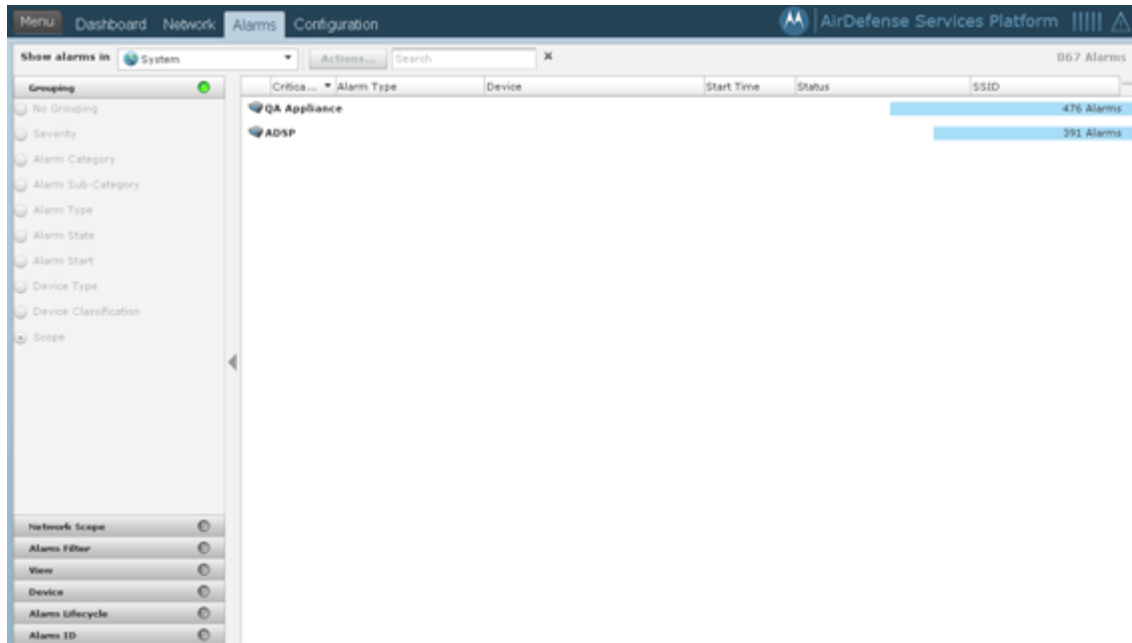
If displaying devices on an appliance level or a network level, only the devices for that appliance or network level are shown.



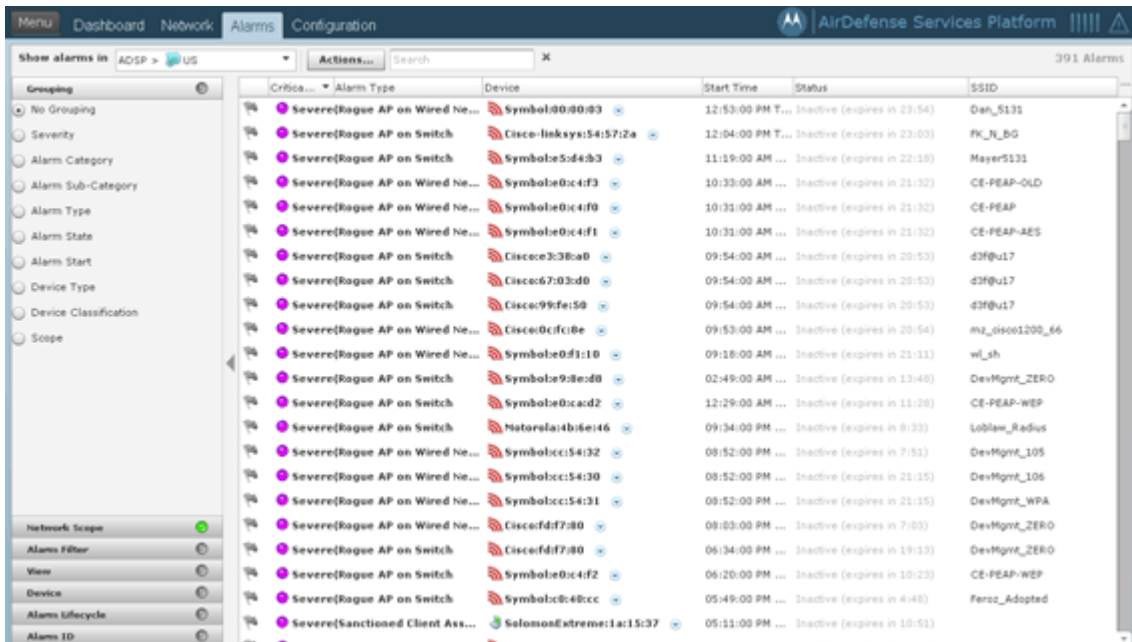
All other functions in the [Network](#) tab work the same.

## 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 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.
- PING—use this to enable or disable ICMP echo request responses.

- 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 the **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.

```

*** 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
(PING) Enable/disable ICMP Echo Request (ping) responses
(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 **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



**NOTE** The HNAME must be configured in the DNS server so that it can be resolved to an IP address. Also, the DNS server must be configured in ADSPadmin before the HNAME can be used in ADSP.

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.

---

## PING

You can enable PING by following these steps:

1. Type **PING** at the command prompt.  
A PING status message is displayed to alert you that PING is enabled or disabled.
2. At the prompt, type **e** to enable PING or **d** to disable.
3. Type **q** to return to the **Config** menu.

## 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

**UIPORT** is used to display the network port that must be used to access the dashboard.

1. Type **UIPORT** at the command prompt to display the network port the GUI is currently using.  
The UIPORT screen displays the current UI port used for dashboard access.
2. Press <Enter> to return to the previous 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	2-513
Access Point Testing Analysis Report	2-129
accessing location tracking	2-558
Account Access	2-473
Account Management	2-473
Action Control	2-119
Action Control commands	2-121
Action Control table	2-120
Action Rules	2-364
Actions	2-237
Activity Log	2-130
Adaptive Scan	2-437
Add Additional Floors	2-600
Add Devices	2-187
add devices	2-189
Add Devices - BSS and Wireless Clients Fields	2-188
Add Floors	2-285
Adding a Infrastructure Device Rule Set	2-412
Adding a Wireless Client/BSS Rule Set	2-406
Adding Certificates	2-451
Adding New AP Test	2-165
Adding New Assessments	2-179
Admin	1-14, 2-475
ADMU	8-8
Adoption History	2-42, 2-50, 2-101, 2-116
ADSP system time	1-17
ADSPadmin	8-1, 8-6
Advance Search	2-249
Advanced Forensic Analysis	2-51
Advanced Spectrum Analysis	2-569, 5-8
Advanced Troubleshooting	5-9
Air Termination	2-437
Air Termination System	2-440
AirDefense Server	1-1
AirWave dropdown menu	2-535
Alarm Action Manager	2-364
Alarm Configuration	2-391
Alarm Filters	2-255
Alarm ID Filter	2-267
Alarm Lifecycle Filter	2-266
Alarm Model	2-253
Alarm Severity Filter	2-225, 2-260
Alarm Table	2-254
Alarm Type Filter	2-226, 2-261
Alberta Netcare Provincial Organizational Wireless Readiness Assessment	2-126
Anomalous Behavior Alarms	2-394
AP placement	3-3
AP Test	5-1
Appliance Certificates	2-451
appliance dropdown menu	2-577
appliance keys	2-281
appliance level properties	2-621
Appliance Licensing	2-274
Appliance Management	2-439
Appliance Platform	4-3
Appliance Replacement Considerations	2-473
Appliance Settings	2-440
Applying a Profile	2-358
Applying an Device Action Manager Template	2-413
APs	2-36, 2-94
Area	2-591
Assessment Results	2-181
Association Analysis	2-21, 2-84
Assurance Suite (Network Assurance)	5-9
Audit Devices	2-240
Authentication, remote	2-485
Auto Refresh	2-489
Auto-Connect Feature	2-493
Auto-Licensing	2-297
Auto-Logout Enabled	2-441
Auto-Logout Timeout (Minutes)	2-441

Automated (Scheduled) Vulnerability Assessment	3-14
Automated AP Test	5-3
Automatic Backups	2-460
Automatic Frame Captures	2-555
Automatic Synchronization	2-472
Autoplace	2-621, 2-622
Auto-Placement Rules	2-293
Available Data Fields, Tables, and Charts	2-135

## B

Background Analysis	2-565
Background SA Scan	2-437
Background Scanning	5-7
Backup / Restore Status	2-442
Backup Recommendations	2-459
Bandwidth Analysis	2-35, 2-71
Basic navigation	1-16
BONDING (ADSPAdmin utility- also see Config program area)	8-1, 8-4
BSS Actions	2-238
BSS dropdown menu	2-516
BSS Inventory Report	2-128
BSSs & Wireless Clients	2-76
build a report	2-134
Building	2-591
Building a new report	2-132
Building your tree	2-284

## C

campus dropdown menu	2-588
Captive Portal Tab	2-159
Certificate / Key Validation	2-443
Certificate Manager	2-445
Certificate Types	2-446
Certificate Validation	2-443
Changing Certificate Password	2-456
Changing, passwords	2-481
Channel Analysis	2-33, 2-67
Channel Settings	2-344, 4-2
Charts, in reports	2-134
CISCO Device Example	2-502
Classification Filter	2-229
CLI Commands	2-359
CLI Configuration	2-355, 4-2
CLI Variable Scenarios	2-505
CLI Variables	2-360
Client Types	2-403
Columns, in reports	2-134
Command Line Interface	1-14
Command Line User	1-14
Command Run and Log	2-247, 2-362
Communication Settings	2-298

Compliance Filter	2-233
Compliance Reports	2-125
Config (ADSPAdmin program area- also see ADSPAdmin utilities)	8-1
Config settings screen	8-2
Configuration Backup	2-458
Configuration Clear	2-461
Configuration Examples	2-499
Configuration Notes	2-512
Configuration Restore	2-463
Configuring Data Fields, Tables, and Charts	2-136
Connection Settings	2-426
Connection Termination, and sensor placement	3-3
Connection Troubleshooting	2-140, 5-4
Copy MAC Formats	2-490
country dropdown menu	2-579
create a report	2-133
Create Network Levels	2-284
Create, report template	2-132
Creating and Changing Group Accounts	2-481
Creating Floor Plans	2-596
Creating Reports	2-122
Custom CLI Example	2-510
Custom Reports	2-132
Customizing Dashboard Views	2-202

## D

Dashboard Components	2-202
Data fields, in reports	2-134
Dbase (ADSPAdmin program area- also see ADSPAdmin utilities)	8-8
Dedicated Analysis	2-566
Dedicated Spectrum View	5-7
default user roles (types)	2-475
Deleting a report	2-137
Department of Defense Report	2-126
Deployment Considerations	3-2
Deployment overview	1-1
deployment requirements	2-494
Device Access	2-337
Device Action Manager	2-405
Device Age Out	2-415
Device Analysis	2-35, 2-69
Device Based	2-72
Device Based Forensic Analysis	3-10, 3-12
Device Density	3-3
Device Filter	2-231, 2-265
Device Firmware	2-340, 4-2
Device Functions Requiring More Explanation	2-537
Device Inactivity	2-490
Device Info	2-15, 2-37, 2-46, 2-77, 2-95, 2-109
Device Reports	2-128
devices dropdown menu	2-513

- DNAME (ADSPadmin utility-  
also see Config program area) . . . . . 8-1, 8-4
- DNS . . . . . 2-526
- DNS (ADSPadmin utility--also see Config program area)  
8-1, . . . . . 8-4
- DNS servers . . . . . 8-4
- Domain Name Server . . . . . 8-1
- Download Logs . . . . . 2-464
- dropdown menu for Access Points . . . . . 2-513
- dropdown menu for AirWave . . . . . 2-535
- dropdown menu for appliances . . . . . 2-577
- dropdown menu for BSSs . . . . . 2-516
- dropdown menu for buildings . . . . . 2-591
- dropdown menu for campuses . . . . . 2-588
- dropdown menu for cities . . . . . 2-585
- dropdown menu for floors . . . . . 2-594
- dropdown menu for network levels . . . . . 2-576
- dropdown menu for regions . . . . . 2-582
- dropdown menu for Sensors . . . . . 2-522
- dropdown menu for unknown devices . . . . . 2-531
- dropdown menu for unplaced devices . . . . . 2-620
- dropdown menu for Wired Switches . . . . . 2-529
- dropdown menu for Wireless Switches . . . . . 2-526
- dropdown menu WLSE . . . . . 2-533
- dropdown menus . . . . . 2-513
- dropdown menus for devices . . . . . 2-513
- dropdown menus for network levels . . . . . 2-576
- dropdown menus for Wireless Clients . . . . . 2-519
- Duration . . . . . 2-253
- E**
- EAP Key Generation and Certificates . . . . . 2-155
- Editing Floor Plans . . . . . 2-602
- Enable Location Tracking RSSI Scan . . . . . 2-437
- Environment Monitoring . . . . . 2-335, 3-9
- Exploits Alarms . . . . . 2-394
- Export Captured Frames . . . . . 2-149
- Export Devices . . . . . 2-247
- Export ZIP . . . . . 2-611
- Exporting . . . . . 2-457
- exporting a report . . . . . 2-139
- Extensive Traffic Data . . . . . 2-133
- F**
- File Format . . . . . 2-312
- Filters, in reports . . . . . 2-136
- First/Last Seen Filter . . . . . 2-223
- FISMA Federal Information Security  
Management Act Report . . . . . 2-126
- FIX7131 . . . . . 8-8
- Flag Filter . . . . . 2-224
- Floor Manipulation . . . . . 2-611
- floor manipulation tools . . . . . 2-557
- Floor Plan . . . . . 5-5
- Forensic Analysis . . . . . 2-10, 3-10, 3-11
- Forensic Analysis, Device Based . . . . . 3-12
- Forensic and Log Backup . . . . . 2-467
- Forensic Comparison Tab . . . . . 2-614
- Forensic RF . . . . . 5-6
- Frame Capture Analysis . . . . . 2-5
- Functional Roles . . . . . 2-477
- G**
- Generate a CSR . . . . . 2-452
- Generate Alarm Policy for New Devices . . . . . 2-314
- Generate Bill of Materials . . . . . 2-608
- GLBA Compliance Report . . . . . 2-126
- Graphical User Interface (GUI) . . . . . 1-14
- Grouping Filter . . . . . 2-218, 2-256
- Guest . . . . . 1-15, 2-475
- H**
- HALT . . . . . 8-8
- Helpdesk . . . . . 1-15, 2-475
- HHMM format . . . . . 8-5
- HHMMSS format . . . . . 8-5
- Hierarchy Filter . . . . . 2-221
- High-water mark . . . . . 2-254
- HIPAA Compliance Report . . . . . 2-126
- HNAME (ADSPadmin utility-  
also see Config program area) . . . . . 8-1, 8-4
- How Backups Work . . . . . 2-458
- How Synchronization Works . . . . . 2-471
- HTTP . . . . . 8-7
- HTTP (ADSPadmin utility-  
also see Config program area) . . . . . 8-2
- I**
- Import and Discovery . . . . . 2-190
- import appliance CLI command . . . . . 2-310
- import Auto-Placement Rules . . . . . 2-296
- Import CLI Variables . . . . . 2-245
- import communications settings . . . . . 2-303
- import device file format . . . . . 2-312
- Import PDF . . . . . 2-610
- Import Relay Server Information . . . . . 2-309
- import remote file . . . . . 2-191
- Import ZIP / SPZ . . . . . 2-609
- Import/Discover Devices . . . . . 2-190
- import/discover devices . . . . . 2-191, 2-192, 2-194
- Import/Discover Devices - Local File . . . . . 2-190
- Import/Discovery . . . . . 2-309
- importing a report . . . . . 2-138

Importing Auto-Placement Rules . . . . . 2-296  
 importing communications settings . . . . . 2-303  
 importing maps . . . . . 2-557  
 Infrastructure Alarms . . . . . 2-395  
 Infrastructure Device Rule Set . . . . . 2-412  
 Infrastructure Management . . . . . 2-336, 4-2  
 Infrastructure Management Reports . . . . . 2-131  
 INTCK . . . . . 8-8  
 IP (ADSPadmin utility-  
 also see Config program area) . . . . . 8-1, 8-2  
 IP address . . . . . 8-6  
 IPv4 . . . . . 2-525  
 IPv6 . . . . . 2-525, 8-1  
 IPv6 (ADSPadmin utility-  
 also see Config program area) . . . . . 8-3  
 IREPAIR . . . . . 8-8  
 IRESTORE . . . . . 8-8

**J**

Job Status . . . . . 2-415

**K**

Key Validation . . . . . 2-443

**L**

LAN Planner, and sensor placement . . . . . 3-5  
 Language . . . . . 2-468  
 LBS Alarms . . . . . 2-397  
 LBS Profiles . . . . . 6-1  
 license management . . . . . 2-274  
 Linux Installation . . . . . 2-4  
 Live Comparison Tab . . . . . 2-613  
 Live Monitoring session . . . . . 2-5  
 Live RF / Floor Plan dropdown menu . . . . . 2-594  
 Live RF Settings . . . . . 2-317  
 Live Tab . . . . . 2-612  
 Live View Filter . . . . . 2-543  
 Live View Settings . . . . . 2-542  
 LiveRF . . . . . 5-5  
 Local Authentication . . . . . 2-484  
 local file import . . . . . 2-190  
 local system time . . . . . 1-17  
 Locate . . . . . 2-556  
 Location & Region Events . . . . . 2-427  
 Location Analysis . . . . . 2-90  
 Location Based Services . . . . . 6-1  
 Location Tracking . . . . . 2-556  
 Location Tracking, and sensor placement . . . . . 3-3, 3-7  
 Log Level . . . . . 2-490  
 Login / SSH Banners . . . . . 2-468

**M**

Mail Relay Server . . . . . 2-440  
 Manage (ADSPadmin utility-  
 also see Config program area) . . . . . 8-8  
 Managing Profiles . . . . . 2-166, 2-181  
 Manual Backups . . . . . 2-459  
 Manual Frame Captures . . . . . 2-554  
 Manual Synchronization . . . . . 2-471  
 Meru Network Support . . . . . 2-210  
 MMDDYYYY format . . . . . 8-5  
 Mobile, and sensor placement . . . . . 3-5  
 Motorola AirDefense Sensor . . . . . 1-14  
 Move Devices . . . . . 2-243

**N**

NETPORT . . . . . 8-1, 8-3  
 Network Assurance . . . . . 2-317, 5-9  
 Network Device Actions . . . . . 2-237  
 network level properties . . . . . 2-621  
 network levels dropdown menu . . . . . 2-576  
 Network New Column Preferences . . . . . 2-491  
 Network Scope Filter . . . . . 2-222, 2-259  
 Network Structure . . . . . 2-283  
 Network Tab . . . . . 2-160  
 No Wireless Compliance Report . . . . . 2-126  
 North American Electric Reliability Corporation - Critical  
 Infrastructure Protection Standard . . . . . 2-127  
 NTP (ADSPadmin utility-  
 also see Config program area) . . . . . 8-1, 8-6

**O**

Observed Network . . . . . 2-149  
 Offline Sensor Report . . . . . 2-128  
 On Network Filter . . . . . 2-230  
 On-demand AP Test . . . . . 5-2  
 On-Demand Assessment . . . . . 2-170  
 On-Demand Vulnerability Assessment . . . . . 3-13  
 Operation Center . . . . . 1-15, 2-475  
 Operational Management . . . . . 2-363, 4-3  
 OUI . . . . . 8-8

**P**

PANIC (ADSPadmin utility-  
 also see Config program area) . . . . . 8-2, 8-7  
 PASSWD . . . . . 8-8  
 Password Reset . . . . . 2-485  
 Passwords, changing . . . . . 2-481  
 pcap file . . . . . 2-5  
 PCI DSS v1.1 Compliance Report . . . . . 2-127  
 PCI DSS v1.2 Compliance Report . . . . . 2-127

PCI Visa CISP Security Compliance Report . . . . . 2-127  
 Pending State Audit . . . . . 2-431, 4-3  
 Performance Alarms . . . . . 2-397  
 Performance Alarms Analysis Report . . . . . 2-129  
 Performance Analysis . . . . . 2-51, 2-118  
 Performance Network Utilization Report . . . . . 2-129  
 Performance Profiles . . . . . 2-323, 3-9  
 Performance Reports . . . . . 2-129  
 Physical and Electromagnetic Interference . . . . . 3-3  
 planned devices limitations . . . . . 5-7  
 Platform Health Alarms . . . . . 2-398  
 Policy Compliance Alarms . . . . . 2-399  
 Policy Enforcement, and sensor placement . . . . . 3-3  
 Policy-based Air Termination System Enabled . . . . . 2-441  
 Polling . . . . . 2-305  
 Port Lookup . . . . . 2-559  
 Port Suppression System . . . . . 2-441  
 Power and Data cabling . . . . . 3-4  
 Predictive RF . . . . . 5-6  
 predictive RF . . . . . 5-6  
 Presence Events . . . . . 2-428  
 properties for other levels except appliance level . . . . . 2-622  
 Push Configuration . . . . . 2-621, 2-622

## R

Radio Analysis . . . . . 2-43, 2-103  
 Radio Info . . . . . 2-44, 2-106  
 Radio Settings . . . . . 2-345, 4-2  
 Readiness Test . . . . . 2-562  
 REBOOT . . . . . 8-8  
 Reconnaissance Alarms . . . . . 2-400  
 Redundant Appliance Sync . . . . . 2-470  
 region dropdown menu . . . . . 2-582  
 Relay Server . . . . . 2-306, 4-3  
 Remote Authentication . . . . . 2-485  
 Remote authentication . . . . . 2-485  
 Remote File Fields . . . . . 2-191  
 Remove Devices . . . . . 2-243  
 Report Builder . . . . . 2-122, 2-132  
 report descriptions . . . . . 2-125  
 Reports, building . . . . . 2-132  
 Reports, creating . . . . . 2-122  
 Reports, templates . . . . . 2-132  
 RESTART . . . . . 8-8  
 Retrieve Diagnostic Logs . . . . . 2-241  
 RF-Domain . . . . . 2-342  
 Rogue Activity Alarms . . . . . 2-401  
 Rogue Detection, and sensor placement . . . . . 3-3  
 RSSI Data . . . . . 2-429  
 RSSI Scan Data . . . . . 6-2

## S

save a report . . . . . 2-133  
 Scan Mode . . . . . 2-438  
 Scan Tab . . . . . 2-176  
 Schedule Spectrum Analysis . . . . . 2-573  
 Scheduled AP Test . . . . . 2-149, 5-3  
 Scheduled Assessment . . . . . 2-178  
 Scheduled Tests . . . . . 2-164  
 Scheduled Vulnerability Assessment . . . . . 2-169, 3-14  
 Scope Based . . . . . 2-52  
 Scope Based Forensic Analysis . . . . . 3-10, 3-11  
 Scope Permissions . . . . . 2-477  
 Sections, in reports . . . . . 2-134  
 Security - Polled Filter . . . . . 2-236  
 Security - Sensed Filter . . . . . 2-235  
 Security & Compliance . . . . . 2-313  
 Security AdHoc Networks Report . . . . . 2-130  
 Security BSS Policy Violations Report . . . . . 2-130  
 Security Discovered BSSs Report . . . . . 2-130  
 Security Discovered Wireless Client Report . . . . . 2-130  
 Security Probing Wireless Clients Report . . . . . 2-130  
 Security Profiles . . . . . 2-286, 2-313, 3-9  
 Security Reports . . . . . 2-129  
 Security Rogue Detail Report . . . . . 2-130  
 Security Tab . . . . . 2-154, 2-173  
 Selecting Dashboard Scope . . . . . 2-201  
 Send CSR to a CA and Get Certificate Files . . . . . 2-452  
 Sensor Cloaking Limit . . . . . 2-441  
 Sensor Coverage Survey Process . . . . . 3-5  
 Sensor dropdown menu . . . . . 2-522  
 Sensor Inventory Report . . . . . 2-128  
 Sensor Monitoring . . . . . 3-9  
 Sensor Operation . . . . . 2-435  
 Sensor placement . . . . . 3-2  
 Sensor placement, and Location Tracking . . . . . 3-7  
 Sensor Quantity, Location, and Installation . . . . . 3-4  
 Sensor User Interface (Sensor UI) . . . . . 1-14  
 Sensors . . . . . 1-1, 2-25  
 SERVMOD . . . . . 8-8  
 setup prerequisites for zero touch  
 WLAN infrastructure deployment . . . . . 2-495  
 Sharing Certificates . . . . . 2-447  
 Sharing Certificates in Default State . . . . . 2-447  
 Sharing Certificates not in Default State . . . . . 2-449  
 Show Job Initiation Message Dialogs . . . . . 2-492  
 Signal Analysis . . . . . 2-24, 2-89  
 Signal Strength Filter . . . . . 2-234  
 Simple Components . . . . . 2-134  
 Single BSS Analysis Report . . . . . 2-128  
 Single Wireless Client Analysis Report . . . . . 2-128  
 SNMP Discovery . . . . . 2-192  
 SNMPA . . . . . 8-6  
 SNMPA (ADSPadmin utility-

also see Config program area) . . . . . 8-2  
 SNMPC . . . . . 8-6  
 SNMPC (ADSPadmin utility-  
 also see Config program area) . . . . . 8-2  
 SNMPT . . . . . 8-7  
 SNMPT (ADSPadmin utility-  
 also see Config program area) . . . . . 8-2  
 Software (ADSPadmin utility-  
 also see Config program area) . . . . . 8-8  
 SOX Report . . . . . 2-127  
 SOX Summary . . . . . 2-127  
 Spectrum Analysis . . . . . 2-9, 2-565, 5-7  
 Spectrum Scan Timeout . . . . . 2-441  
 Station Tab . . . . . 2-157, 2-174  
 STATUS . . . . . 8-8  
 Status Filter . . . . . 2-233  
 Switches . . . . . 2-45, 2-108  
 Synchronization Rules . . . . . 2-471  
 SYSLOG . . . . . 8-8

## T

Tables, in reports . . . . . 2-134  
 Terminate . . . . . 2-576  
 Threat Analysis 2-18, 2-26, 2-39, 2-48, 2-56, 2-80, 2-98,  
 2-112  
 Threat Breakdown . . . . . 2-29, 2-59  
 Throughput Tab . . . . . 2-161  
 TIME (ADSPadmin utility-  
 also see Config program area) . . . . . 8-1, 8-5  
 Time Stamp . . . . . 1-17  
 Time Window . . . . . 2-55  
 Toolkit Installation . . . . . 2-2  
 Track . . . . . 2-615  
 Traffic Analysis . . . . . 2-23, 2-30, 2-62, 2-86  
 Traffic Breakdown . . . . . 2-32, 2-64  
 Tree . . . . . 2-283  
 Tree Setup . . . . . 2-282, 2-284  
 Triangulation considerations, and  
 tree organization . . . . . 2-283  
 TRIMLOG . . . . . 8-8  
 Troubleshooting tool . . . . . 5-4  
 TZ (ADSPadmin utility-  
 also see Config program area) . . . . . 8-1, 8-5

## U

UI scope considerations, and tree organization . . 2-283  
 UIPORT (ADSPadmin utility-  
 also see Config program area) . . . . . 8-2, 8-8  
 Unknown Devices Actions . . . . . 2-238  
 unknown devices dropdown menu . . . . . 2-531  
 unplaced devices dropdown menu . . . . . 2-620  
 Updating Default Certificate Information . . . . . 2-455

Upgrade Devices . . . . . 2-244  
 Upload Image . . . . . 2-597  
 Use Proxy to Access Appliance . . . . . 2-491  
 user accounts, creating and changing . . . . . 2-478  
 User Preferences . . . . . 2-489  
 user roles . . . . . 2-474  
 User Session Limit . . . . . 2-440  
 User types . . . . . 1-14  
 User types (roles) . . . . . 2-475

## V

View Filter . . . . . 2-264  
 Viewing Certificates . . . . . 2-446  
 Viewing User Information . . . . . 2-477  
 Vulnerabilities Alarms . . . . . 2-402

## W

Web Reporting interface . . . . . 2-122  
 WEP Cloak . . . . . 2-437  
 WEP Cloaking . . . . . 3-3, 3-16  
 WiFi Direct Network Activity . . . . . 2-130  
 Windows Installation . . . . . 2-3  
 Wired Network Monitoring . . . . . 2-313, 3-9  
 Wired Switch dropdown menu . . . . . 2-529  
 Wireless Client Actions . . . . . 2-238  
 Wireless Client Inventory Report . . . . . 2-129  
 Wireless Client/BSS Rule Set . . . . . 2-406  
 Wireless Clients dropdown menu . . . . . 2-519  
 Wireless Manager/Switch . . . . . 2-194  
 Wireless Security Posture Details Report . . . . . 2-131  
 Wireless Switch dropdown menu . . . . . 2-526  
 Wireless Vulnerability Assessment (WVA) Scan . . 2-131  
 WLAN Management . . . . . 4-1  
 WLAN Profiles . . . . . 4-2  
 WLSE dropdown menu . . . . . 2-533  
 WS2000 Upgrades . . . . . 2-512

## Z

zero touch configuration . . . . . 2-494  
 Zero Touch WLAN Infrastructure Deployment . . . . 2-494





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.  
© 2014 Motorola Solutions, Inc. All Rights Reserved.

