AirDefense Services Platform 9.1.3 User Guide

TABLE OF CONTENTS

Chapter 4: The Dashboard

Chapter 5: Network

ABOUT THIS GUIDE

Introduction

This guide is designed to help you use the AirDefense™ Services Platform (ADSP) 9.1.3 Service Module. ADSP is designed to protect your network from wireless threats and attacks, maximize your wireless network performance and enforce policy compliance. As a standalone platform, ADSP is part of a system that includes the ADSP appliance. The ADSP appliance comes ready with the application and all supporting software preloaded.

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

This guide does not cover initial hardware installation or the basic device configuration you need to perform to get the appliance up and running. For hardware installation instructions, see the *AirDefense Services Platform 9.1.3 Appliance Installation Guide*, available at the following URL:

www.zebra.com/support

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 the Support Center for your region. Contact information is available at: *www.zebra.com/support*

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.

The Support Center staff responds to calls by email, telephone or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Support, you may need to return your equipment for servicing and will be given specific directions. We are 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 business partner, contact that business partner for support.

CHAPTER 1 SYSTEM OVERVIEW

Introduction

The AirDefense Services Platform (ADSP) is an advanced wireless intrusion prevention system (WIPS) providing automatic protection against wireless threats and a key layer of security for wireless VPNs, including encryption and authentication. The platform provides you with a cost effective and simplified way to fully customize your wireless management and monitoring solutions to meet organizational needs and industry requirements. ADSP offers:

- 24x7 Wireless Intrusion Prevention (WIPS)
- Network Assurance Tools
- Multi-vendor WLAN Infrastructure Management
- Proximity and Analytics capabilities
- Forensic Analysis capabilities.

These tool-sets are seamlessly integrated into a single console to simplify the operation and security of your wireless network. With the device management system, you can manage your network remotely from a central location.

ADSP consists of program areas and drill-down views. Each view gives you more details to help troubleshoot specific threats or performance problems reported by the AirDefense Services Platform. The comprehensive configuration features give you full control over your network from a central location.

ADSP in Standalone Mode

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.

ADSP/WiNG Unified Mode Platform

In Unified Mode, WiNG and ADSP work together as a single integrated application. ADSP runs as a virtual machine (VM) on an NX controller with WiNG as the operating system. You can install ADSP as a VM on the WiNG NX95x0 controller running WiNG 5.5.2 and later.

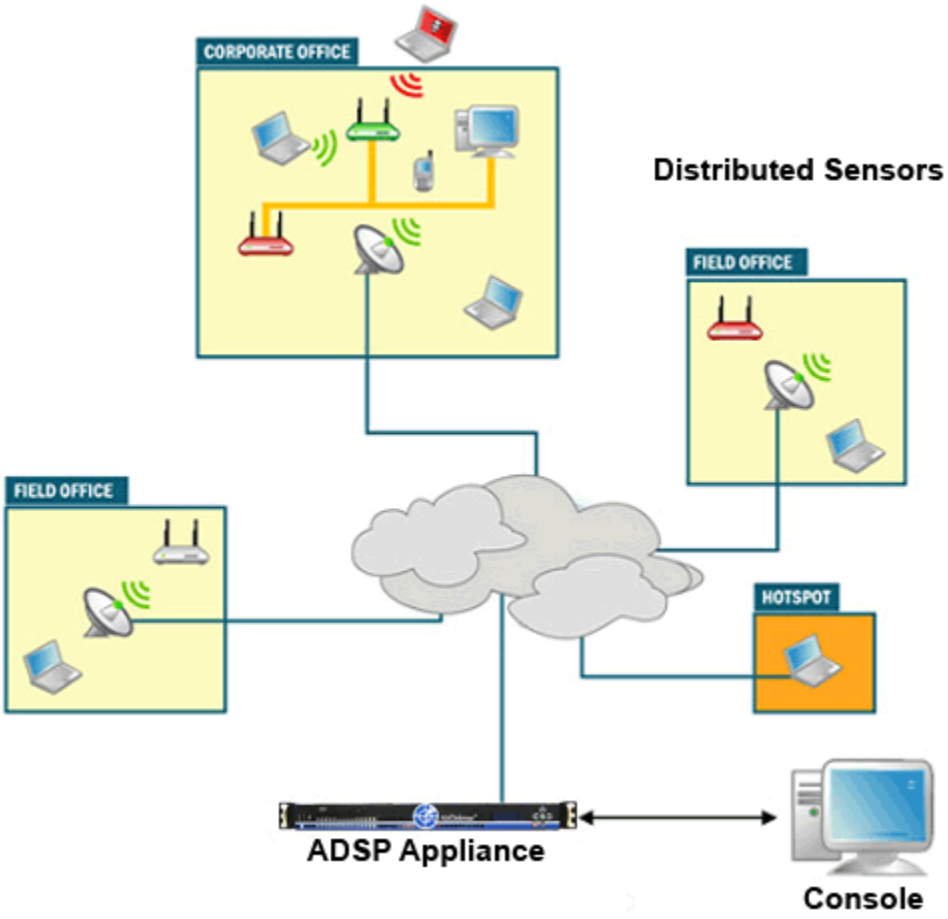
✓ *NOTE* ADSP/WiNG Unified Mode is supported only on WiNG NX95x0 SKU, not on ADSP NX95x0 SKU.

The WiNG and ADSP tree hierarchies are synchronized and the ADSP network assurance tools are available for both applications. You will need to install all required ADSP licenses.

✓ *NOTE* Unified Mode will no longer be supported going forward. Version 9.1.3-10 is the last ADSP release that will support Unified Mode. We recommend that existing Unified Mode customers migrate to standalone mode.

System Components

ADSP provides advanced Wireless LAN monitoring with a distributed architecture of remote sensors and APs that communicate with a centralized server (appliance.) A basic ADSP system consists of an AirDefense appliance and one or more sensors.



The ADSP remote sensors collect frames being transmitted by 802.11a-, ac, b-, g-, and n-compliant devices, and sends that data to a central ADSP appliance for analysis and correlation.

System Requirements

Supported Hardware Appliances

- Model NX95x0
- Model SV-4250
- Model SV-3652
- Model SV-1252.

NOTE

- ADSP 9.0.x and later do not support legacy appliances without 64-bit OS support. Customers that have a 32-bit server cannot upgrade beyond 8.1.3.
- ADSP 9.1.x and later do not support legacy appliances without 2GB of RAM or greater. Customer that have a 1GB server cannot upgrade beyond 9.0.3.

Supported Browsers

- Firefox 32 and higher
- Internet Explorer 9 and higher
- Google Chrome 37 and higher.

Flash Player 10.1 or later is required.

Supported OS

- Windows 7
- Linux

Version Compatibility for Upgrade

Version 9.1.3-10

For version 9.1.3-10, you can upgrade directly from versions 9.1.2-17 or 9.1.2-17a6. Direct upgrade from any other version is not supported.

NOTE For existing customers who would like to upgrade to 9.1.3, you must have an ADSP support contract. Please contact your Zebra Technologies sales person if you currently do not have a support contract and would like to receive access to software updates for this product.

WiNG Version Compatibility

ADSP 9.1.3 is compatible with the following versions:

- WiNG 5.5.6; with the exception of the NX9600 running WiNG 5.5.6
- WiNG 5.7
- WiNG 5.7.1
- WiNG 5.7.2
- WiNG 5.8 has been tested against ADSP 9.1.2a6, but not yet tested against ADSP 9.1.3.

NOTE See the section titled *DFS Tables, Sensor and Radio Share* in the corresponding WiNG release notes for a detailed matrix of sensor features supported for each AP in that WiNG release.

Connecting to Hardware Appliance

Connect a Laptop

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 AirDefense Operations.

Connect a Monitor and Keyboard

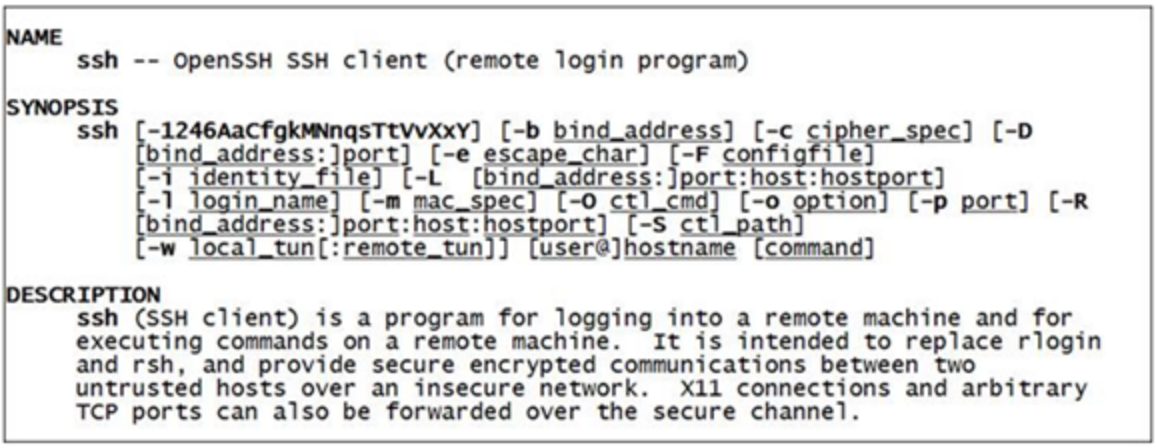
You can physically connect a monitor, keyboard and mouse to the appliance. Use the connectors (such as PS2 or USB) to plug in to the server directly.

Access Appliance Remotely

To access the appliance remotely, use the SSH protocol 2.

NOTE You must have a client that supports SSH protocol 2 installed on the remote workstation used to connect to the ADSP appliance. If you attempt to use SSH protocol 1, you will receive a protocol error message in **syslog**.

Launch your SSH client and connect to the IP address of the ADSP appliance. See the following example:



```
NAME
     ssh -- OpenSSH SSH client (remote login program)

SYNOPSIS
     ssh [-1246AaCfgkMNnqsTtVvXxY] [-b bind_address] [-c cipher_spec] [-D
         [bind_address:]port] [-e escape_char] [-F configfile]
         [-i identity_file] [-L  [bind_address:]port:host:hostport]
         [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port] [-R
         [bind_address:]port:host:hostport] [-S ctl_path]
         [-w local_tun[:remote_tun]] [user@]hostname [command]

DESCRIPTION
     ssh (SSH client) is a program for logging into a remote machine and for
     executing commands on a remote machine.  It is intended to replace rlogin
     and rsh, and provide secure encrypted communications between two
     untrusted hosts over an insecure network.  X11 connections and arbitrary
     TCP ports can also be forwarded over the secure channel.
```

Configuring the Appliance

You will need to configure your ADSP appliance after the initial installation.

✓ *NOTE* For details on installing the ADSP appliance, see the *AirDefense Services Platform Appliance Installation Guide* at the following URL: www.zebra.com/support

The following table shows the basic activities you will need to perform to commission your ADSP appliance.

ADSP Basic Commissioning	
Planning and Assessment	Review your security policies, network infrastructure and WLAN sensor coverage requirements, and then establish your ADSP policy configuration.
Analysis and Design	Develop a system implementation design tailored to your specific wireless security requirements.
Appliance Implementation	Configure the ADSP appliance to work with your wireless infrastructure as required. (You can also commission additional appliances as needed.)

Add-On Modules

You can add on modules in order to customize AirDefense to fit your needs. You can add one module or multiple modules, categorized as follows:

- Security and Compliance
- WLAN Management
- Proximity Awareness

- Network Assurance.Mac (Thin Client Applications Only)

Module	Actions	Category
WIPS (Wireless Intrusion Prevention System)	• License and configure. License is per sensor. • Set up the automated configuration for policies and associated devices. • Configure optimal rogue detection and mitigation. • Define and tune threat monitoring policy.	Security and Compliance
Part-time WIPS	• License RadioShare WIPS. License is per AP. Install licenses based on number of APs.	Security and Compliance
Wireless Vulnerability Assessment	• License and configure.License is per sensor.	Security and Compliance
Advanced Forensics	• License and configure. License can be per sensor or per AP (RadioShare licenses).	Security and Compliance
WLAN Management	• License and configure. • Create the device profile template. • Build reports. • Install firmware updates and upgrades as needed. • Create and import one (1) template for wireless controllers and one (1) for APS—as required.	WLAN Management
Presence Service	• License and configure. Comes with Proximity licenses.	Proximity and Awareness
Wi-Fi- Analytics	• License and configure. Comes with Proximity licenses.	Proximity and Awareness
Zone Tracking	• License and configure. Comes with Proximity licenses.	Proximity and Awareness
Position Tracking	• License and configure. Comes with Proximity licenses.	Proximity and Awareness
Historical Location Analysis	• License and configure. Comes with Proximity licenses.	Proximity and Awareness
Spectrum Analysis	• License and configure. License can be per sensor or per AP (RadioShare licenses).	Network Assurance
Advanced Troubleshooting	• License the ADSP appliance. License can be per sensor or per AP (RadioShare licenses).	Network Assurance
Connectivity Troubleshooting	• License and configure. License can be per sensor or per AP (RadioShare license).	Network Assurance

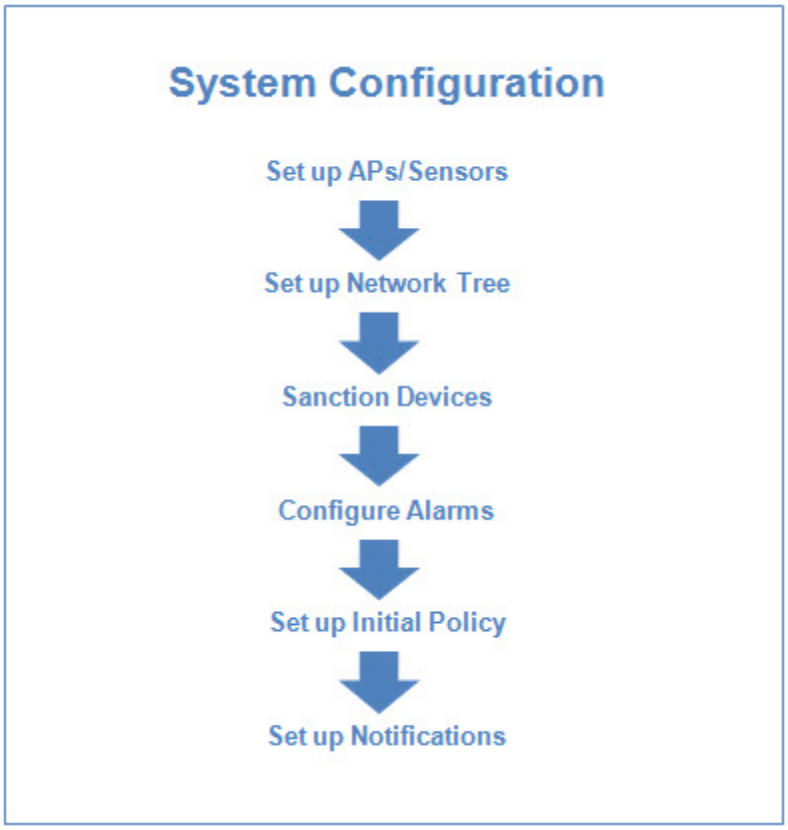
Module	Actions	Category
Live RF	• License and configure. License can be per sensor or per AP (RadioShare license). • Import the maps as required for specific floors.	Network Assurance
AP Testing	• License and configure. License can be per sensor or per AP (RadioShare license).	Network Assurance
Central Management	• License and configure.	Central Management Console (CMC)

Hardware Dependencies

Certain software modules may be hardware dependent. For example, Spectrum Analysis is dependent on the radio chipset, which varies between hardware platforms. Other software modules such as AP Testing or Wireless Vulnerability Assessment require a client on each sensor, which may also be hardware dependent. Please verify hardware and firmware requirements for each software module needed.

System Configuration

In order to configure ADSP, you will need to follow the steps shown in the following chart:



Deploying APs and Sensors

Selecting APs and Sensors

Consider the following points when selecting your access points (APs) and sensors:

- Most AP models can have internal or external antennas. APs with internal antennas work best in an indoor environment. AP/Sensors with external antennas work best for warehouse deployments, mount-in-plenum spaces or deployments where specialized antennas may be required.
- AP and sensor SKUs can be ordered for different RF domains to comply with regulatory requirements. Shipping locations may be limited by configured RF domain.

Supported APs

- AP 6511
- AP 621, AP 6521
- AP 622, AP 6522, AP 6562
- AP 650, AP 6532
- AP 7131, AP 7161, AP 7181
- APs 7522, 7532 (9.1.2 or later)
- AP 7652 (standalone)
- AP 8122, AP 8132, AP 8163
- AP 8232 (with 3rd radio sensor module only)
- TW 511

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

Off-Channel Scanning (OCS)

RadioShare and off-channel scanning (OCS) work hand-in-hand to allow either or both radios to carry client data and act as a sensor, providing dual-band sensing. OCS essentially allows the AP to tune its radio to a different channel for a finite amount of time.

Example:

An AP that is providing client access on channel six will monitor other channels as well. The AP will stay on channel six for 10 seconds. During the 10-second interval, the AP is capable is sending transmissions to an associated client as well as receiving transmissions from an associated client. After the 10-second interval, the AP will listen off-channel on channel seven for 110 ms. This

round-robin method of off-channel scanning is used by the APs to listen for the transmissions of other APs as well as monitor for any other RF transmissions off-channel.

NOTE When utilizing OCS, the APs/sensors will require more time for detection of threats than when utilizing a dedicated sensor. The amount if time required depends on several factors, e.g. data load, timing and the channel where the threat is active.

Setting Up APs and Sensors

In order to implement WLAN monitoring, you must set up APs and sensors in the vicinity of the airwaves carrying the WLAN traffic. The AirDefense smart sensors passively observe all wireless LAN traffic within 40,000 to 60,000 square feet of typical office space. The sensors collect and analyze data on the wireless network by monitoring the following factors:

- Wireless devices present on the network, along with their associations
- Devices using encryption and authentication
- Device vendor information
- Total data transferred.

Modifying Resources

In standalone mode, you can modify the ADSP resources by using the CLI interface. In Unified Mode, you can make changes to the virtual machine from the WiNG Application Center. However you cannot exceed the maximum resources allowed.

NOTE Before you make changes to resources in Unified Mode, you must stop the ADSP virtual machine.

Connecting to the Network

There are various methods of connecting to the network. You should always use the most secure connection possible. When connecting via browser, use SSL (https:443) when possible.

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

Assigning 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 interface 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)	AirDefense Sensor	Sensor Configuration	Sensor User

For detailed information on configuring and assigning user accounts, refer to Chapter 7, *Configuration*, and the sections on *Account Management* and *Account Access*.

Default Login

The default GUI login for ADSP is **admin**/**admin123**.

User Accounts

ADSP has one default Admin User account. Admin Users may 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 Admin User uses four templates to create user accounts with permissions. These templates 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.
- Help desk—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 Admin User can bypass the templates and customize user accounts to fit your needs.

System Access 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.

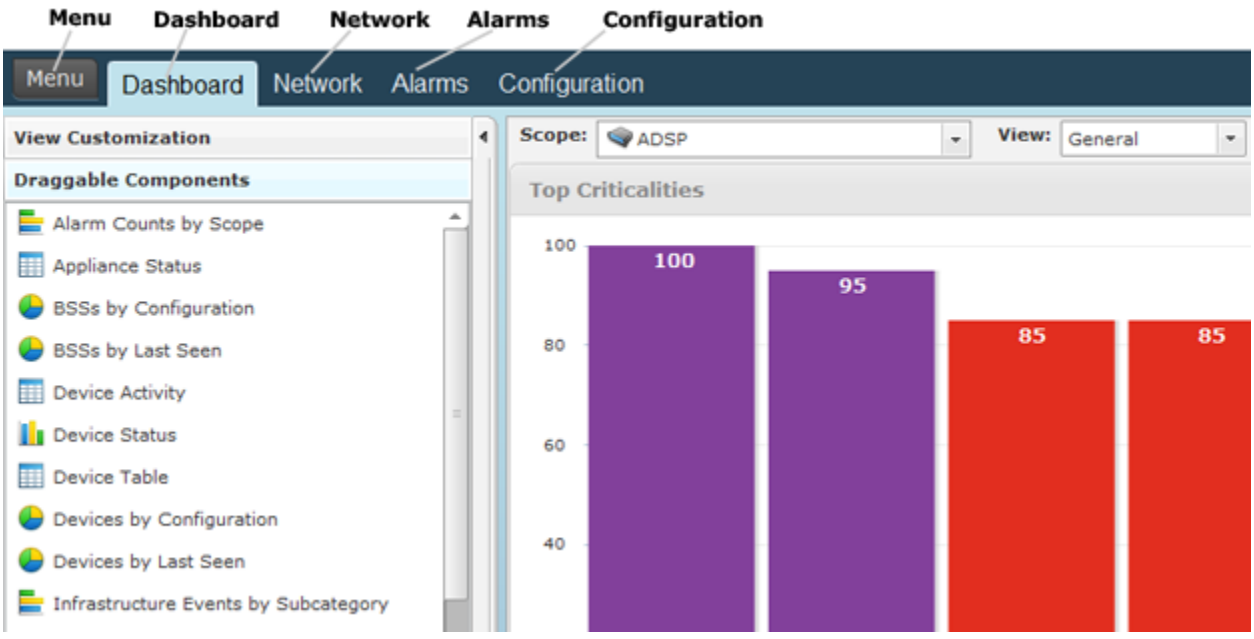
Example:

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

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 ADSP GUI will make it easy to navigate. The following graphic shows where to find the elements described below.



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

Tree Structure

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

NOTE In Unified Mode the tree structure is controlled by the WiNG OS.

Device Search

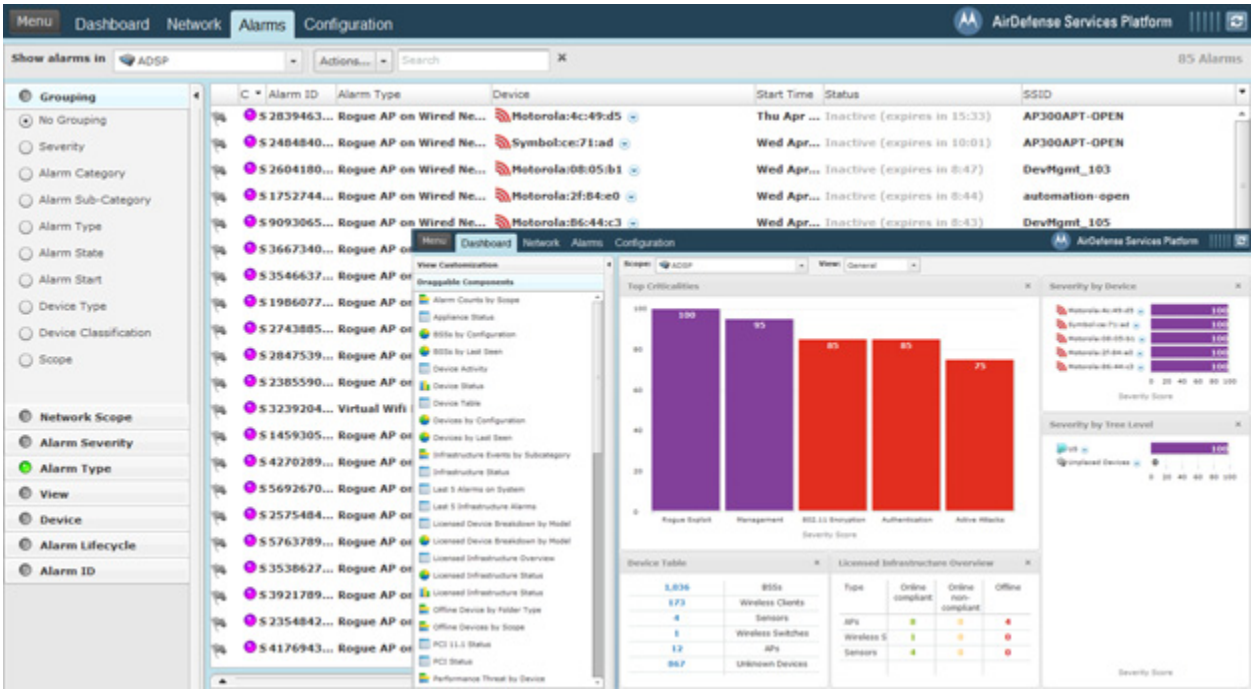
The **Network** tab contains a search option that enables you to find specific devices that are being detected by ADSP.

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. For 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.

Alarm Time Reporting

ADSP reports alarms and device information and traffic statistics every minute. To understand the data that appears in ADSP, you must understand how ADSP addresses system time versus the local GUI time, particularly in regard to alarms.

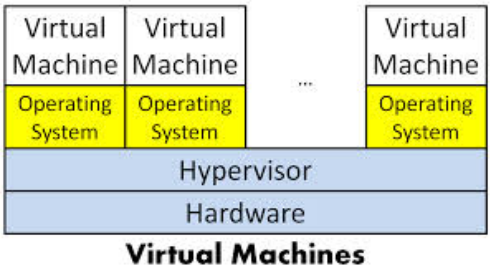
When an alarm occurs, ADSP detects the alarm in system time, and records this time in its database. You can configure ADSP system time by using the Command Line Interface (CLI) found in the **Config** menu.

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.

CHAPTER 2 ADSP ON VIRTUAL PLATFORM

Introduction

AirDefense Services Platform (ADSP) can be pre-loaded on an appliance or can run as a virtual machine (VM) on a supported virtual platform. When you install the AirDefense platform on a hypervisor (for example, the Xen Project™ Hypervisor 4.x) it appears that ADSP has the host hardware's processor, memory and resources.



Virtual Machines

This chapter provides step-by-step instructions on how to install the AirDefense Services Platform (ADSP) on a virtual platform.

Prerequisites

Supported Virtual Platforms

You can install ADSP as a VM on the following virtual platforms:

- VMware® vSphere 5.0 (ESXi)
- Xen Cloud Platform (XCP) 1.6
- Xen Hypervisor 4.x

Required Files

Depending on the platform that you want to install ADSP on, you must download one file for VMware and Xen Cloud Platform, or two files for Xen Hypervisor:

- AD-VM-adsp-9-0-3-23-dvd.ova (VMware)
- AD-VM-adsp-9-0-3-23-dvd.xva (Xen Cloud Platform)
- AD-VM-adsp-9-0-3-23-dvd.gz and AD-VM-adsp-9-0-3-23-dvd.xm (Xen Hypervisor).

You can download the four files from Zebra Technologies Support at the following URL: *www.zebra.com/support*

Required License

You must have an ADSP Platform license in order to use ADSP on a virtual platform.

Required System Configuration

The following CPU, memory and hard disk configuration is required for installation of ADSP on virtual platforms to support appropriate network devices:

Platform Category	vCPUs for ADSP VM (on Intel 2.33GHz Xeon or equivalent)	Memory for ADSP VM	Hard Disk for ADSP VM	Scanning Sensors	RadioShare non scanning	Network Devices	Active WLAN Devices	Total WLAN Devices
Advanced	16	36GB	2x1TB	1700	2550	14,875	68,000	306,000
High-End	8	8GB	2x500GB	850	1275	8925	34,000	191,250
Mid-Level	4	4GB	2x250GB	425	637	4165	17,000	76,500
Entry-Level	2	2GB	1x250GB	85	85	595	3400	15,300

✓ *NOTE* In a multi-VM environment, over-allocation of CPUs to other VMs could potentially impact performance of ADSP VM.

✓ *NOTE* Higher sensor count will cause forensic analysis to take longer to run.

Upgrading ADSP Versions

Standalone to UM

To upgrade an existing standalone installation to a Unified Mode installation, you must be running ADSP 9.1.0 or later. If a system planned for migration to Unified Mode is currently running 9.0.x or earlier, then the system should be upgraded to 9.1.0 prior to making a backup. The 9.1.0 system should be checked to assure the restore is correct prior to continuing with the installation.

✓ *NOTE* Restoring a standalone backup from a 9.0.x or earlier system to a 9.1.2 or 9.1.3 Unified Mode system is not supported.

Unified Mode to 9.1.3

To upgrade a Unified Mode installation from 9.1.2-17/ 9.1.2-17a6 to 9.1.3, use the following procedure

1. Upload the 9.1.3-10.tar unified mode firmware file to /usr/local/tmp. You can use a tool like WINSCP for this.
2. Use the “virtual-machine console adsp” command on the NX9500.
3. Use the WIPSadmin/Software/Servmod command to install the upgrade.

Configuring ADSP as a VM

The Virtual Machine Console is a remote access feature that allows you to configure ADSP as well as perform maintenance functions. You can also use the CLI console to monitor ADSP as it is booting up or shutting down.

```
nx9500-dc-1# virtual-machine console adsp

To disconnect from the console, press: 'CTRL+]'

ADSP release 9.1.0-b32

adsp-1.tmelabs.local login: smxmgr
Password: smxmgr

****** ADSPadmin ******


choose from the following:

(M)   Manage
(D)   Dbase
(S)   Software
(C)   Config
```

1. From the NX9500 command line, enter the command: **virtual-machine console adsp**. The system boots up as ADSP with the current release number.
2. Log in as ***smxmgr*** with the password: ***smxmgr***. This logs you in to the ADSPadmin menu.

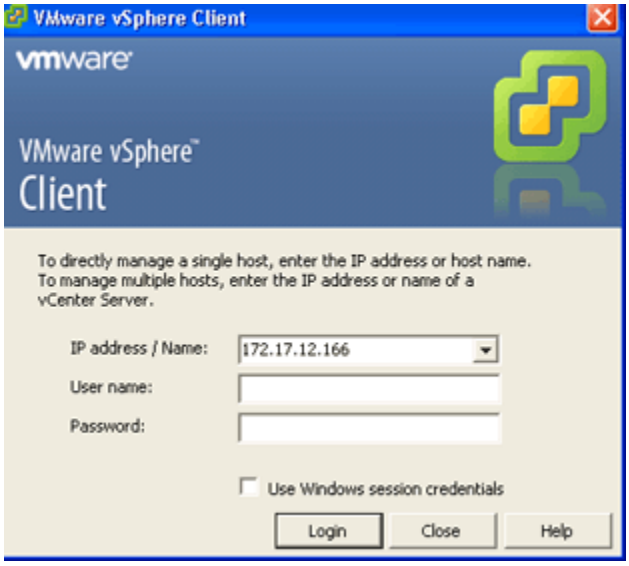
> ***NOTE*** To disconnect from the console, press CTRL+].

Choose from the commands to monitor, configure and maintain ADSP. For details on configuring ADSP from the ADSPadmin console, see the section on *Using ADSPadmin to Configure ADSP*.

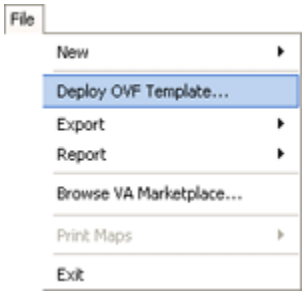
Installing ADSP 9.1.3 on VMware

Follow these steps to install ADSP on **VMware**:

1. Install VMware ESXi according to the instructions located at https://my.vmware.com/web/vmware/evalcenter?p=vmware-vsphere51-ent
2. Install the vSphere Client to install and manage the ADSP VM running on a VMware ESXi host. Follow the vSphere Client instructions located at https://my.vmware.com/web/vmware/evalcenter?p=vmware-vsphere51-ent
3. Once **VMware** is installed, double-click the VMware **vSphere Client** icon on your desktop to access the VMware vSphere server.

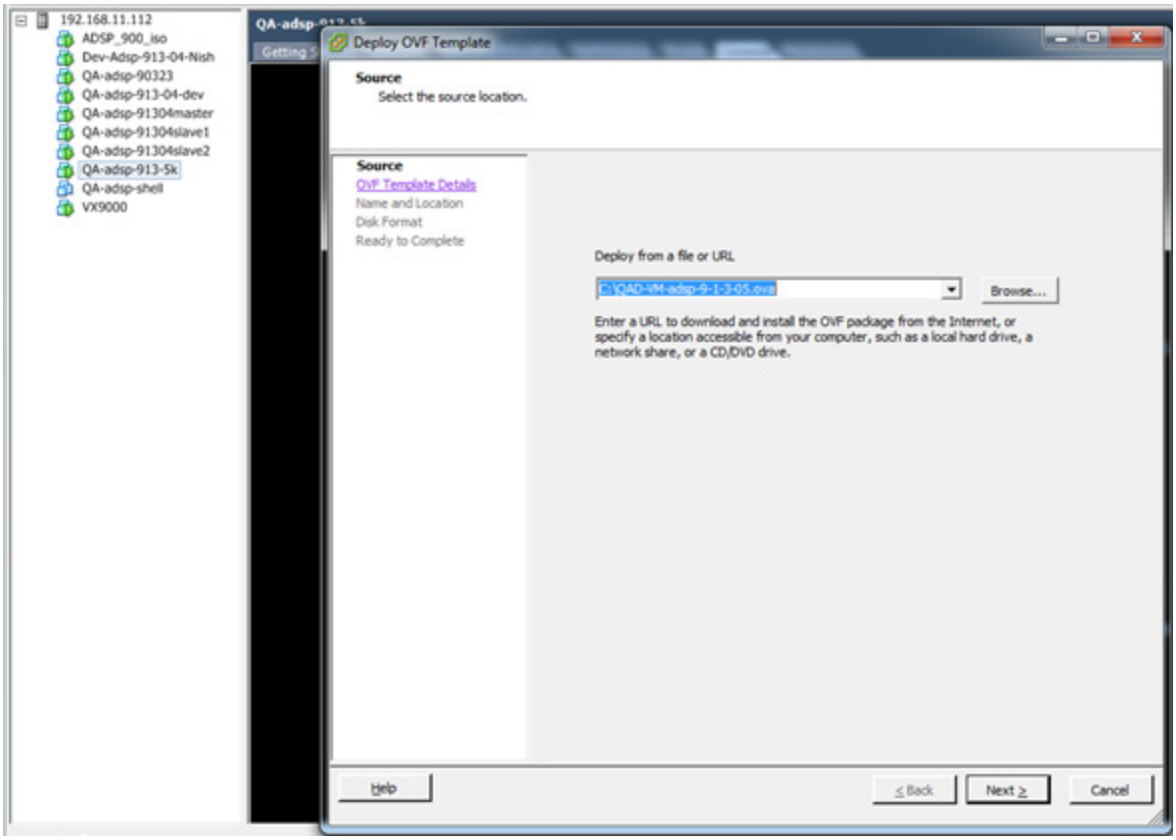


4. Enter your user name and password; then, click **Login**.
5. Select **File** > **Deploy OVF Template**.

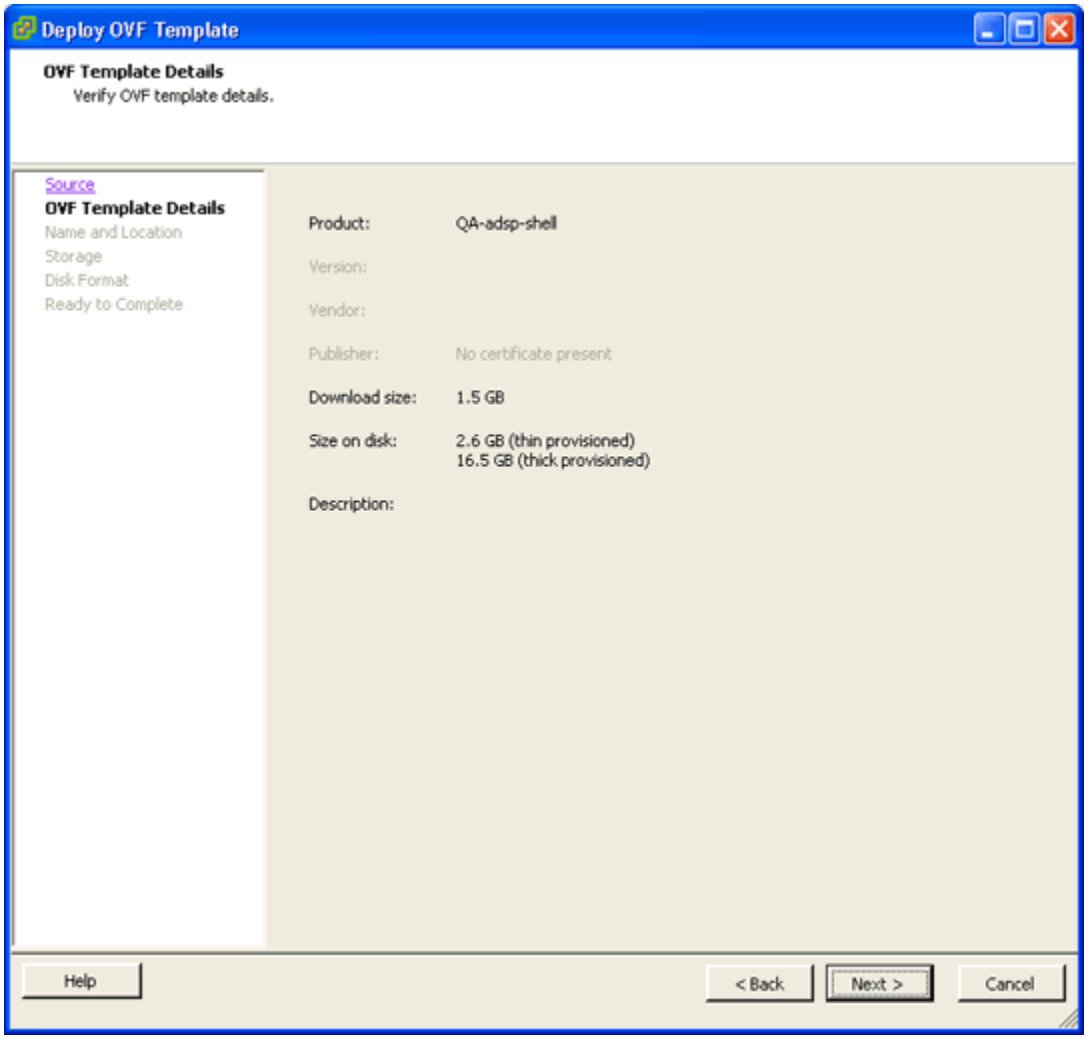


The **Deploy OVF Template** window is displayed.

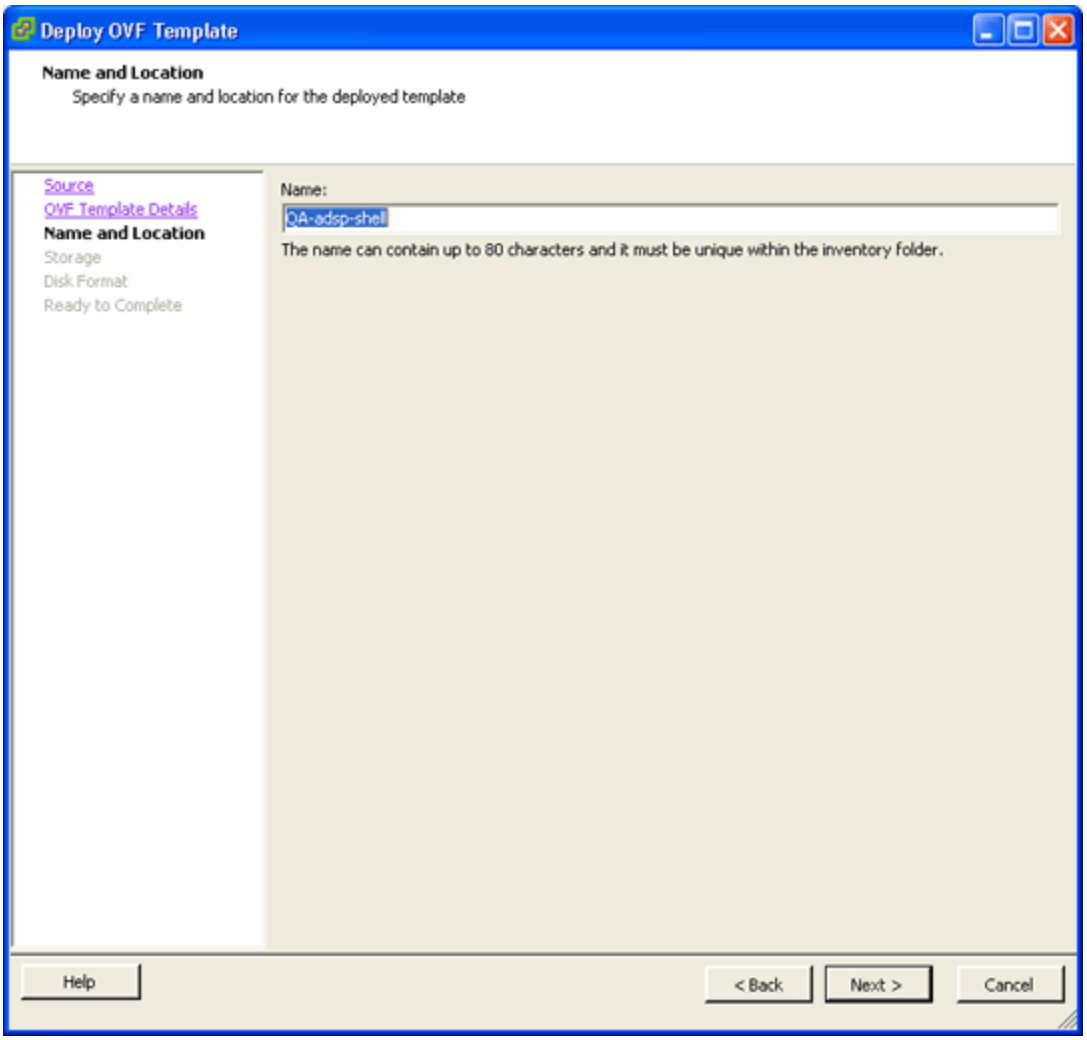
6 Click **Browse** and select the **VMware** image for the latest version of ADSP. In the following example, you would select the **QAD-VM-adsp-9-1-3-05.ova** file from your local PC.



7 Click **Next**. The OVF template details window displays.

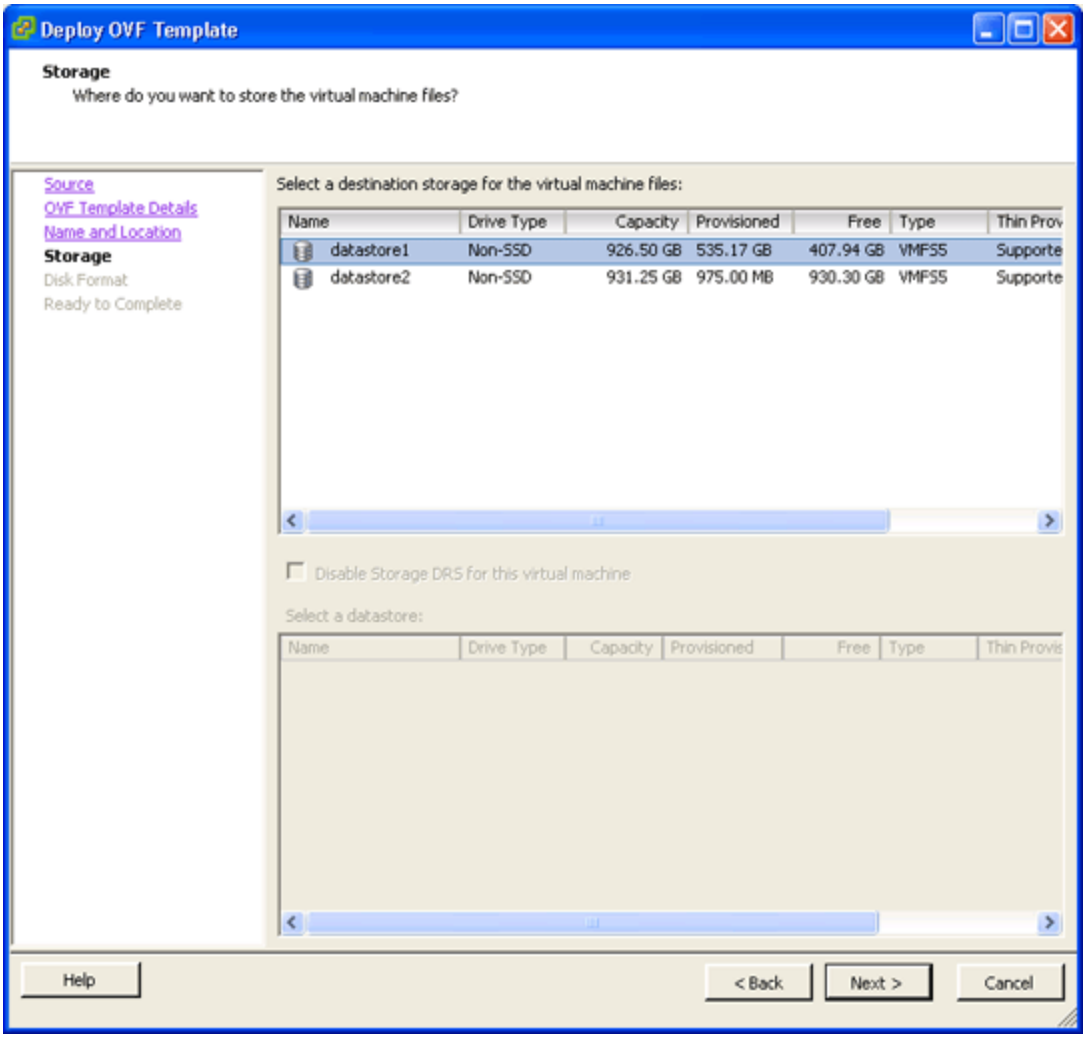


8 Verify the OVF template details and then click **Next.** The Deploy OVF Template window displays.

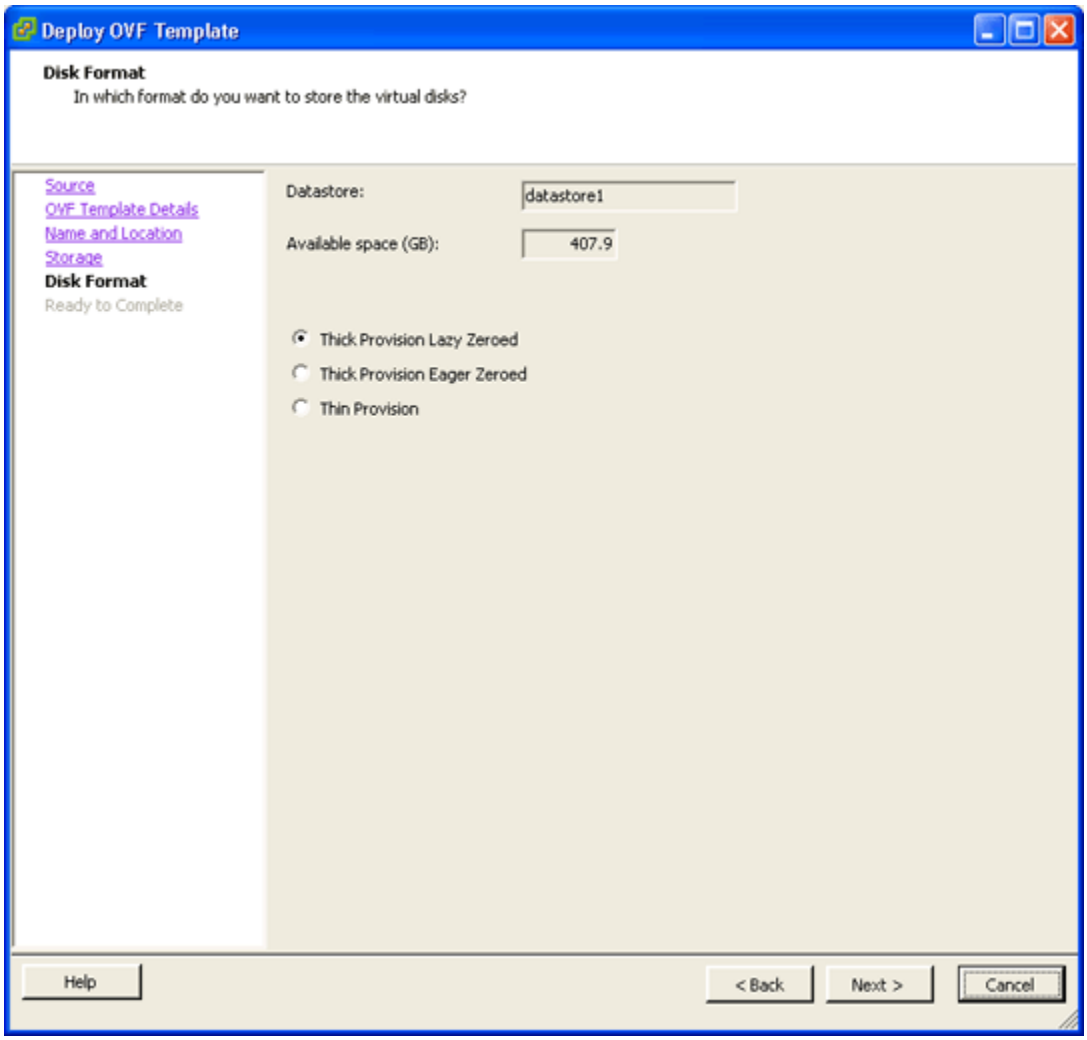


9 Enter a name (for example, **adsp-shell**) and then click **Next**.

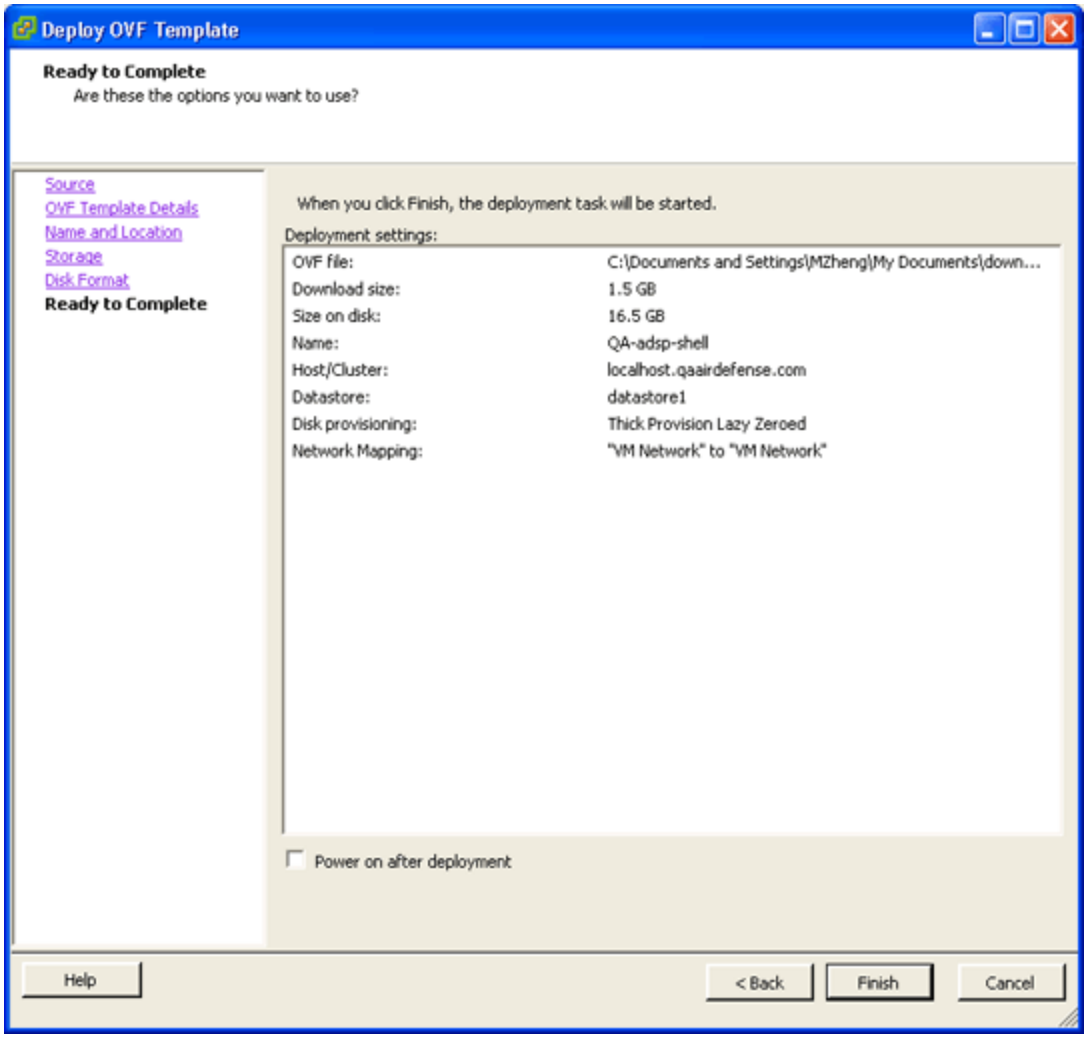
10 You must select a destination for storage of the VM files. For example, datastore1, and then click **Next**.



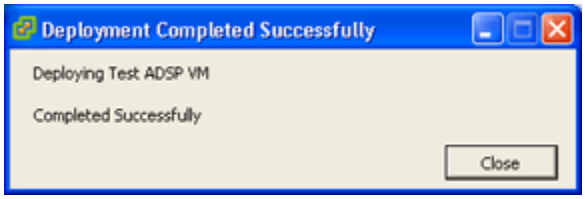
11 Select a **Disk Format** and then click **Next**.



12 Verify the information. De-select **Power on after deployment** if it is selected and then click **Finish** to deploy.



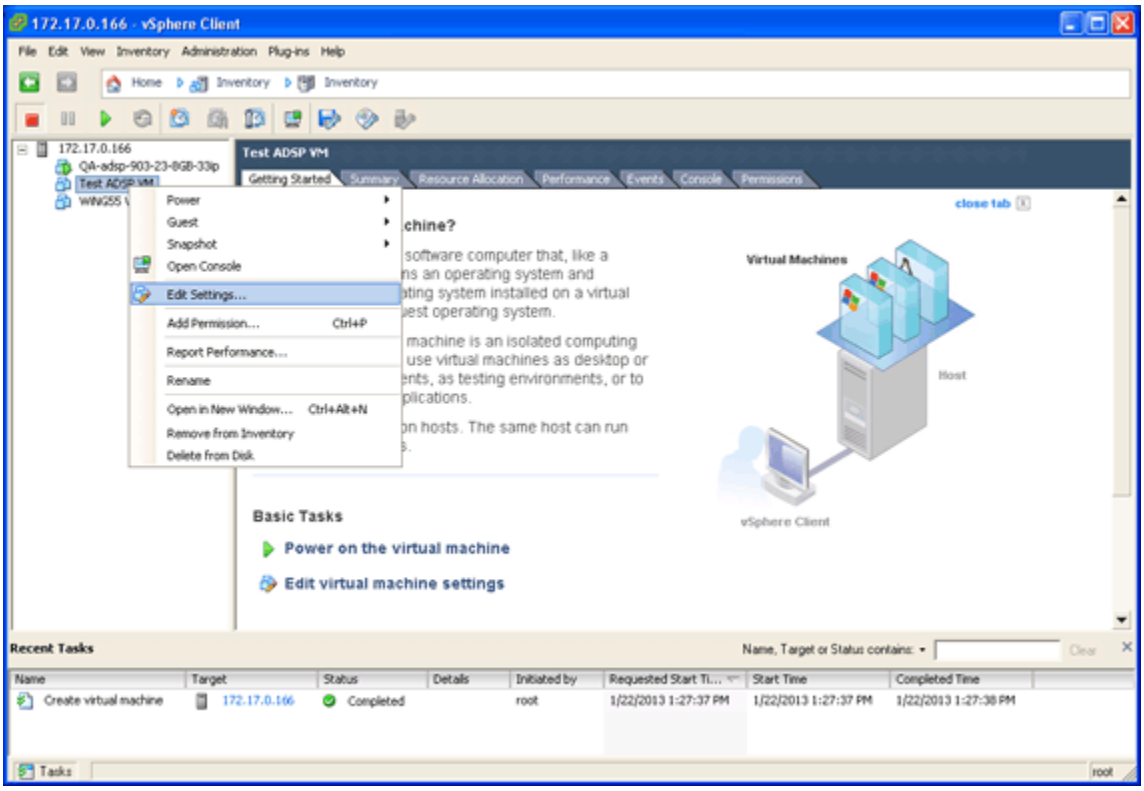
13 Wait until the **Deployment Completed Successfully** dialog box displays. This could take several minutes to hours depending on the location (local or Internet) of the ADSP image being deployed.



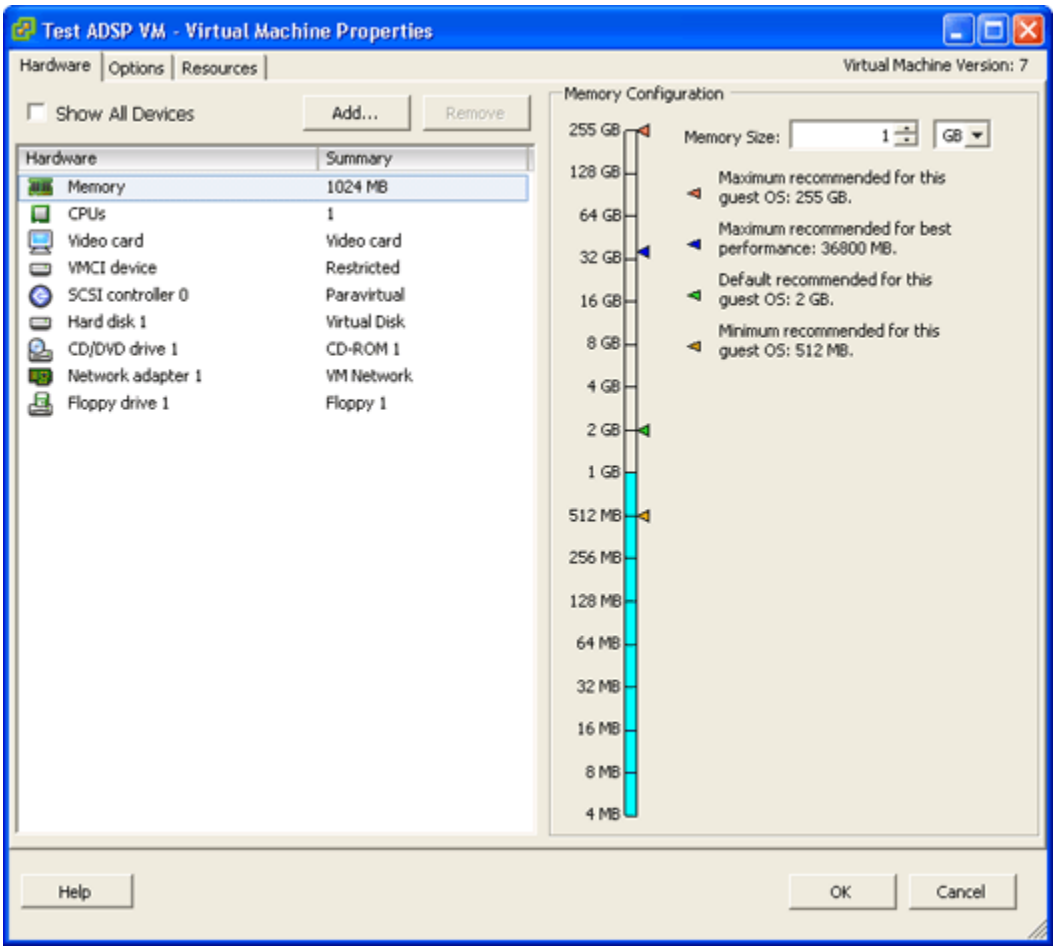
14 Click **Close**.

✓ *NOTE* If you receive a deployment error, download the *zlib1.dll*file from the Zebra Support Center at *www.zebra.com/support* and copy the file to your C:/ drive.

15 Right-click on the VM and then select **Edit Settings**.



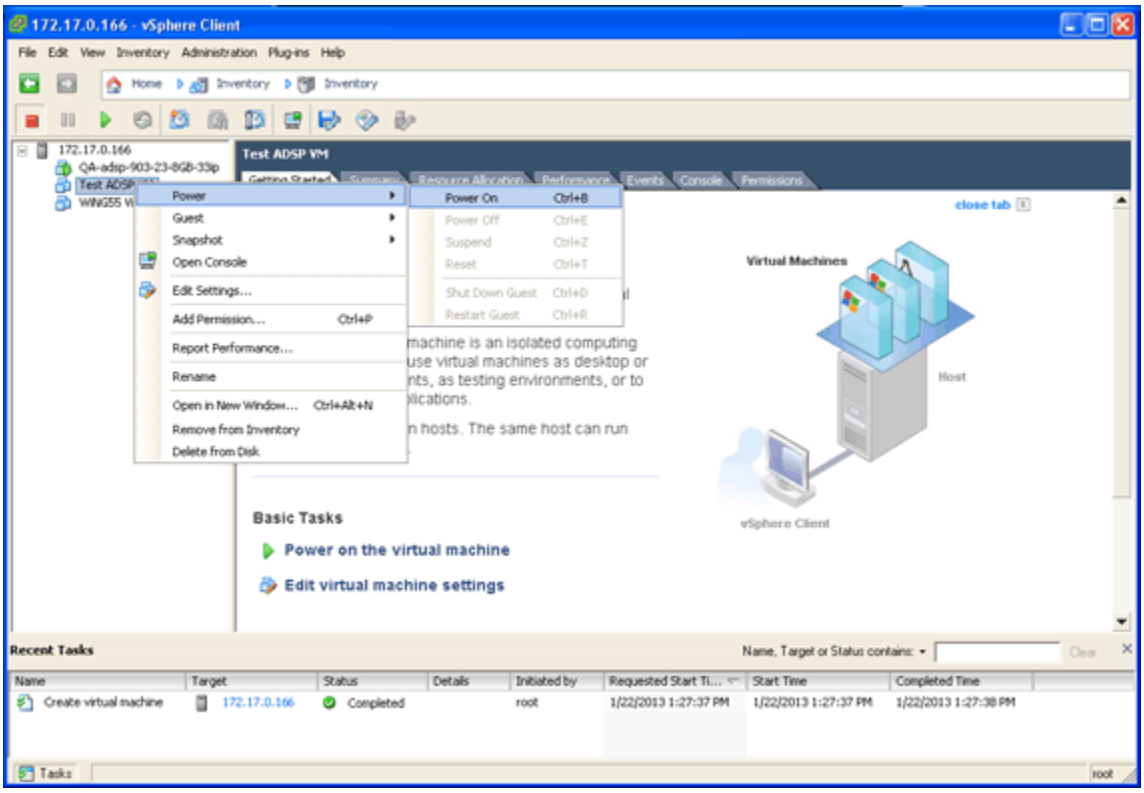
The following window is displayed.



16 Set **Memory**, **CPUs** and hard disk size as specified in Section 2 based on the network devices and clients to be supported by ADSP.

17 Click **OK**.

18 Right-click on the ADSP VM and then select **Power** > **Power On**.



19 Double-click the VM, then select the **Console** tab, and wait for login prompt. While waiting, ADSP VM configures automatically.

20 When login prompt displays, log into ADSP and configure just like you would any ADSP appliance.

✓ *NOTE* If you lose control of the cursor, press **Ctrl-Alt** to regain control.

Install ADSP on Xen Cloud Platform (XCP)

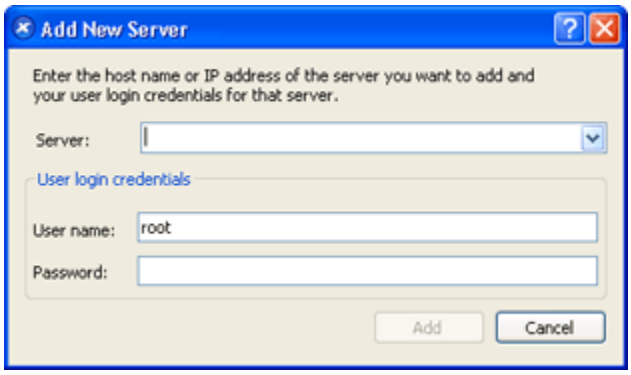
Follow these steps to install ADSP on the Xen Cloud platform:

1 Install Xen Cloud Platform 1.6 following Xen instructions. Follow the Xen instructions located at http://www.xen.org/download/xcp/index.html .

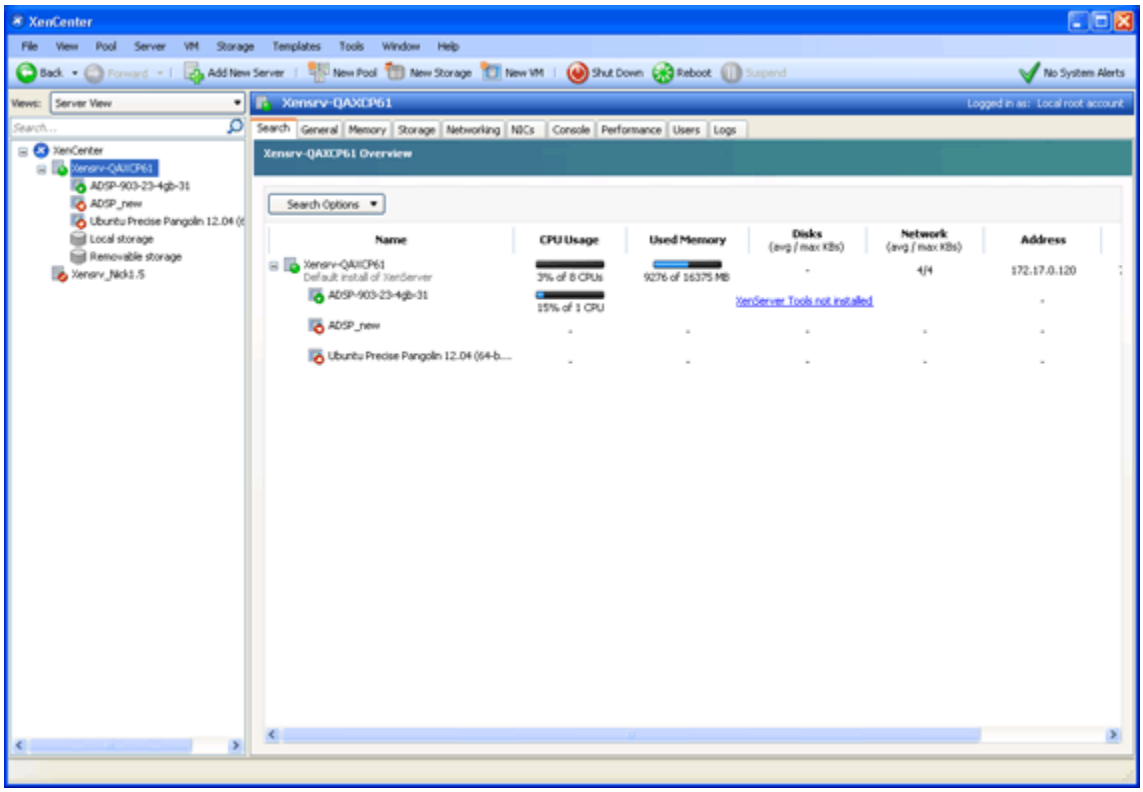
2 Install Citrix Xen Center to manage Xen Cloud Platform. Follow the Citrix instructions located at http://support.citrix.com/article/CTX118531 .

3 Double-click the **Xen Center** icon on your desktop.

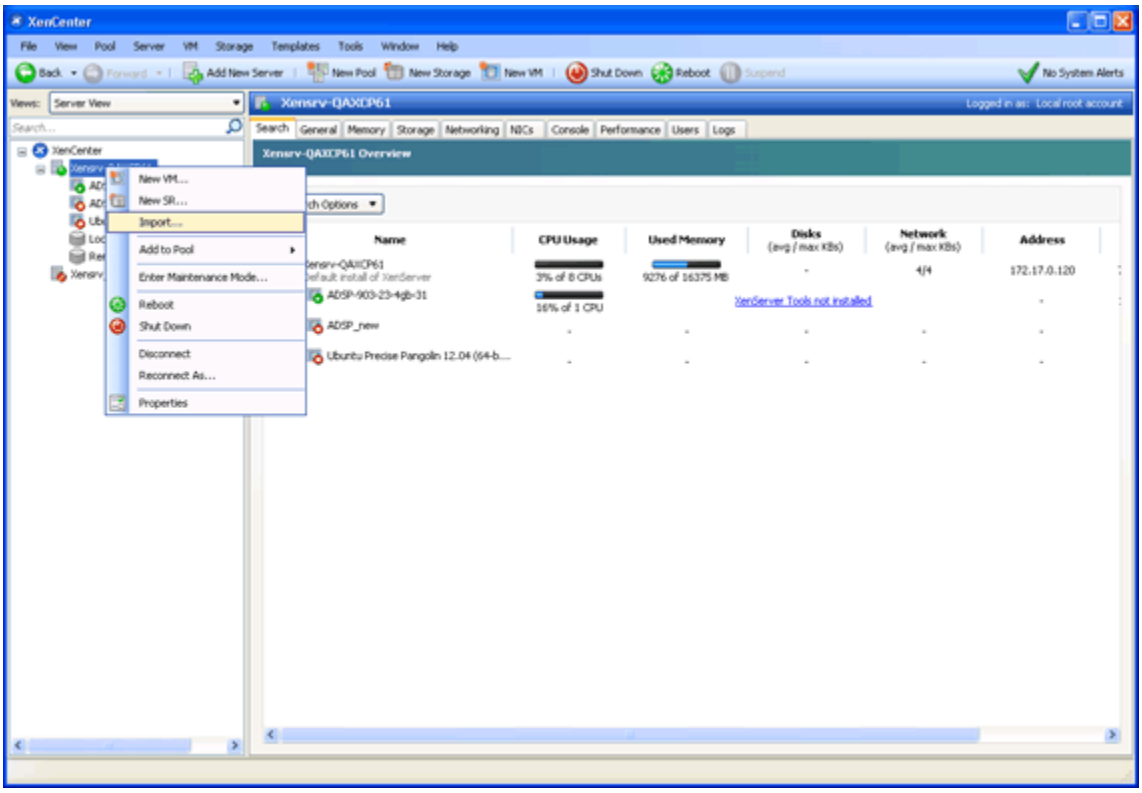
4 Select **ADD a server**.



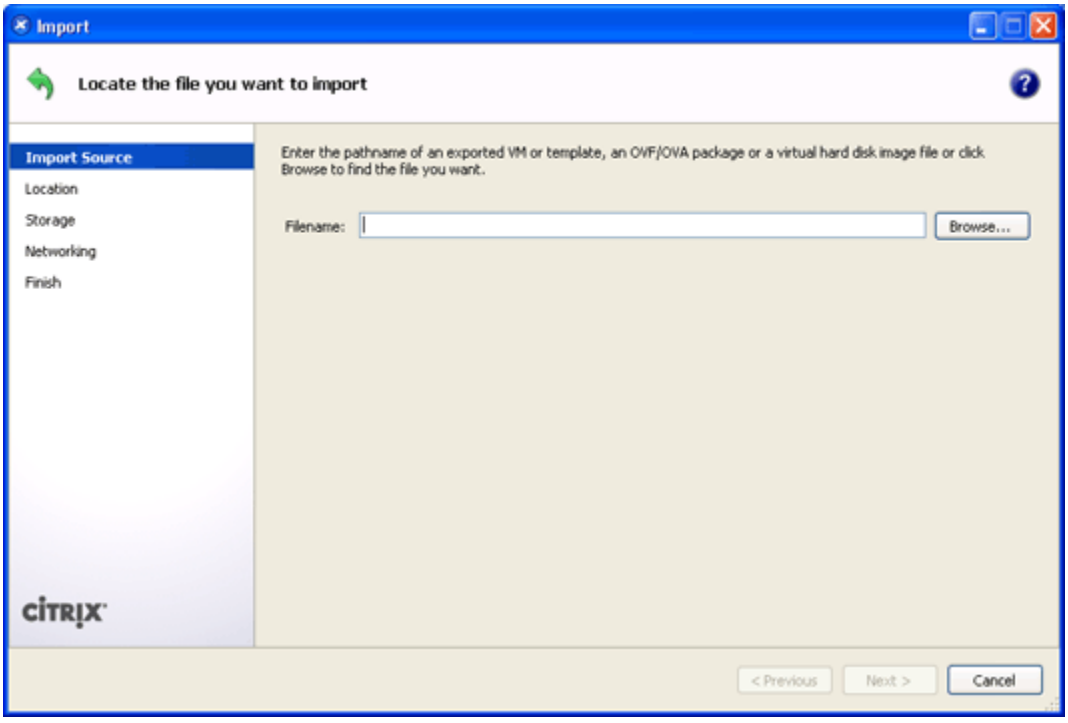
5 Enter Xen Cloud server IP address on which ADSP VM is to be deployed, along with username and password. Then, click **Add**.



6 Right-click on the Xen Cloud server and select **Import**.



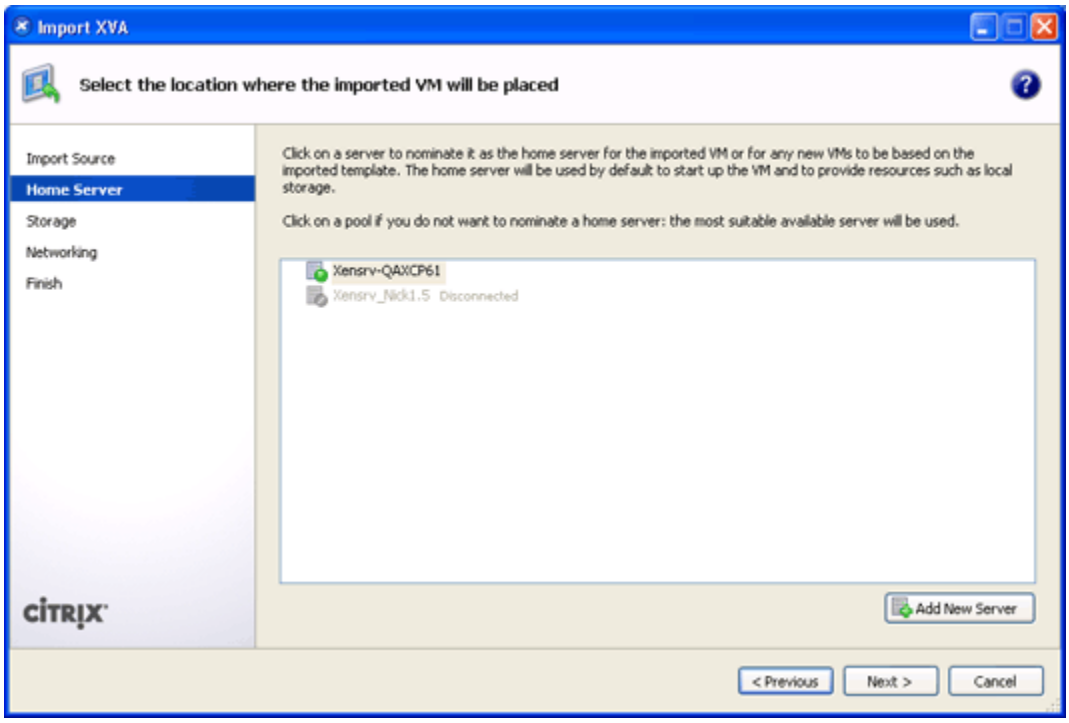
After selecting **Import**, the following window is displayed.



7 Click **Browse** and navigate to the location where you downloaded the ADSP images.

8 Select the **Xen Cloud Platform** image (AD-VM-adsp-9-0-3-23-dvd.xva) and click **Open**.

9 Click **Next**.

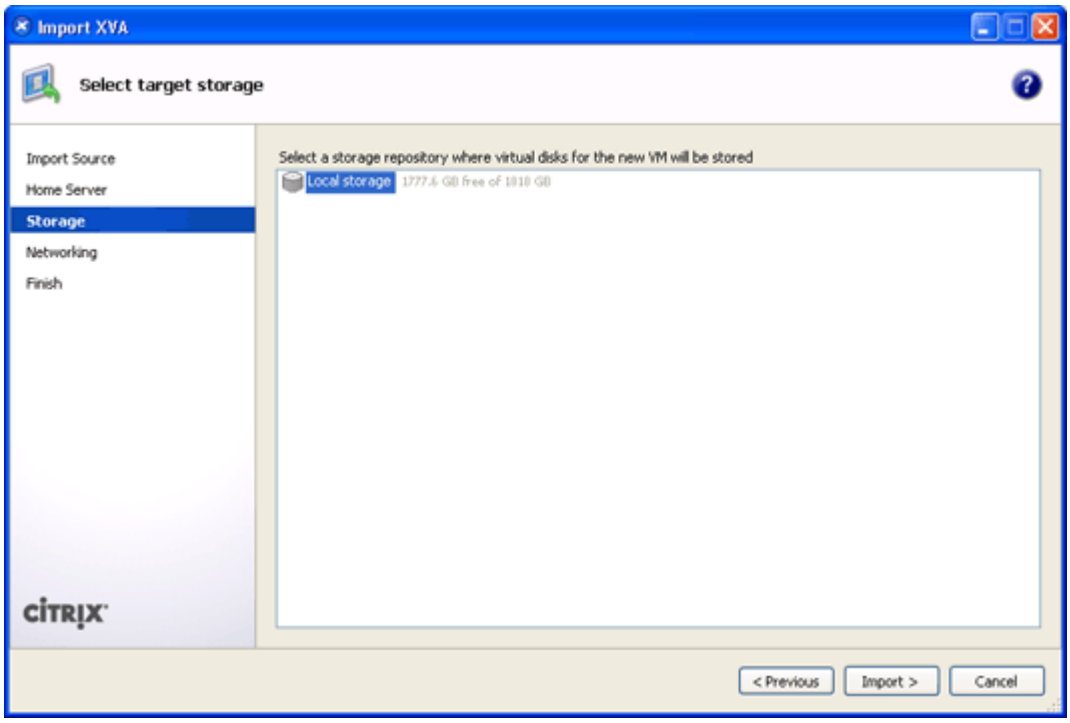


10 Select (highlight) a server for **Home Server**. The selected server will be used by default to start up the VM and to provide resources such as local storage.

11 Click **Next**.

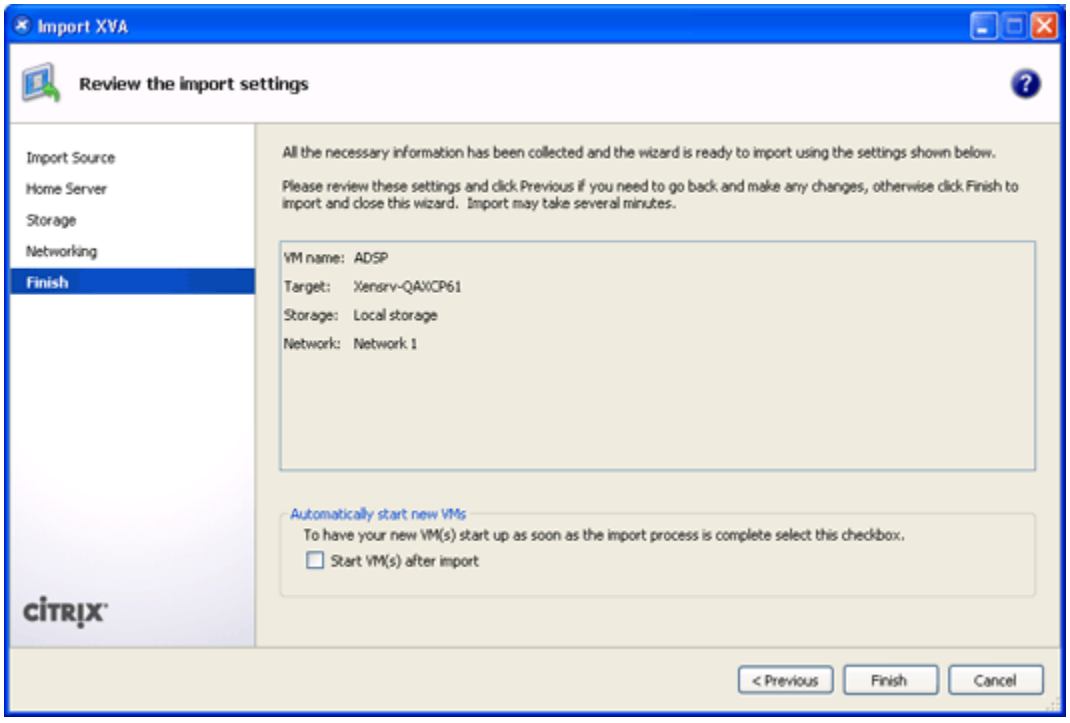
12 Click **Next** for **Storage** and select storage.

13 Click **Import**.



This could take several minutes to hours depending on the location (local or internet) of the ADSP image being imported.

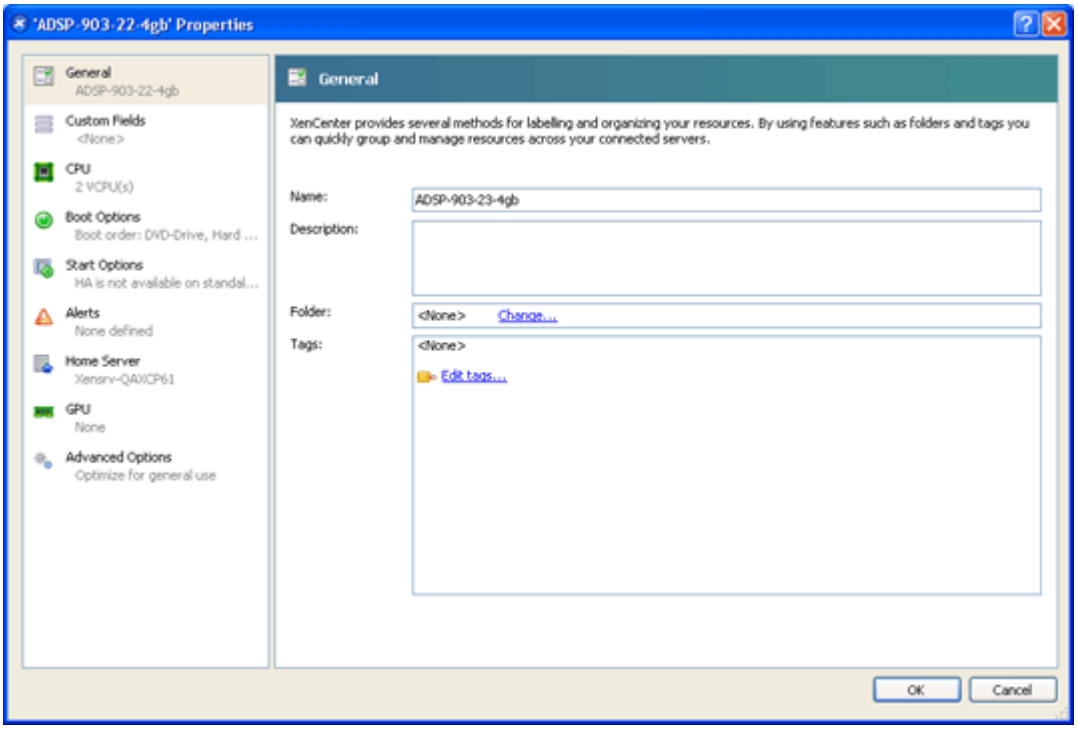
14 Select (highlight) a virtual network interface for Networking and then click **Next**.



15 Review the import settings, uncheck **Start VM(s) after import** and then click **Finish**.

Wait for the import to finish. This could take several minutes to hours depending on the location (local or internet) of the ADSP image being imported.

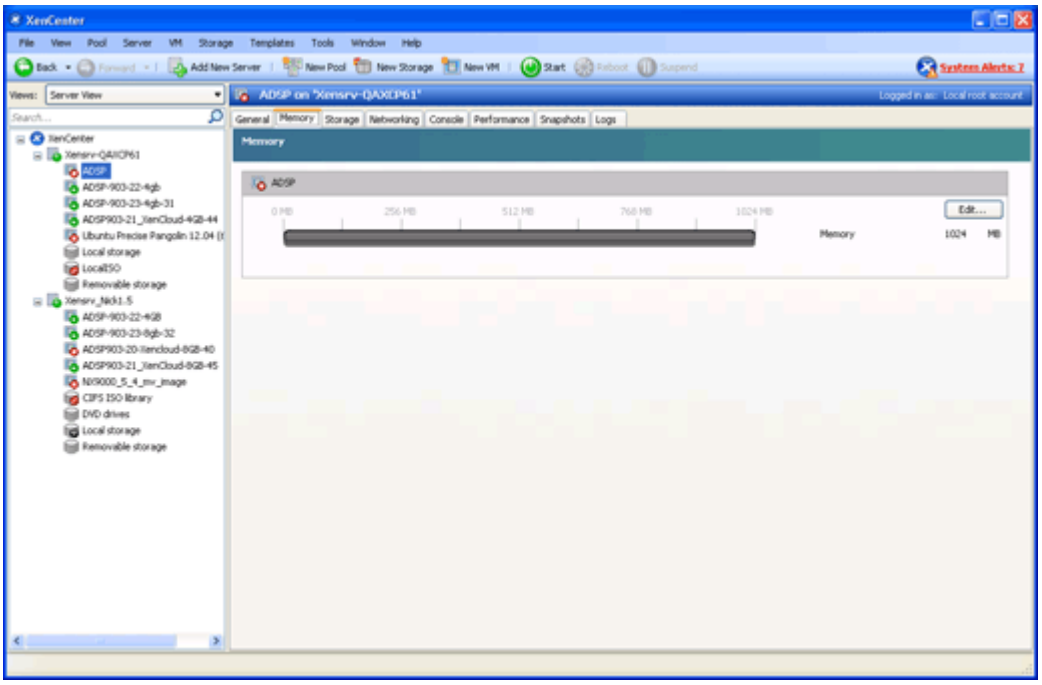
16 Right-click the ADSP VM and then select **Properties**.



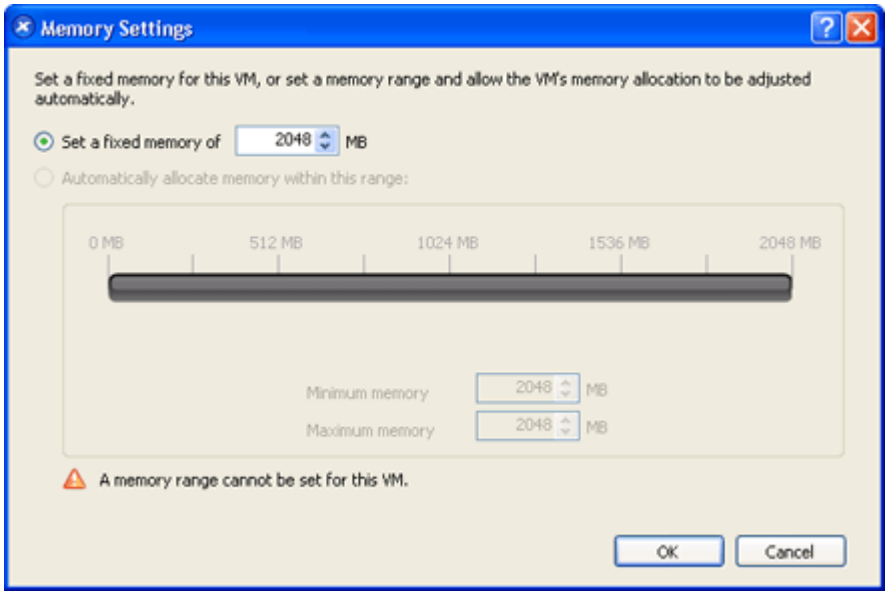
17 Change the VM name.

18 Select CPUs as specified in Section 2 based on the network devices and clients to be supported by ADSP, and then click **OK**.

19 Return to the Xen Center and select the **Memory** tab.



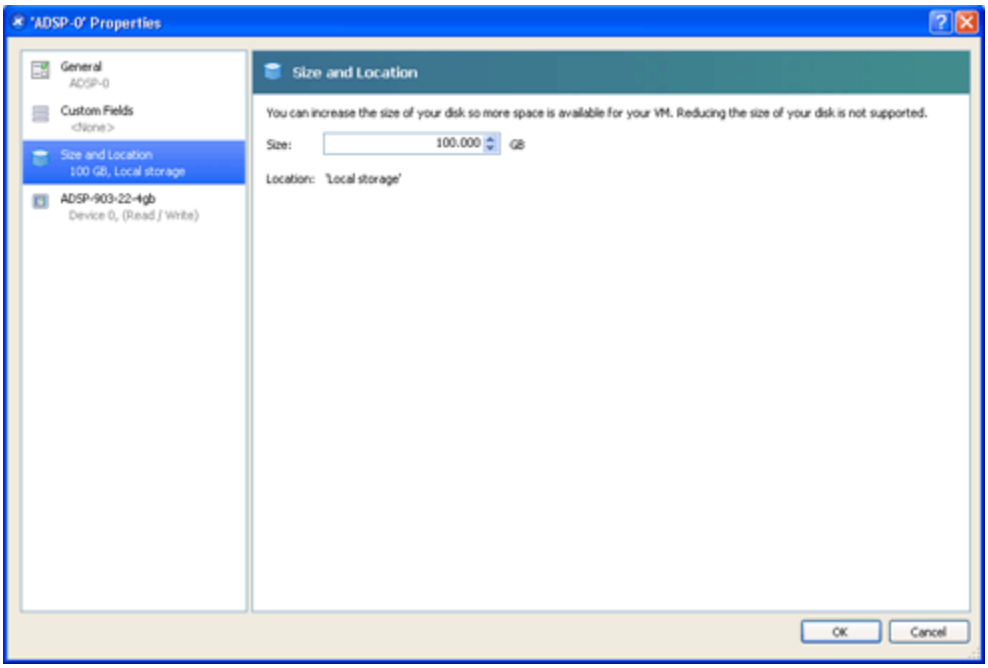
20 Click the **Edit** button.



21 Set the memory as specified in Section 2 based on the network devices and clients to be supported by ADSP, and then click **OK**.

22 Select the **Storage** tab and then double-click on the virtual disk.

23 Select **Size and Location**.



24 Set the disk size as specified in Section 2 based on the network devices and clients to be supported by ADSP, and then click **OK**.

25 Right-click on the ADSP VM and select **Start**.

26 Go to the **Console** and wait for login prompt.

27 Log in to ADSP and configure just like you would any ADSP appliance.

Install ADSP on Xen Hypervisor

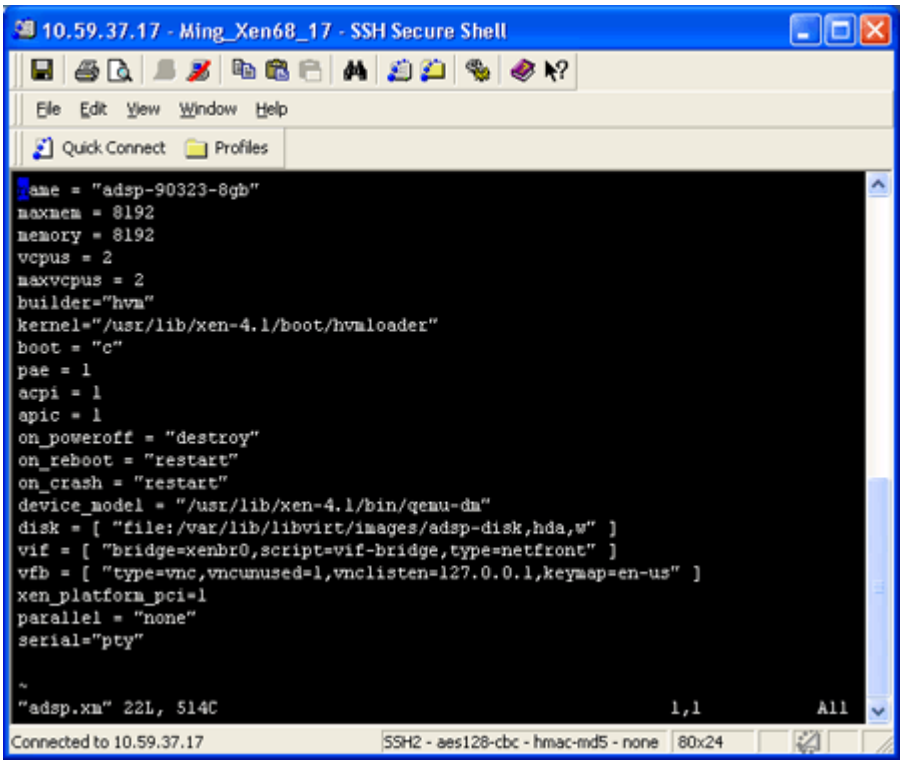
Follow these steps to install ADSP on the Xen Hypervisor:

1 Install Xen Hypervisor 4.x. Follow the Xen instructions located at http://wiki.xen.org/wiki/Xen_Overview

2 SCP the disk image (AD-VM-adsp-9-0-3-23-dvd.gz) configuration file (AD-VM-adsp-9-0-3-23-dvd.xm) to a location on your Xen server. Let's assume that the location is: */var/lib/libvirt/images*.

3 Unzip the disk image using the following command: **gunzip AD-VM-adsp-9-0-3-23-dvd.gz**.

4 Go to */var/lib/libvirt/images* and edit the configuration file: **vi AD-VM-adsp-9-0-3-23-dvd.xm**.



5 Change the line beginning with disk to point to your the location of your ADSP image:

6 disk = [file:/var/lib/libvirt/images/adsp-disk,hda,w]

7 Change the values for **name**, **maxmem**, **memory**, and **maxvcpus** to match your criteria. Refer to Section 2 for the recommended resource configuration for ADSP.

8 Create an ADSP VM from the new configuration file:

9 xm new AD-VM-adsp-9-0-3-23-dvd.xm

10 Start the ADSP VM:

xm start adsp-903-01082013

✓ *NOTE* The VM name is the same as the one you specified in the configuration file.

11 The ADSP Console can be started with the following command:

xm console <*ADSP VM name*>

12 Log in to Virtual ADSP and configure as you would any ADSP appliance.

CHAPTER 3 THE MENU

Menu

The Menu gives you access to the ADSP features.

Features such as **Add Devices** and **Import/Discover Devices** are features that are an integral part of ADSP. **Reports** and **Help** are web-based applications. Most of the rest of the features are Java applets. 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.)

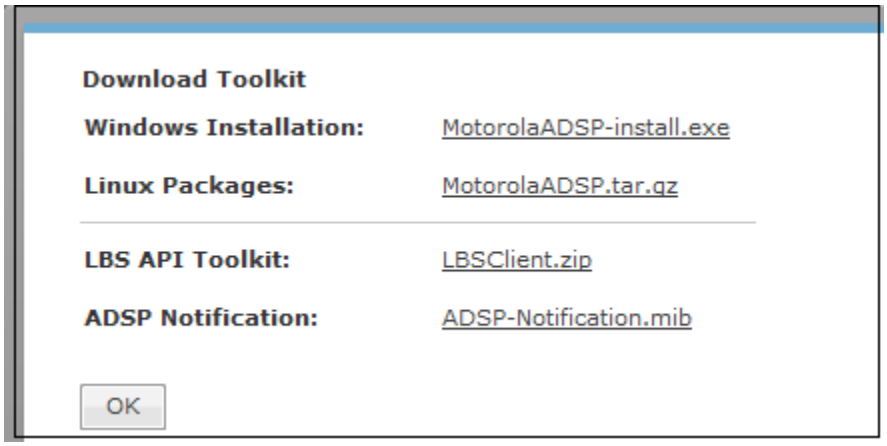
Installing Toolkit

You will need to install the ADSP toolkit on your workstation after your initial ADSP installation and also each time you upgrade to a new release.

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 or Linux) and then follow the instructions for your OS.



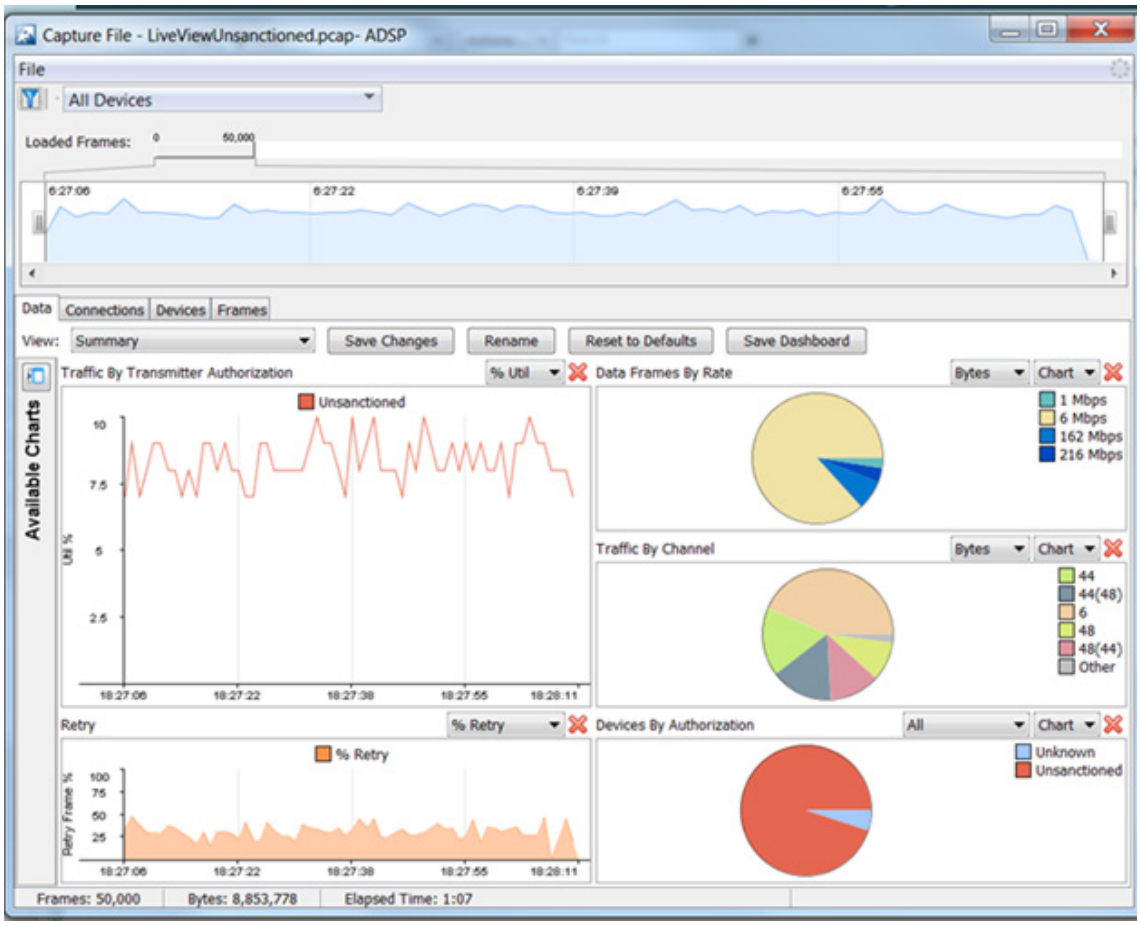
Open

Click **Open** to access a saved Frame Capture or Spectrum Analysis file.

Frame Capture Analysis

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

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

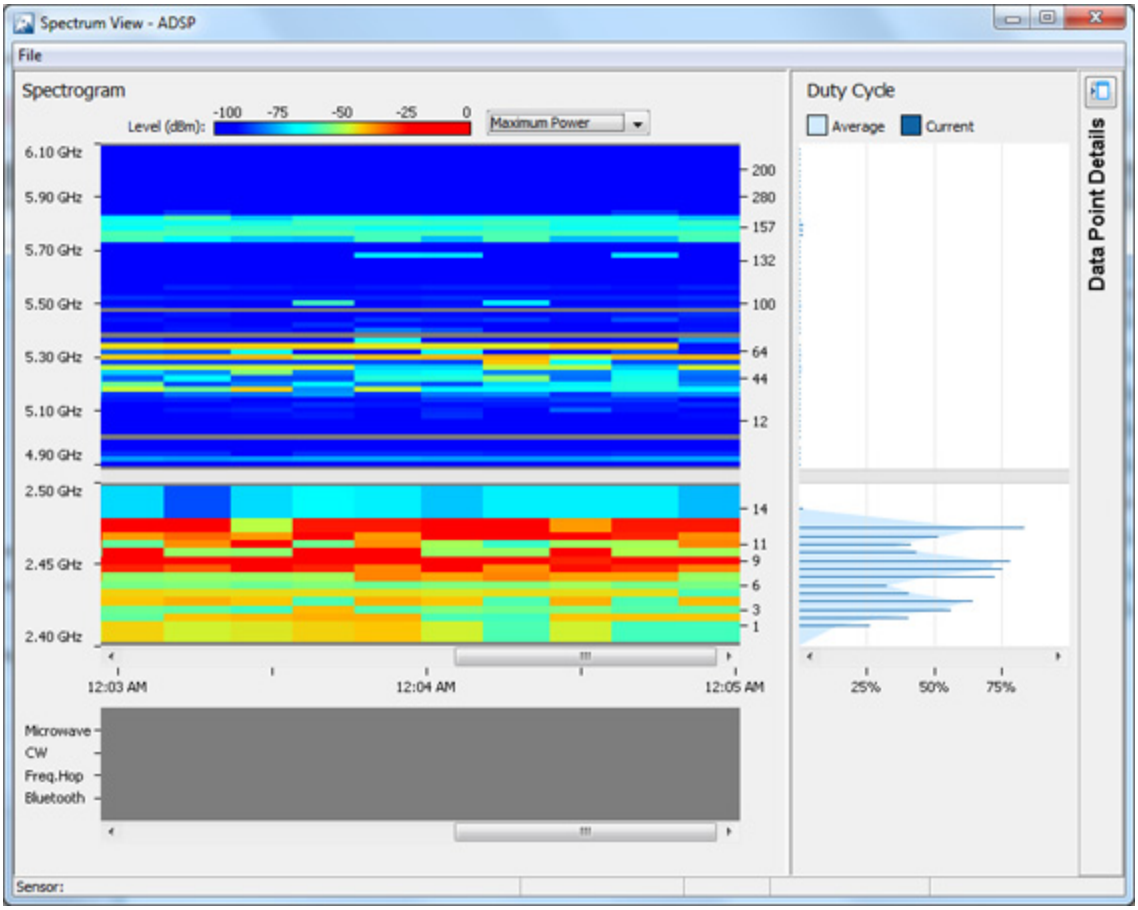


The **Capture File** window is basically the same as the **Live View** window minus the buttons and menus that are not needed for Frame Capture Analysis. The tabs display the same information as the **Live View** window.

Spectrum Analysis

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

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



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

Forensic Analysis—Basic

Using Forensic Analysis, you can analyze historical data collected and stored for wireless devices. Forensics furnishes details on devices detected by ADSP, e.g., APs, sensors, switches, BSSs and wireless clients. When you need to investigate a suspicious device or troubleshoot a WLAN problem, use the Forensic Analysis tool to analyze any device seen by the system and display the following information:

- threat level of the device
- device alarms
- device associations.

Accessing Forensic Analysis

Method 1:

To access forensic data for a device, select **Menu** > **Forensic Analysis**, then enter the MAC address of the device.

Method 2:

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

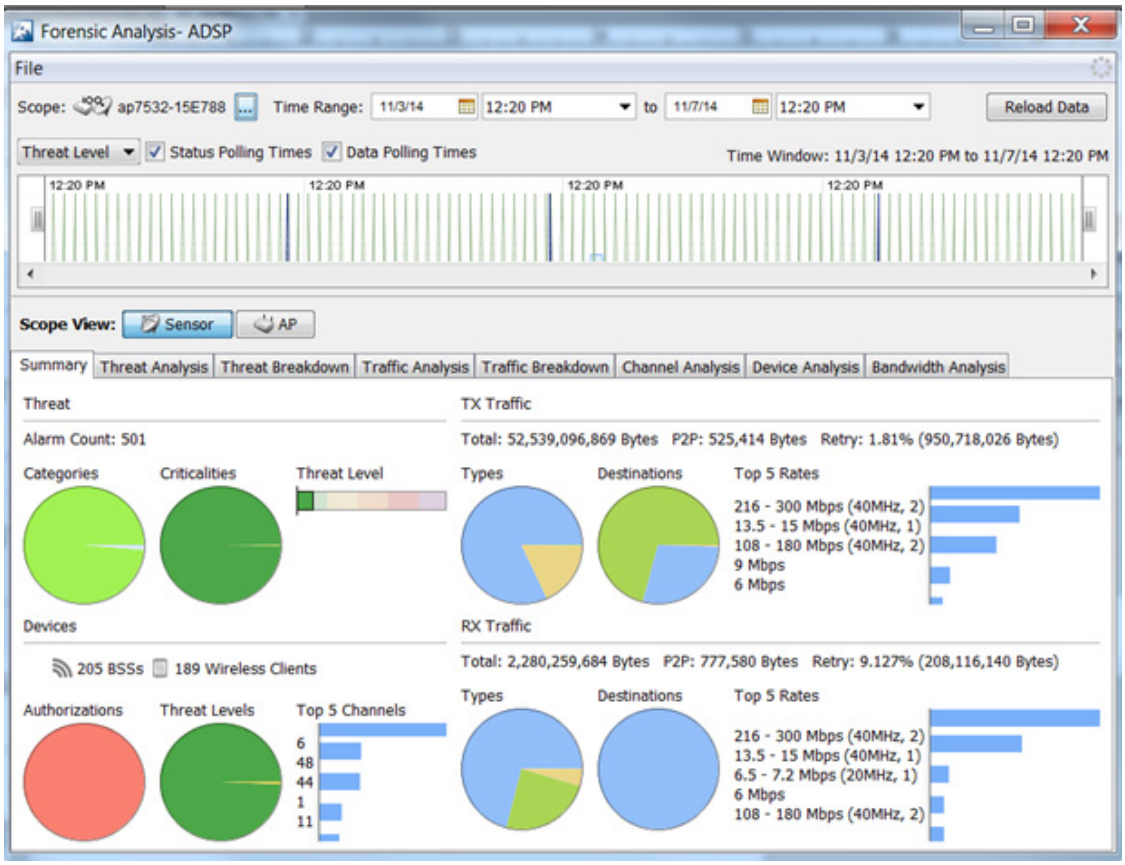
Setting Time:

Once you have accessed Forensic Analysis, a time window displays and you must select the device and time range. Basic Forensic Analysis, by default, only shows 24 hours worth of data. For detailed historical analysis, you can change the 24 hour time period by selecting a new date and time. However, you cannot view more than 24 hours of data at any one time.

NOTE Advanced Forensic Analysis allows you to specify your own time period which can exceed 24 hours. For more details, see the section Advanced vs. Basic Forensic Analysis.

Forensic Data

When you first access Forensic Analysis, you can view a summary of forensic data with information about threats, associations, device information, transmitting traffic, and receiving traffic. Below is an example of a forensic data file:



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

NOTE The tabs displayed will vary depending on the device selected and on whether you have installed Basic Forensic Analysis or Advanced Forensic Analysis.

You can access the following tabs in Forensic Analysis for more detail:

- **Adoption History** (APs and Switches.) For APs, adoption history provides a table of devices that have adopted the selected AP. For switches, it provides a table of devices that the selected switch has adopted.
- **Association Analysis** (BSSs and Wireless Clients) lists the associations between the device being analyzed and other wireless devices.
- **Bandwidth Analysis** (APs and Switches) displays a chart showing the bandwidth utilization for the selected AP or switch.
- **Channel Analysis** (BSSs and Wireless Clients) provides a visual representation of all channels.
- **Device Info** (All devices) displays the current settings for the device being analyzed.

- **Device Analysis (All Devices)** provides a visual representation of all channel bandwidths.
- **Performance Analysis** (Switches) provides performance raw data and usage percentages for the selected switch.
- **Radio Analysis** (APs) provides information that can be used to analyze the radio on the selected AP.
- **Radio Info** (APs) provides radio information that is recorded at the time displayed on the selected AP.
- **Signal Analysis** (BSSs and Wireless Clients) displays the signal strength of a device (in dBm) as measured by various sensors.
- **Threat Analysis** (All devices) displays a table of alarms generated by the device being analyzed.
- **Threat Breakdown** (APs, BSSs and Wireless Clients) displays devices broken down by type/manufacturer.
- **Traffic Analysis** (BSSs and Wireless Clients) displays traffic transmitted and received by the device being analyzed.
- **Traffic Breakdown** (APs, BSSs and Wireless Clients) displays devices broken down by type/manufacturer.

Advanced Forensic Analysis

The Advanced Forensic Analysis module allows you to access the full potential of Forensic Analysis. When installed, Advanced Forensic Analysis replaces the Basic Forensic Analysis that is included in AirDefense Services Platform.

Advanced vs. Basic Forensic Analysis

Advanced Forensic Analysis has all the features of Basic Forensic Analysis plus some very powerful enhancements. 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. See the following table for a comparison of the features that are available with Basic vs. Advanced Forensics.

Table 3-1 ***Advanced vs. Basic Forensic Analysis***

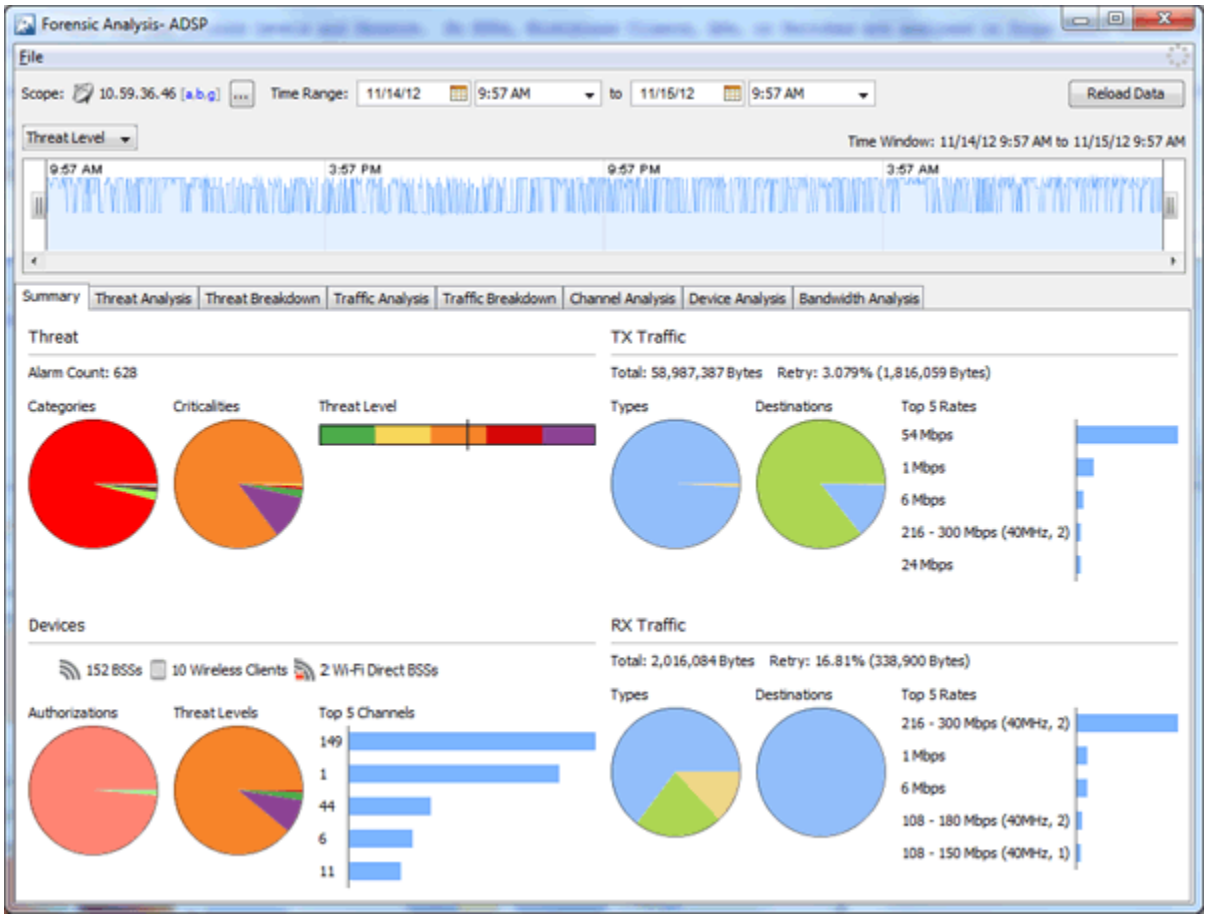
Basic Forensic Analysis	Advanced Forensic Analysis
Forensic data is available only for BSS and Wireless Client devices.	Forensic data is available for the entire system, a single network level, or a single sensor (Scope Based only.)
No Location data is available.	Location data is available and the Location Analysis tab is activated (Device Based only).
No Graphical views of data analysis are available.	Graphical views of data analysis are available in all tabs.
Data is displayed only in 24 hours increments. You cannot configure a different time period, but you can choose whatever 24 hour period that you want.	You can select a time frame for more than a 24 hour time period to display data.
Only the selected 24 hour time period is displayed; you cannot adjust the time window using sliders.	You can adjust the time window using sliders.
No data filters are available.	Data filters are enabled.

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. There are two categories of Advanced Forensic Analysis:

- Scope Based Forensic Analysis
- Device Based 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.

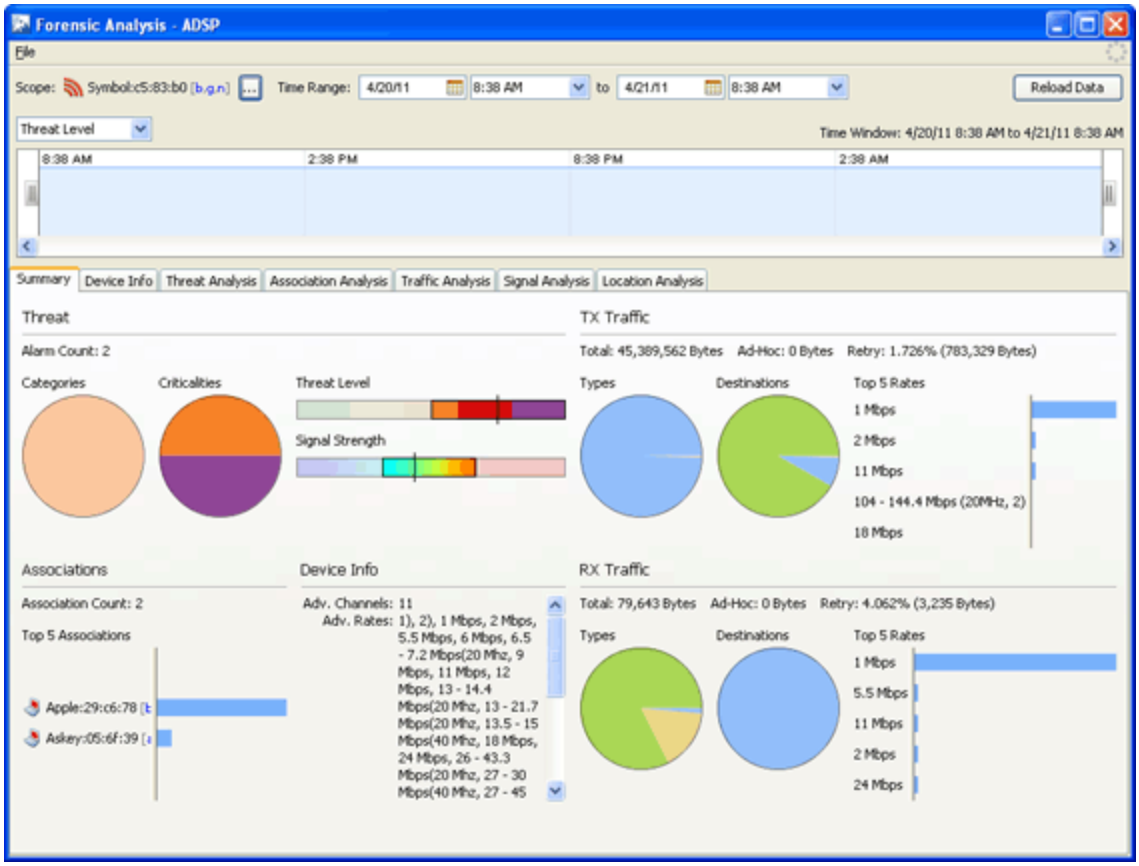


The following forensic data is included with Scope Based Forensic Analysis:

- 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.

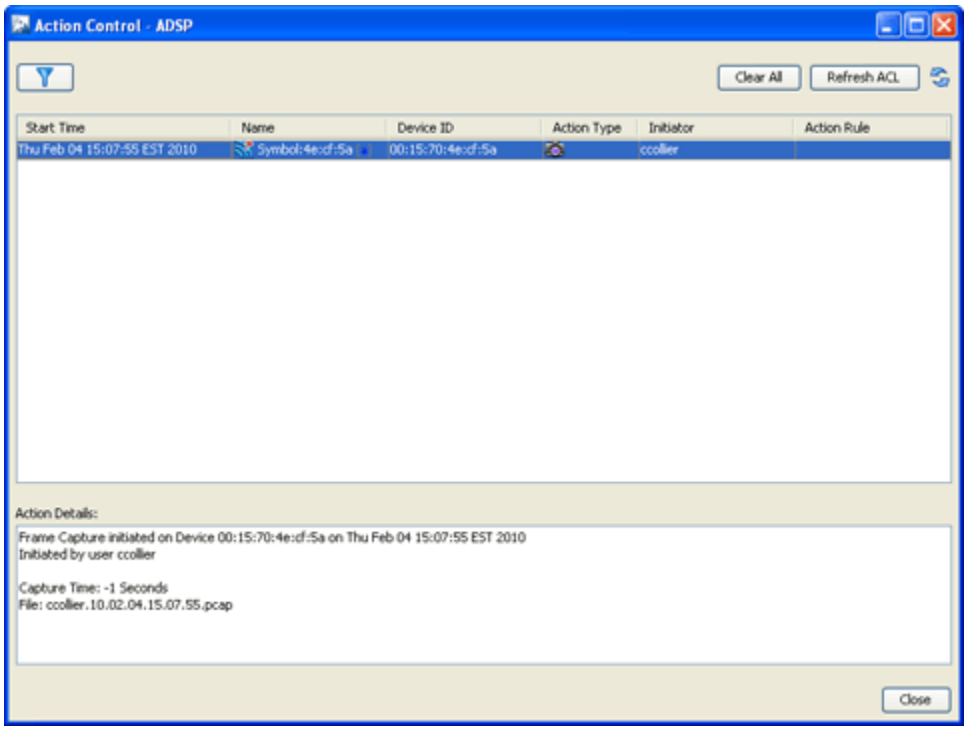
The **Location Analysis** tab provides information to help administrators locate devices in their wireless network. A Heat Map and a Location Map are used to locate a device. A table view is provided to display the coordinates of a device. To use the map feature, you must first import the location map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

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.

Reports

ADSP provides a dual approach to reporting. You can access a web reporting interface and populate report templates with data or use a flexible report builder application to create custom reports.

- 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.

Web Reporting Interface

To access the Web Reporting web site, log in to the GUI and then select **Menu** > **Reports**. The report names are displayed by category. Select the desired report and click on the link to display it. The Web Reporting interface consists of three tabs: Reports, Published and Favorites.

To move from one page to another, click the tab name. See the following list for a description of each tab.

- **Reports**—The Reports tab is the default tab; it lists standard and custom report templates by category. You can select a report, specify applicable settings, and then display the report with data.
- **Published**—The Published tab lists the reports that you have run and saved as a published report. You cannot view a report published by another user unless that user shares the report. Once a report is published, you can:
  - View published report data by clicking on the report's name.
  - Delete a published report by checking its checkbox and clicking **Delete**.
  - Share a published report by checking its checkbox and clicking **Share**.
  - Make a published report private by checking its checkbox and clicking **Unshare**.
  - Rename a published report by clicking **Rename**, typing in a new report name, and then clicking **Apply**.

- **Favorites**—The Favorites tab is where you save reports that you run often. When a report is designated as a favorite, you can:
  - Edit the favorite report settings that are set when you create a report by clicking **Edit Settings**.
  - Schedule the report to run automatically.
  - Delete a favorite report by checking the checkbox next to the report and then clicking the **Delete** button.

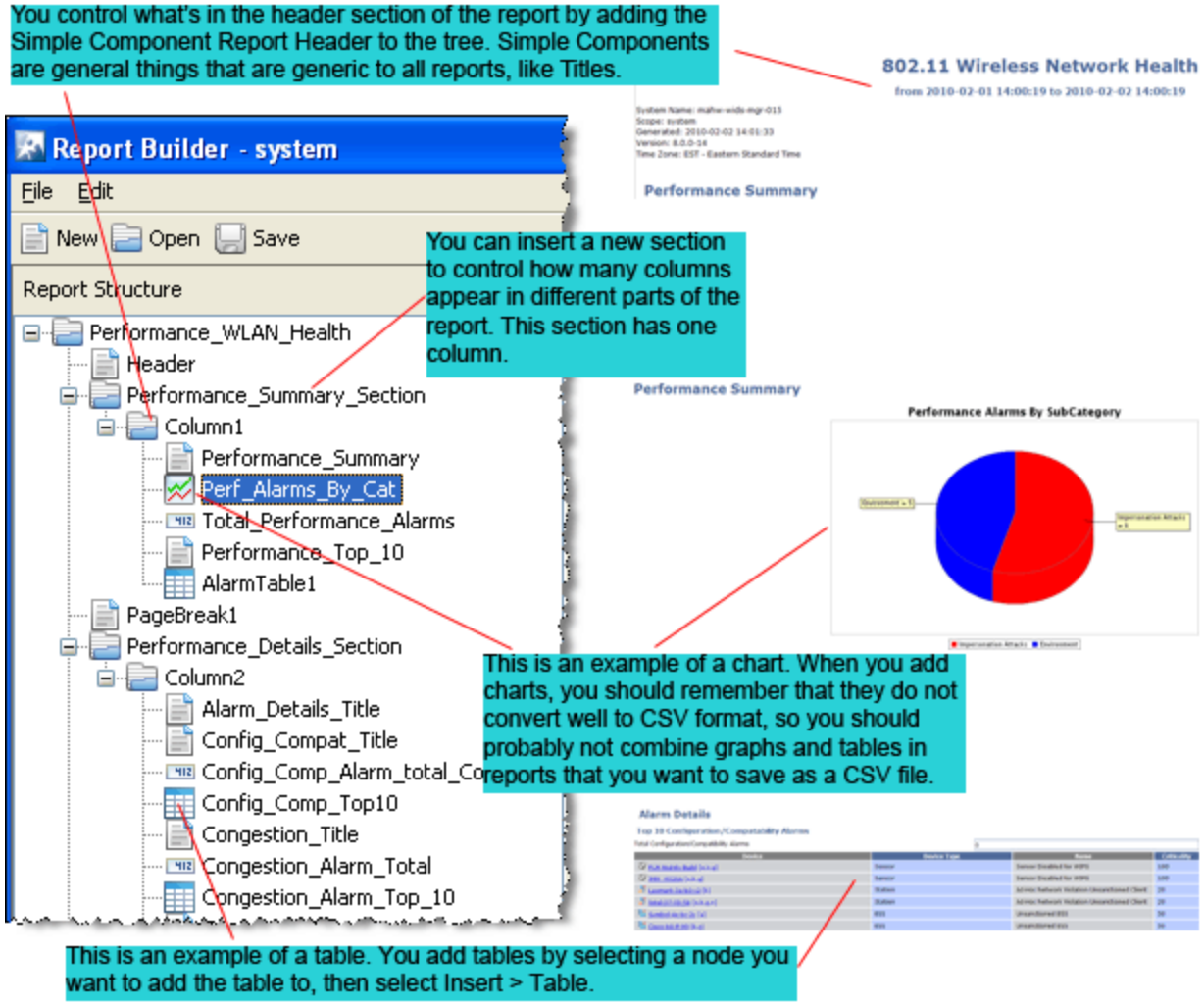
The Online Help describes each of these tabs in detail and explains how to create reports, add reports to the Favorites tab, and schedule reports.

Report Builder

Report Builder allows advanced users to 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.

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.



Adding a Report

1. Click **New** on the Report Builder tool bar.
2. Choose a template. Either choose an existing report to edit, or choose the blank report for either a single device or for multiple devices.

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

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**.

Adding Report Components

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

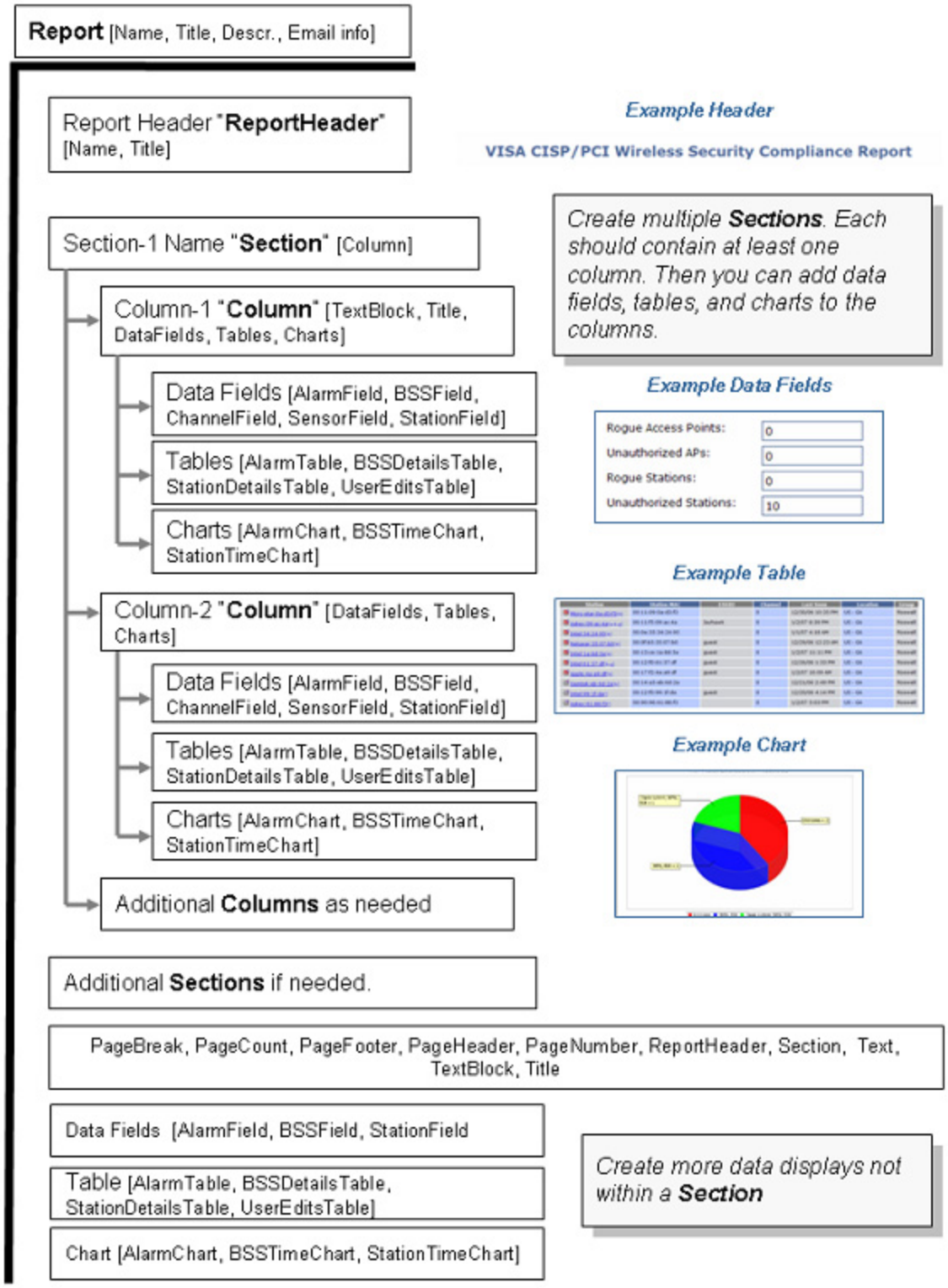
NOTE Right-click menus make it easy to work with report components. Report Builder displays the right-click options that are available, and grays out those that are not.

- **Add sections**—Right-click on the name of the report in the tree. Select **Insert Simple Components**, and then select **Section**.
  - Sections are simply containers for the columns in a report area. For example, if you want three tables to appear side-by-side, you create a section, add three columns, then insert the tables as described below.
  - Use the up and down arrow buttons to move sections up and down in the tree to place them where you want them.
  - 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.
  - 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 Report Components

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 Report Components

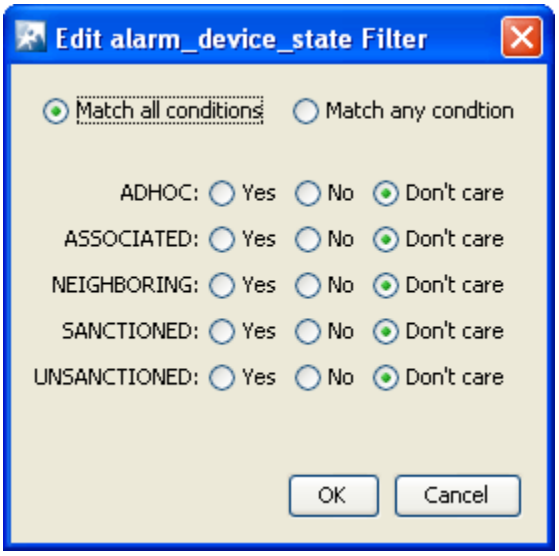
Every report component (data field, table, or chart) has configuration options you can use to create reports that contain the exact information you need. After you add a report component to your report tree, Report Builder displays the configuration options for that component. You can name the component, 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).

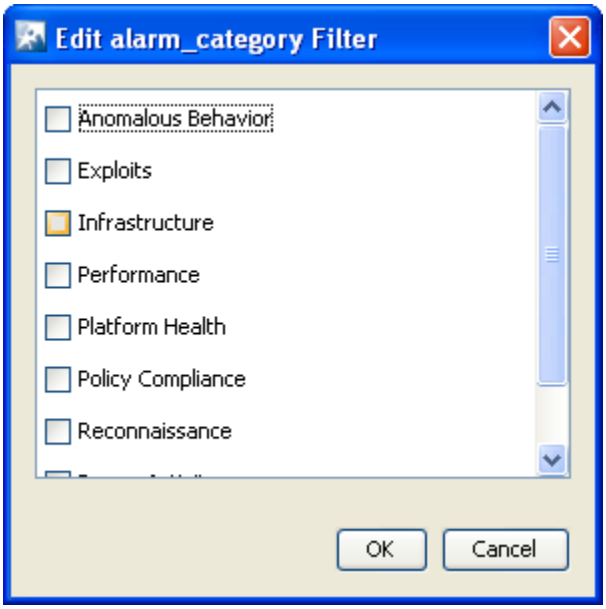
Configuring Report Filters

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):

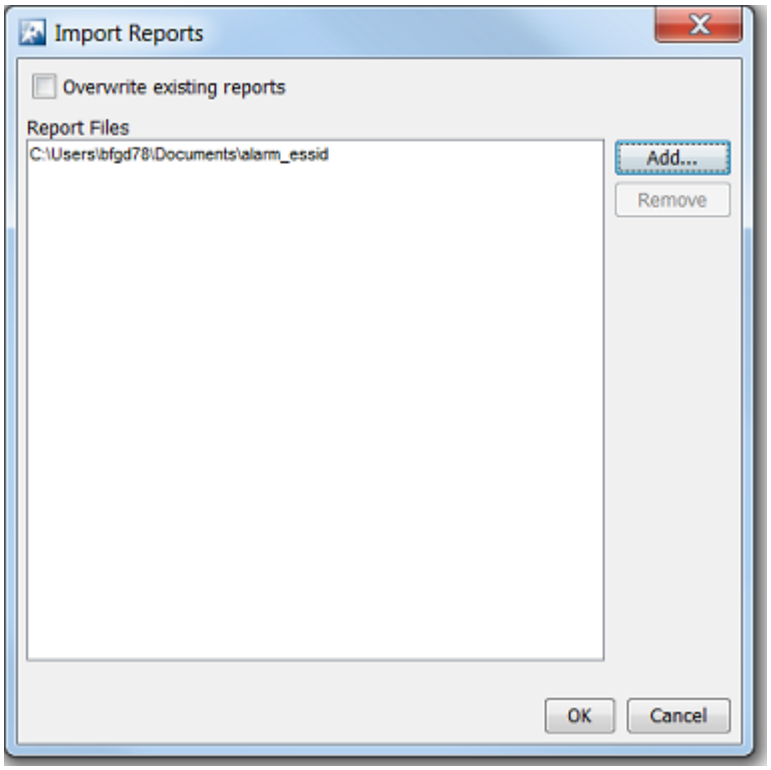
- Text box (example):

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 from the Report Builder screen by using the following steps.

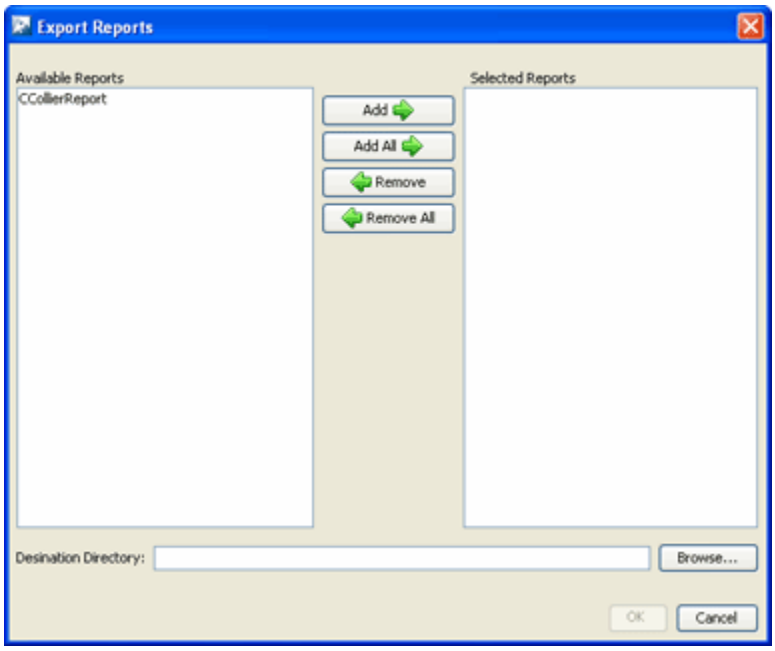


Select **File** > **Import**. The Import Reports window is displayed.

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

Exporting a Report

You can export a report from the Report Builder screen by using the following steps.



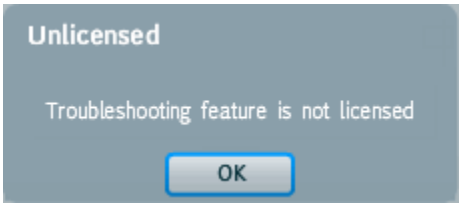
1. Click **File** > **Export**. The Export Reports window is displayed.
2. Select (highlight) one or more reports that you want to export.
3. Click **Add** to add the reports to the **Selected Reports** list.

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

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.

✓ 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.

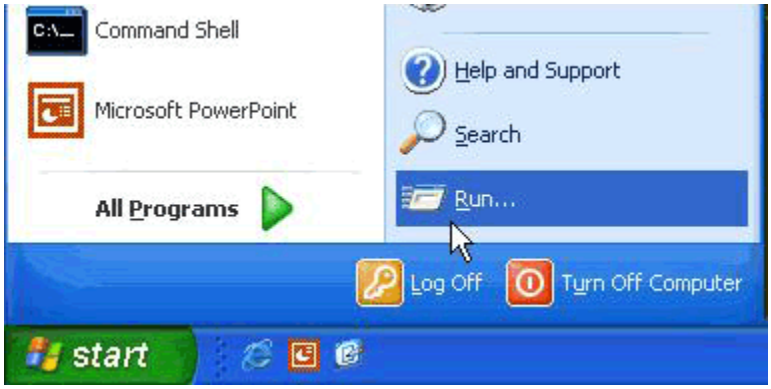
When 100% of the troubleshooting data is loaded, the data is displayed in the application. For an explanation of the loaded data, refer to the Wireless Client Status, Results Summary, and Observed Network topics.

MAC Address Hints

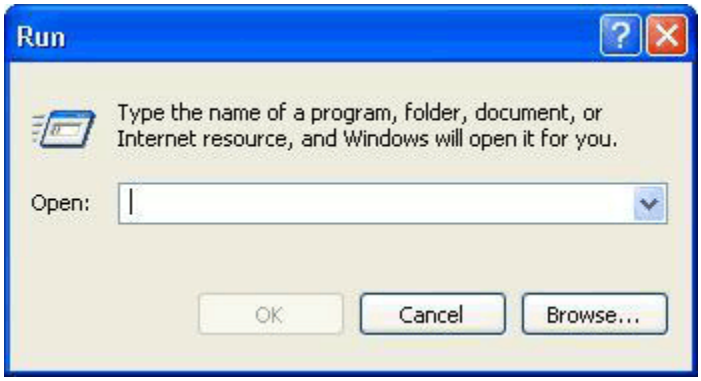
Click on the question mark next to the **Troubleshoot Device** field to display hints on how to determine the MAC address or device name of a Wireless Client.

Find MAC Address-Windows

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

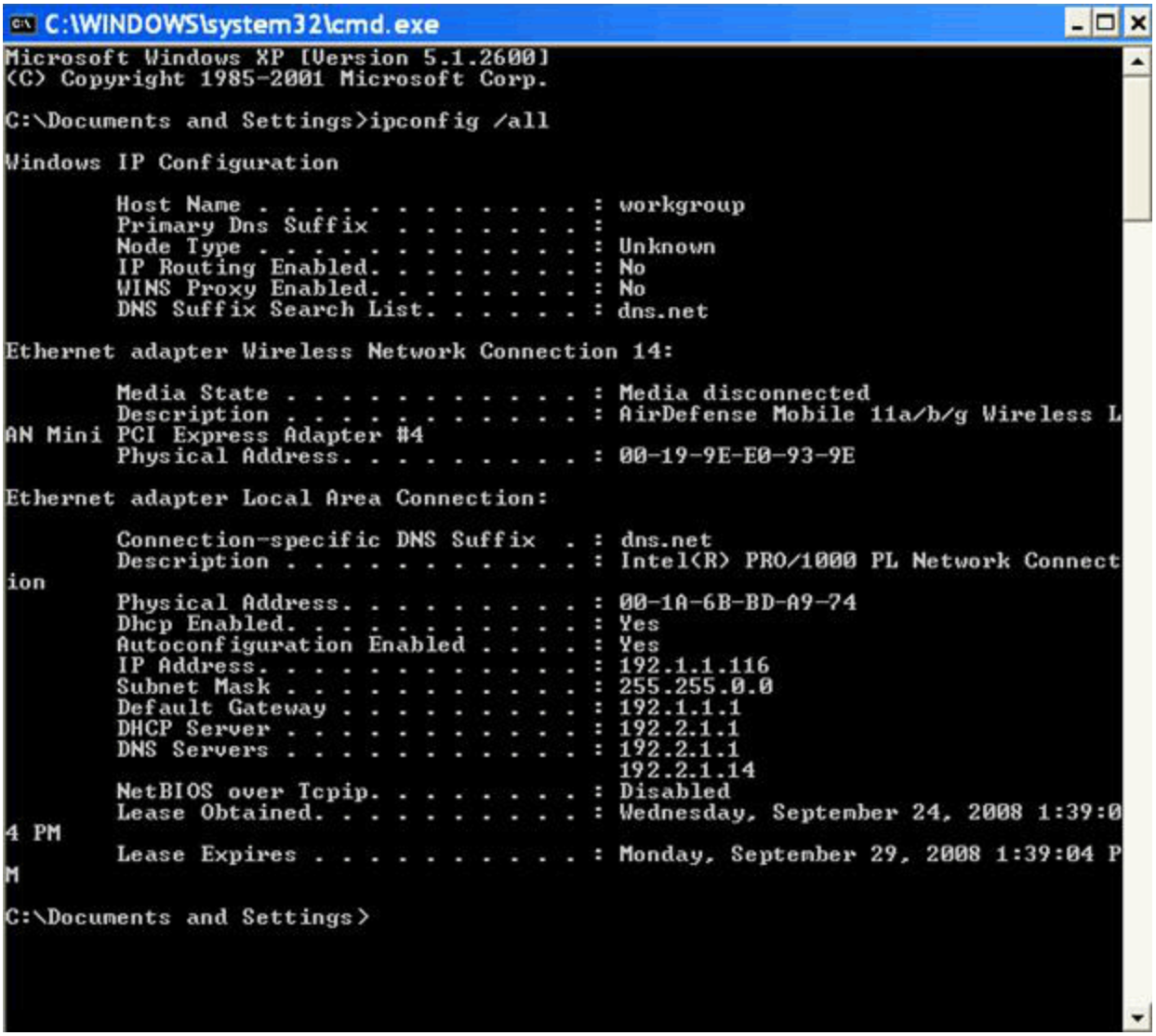


The **Run** window will open. Enter **cmd** and click **OK**.



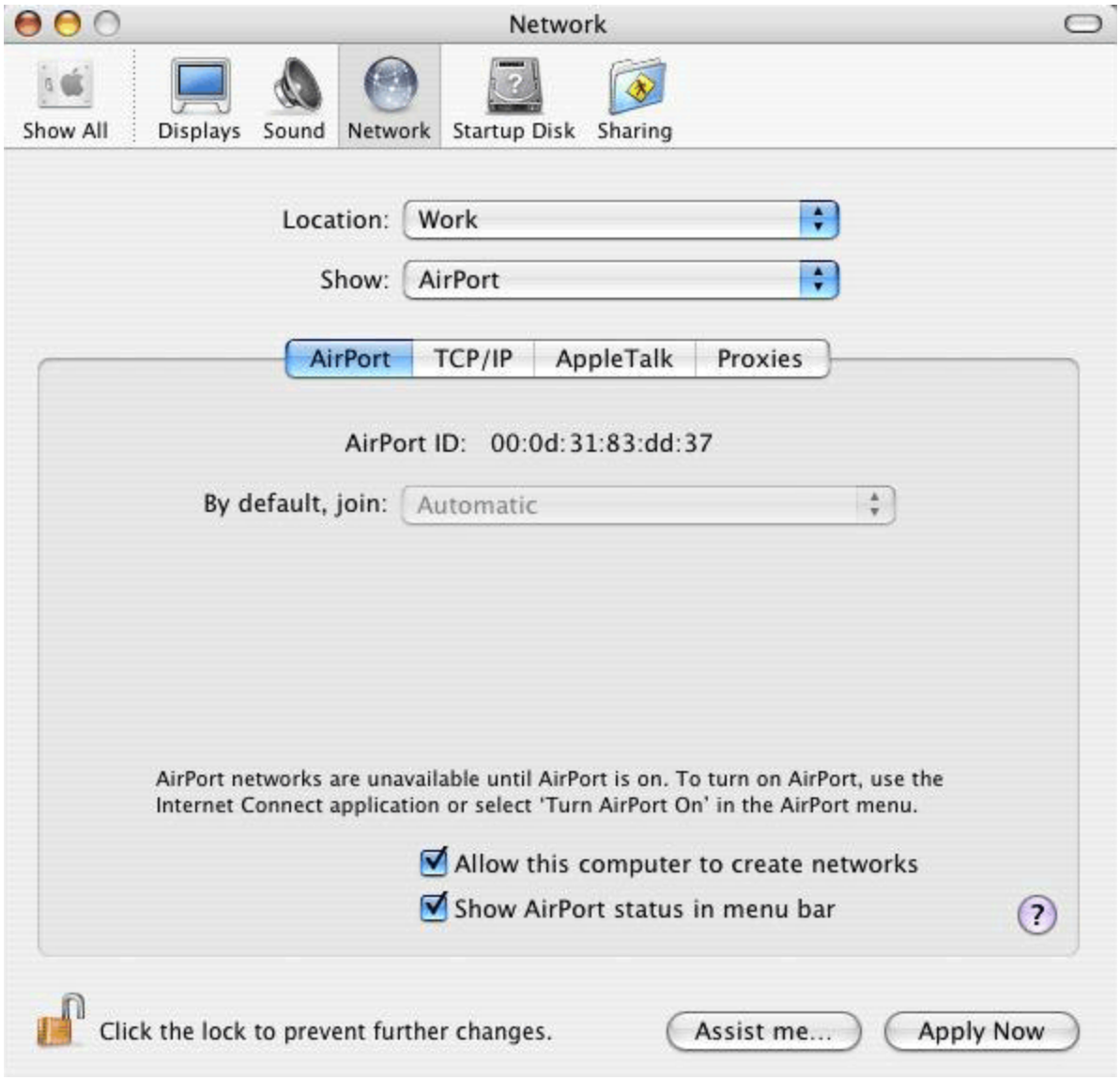
In the **cmd** window that opens, type ipconfig /all<**Enter**> to get the list of network interfaces. If the system has multiple wireless adapters, search for the wireless adapter. In the example below, the wireless adapter is Ethernet adapter Wireless Network Connection 14:. Once the adapter has been

identified, the MAC address is the physical address. The wireless mac in the example below is 00-19-9E-E0-93-9E.



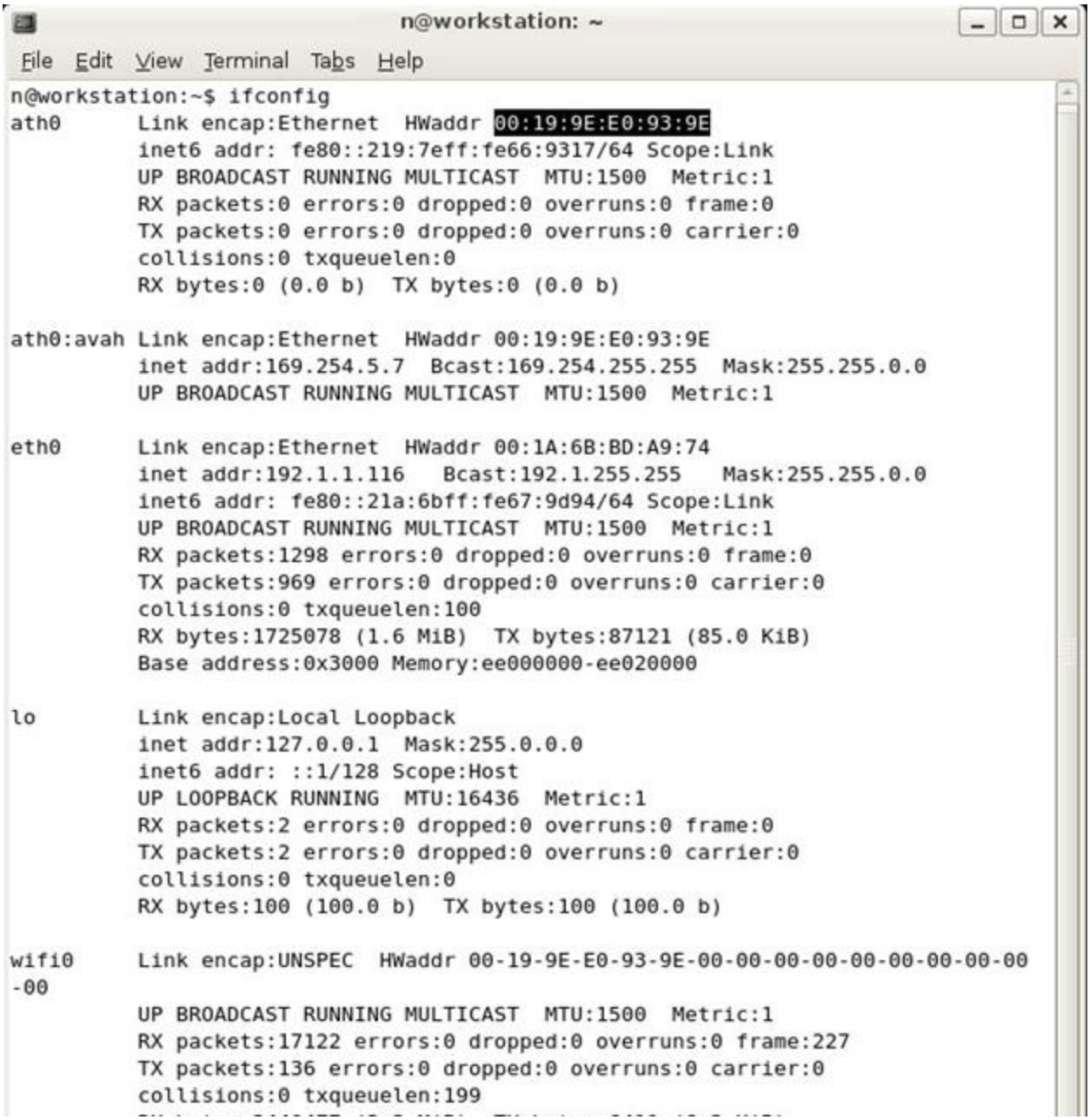
Find MAC Address-MAC OSx

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

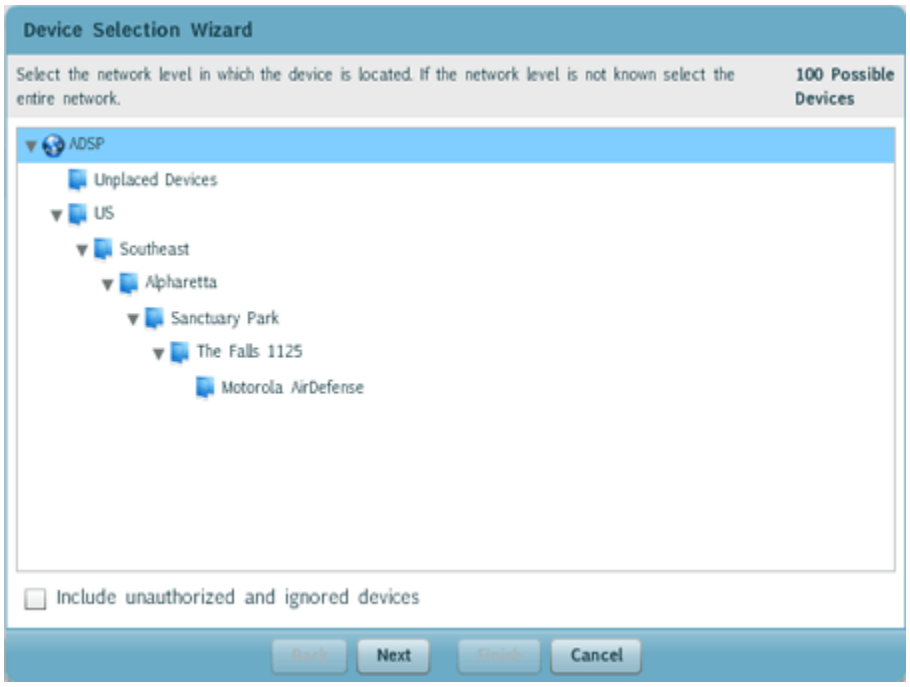
Open a terminal and type ifconfig<**Enter**> at the prompt. This will display information for all network adapters on the machine. Identify the wireless adapter. The HWaddr is the MAC address which is 00:19:9e:e0:93:9e in the screen shot below.



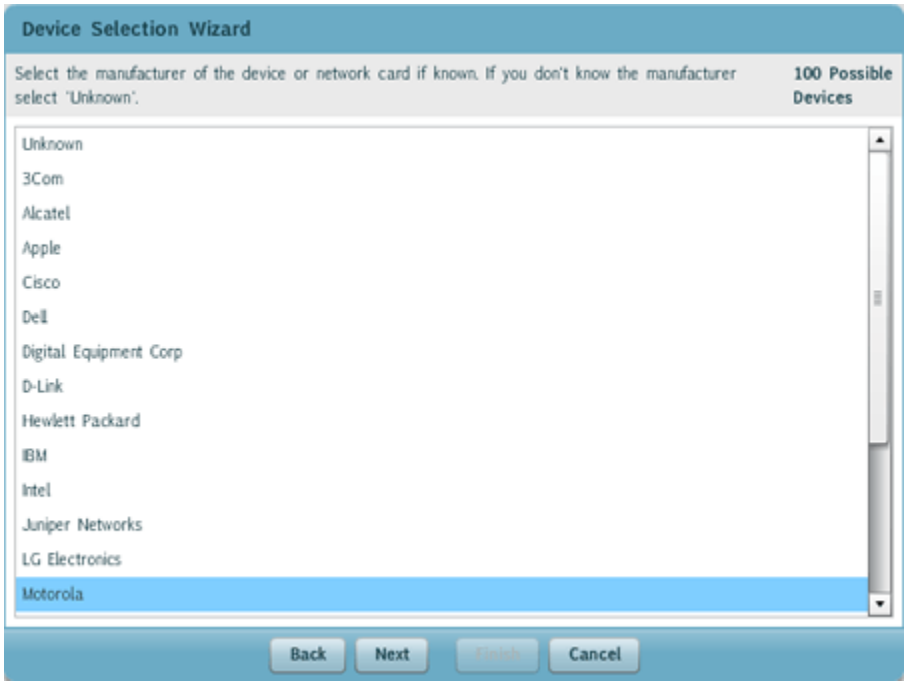
Device Selection Wizard

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.

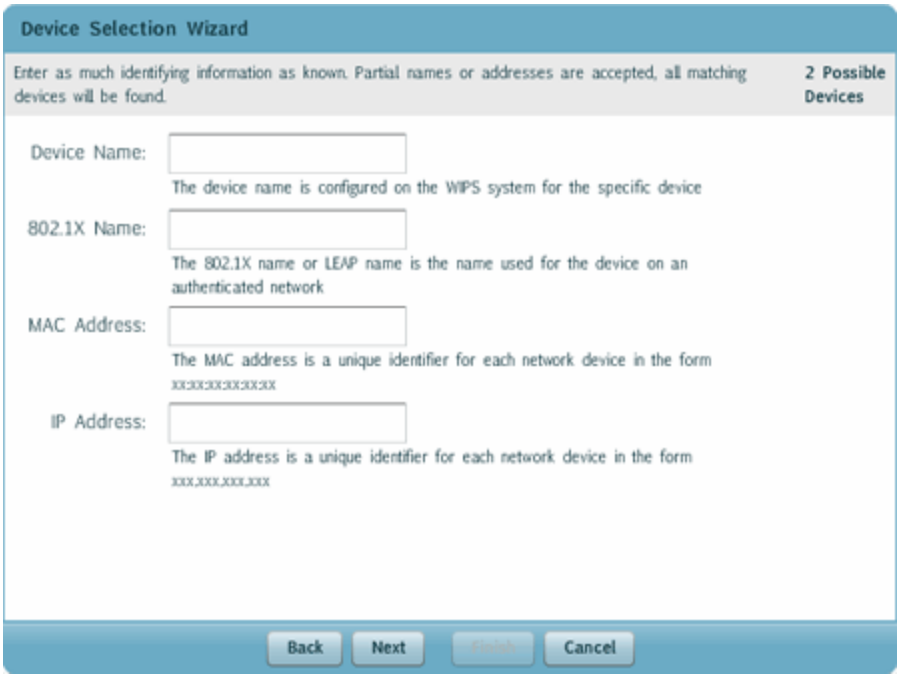
1. Select a scope by highlighting the appliance or a network level. You should try to narrow the scope as much as possible. Only authorized stations are included in the device list. To include unauthorized or ignored devices, click the checkbox near the bottom of the wizard to place a checkmark in the 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.



3. 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.



4. 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:

   a. Select the nearest Sensor from the drop-down list.

   b. Turn the Wireless Client off and then click the **Device is Off** button. The wizard starts collecting data.

   c. 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.

   d. 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.

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.

The Troubleshooting data loads.

Wireless Client Status

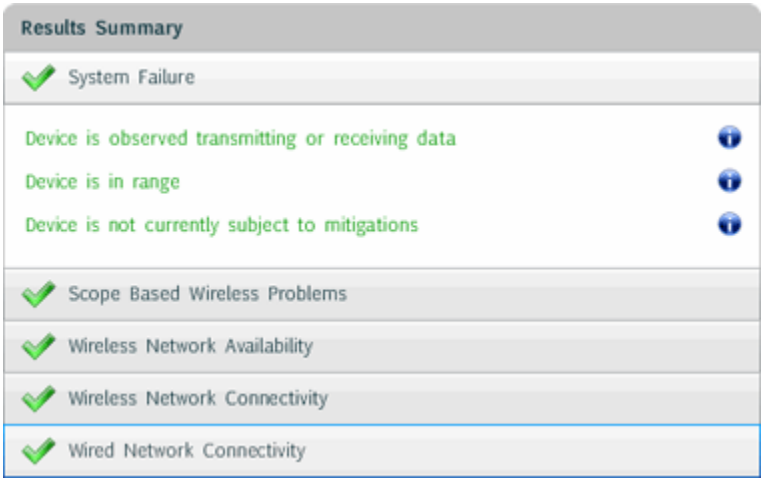
A Wireless Client status message is displayed after troubleshooting has completed. If no problems were observed, a green message box is displayed that indicates so.

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

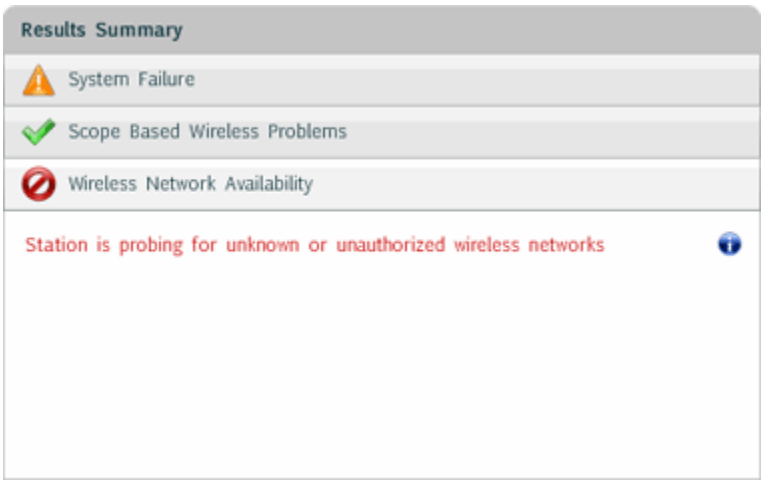
If a problem was observed that is definitely the reason a station cannot connect to the network, a red message box is displayed showing the reason for failure.

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.



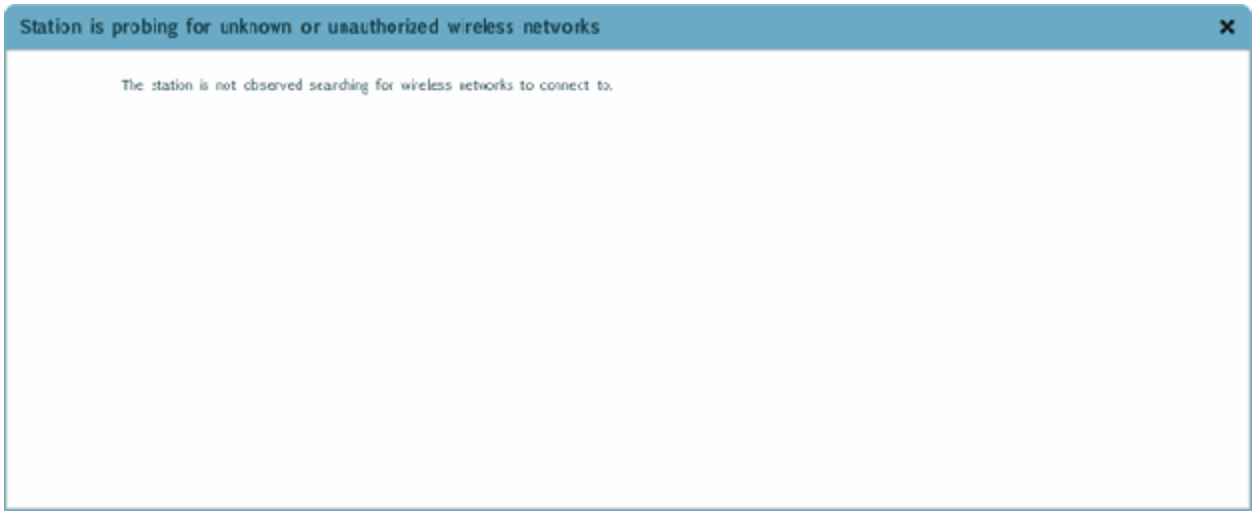
If problems were observed, you may see a **Results Summary** window similar to the one shown below.



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

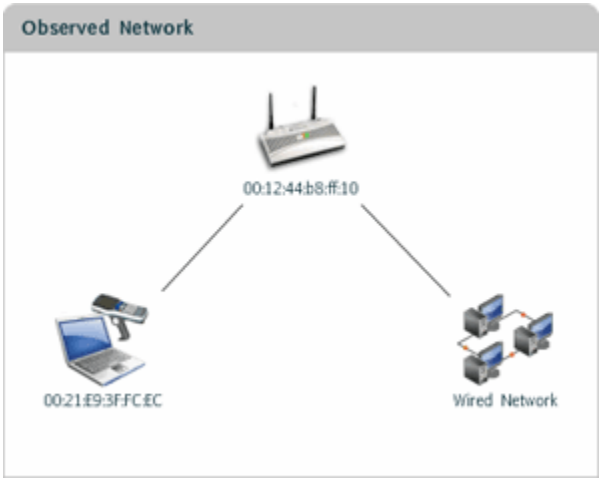
- No problem observed.
- Possible problem; needs further investigation.
- Definite problem observed.

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 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.

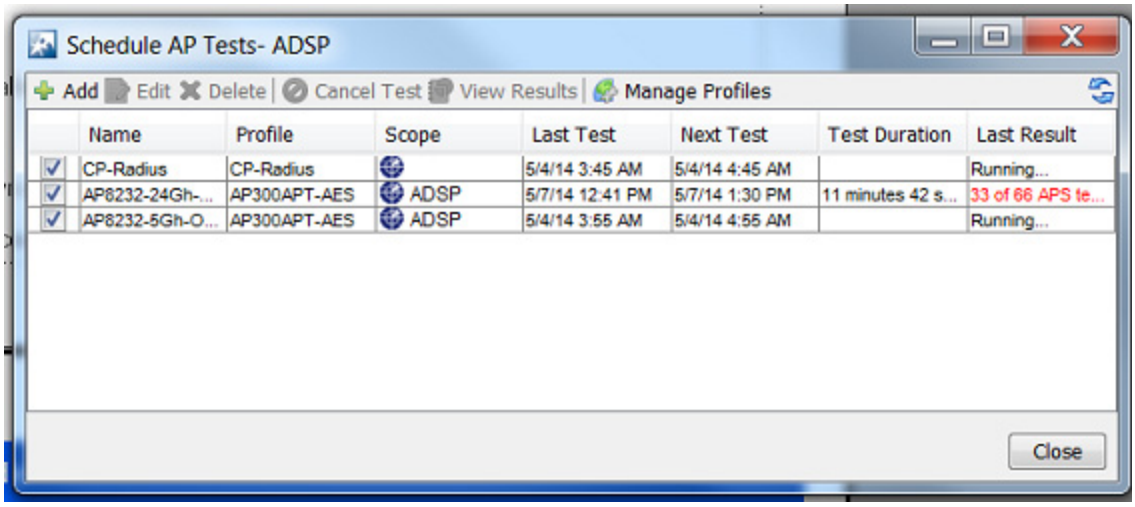
You can only export captured frames from the current Troubleshooting test. Therefore, you must export captured frames that you want to save before running the next test.

AP Testing

AP connectivity testing allows remote testing of network connectivity from the perspective of a wireless station. By utilizing the radio of the wireless sensor to simulate a wireless client station, true end-to-end network testing can verify all aspects of the wireless application’s data path. Connectivity test can be configured two ways: scheduled and on-demand.

Scheduled AP Tests

From the **Schedule AP Tests** window you can schedule an AP test and view a list of all scheduled AP tests. Go to **Menu > Schedule AP Tests** to display the AP test schedule.



From this window you can:

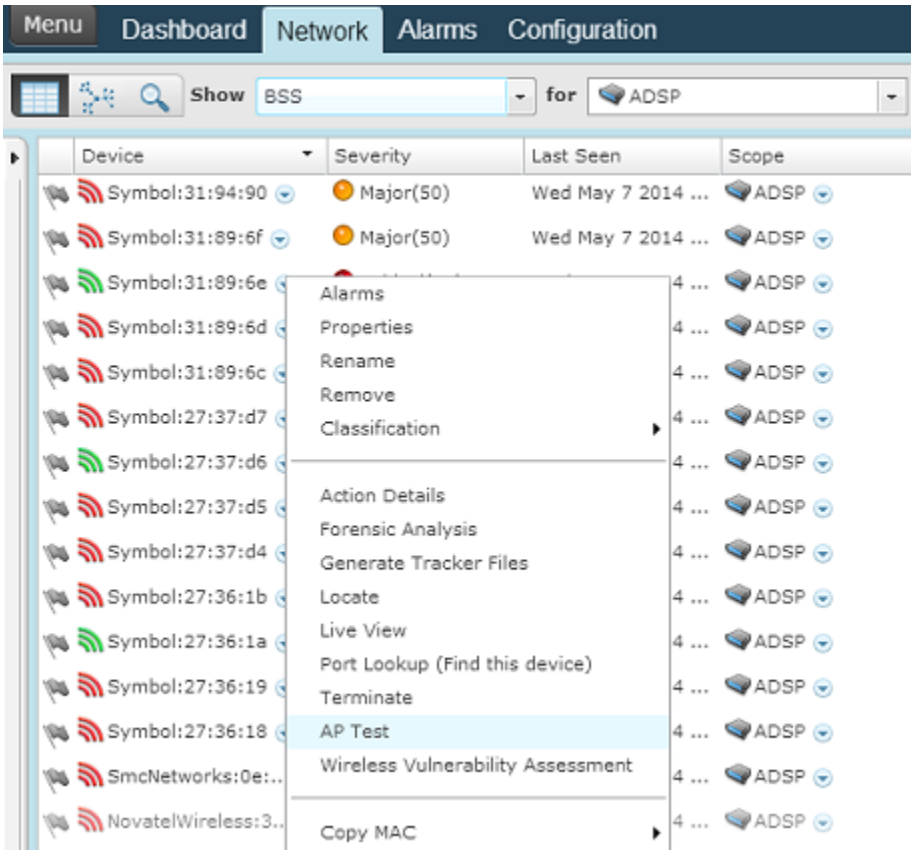
- Add, edit, delete, and cancel tests
- View detail test results
- Manage the profiles that are used to run tests on similar APs.

On-demand AP Tests

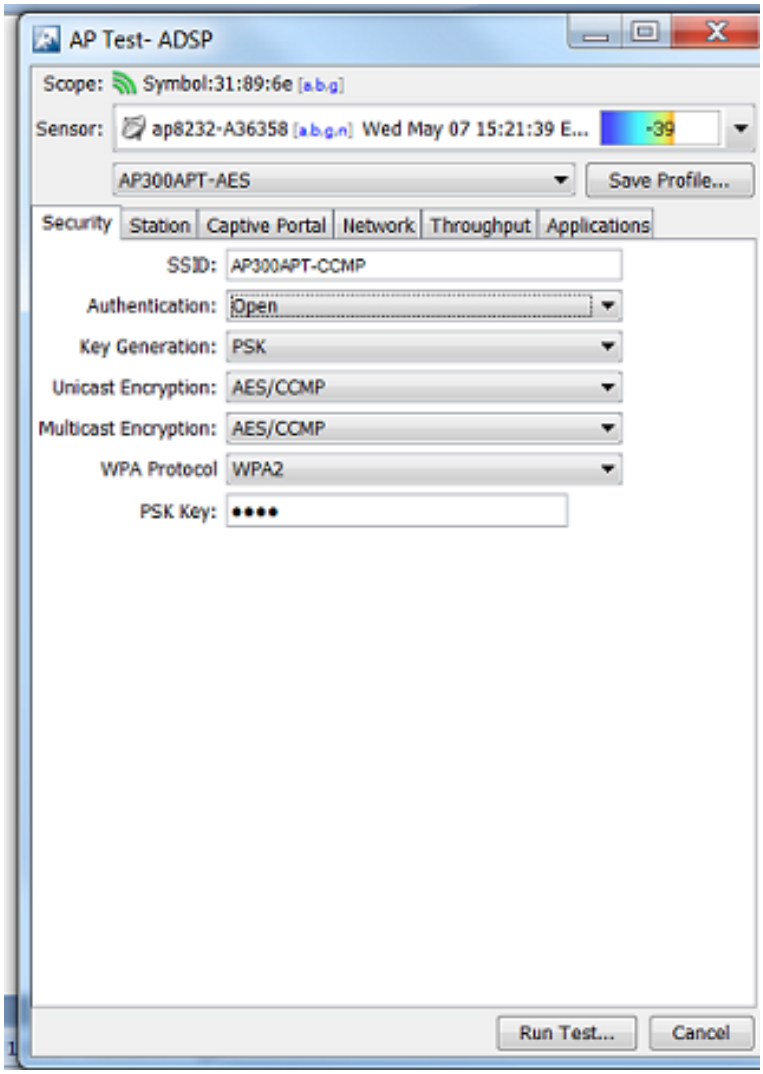
1. Click the Network tab.
2. Select **BSS** from the **Show** drop-down menu.
3. Select the AP you wish to test.

NOTE The AP must be sanctioned, as indicated by the green symbol on the device.

4. Click on the down arrow on the device and launch **AP Test**.

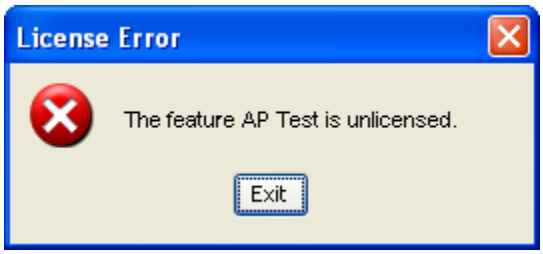


The test results for that device are displayed in a window.



AP Test License

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



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

Vulnerability Assessment

Wireless vulnerability assessment provides remote wireless security testing. By simulating attacks from a wireless hacker's point of view, administrators can now identify sensitive systems exposed to the wireless network. This eliminates the need to go on-site and perform penetration testing.

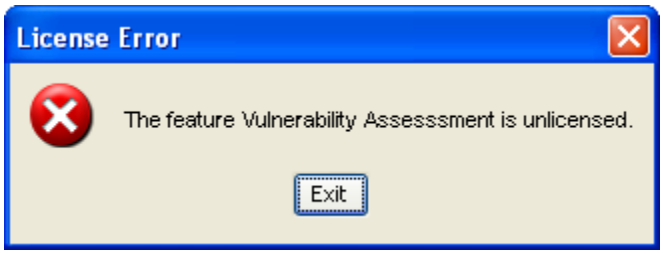
Scheduled Vulnerability Assessment

Go to **Menu > Scheduled Vulnerability Assessment**. You are directed to the Vulnerability Assessment window.

- If the vulnerability assessment schedule has been set up, the test schedule is displayed.
- If you need to add an assessment, Click **Add** in the top left corner of the window and complete the **Add Scheduled Vulnerability Assessment** form. Click **OK** when completed.

Vulnerability Assessment License

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



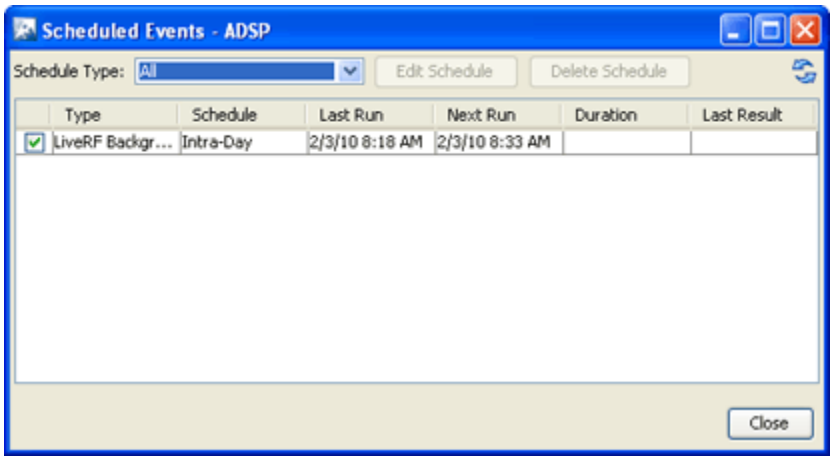
Click **Exit** to close this dialog window.

Scheduled Events

The Scheduled Events feature allows you to monitor all scheduled events from one source. You can schedule events throughout ADSP, and monitor the scheduled events from the Scheduled Events window.

Monitoring Scheduled Events

You can access Scheduled Events by selecting **Menu** > **Scheduled Events**.



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

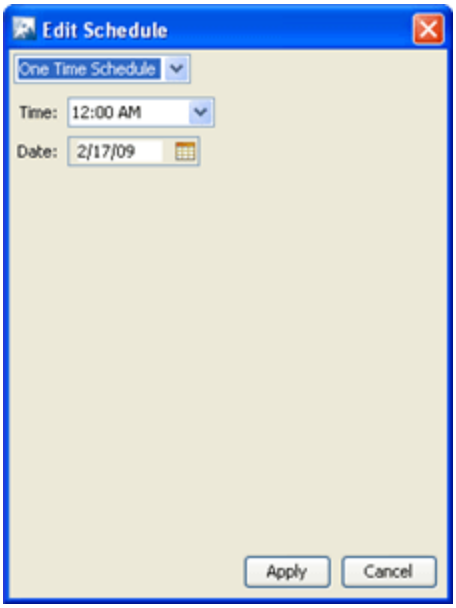
- AP Test
- Auto Classification
- Backups
- Firmware Upgrade
- Frame Capture
- Appliance Synchronization
- Forensic Backup
- Device Import
- Vulnerability Assessment
- Device Management Poll
- Device Configuration
- LiveRF Background Analysis.

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

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

Altering Event Schedules

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

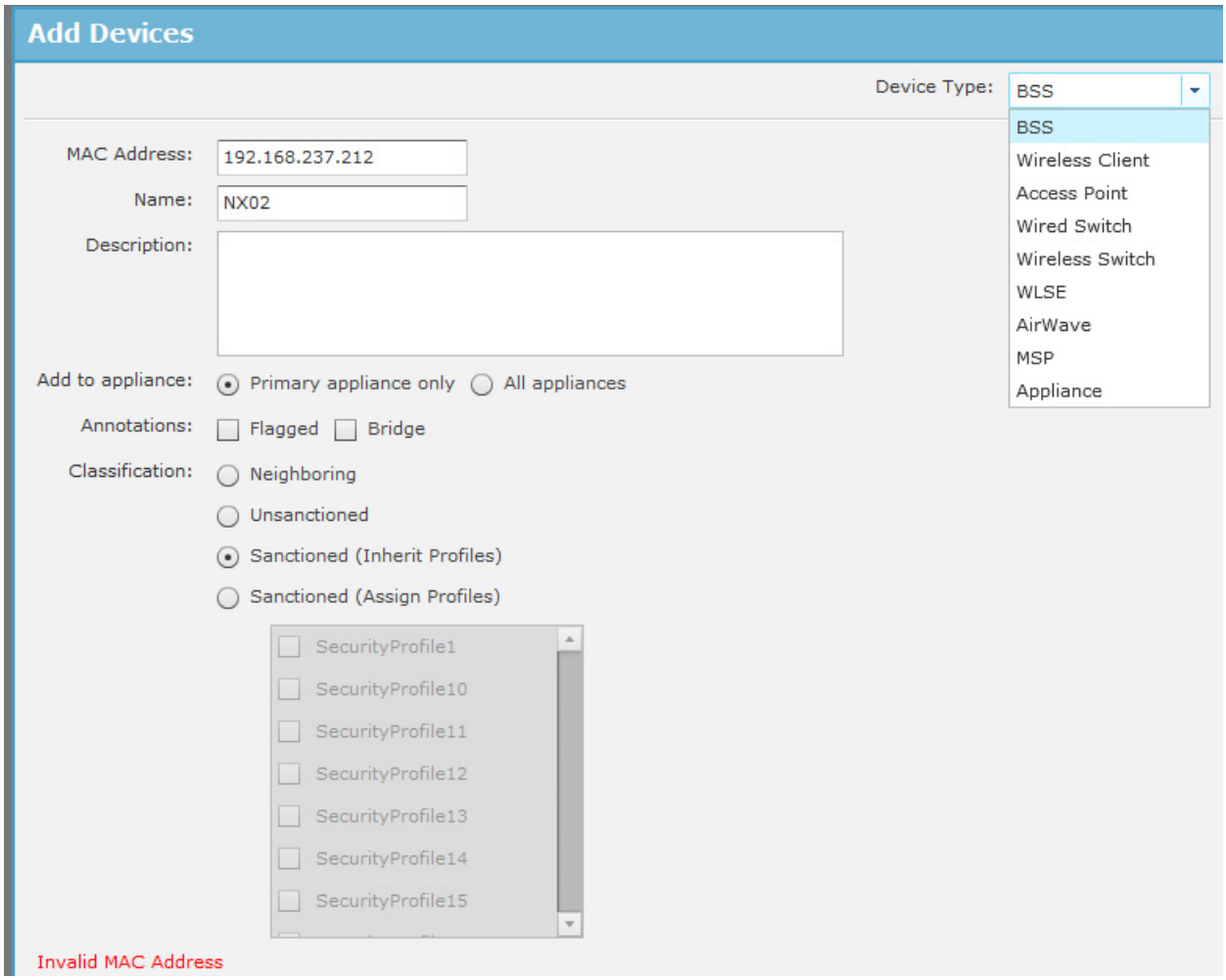


You can change how often the event is conducted by selecting **One Time Schedule**, **Intra-Day Schedule**, **Daily Schedule**, **Weekly Schedule**, or **Monthly Schedule** from the drop-down menu. Depending on the interval you select, fill in the related fields using the following table:

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

Add Devices

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

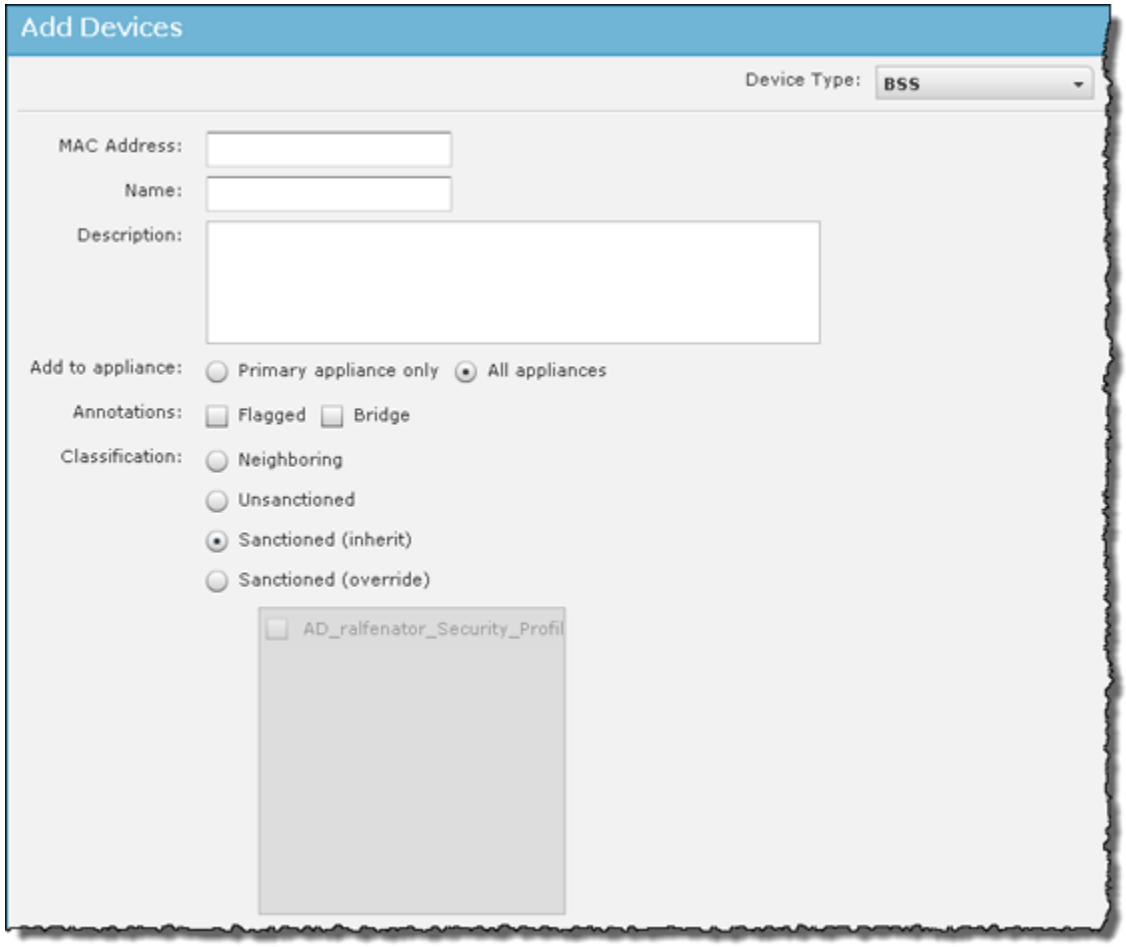


You can add any of the following devices by selecting the device from the **Device Type** menu:

- BSS
- Wireless Client
-
- Wired Switch
- Wireless Switch
- WLSE
- AirWave
- MSP
- Appliance

The fields change according to the selected device.

BSS Fields

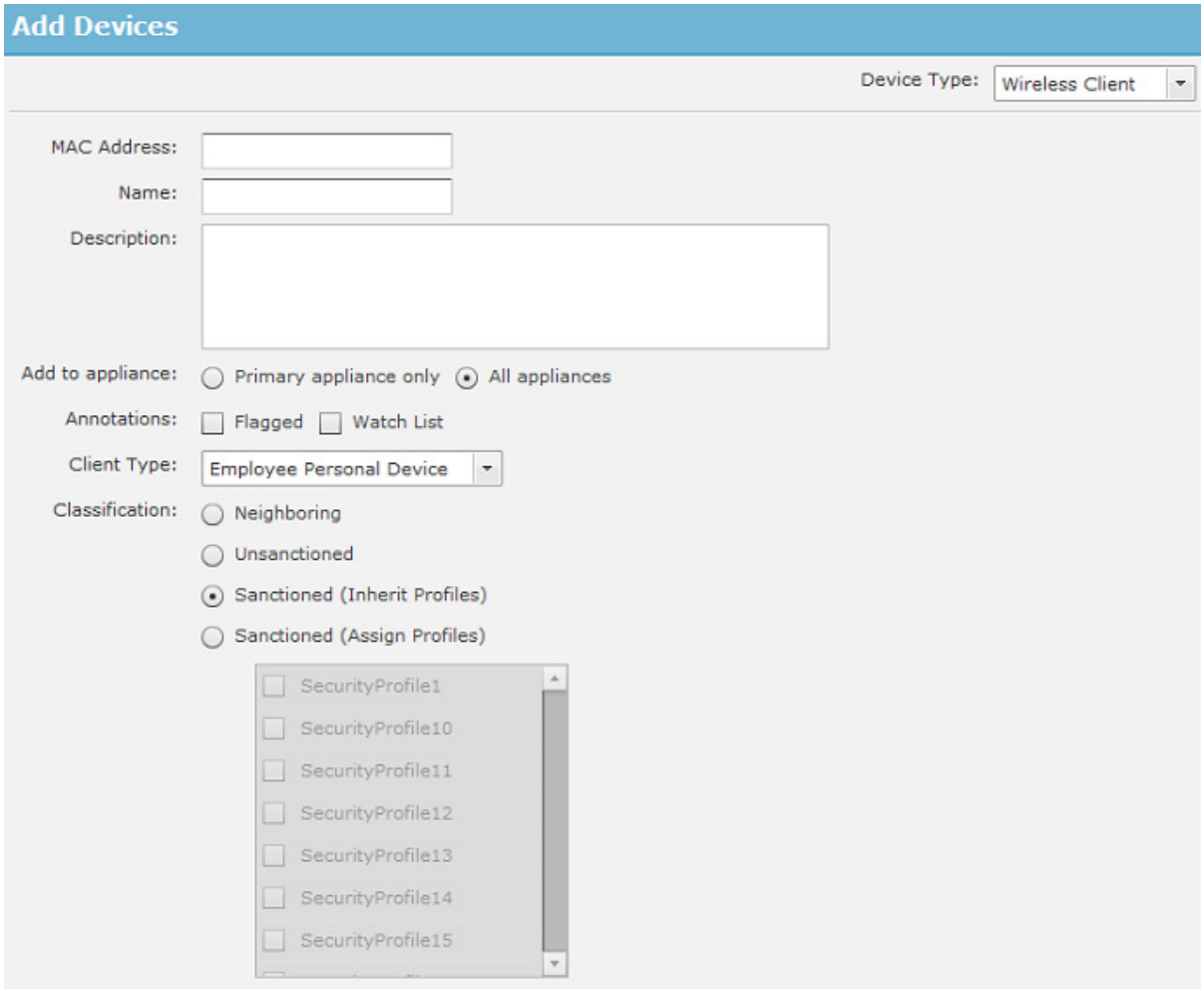


The following fields are available when adding BSSs:

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

Field	Description
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: • Neighboring • Unsanctioned • Sanctioned (inherit) • Sanctioned (override)—a list of available profiles is displayed to use as the override profile(s). You may select one or more profiles.

Wireless Client Fields

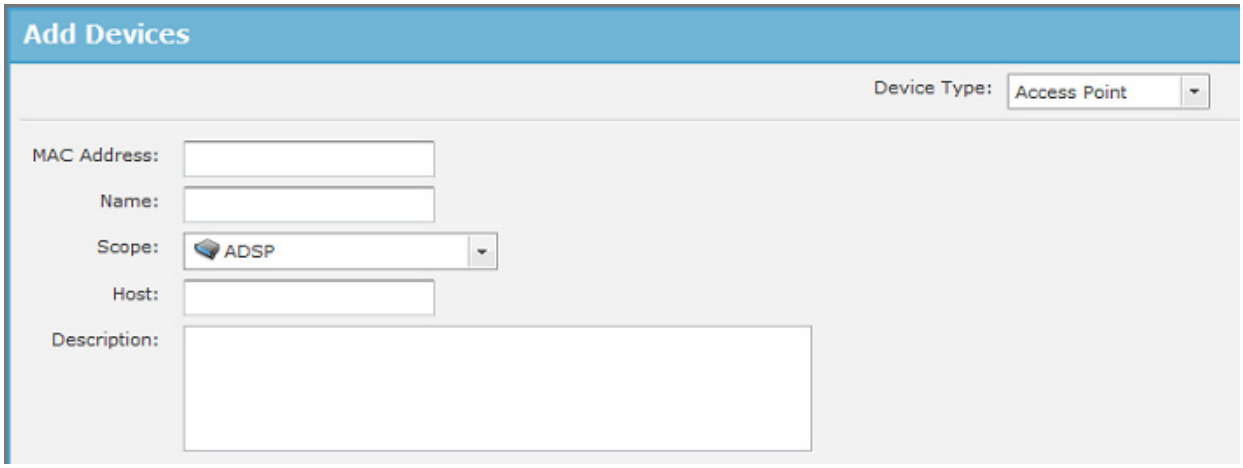


The following fields are available when adding Wireless Clients:

Field	Description
MAC Address	The MAC address of the device
Name	The name you want your device to display in your network
Description	Select a scope (usually a floor network level) from the drop-down menu
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.

Field	Description
Annotations	Specify if the device should be flagged or if it will be on a watch list. Select the appropriate checkbox.
Client Type	Select the client type from the drop-down list. The choices are: • Employee Personal Devices • Guest Wi-Fi User • In-store Customer • Laptop • Loyalty Customer • Phone • Potential Customer • Scanner • Tablet • Uncategorized Device
Classification	Specify if the device should be classified as: • Neighboring • Unsanctioned • Sanctioned (inherit) • Sanctioned (override)—a list of available profiles is displayed to use as the override profile(s). You may select one or more profiles.

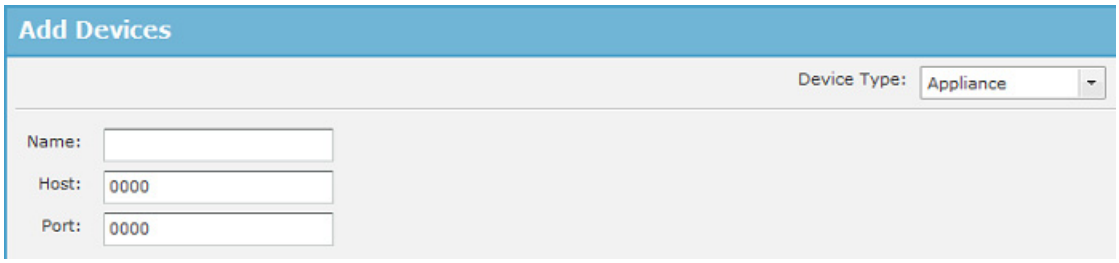
Other Device Fields



The following fields are available when adding APs, Wired Switches, Wireless Switches, WLSE, AirWave, and MSPs.

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.

Appliance Fields



The following fields are available when adding appliances.

Field	Description
Name	The name you want your device to display in your network.
Host	The host name of the device.
Port	The port where the devices is connected.

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

Import and Discovery

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

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

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

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

Importing profile settings requires 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.

Import Local File

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)

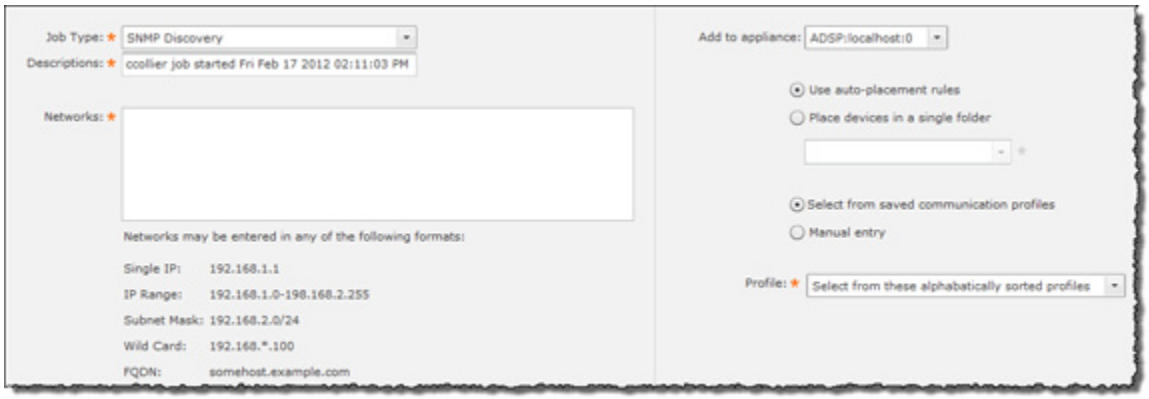
Field	Description
Select a sample CSV file	Selects a sample CSV file from the drop-down list. Once a file is selected, click **Open in New Window**. A new window is opened containing the selected file. You can copy this file and use it to create an import file.
Add to appliance	Appliance where you want 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.

Import Remote File

The following fields are available when importing remote files:

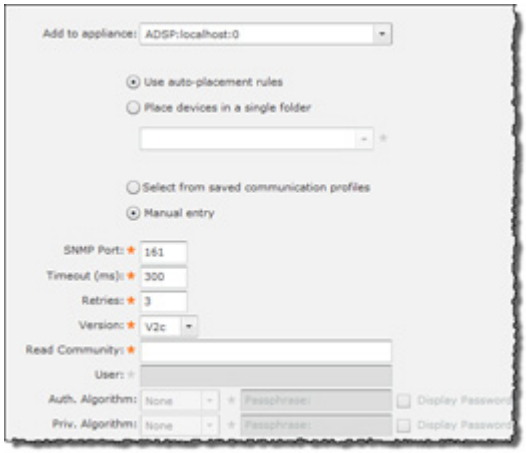
Field	Description
Job Type	**Import Remote File**
Descriptions	System generated description. You may change if you want.
Host	Host name or IP address
Protocol	Protocol used for communications
Path	Path name on the remote host including the import filename (e.g., /usr/local/tmp/filename)
User	User name 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

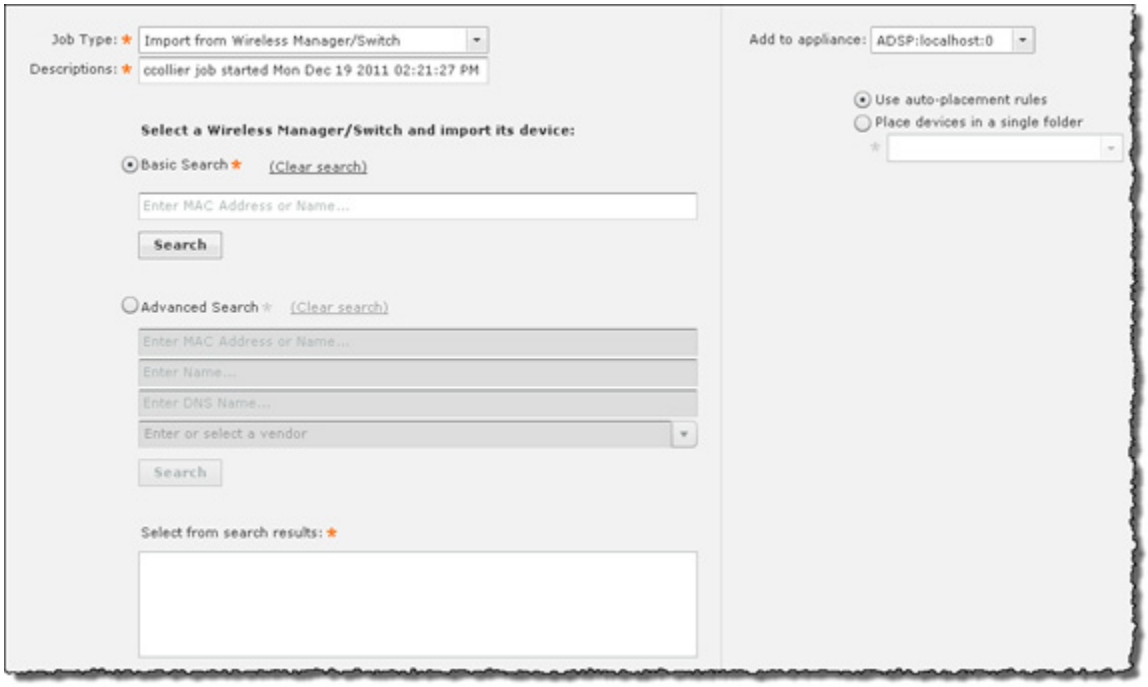


The following fields are available during SNMP discovery:

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

Field	Description
Add to appliance	Appliance where you want to import device (will only list your appliance unless you have a Central Management license).
Device placement	You have the option of using the auto-placement rules or selecting a folder from your network tree.
Execution Method	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.  The additional options for manual entry are: • SNMP Port—Device SNMP port number; normally set to 161 but can be different • Timeout (ms)—Timeout in milliseconds to attempt import • Retries—Number of retries to attempt import • Version—SNMP version used: V1, V2c or V3 • Read Community—Read Community string used for the SNMP authentication • User—Name of the V3 user, which is configured on a switch for SNMP V3 access. This option is inactive until V3 is selected as the version. • Authentication/Privacy Algorithm—You may optionally supply an authentication and privacy algorithm along with a passphrase for each. These parameters must match settings on the switch exactly. These options are inactive until V3 is selected as the version. Selecting the Display Password checkbox displays the passphrase as text.

Import from Wireless Manager/Switch



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.
Basic Search	Specify a partial or full MAC address of a Switch or enter the name; then, click Search. The search results are listed in the Select from search results box. Select a device from the list and then click one of the Start Import buttons. Devices associated with the Wireless Manager/Switch are imported into ADSP.
Advanced Search	Enter search criteria in one or more fields, then click **Search**. The search results are listed in the **Select from search results** box. Select a device from the list and then click one of the **Start Import** buttons. Devices associated with the Wireless Manager/Switch are imported into ADSP. The following search criteria are available: • MAC address • Name • DNS name • Vendor name.
Add to appliance	Appliance where you want to import device (will only list your appliance unless you have a Central Management license).
Device placement	You have the option of using the auto-placement rules or selecting a folder from your network tree.

Import File Formats

There are two types of import files:

- Devices, and
- Profiles (configurations).

Import files contain records, made up of columns (fields), that are used to import devices or profiles and configuration settings into ADSP.

You will need to use text files to import devices and profiles. There are two commonly used text file formats:

- Comma separated values text files (CSV), in which the comma character typically separates each field of text.
- Delimited text files (TXT), in which the TAB character typically separates each field of text.

Use a text file, such as a Comma Separated Values (CSV) file, to import devices and profiles. To create an import file, use a text editor such as Notepad.

NOTE A CSV file can be used instead of a TXT file.

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.

You can find more detailed information about the records 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
- BLUETOOTH

- 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)—enter true for AP Test; false for Vulnerability Assessment.
- Profile name

- Scope [BSS MAC address or path to folder separated by a slash (/)]
- Number of retries
- Switch Sensors on retry (true or false)
- Signal threshold
- Last seen time in minutes
- Skip test on sensor busy (true or false)
- Filter on SSID (true or false)
- Time to wait for Sensor in minutes
- Number of tests (assessments) to run in parallel
- Prefer OTA tests (true or false)
- Schedule name
- Schedule type (daily, intraday, monthly, weekly, or onetime)
  - 'Daily' has the following sub-fields:
    - hours (the hour of the day)
    - minutes (the minute of the hour)
    - type (interval, weekdays, or weekends)—interval means run in every x days. weekdays means run on weekdays. weekends means run on weekends.
    - interval (in days)—an interval of 1 means every day; an interval of 4 means every four days (this sub-field is only used if type is interval)
  - 'Intraday' has the following sub-fields:
    - hours (the hour of the day)
    - minutes (the minute of the hour)
    - number of hours between runs (must be > 1)
  - 'Monthly' has the following sub-fields:
    - hours (the hour of the day)
    - minutes (the minute of the hour)
    - months to run [colon(:) delimited]; i.e., January:February:etc
    - type (day, last, or specific)—day means run on the nth day of the month. last means run on last day of the month. specific means run on the last, first, second, third, fourth, or fifth occurrence on the specified day of the week (Monday, Tuesday, Wednesday, etc).
  - 'Weekly' has the following sub-fields:
    - hours (the hour of the day)
    - minutes (the minute of the hour)
    - days to run [colon(:) delimited]; i.e., Sunday:Wednesday
    - interval (weeks between runs)
  - 'Onetime' has the following sub-fields:
    - hours (the hour of the day)
    - minutes (the minute of the hour)
    - month (1 - 12 with 1 being January and 12 being December)
    - day of the month (1 - 31)
    - year (i.e., 2012)

Examples:

scheduled_test,TRUE,APT_ProfileName1,00:11:22:33:44:55,2,TRUE,-70,10,TRUE,TRUE,10,20,Schedule1,onetime,6,30,5,5,2012

scheduled_test,FALSE,WVA_ProfileName1,ADSP/Unplaced Devices,2,TRUE,-70,10,TRUE,TRUE,10,20,TRUE,Schedule2,daily,interval,10,20,1

Bluetooth Monitoring

Bluetooth monitoring is a feature that provides 24x7 monitoring of Bluetooth devices in Enterprise environments. With this feature, ADSP can automatically scan and detect security threats from unsanctioned Bluetooth devices, as described in the following list.

- Detection of any unsanctioned Bluetooth device.
- Detection of any unsanctioned Bluetooth device present longer than the configured duration.
- Detection of any unsanctioned Bluetooth device detected outside of business hours.

The system also generates notifications to administrators when a threat is detected.

Installing the Bluetooth Sensor

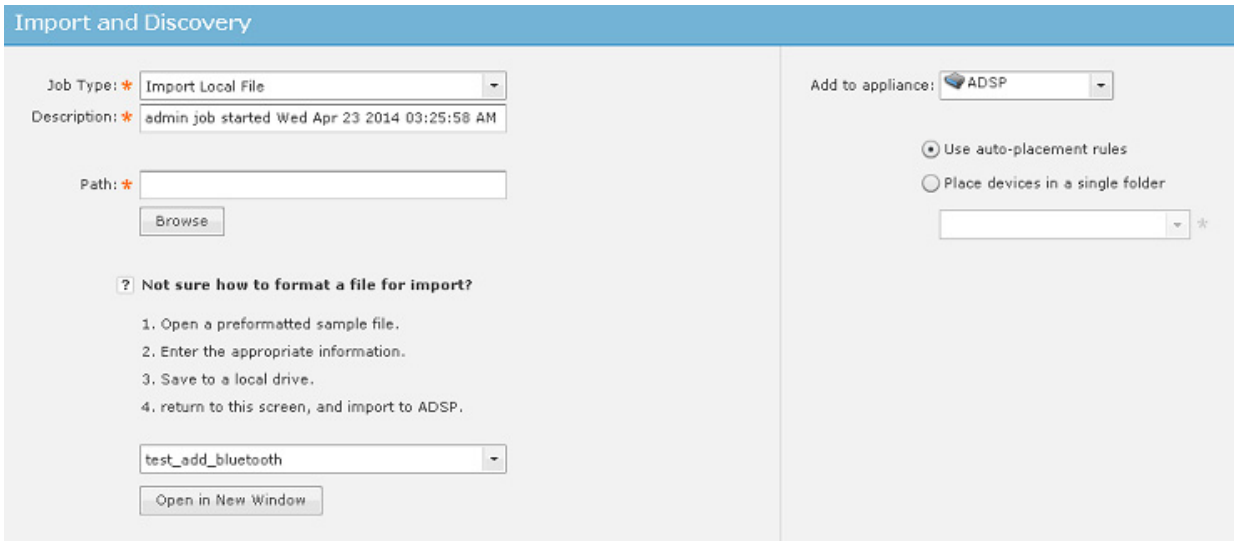
The Bluetooth sensor is an IO Gear GBU321 BT sensor. It is used in conjunction with the modular AP8132 device for providing a BT monitoring solution. To install, plug the BT sensor into the USB interface of the AP8132. The MAC address of the BT sensor is displayed in the LiveRF floor map next to the AP8132 device it is plugged into.

Importing Bluetooth Devices

To import Bluetooth devices, go to Menu in the ADSP UI, and then click on **Import and Discovery**. In the Job Type box, select Import Local File. Browse to the location of the CSV file. When the file name is displayed, click on **Open in New Window**. The CSV file is displayed.

- The format of the CSV file is similar to that of WLAN client/station, except that the security and performance policy fields are blank (represented as “,” separated columns.)
- When a Bluetooth device is detected by ADSP, it is marked as “Sanctioned” or “Unsanctioned” depending on its classification in the CSV file.

- The Bluetooth monitoring support and alarms are enabled only when the WIPS license is assigned to the WLAN sensor on the AP8132 device.



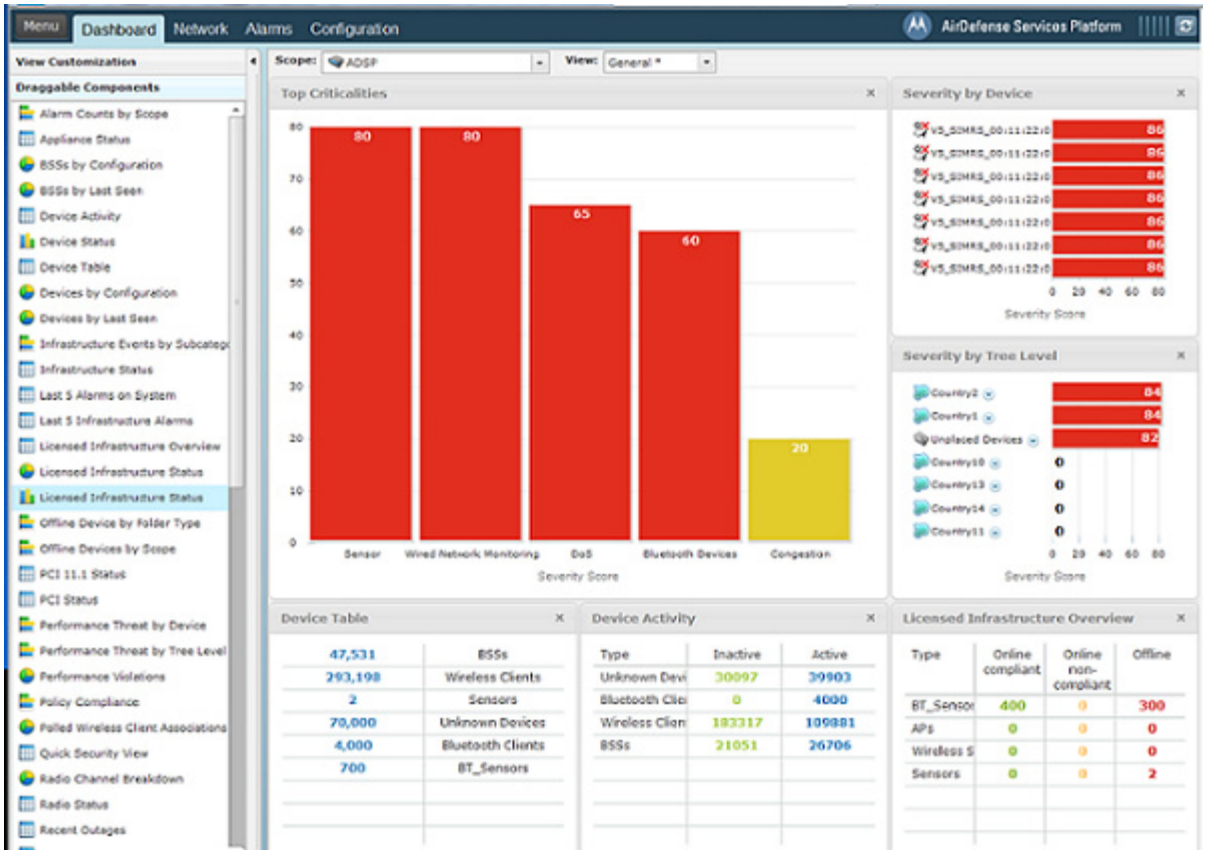
Bluetooth License

You must have a Bluetooth license in order to access the Bluetooth feature.

CHAPTER 4 THE DASHBOARD

Dashboard Tab

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.

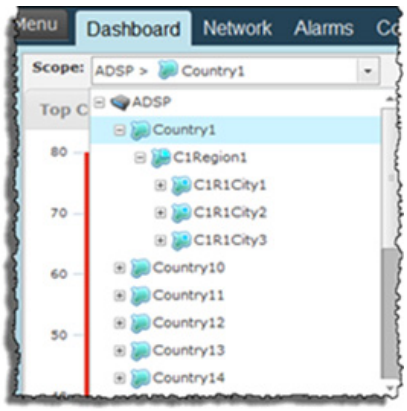
See the *Dashboard Components* topic for a description of all the available components.

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**, as shown in the following example:



Scopes are defined as the following network levels:

- System—Displays information for your entire network (system). If you have a Central Management license, selecting **System** as the scope displays a combination of all appliances being managed.
- 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.

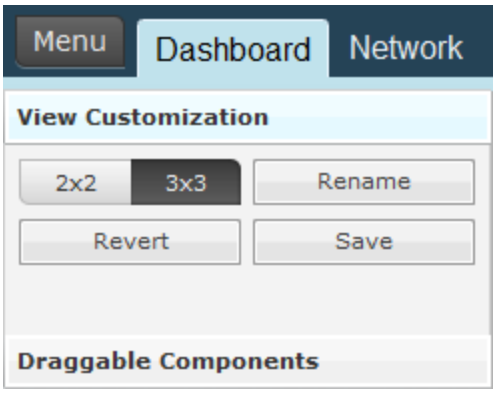
Capabilities with a Central Management License

With a Central Management license, the Dashboard becomes a monitor of all appliances along with their associated devices. You can monitor your entire system at once or each individual appliance. Additionally, 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

View Customization

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 **View Customization** button. The following screen is displayed:



You can click on the **2x2** or **3x3** button. You can then change the name of a view by clicking the **Rename** button, typing in the new name, and then clicking **OK**.

Draggable Components

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. (Such as 'General.')
2. Click the **Draggable 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.

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 counts.
Appliance Status	Displays the alarm status of the appliances on your network.
Bluetooth Clients	Displays Bluetooth clients (sanctioned, unsanctioned, and neighboring) seen on your network.
BT_Sensors	Displays Bluetooth sensors see 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, BSSs, and Bluetooth Devices seen on your network in tabular form.
Device Status	Displays the active/inactive state of Unknown Devices, Wireless, Clients, and BSSs, and Bluetooth Devices seen on your network in graphical form.
Device Table	Individually lists the total number of BSSs, Wireless Clients, Sensors, Unknown Devices, Bluetooth Clients, and BT_Sensors on your network.
Devices by Configuration	Displays a pie chart of devices by configuration (authorized, ignored, and unauthorized). Also lists the total number of devices seen on your network.
Devices by Last Seen	Displays a pie chart of the devices seen on your network over the last five days. Also lists the total number of devices as well as the totals for each day.
Infrastructure Events by Subcategory	Displays a bar chart showing infrastructure events by subcategory.
Infrastructure Overview	Displays a list of infrastructure devices in three columns (Online compliant, Online non-compliant, and Offline).
Infrastructure Status	Displays a list of infrastructure devices showing if they are online or offline, and the total number of each device type.
Last 5 Alarms on System	Displays a list of the last 5 alarms generated by ADSP.

Component	Description
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.
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.

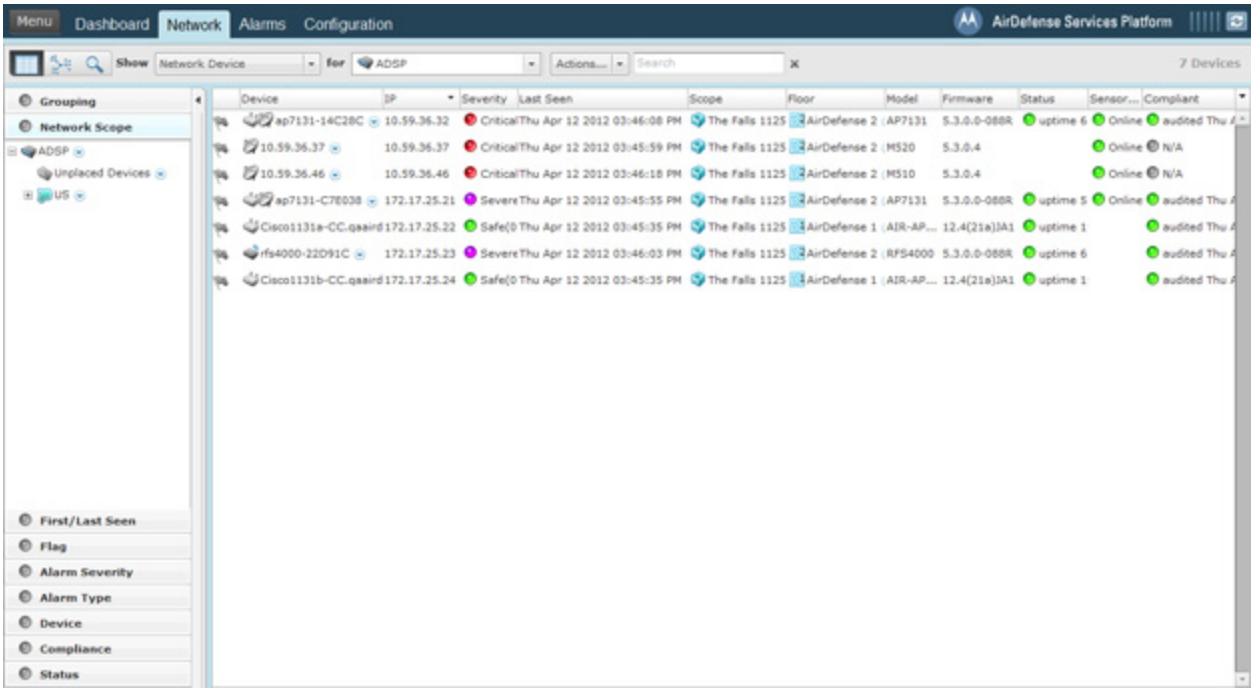
Component	Description
Radio Status	Displays the radio status by band (2.4 GHz and 5 GHz) and lists the online APs and Sensors. A count is displayed in the form of x of x.
Recent Outages	Lists devices with recent outages along with the associated appliance, start time of the outage, the type, and criticality.
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.
System Load	Displays a column chart reflecting system load. Charts include percentages for: • Sensor count • Managed network devices • Total device load • Active device load.

Component	Description
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.

CHAPTER 5 NETWORK

Network Tab

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



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 Filter.

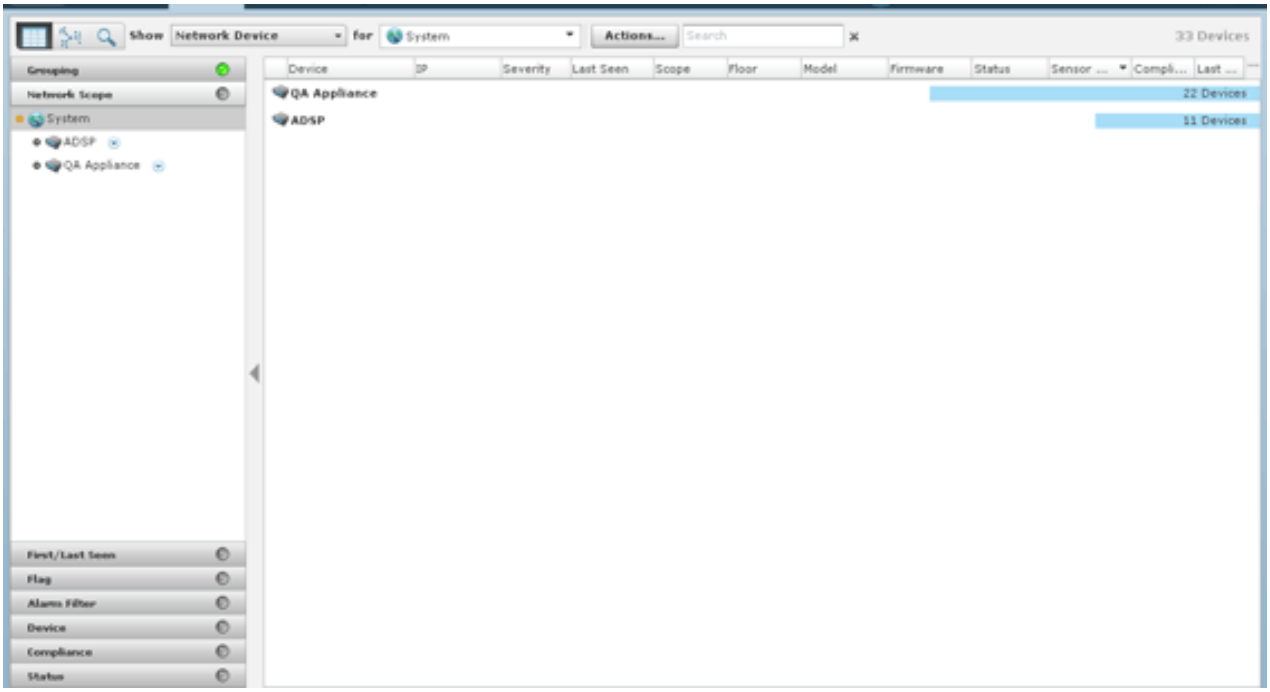
The information displayed depends on the type of device selected. You can sort device information according to information in a column by clicking the column header.

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 after the last column (Compliant.) The menu changes according to the selected device in the **Show** drop-down menu.

Capabilities with a Central Management License

With a Central Management license, you can display devices from any managed appliance in the Network tab. If displaying devices on an appliance level or a network level, only the devices for that appliance or network level are shown.



Select Network View

Show Menu

Use the **Show** menu on the top menu bar to select the devices that you want to display in the Network tab.

Viewing the Network

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 APs, Sensors, Wired Switches, Wireless Switches, WLSE devices, AirWave devices, and Managed Services Providers (MSPs).
- BSSs
- Wireless Clients

- Unknown Devices
- Bluetooth 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.

Types of Devices

From the drop-down menu under **Show**, you can select a device. The choices are:

- Network Devices
- BSS
- Wireless Clients
- Unknown Devices
- Bluetooth.

Select for ADSP system or a specific city, building, floor, etc.

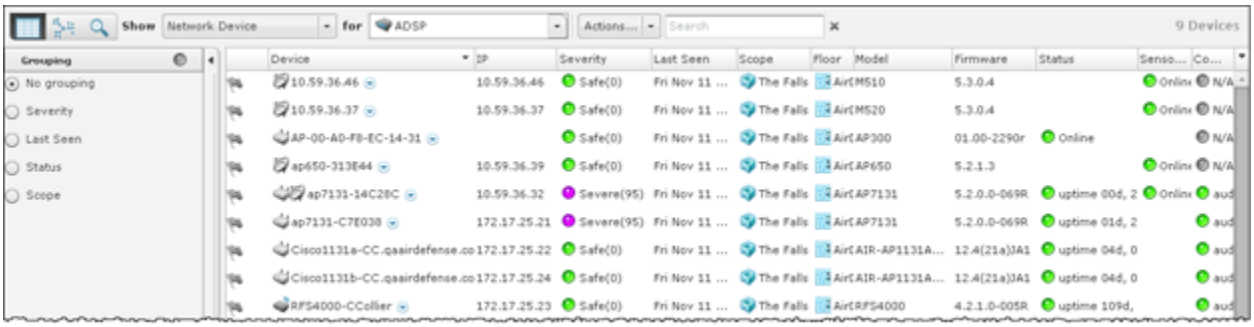
Actions Menu

From the drop-down menu under **Actions** on the top menu bar, you can select a an action to apply to the selected device. The actions available vary by device, as explained in the following section, *Network Devices*.

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.

Network Devices

Click the drop-down menu under **Show** and click on **Network Device**. ADSP displays a list of APs, Sensors, Wireless Switches, and Wired Switches seen in your network.



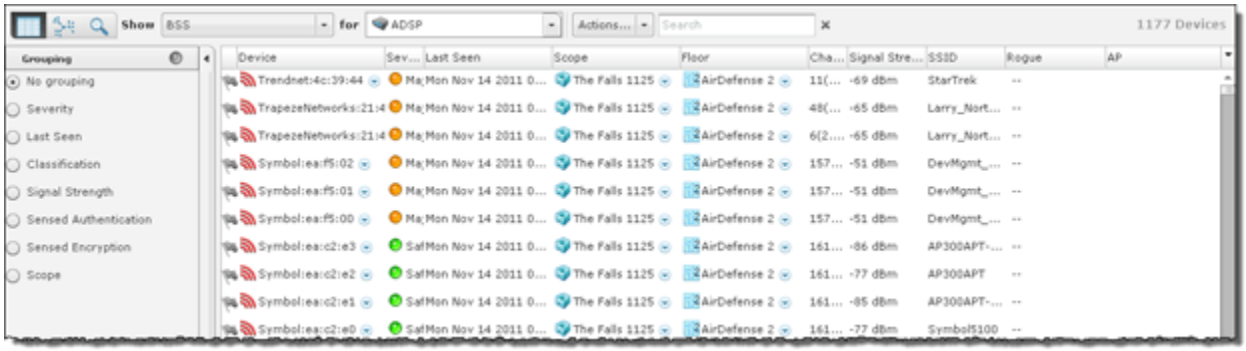
The list of Network Devices are displayed in a tabular format using a combination of the following columns:

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)
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)

Column	Description
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

Click the drop-down menu under **Show** and click on **BSS**. ADSP displays a list of all BSSs seen in your wireless network.



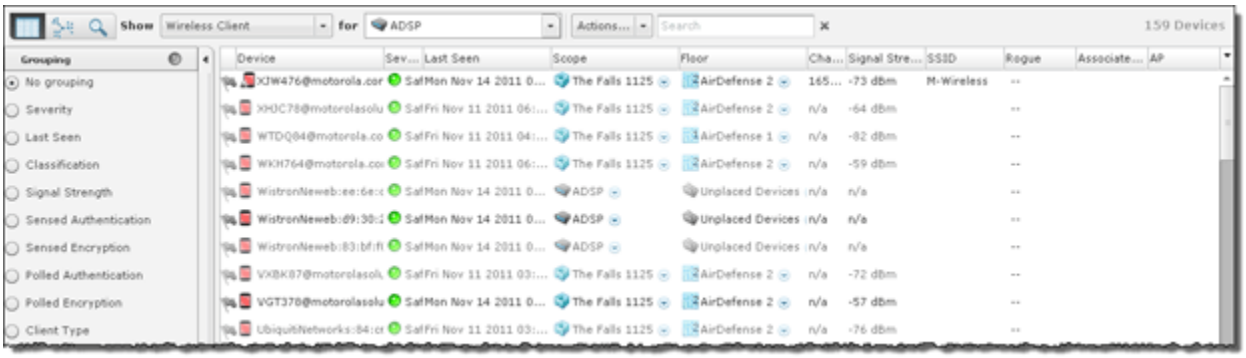
The list of BSSs are displayed in a tabular format using a combination of the following columns:

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)
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 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)

Column	Description
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	Indicates a current live state. • AP Test— • Wireless Vulnerability Assessment— • Termination— • Dedicate Spectrum Analysis — • Inline Spectrum Analysis—
Sensor	Displays the name of the Sensor that sees the BSS.
AP	Displays the name of the . (default header)
Associated Clients	Displays the number of clients that have associated with the BSS.

Wireless Client

Click the drop-down menu under **Show** and click on **Wireless Client**. ADSP displays a list of all Wireless Clients seen in your wireless network.



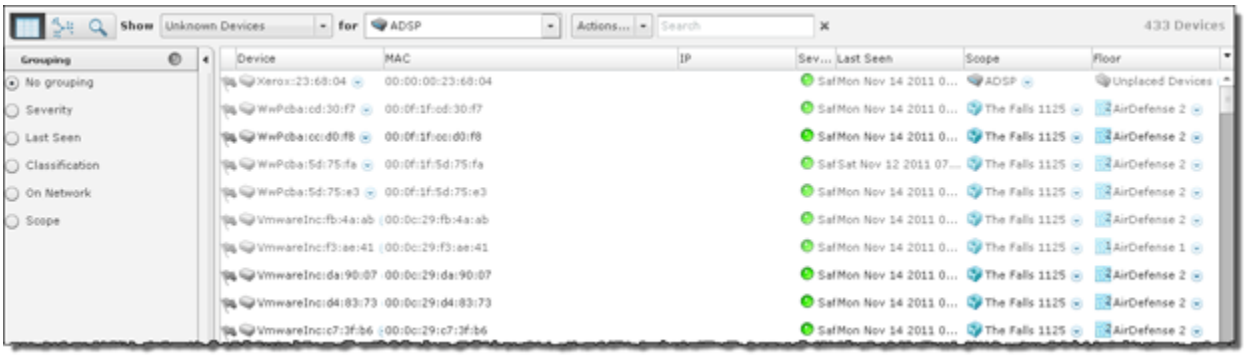
A list of wireless clients is displayed in a tabular format using a combination of the following columns:

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.
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)

Column	Description
Device Actions	Indicates if any of the following actions have occurred: • AP Test— • Wireless Vulnerability Assessment— • Termination— • Dedicate Spectrum Analysis — • Inline Spectrum Analysis—
Associated BSS	Displays the BSS that the Wireless Client has associated with.
AP	Displays the name of the . (default header)
Sensor	Displays the name of the Sensor that sees the Wireless Client.

Unknown Devices

Click the drop-down menu under **Show** and click on **Unknown Devices**. ADSP displays a list of all 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.



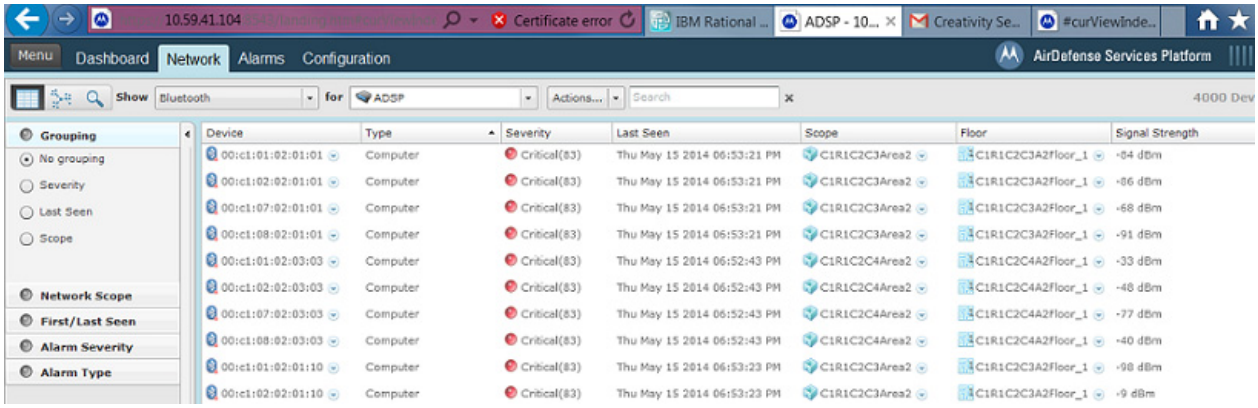
The list of Unknown Devices are displayed in a tabular format using a combination of the following columns:

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	Identifies how ADSP obtained the MAC address of a non-wireless device. The different entries are: • Sensor Segment—The frame containing MAC address was detected by a sensor on its wired port. This device is therefore known to be on a LAN segment containing the sensor and is therefore on the same wired infrastructure. • 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. • 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 of the ADSP protected infrastructure. • 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.
Classification	Displays how the Unknown Device is classified.

Bluetooth Devices

Click the drop-down menu under **Show** and click on **Bluetooth**. ADSP displays a list of all Bluetooth devices seen in your wireless network.



The list of Bluetooth devices are displayed in a tabular format using a combination of the following columns:

Column	Description
Device	Contains the MAC address. Click on the down-arrow to display the MAC address, appliance, when last seen, and signal strength.
Type	Displays the type of Bluetooth device (such as ‘computer’.)
Severity	Displays the threat level to your network. Green indicates a sanctioned device. Red indicates an unsanctioned device. (default header)
Last Seen	Displays the last time the Bluetooth device was seen on the network. (default header)
Scope	Displays the area where the Bluetooth device is located within the network scope. (default header)
Floor	Displays the floor where the Bluetooth device is located. (default header)
Signal Strength	Displays the signal strength of the Bluetooth device in dBm. (default header)

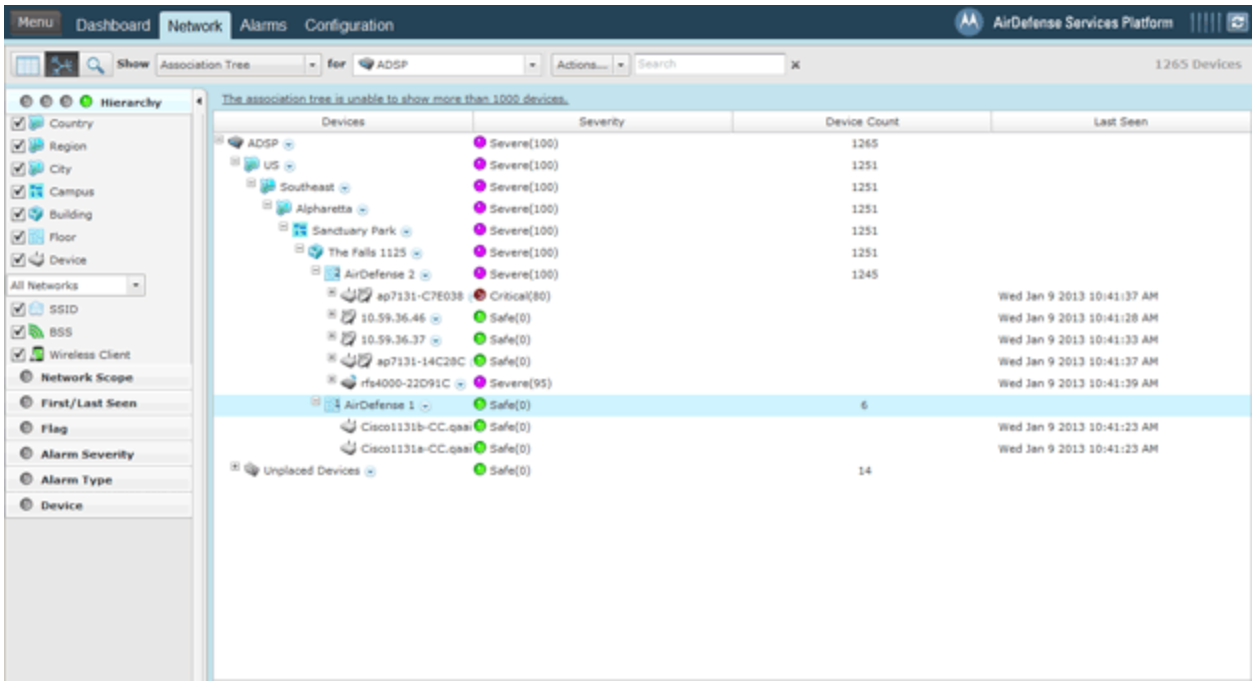
Menu Network Support

NOTE Live View is not supported on Menu Networks.

Menu Networks only display virtual MAC addresses in the Network tab. To display the true MAC addresses, contact Customer Support and have them enable Menu Network support on your appliance. When enabled, the true MAC addresses are displayed in the **Network** tab.

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.



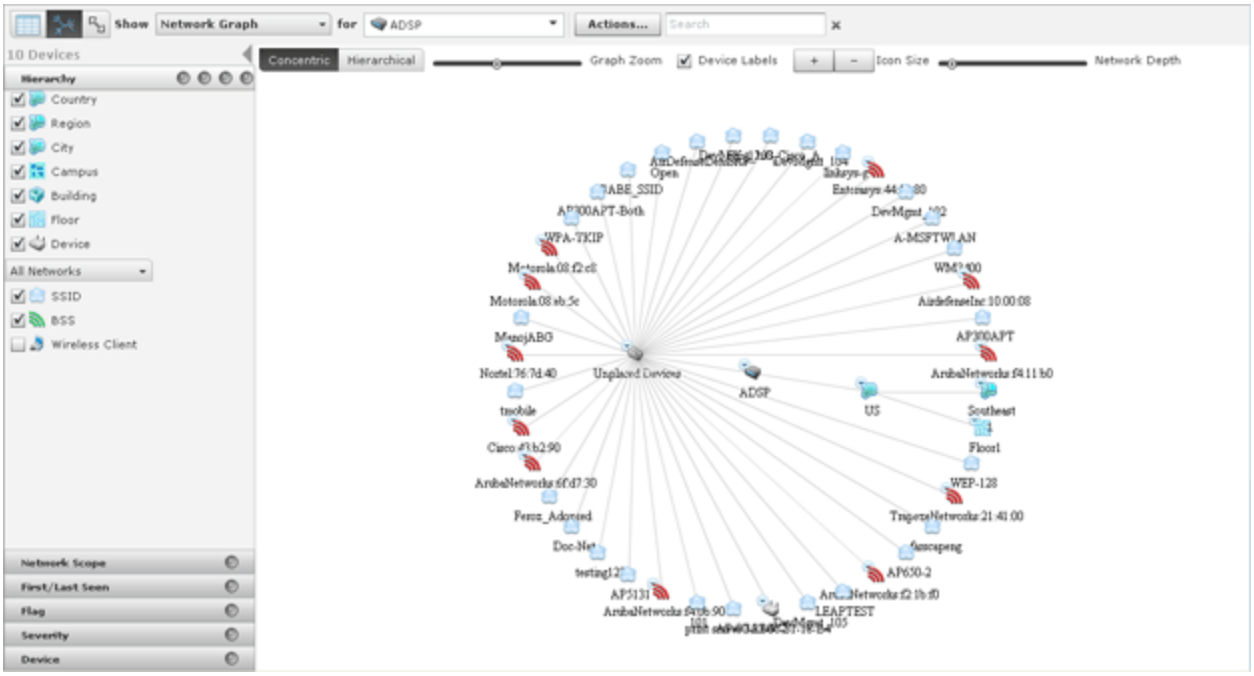
Click the Expand– ⊞ button to open a branch of the tree. Click the Collapse– ⊟ button to close a branch of the tree. The table columns for the Association Tree are:

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.

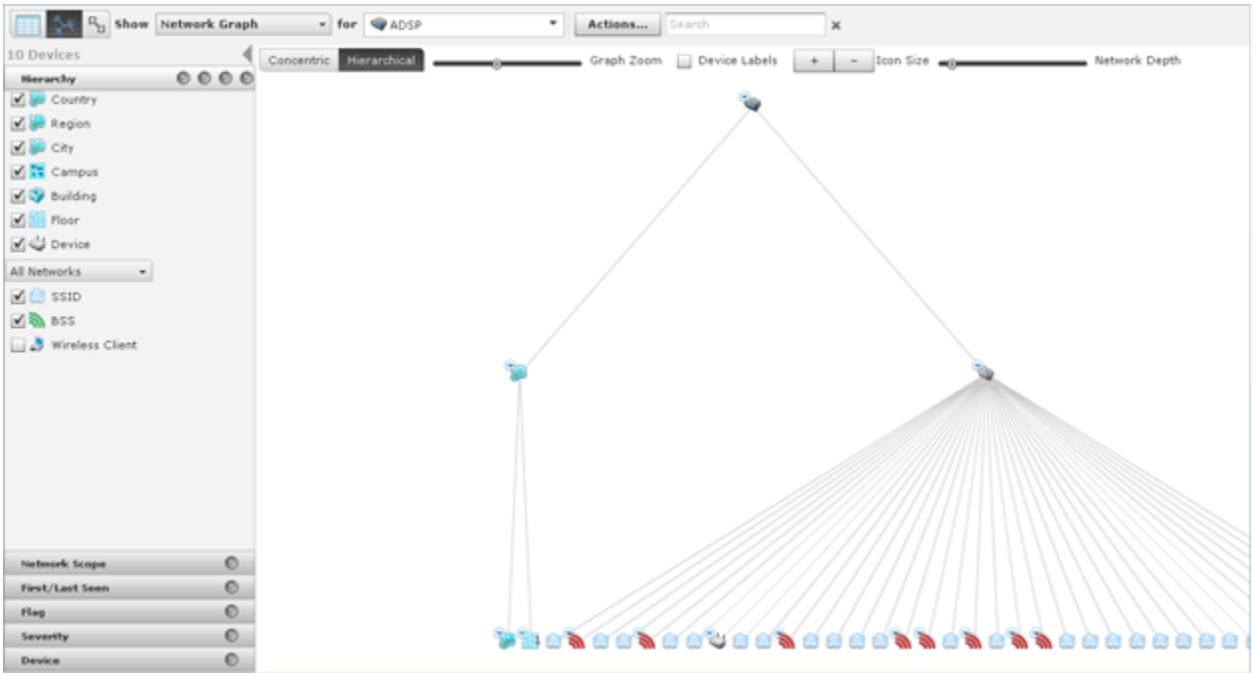
Network Graph

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.



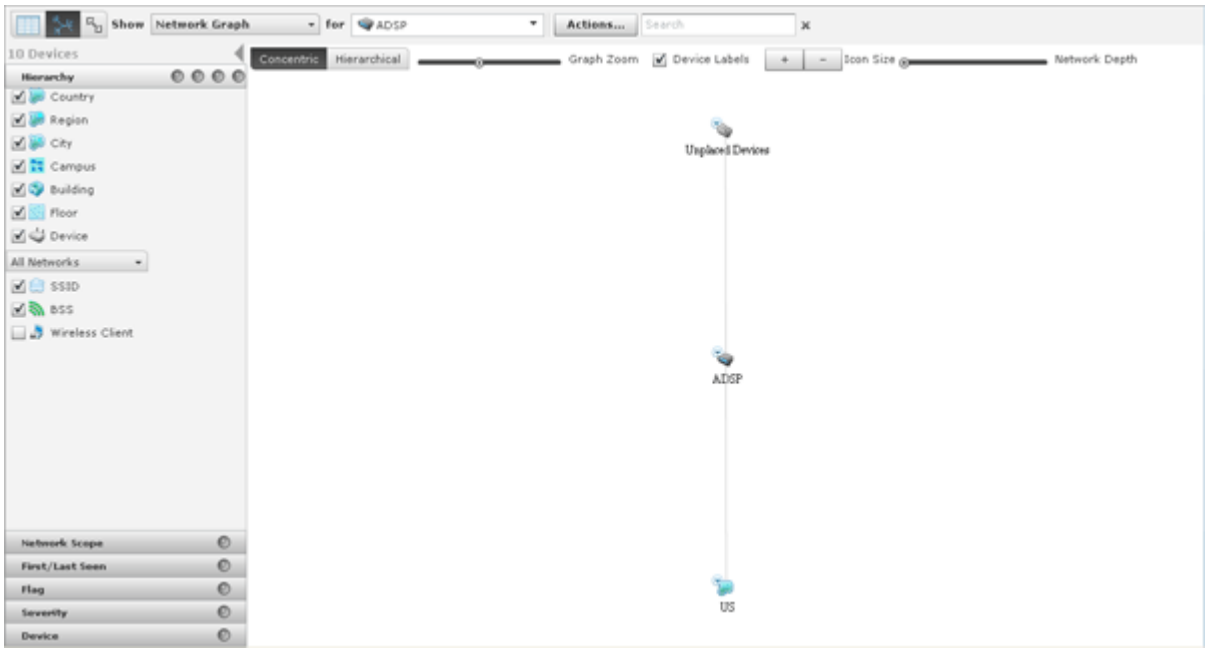
To switch to the Hierarchical view, click the **Hierarchical** button.



Click **Concentric** to return to the Concentric view. You can manipulate the graph by using:

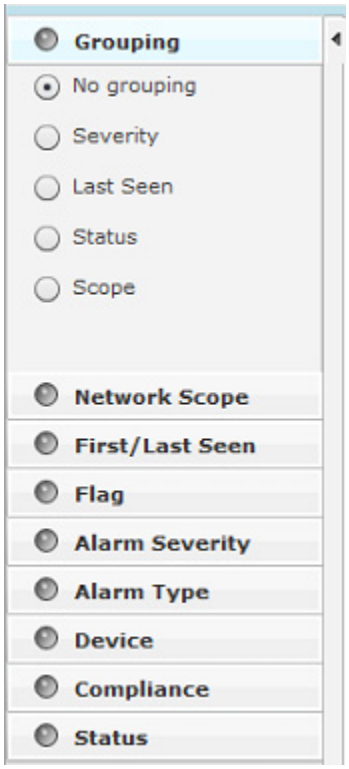
- **Graph Zoom** to zoom the graph in and out.
- **Device Labels** to remove or display the device labels.
- **Icon Size** to increase or decrease the size of the icons.

- **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.



The different filters are:

- **Grouping**—you can view devices by grouping them using similar criteria.
- **Network Scope**—you can view devices according to where they are in the network tree.
- **First/Last Seen Filter**—filters devices according to when they where first seen and/or last seen on your network.
- **Flag**—you can optionally view all flagged devices.
- **Alarm Severity**—you can view devices by alarm criticality.
- **Alarm Type**—filters devices by alarm type.
- **Device**—filters devices by model, manufacturer, and/or capabilities.
- **Compliance**—displays devices according to state of compliance with network policies.
- **Status**—displays devices according to their uptime/offline status.
- **Signal Strength**—filters devices within a specific signal strength range.
- **Security-Sensed Filter**—displays 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.

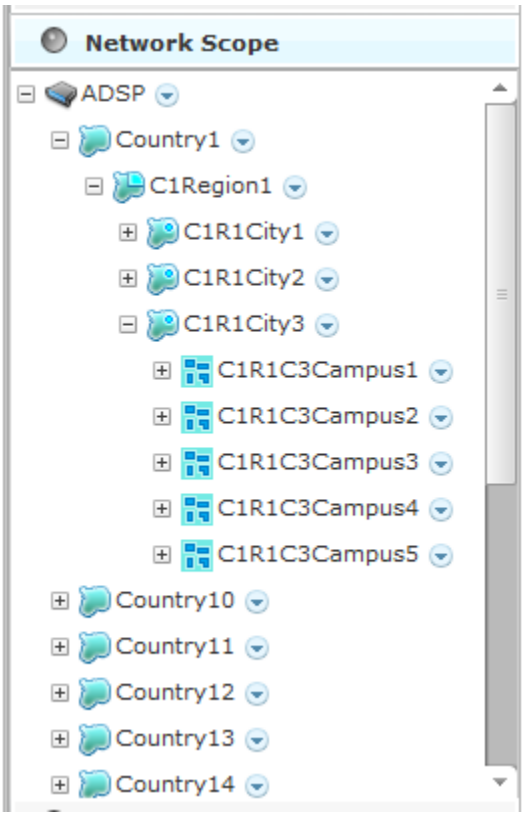
- **Status**—Groups devices based on their online/offline status. This view is accessible when displaying Network Devices.

- **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.

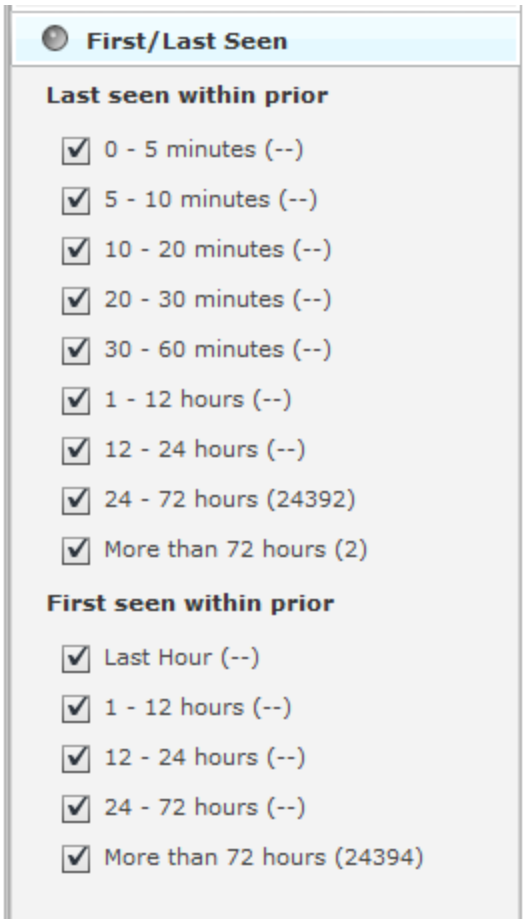
Network Scope Filter

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 where first seen and/or last seen on your network.



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:

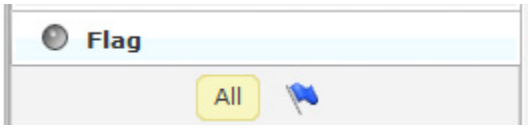
- Any time period
- 1 - 12 hours

- 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

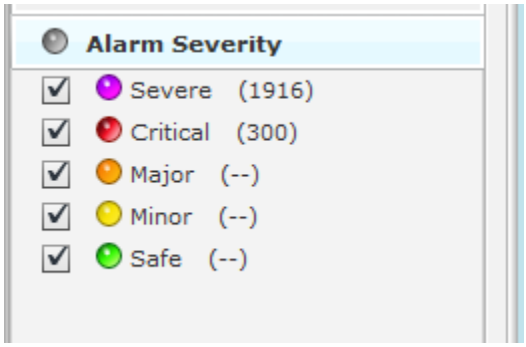
The **Flag** filter gives you the option of viewing all devices or only flagged devices.



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.



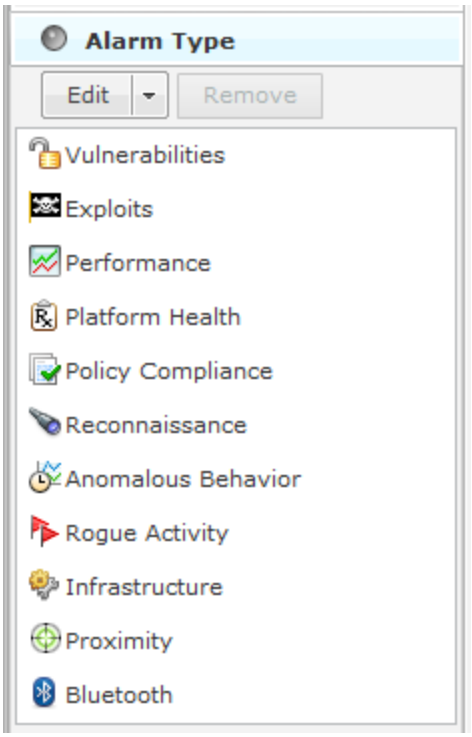
The severities are:

- 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

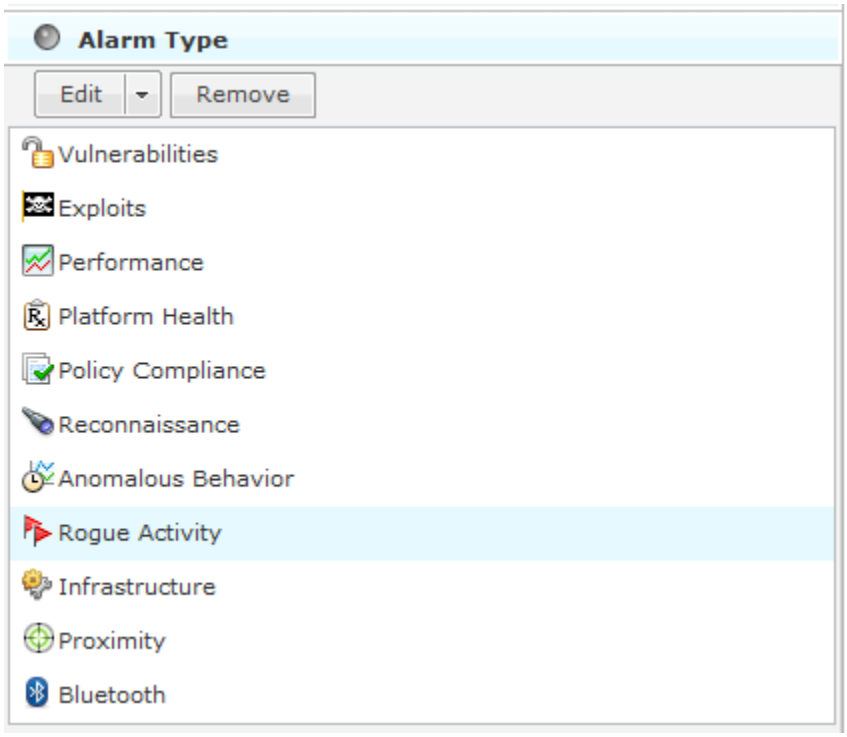
The **Alarm Type** filter allows you to view devices by alarm type. Devices are grouped together according to their alarm threat to your network.



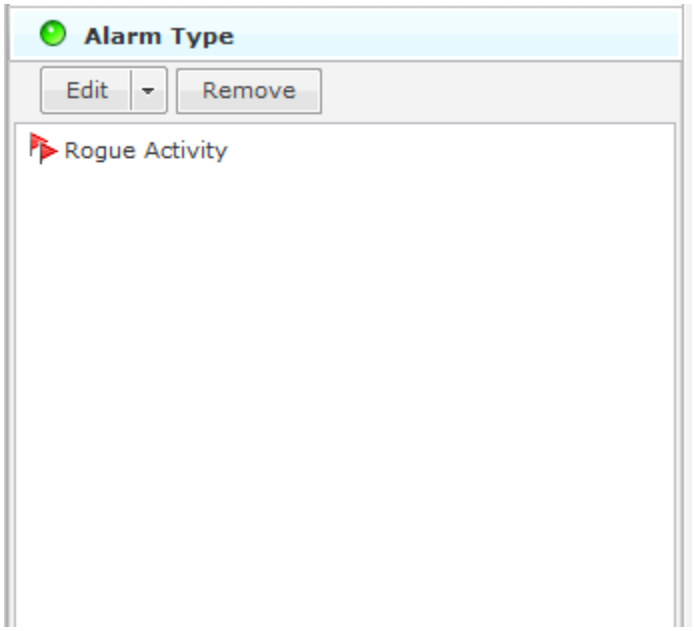
You have the option of displaying all alarm types or filtering alarms by a specific type. The different alarm types are:

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

Click the **Edit** button to select the alarm types that you want to display.



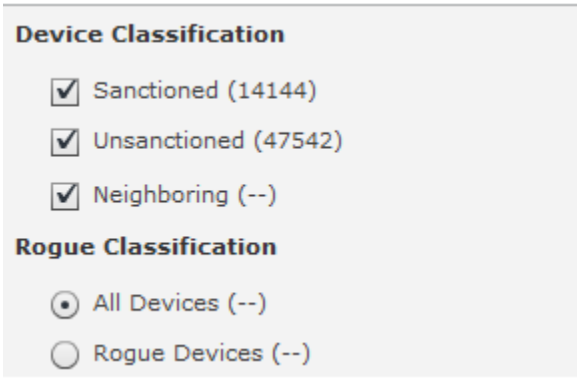
Click **Edit**, select the alarm type(s), and then click **OK**. The following graphic shows that you only want to display rogue alarms.



To remove an alarm type, select (highlight) the alarm type and click **Remove**.

Classification Filter

The **Classification** filter is used to filter devices by their device classification.



Devices are displayed by the following classifications:

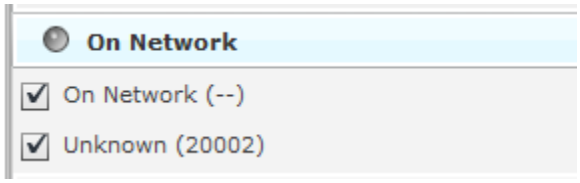
- Sanctioned—Display sanctioned devices.
- Unsanctioned—Display unsanctioned devices.
- Neighboring—Display neighboring devices.

Select the checkbox(es) for the classification(s) that you want to display. You can also display devices by rogue classification. You options are to display all devices or to display only rogue devices. Select the appropriate radio button.

NOTE The Classification filter is not available when displaying Network Devices. It is available for BSS, Wireless Client and Unknown Devices.

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.

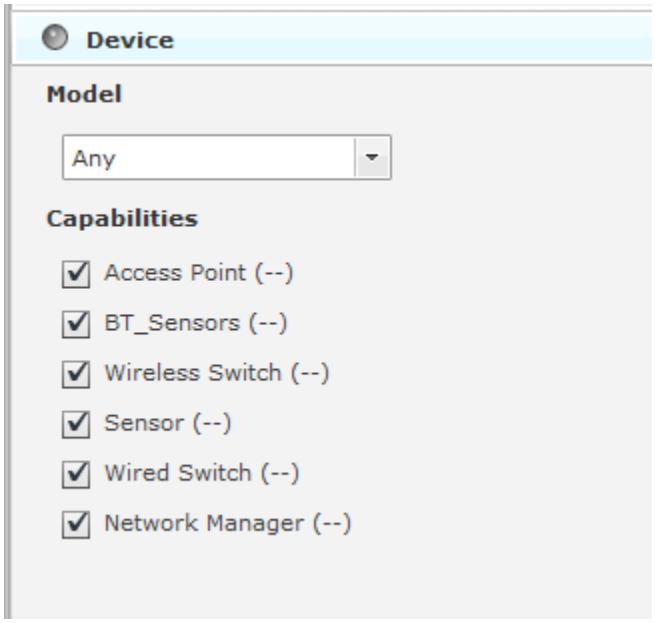
NOTE The On Network filter is only available when displaying network devices.

Device Filter

The **Device** filter is used to filter devices by model, manufacturer, and/or capabilities. The filter changes depending on the types of devices being displayed.

Network Devices

For network devices, you can filter devices based on the model type. Select a model from the Model drop-down menu.

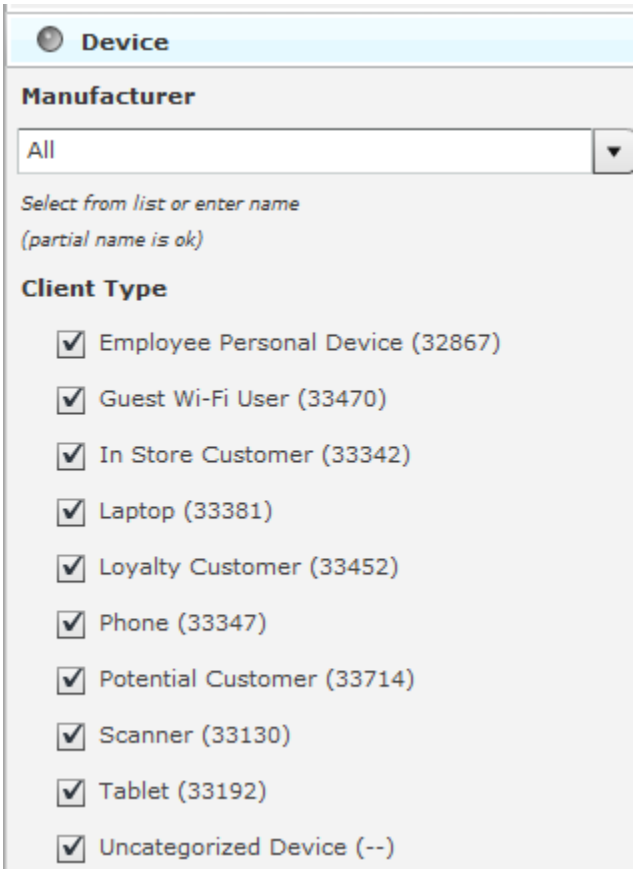


You can also filter network devices based on the capability of the device. When you select a capability, only devices with that capability are displayed. For network devices, you may select:

-
- BT_Sensors
- Wireless Switch
- Sensor
- Wired Switch
- Network Manager.

Wireless Clients

For wireless clients, you can filter devices based on the manufacturer. Select the manufacturer from the drop-down menu. You may also type in the manufacturer's name, including a partial name.

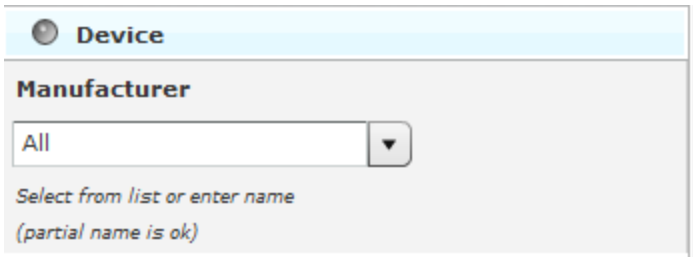


You can also filter Wireless Clients based on the client type. When you select a client type, only devices of that type are displayed. You may select from the following client types:

- Employee Personal Device
- Guest Wi-Fi User
- In-Store Customer
- Laptop
- Loyalty Customer
- Phone
- Potential Customer
- Scanner
- Tablet
- Uncategorized Device

BSSs and Unknown Devices

For BSSs and Unknown Devices, you can filter devices based on the manufacturer but not on client type or capabilities. Select the manufacturer from the drop-down menu. You may also type in the manufacturer's name, including a partial name.

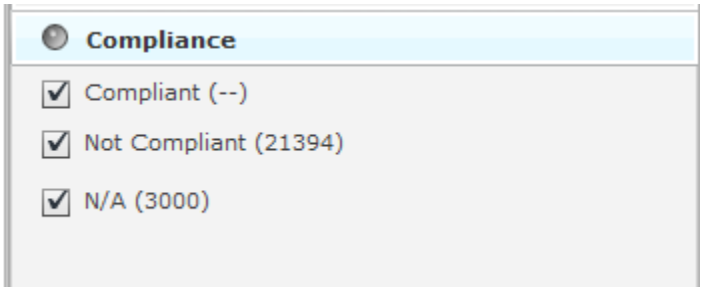


Bluetooth Devices

For Bluetooth devices there is no device filter.

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

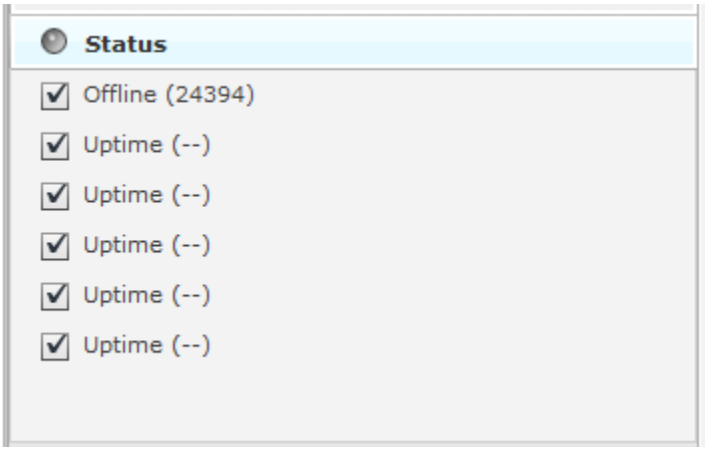


.Devices are displayed if you have their compliance state checked. The different states are:

- **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/off-line status. This filter is only available when displaying Network Devices.



You may select one or more of the following statuses:

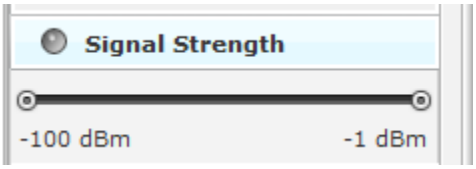
- **Offline**—Displays any offline devices.
- **Uptime (0 - 1 hours)**—Displays devices that have been online from 0 to 1 hour.

  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.

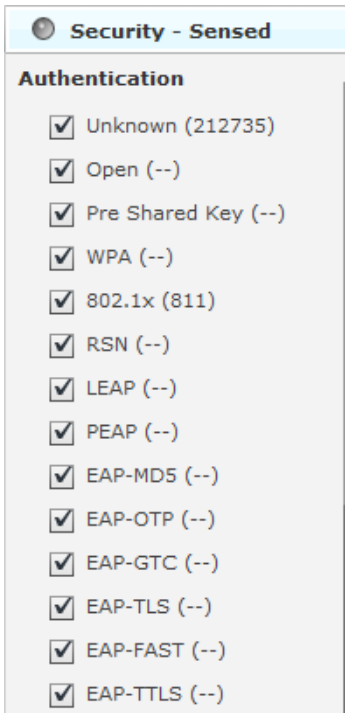


You may adjust the signal strength range by sliding the adjusters. The maximum range is -100 dBm to -1 dBm. Sliding the left slider adjusts the minimum signal strength. Sliding the right slider adjusts the maximum signal strength.

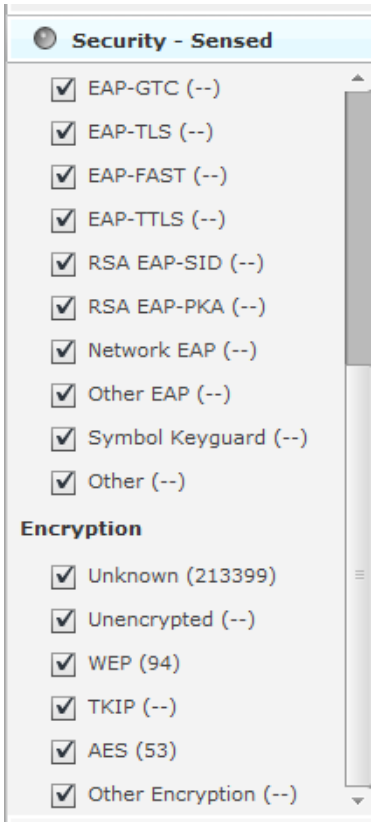
Security-Sensed Filter

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. The security-sensed filter has two fields: authentication and encryption.

Authentication



Encryption



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.

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:

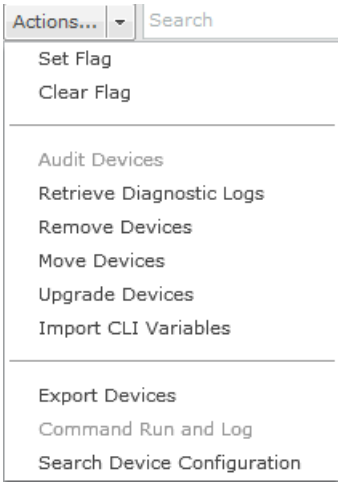
- Unencrypted
- WEP64

- WEP128
- AES(CCMP)
- TKIP
- Symbol Keyguard
- WPA2 PSK.

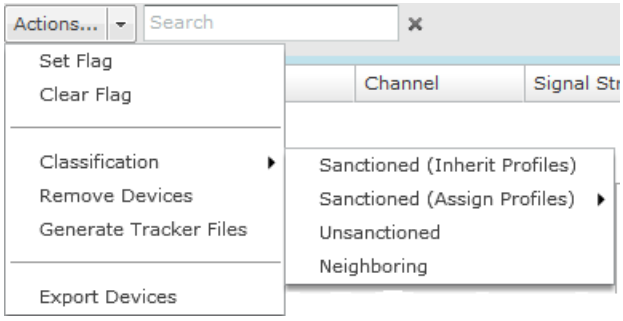
Actions Menu

The **Network** tab includes an **Actions** menu where you can execute an action. Depending on the device type, clicking the **Actions** button displays one of the following menus:

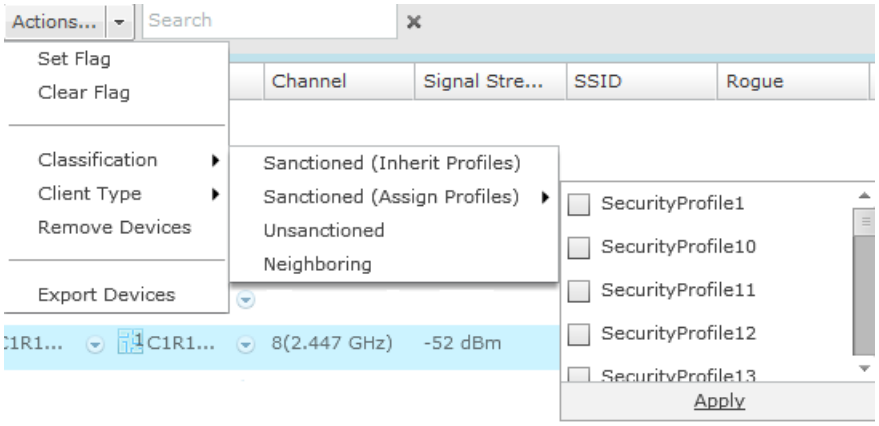
Network Device Actions

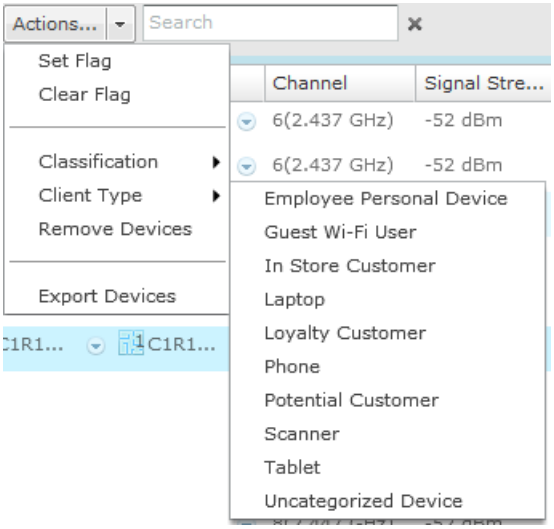


BSS Actions

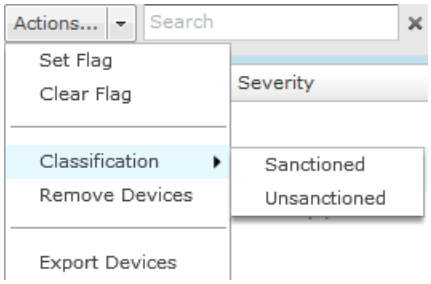


Wireless Client Actions

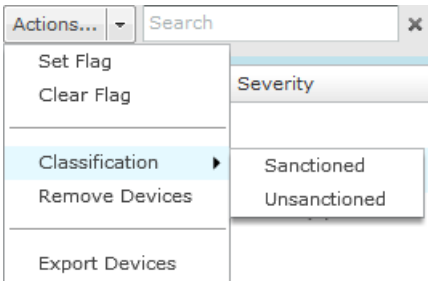




Unknown Devices Actions



Bluetooth Devices Actions



Actions Descriptions

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

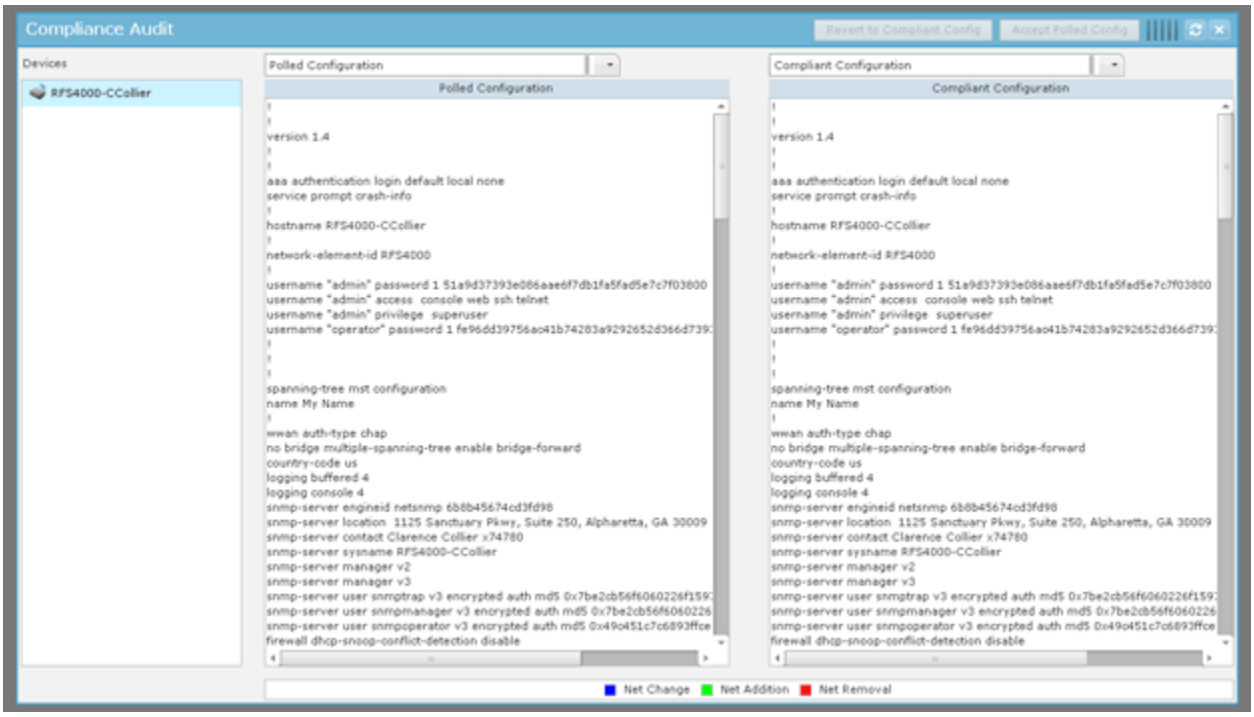
this case, no other input is required. Other actions will display a dialog that require more input. Descriptions of the actions are as follows:

Action	Description
Set Flag	Allows you to flag the selected device(s) to indicate attention is required.
Clear Flag	Allows you to remove a flag from the selected device(s).
Classification	Sanctioned (inherit) Classify the selected device(s) as a sanctioned device that inherits its traits from wherever its location in the network tree. Sanctioned (override) Classify the selected device(s) as a sanctioned device using traits that override the inherited traits. For example, a security profile can be applied to a BSS that overrides the inherited traits. Sanctioned Classify the selected device(s) as sanctioned (Unknown Devices only) Unsanctioned Classify the selected device(s) as unsanctioned. Neighboring Classify the selected device(s) as a neighboring device.
Client Type	Classifies a Wireless Client as one of the following types: • Employee Personal Device • Guest Wi-Fi User • In Store Customer • Laptop • Loyalty Customer • Phone • Potential Customer • Scanner • Tablet • Uncategorized Device
Audit Devices	Allows you to conduct a compliance audit on the selected device(s) (see *Audit Devices*.)
Retrieve Diagnostic Logs	Allows you to display the diagnostic logs for the selected device(s). If no logs are available, you will receive a message stating so (see *Retrieve Diagnostic Logs*.)
Remove Devices	Allows you to remove selected device(s) from monitoring (see *Remove Devices*.)
Move Devices	Allows you to place selected device(s) on a floor (see *Move Devices*.)
Upgrade Devices	Allows you to upgrade the firmware for the selected device(s) (see *Upgrade Devices*.)

Action	Description
Import CLI Variables	Allows you to import CLI variables at the device level (see *Import CLI Variables*.)
Export Devices	Allows you to export information about selected device(s) to a CSV file (see *Export Devices*.)
Command Run and Log	Allows you to execute CLI commands for selected device(s) and save results in a log file (see *Command Run and Log*.)
Search Device Configuration	Allows you to search for device configurations on the network.
Generate Tracker Files	Allows you to generate tracker files and save the files to a directory on your computer (see *Tracker Integration*.)

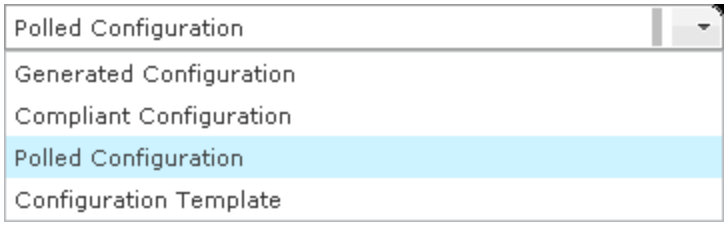
Audit Devices

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.



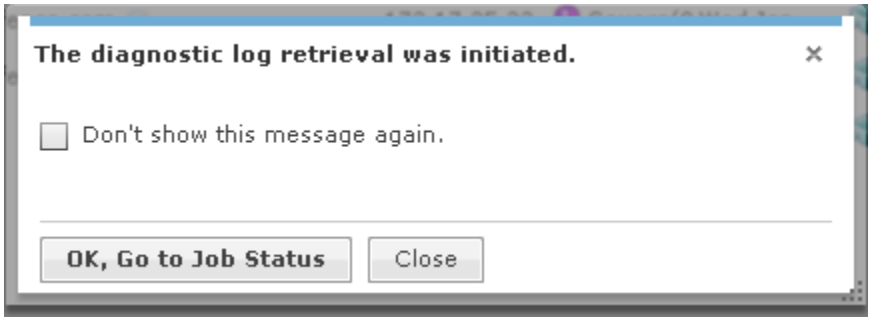
When you change a configuration type, the CLI commands for that type are displayed. If there are differences, they are highlighted.

Click **Revert to Compliant Config** to update the highlighted device with the CLI commands from **Compliant Configuration**. Click **Accept Polled Config** to accept the CLI commands from **Polled Configuration**.

Click **Close–x** button exit the compliance audit overlay.

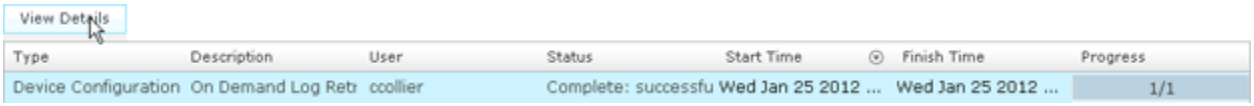
Retrieve Diagnostic Logs

To to retrieve the diagnostic logs for the selected device in one consolidated file, elect (highlight) a device and then click **Actions** > **Retrieve Diagnostic Logs**.

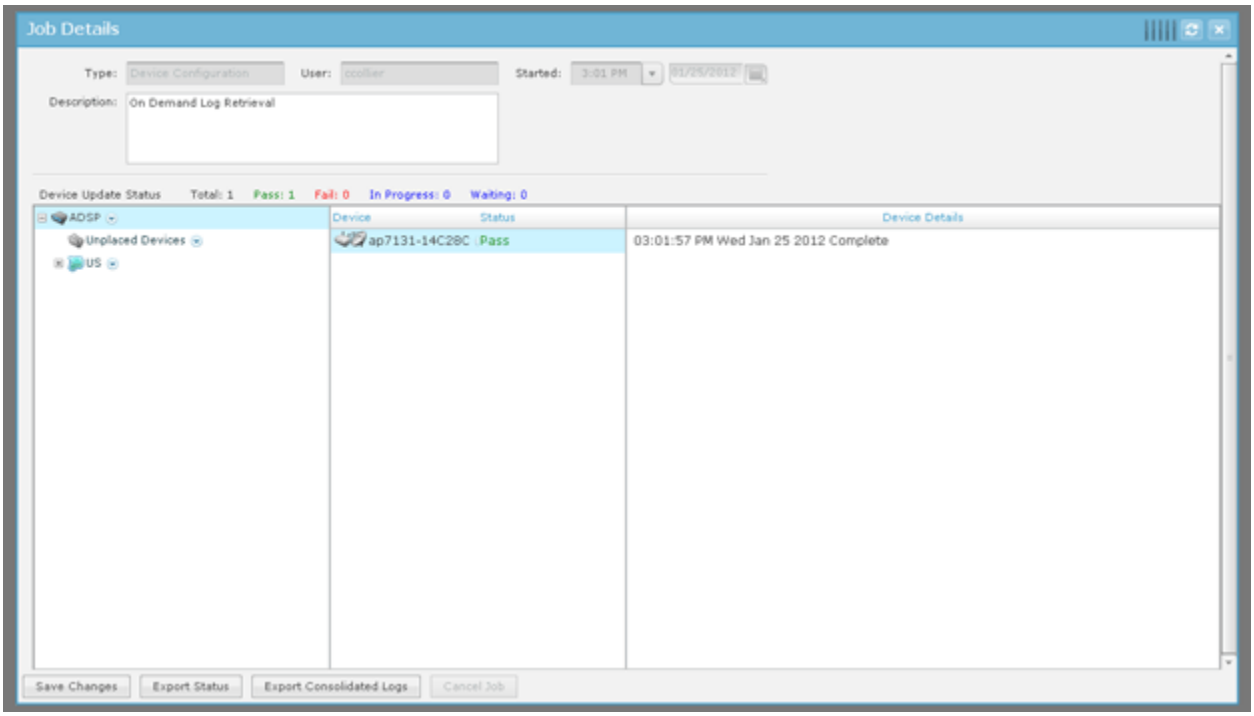


NOTE You can elect not to show this message again by selecting the checkbox.

At this point, ADSP starts retrieving the diagnostic logs. When you click **OK, Go to Job Status**, the Job Status is displayed.

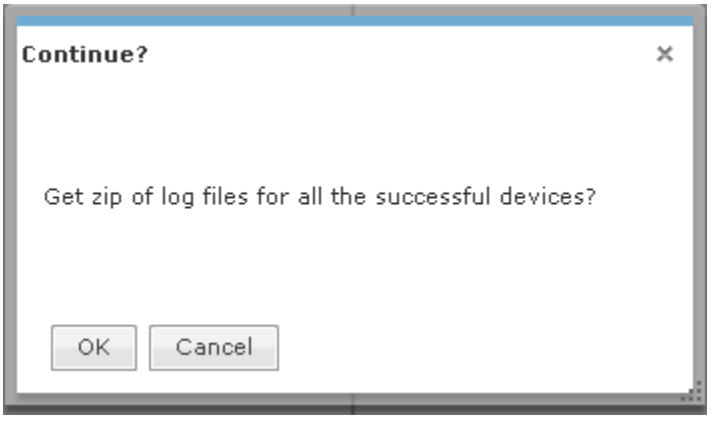


Select your job and then click **View Details** to display the job details.



To view your diagnostic logs, you will have to export them to your workstation by clicking **Export Consolidated Logs**.

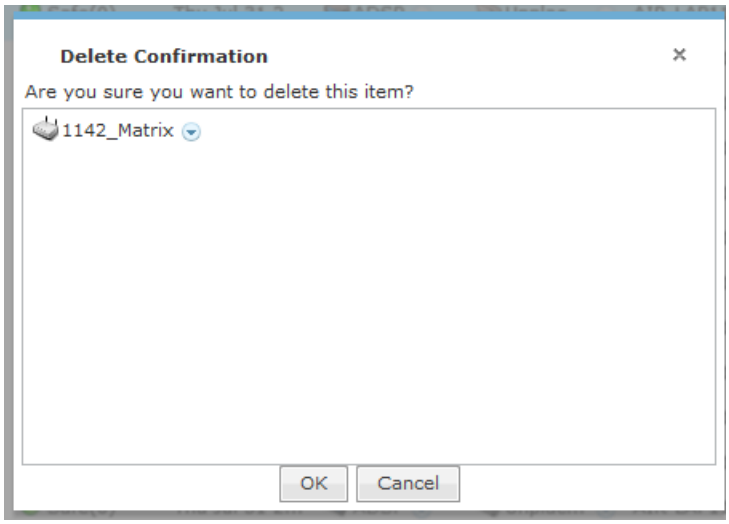
NOTE The **Export Consolidated Logs** button is inactive until the status changes to Pass and the diagnostic logs are ready to export.



Click **OK** to continue. Navigate to a location and click **Save**. The consolidated logs are saved in a ZIP file using the specified file name. You can now view the logs.

Remove Devices

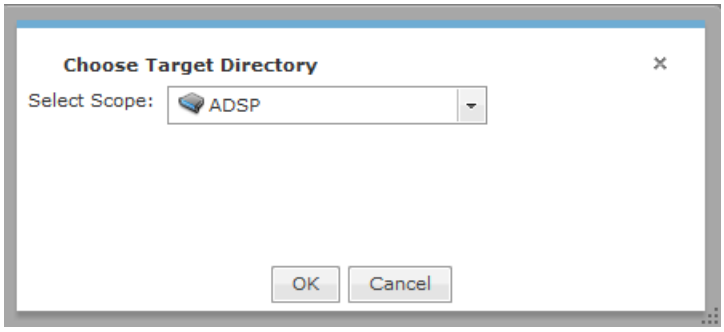
Click **Remove Devices** to remove a selected (highlighted) device. You are prompted to confirm removal.



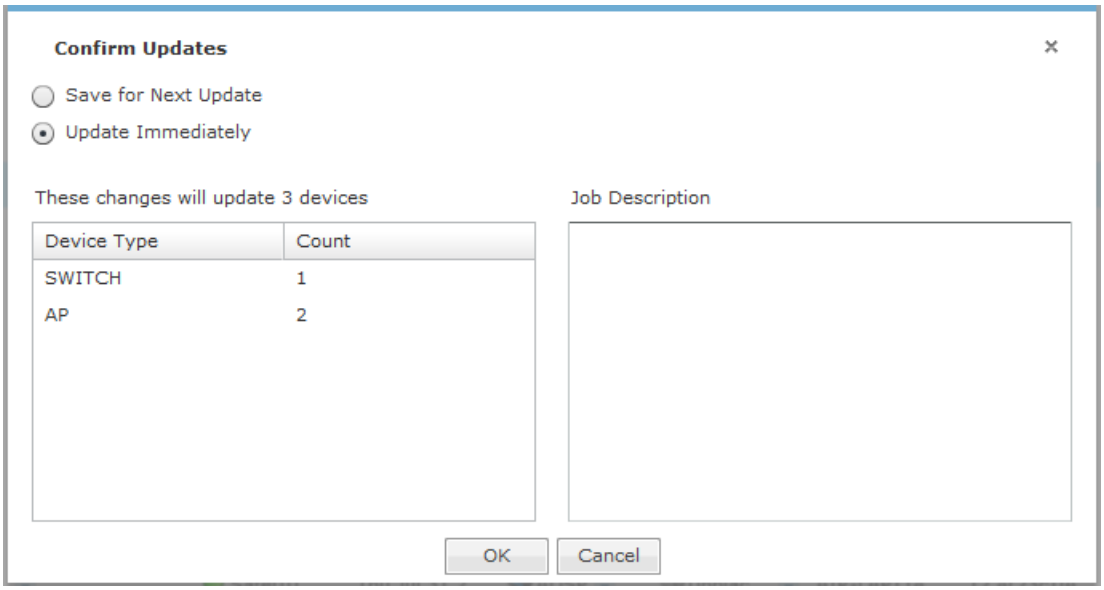
Click **OK** to remove the listed devices. Click **Cancel** to exit without removing the device(s).

Move Devices

Click **Move Devices** to move a selected (highlighted) device to a scope (floor) that you specify. When selected, you are prompted to select a scope.



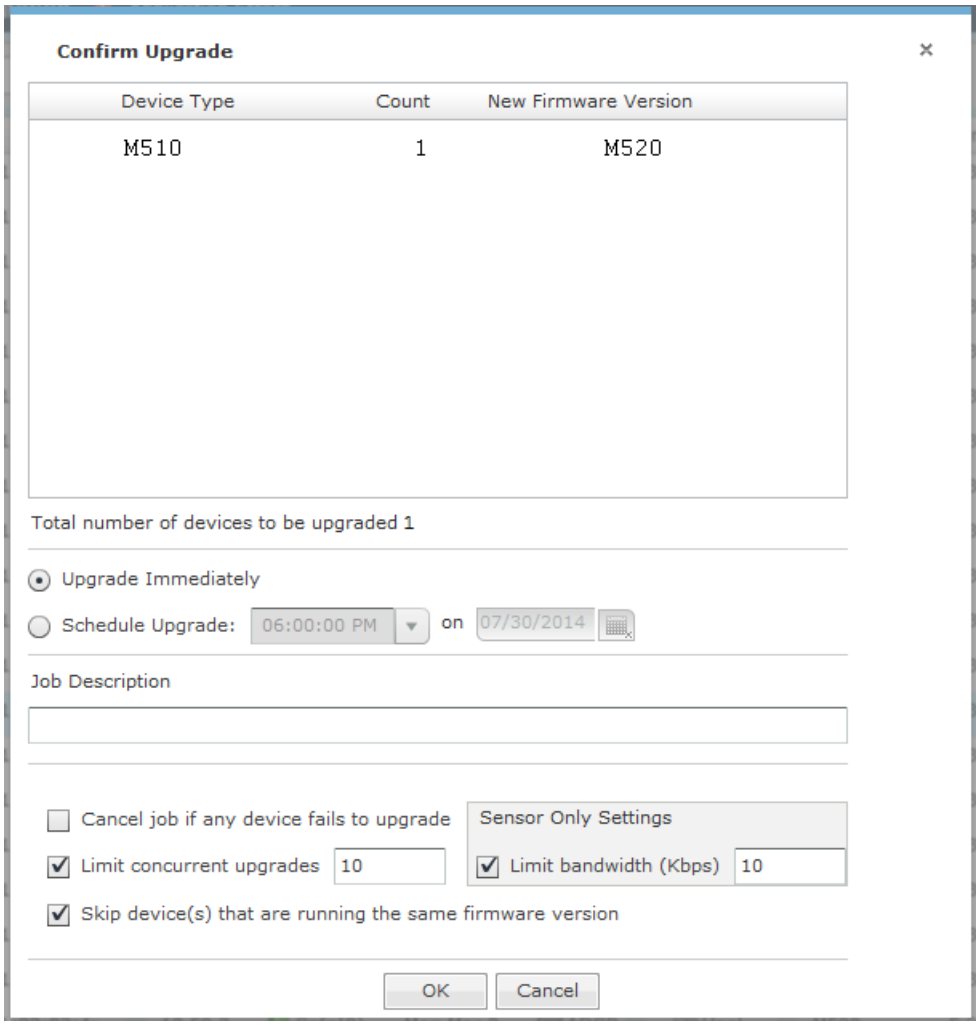
Click the drop-down menu to make your selection and then click **OK**. You are prompted to confirm your selection.



Click **OK** to move the device(s). Click **Cancel** to exit without moving the device(s).

Upgrade Devices

To upgrade the firmware for devices on your network, select (highlight) a device 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 ented 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.

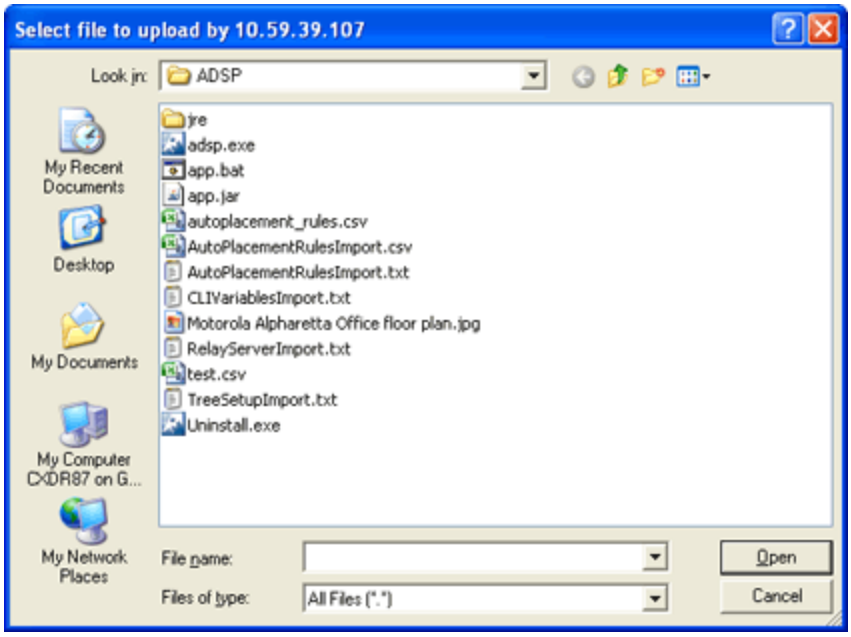
The first line is reserved for header information. If you do not want to include header information, make the first line a blank line.

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_Cube
44
```

NOTE deviceType can be blank if designating a folderPath.

When you select the **Import CLI Variables** action, 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:

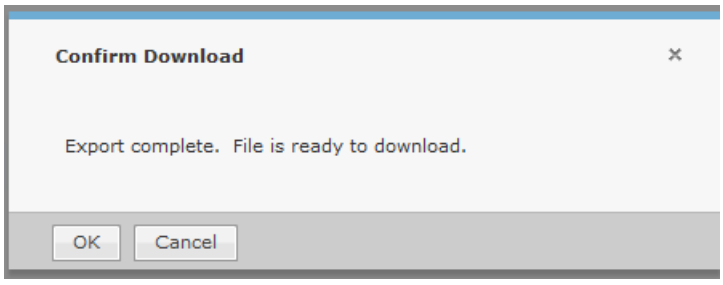
1 Click the device's drop-down menu button– .

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.

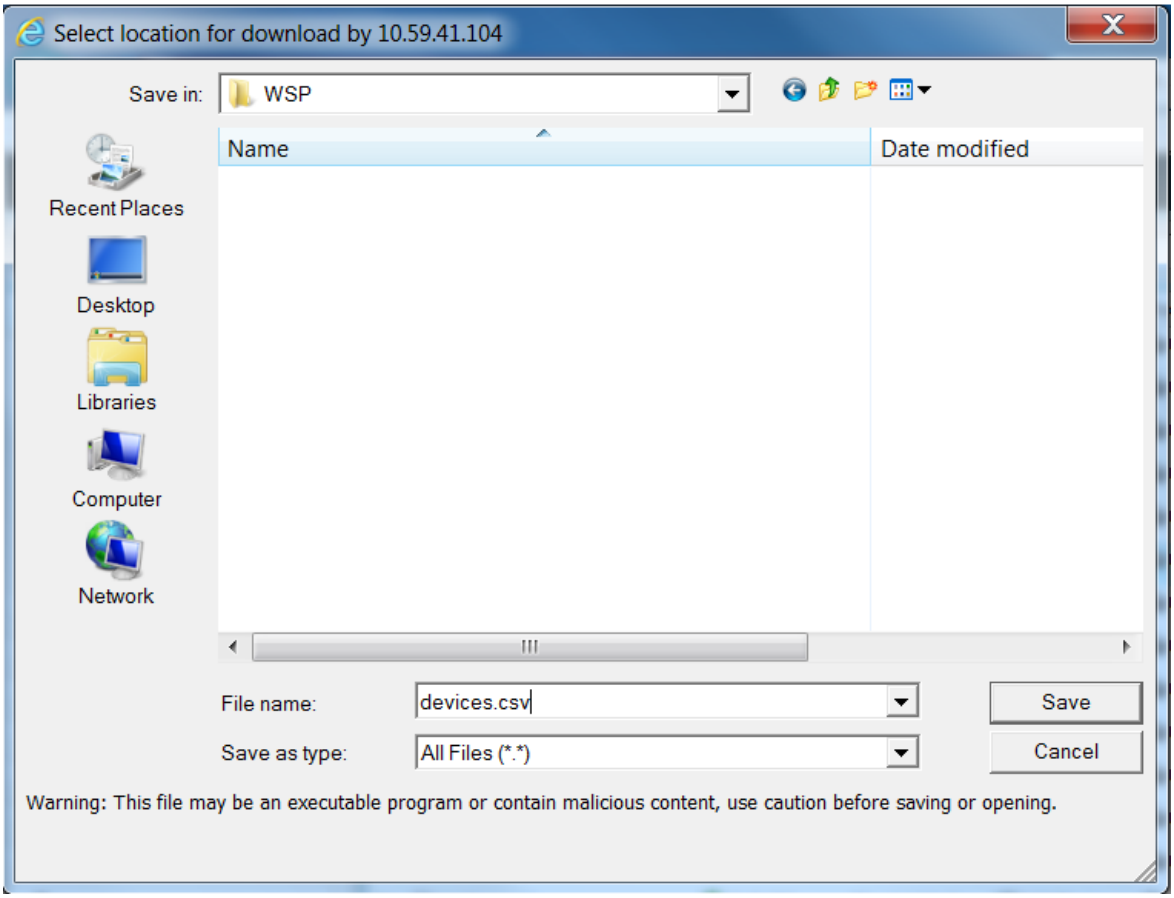
Export Devices

To export information about your devices to a CSV file on your local workstation, select a device and click **Export Devices** from the Actions menu. A pop-up box asked you to confirm the download.



Click **OK** to confirm or click **Cancel** to exit without exporting the device(s).

When you click **OK**, 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.

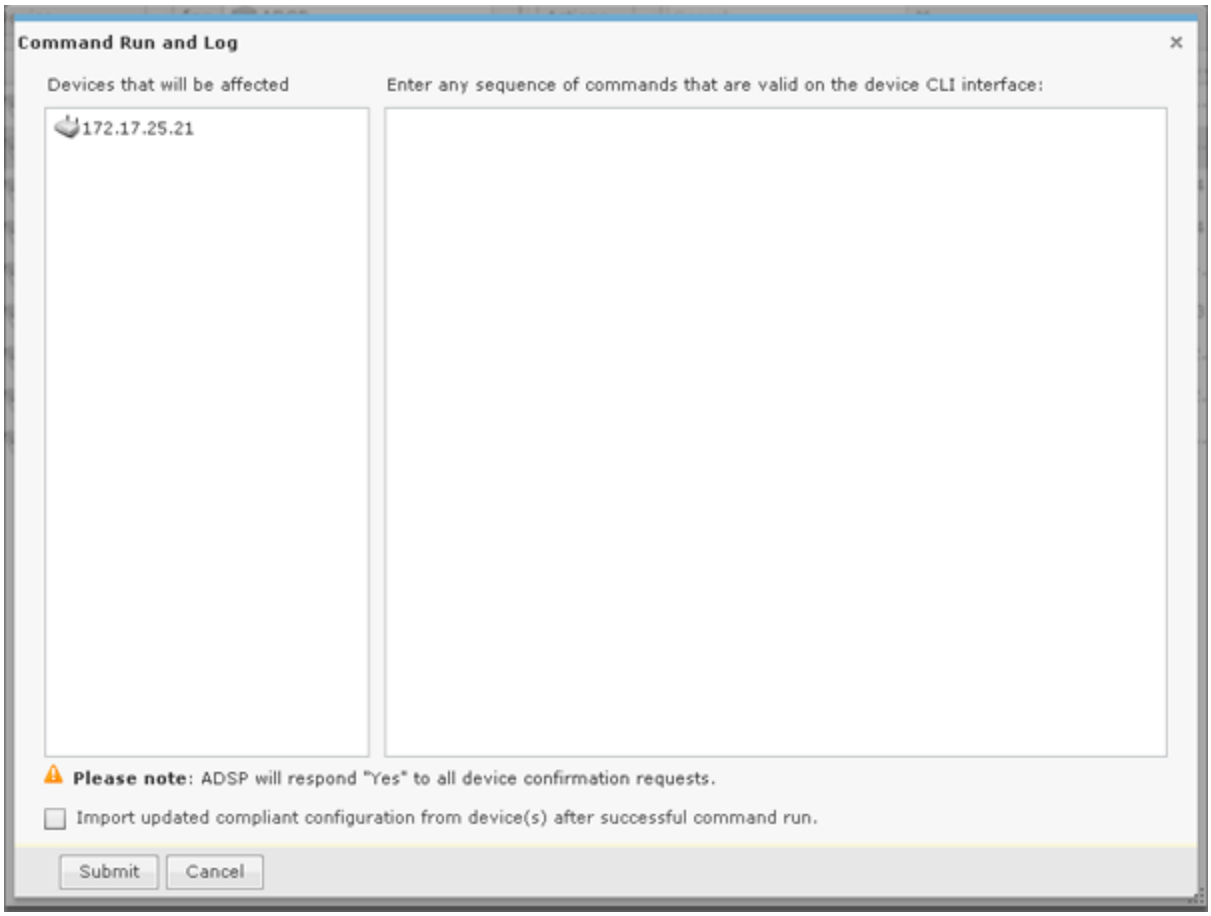
ADSP names the CSV file devices.csv by default. You can keep that name or change it.

Click **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

Use the **Command Run and Log** action 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, Communication Settings Profile must exist for the affected devices.



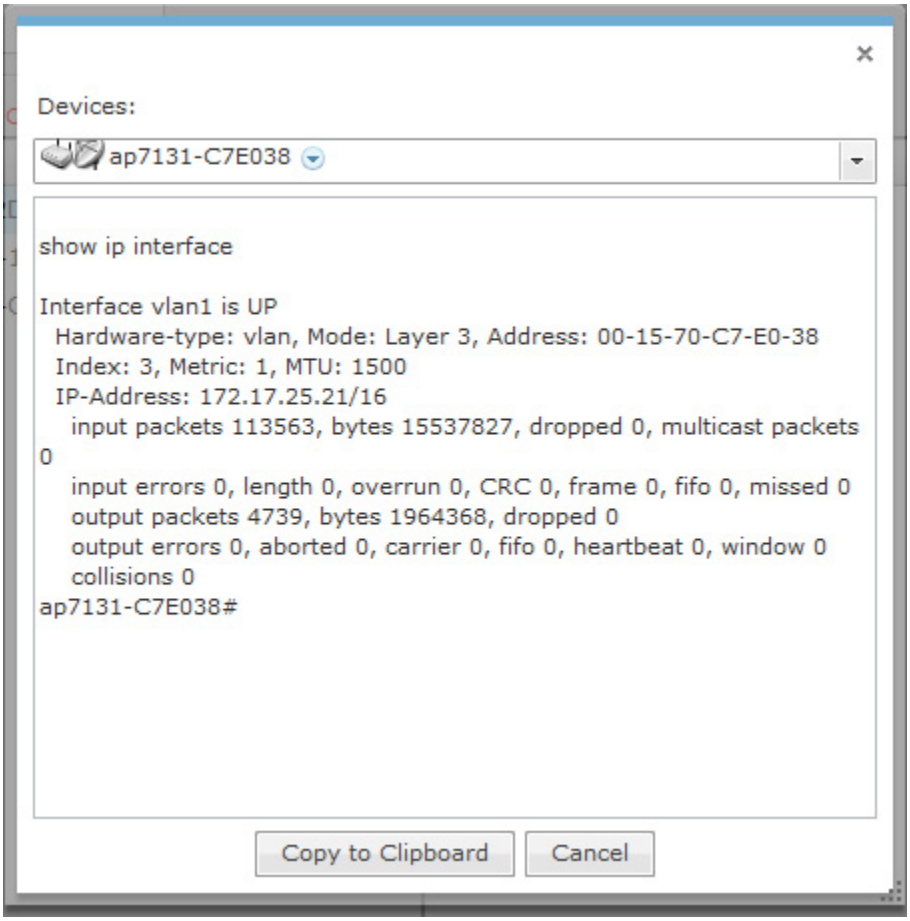
The commands are applied to all devices selected in the **Network** tab. Selected devices are listed in the **Devices that will be affected** field.

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.

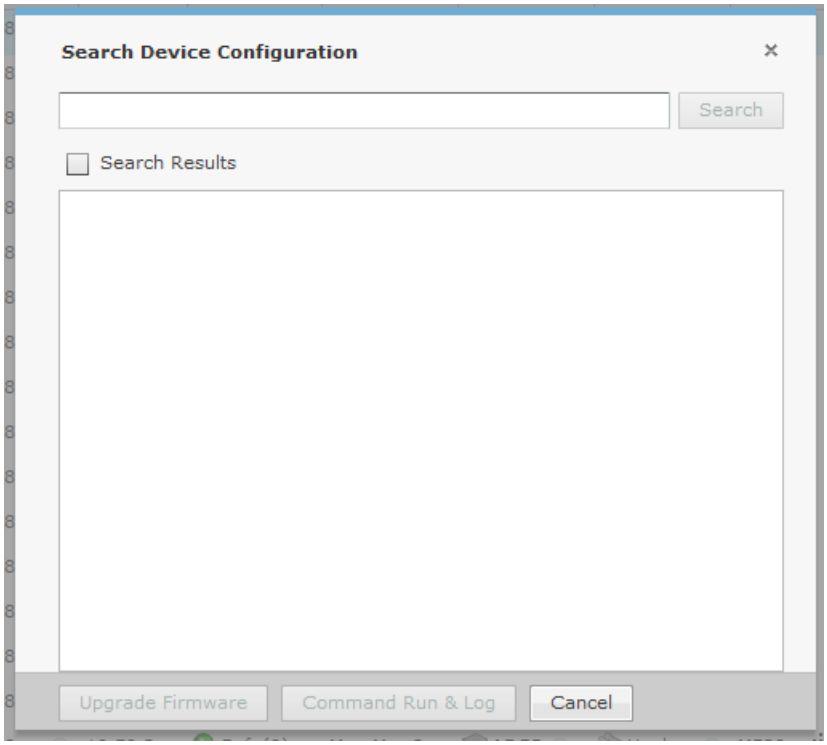


You can view the log of another device by selecting the device from **Devices** drop-down menu. Click **Copy to Clipboard** to copy the log contents to the clipboard. Click **Cancel** to exit the log.

Search Device Configuration

Use the **Search Device Configuration** action to search for devices by configuration. Depending on the number of infrastructure devices in network, the process can take some time. Follow these steps to search for device configurations:

1. Select Network Device from the Show menu.
2. Highlight the desired device(s).
3. From the **Actions** menu, select **Search Device Configuration**.



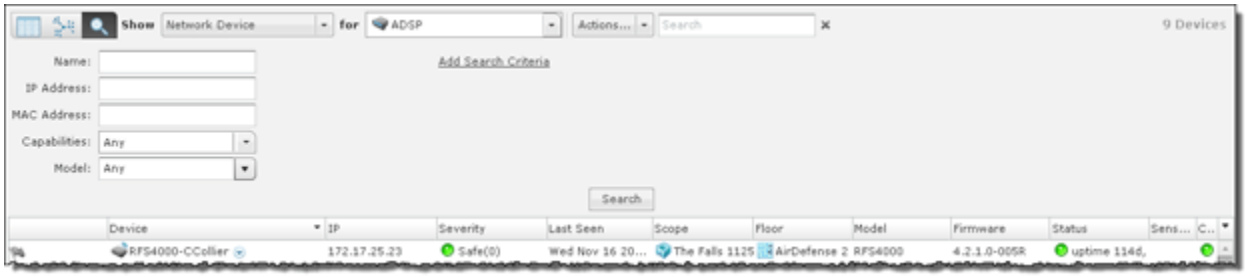
4 Enter the name of the device configuration you are searching for.

5 Check **Search Results** to display the search results.

6 When the devices are found, click **Upgrade Firmware** to upgrade; **Command Run & Log** to run the command log; and **Cancel** to exit without saving.

Advanced Search

The **Network** tab has an advanced search feature that allows you to supply additional criteria to the basic search. Click the **Advance Search** icon–  to access the advanced search feature.

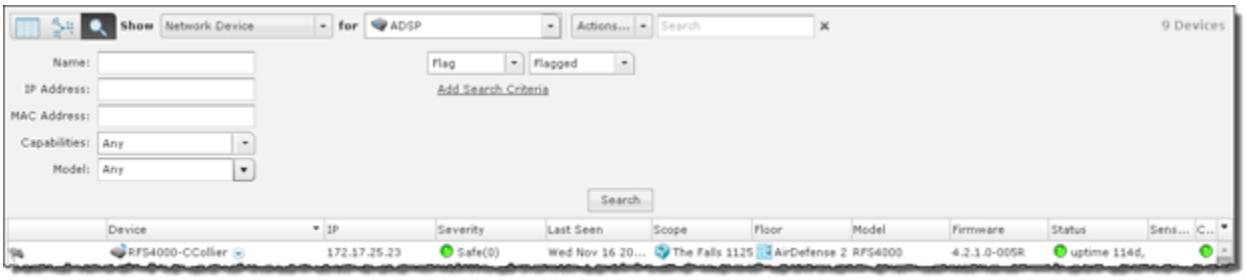


With the advanced search feature, you can supply additional information such as:

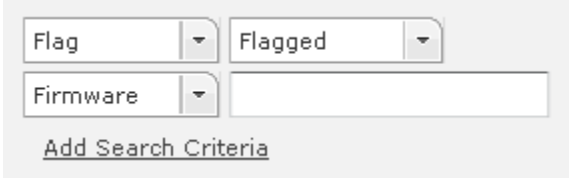
- The name of the device
- The IP address of the device
- The MAC address of the device

- The capabilities of the device (Any, , 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 ✖ 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 sanction, 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.

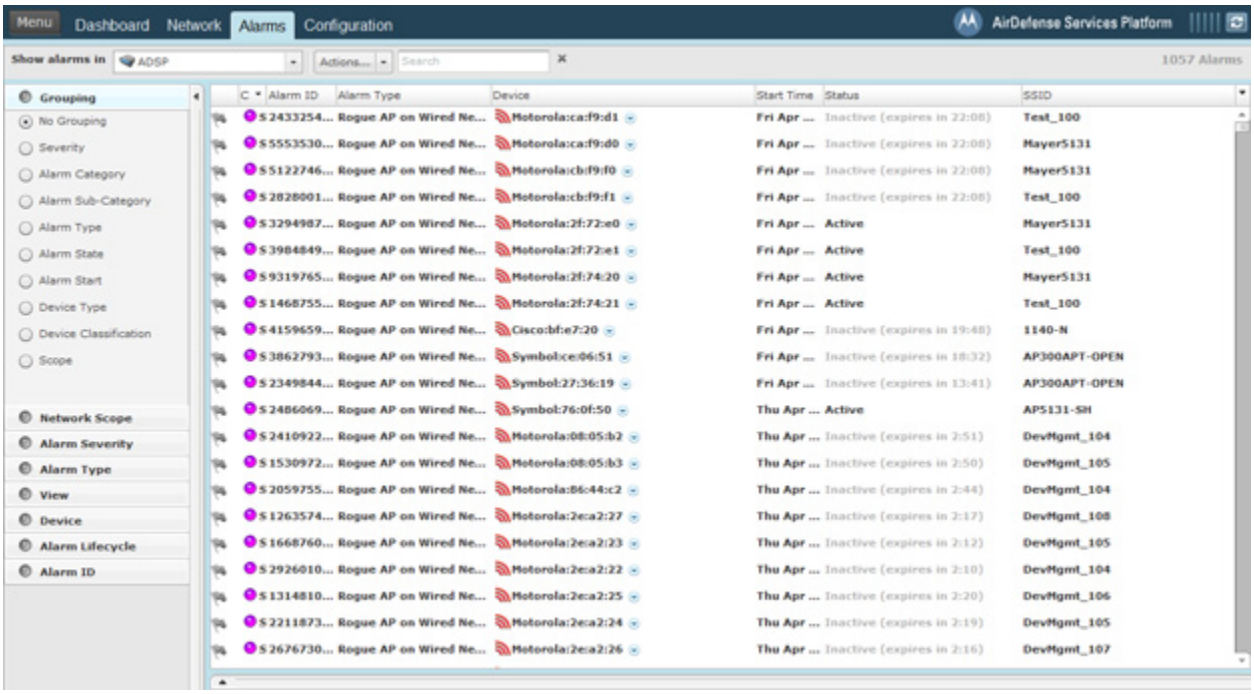
Once you have entered or selected your search criteria, click **Search** to display devices matching your search criteria.

CHAPTER 6 ALARMS

Alarms Tab

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.



The alarms listed in the table are determined by the network level and the filters you have selected. Select the network level in **Show alarms** in the drop-down menu. Select filters using the instructions described in the *Alarm Filters* section.

You can hide (uncheck) or view (check) columns by clicking the drop-down button– ▪ located to the right of the last column.

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–  .

ADSP Alarm Model

Suppressed Alarm Repetition

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.

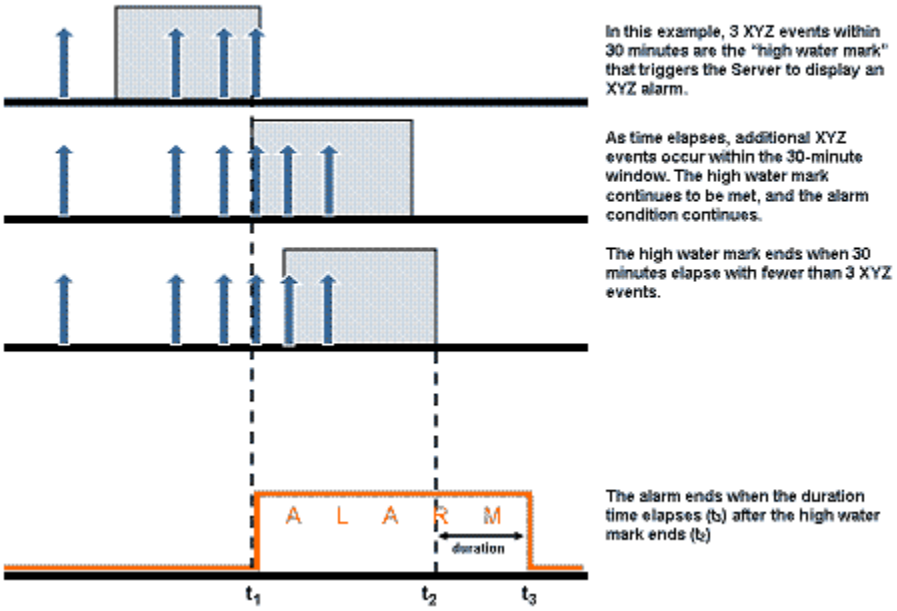
How an Alarm is Generated

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

The AirDefense wireless security research team maintains algorithms for correlating observed security events, to identify when a predefined 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.

Example: Generated Alarm

“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.



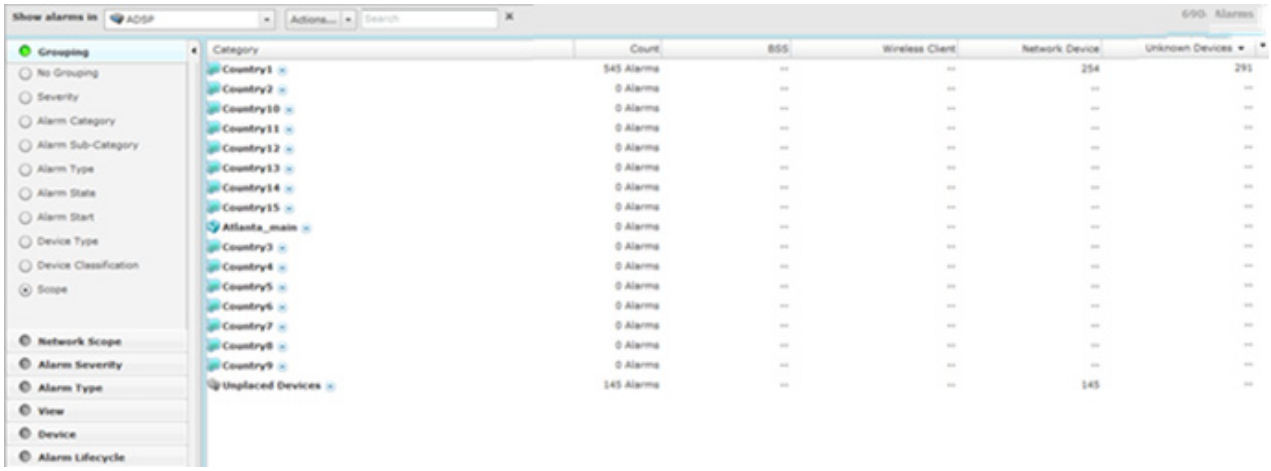
Duration of Alarm

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 AirDefense has determined default duration times correlated to the expected life-cycle of each specific event. When the duration time ends, the alarm becomes inactive. You can use the forensic analysis to view historical alarms.

Capabilities with a Central Management License

A Central Management license allows you to display alarms generated on any managed appliance in the Alarms tab. In the example below, the grouping selected is Scope, and the level is County1. The

alarm count shows as 545 alarms; 254 alarms on network devices; and 291 alarms on unknown devices. The total alarms is displayed in the upper right corner and shows 690 alarms.



If displaying alarms on an appliance level or a network level, only the alarms generated by that appliance or network level are shown.

Alarm Table

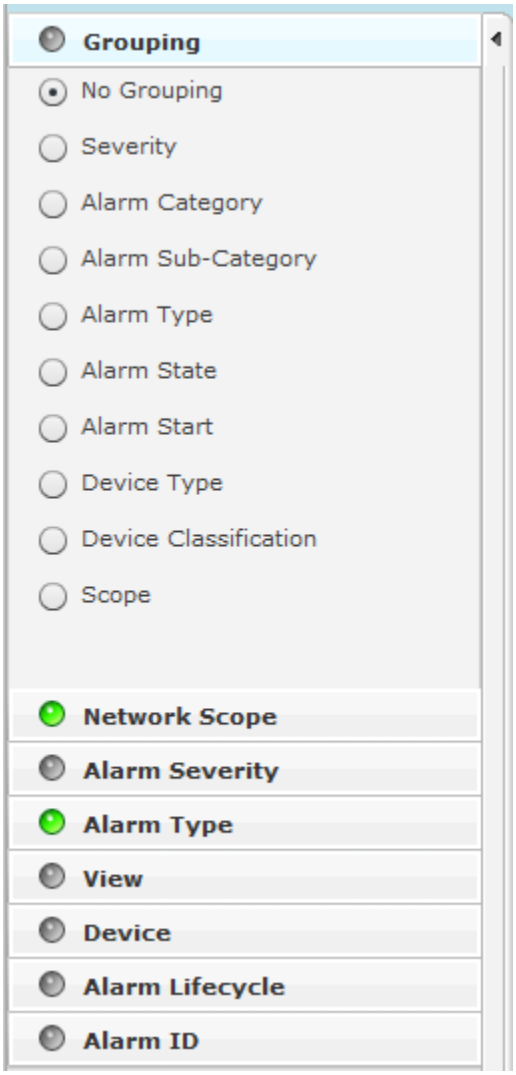
The alarm table is customizable and includes the following information (columns):

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

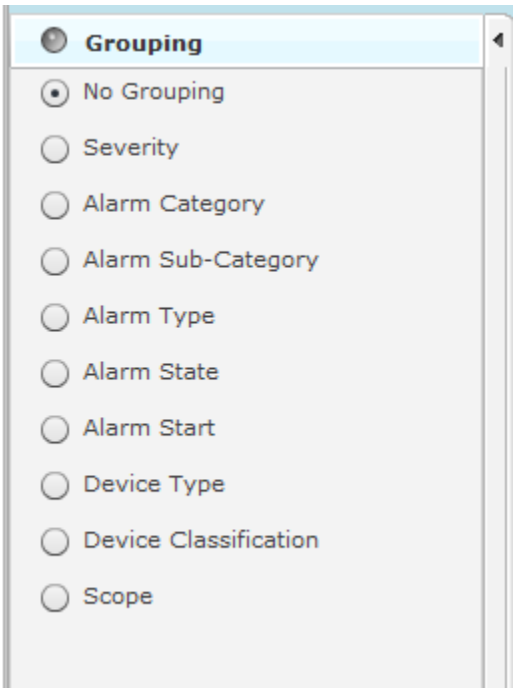
The different filters are:

- 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—filters alarms over the life cycle of an alarm.
- 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.

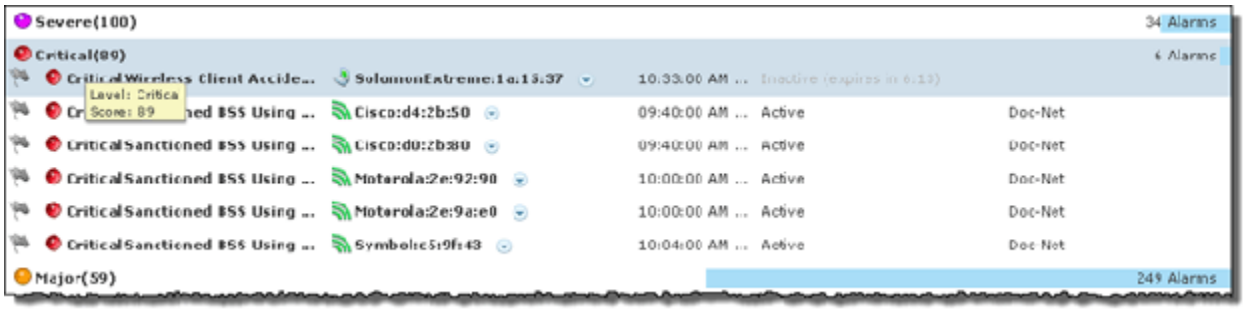
- Alarm Start—Groups alarms by when they started.

- Device Type—Groups alarms by the device type.

- Device Classification—Groups alarms based on the device classification.

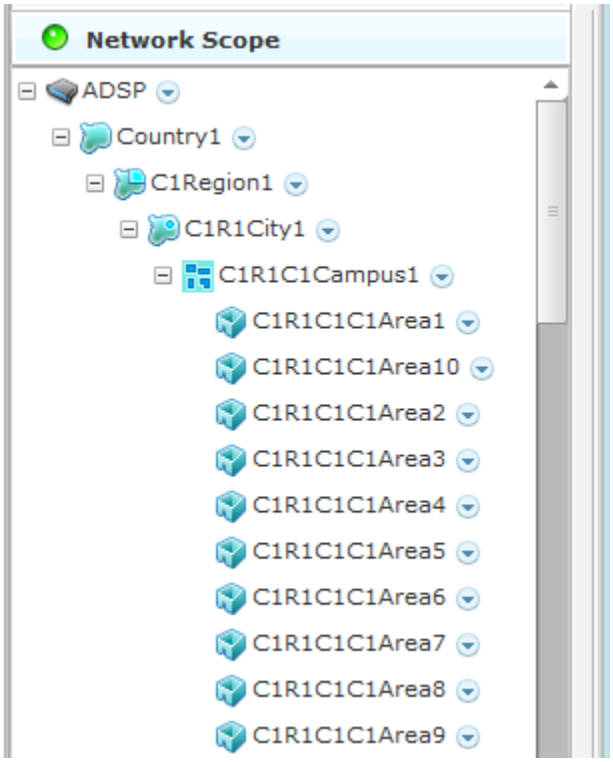
- Scope—Groups alarms based on where they are in the network. The highest network levels under the appliance level are displayed as the group.

Clicking on a group will display the individual alarms in that group.



Network Scope Filter

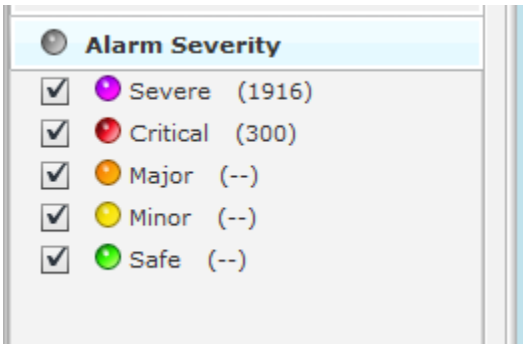
The **Network Scope** filter is used to view alarms according to where they are in the network tree. By selecting a network level, you limit the displayed alarms to only the ones under that particular network level.



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.



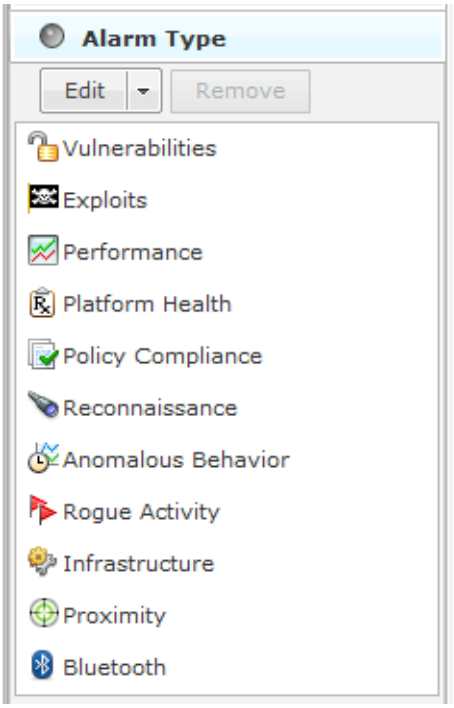
The severities are:

- 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

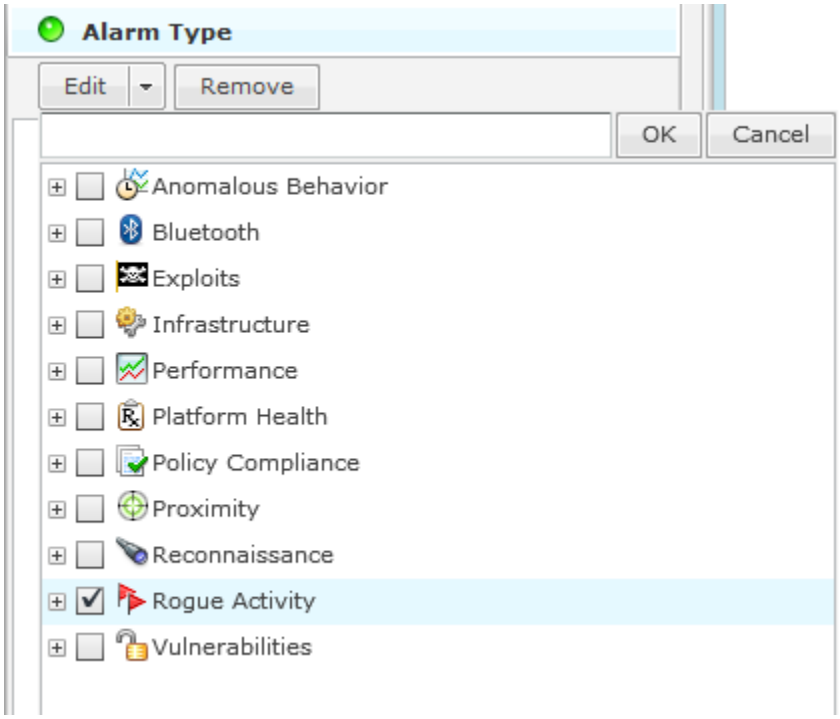
The **Alarm Type** filter allows you to view devices by alarm type.



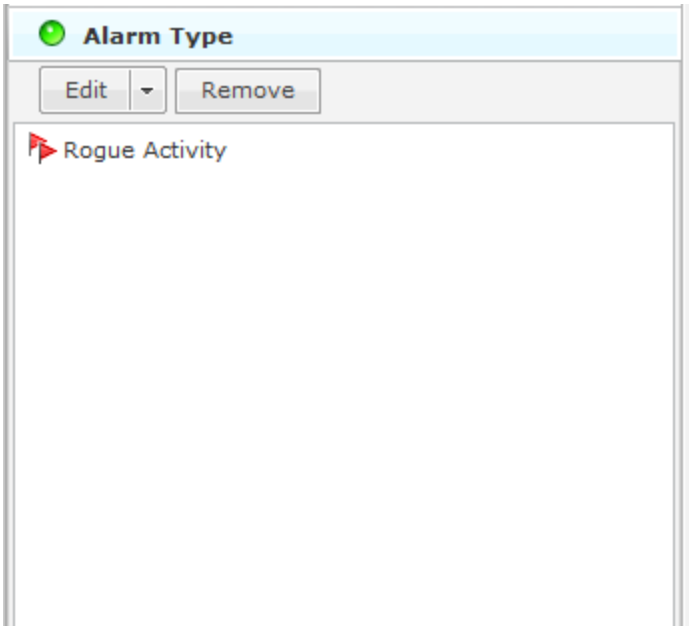
You also have the option of displaying all alarm types or you may filter alarms by a specific type. The different alarm types are:

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

Use the **Edit** button to select the alarm types that you want to display.



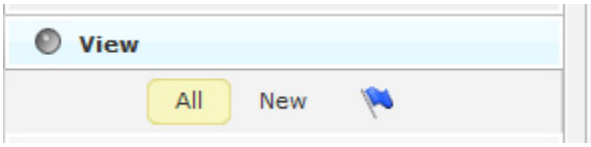
Click the **Edit** button, select the alarm type(s), and then click **OK**. The following screen shots shows that you only want to display rogue alarms.



To remove an alarm type, select (highlight) the alarm type and click the **Remove** button.

View Filter

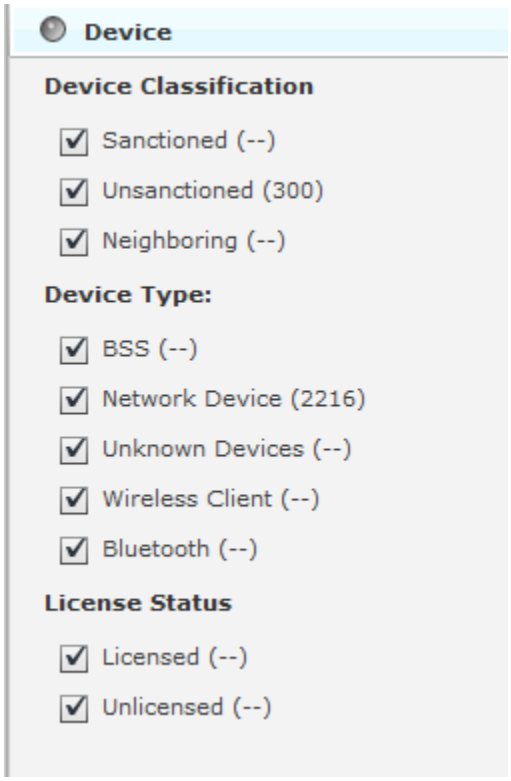
The **View** filter gives you the option of viewing all alarms, new alarms, or flagged alarms.



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.



Alarms can be displayed by the following device classifications:

- 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.
- Neighboring—Display alarms for neighboring 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 Devices
- Wireless Client
- Bluetooth

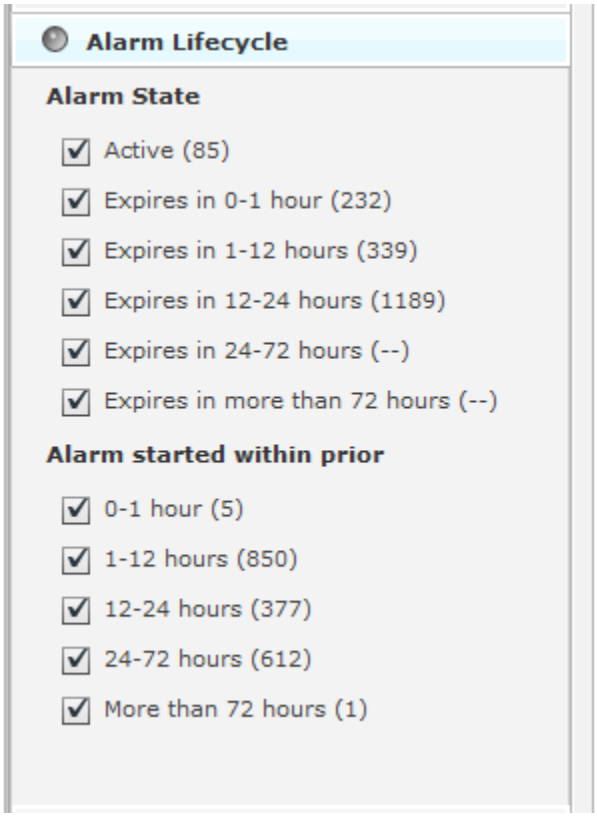
Also, alarms can be displayed by license status:

- Licensed
- Unlicensed

Select the checkbox(es) for the device classifications and/or device types that you want to display.

Alarm Lifecycle Filter

Use the The **Alarm Lifecycle** filter to filter alarms over a specified range of time.



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.

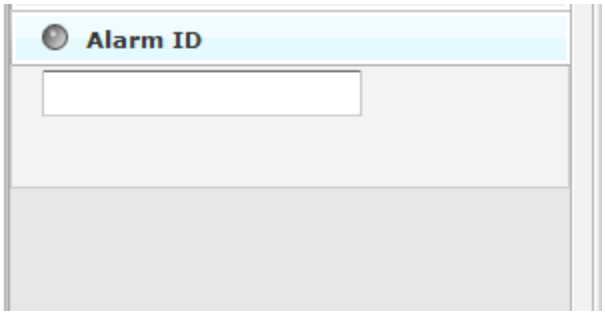
The time range when alarms started include:

- 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.



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.

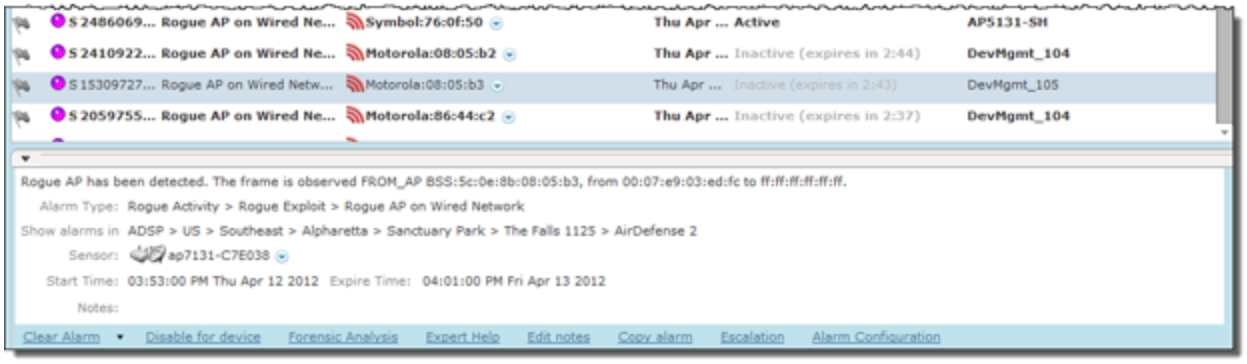
Alarm Criticality

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

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

Alarm Details

Additional alarm information can be displayed by selecting an alarm. 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

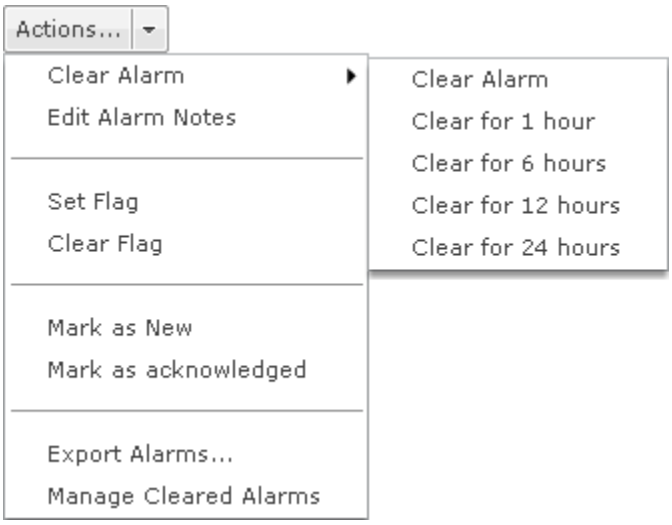
- The network level of the device
- The Sensor that observed the device
- The time when the alarm started
- The time when the alarm will expire
- Any notes added by a user.

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 **Clear Alarm** in the **Actions** menu.
Disable for device	Disables the alarm specifically for the device causing the alarm. If you wish to re-enable the alarm, you must go to Alarm Configuration and remove the device from the disabled list.
Forensic Analysis	Accesses Forensic Analysis where you can analyze historical information about the device.
Expert Help	Provides comprehensive descriptions on the alarm in four tabs: • Summary—displays a summary about the alarm type. • Description—displays detailed information about the alarm type. • Investigation—advises you on how to investigate the alarm type. • Mitigation—advises you on how to mitigate the alarm type.
Edit notes	Allows you to edit or add notes for the alarm.
Copy alarm	Copies all the detailed information about the alarm to the Clipboard for later use.
Escalation	Displays an escalation window displaying what you need to do to escalate a problem. The escalation information is defined in the alarm configuration for the specific alarm.
Alarm Configuration	Opens **Alarm Configuration** in the **Configuration** tab.

Alarm 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	Clear the selected alarm using one of the following options: • Clear Alarm (no time limit) • Clear for 1 hour • Clear for 6 hours • Clear for 12 hours • Clear for 24 hours. 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.
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 **Remove Alarms**. Click **Close**–***x*** to exit the overlay.

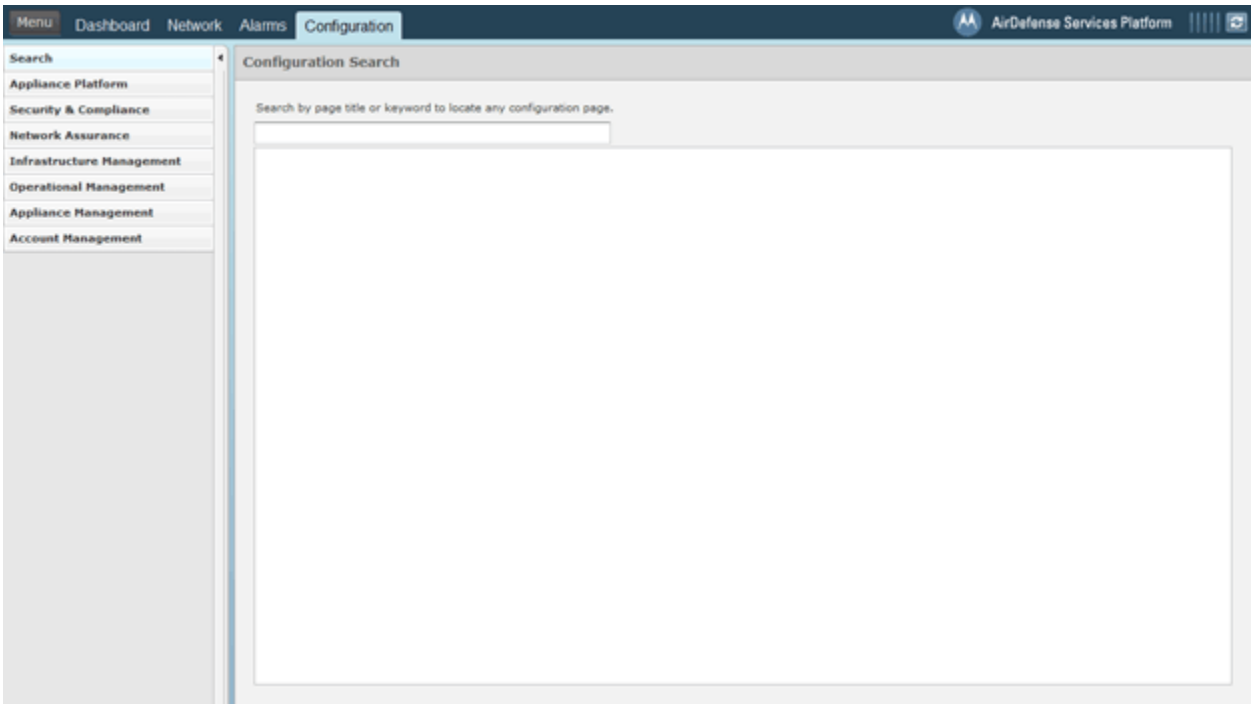
CHAPTER 7 CONFIGURATION

Configuration Tab

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:

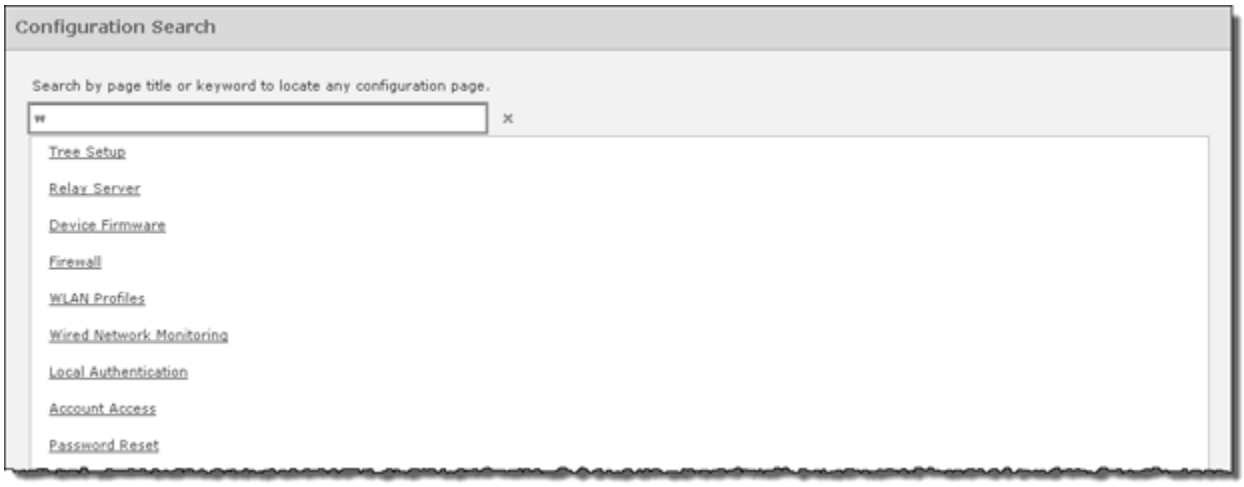
- Appliance Platform is used to initially set up ADSP.
- Security & Compliance is used to define the security configurations of sanctioned wireless clients and monitor the wired network devices in your system.
- Network Assurance provides WLAN performance monitoring. and performs traffic analysis and RF analysis—among other actions—to determine coverage gaps. Use it to configure Live RF settings, create performance profiles, and set up environment monitoring.
- Infrastructure Management is used to configure devices so that they can communicate on your network and be managed by ADSP.
- Operational Management is used to configure features that apply to the normal operations of ADSP.
- Appliance Management is used to configure the ADSP appliance.
- Account Management is use to set up user account parameters, including access, authentication and passwords.



Search

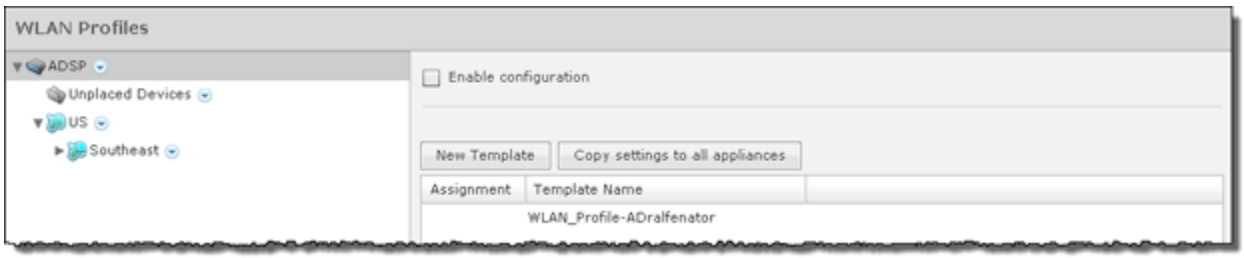
This feature allows you to Searches the **Configuration** tab for quick location of a configuration feature.

To conduct a search, just start typing.



Typing just one 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.

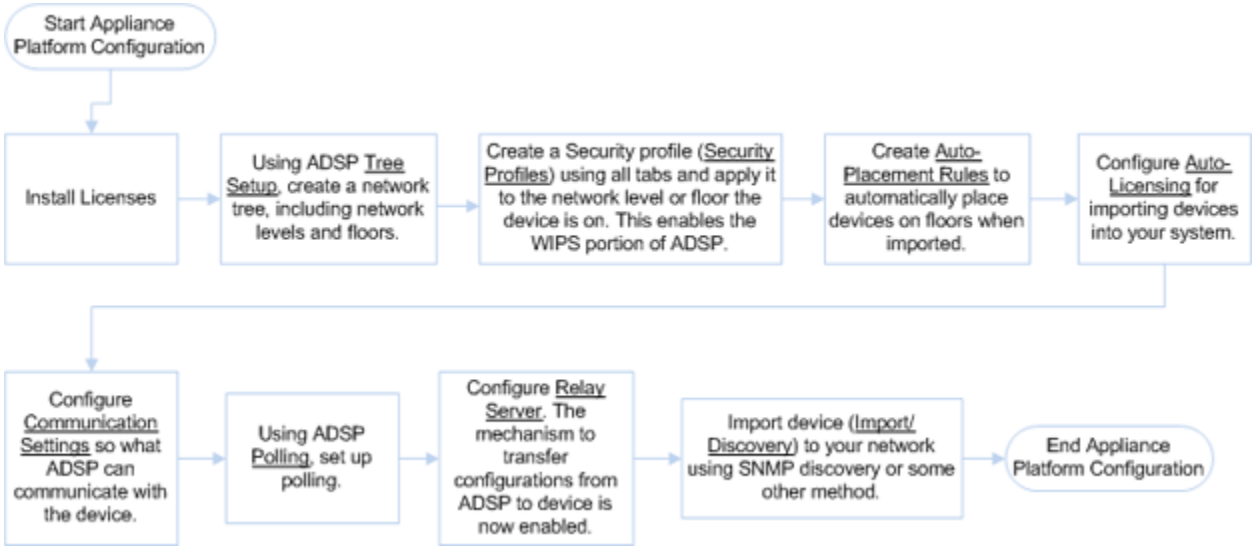
The Appliance Platform category allows you to:

- 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.

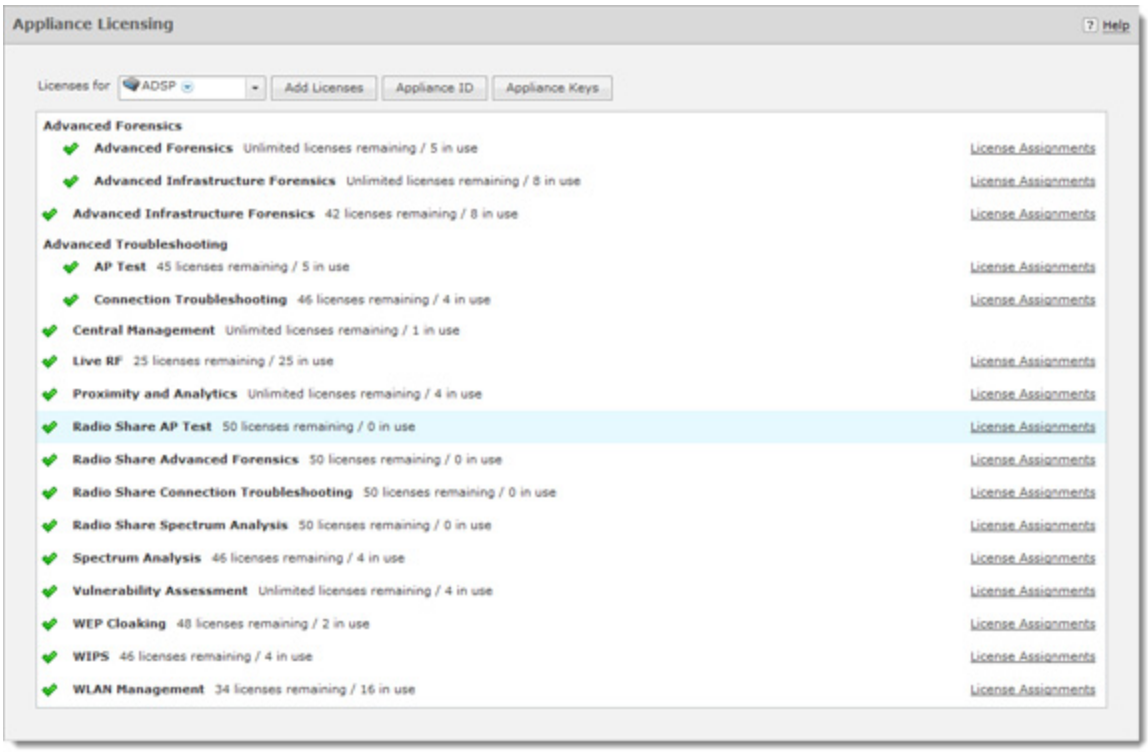


Appliance Licensing

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 License, which includes:
  - Advanced Forensics
  - Advanced Infrastructure Forensics
- Advanced Troubleshooting License, which includes:
  - AP Test (available as a separate license)
  - Connection Troubleshooting (available as a separate license)
- Assurance Suite License, 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 License
- Proximity and Analytics License

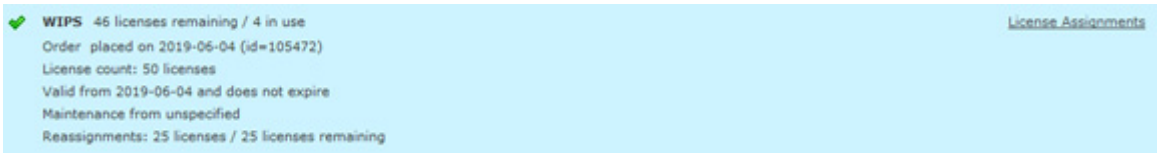
- Radio Share Network Assurance License, which includes:
  - Radio Share AP Test (available as a separate license)
  - Radio Share Advanced Forensics (available as a separate license)
  - Radio Share Connection Troubleshooting (available as a separate license)
  - Radio Share Spectrum Analysis (available as a separate license)
- Vulnerability Assessment License
- WEP Cloaking License
- WLAN Management License

License Status

License status is determined 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.

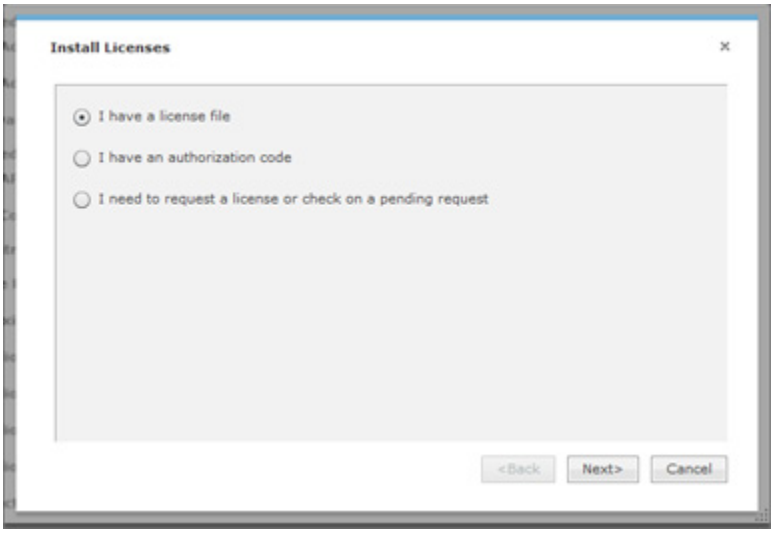


Field	Description
Order Date	Indicates the date the license was ordered and the license ID number.
License Count	Includes the following information: • The number of units. The number of active units cannot exceed this number. Unit counts may be 0, a specific number, or unlimited. • A style that specifies that the unit count is fixed or floating. Fixed licenses get consumed as they are used and are not released. Floating licenses get released when they are not being used anymore. • A unit identifier. Units may be Sensors, APs, switch, etc. • A maximum value limiting the number of units. • A warning limit used to display an alarm that the unit count is being approached and that user should consider purchasing additional licenses.

Field	Description
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.

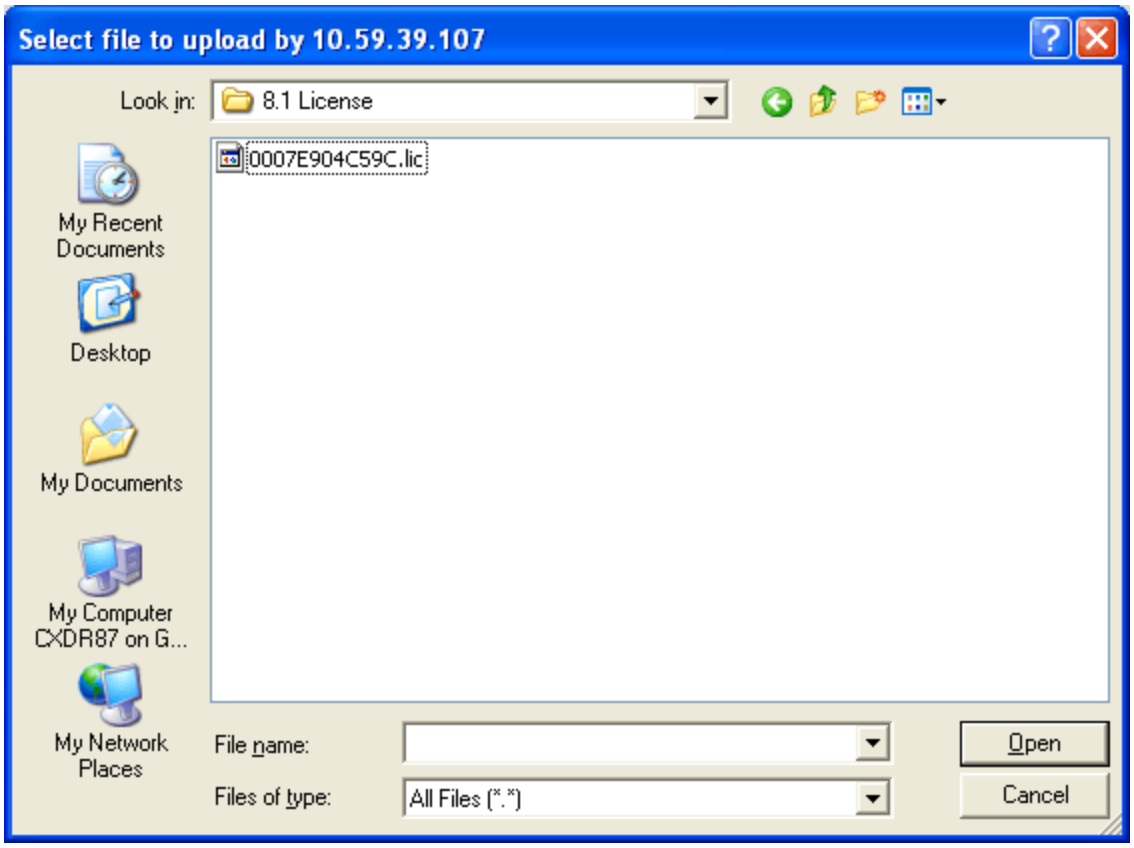


There are three ways to install a license:

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

Using a License File

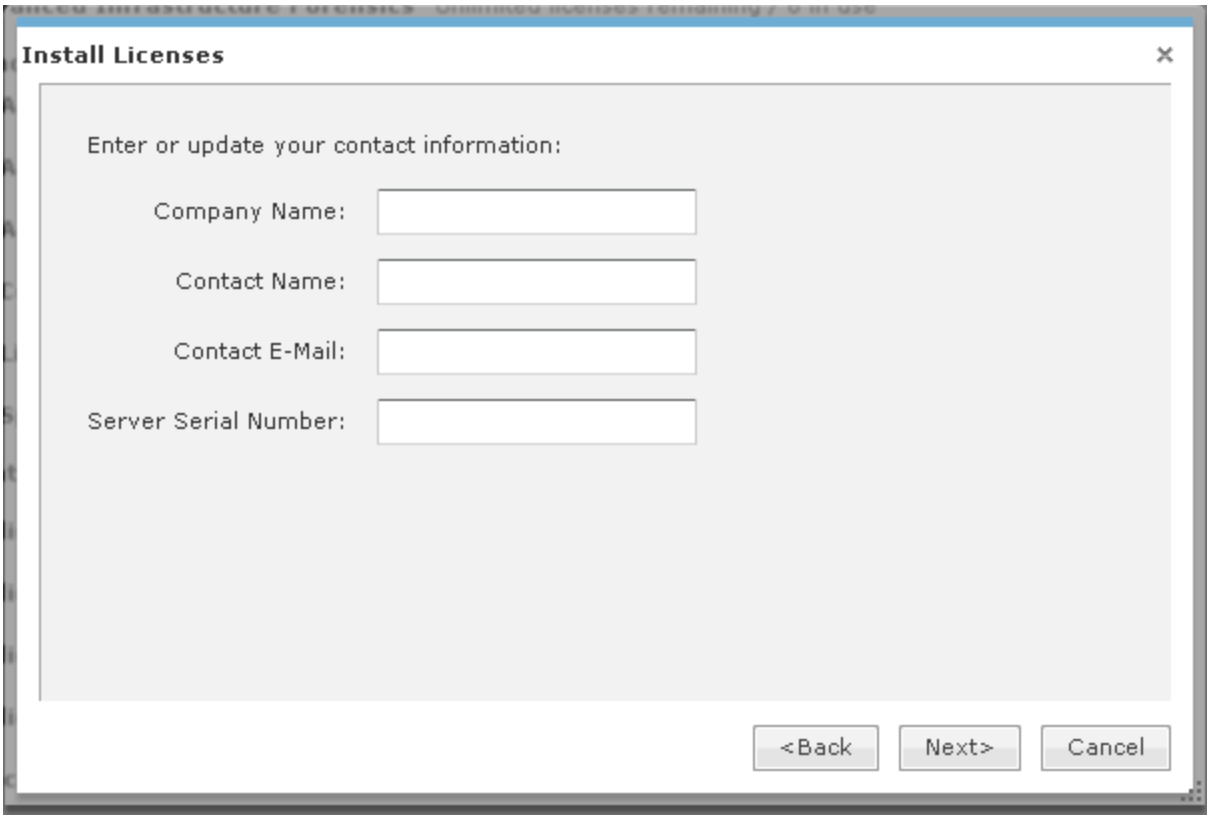
A license file contains information about your license. If you have a license file, select the **I have a license file** option and then click **Next**.



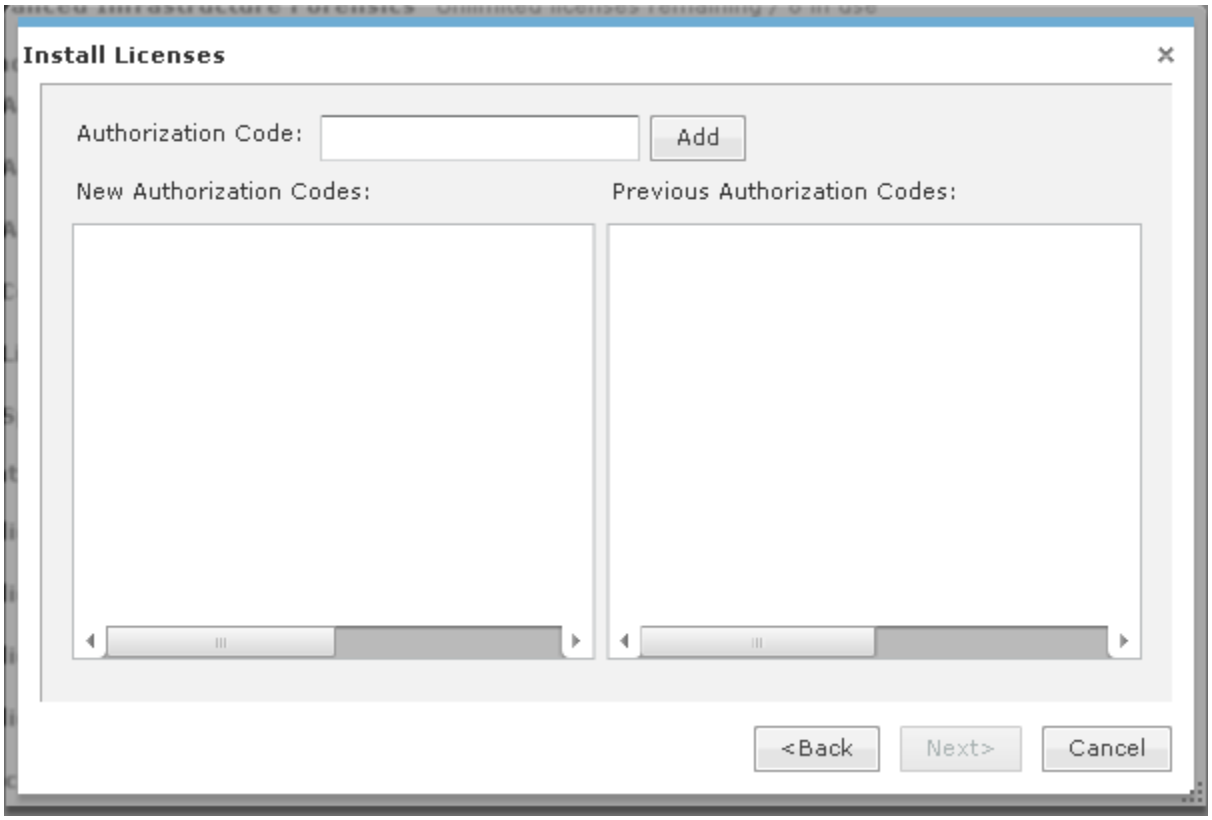
Navigate to the file and select it. Once you have selected the licensing file, click **Open**. The license information is updated.

Using an Authorization Code

If you have an authorization code, select the **I have an authorization code** option and then click **Next**.



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

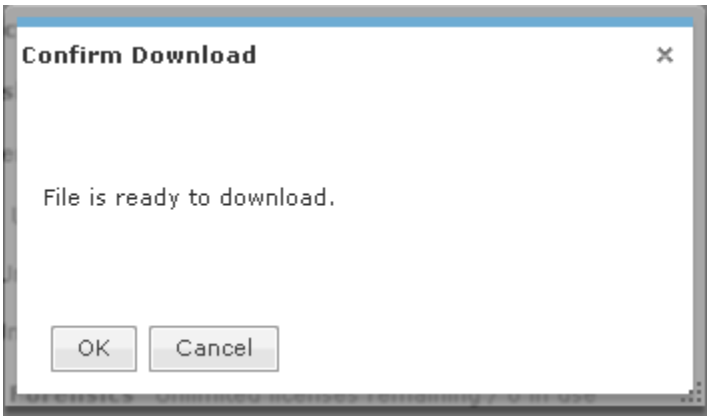
You can display the appliance's ID where you can copy it for later use. Click the **Appliance ID** button to display the ID.

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 **Save**.

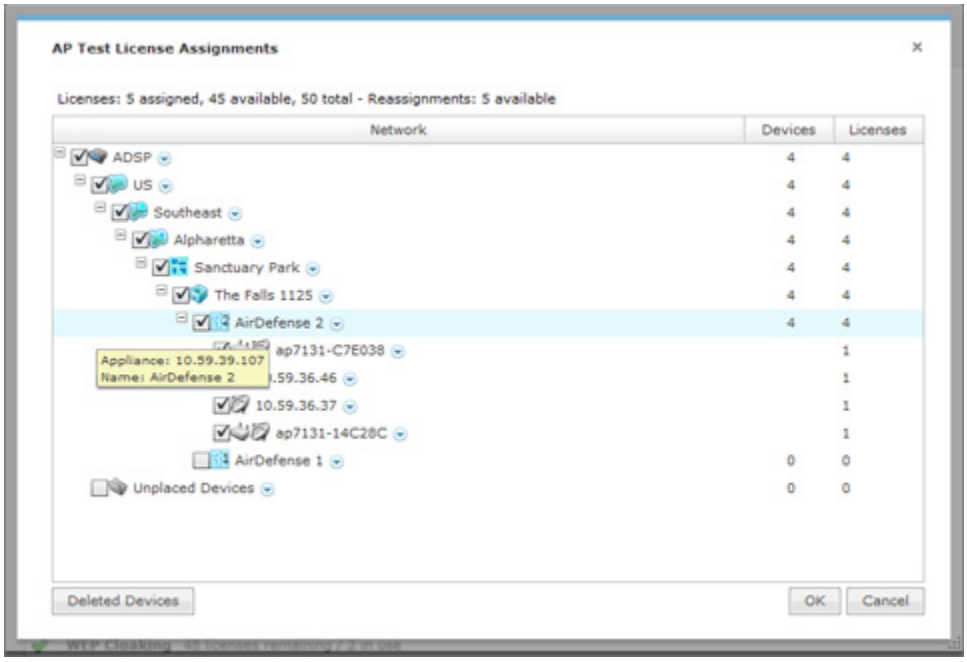
License Assignments

Use the **License Assignments** link 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

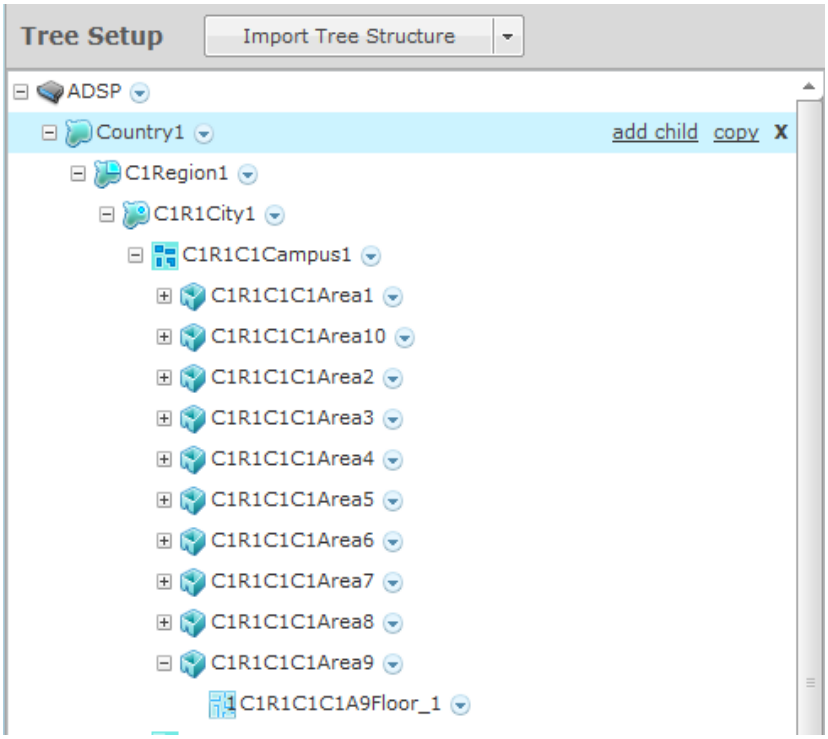
Use the **Tree Setup** feature to configure your network tree.

NOTE You must set up your network tree on order to take full advantage of the functionality of ADSP!

Planning Your Network Tree

Your network tree 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.



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 Network 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.

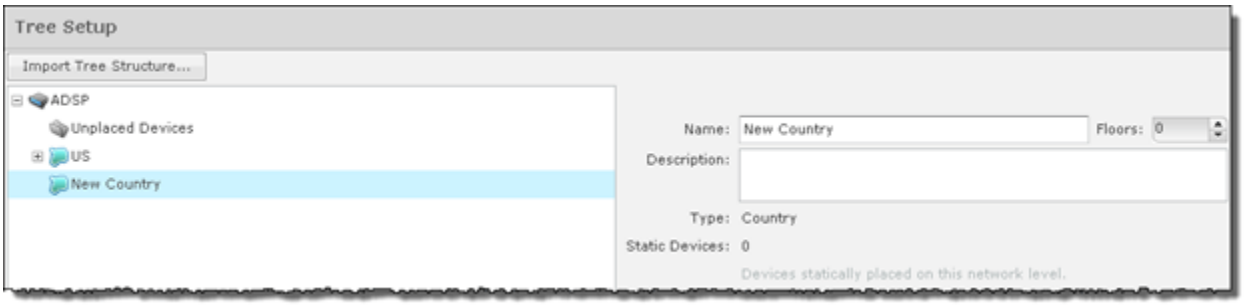
NOTE The menu will only display the network level that is available at the selected level. You cannot add a network level that is higher up in the network tree.

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.

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.

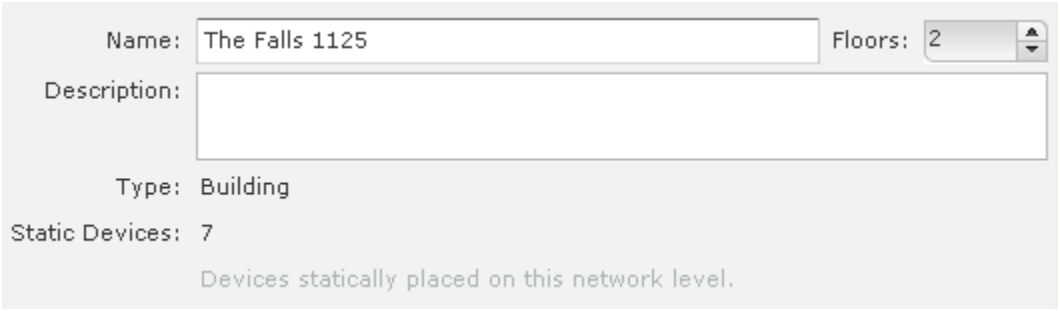


You can now name your new network level and give it a description. The name and description can be changed at any time. Repeat this process until you have defined your network tree.

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 Network 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 a new CSV files does not replace an existing tree structure; instead, you can use the commands add or delete at the end of an import line 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.

Examples:

```
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 exists. 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
```

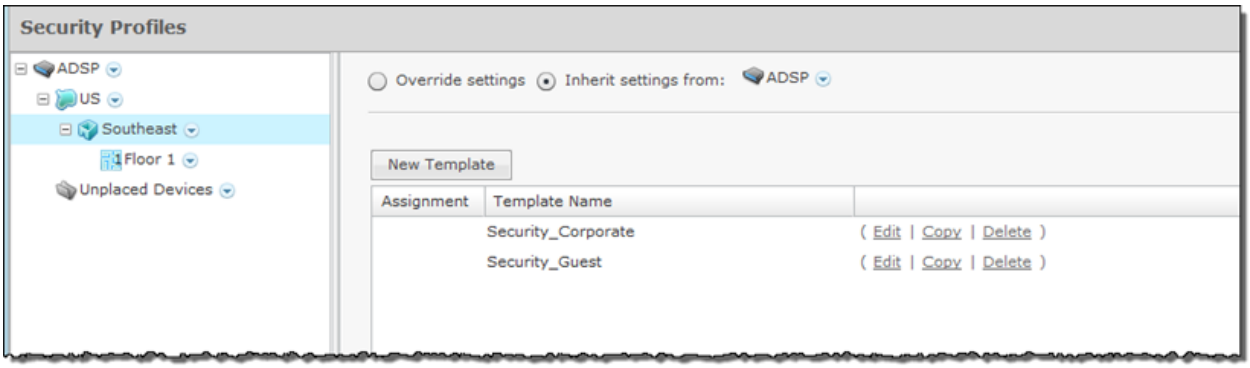
Once you have finished building your network tree, click the **Apply** button to save your changes. This applies even when importing Auto-Placement rules with the **Import Tree Structure** button. You may click the **Reset** button to revert back to your previous network tree configuration.

Security Profiles

Security Profiles are used to 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.

View Security Profiles

To access security profiles, go to **Configuration** > **Appliance Platform** > **Security Profiles**. Existing profiles are displayed in the right column.



Modify Security Profiles

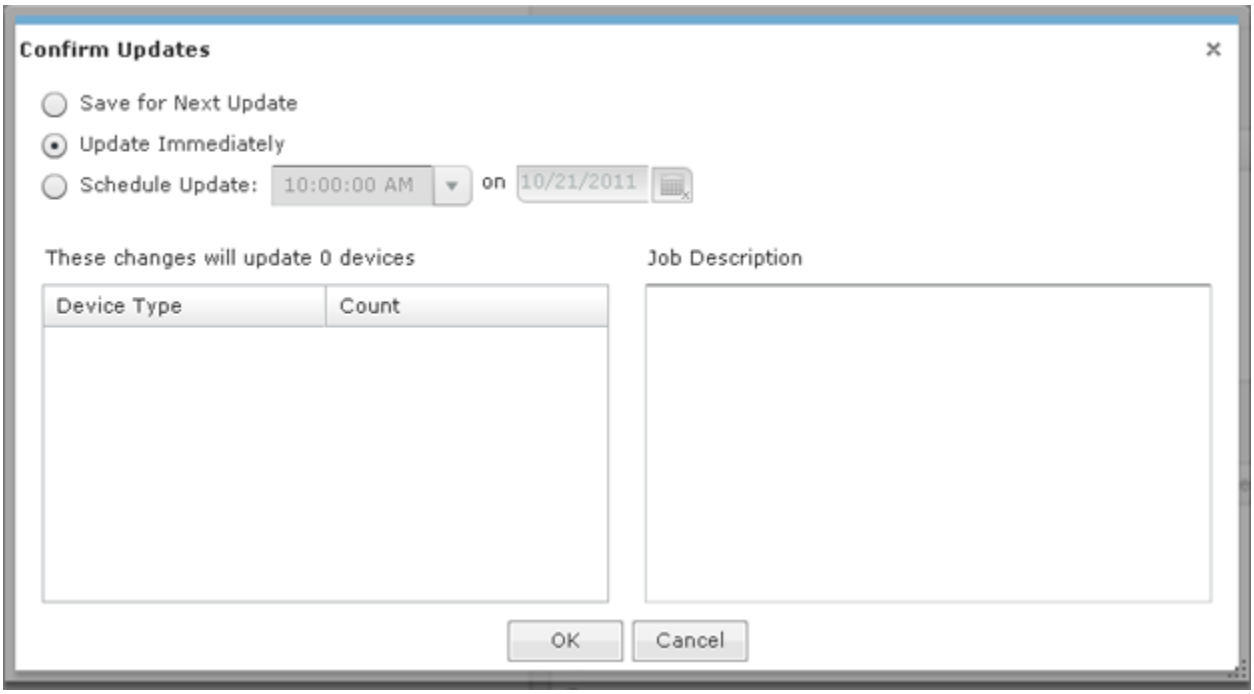
You can edit, copy or delete any selected (highlighted) profile by clicking the appropriate link.

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.

Click the **Copy settings to all appliances** button to 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.



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).

Add a New Security Profile

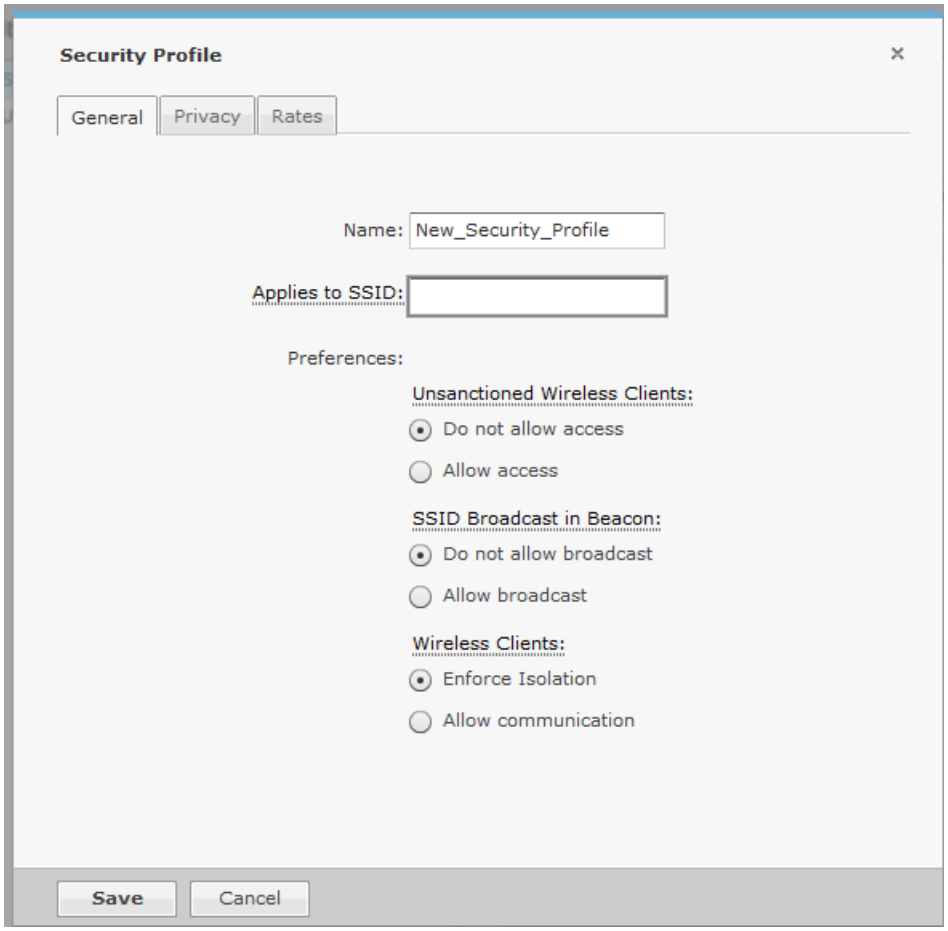
All profiles have three tabs that are used to set security threshold policies for your system, as follows:

- 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.

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.



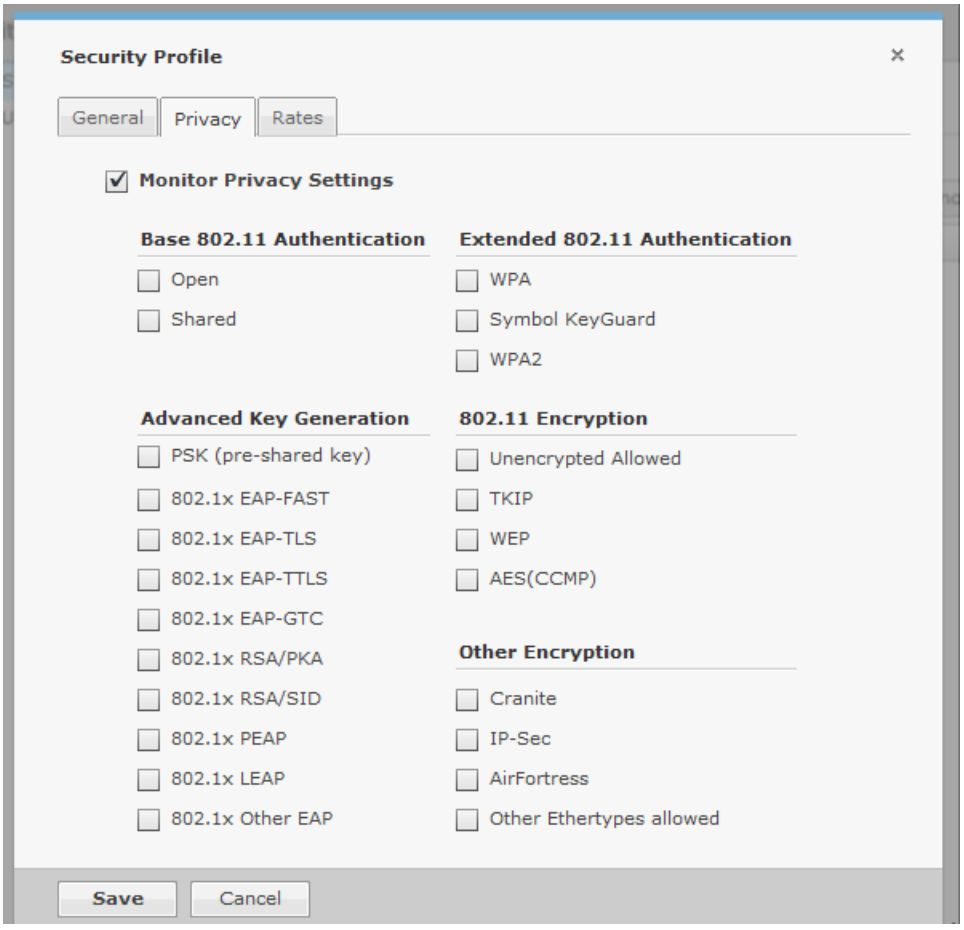
The **Name** field specifies the profile name. If you are adding or copying a Security Profile, ADSP gives the profile a default name beginning with New_Security_Profile and ending with a system generated number. You should change the default name to one that is more appropriate to its function. Once 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.



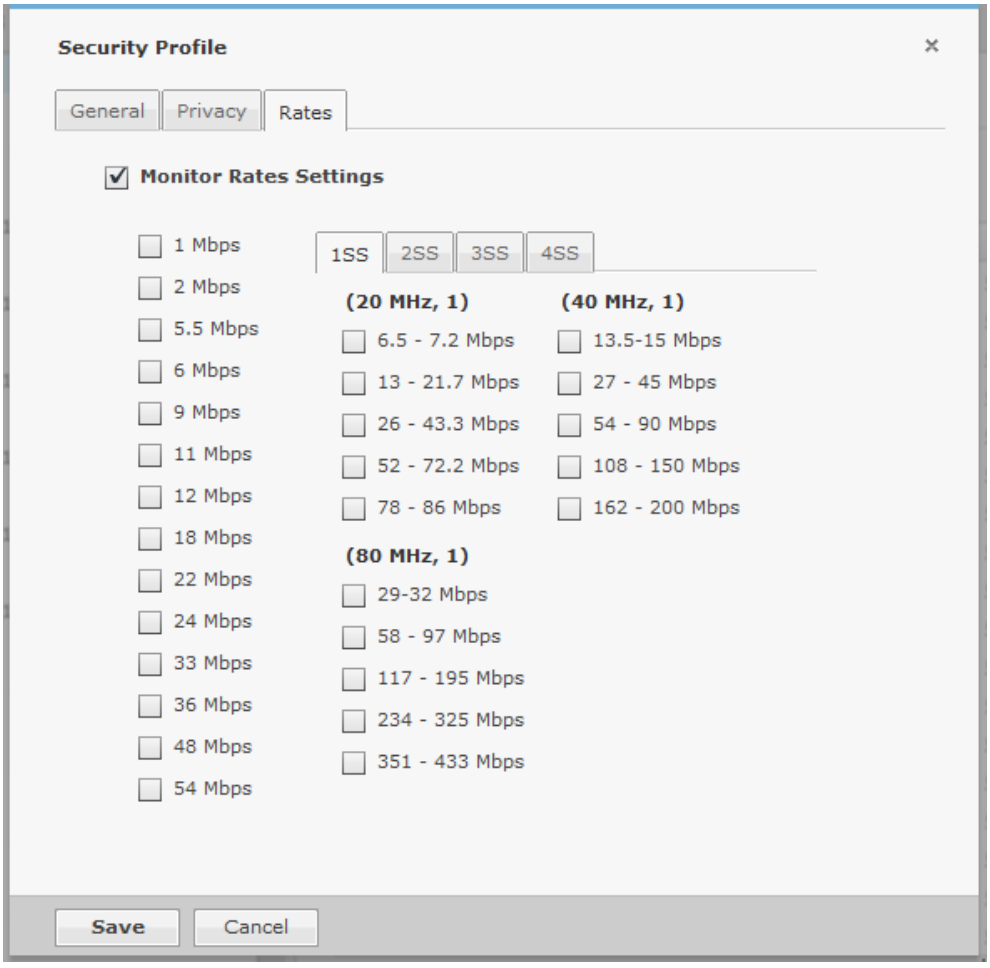
You must check the **Monitor Privacy Settings** checkbox to activate the functions. The functions are:

Function	Description
Base 802.11 Authentication	**Open**—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). **Shared**—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 over a secure channel that is independent of 802.11. In practice, the shared key authentication secret is manually distributed and typed.
Extended 802.11 Authentication	**WPA**—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. **WPA2**—Short for Wi-Fi 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. **Symbol KeyGuard**—When this checkbox is selected, it activates Symbol KeyGuard authentication protocols, which is provided by Symbol.
Advanced Key Generation	**PSK (preshared key)**—When selected, it activates the Pre-shared Key authentication. **802.1x EAP-FAST**—When selected, it keys 802.1X EAP Flexible Authentication via Secure Tunneling. **802.1x EAP-TLS**—When selected, it keys EAP Transport Level Security. **802.1x EAP-TTLS**—When selected, it keys EAP Tunneled Transport Layer Security. **802.1x EAP-GTC**—When selected, it keys EAP Generic Token Card. **802.1x RSA/PKA**—When selected, it keys EAP RSA Public Key Authentication Protocol. **802.1x RSA/SID**—When selected, it keys EAP RSA SecurID. **802.1x PEAP**—When selected, it keys any 802.1X Protected Extensible Authentication Protocol (PEAP). **802.1x LEAP**—When selected, it keys EAP Lightweight Extensible Authentication Protocol. **802.1x Other EAP**—Keys any 802.1x EAP authentication/key distribution mechanism other than the types previously mentioned.

Function	Description
802.11 Encryption	**Unencrypted Allowed**—Select this checkbox to allow no 802.11 encryption for wireless traffic. **TKIP**—When selected, this enables the BSS to advertise support for Temporal Key Integrity Protocol (TKIP). **WEP**—When selected, causes the BSS and Wireless Client to use WEP as their encryption policy. **AES (CCMP)**—When selected, causes the BSS to advertise support for Advanced Encryption Standard (AES-CCMP).
Other Encryption	**Cranite**—When selected, enables AP usage of Layer 3 Cranite encryption. **AirFortress**—When selected enables AP usage of Layer 3 Airfortress encryption. **IP-Sec**—When selected, enables AP usage of Layer 3 IP security protocol as encryption. **Other Ethertypes allowed**—When selected, enables AP usage of other Layer 3 encryption mechanism which is not specified here.

Rates Tab

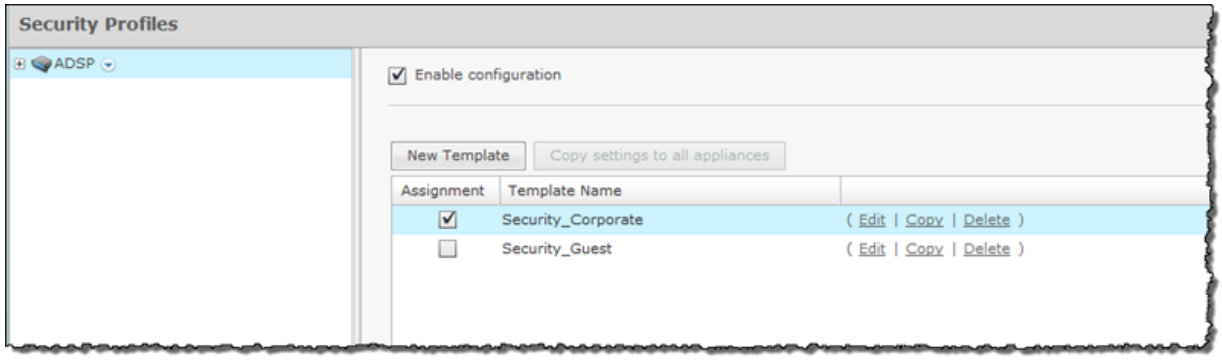
The **Rates** tab is where you can select transmit and receive data rates for BSSs to use.



You must check the **Monitor Privacy Settings** checkbox to activate the settings. Select the transmit and receive data rates you want BSSs to use.

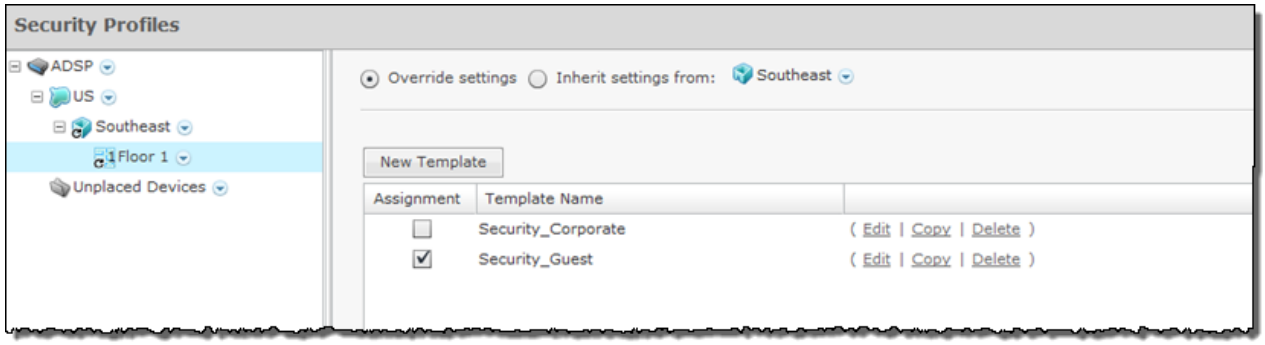
Apply a Security Profile

Once you have defined and added a Security Profile, 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 screenshot, the Security Profile for ADSP is the **Security_Corporate** profile. Then, for a special case, you can override the Security Profile at the ADSP level and apply the **Security_Guest** profile to the **Floor_1** 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 determine where devices will be placed in the network tree when they are imported. Any device that has the specified parameter(s) and qualifying value(s) will be placed in the selected network level.

Auto-Placement Rules for Devices

Auto-Placement rules can be used in two ways: one method is for sensors and the other is for APs and switches.

Sensors

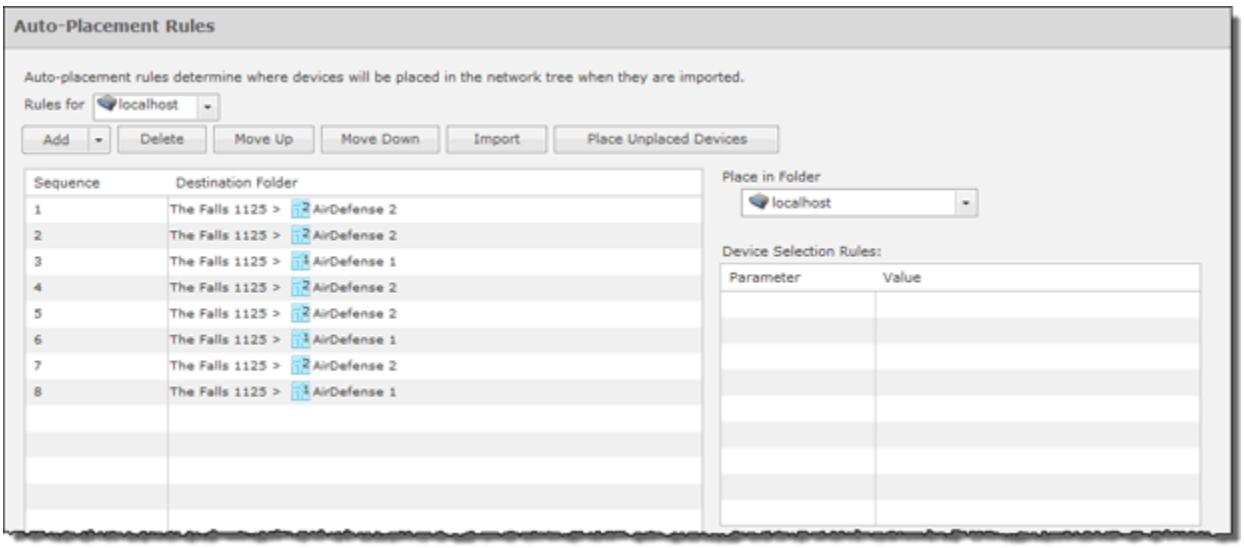
Auto-Placement rules for sensors are applied every 20 minutes. If a rule exists, new sensors in the **Unplaced Devices** folder are moved into a predefined scope level. This only happens to sensors seen in your network since the last 20 minute poll. Sensors seen before the last 20 minute poll are excluded.

APs and Switches

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 predetermined scope level.
- If no rule exists, the AP or switch is moved into the **Unplaced Devices** folder.
- Adopted APs discovered from a controller but without an applicable auto-placement rule are 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.



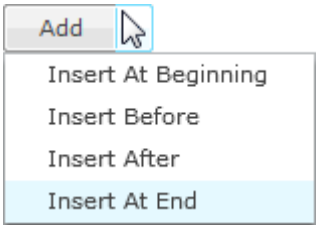
NOTE Before you can define any Auto-Placement rules, the network tree must already be configured.

Add Auto-Placement Rules

Follow these steps to add 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.

Field	Description
DNS Server	The DNS server that the device(s) are using. This parameter only works with sensors not APs and switches.
Uses DHCP	Specify whether or not DHCP is used (**True** or **False**). This parameter only works with sensors not APs 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 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.

Import 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:

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

Example:

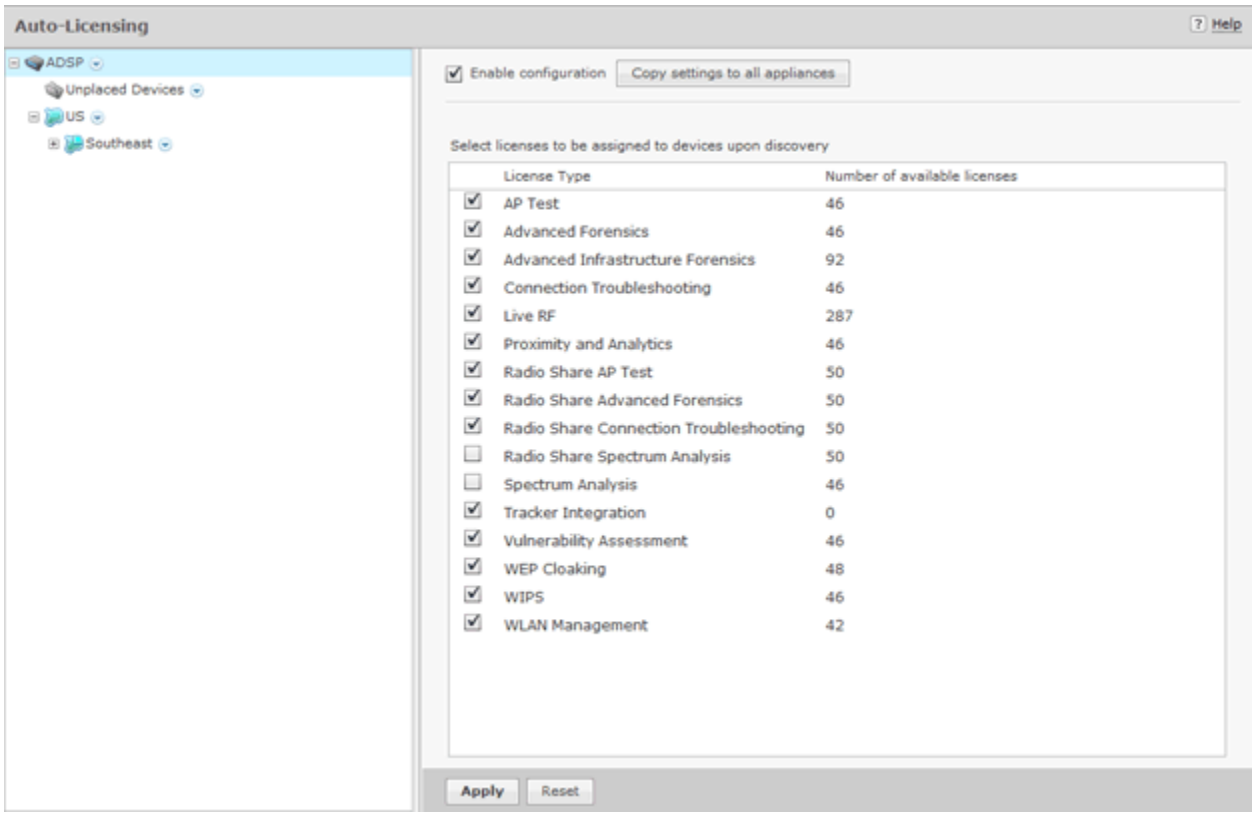
```
autoplacement_rule,localhost,/USA/AutoPlacementTest/Floor
1,,172.17.17.0-172.17.17.19,,,,,,6.0.196.0
autoplacement_rule,localhost,/USA/AutoPlacementTest/Floor
6,,172.17.15.0-172.17.15.200,,,,,,6.0.196.0
autoplacement_rule,localhost,/USA/AutoPlacementTest/Floor 4,172.17.18.0/24,
172.17.18.100-172.17.18.101,00:16:5d:20:47:60-00:16:5d:20:47:61,172.17.0.83,
disable,BA-Sensor-240,M520,5.2.0.11.1234567890
```

Auto-Licensing

Auto-Licensing allows you to select licenses to be assigned to devices upon discovery. You can 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**.

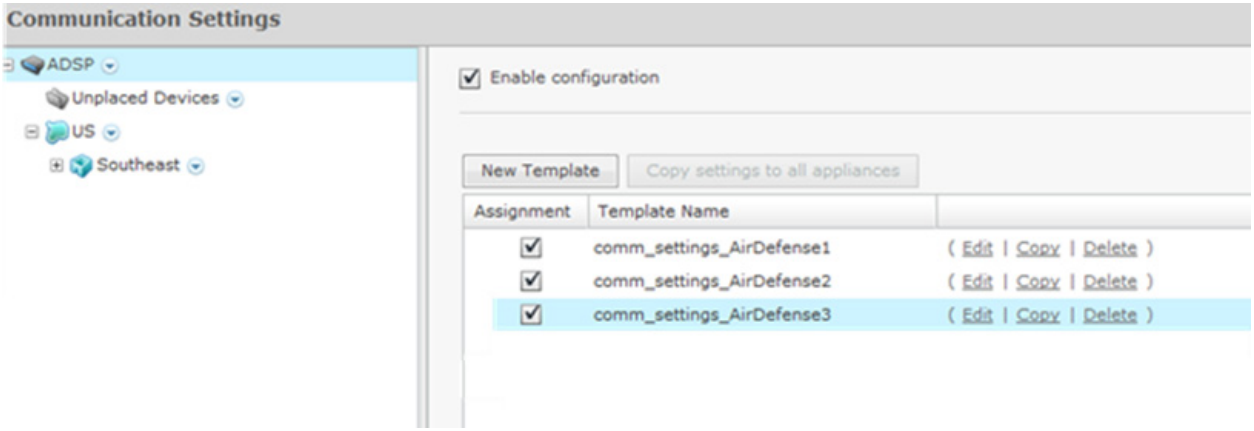
NOTE You must have a Central Management license in order to copy settings to all appliances.

Communication Settings Profile

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

View Communication Settings Profile

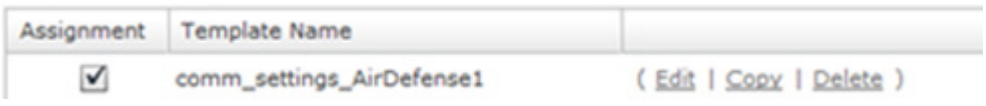
To access communication settings, go to **Configuration** > **Appliance Platform** > **Communication Settings**. Existing profiles are displayed in the right column.



NOTE When ADSP is set up as a VM on WiNG in Unified Mode, the WiNG default communications settings profile is available. The profile is automatically assigned to the NX95x0 in Unified Mode. Administrators must ensure that this profile matches the NX95x0 Management Profile.

Modify Communication Settings Profile

You can edit, copy or delete any selected (highlighted) profile by clicking the appropriate link.



To copy or edit a profile, select (highlight) the profile, click the **Copy** or **Edit** link, and then make changes in any of the three tabs. Click **Save** to save your changes.

The **Copy settings to all appliances** button will copy Communication Settings to all appliances in your system.

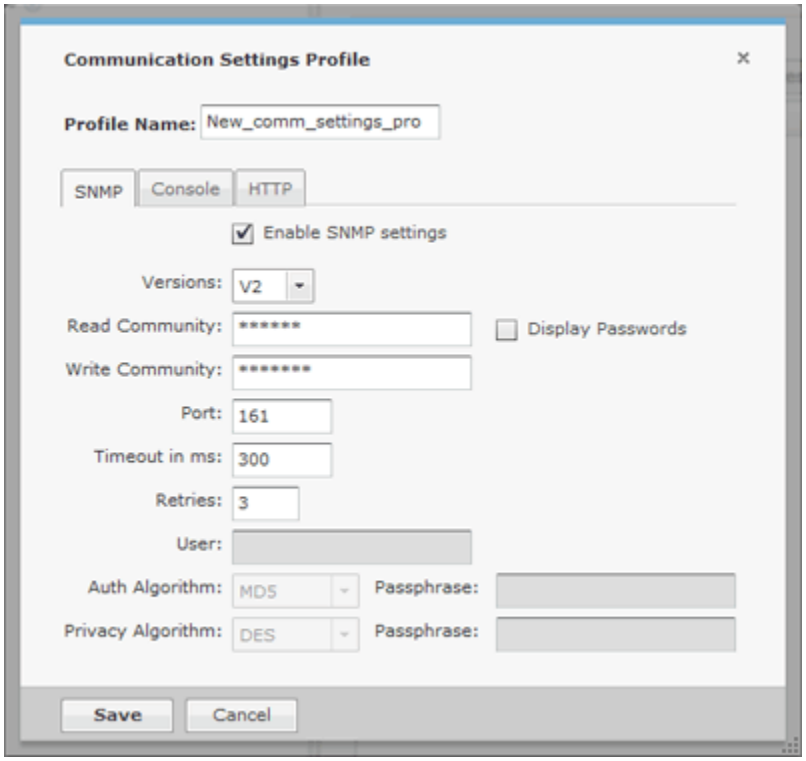
NOTE It is recommended that you do not modify the default profiles for the following reason: when you apply a profile, ADSP will search the existing profiles list for the best match, starting at the top of the list and working its way down to the bottom of the list. In order for this event to work properly, the default profiles should not be changed.

Add a New Communications Settings 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 Tab

Use the **SNMP** tab to configure connectivity settings for SNMP devices.



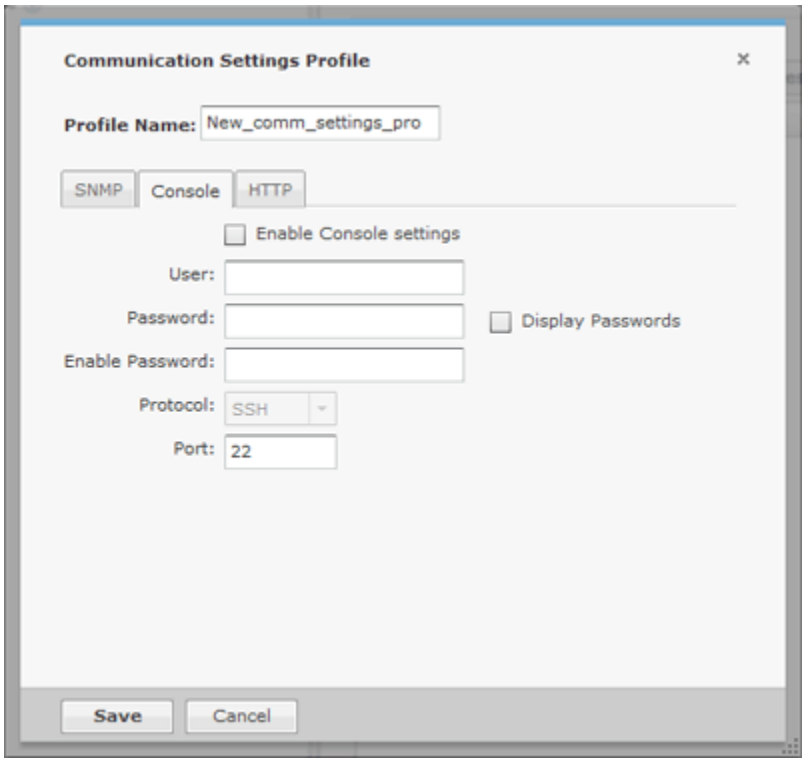
The following SNMP fields can be set:

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 **V2** or **V3** as the SNMP version used.

Field	Description
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.
Auth Algorithm	The authentication algorithm is a SNMP V3 parameter that must match what is set on the device. The options are **MD5**, **SHA** and **None**. You must also supply a passphrase which must also match what is set on the device.
Privacy algorithm	The privacy algorithm is a SNMP V3 parameter that must match what is set on the device. The options are **DES**, **3DES**, **AES128**, **AES192**, **AES256** and **None**. You must also supply a pass-phrase which must also match what is set on the device.

Console Tab

Use The **Console** tab to supply login credentials for devices that interface with a console.

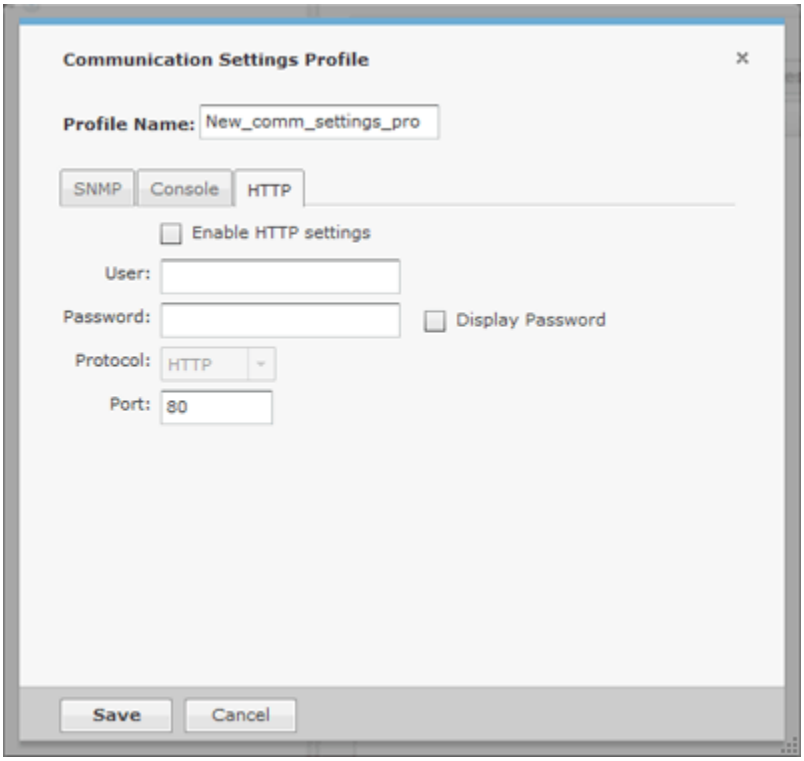


The following fields must be set when using a console to interface with a device:

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.
Protocol	The protocol used to log into a device. The available options are **SSH** and **Telnet**.
Port	The port number that is used for communications. Port 22 is normally used but it may be another port number.

HTTP Tab

Use the **HTTP** tab is to configure login credentials for the devices that use a web UI to interface with them.



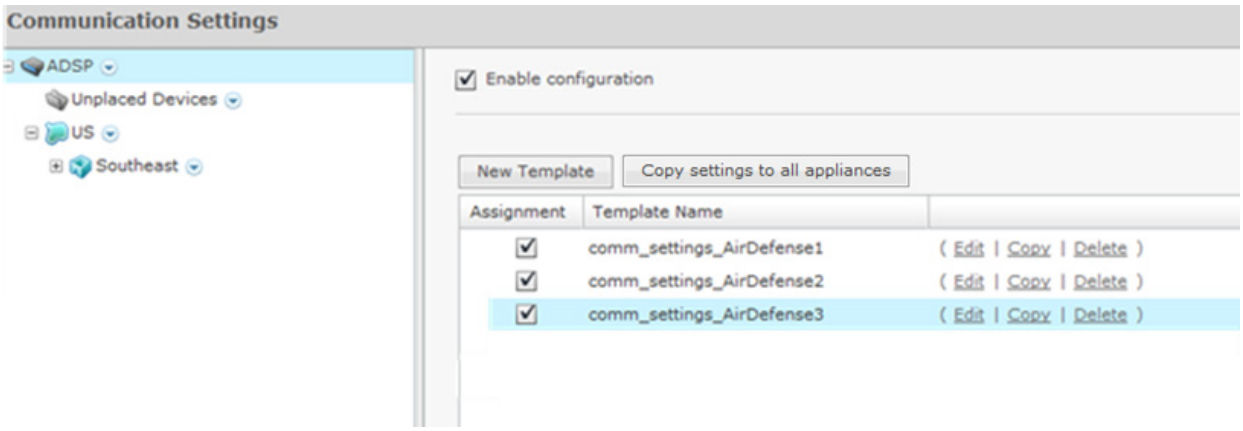
The following fields must be set when using a web UI to interface with a device:

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

Once you have configured your communication settings, click **Save** to save your profile or **Cancel** to exit without saving the profile.

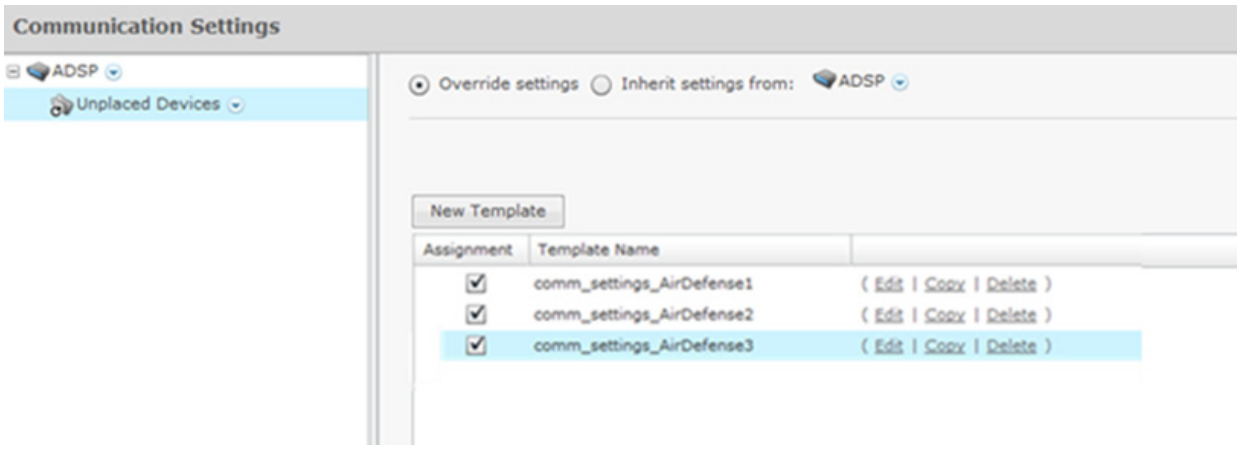
Apply a Communication Settings Profile

Once you have defined a Communication Settings Profile, 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.

Import Communications Settings

You may import Communications settings for a device using one of the following methods:

- Manually via **Menu** > **Import and 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

Examples:

```
comm_settings,ProfileName,3,public,private,snmpV3user,snmpV3authpassphr,snmpV3privpas
sphr,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**.

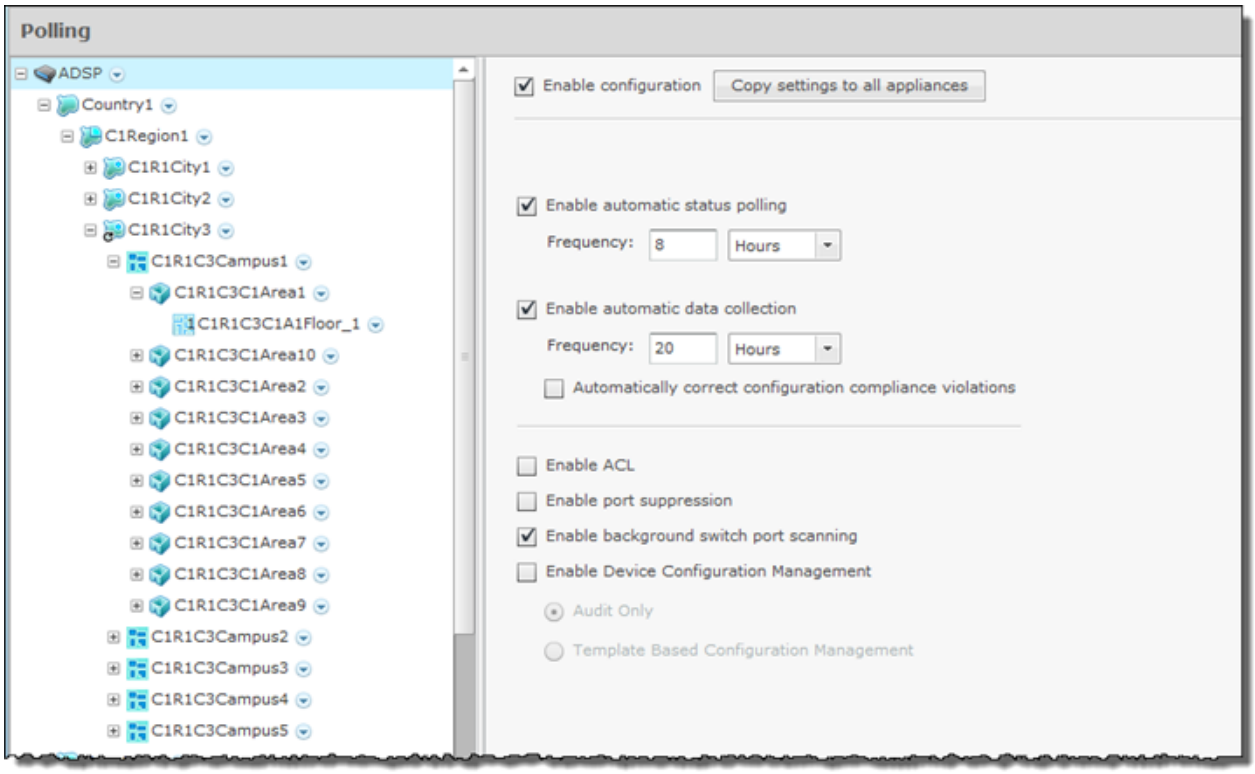
Examples:

```
comm_settings_loc,ProfileName,00:23:04:5e:d3:00,ap
comm_settings_loc,ProfileName,/US/Southeast/AirDefense,folder
3
```

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

Network devices access relay servers to obtain configuration, firmware and provisioning information.

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. 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.

Configure Relay Server

From the Relay Server screen, 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.

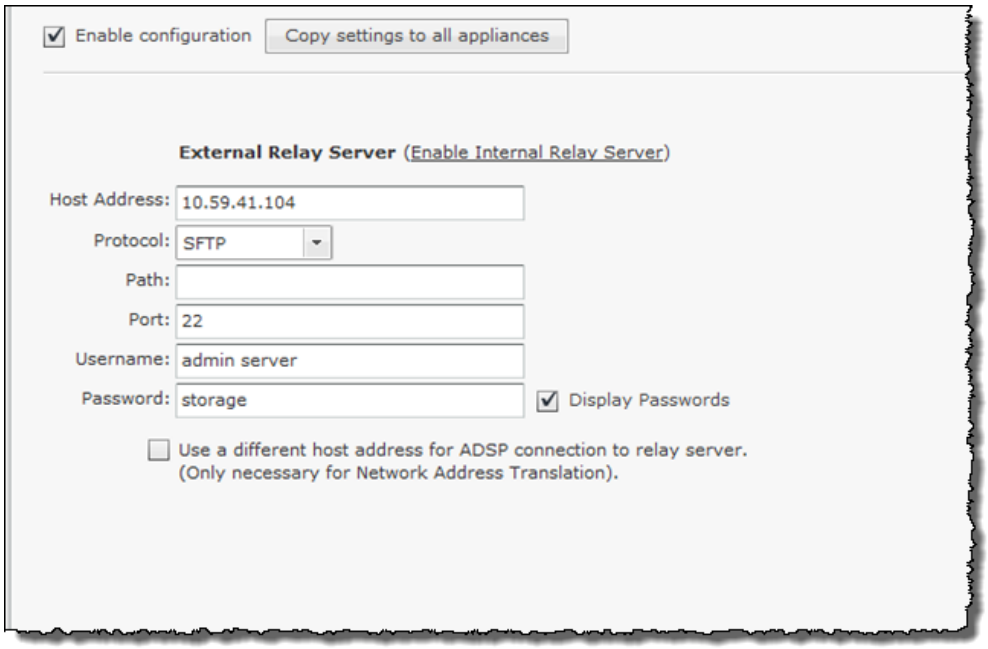
Click the **Apply** button to save any additions or changes. This applies even when importing Relay Server parameters with the **Import Parameters** button.

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.

External Relay Server

After selecting the **Enable configuration** checkbox, you will need to set up an external (or internal) server. The screen defaults to **External Relay Server**. Complete the fields to set up the External Relay Server.



Set the following values:

- Enter the **Host** name of the external 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 (/).
- The **Port** field is automatically populated.
- Create and enter a **Username**.
- Create and enter a **Password**. You have the option of having the password displayed.

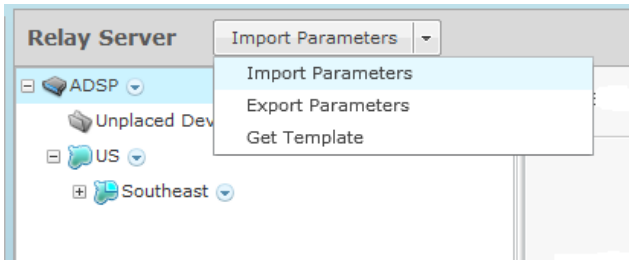
You also have the option of using your own external relay serve; you will have to supply all vital information required for the server to work with ADSP.

- 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.

Once you are finished, click **Apply**.

Import Relay Server Information

When using an external relay server, you can import relay server information using the **Import Parameters** button on the **Relay Server** bar.



When you click **Import Parameters**, you can browse to the location of the file you wish to import. You will need to use Comma delimited files to import relay server information. The format of the file is:

```
relay_params,server,folderpath,deviceHost,deviceProtocol,devicePath,devicePo
rt,deviceUsername,devicePassword,
applianceHost,applianceProtocol,appliancePath,appliancePort,applianceUsernam
e,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.

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 included 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:

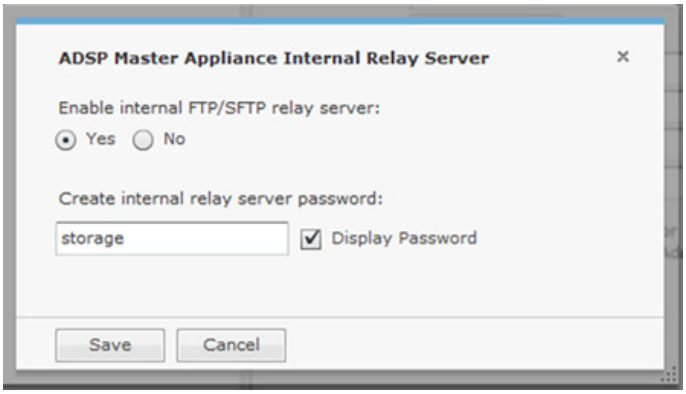
```
relay_params,localhost,/ADSP,172.17.0.80,ftp,/,21,anonymous,anonymous,172.17
.0.80,ftp,/,21,anonymous,anonymous
relay_params,localhost,/US/Southeast/AirDefense,172.17.0.80,ftp,/,21,anonymo
us,anonymous,172.17.0.80,ftp,/,21,anonymous,anonymous
relay_params,localhost,/relay_test,172.17.0.80,tftp,/,69,,,172.17.0.85,ftp,/
,21,anonymous,anonymous
```

You have two other options available: **Export Parameters** and **Get Template**. 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.

Internal Relay Server

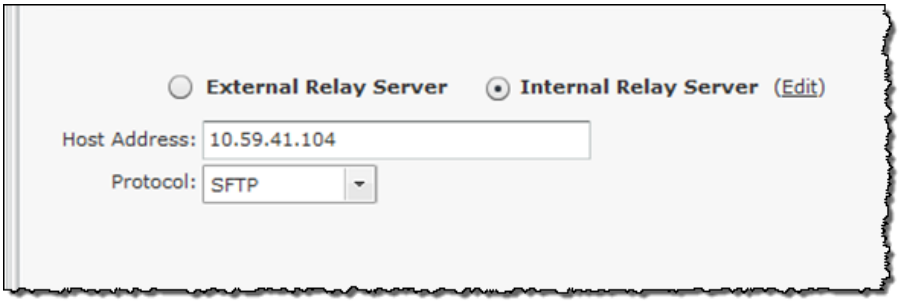
In order to set up an internal relay server, click the link (**Enable Internal Relay Server**.)

The following window displays:



Select **Yes**, create a password and click **Save** to set up the internal relay server.

You can edit the internal relay server initialization parameters by clicking the **Edit** link next to the **Internal Relay Server** radio button.



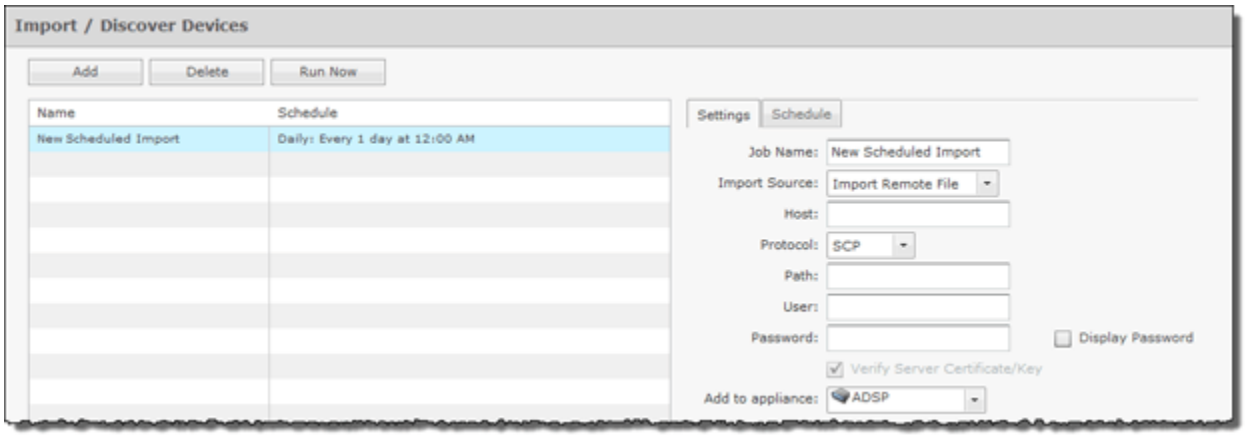
This displays the same window where you can make changes and click **Save** to save the changes.

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.

Go to **Configuration** > **Appliance Platform** > **Import/Discover Devices.** 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 define the *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

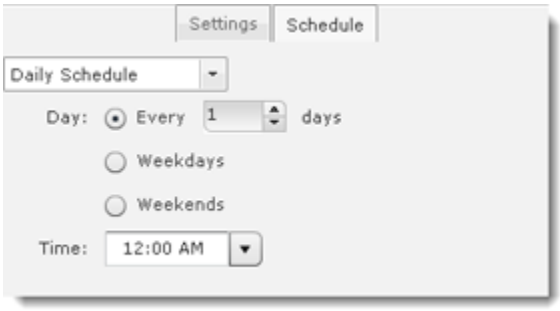
Available Fields for SNMP Discovery

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.

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

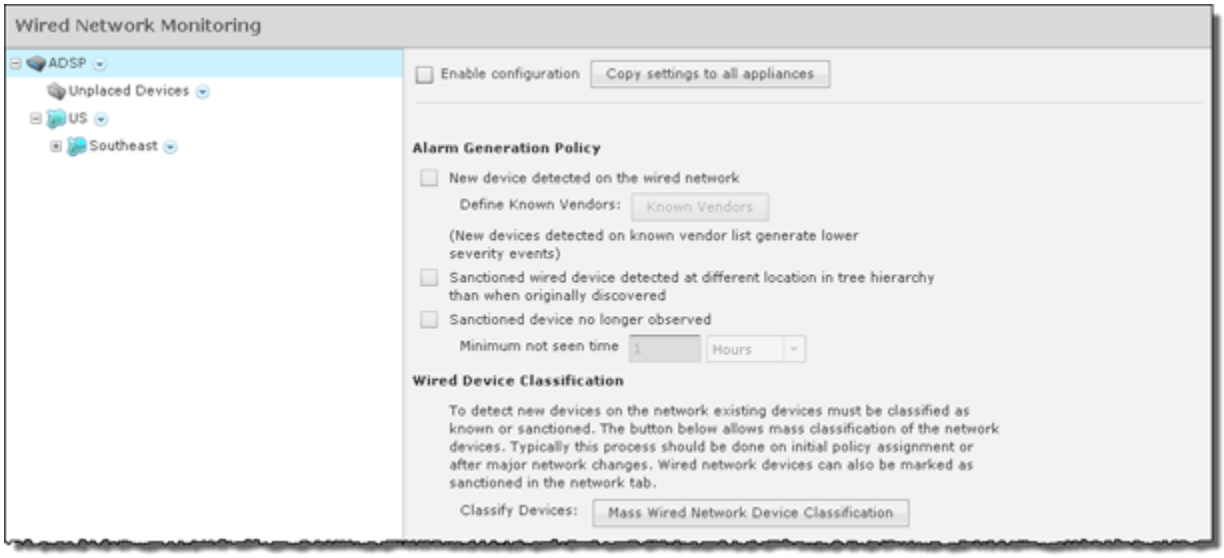
Security Profiles (also part of Appliance Platform) define the security configurations of sanctioned wireless clients on your wireless LAN. Refer to *Security Profiles* under the Appliance Platform.

Wired Network Monitoring

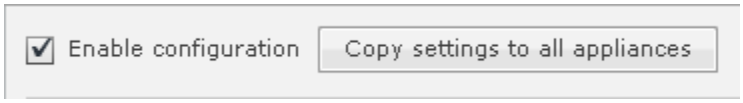
Wired Network Monitoring is used to monitor the wired network devices in your system. You can generate an alarm policy for your wired network by selecting any of the following conditions:

- 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.



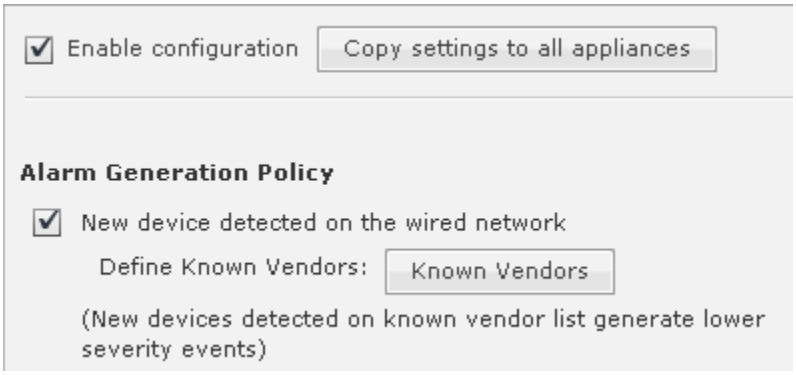
Then, if you have a level that needs to be monitored using different settings, you can monitor that level by selecting the network level from the network tree, overriding the inherited Wired Network

Monitoring (select **Override settings** radio button), and then defining different settings for Wired Network Monitoring.

Generate Alarm Policy for New Devices

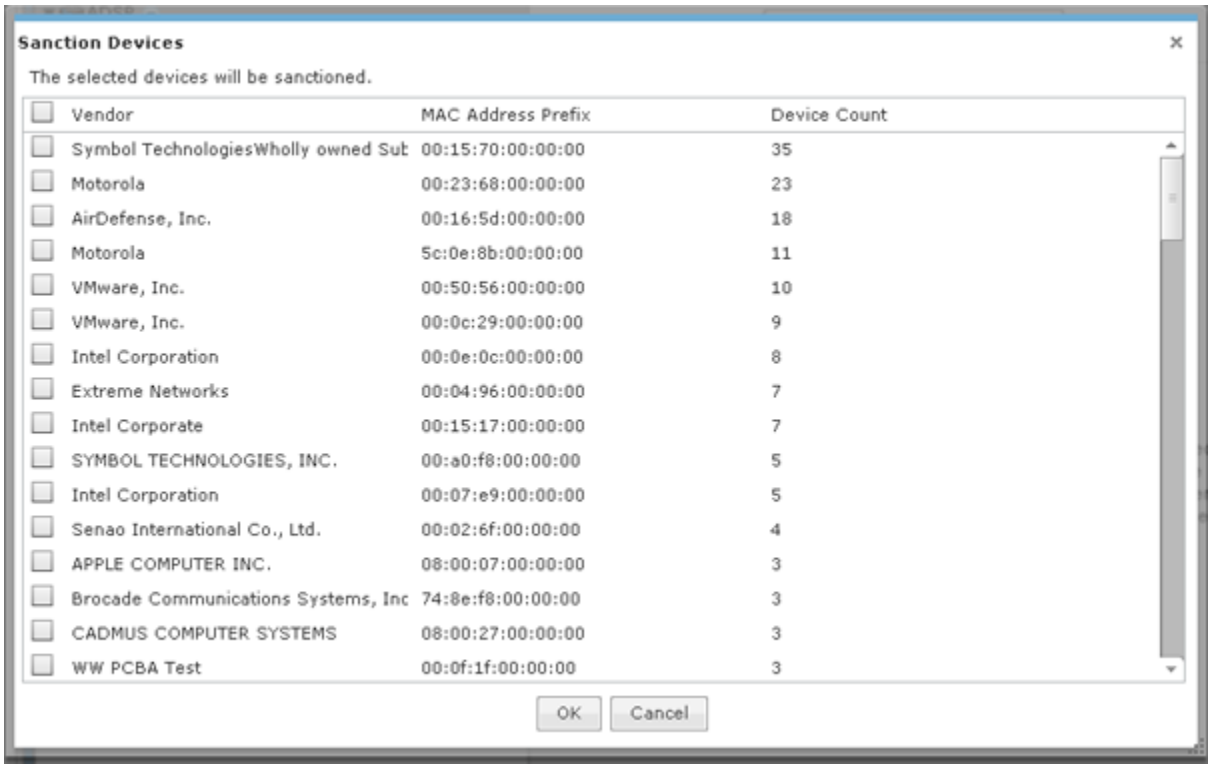
You should generate an alarm policy for new devices detected on your wired network by following these steps:

1 After enabling monitoring, select the New device detected on the wired network checkbox.



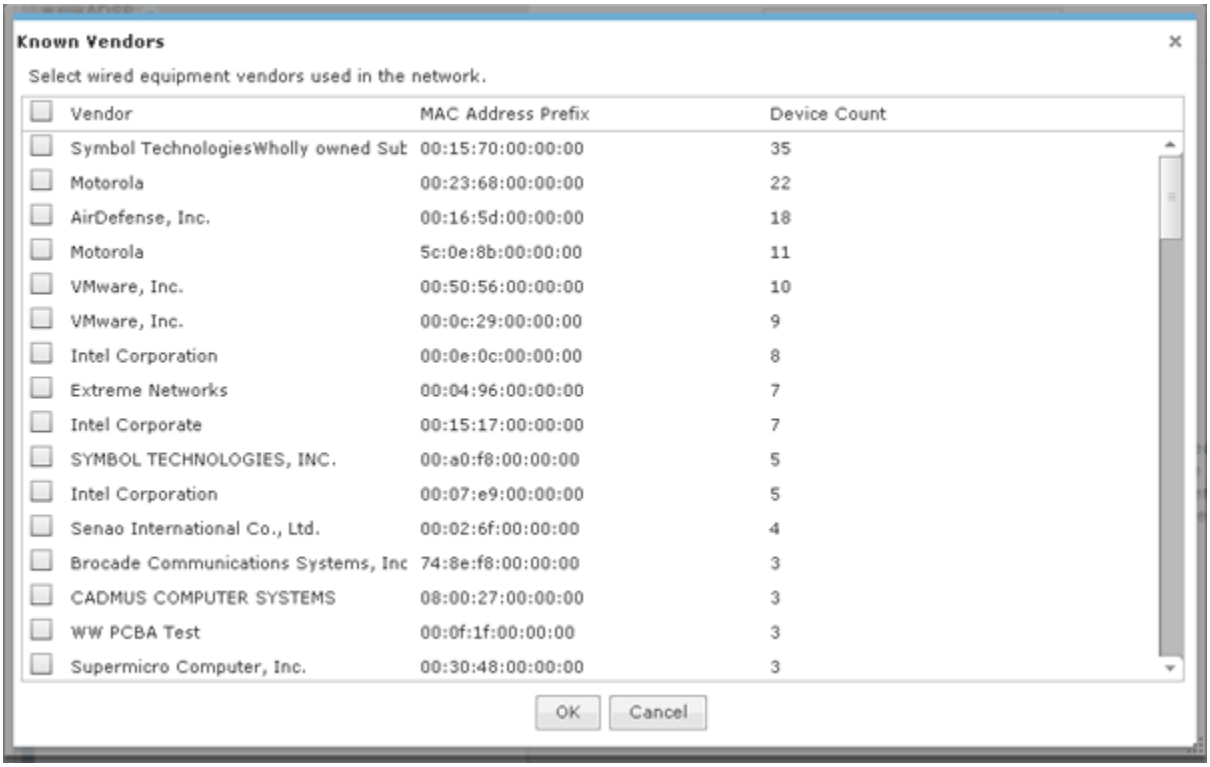
To authorize all detected devices for the first time, or at any major infrastructure change, click on the **Mass Wired Network Device Classification** button.

The **Sanction Devices** dialog opens.



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**.

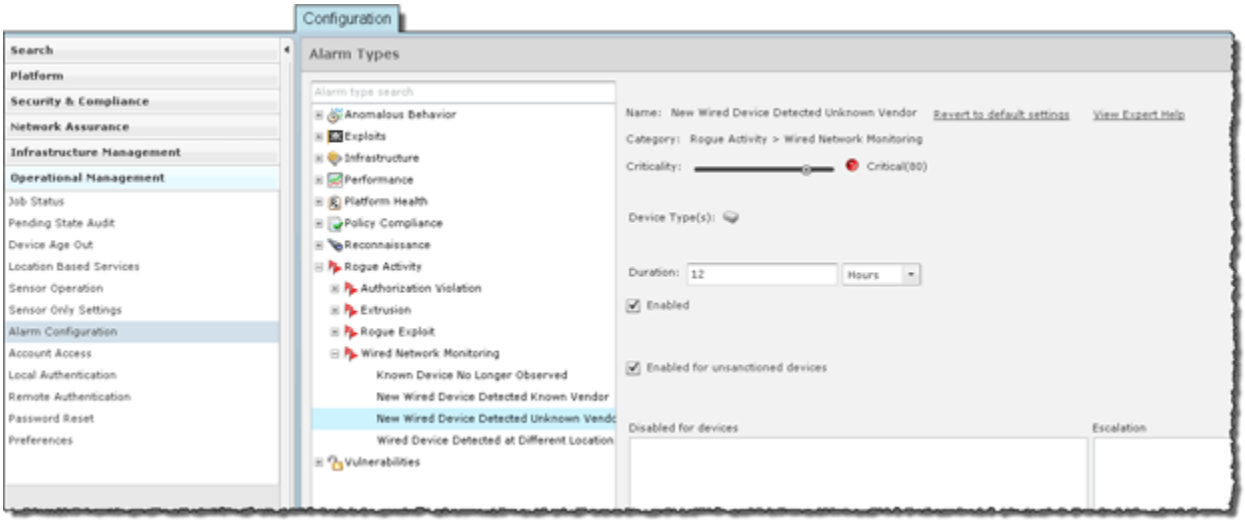
To have a finer control over alarms about new known vendor devices and new unknown vendor devices, you can utilize the Known Vendors classification tool. Click on the **Known Vendors** button to display a list of known vendors.



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

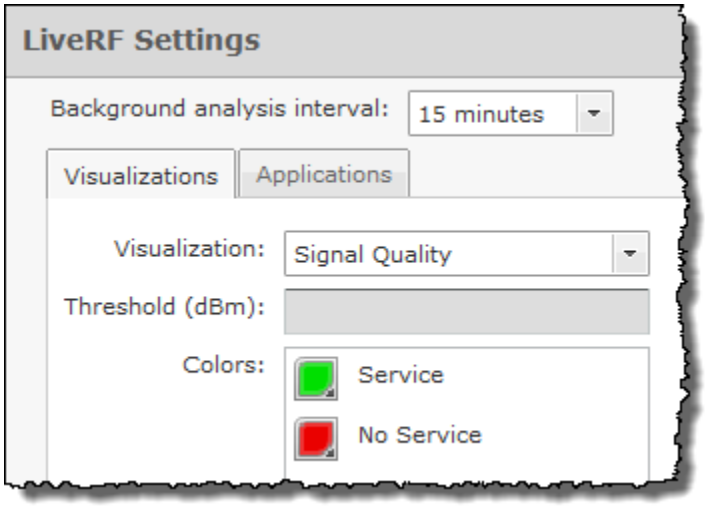
The Network Assurance category allows you to:

- 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).

Capabilities with a Central Engagement License

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.

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

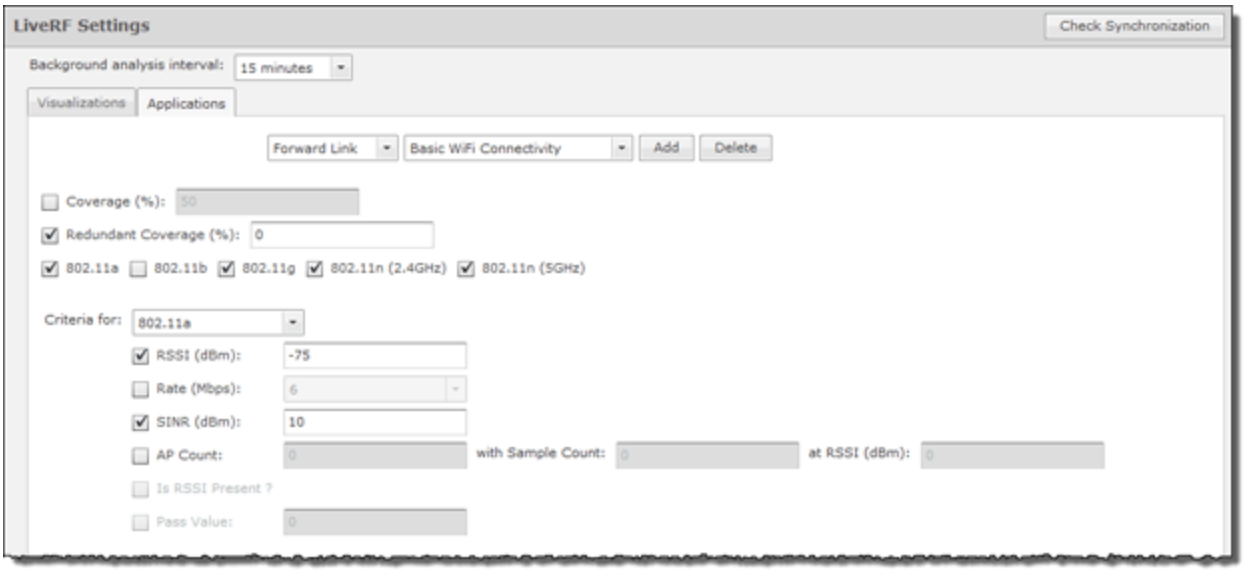
Visualization	Default Colors
Signal Coverage (Threshold inactive)	Above -10 dBm -20 to -10 dBm -30 to -20 dBm -40 to -30 dBm -50 to -40 dBm -60 to -50 dBm -70 to -60 dBm -80 to -70 dBm Below -80 dBm
Signal To Interference (Threshold inactive)	Above 30 25 to 30 20 to 25 15 to 20 10 to 15 5 to 10 Below 5

Visualization	Default Colors
Peak Data Rate (Threshold inactive)	Above 100 Mbps 54 to 100 Mbps 48 to 54 Mbps 36 to 48 Mbps 25 to 36 Mbps 18 to 25 Mbps 12 to 18 Mbps 11 to 12 Mbps 9 to 11 Mbps 6 to 9 Mbps 5.5 to 6 Mbps 2 to 5.5 Mbps 1 to 2 Mbps Below 1 Mbps
Noise (Threshold inactive)	Above -50 dBm -60 to -50 dBm -70 to -60 dBm -80 to -70 dBm -90 to -80 dBm Below -90 dBm

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.



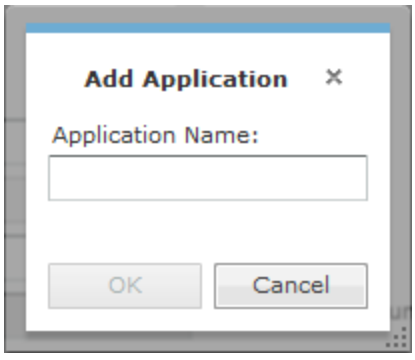
The default applications are:

- Basic Wi-Fi 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	Specifies the protocols that you want to use to consider your network is covered. The choices are: **802.11a**, **802.11b**, **802.11g**, **802.11n (2.4 GHz)**, and **802.11n (5Ghz)**. For every protocol you select, that protocol is added to the **Criteria for** drop-down menu. You can then select a protocol from the drop-down menu and select the following options to use with that protocol: • RSSI—When selected, specify the RSSI value in dBm that you consider acceptable for the selected protocol. • Rate—When selected, specify the rate that you consider acceptable for the selected protocol. • SINR—When selected, specify the SINR value in dBm that you consider acceptable for the selected protocol. • AP Count—When selected, specify the number of APs that you consider acceptable for the selected protocol. Also, specify an acceptable RSSI value for the APs.

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.

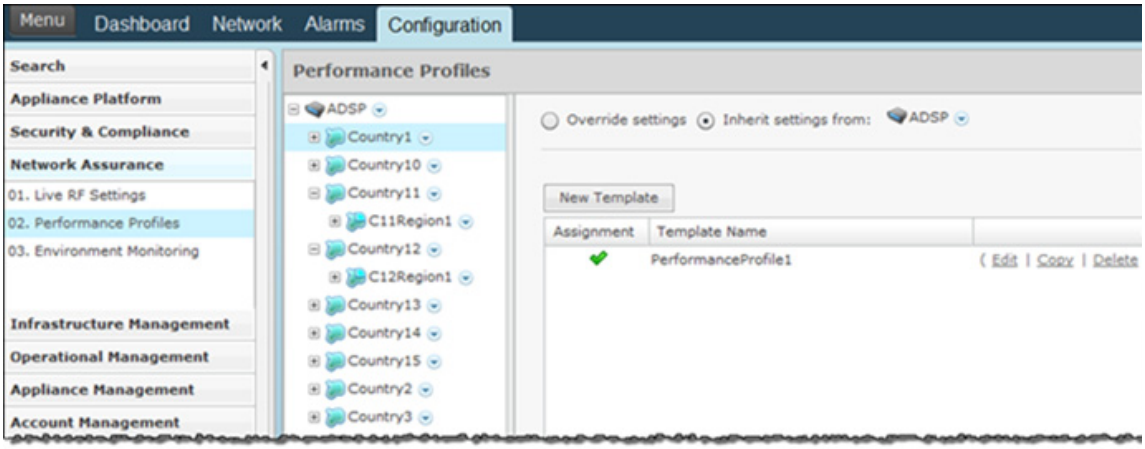
Performance Profiles

Performance Profiles are used to create network performance threshold policies for BSSs and wireless clients on your wireless LAN. When a Performance Profile is applied to your system, a performance alarm is generated if the performance thresholds for that profile are exceeded. 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.

View Performance Profiles

To access the Performance Profiles configuration screen, go to **Configuration** > **Network Assurance** > **Performance Profiles**. Existing Performance Profiles are displayed in the right column.



Edit Performance Profiles

Existing profiles are displayed in the table below the row of buttons.

You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link.

- To edit a profile, select (highlight) the Performance Profile. Click the **Edit** link and then make changes in any of the four tabs. Click **Save** to save your changes.
- To copy a profile, select (highlight) the Performance Profile, click the **Copy** link. Click **Save** and the copied profile appears.
- To delete a profile, select (highlight) the Performance Profile, click the **Delete** link.

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.

Add a New Performance Profile

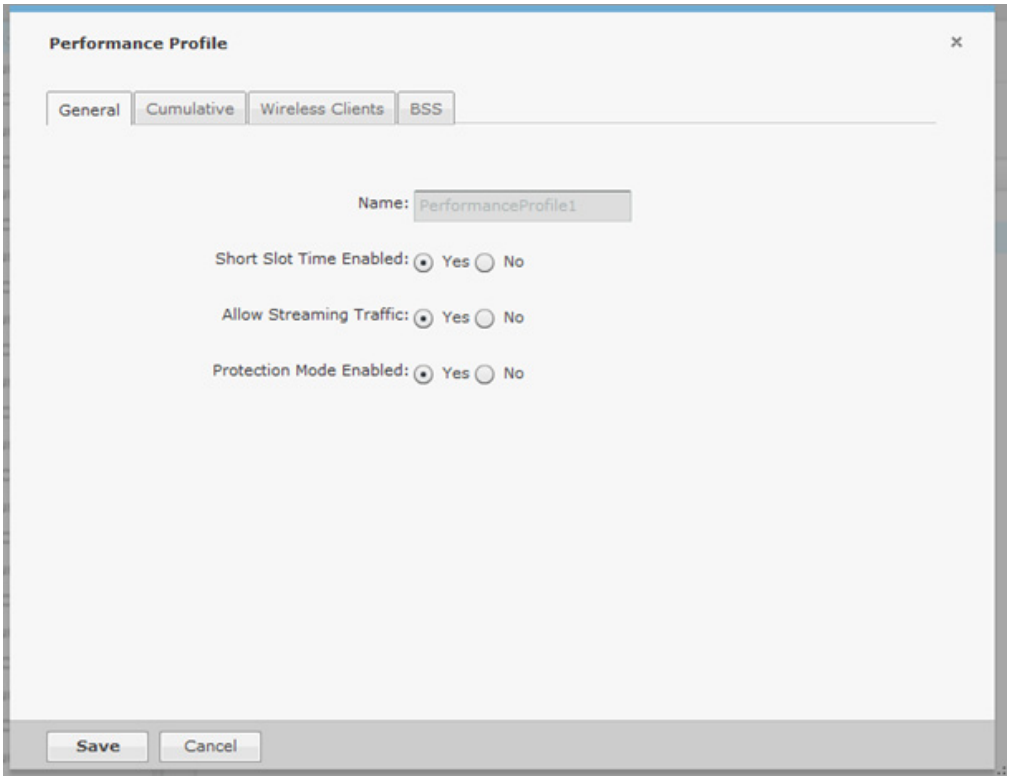
Click the **New Profile** button to add a new profile. Define your Performance Profile using the **General**, **Cumulative**, **Wireless Clients**, and **BSS** tabs. Once you have defined your Performance Profile, click **OK** to save your profile or **Cancel** to exit without saving the profile.

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 AP'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 AP'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.

General Tab

The General tab is where you name your Performance Profile and specify whether or not you want to use certain functions.



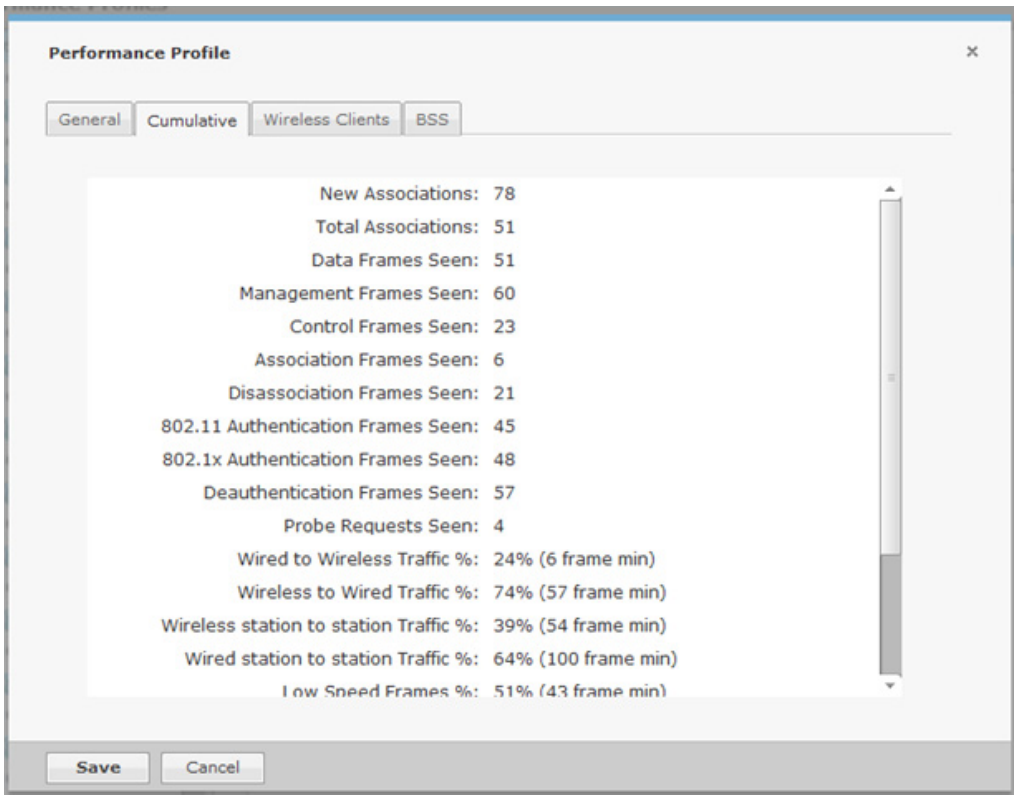
The Name field specifies the profile name. If you are adding or copying a Performance Profile, ADSP gives the profile the default name New_Performance_Profile. You should change the default name to one that is more appropriate to its function. Once you save your profile, you cannot change the name. The functions are:

Function	Description
Short Time Slot Enabled	Choose Yes 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. Choose No to disable.
Allow Streaming Traffic	Choose Yes 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. Choose No to disable. **Warning**: Streaming traffic applications consume large bandwidth and can adversely impact all other Wireless Clients connected on the Wireless LAN.
Protection Mode Enabled	Choose Yes 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. Choose No to disable. **Warning**: 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 AP'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	Enter the maximum number of new associations per minute ADSP will allow between a BSS and all Wireless Clients combined. Default = 20. 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. 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.
Total Associations	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. Default = 15.
Data Frames Seen	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. Default = 0.
Management Frames Seen	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. Default = 0.
Control Frames Seen	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. Default = 0.
Association Frames Seen	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. Default = 0.
Disassociation Frames Seen	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. Default = 0.
802.11 Authentication Frames Seen	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. Default = 0.

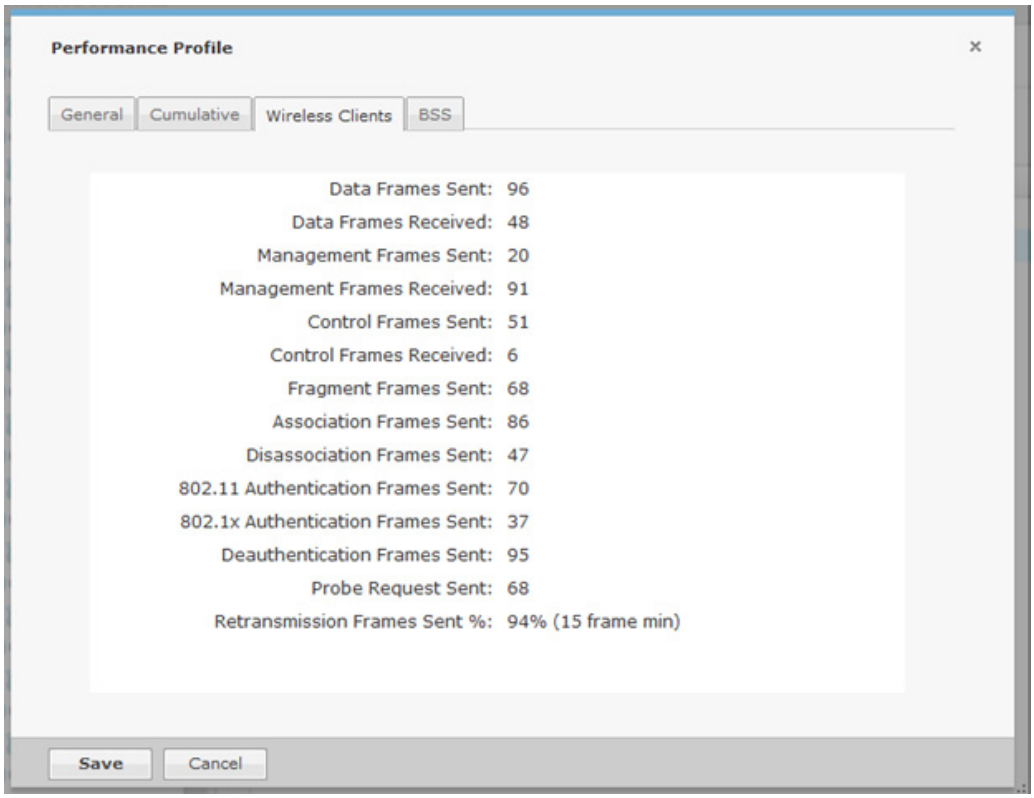
Threshold	Description
802.1x Authentication Frames Seen	Enter the maximum number of 802.1x authentication frames allowed to be transmitted or received from all Wireless Clients. If ADSP detects a greater number, it generates an alarm. Default = 0.
Deauthentication Frames Seen	Enter the maximum number 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.

Threshold	Description
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.
Layer 3 Broadcast Frames %	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. 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. Default = 0.
Retransmission Frames %	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. Default = 0.
PS Poll Frames Seen	An alarm is generated by a DOS attack using an excessive number of PS-POLL frames have been detected. 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.

Wireless Clients Tab

The Wireless Clients tab is where you assign BSS thresholds that apply to any individual Wireless Client. These thresholds 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:

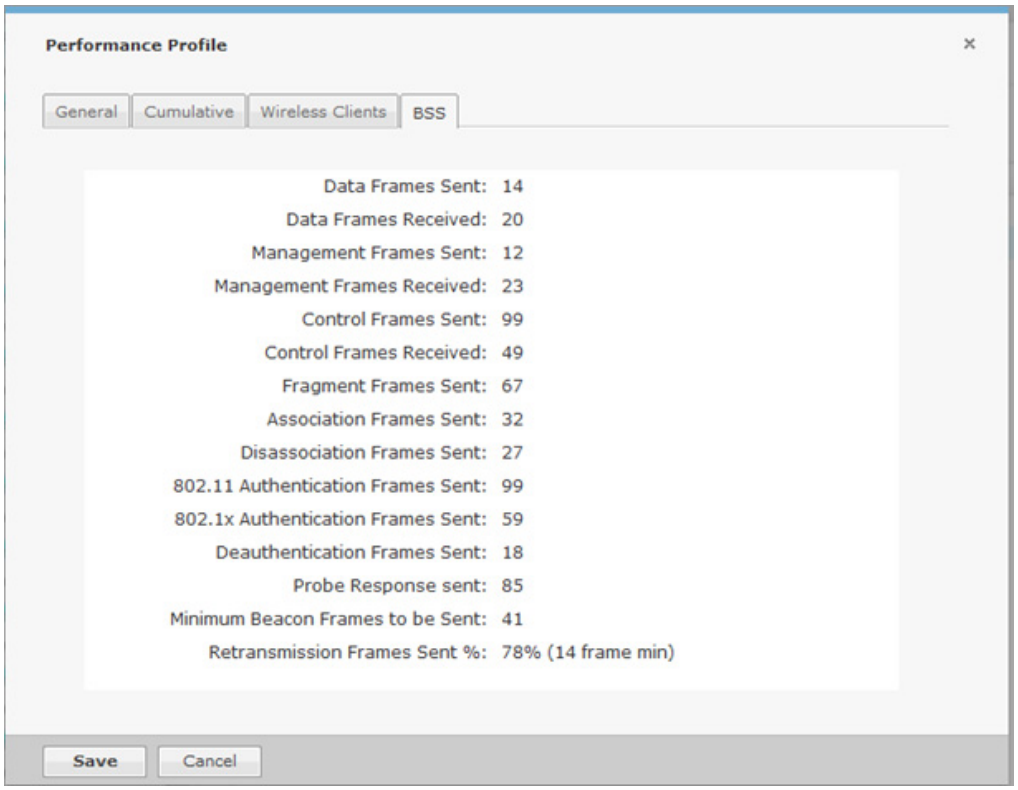
Threshold	Description
Traffic Sent %	Enter the maximum percentage of data per minute any Wireless Client is allowed transmit. If ADSP detects a greater number, it generates an alarm. Default = 30.
Traffic Received %	Enter the maximum percentage of data per minute any Wireless Client is allowed to receive. 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.

Threshold	Description
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.
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.

Threshold	Description
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 deauthentication 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.



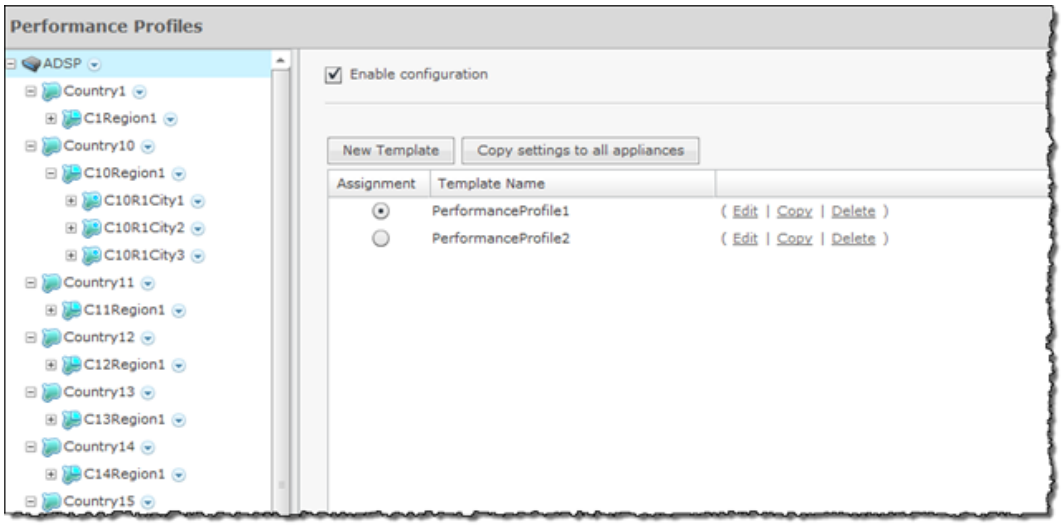
The thresholds are:

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.
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.

Threshold	Description
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.

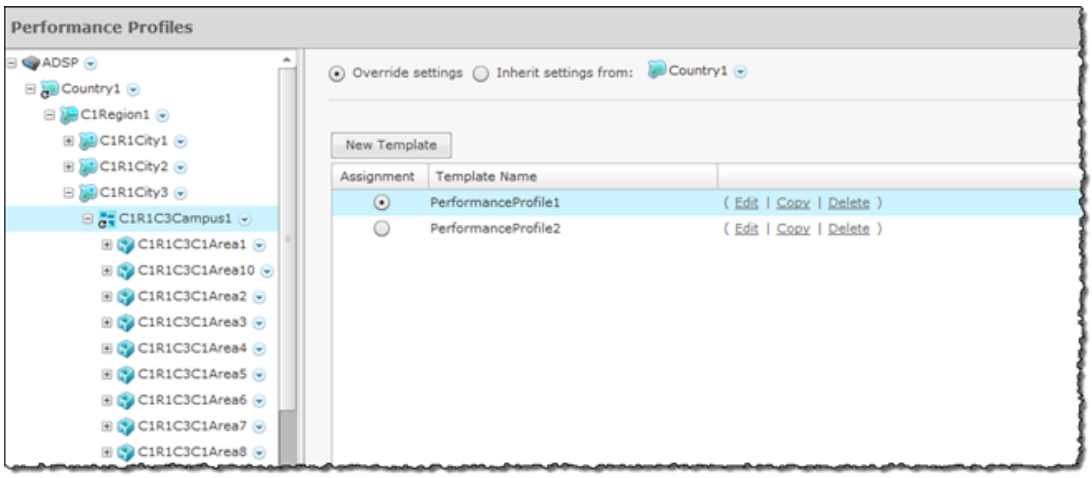
Apply a Performance Profile

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.

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.

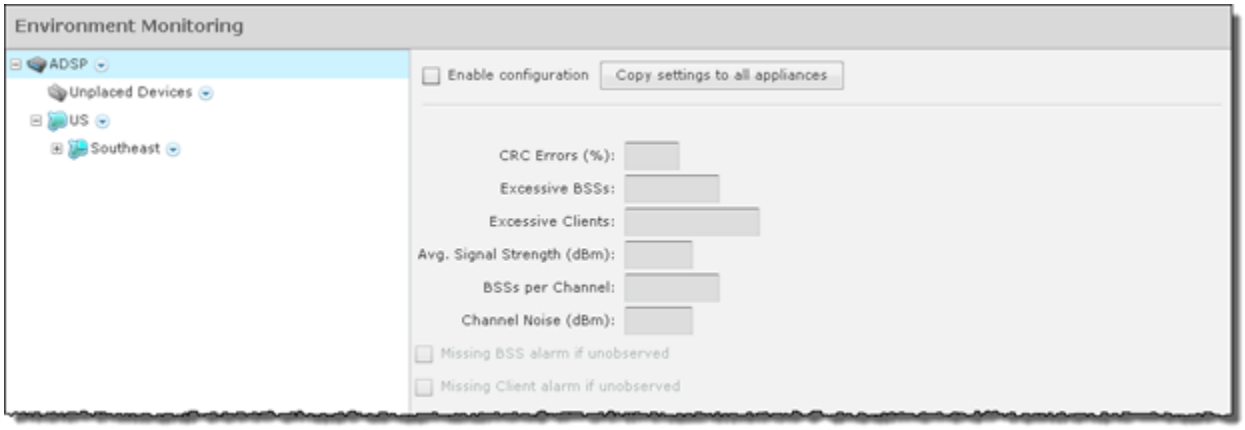


In this example, the **PerformanceProfile2** profile will be accessible to corporate-wide employees and guests while the **PerformanceProfile1** profile will be available employees and guests on Campus1 of the facilities.

Click the **Apply** button at the bottom of the screen 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.
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, and
- 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).

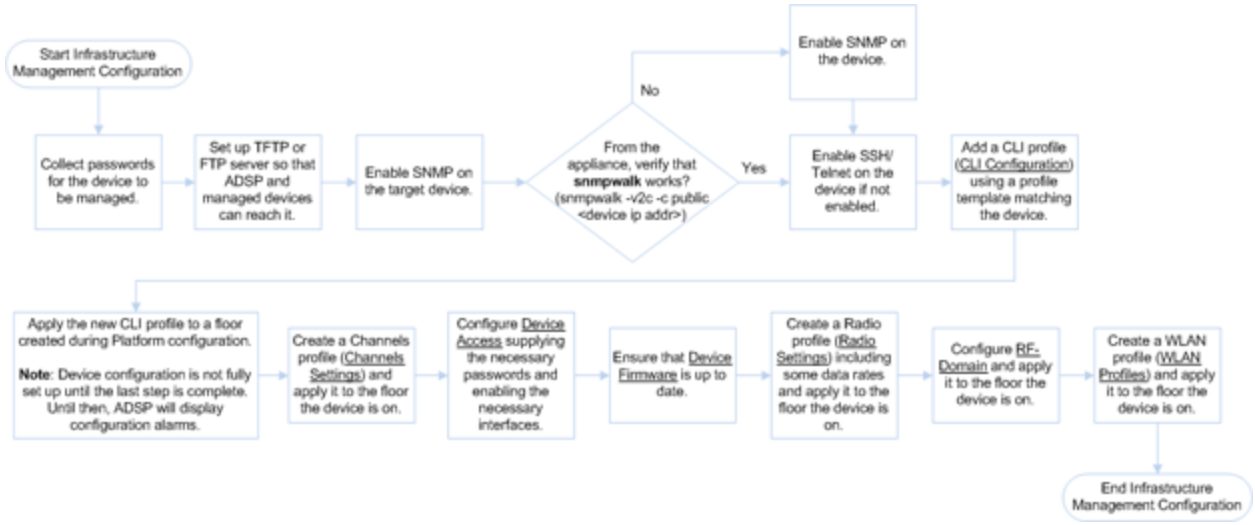
NOTE You must configure the Platform before configuring Infrastructure Management.

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.

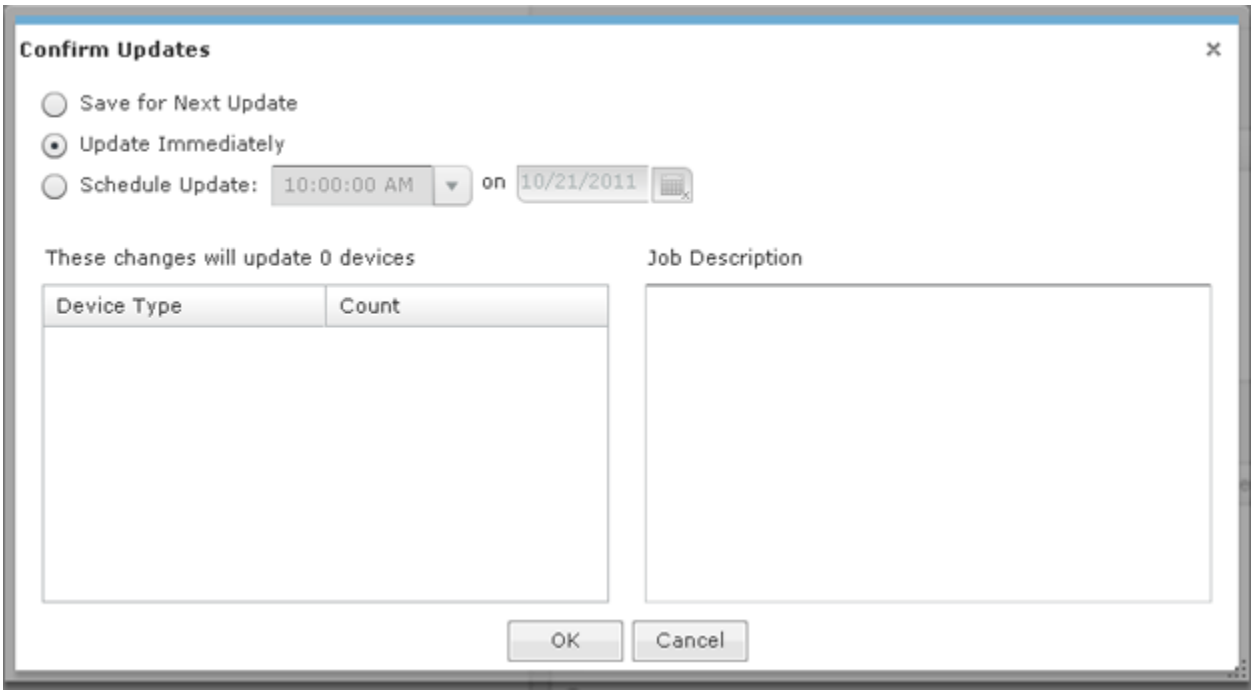
NOTE The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**–⊞ button to reveal the other levels.

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.



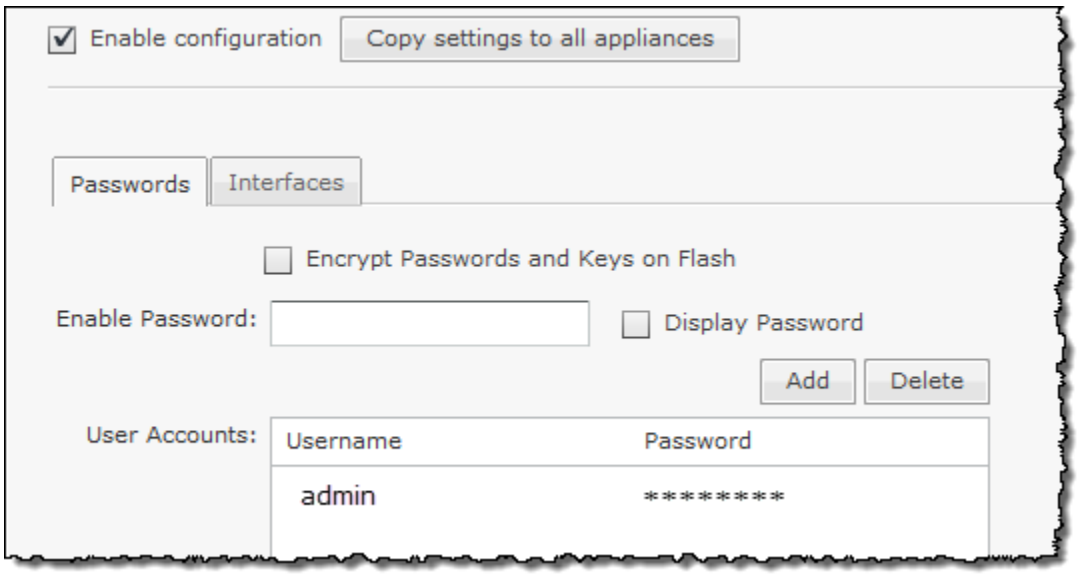
You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later. A list of device types along with the number of affected devices that will be updated 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.

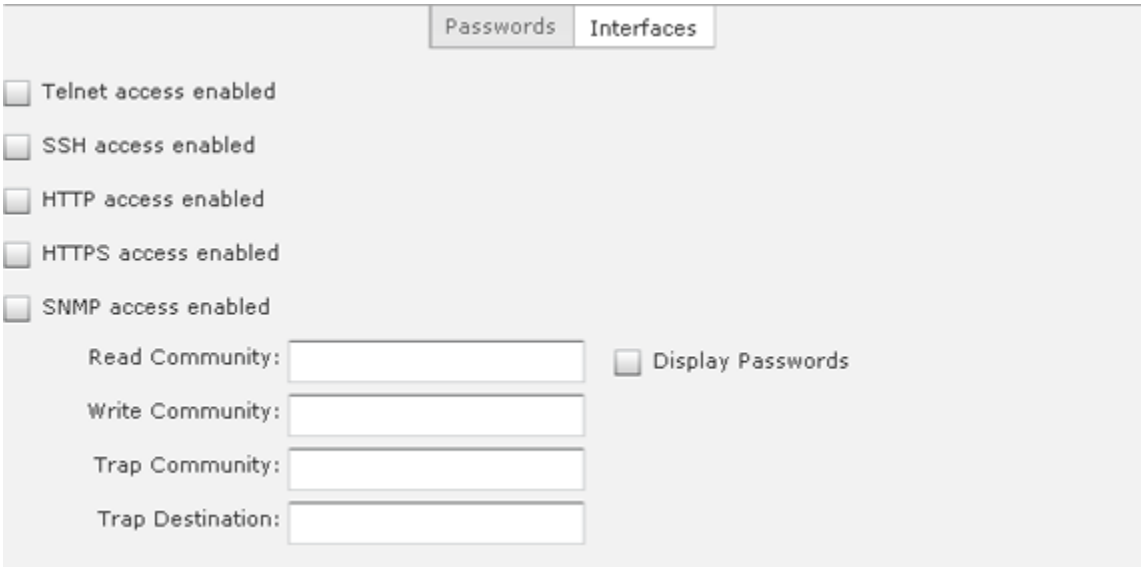


The following fields are available:

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

Interfaces Tab

The **Interfaces** tab is used to specify the interfaces that can be used to access devices.

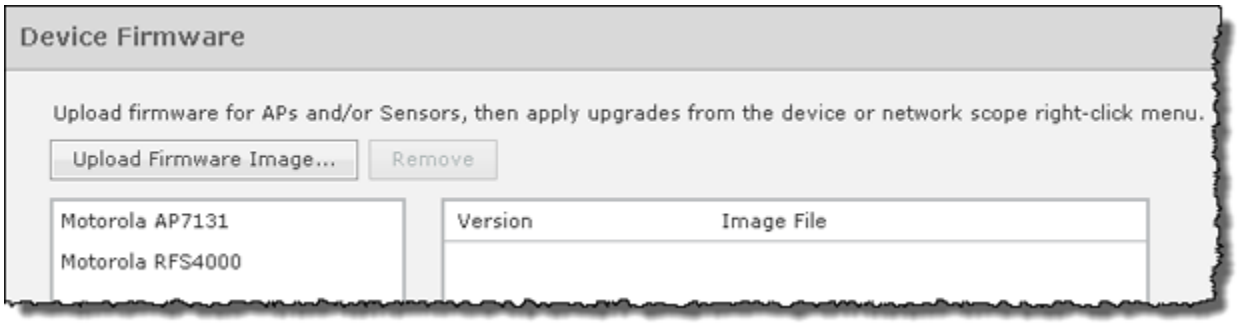


The following fields are available:

Field	Description
Telnet access enabled	Enables access to telnet.
SSH access enabled	Enables access to SSH.
HTTP access enabled	Enables access to HTTP.
HTTPS access enabled	Enables access to HTTPS.
SNMP access enabled	Enables access via SNMP. If you enable SNMP access, you must also specify the following passwords: • Read Community • Write Community • Trap Community • Trap Destination.

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.

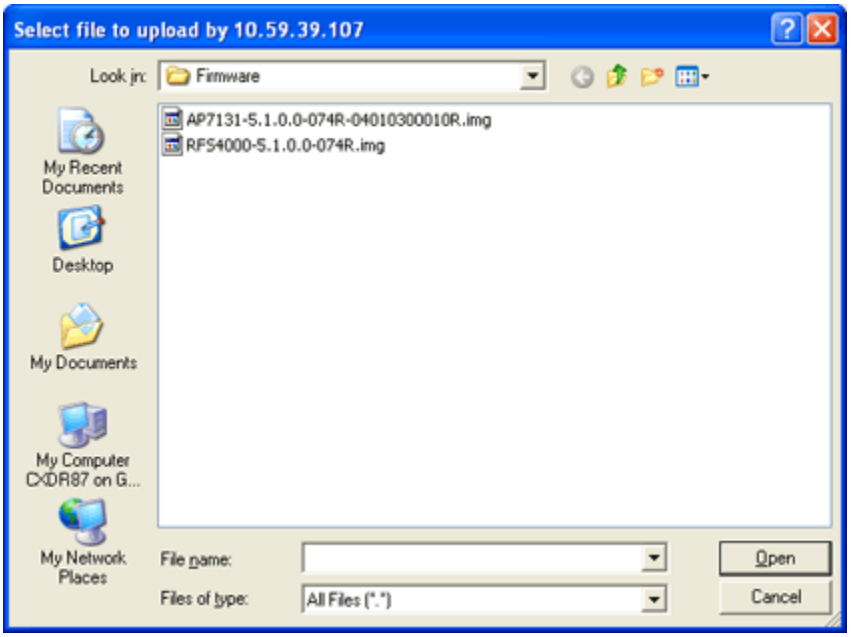


Uploaded firmware images are listed by device type, version number, and image file name. Just select (highlight) a device type to display the version number and image for that device.

Follow these steps to upload firmware:

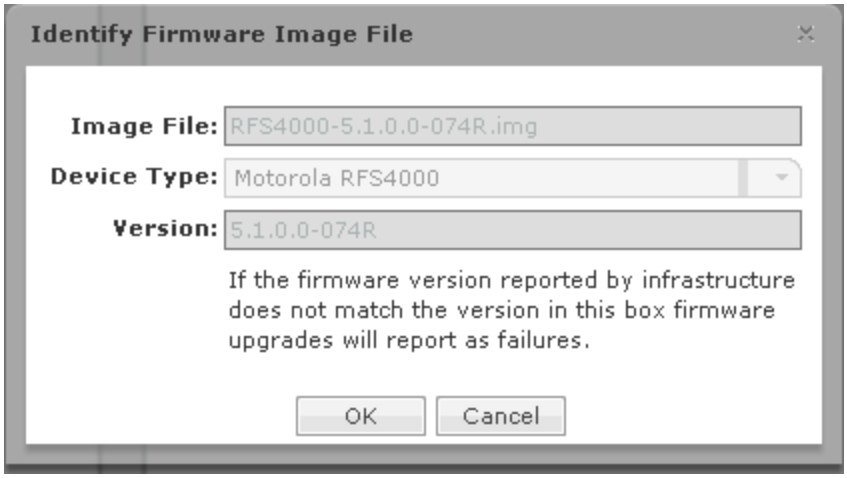
1 Click the **Upload Firmware Image** button. A browse window displays for you to select a firmware file.

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.)

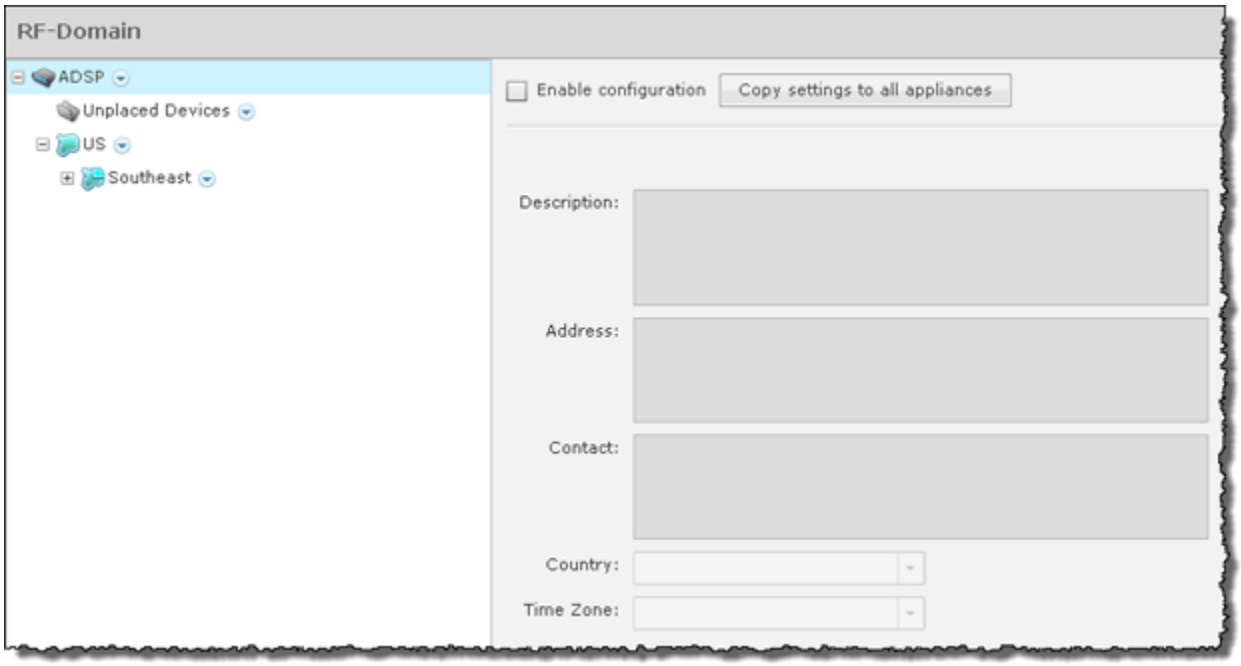
NOTE You must have a Central Management license in order to use the Check Synchronization feature.

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.



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:

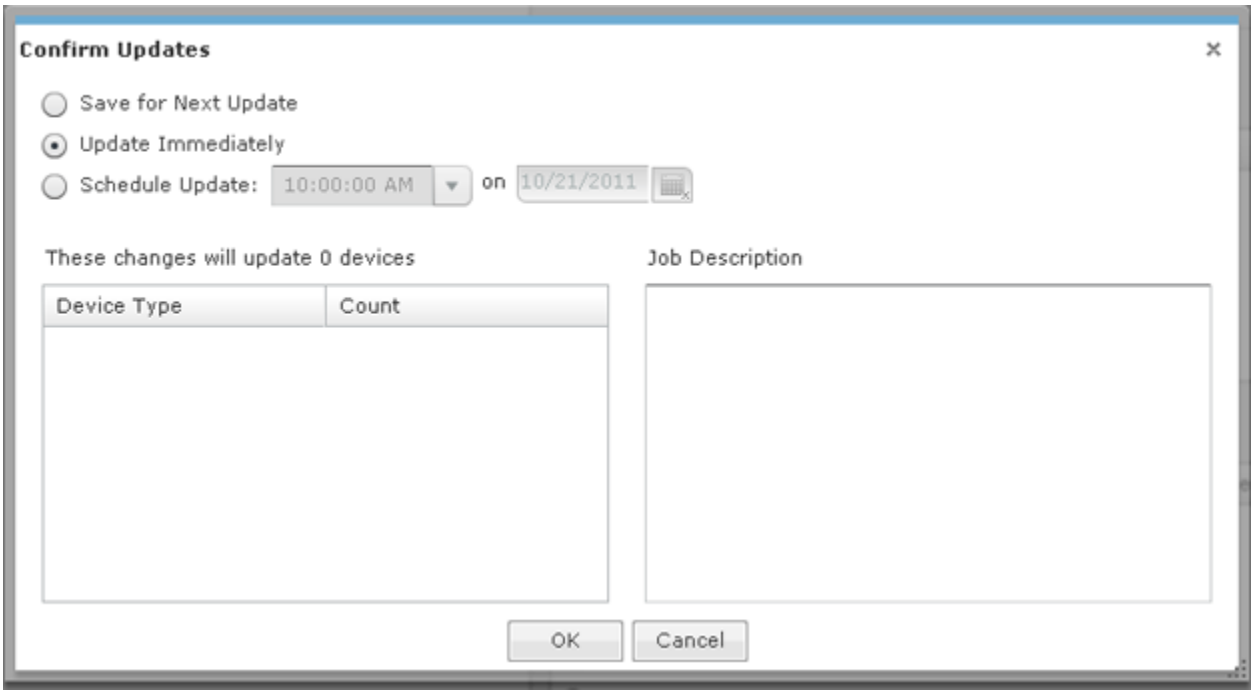
NOTE You should enter data for each field on one line with no carriage returns.

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.



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.

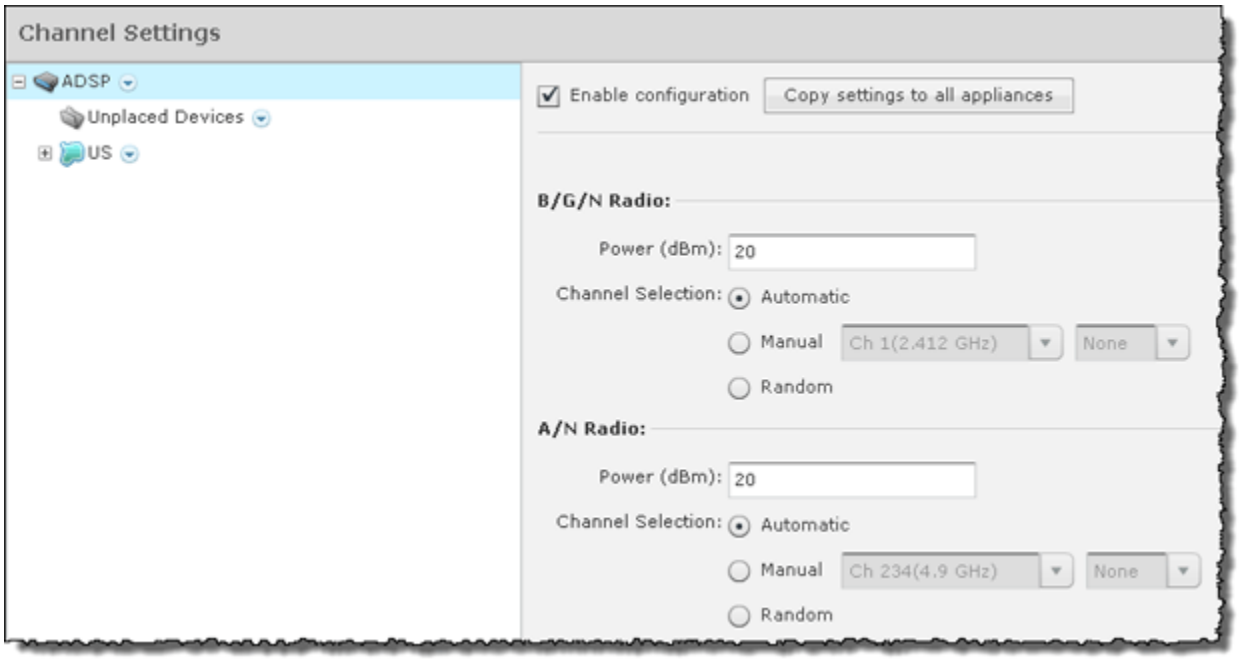
Click the **Reset** button to discard your changes.

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.



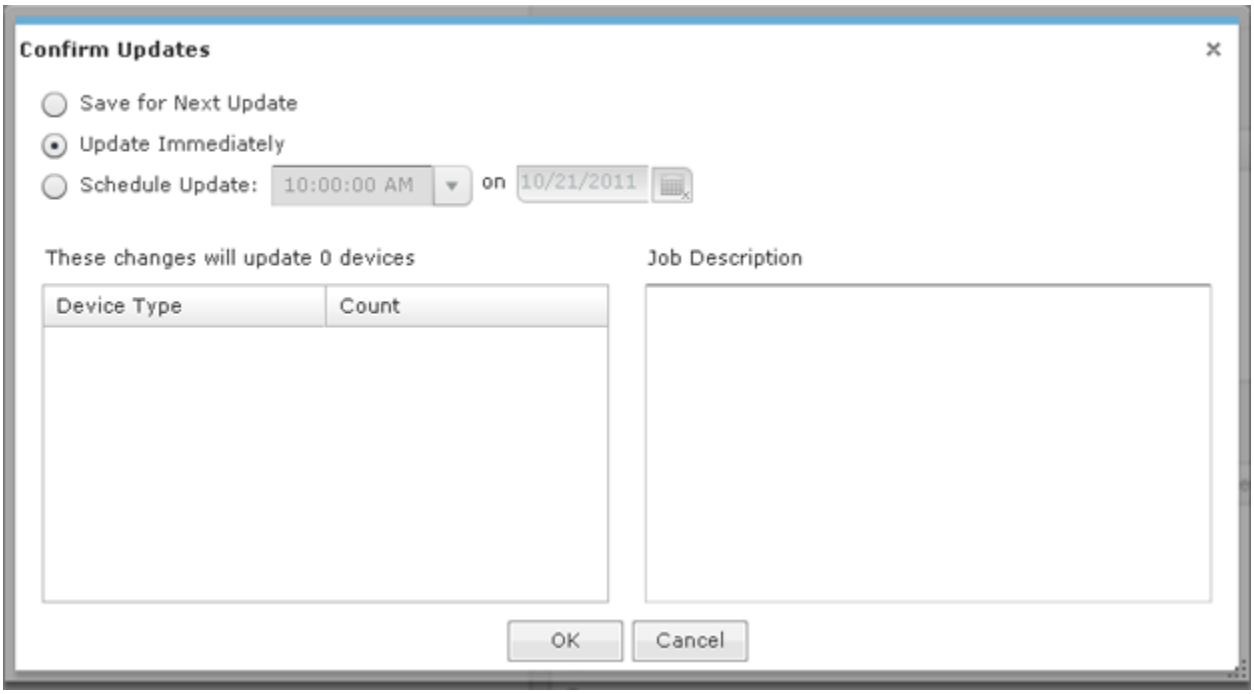
By default, Channel Settings are enabled, and are set for maximum power and automatic channel selection. The configuration fields for each radio are:

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: • Automatic—ADSP automatically sets which channel is used. • Manual—Select a channel to use from the drop-down menu and then select the extension range (none, upper, or lower). • Random—ADSP randomly sets the channel.

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.



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.

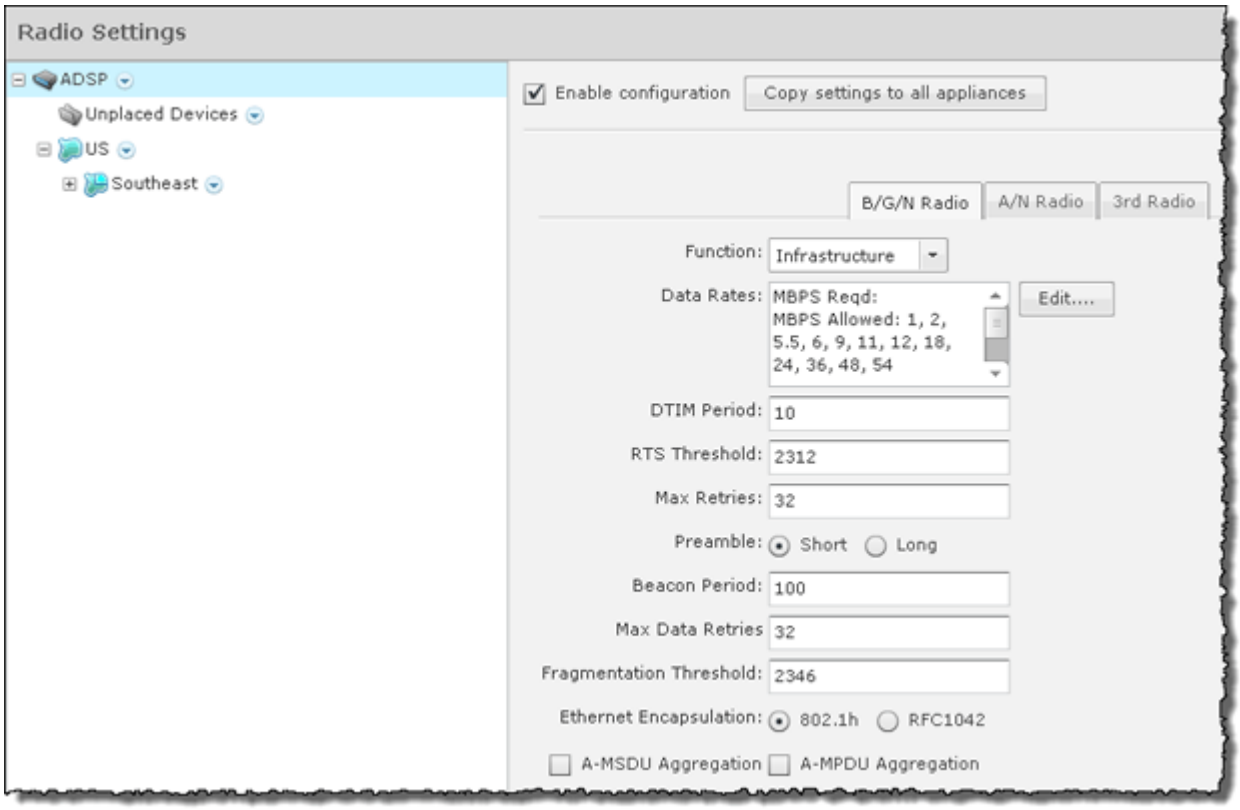
Radio Settings

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.

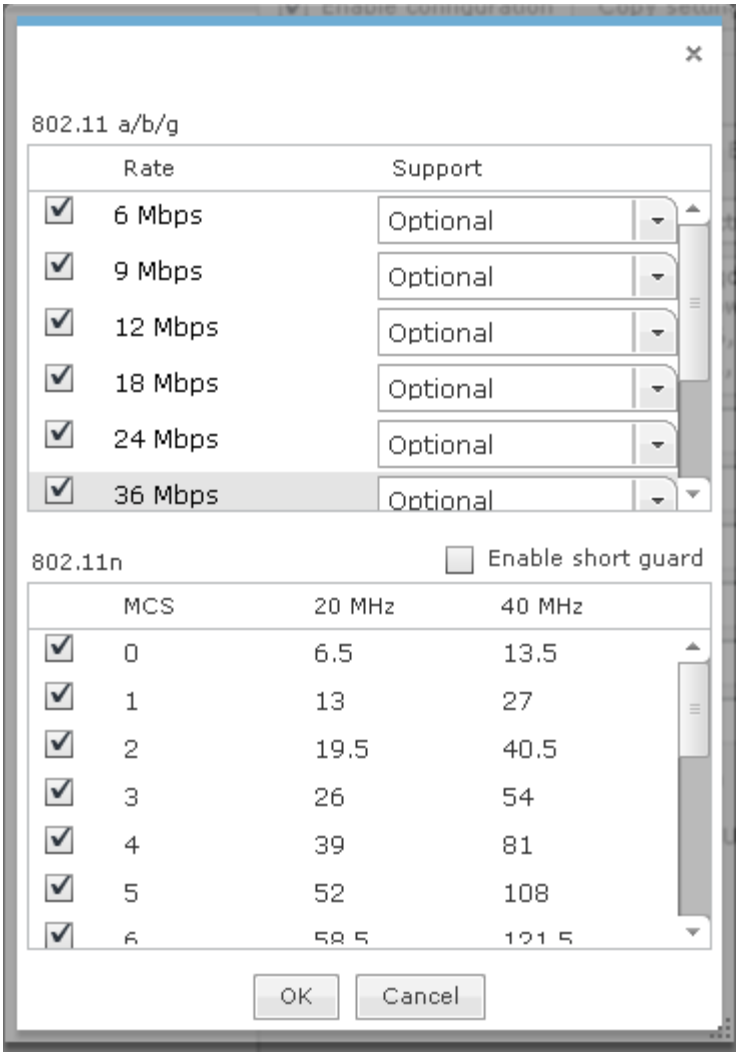


There are three possible radio configurations:

- 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	Sets the data rates for the radios. Click the **Edit** button to set the rates.  By default, all data rates are selected. 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. For 802.11n, select the MCSs that you want to support. Also, specify if you want to enable short guard.
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.

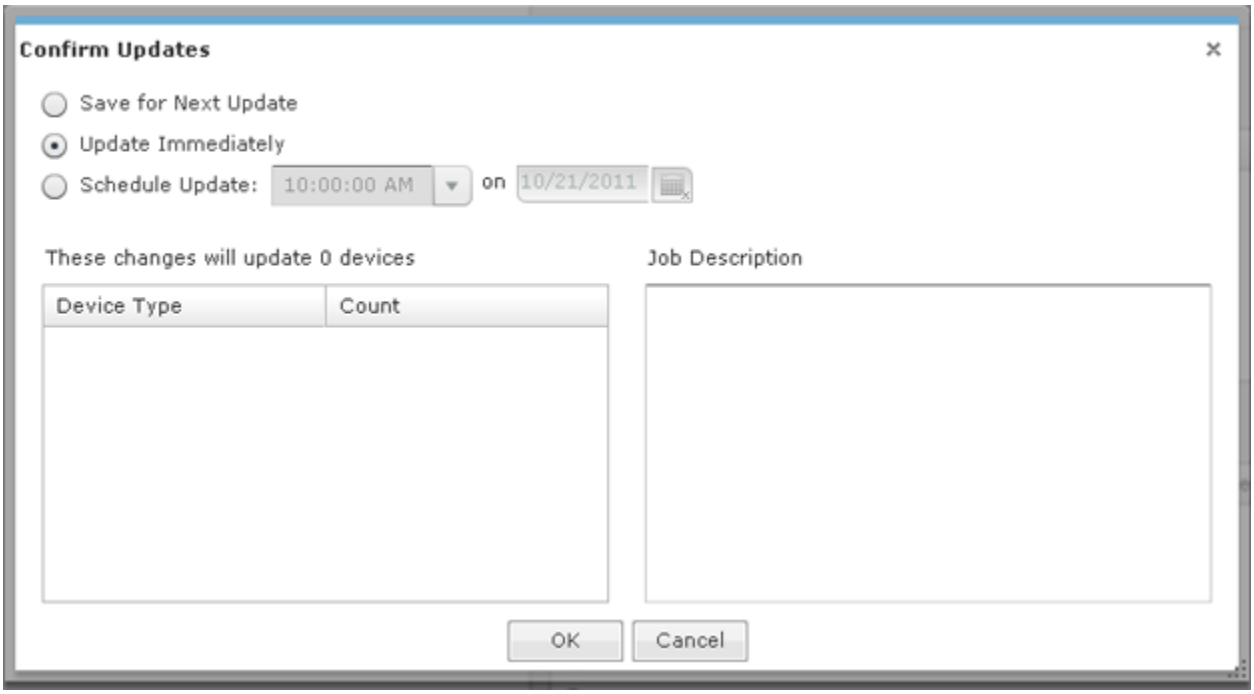
Field	Description
Max Retries	Specifies the supported number of RTS retries. This can be a value between 1 and 128. The default value is 32.
Preamble	Specifies that the preamble is short or long. This field is not available for A/N radios.
Beacon Period	Specifies the supported beacon interval (period) in kilo-microseconds. The default values 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.



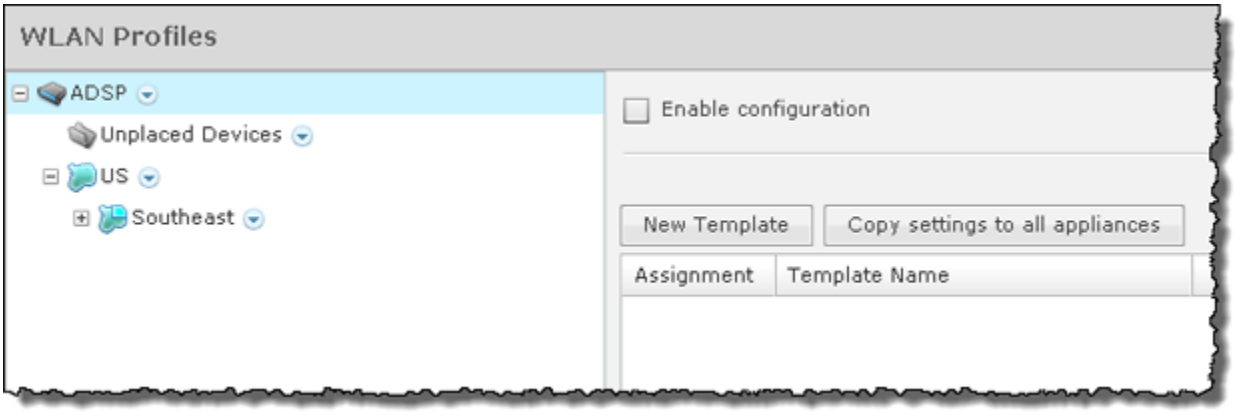
You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later. A list of device types along with the number of affected devices that will be updated 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

Use the WLAN Profiles feature to configure the WLAN settings for devices utilizing your network. To access WLAN profiles, go to **Configuration** > **Infrastructure Management** > **WLAN Profiles**.



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 Template Name column.

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.

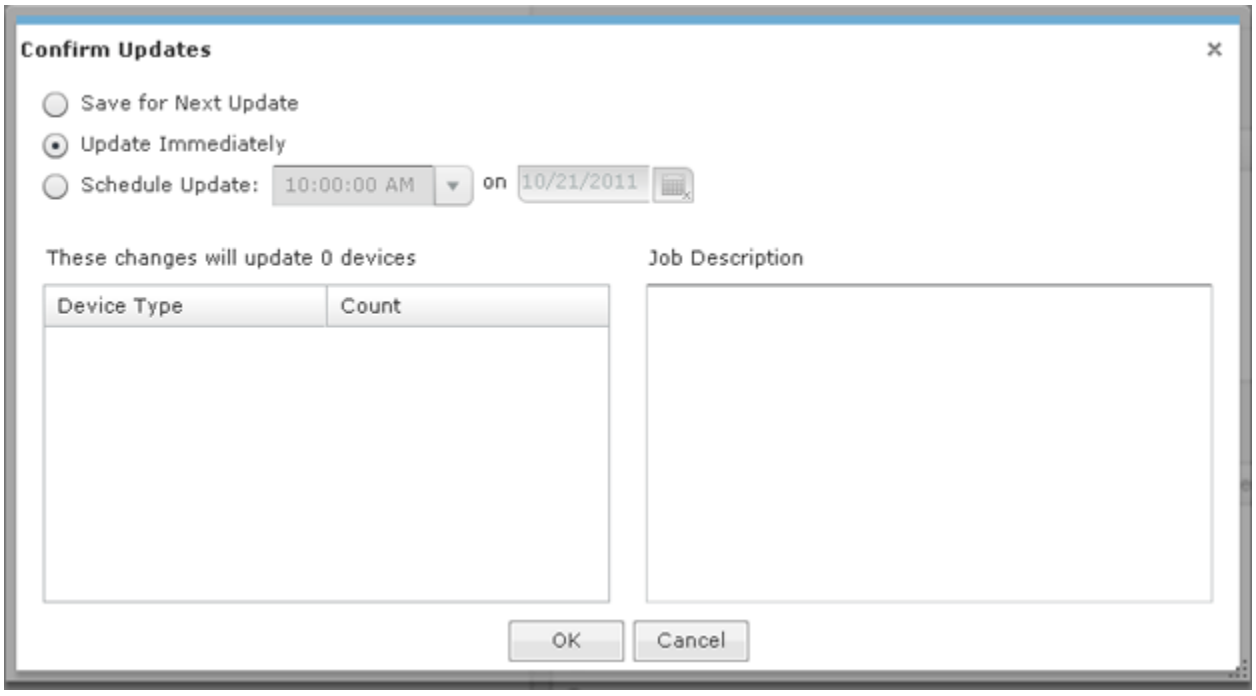
- General
- Security.

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 **Apply** 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.

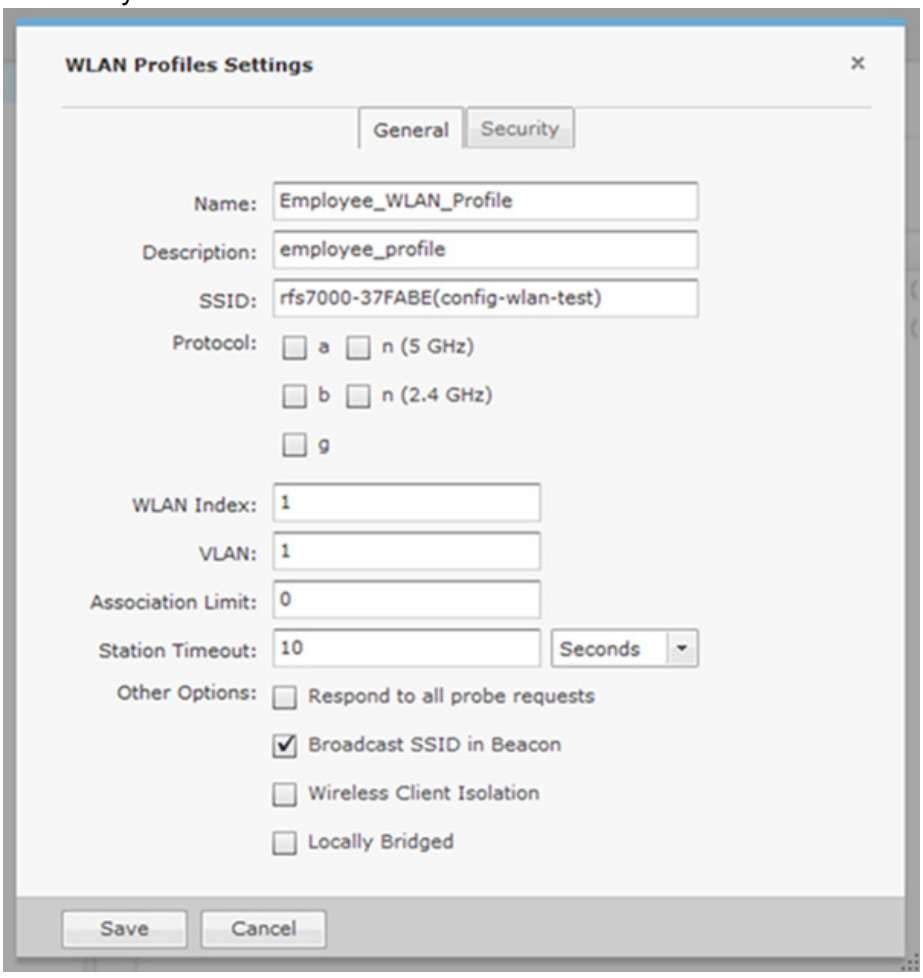
Click the **Reset** button to discard any additions (changes).

Add a WLAN 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.



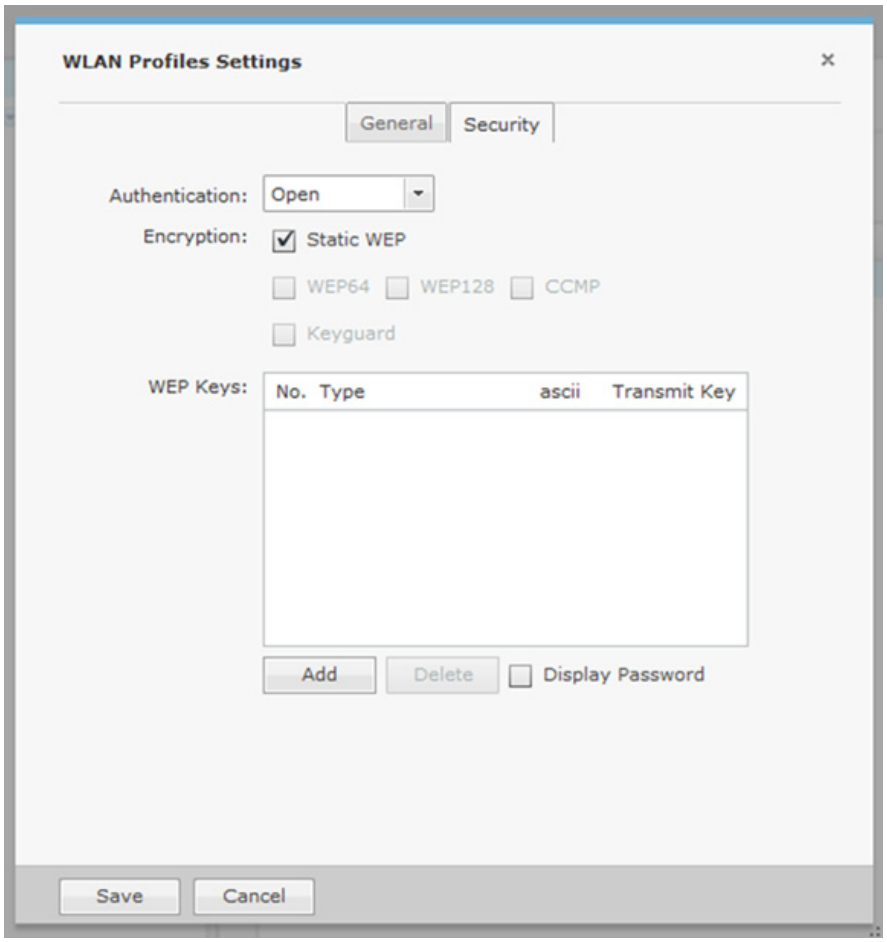
Complete the required fields as follows:

Field	Description
Name	Enter the profile name.
Description	Enter a short description of the profile.
SSID	Enter the Service Set Identifier (SSID) for devices.
Protocol	Enter the protocol that the device can use [a, b, g, n (2.4 GHz), or n (5 GHz)].
WLAN Index	Enter the order in which WLAN profiles will be assigned to a sensor. For example, WLAN1 can have index 4, WLAN2 can have index 2, WLAN3 can have index 1, and WLAN4 can have index 3.
VLAN	Enter the Virtual Local Area Network (VLAN) the device is authorized to use.
Association Limit	Enter the number of associations allowed per device.
Station Timeout	Enter the number of seconds or minutes that a device is allowed to become a sanctioned device.
Other Options	Specify which of the following options a device may perform: • Respond to all probe requests • Broadcast SSID in Beacon • Wireless Client Isolation • Locally Bridged.

Click **Save** when complete. The template is now displayed in the Template column.

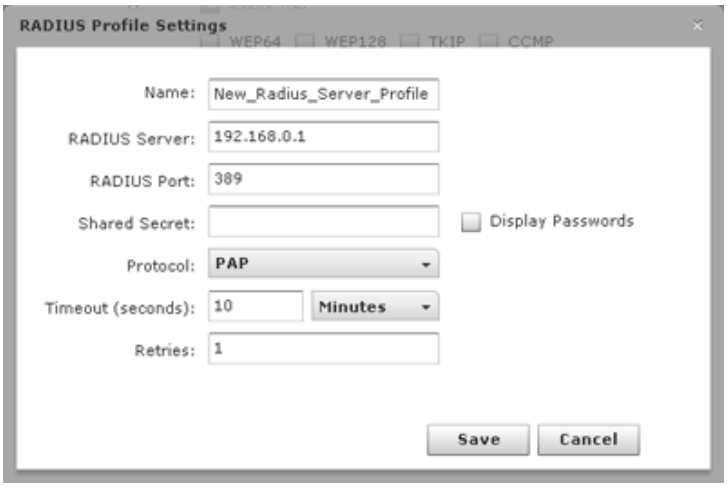
Security Tab

The Security tab is where you define the security aspects of your WLAN Profile.



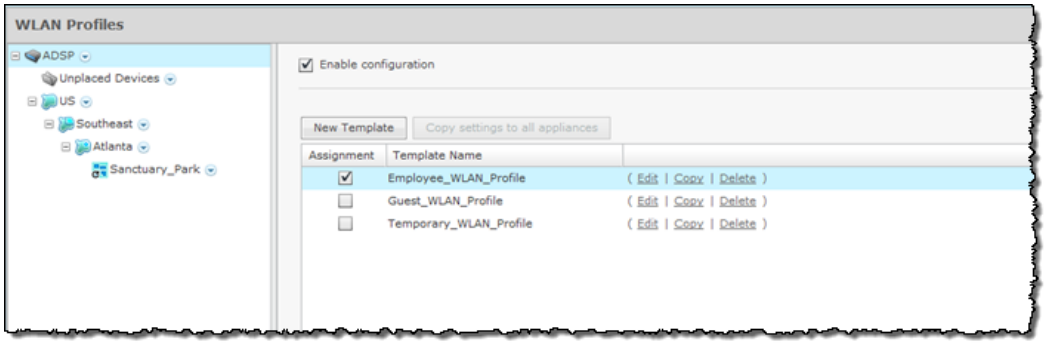
Complete the required fields as follows:

Field	Description
Authentication	Specify the type of authentication devices may use (Open, Shared, WPA, WPA PSK, WPA2, WPA2 PSK, or Legacy EAP).
Encryption	Specify the type of encryption devices may use (Static WEP, WEP64, WEP128, TKIP, CCMP, or Keyguard). You may select one or more encryption types.

Field	Description
WEP Keys	Specifies the WEP keys used to connect to the network. The WEP key may be ASCII or hexidecimal. You may also elect to transmit the WEP key. Check the **Display Passwords** checkbox to display the passwords in plain text. Use the **Add** button to add a new key or the **Delete** button to delete a key.
RADIUS Servers	NOTE This field is displayed only when the authentication method is WPA, WPA2, or Legacy EAP. Lists any RADIUS servers used in authentication. You can edit or delete a highlighted server by clicking the appropriate button. You can add new servers by clicking the **New Server** button which displays the following overlay:  You must supply the following information: • A name for the RADIUS Server Profile. • The IP address or host name of the RADIUS server. • The RADIUS server port used for communications. • The shared password of the RADIUS server. Select the **Display Password**s checkbox if you wish the password to be displayed while typing it. • A protocol selected from the drop-down menu (**PAP**, **CHAP**, **MSCHAP**, or **MSCHAPv2**). • A timeout value and a time interval selected from the drop-down menu (**Seconds** or **Minutes**). • The maximum number of retries to connect to the RADUIS server. Click **Save** to save the RADIUS server information.

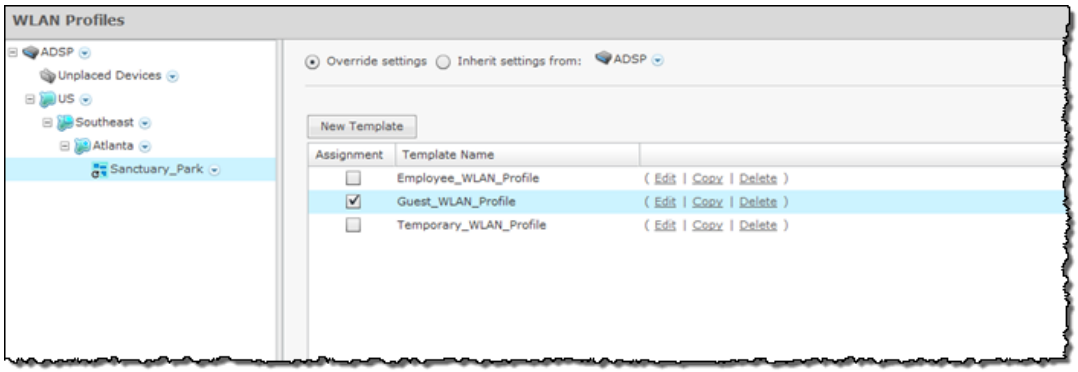
Apply a WLAN Profile

Once you have defined a WLAN Profile, to use it, you must apply it to your system. To apply a WLAN Profile, 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 is the **Employee_WLAN_Profile** and then for a special case you could override the WLAN Profile at the ADSP level and apply the **Guest_WLAN_Profile** to the 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 **Employee_WLAN_Profile** will only be accessible to corporate employees that have the proper credentials while the **Guest_WLAN-Profile** will be available to guests visiting the AirDefense facilities.

CLI Configuration

The Command Line Interface (CLI) for devices is a powerful tool that gives you direct access to APs and switches. Use the CLI commands to configure and control how devices interface with your network.

Using ADSP, you can create and update device configurations by revising the configuration files and their CLI command set. You can use the default CLI profiles (configuration templates) or change the profiles 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 APs and switches. The following devices are currently supported:

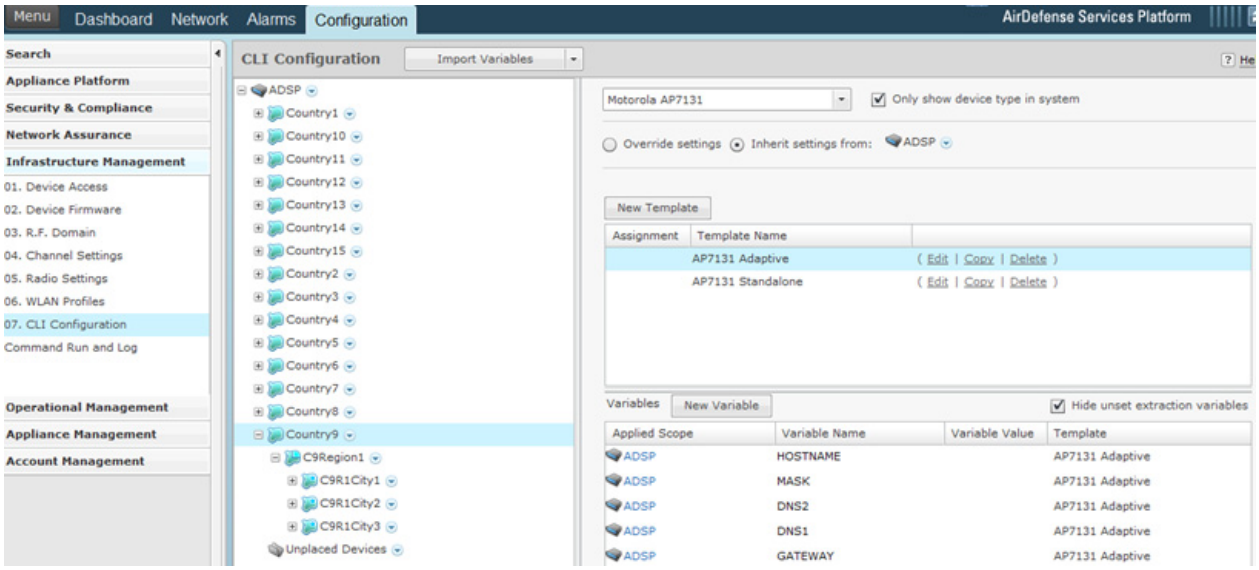
- Alcatel AL v5.x
- Aruba Aruba600
- Brocade BR v5.x
- Brocade BR51X1
- Brocade BR71X1
- Brocade BRX000
- Cisco Autonomous 12x0/11x0
- Extreme Networks AP35X0
- Extreme Networks AP47X0
- Extreme Networks EX v5.x
- Extreme Networks WM3X00
- AP 6511
- AP 621, AP 6521
- AP 7131, AP 7161, AP 7181
- AP 650, AP 6532
- AP 622, AP 6522, AP 6562
- AP 7522, AP 7532
- AP 8122, AP 8132, AP 8163
- AP 8232 (with 3rd radio sensor module only)
- CB3000
- RFSX000
- WiNG v5.x

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.

Add a New CLI Profile

Using ADSP, you can create and update device configurations by revising the configuration files and their CLI command set. You can use the default CLI profiles (configuration templates) or change the profiles 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 APs and switches.To create a new profile:

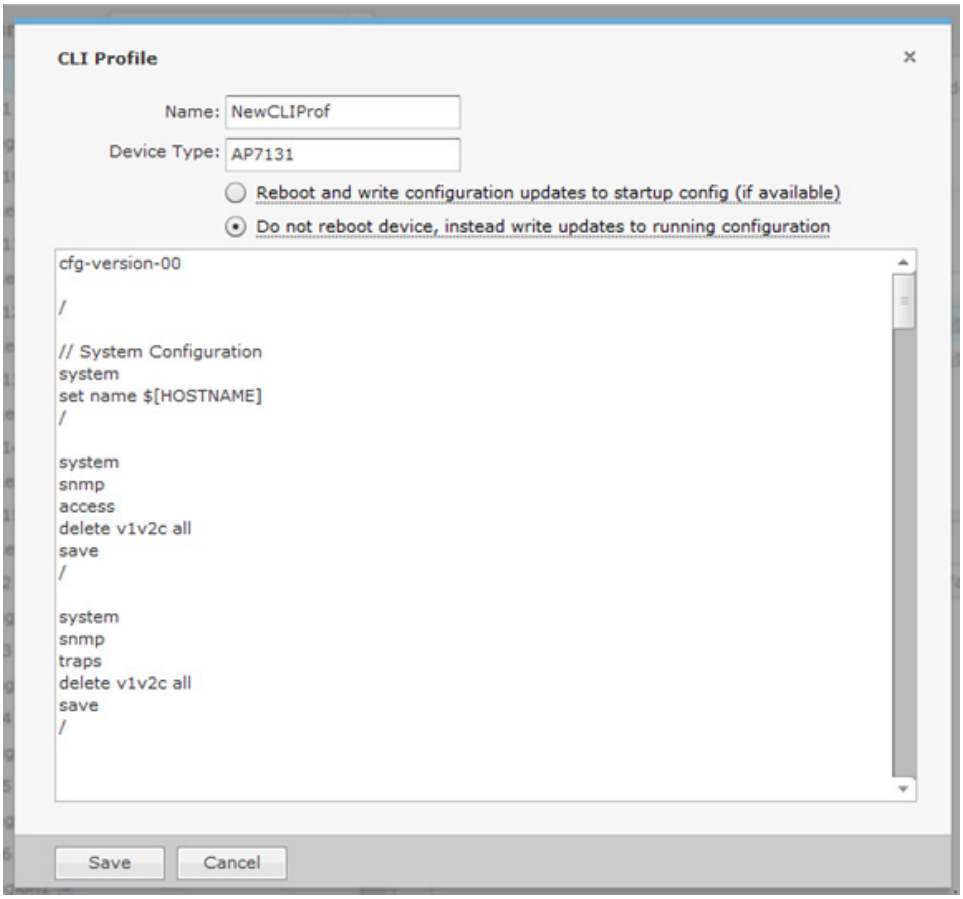
1 Select one of the supported CLI configurations from the CLI Configuration drop-down menu. The selected profile is accessed.



✓ NOTE You can reduce the list of supported devices to only the devices in your system by selecting the **Only show device type in system** checkbox.

2 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 the **Override settings** radio button.

3 Click **New Template**. The template for the selected CLI Profile is displayed. In the following image, the AP7131 template is displayed.



4 Enter a name for the profile.

5 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.

6 Update the CLI commands to match your criteria (see *CLI Commands*).

7 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**).

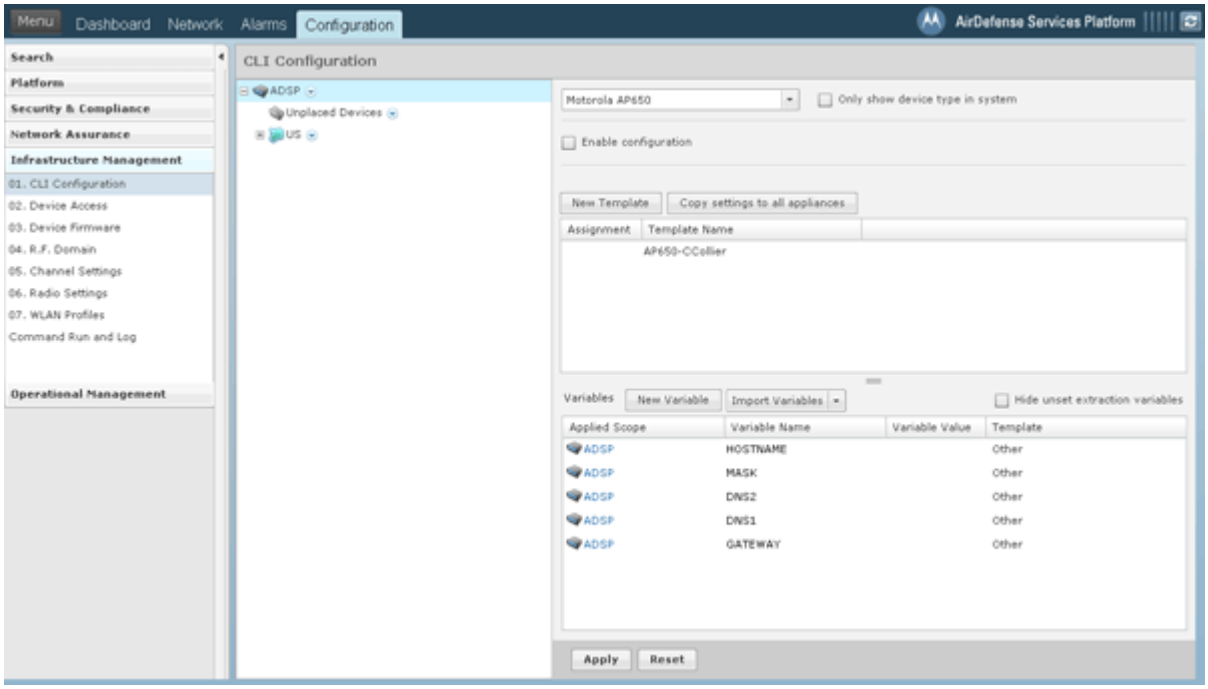
Apply a CLI Profile

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 are displayed in the list of templates.



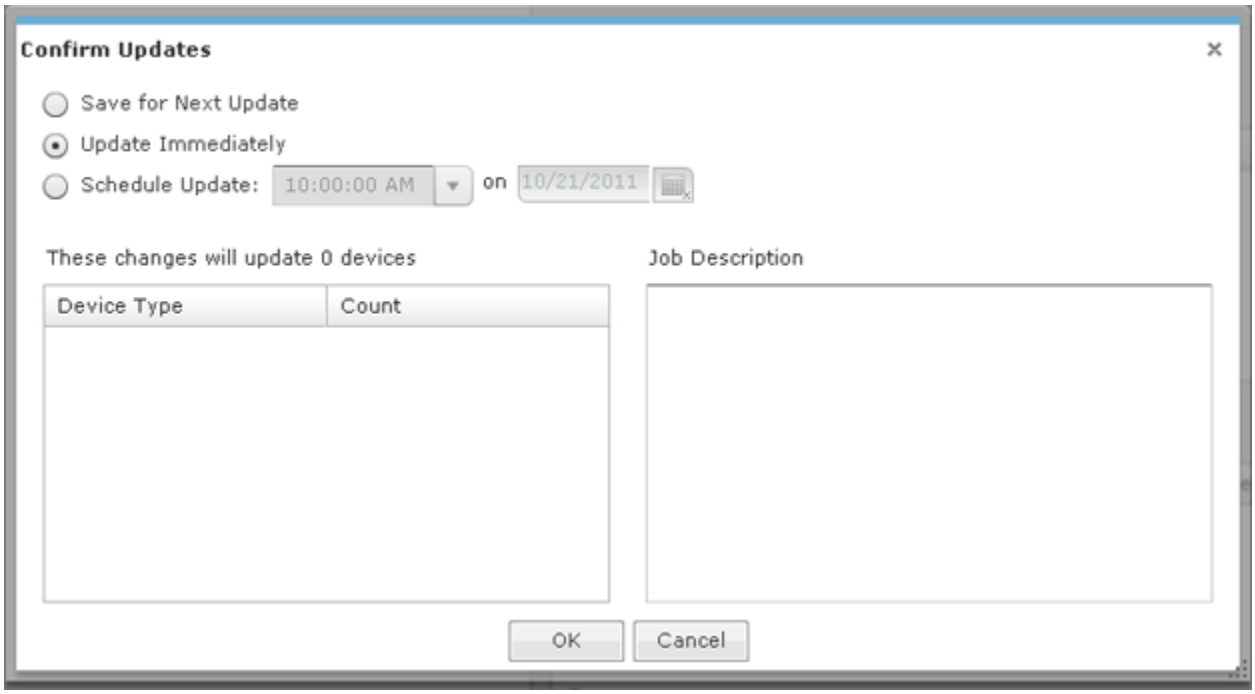
2 To apply a profile:

- To apply a profile at the appliance level in the configuration column and then select the **Enable configuration** checkbox.
- To apply a profile at a lower network level (such as Region), select the appropriate level and select the **Override settings** radio button.
- To inherit settings, select the **Inherit settings** radio button and select the appropriate appliance.

3 Select the profile from the list of profiles.

4 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.



The device type and the total count of affected devices are displayed.

5 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.

6 You may optionally enter a job description.

7 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! Any invalid command that is present in your network could disable a device.

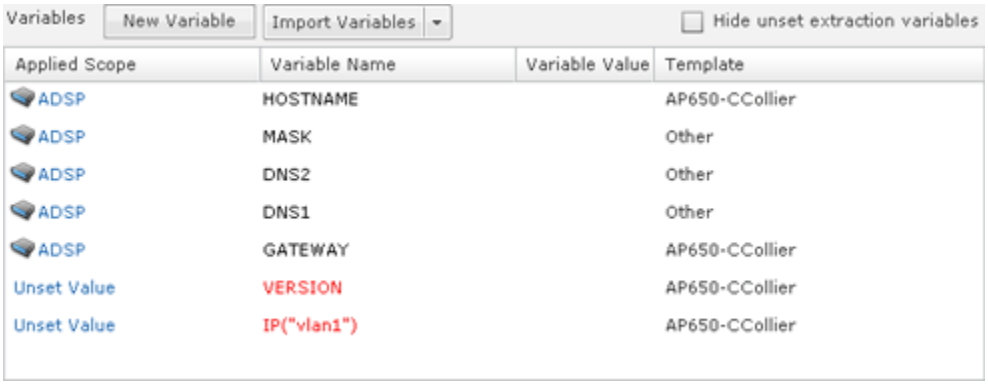
```
!
version $[VERSION]
!
wlan-qos-policy default
 qos trust wmm
!
radio-qos-policy default
!
firewall-policy default
!
mint-security-policy the_policy
!
bridging-policy default
!
management-policy default
  user admin password 1
e4a4b216f889b3e07be9a27af1946dad8fe68048c4b0fa31b29470e38cebdb8a role 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 . 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.



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, it's 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:

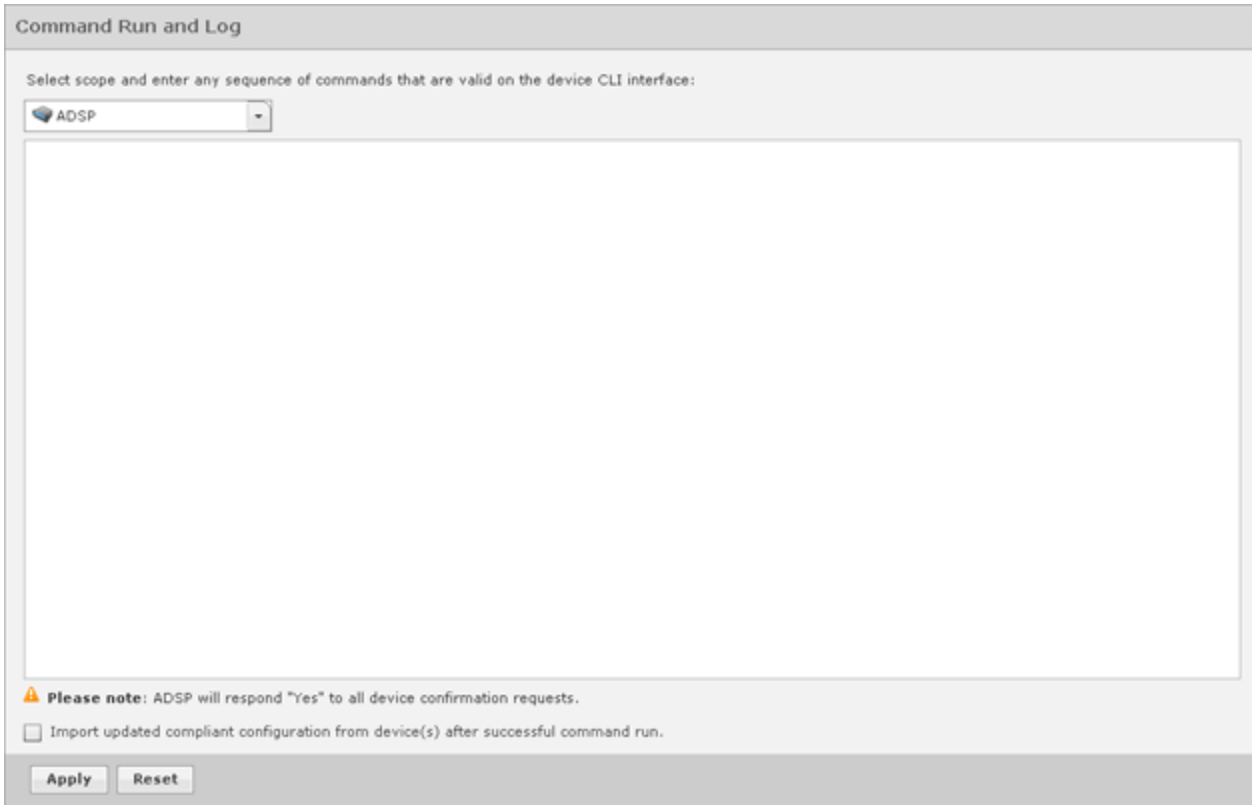
- The **Import Variables** function imports CLI variables. See *Import CLI Variables* for file format and examples.
- The **Export Variables** function exports CLI variables to a file for later use.
- The **Open Variable Template** function displays a template that you can copy, paste the contents into 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, *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.

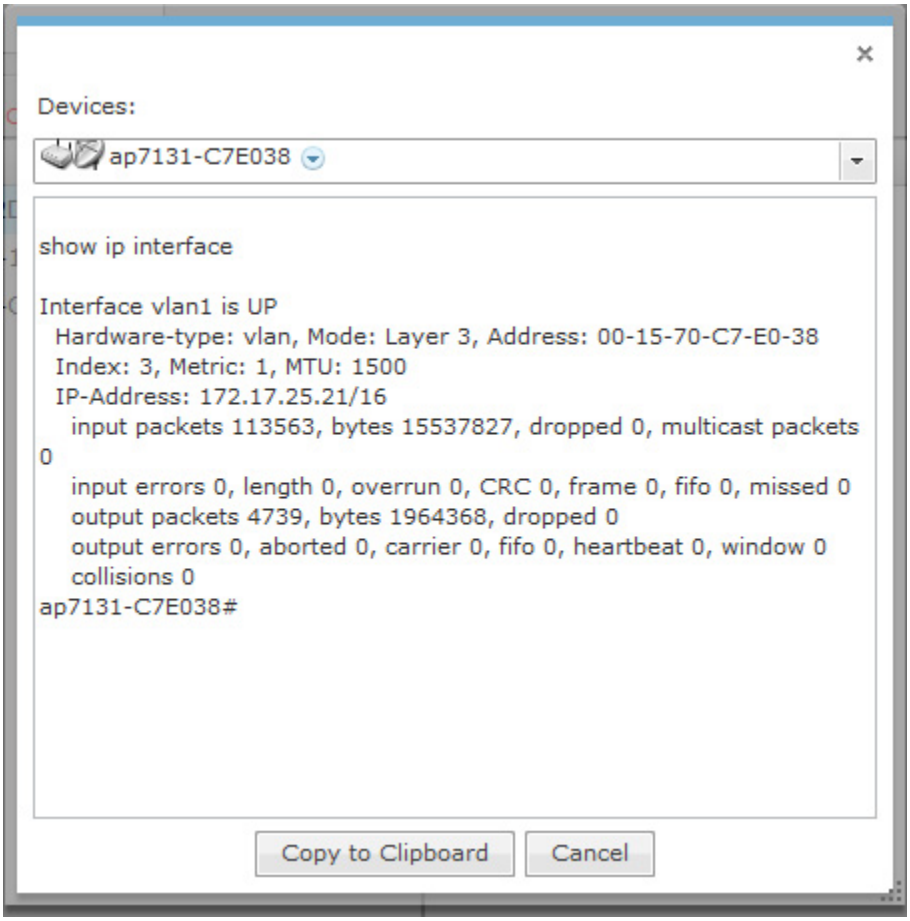
Each command must be on a line by itself. If a command requests a confirmation from a device, ADSP will respond Yes.

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

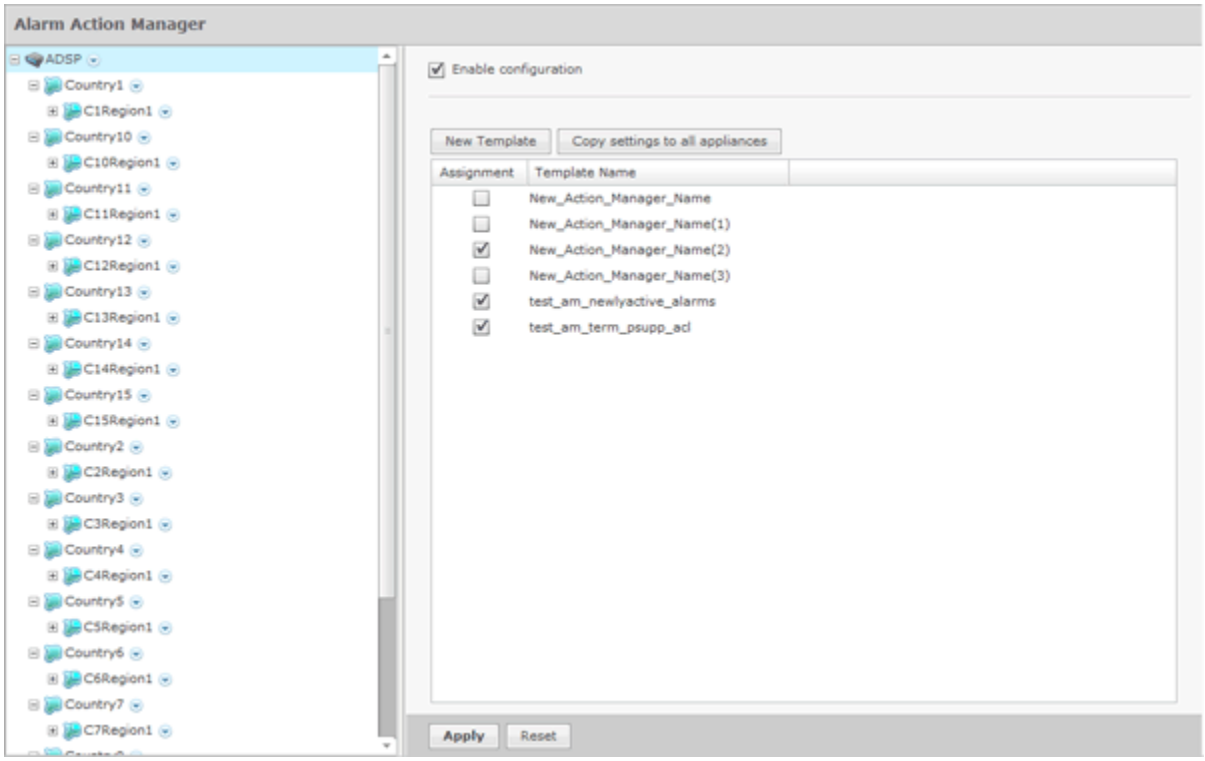
The Operational Management category includes features that apply to the normal operations of ADSP. The Operational Management category allows you to:

- 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 later) that are configured as a Sensor only device.
- Configure Sensor scan settings and Sensor in-line settings for Advanced Spectrum Analysis.

Alarm Action Manager

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 task. 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.

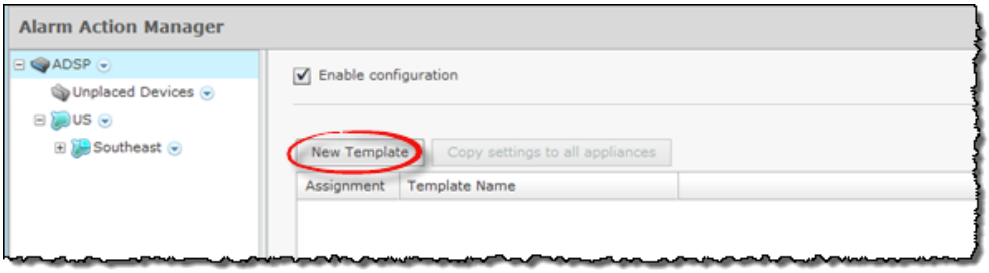
The Alarm Action Manager table displays one rule per row using the following columns:

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.

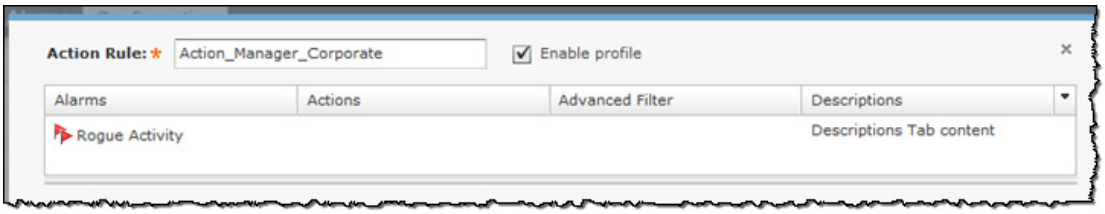
Once a template is added to the Alarm Action Manager, you can edit, copy, or delete it by selecting (highlighting) a template and then clicking on the appropriate link that appears to the right of the template.

Add an Action Rule

From the Alarm Action Manager screen, click **New Template** to configure a new action rule.



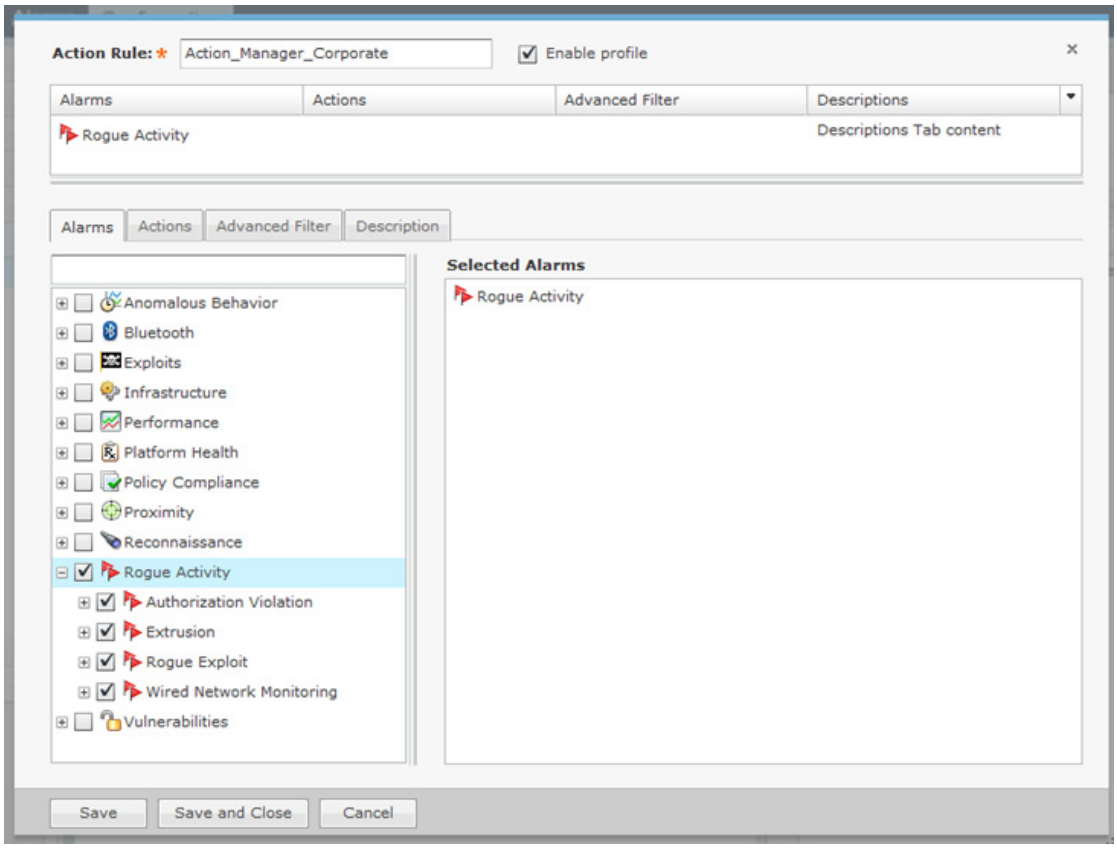
In the **Action Rule** field, give your action rule a name and select the **Enable profile** checkbox to enable the action rule.



The **Action Rule Template** window has four tabs that are used to define an Action Rule: Alarms, Actions, Advanced Filter, and Description. Use each of these to configure the action rule.

Alarms Tab

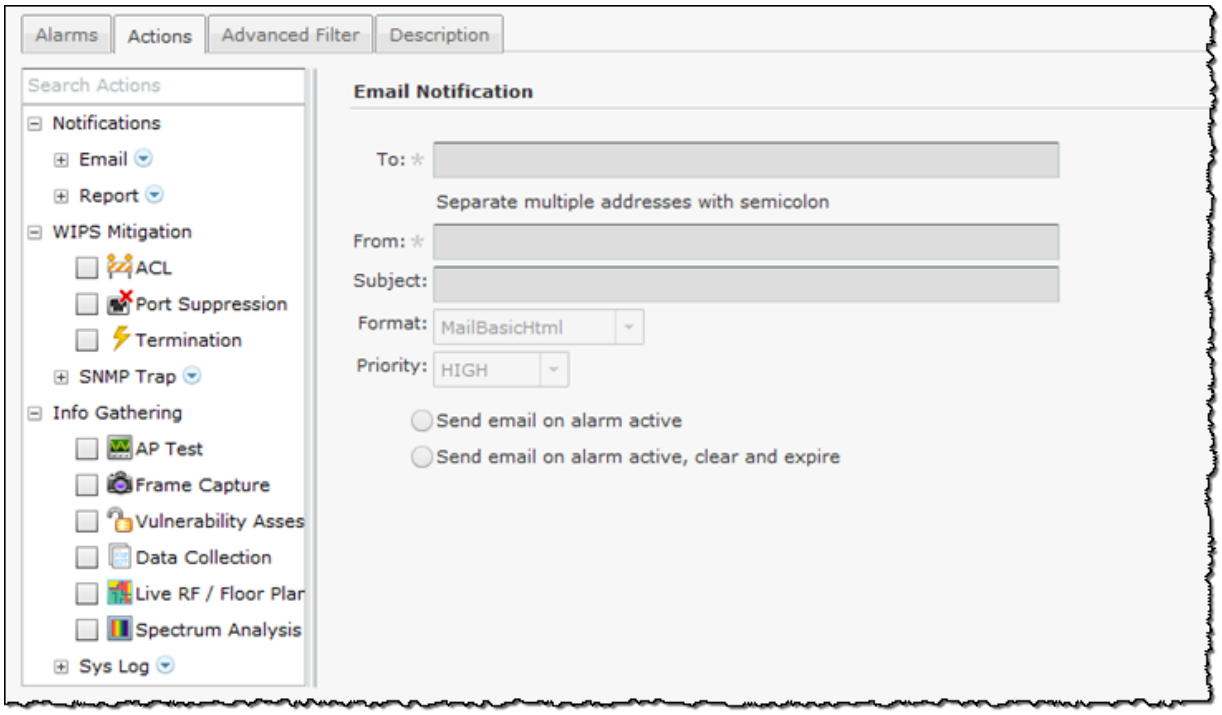
The **Alarms** tab is where you identify the alarms that you want to generate for your Action Rule. You may select one or more alarms to generate when the conditions in the filter are met. In the following example, the Rogue Activity alarm is selected.



Click **Save** to save changes and go to the Actions tab.

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.

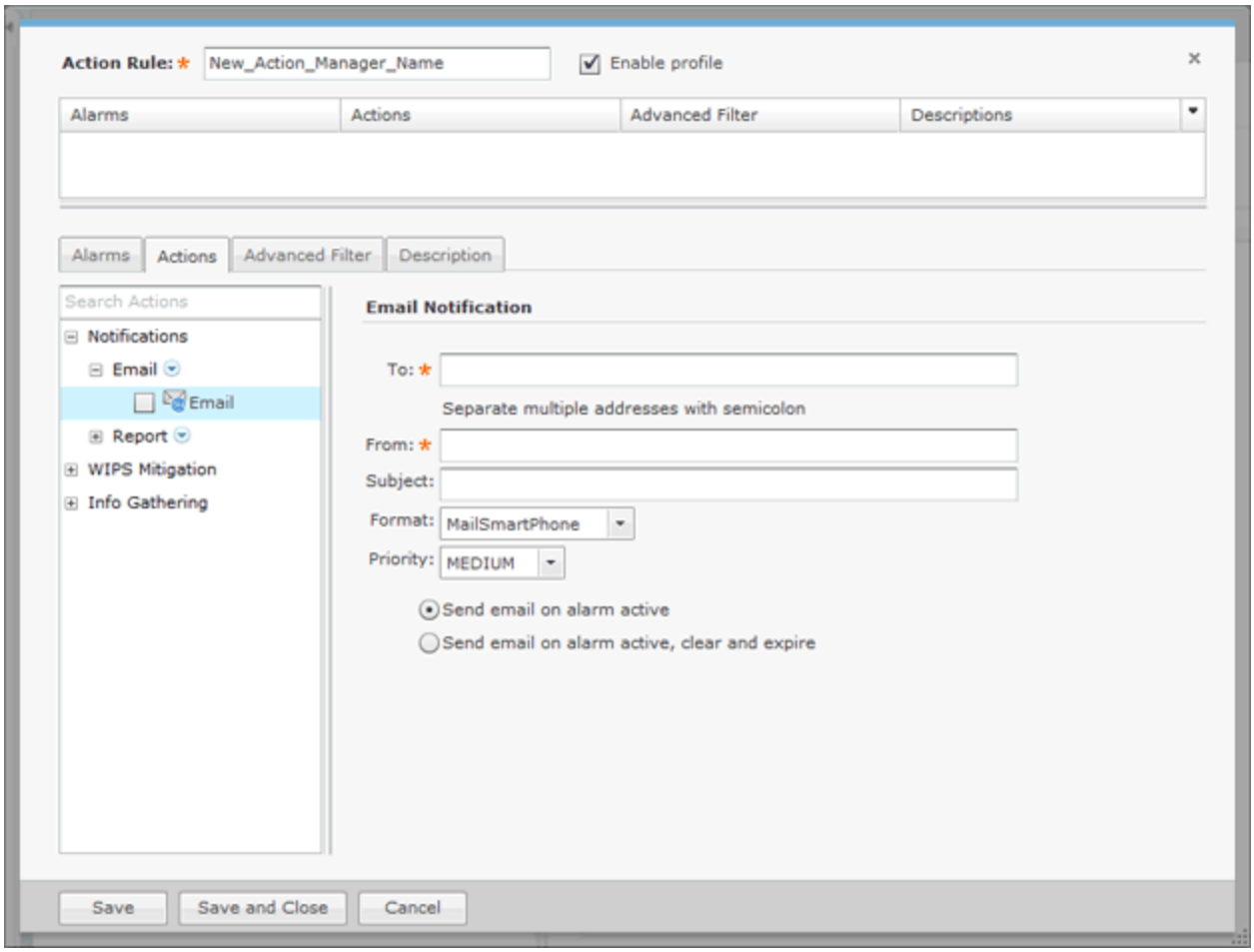
Notifications

The following actions are part of **Notifications**:

- *Email*
- *Report*.

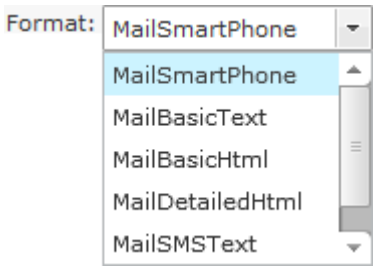
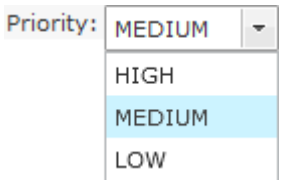
Email

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**.



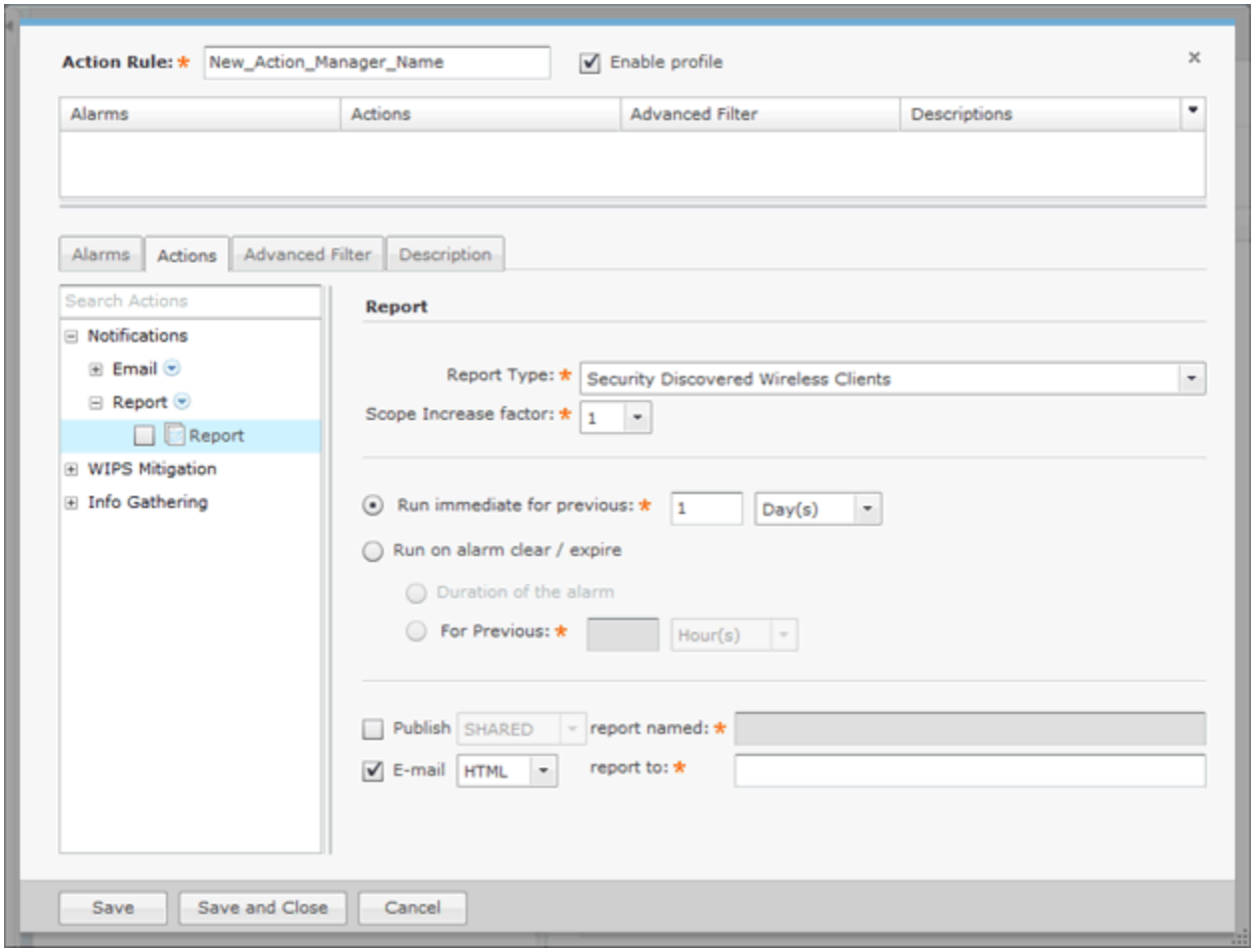
The following fields should be filled:

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	Specifies a format in which to send the email. Choose a format from the drop-down menu. 
Priority	Specifies a priority for the email. Choose a priority from the drop-down menu. 
Send email options	There are two options to send email: • Send email on alarm active—Send email on active alarms. • Send email on alarm active, clear and expire—Send email on active alarms, cleared alarms, and expired alarms.

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: **SHARED** or **PRIVATE**. 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: **HTML**, **PDF**, or **CSV**. You must furnish the email address of the person receiving the report.

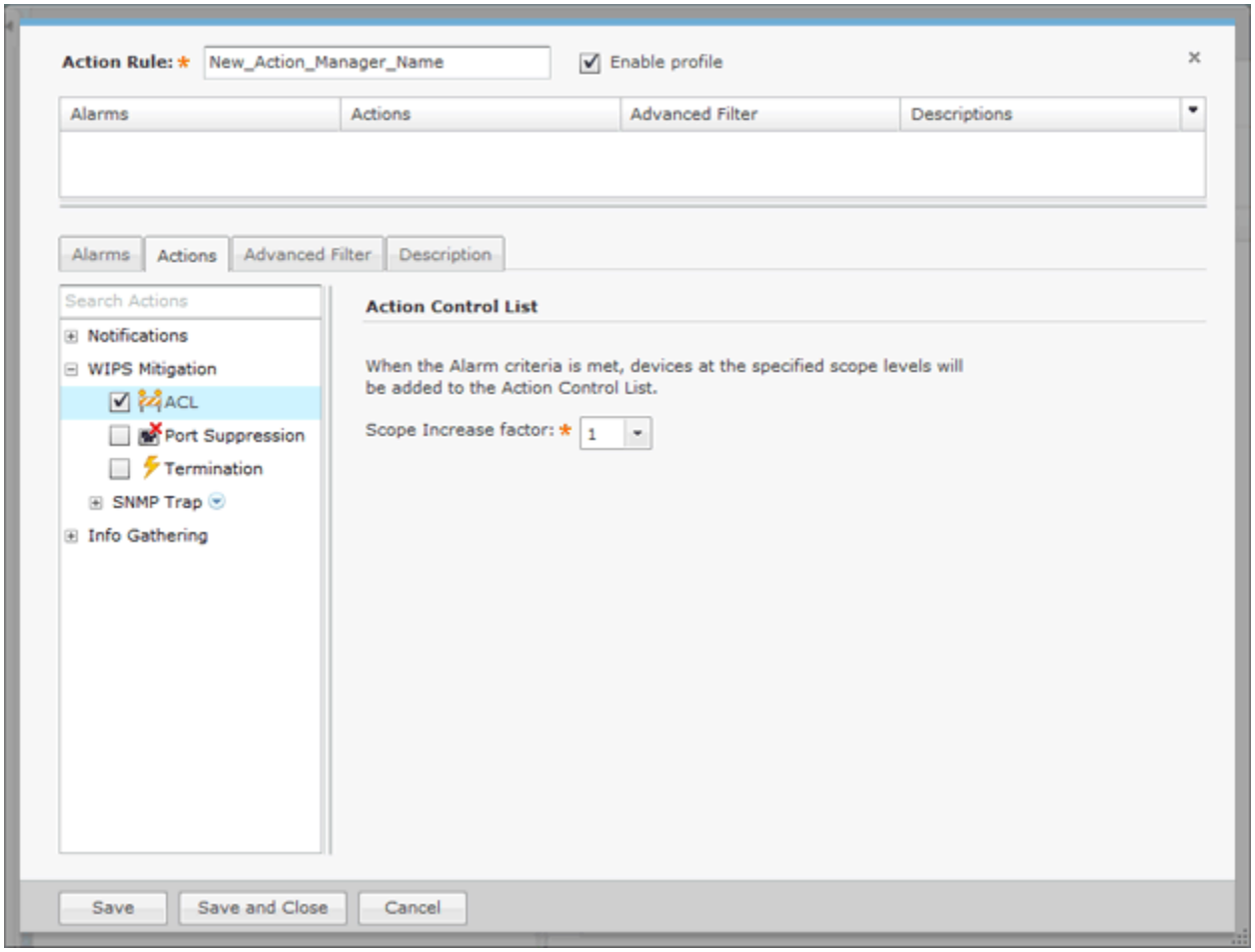
WIPS Mitigation

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**.

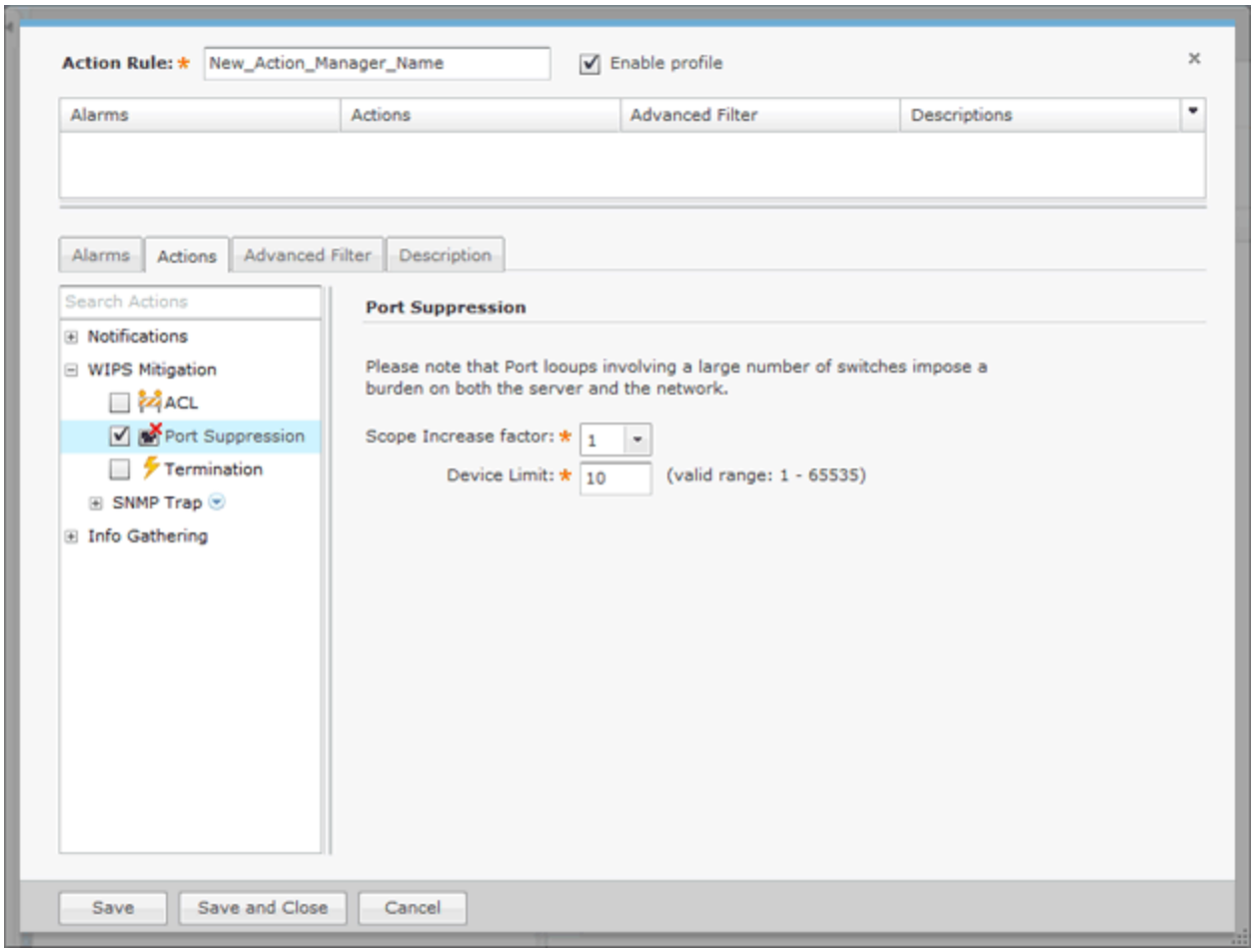


The **Scope Increase Factor** option specifies the number of network levels to expand the scope. A value of 1 means only use the floor level. A value of 2 means use the floor and the floor's parent, and so forth.

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**.



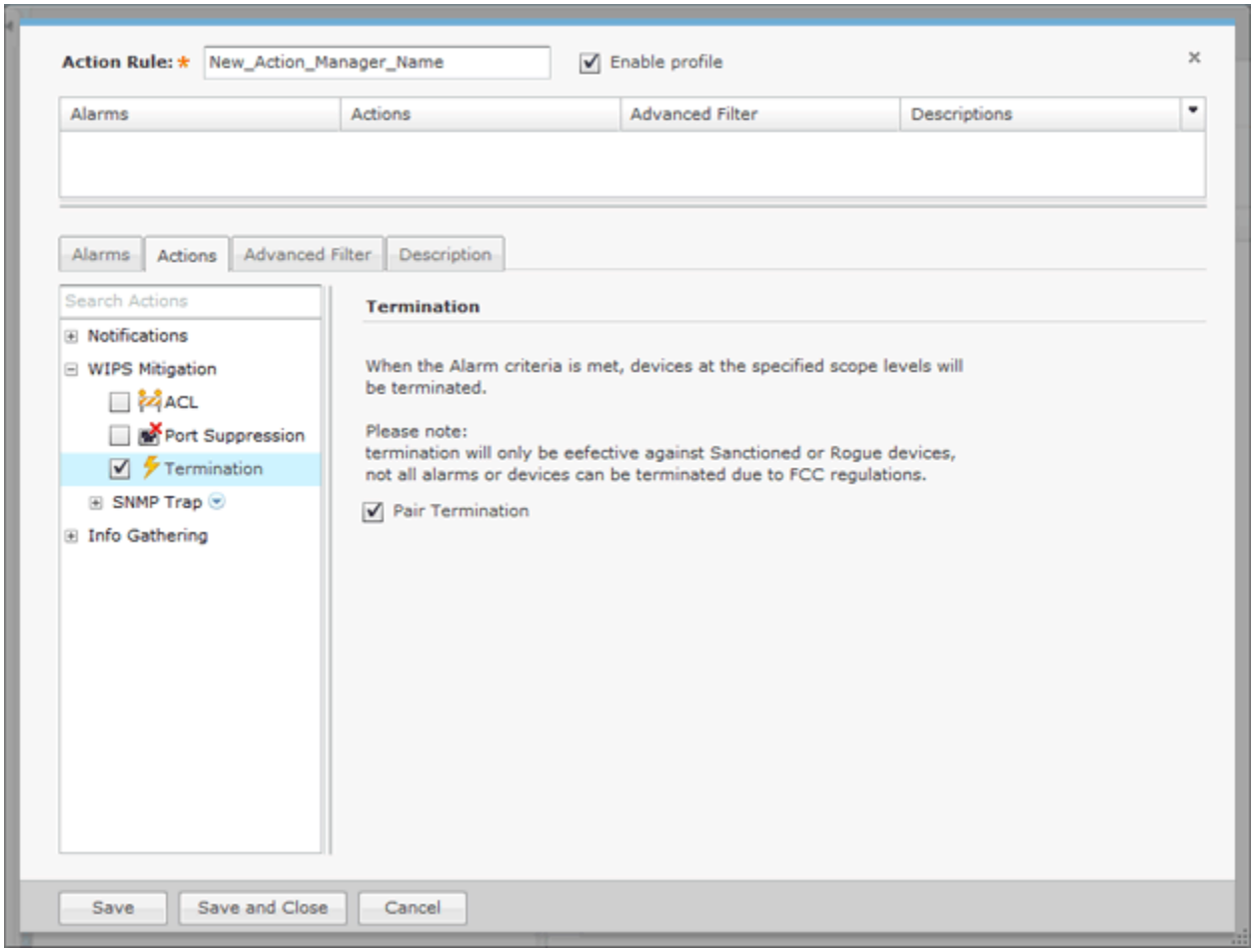
There are two options to configure: **Scope Increase Factor** and **Device Limit**.

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 Wi-Fi
- 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**.

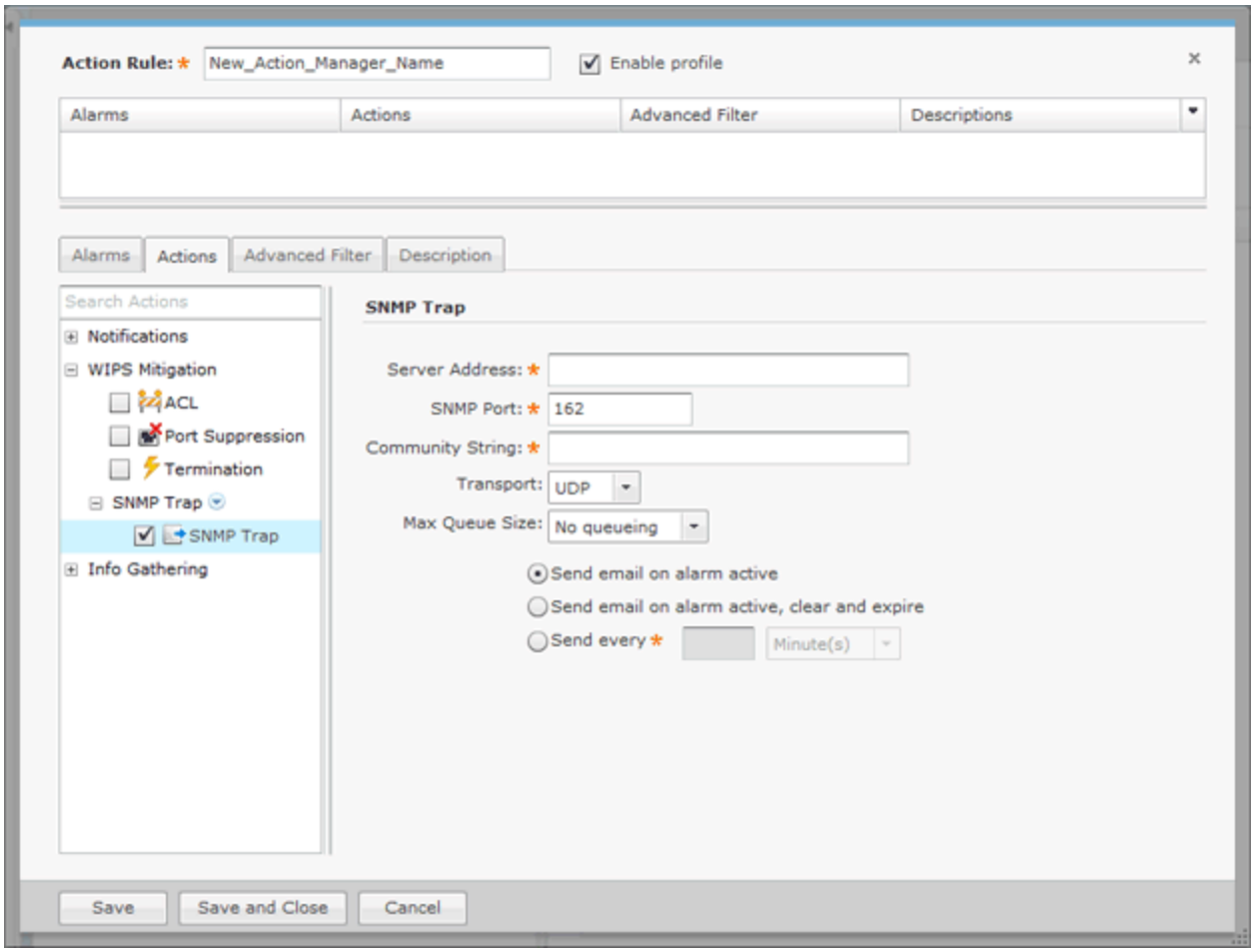
   NOTE If you are not a user with read/write permission to the System Configuration functional area, the settings in **Appliance Management** will not appear, and you cannot edit the **Appliance Settings**.

2. Select the checkbox for **Air Termination system**.
3. Select the checkbox for **Policy-based Air Termination system**.
4. Click the **Apply** button.

SMNP Trap

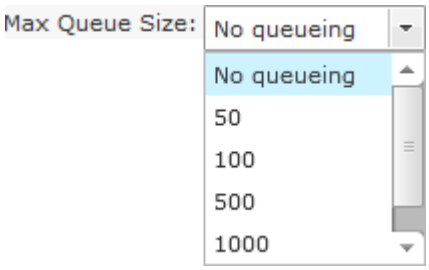
The SNMP Trap action sends an SNMP notification to your SNMP server if the conditions defined in the filter are met. To select the SNMP Trap action, go to **WIPS Mitigation** > **SNMP Trap** and then select **SNMP Trap** from the **Search Actions**.

NOTE Before you can use the SNMP Trap action, you must enable SNMP trap. For information on enabling SNMP trap, see *Using ADSPadmin to Configure ADSP*.



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	Specifies the desired transport protocol. Choices are: • UDP: User Datagram Protocol • TCP: Transmission Control Protocol. Hint: Typically, UDP is the transport for SNMP traps. However, TCP can be useful for tunneling the traps over Secure Socket Layer (SSL).
Max Queue Size	Specifies the maximum queue size for the notification. Choose a size from the drop-down menu. 
Send Time	Specifies when to send the email by selecting one of the following conditions: • Send on alarm active • Send on alarm active, clear and expire • Send every x amount of minutes or hours.

Info Gathering

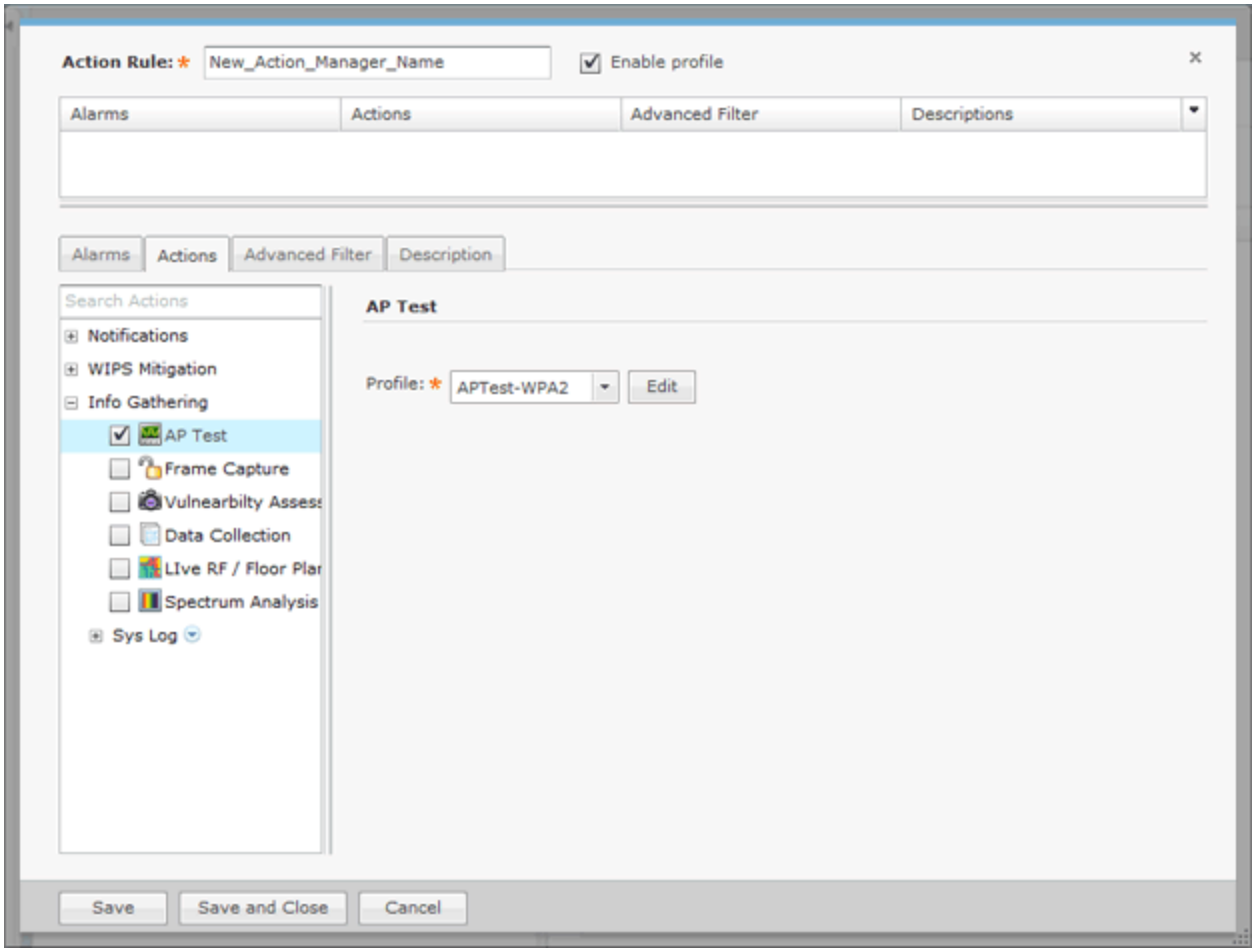
The following actions are part of **Info Gathering**:

- *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**.

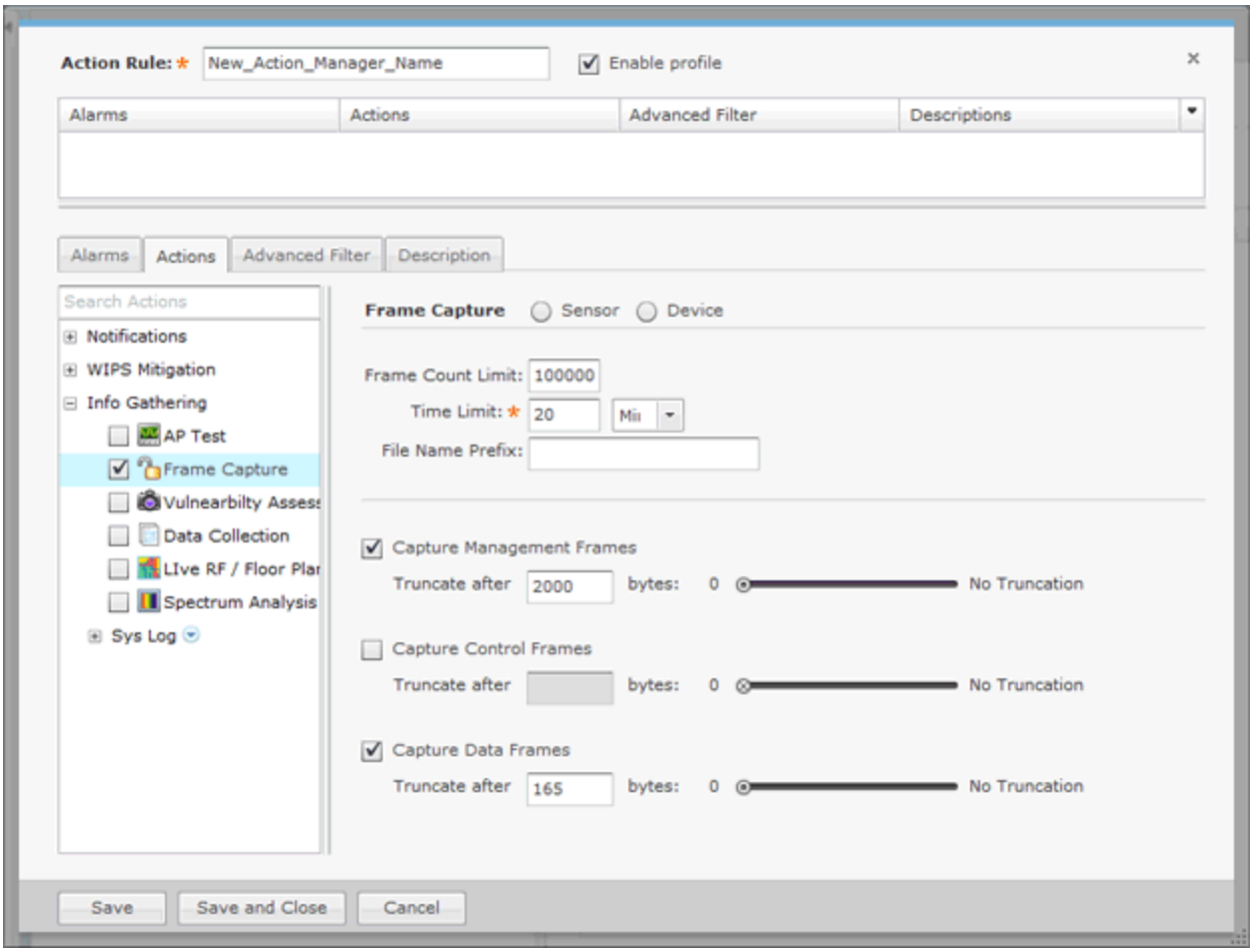


The following field is available:

Field	Description
Profile	Select a test profile from the drop-down menu. The **Edit** button can be used to modify the test profile. See the *AP Testing* topic in *The Menu* chapter for details on how to schedule both automated and on-demand tests for APs.

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.

Field	Description
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.

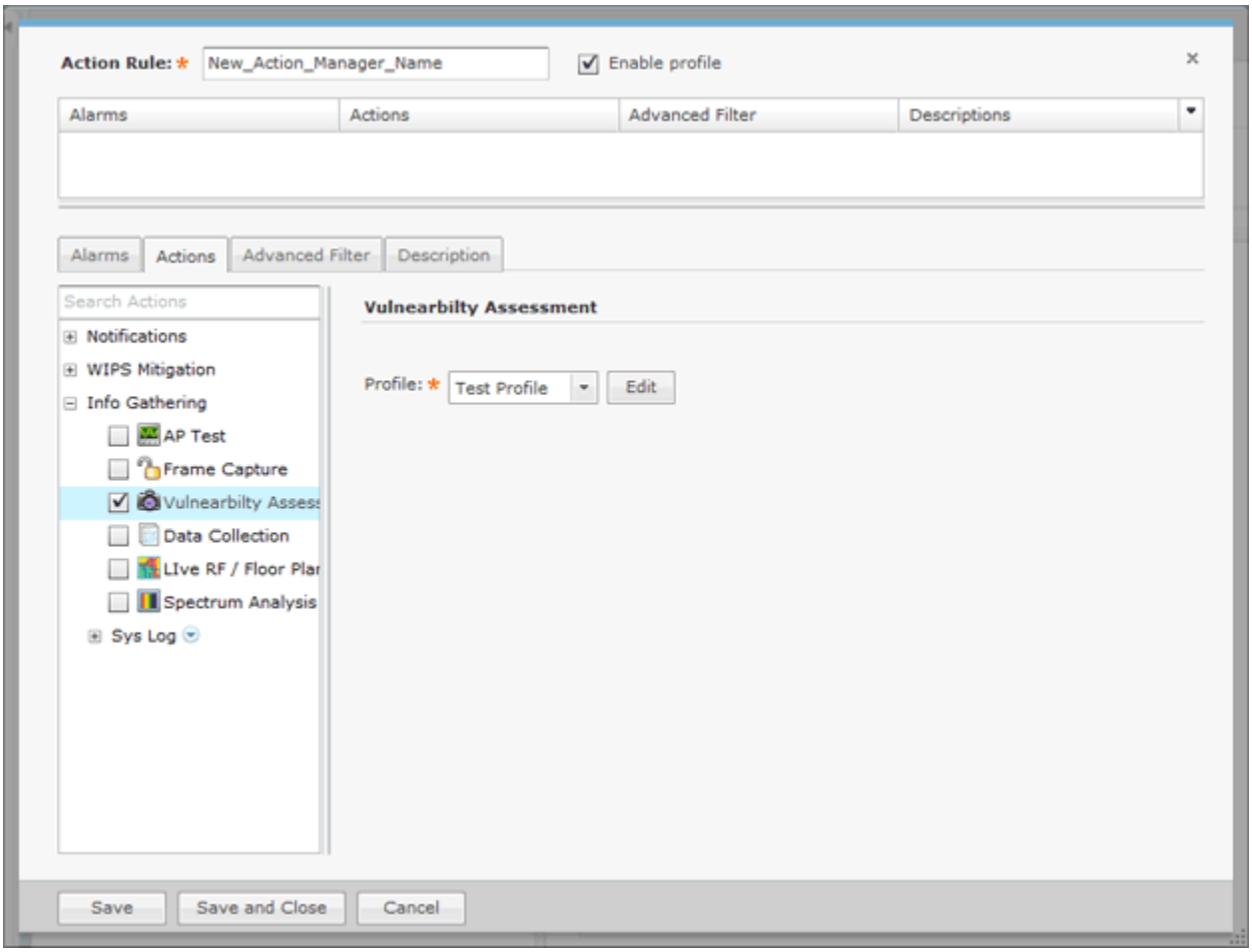
The captured file is stored in either—or, at times, both— of the following directories:

```
/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**.



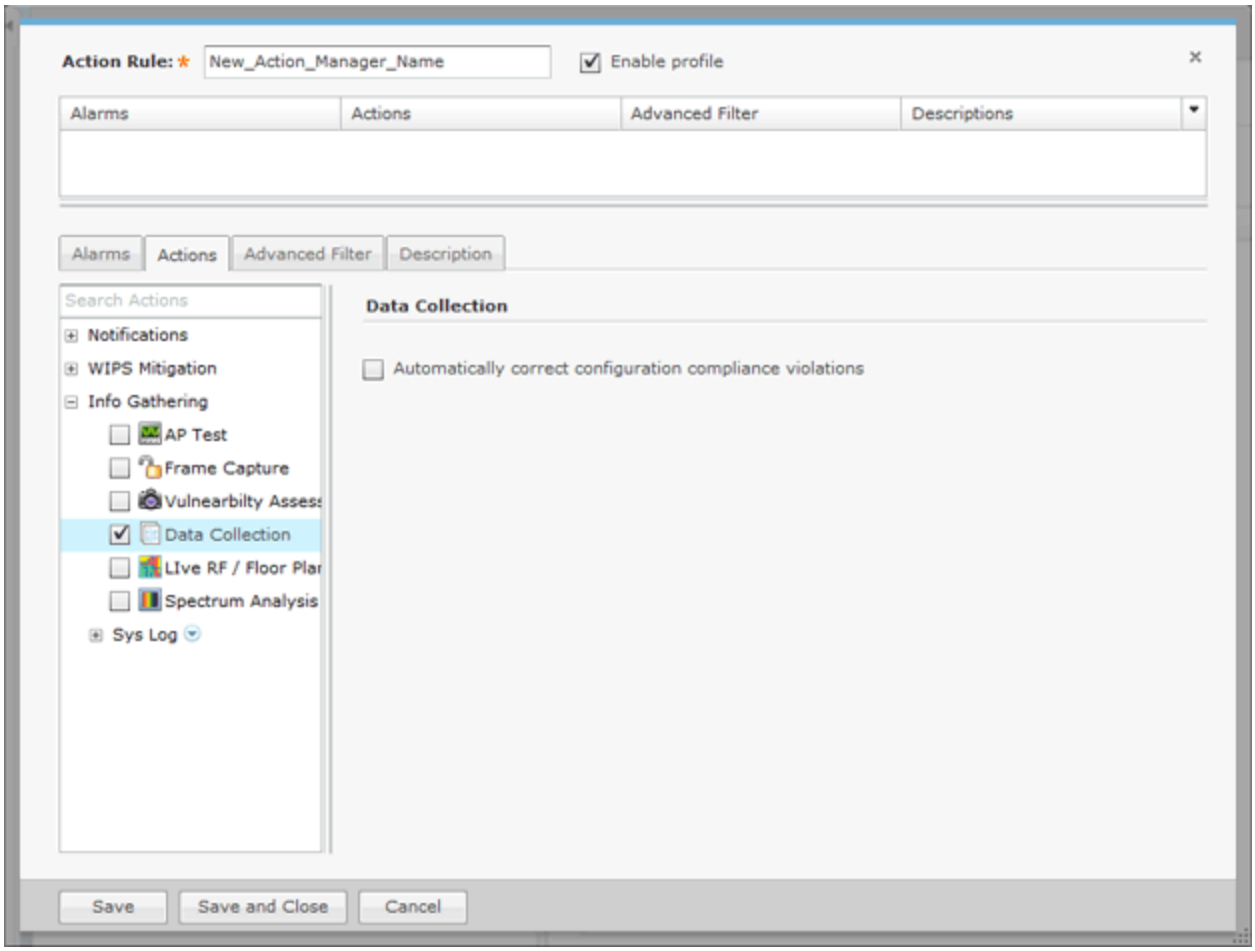
The following field is available:

Field	Description
Profile	Select an assessment profile from the drop-down menu. The **Edit** button can be used to modify the assessment profile. For more information on assessment profiles, refer to the for *Vulnerability Assessment* section in the *Security* chapter.

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**.

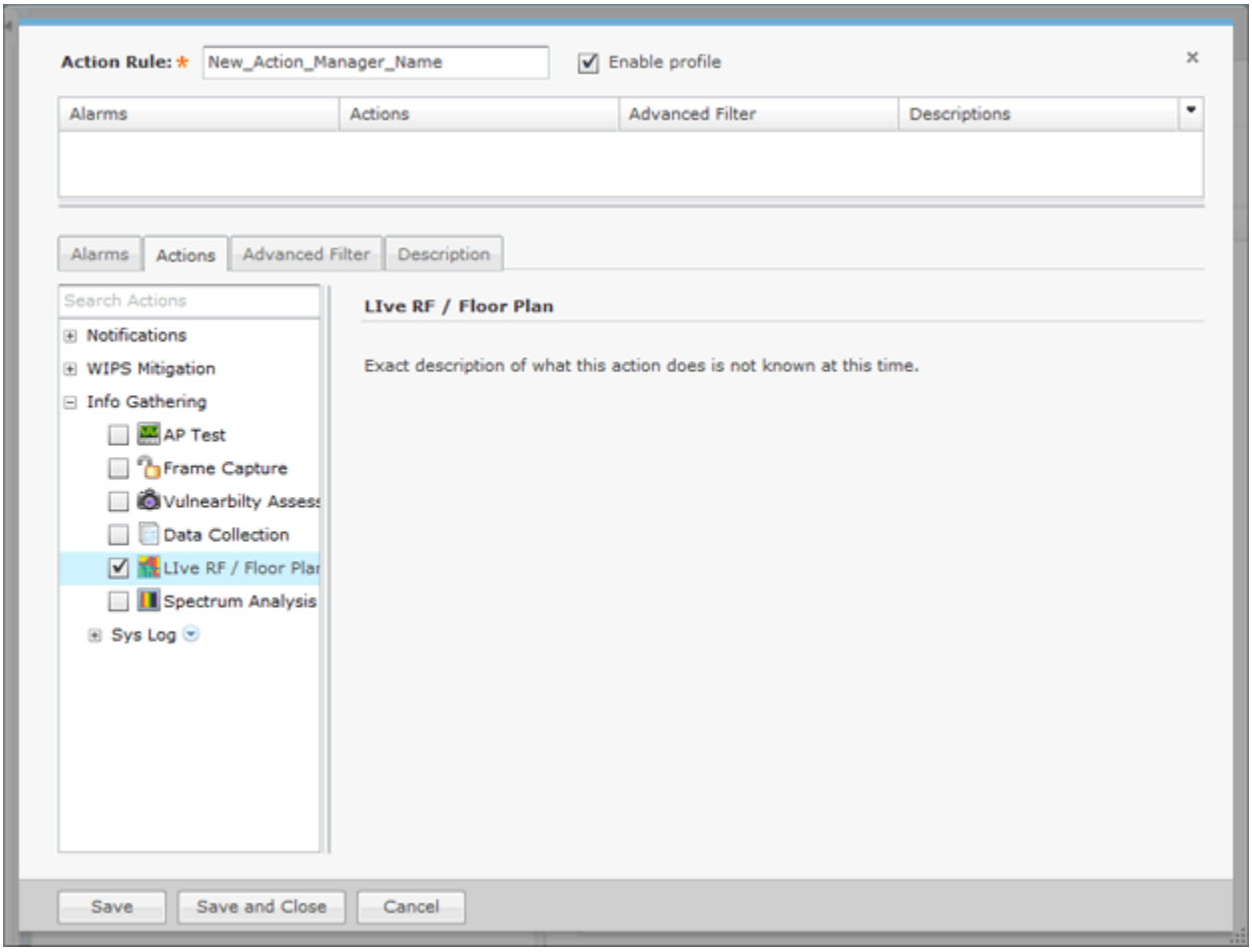


There is only one option: **Automatically correct configuration compliance violations**. When this option is selected and an alarm is generated by a device meeting the conditions specified in the filter, ADSP automatically uploads the last approved configuration to the device to correct any violations.

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 off line. To select the Live RF / Floor Plan action, select **Info Gathering** > **Live RF / Floor Plan** from the **Search Options**.

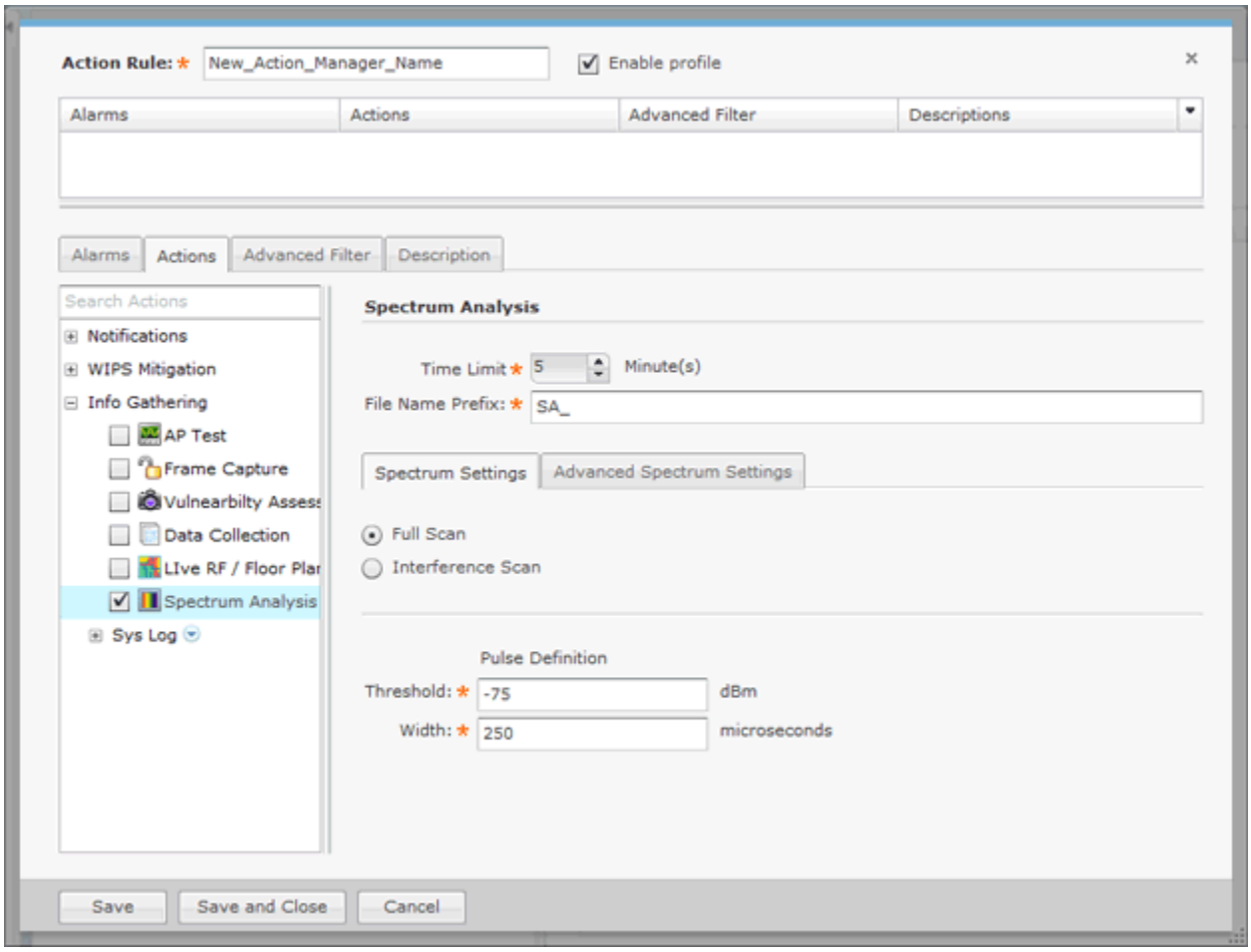


There are no configuration options for Live RF / Floor Plan.

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**.

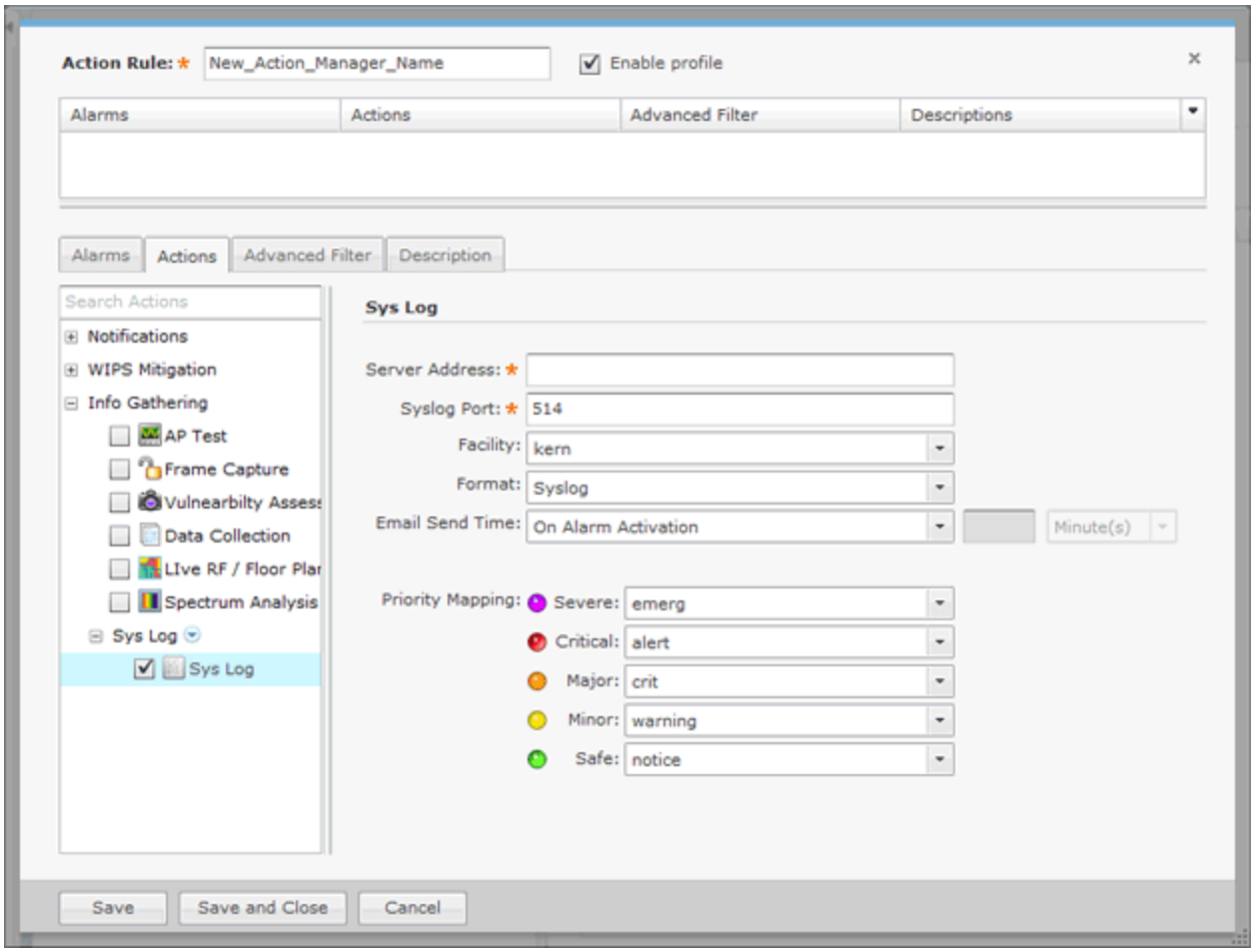


The following fields are available:

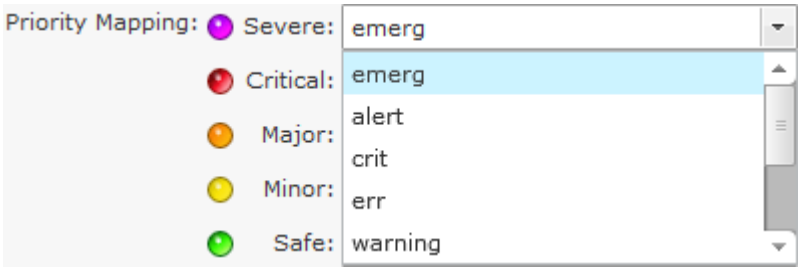
Field	Description
Time Limit	Places a time limit on how long the Spectrum Analysis will run.
File Name Prefix	Defines a prefix for the Spectrum Analysis file. You may add to the prefix if you want to.
Spectrum Settings	Only used in regular Spectrum Analysis. These are the same **Spectrum Settings** described under *Dedicated Analysis*.
Advanced Spectrum Settings	Only used in Advanced Spectrum Analysis. These are the **Dedicated Scan Settings** described under *Advanced Spectrum Analysis*. The **In-Line Scan** options cannot be changed. The **Dedicated Scan** 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**.



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	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. This facility can be very helpful to define rules that split messages, for example, to different log files based on the facility level. Choose a Syslog Facility from the drop-down menu. 
Format	Specifies the format of the notification. At this time, the only option is **Syslog**.
Email Send Time	Specifies when to send the email by selecting one of the following conditions: • On Alarm Activation • On Activation, clear or expire • Every x amount of minutes or hours.
Priority Map	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 **Severe** drop-down menu. 

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:

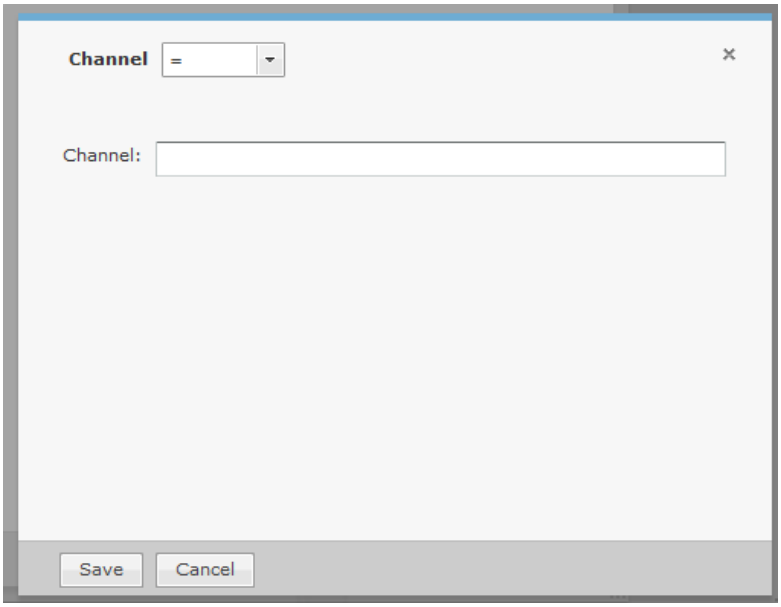
- All—All of the selected conditions must be met (logical “and” operation).
- Any—One or more selected conditions must be met (logical “or” operation).
- None (All)—None of the selected conditions are met (logical “and” operation).
- None (Any)—One or more selected conditions are not met (logical “or” 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 In the following example, the Channel filter has been selected.

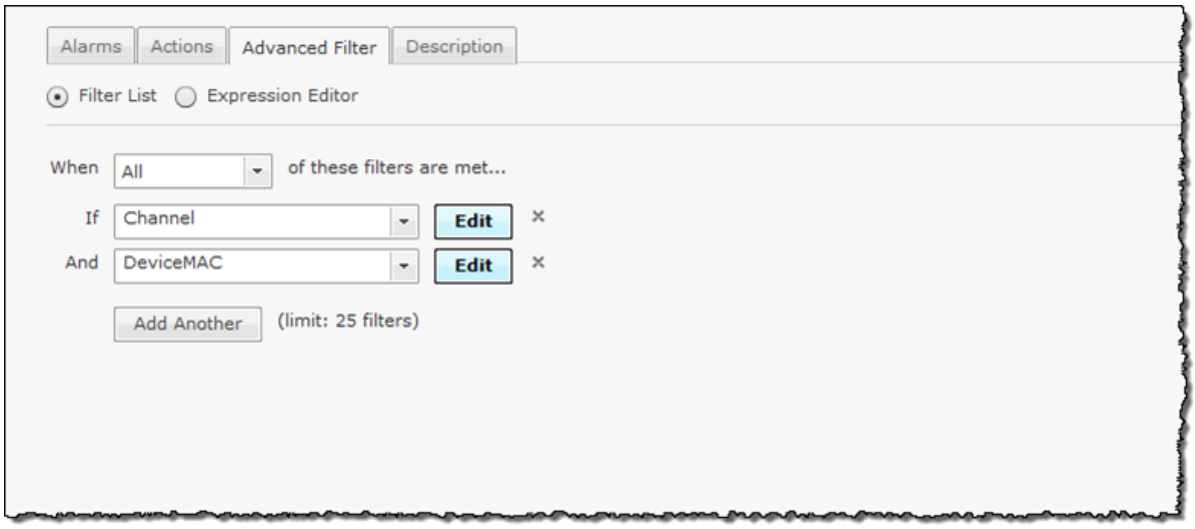


Click the drop-down menu to select the type of comparison. This will vary according to the selected filter. The type of comparison may be:

- = 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 **Save** to save the comparison.

The following screenshot shows an example of a Filter List.



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*.

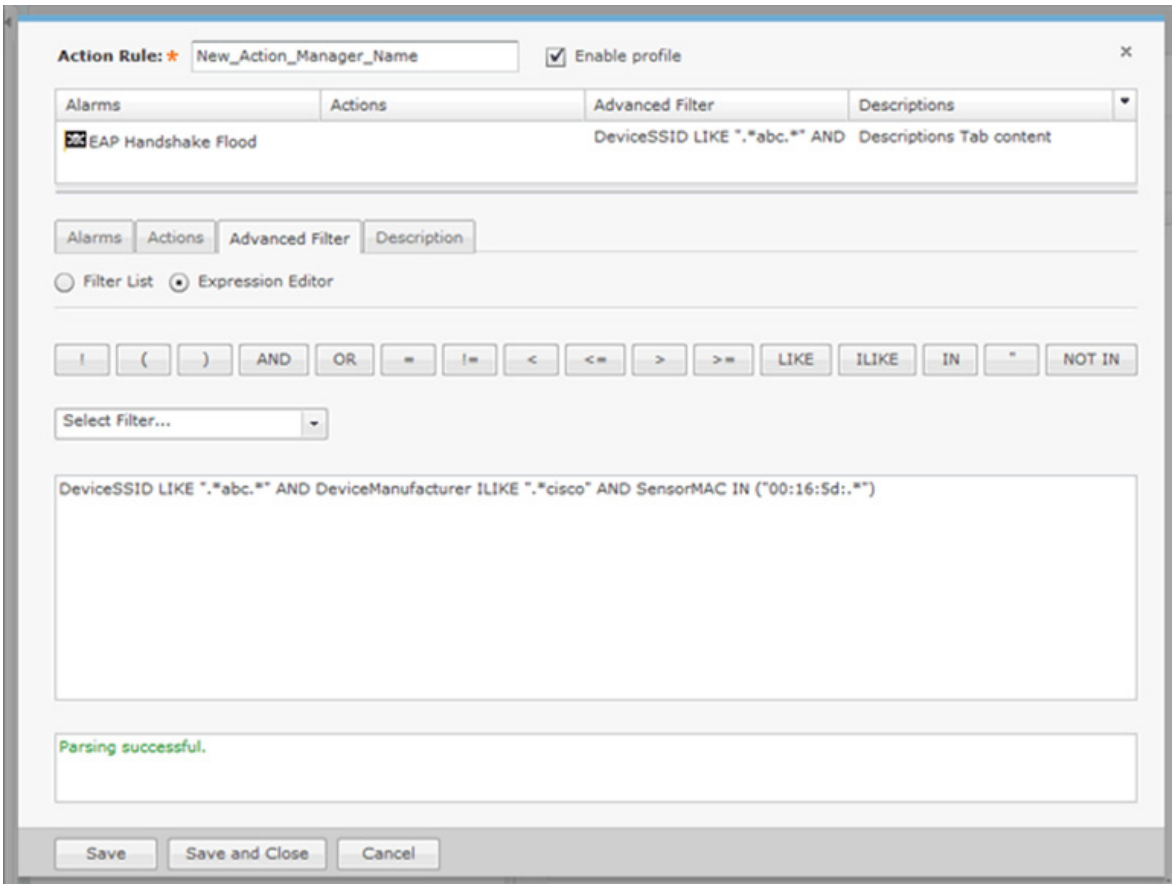
The operators (parentheses and quotation marks) are:

- !
- (
-)
- 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.



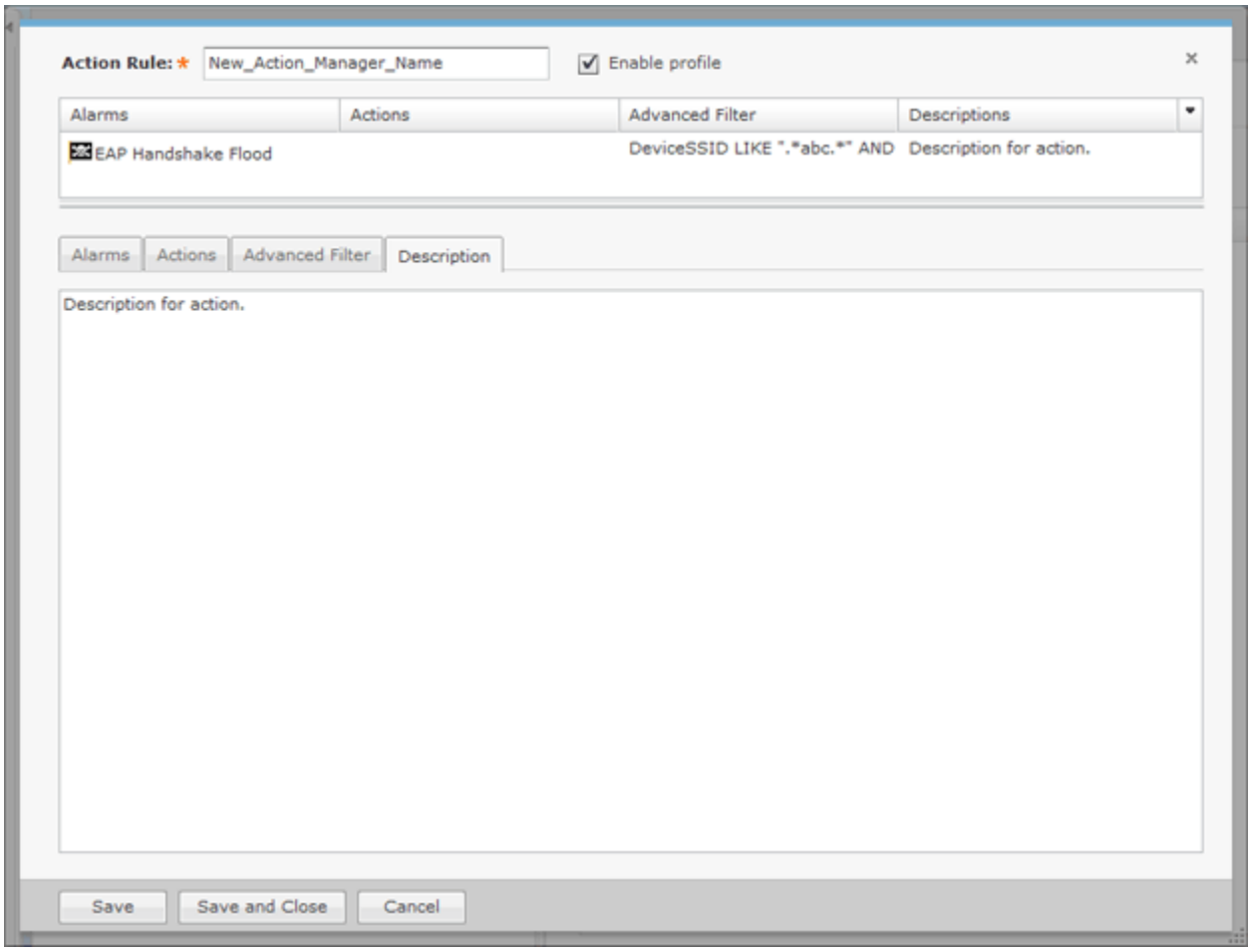
Notice the use of wildcards in the screen shot expression:

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

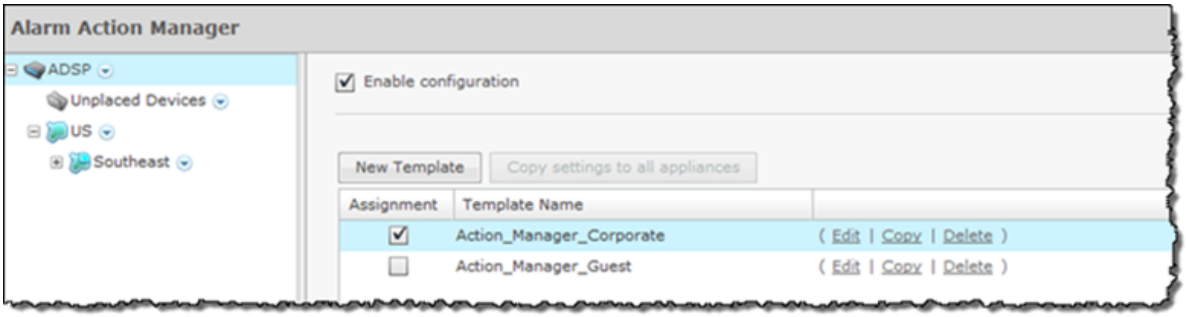
Enter a description of the action on the Description tab.



Type a description and then click **Save** or **Save and Close**.

Apply an Alarm Action Manager Template

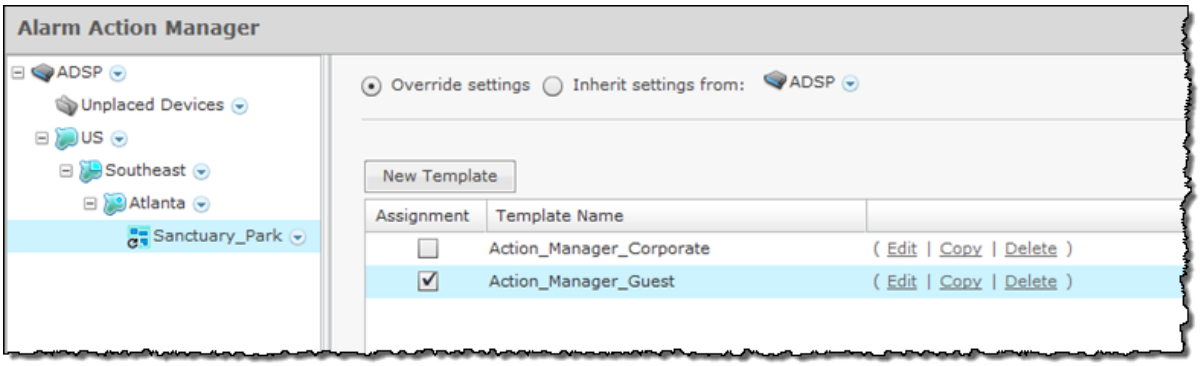
Once you have defined an Alarm Action Manager template, to use it, you must apply it to your system.To apply a template, you must first select the **Enable configuration** checkbox.



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 the appliance is 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** template to the **Sanctuary Park** 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.



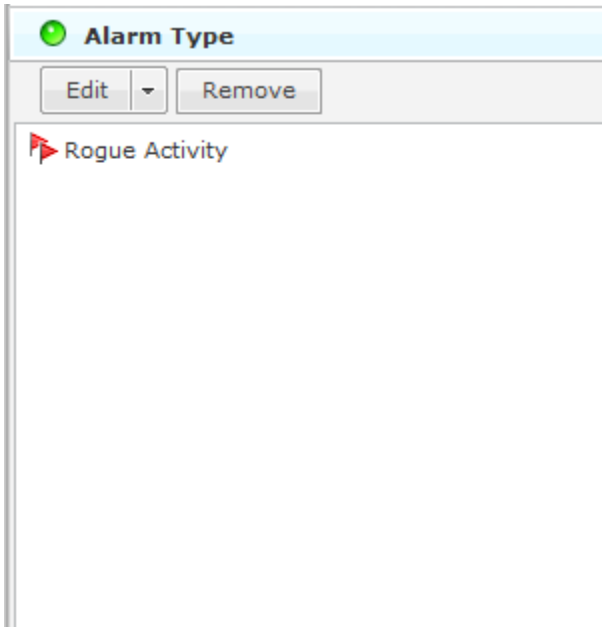
You can copy Alarm Action Manager templates to all your appliances by clicking the **Copy settings to all appliances** button.

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 nine 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 actual alarm. The alarm types are:

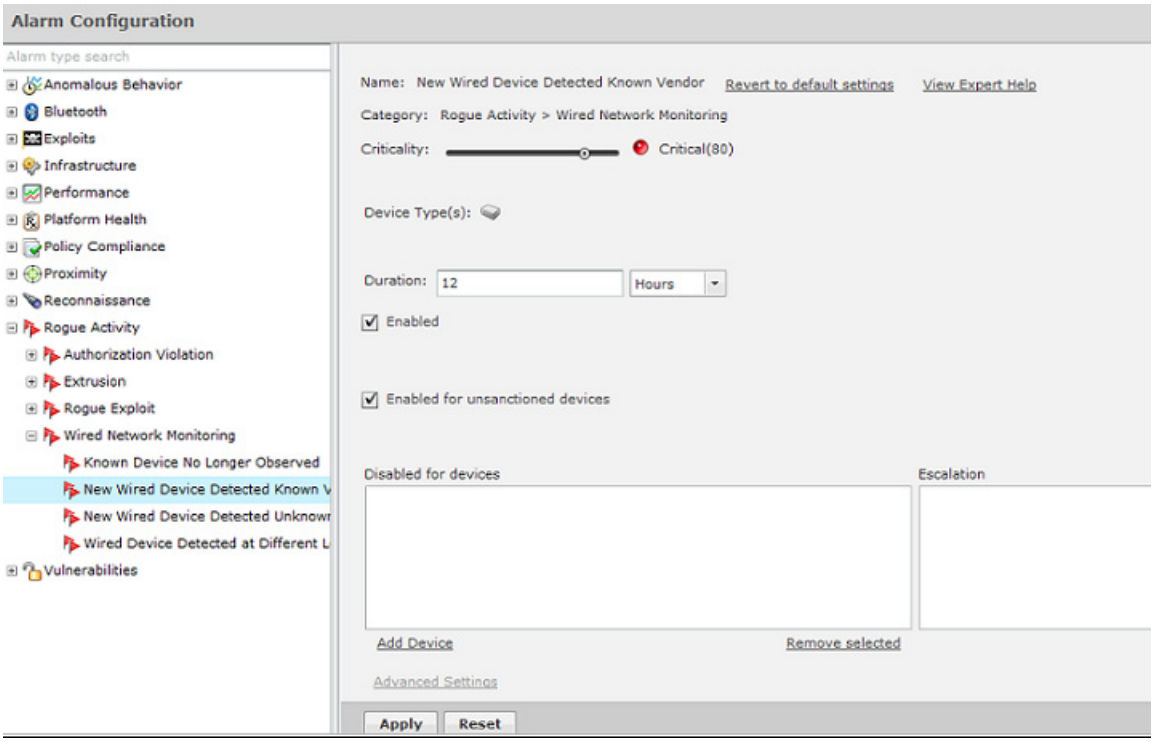
- Anomalous Behavior—Devices that operate outside of their normal behavior settings and generate events that could indicate anomalous or suspicious activity.
- Bluetooth—Bluetooth monitoring is an unique capability in AirDefense for 24x7 monitoring of Bluetooth devices in Enterprise environments.
- Exploits—Events 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.
- Proximity—Proximity Awareness & Analytics provide a number of key functions, including Presence Services, Wi-Fi Analytics, Locationing (RTLS) Services, and Historic Location Analysis.
- 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 (such as Rogue Activity.) Click the '+' sign next to the alarm to display the alarm sub-type(s). Drill down until you reach the actual alarm. When you click on the alarm, the following screen is displayed.



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 name of the alarm.
Criticality	Use the sliding scale to set the alarm criticality to a value between 0 and 100. The designated color will automatically adjust as you move up or down the scale for Safe, Minor, Major, Critical, and Severe. The new numerical value will be used to calculate the Threat Score.
Duration	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 recommended. After the condition and the alarm duration have expired, the alarm becomes inactive, although it will remain visible in the historical logs. (You can view the historical logs using Forensic Analysis.) You can also clear an alarm before the duration expires.
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.

Option	Description
Disabled for devices	The alarm is disabled for any device listed in the table. Click the **Add Device** button to add a device to the list. You are prompted to enter the device's MAC address. Typing a partial MAC address will list all the devices matching your typed string. You can then select the device or devices that you want to select. When you click on a device, it is automatically added to the list. Typing the entire MAC address will list only the device matching that address. Clicking the **Advanced** link will display a **Device Search** dialog window. You can then search for a device using any combination of the following criteria: • Device name • MAC address • 802.1X name • DNS name • Vendor name • SSID • Protocol used. After selecting your search criteria, click the **Search** button to display a list of devices matching the search criteria. Click on the device or devices that you want to add to the device list. Click **Close** when you are done. You can return to the original window by clicking the **Basic** link where you can enter only the MAC address. Clicking the **Remove selected** link will remove the selected device from the list.
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 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.

Bluetooth Alarms

Bluetooth alarms provide 24x7 monitoring of Bluetooth devices in your network. The system can automatically detect security threats from unsanctioned Bluetooth devices and proactively notify administrators about the presence of these threats. The Bluetooth alarm sub-type is Bluetooth Devices:

- Rogue Bluetooth Device
- Rogue Bluetooth Device Out of Hours
- Unsanctioned Bluetooth Device

Alarm Library

To view a list of Bluetooth Alarms for each alarm sub-type, go to **Configuration** > **Operational Management** > **Alarm Configuration**, open **Bluetooth**, 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 exists 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 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 , whereas a more directed attack will only impact a single station leaving other stations connected to the . 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 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 / port status. An 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 APs 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 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 are broken down into the following eight sub-types:

- AP Testing—AP Testing Events track network failures and provide proactive notification that the network resources may be unavailable. The alarms in this category indicate a failure of one of the test conditions. Any alarm should be considered a high priority event as it may be preventing the wireless applications from operating properly.

  These connectivity tests can be run automatically or manually. The AP test uses the deployed sensors as a wireless station to connect to an AP and validate the available resources. The test validates wireless authentication, encryption, DHCP, ACL, firewall testing, general network connectivity and application availability testing.

- 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 892.11 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 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 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 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 APs 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 APs 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 includes alarms that alert you to Wi-Fi Direct devices that are violating your network compliance policy. Wi-Fi Direct is peer-to-peer networking which may present issues with corporate networks controlling Wi-Fi Direct devices. Being able to detect Wi-Fi 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 APs 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.

Proximity

Proximity Awareness and Analytics alarms provide a number of key functions, including Presence Services, Wi-Fi Analytics, Locationing (RTLS) Services, and Historic Location Analysis. Proximity Alarms are broken down into the following sub-types:

- Location Subscribers—Web servers can be registered as “Location Subscribers” on an ADSP appliance. ADSP will then proactively “push” Proximity data to these subscriber servers as it becomes available. Alarms in this category describe communication failures with those subscriber servers.
- Presence—The Presence function supports identification of Wi-Fi devices using the sensors in the target environment. Presence allows the system user to prepare for arrival of the subject device in the target environment. Detection of devices is automatic and alerts the system that a device has been detected on site or in the facility. The presence function also supports the push of information using the API to external systems and applications which may use the information to trigger additional actions. Presence is engineered for quick setup and does not require any information regarding the physical environment of the store or facility.
- Region Events—The Locationing function supports real-time tracking of Wi-Fi targets based on the Real-Time Locating System standard (RTLS). This capability allows solution operator to resolve the position of a target device to within a radius of three meters. The system will also

track the target and, with additional information such as the physical layout of a facility, will enable the operator to support enhanced engagement based on defined boundaries, device profiles and behaviors. Real-life applications of the capability include: Geofencing, Prioritized Device Tracking, and Wi-Fi Device Inventory.

Alarm Library

To view a list of Proximity Alarms for each alarm sub-type, go to **Configuration** > **Operational Management** > **Alarm Configuration**, open **Proximity**, 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 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 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 APs that are in the vicinity of the station. Once a client connects to an AP, 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—APs 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 AP 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 devices participating in unauthorized communication in your airspace. Events included in this category range from detection of a wireless device operating in the airspace to detection of the most severe risks, e.g., unsanctioned wireless device communicating with the wired network. ADSP makes a clear distinction between an unauthorized device—which may be a neighboring device transmitting into the monitored airspace—and a rogue device—which is a device 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 capability allows the administrator to safely ignore neighboring APs while focusing his attention to real threats. 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 Wi-Fi Direct devices on your network. Wi-Fi Direct is peer-to-peer networking which may present issues with corporate networks controlling Wi-Fi Direct devices. Being able to detect Wi-Fi 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 an unauthorized AP 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 APs 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 APs 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 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 APs, 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 AP until the vulnerability has been remediated.

- Wired Leakage—In wireless networks unencrypted wired side traffic leakage into the air is a result of basic AP functionality. The AP 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 AP 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 AP 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 AP 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 APs on a dedicated subnet which will limit the broadcast domain of the network to minimize wired side leakage.

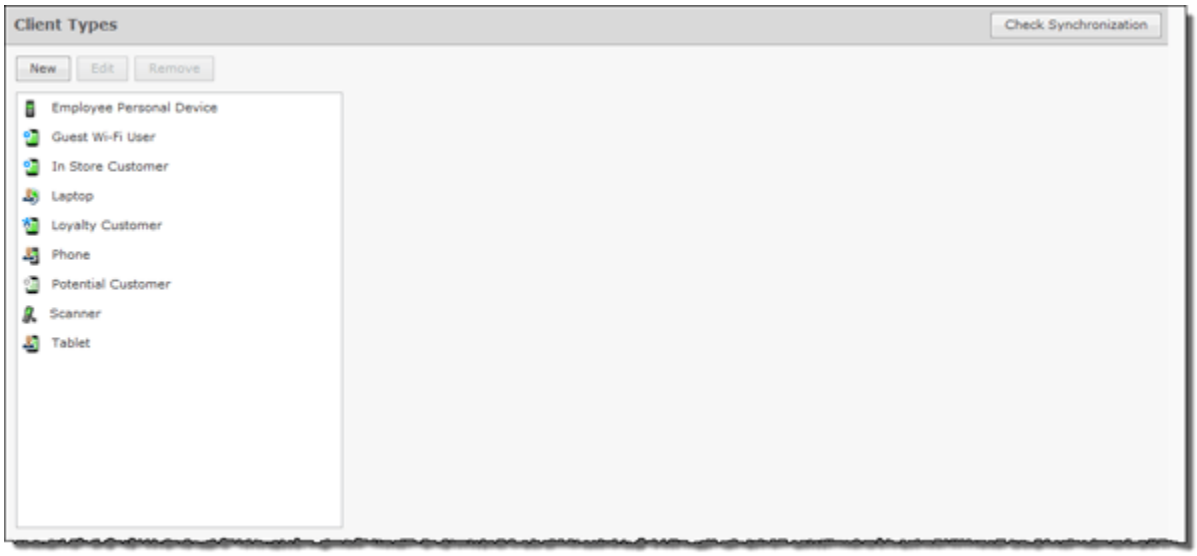
Alarm Library

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.

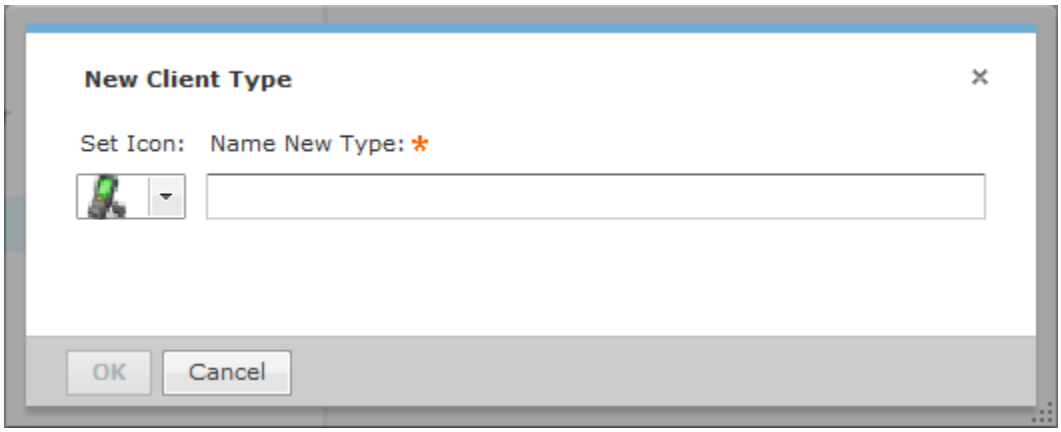
Client Types

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.



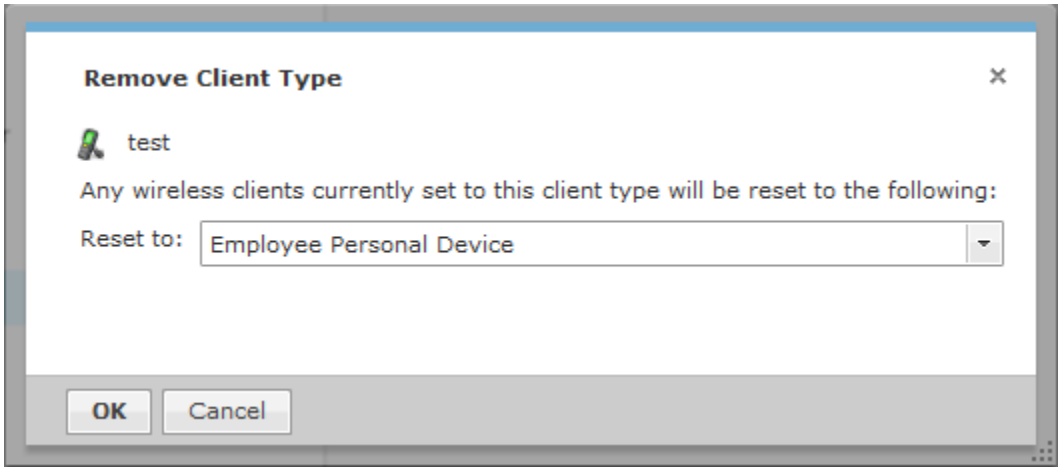
Click the **New** button to add a new client type.



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.

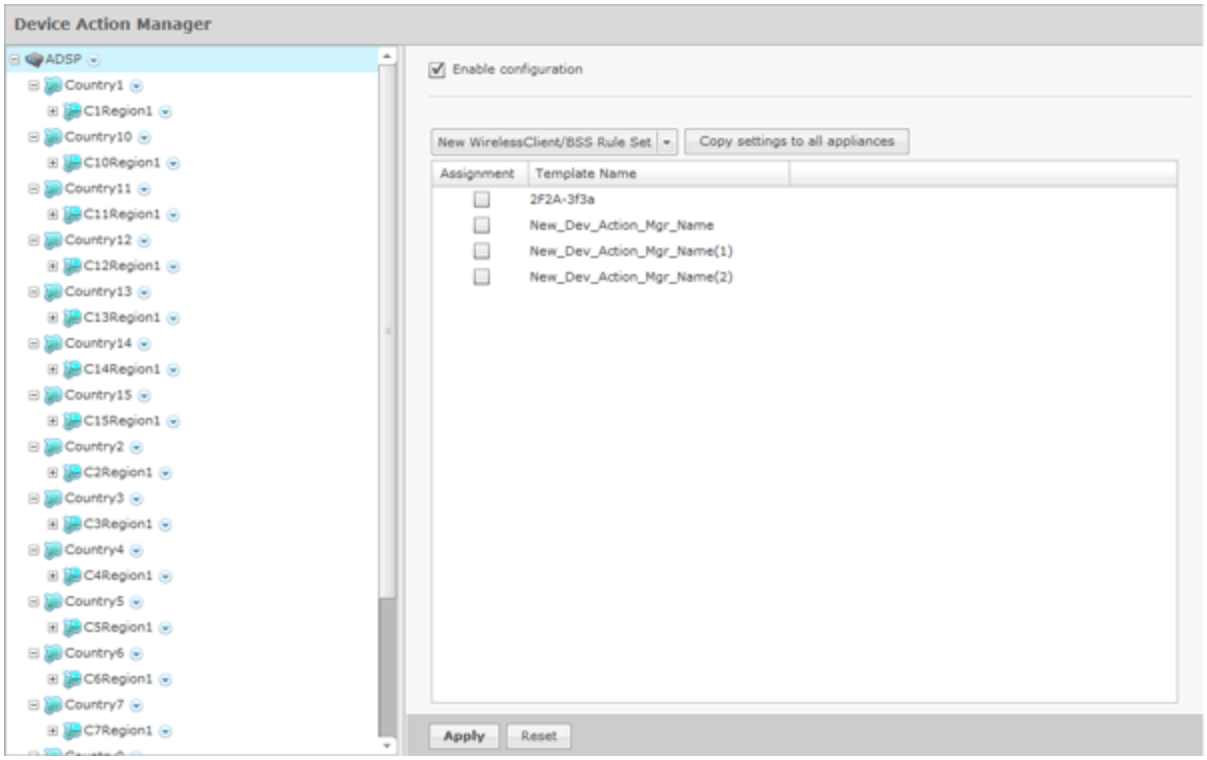


Click **OK** to remove the client type.

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 task; thus reducing management overhead. You may define as 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.

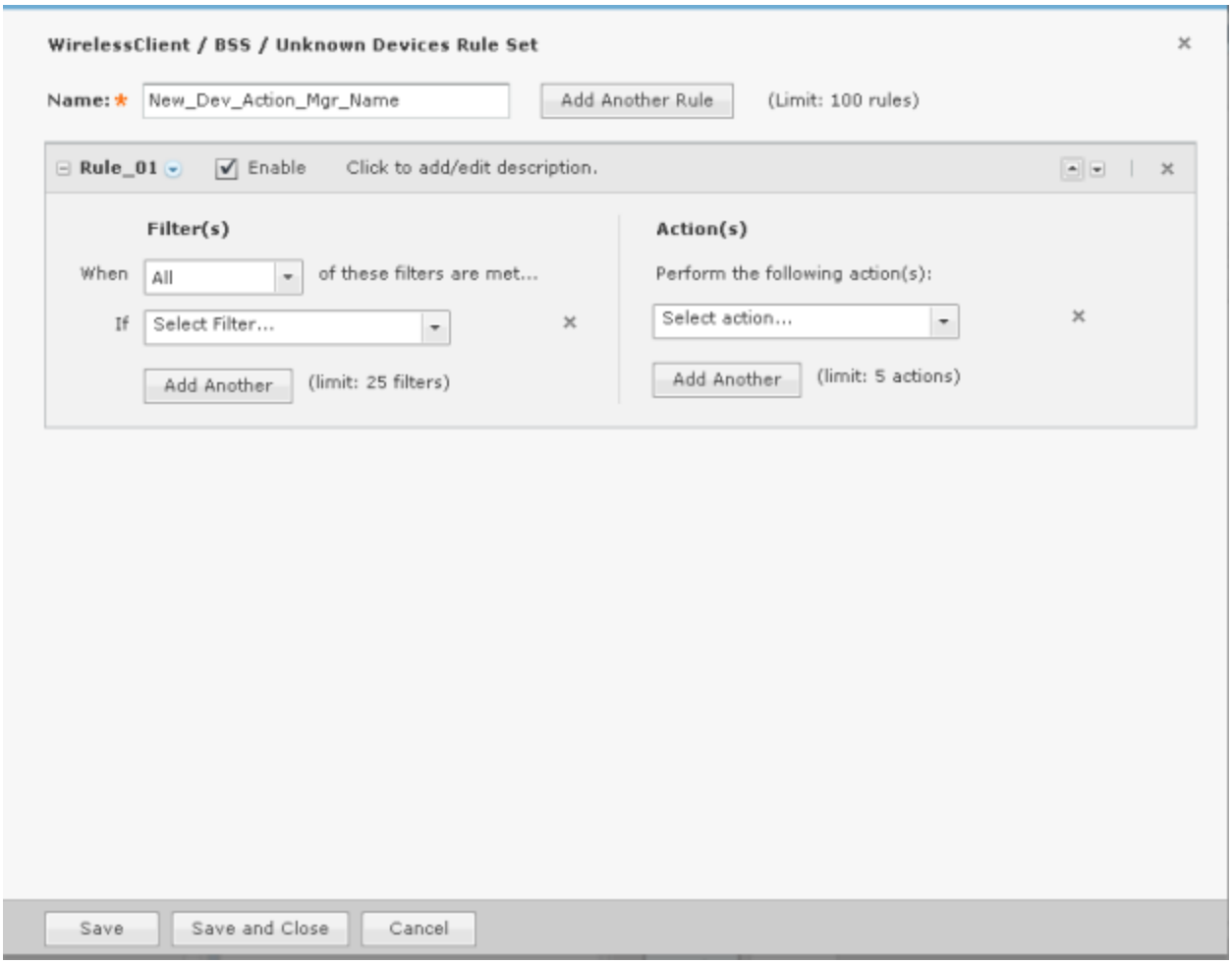
The Device Action Manager supports two types of rule sets: one for Wireless Clients/BSSs and one for Infrastructure devices. ADSP uses a dual purpose button to access the rule sets:

- 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.

Add a New Wireless Client/BSS/Unknown Devices 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.

Configuring Filters

Configure your filters by using a **When** statement and an **If** statement. Begin by 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:

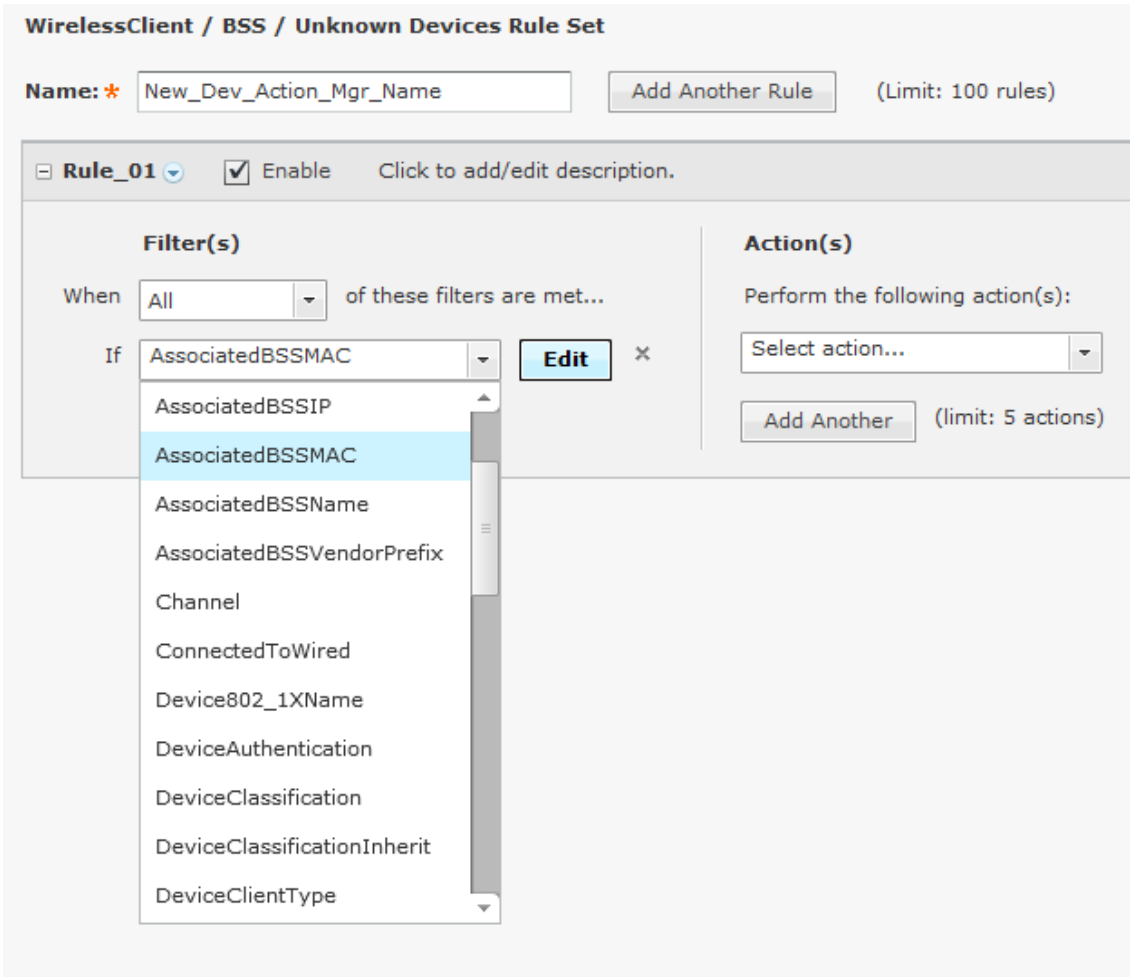
- Adhoc
- Associated
- AssociatedBSSClassification
- AssociatedBSSIP
- AssociatedBSSMAC
- AssociatedBSSName
- AssociatedBSSVendorPrefix
- Channel
- ConnectedToWired
- Device802_1XName
- DeviceAuthentication
- DeviceClassification
- DeviceClassificationInherit
- DeviceClientType
- DeviceEncryption
- DeviceFirstPolled
- DeviceFirstSeen
- DeviceIP
- DeviceLastPolled
- DeviceLastSeen
- DeviceMAC
- DeviceManufacturer
- DeviceName
- DevicePolledID
- DevicePolledSSID
- DeviceProtocol
- DeviceSSID
- DeviceSensedID
- DeviceSensedSSID
- DeviceType

- DeviceVendorPrefix
- SensorIP
- SensorMAC
- SensorName
- SignalStrength
- WatchList
- WiFiDirect.

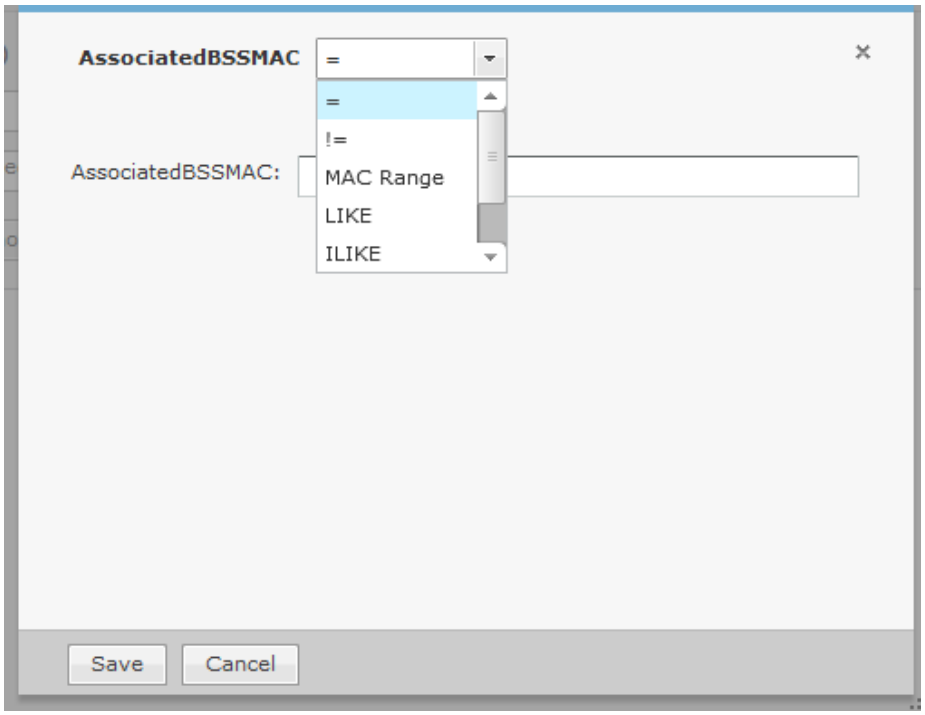
IMPORTANT In DeviceActionMgr, the filters order within the rule are order dependent. For example, if you want create a rule to sanction BSSs, the first filter would be DeviceType=Include BSS (this would ignore all clients), then DeviceManufacturer and then SSID. If you are using LIKE or ILIKE the % sign is a wildcard. (LIKE or ILIKE can also be used for wildcards.)

Selecting Filters

Select a filter by clicking the drop-down arrow next to the Select Filter box.



When you select a filter, 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.



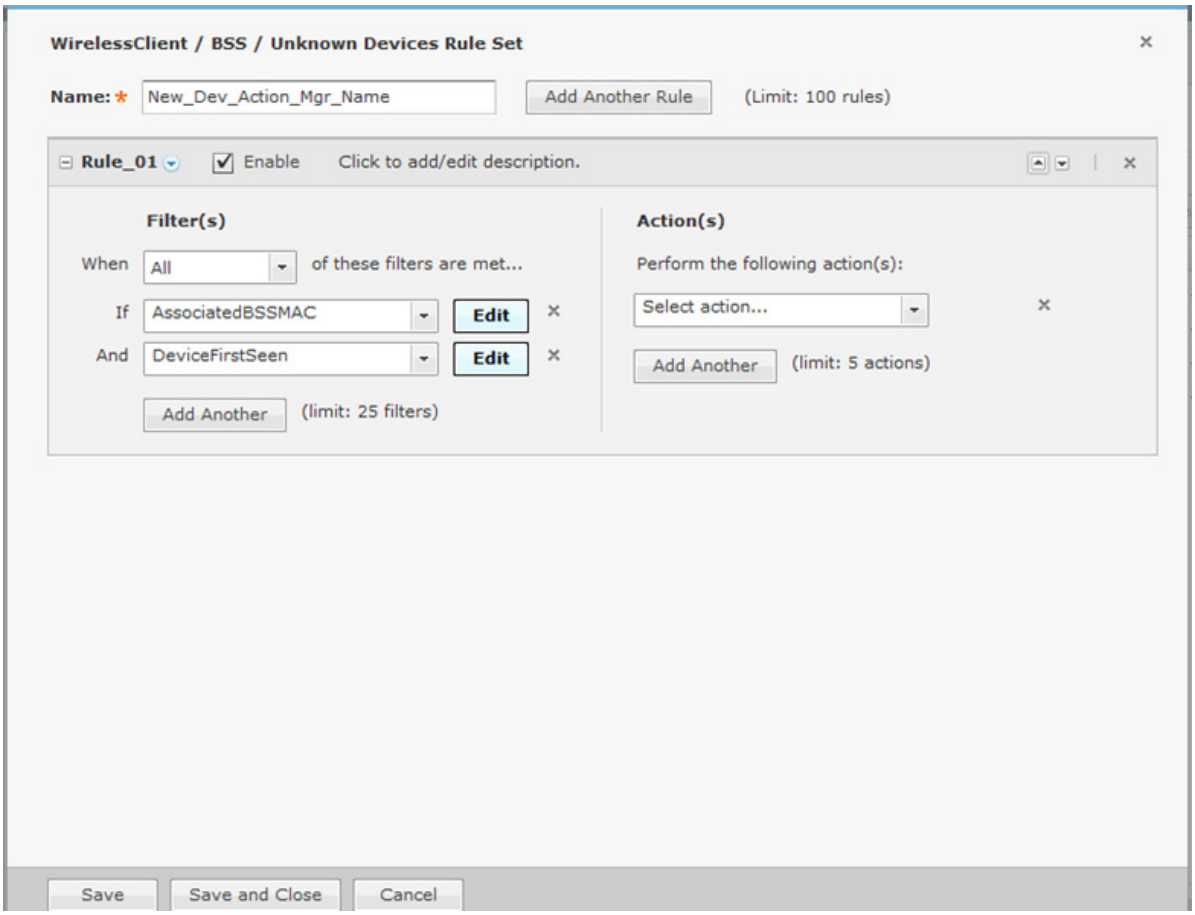
Click the drop-down menu to select the type of comparison. This will vary according to the selected filter. The type of comparison may be:

- = Is equal to
- != Is not equal to
- < Is less than
- <= Is less than or equal to
- MAC Range Range to pick up MAC address.
- > 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 **Save** 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.

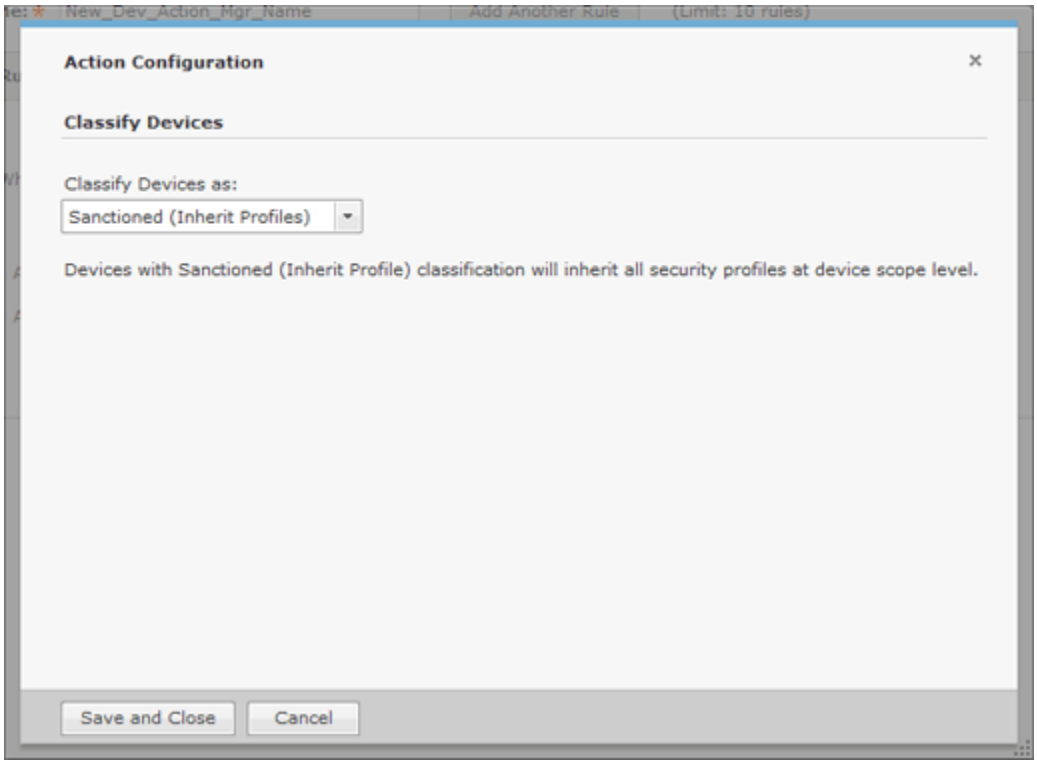
Actions

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.

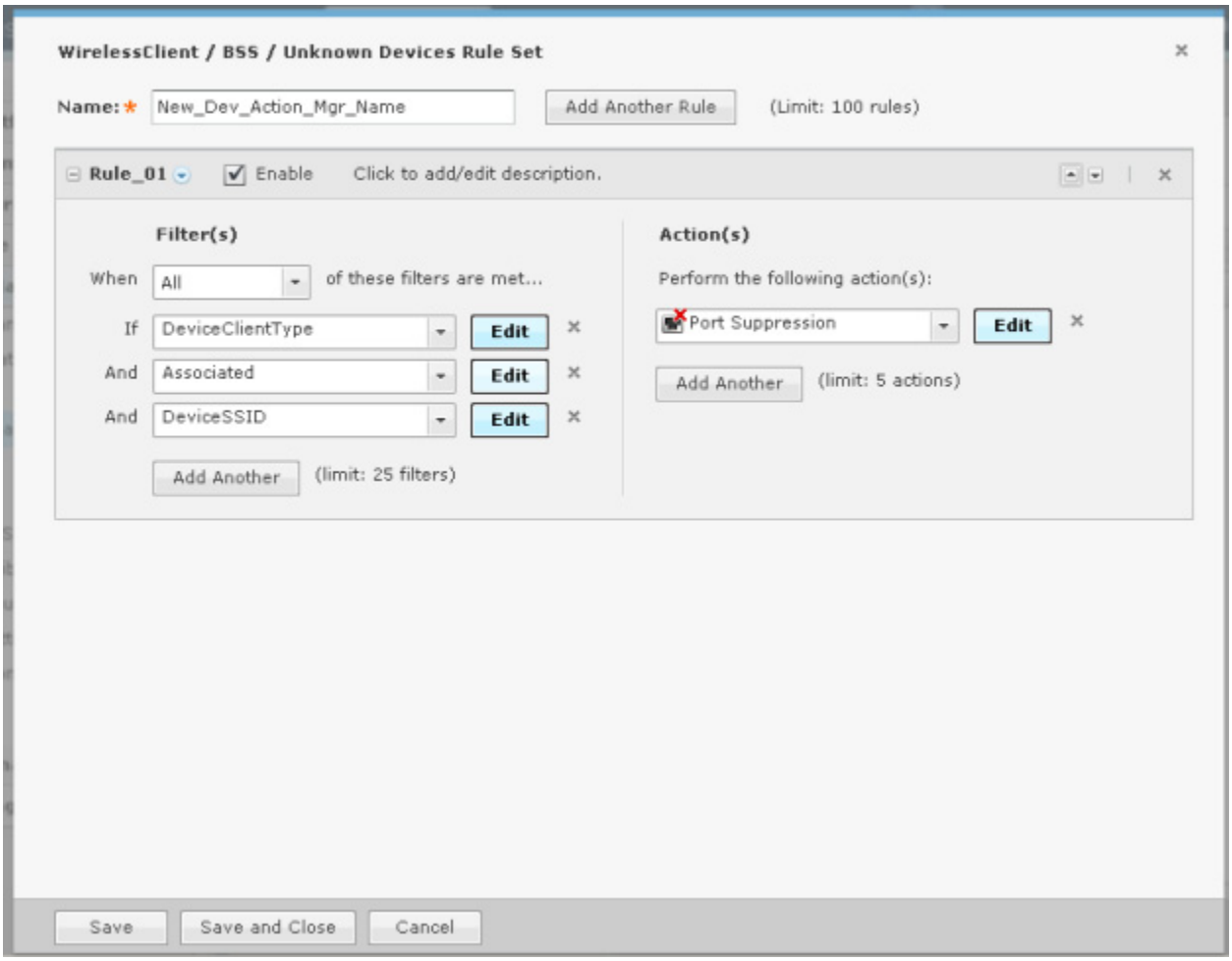
- Frame Capture—Monitors and analyzes real-time data traffic flow from devices in your wireless LAN and saves the data in a file if the conditions defined in the filter(s) are met.
- Vulnerability Assessment—Runs an vulnerability assessment using the specified profile if the conditions defined in the 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.

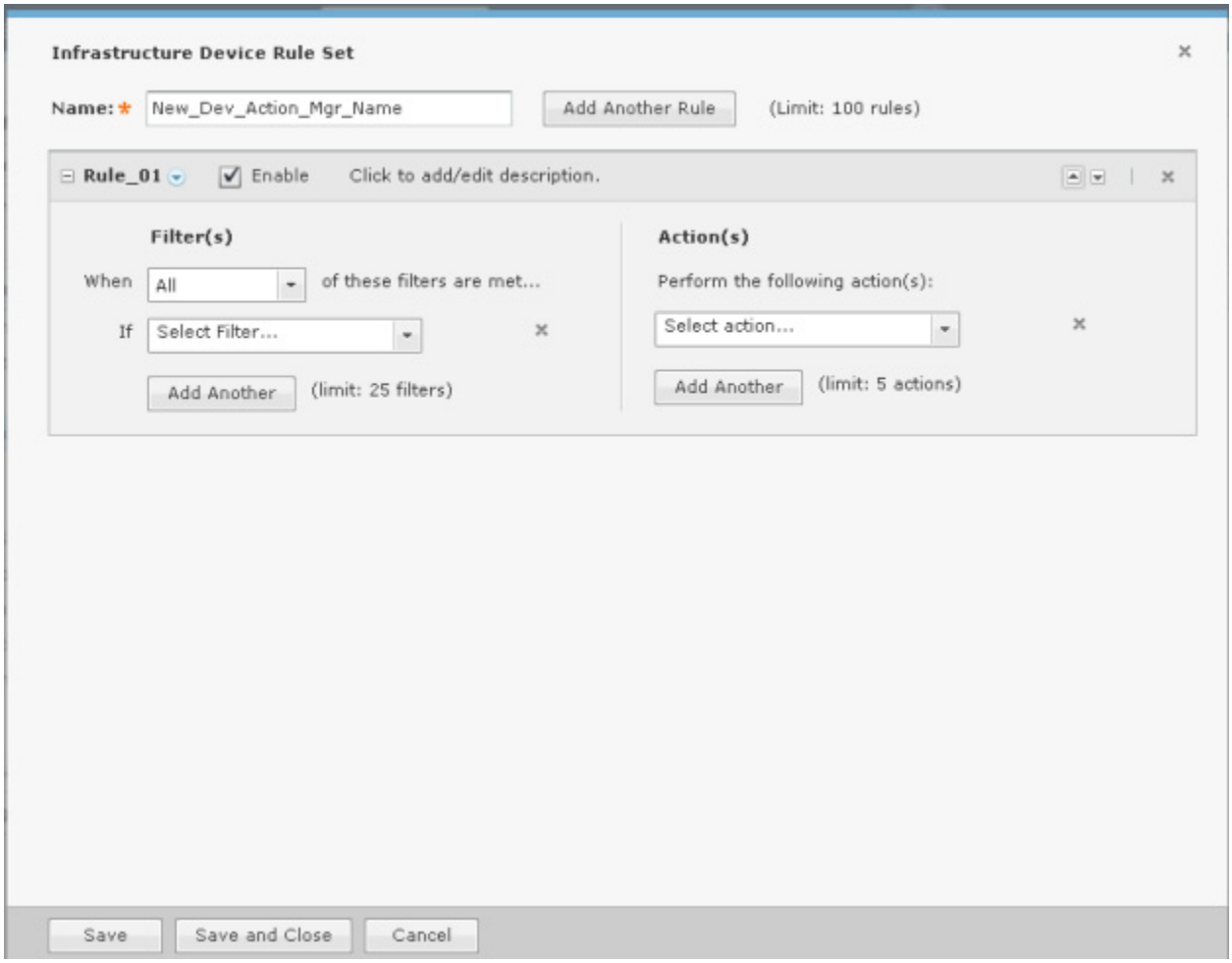


You can remove an action by clicking the **x** next to the action.

Click the **Save and Close** button to save the rule set and exit the window.

Add an 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.



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.

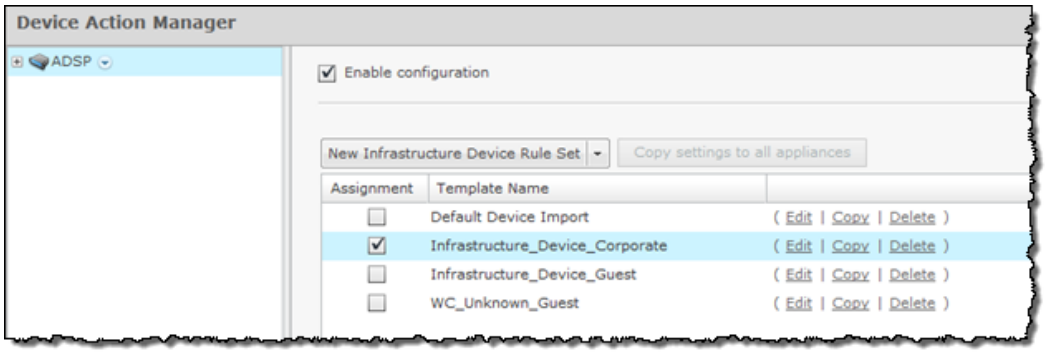
Actions

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).

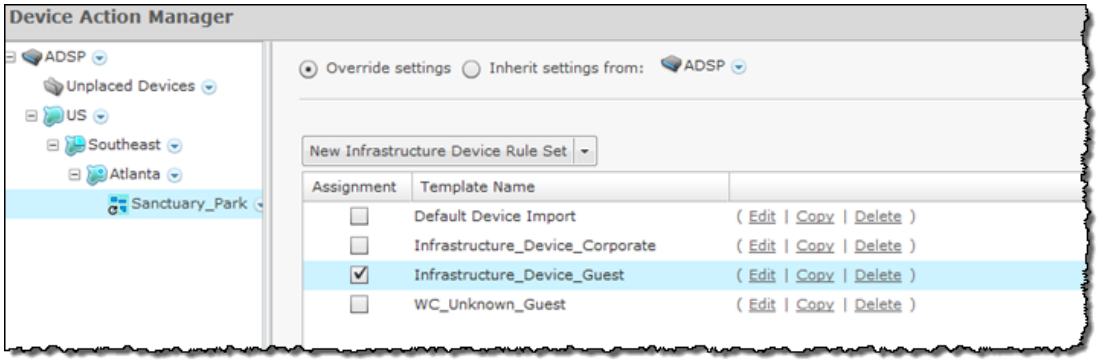
Applying a Device Action Manager Template

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 **Infrastructure_Device_Corporate** template; 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 **Infrastructure_Device_Guest** templates to the **Sanctuary Park** 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.

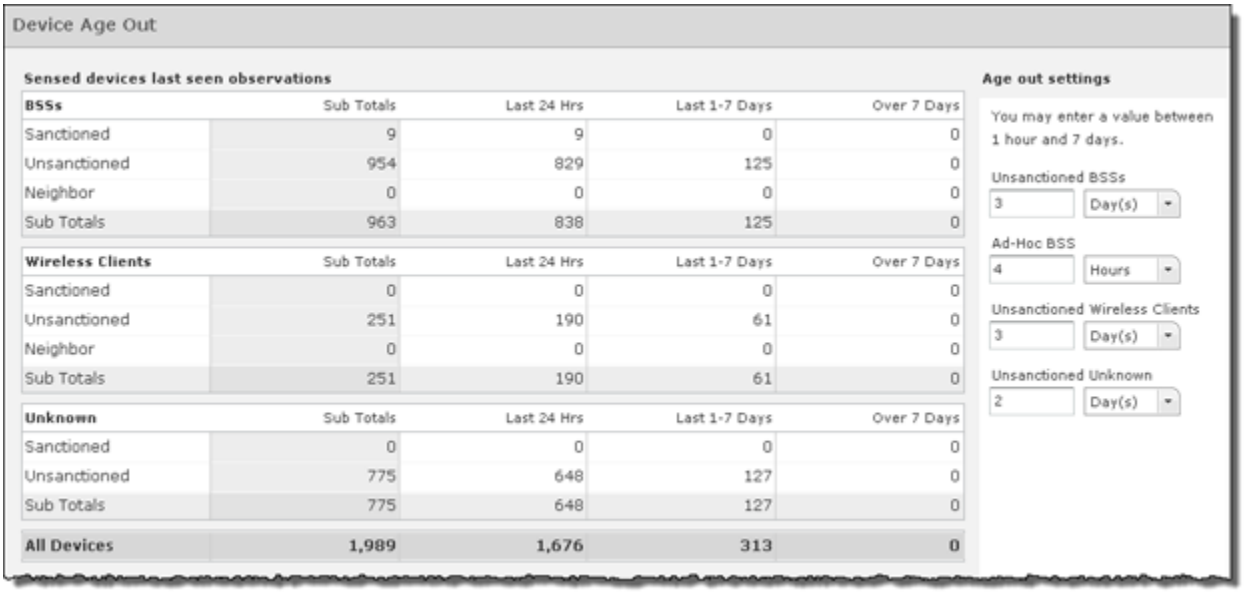
Sequence of Rules in Rule Sets

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.



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

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

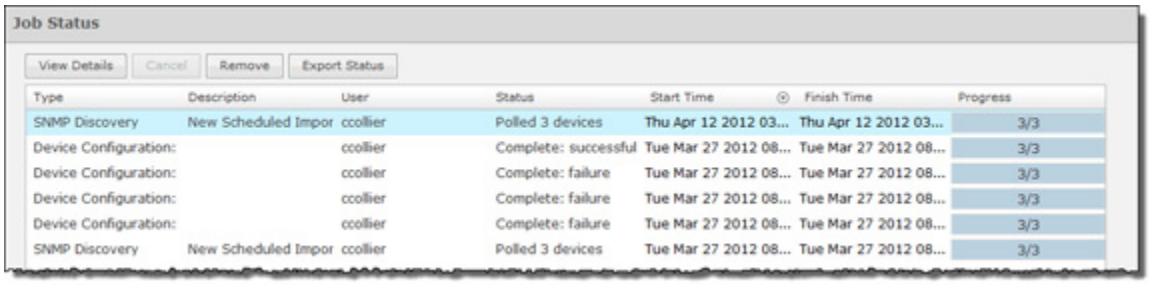
Values are specified in hours or days with a minimum of 1 hour and a maximum of 7 days. If you enter an illegal value, the field is highlighted by a red box.

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.



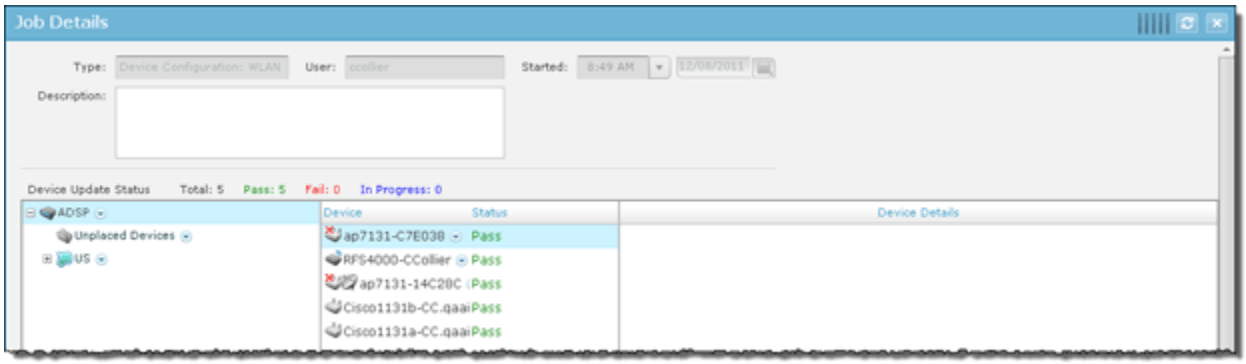
Job statuses are displayed in table format with seven columns.

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.

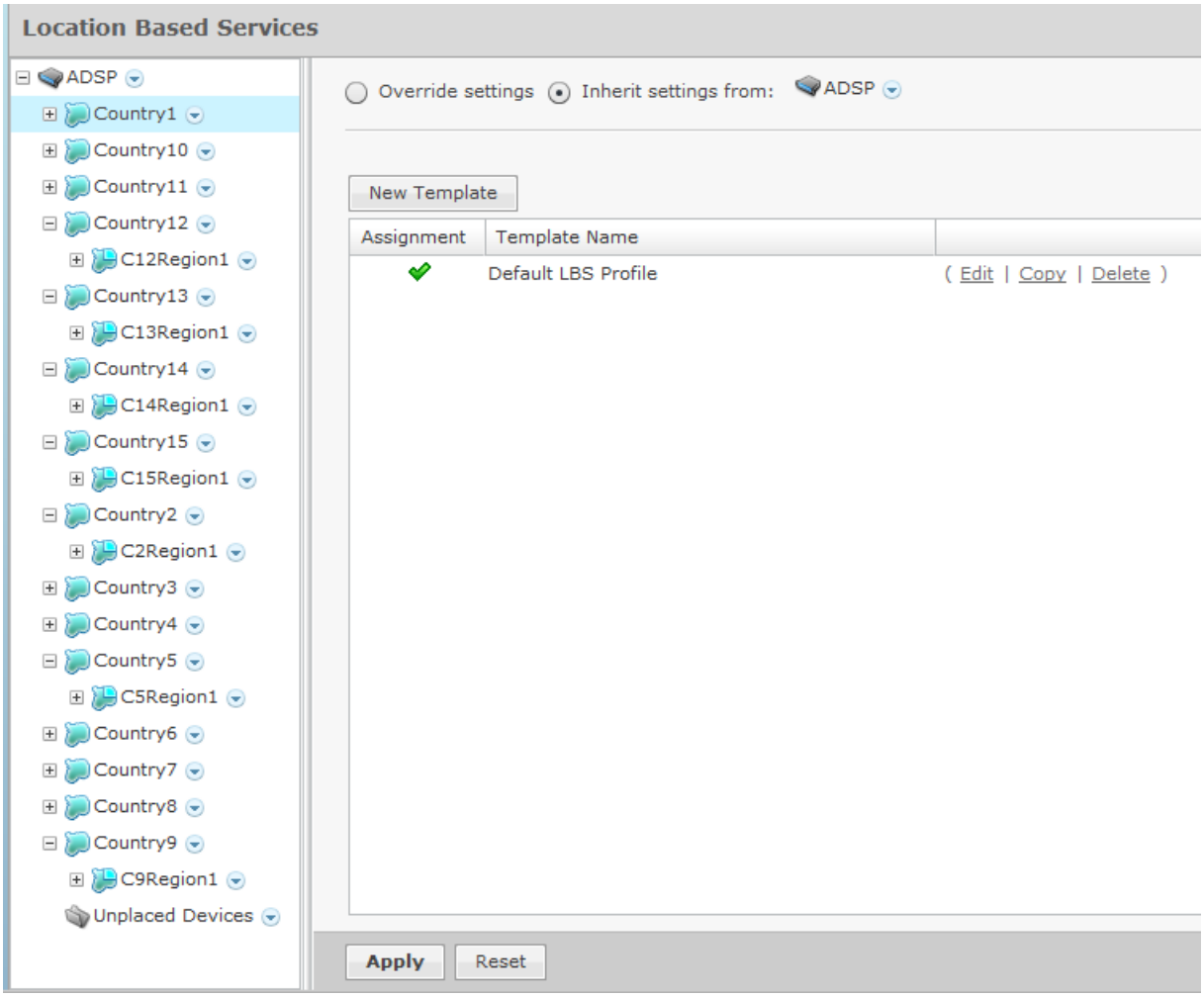
Location Based Services

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. For each device type, you will need to create and assign an LBS profile.

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

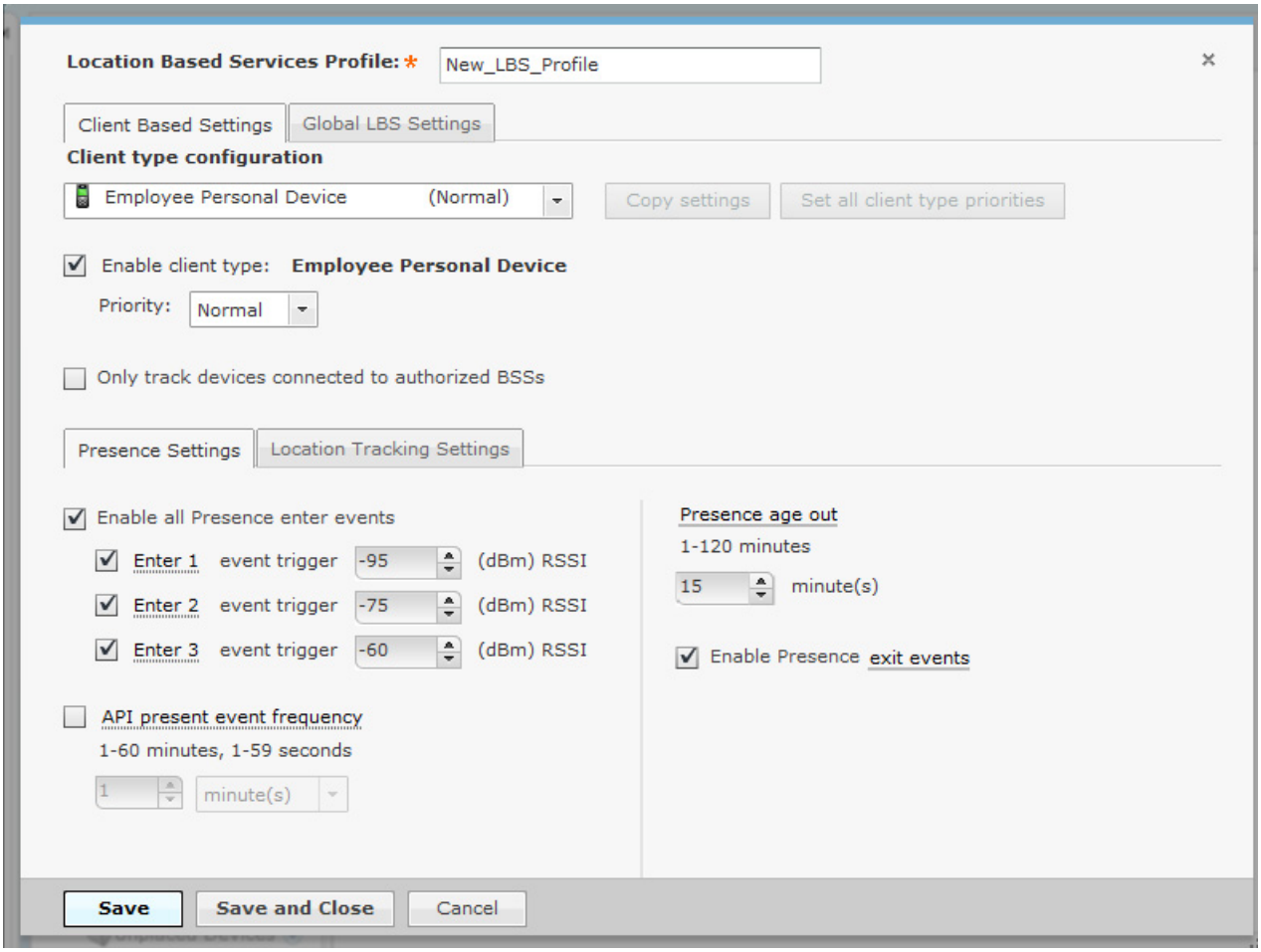
Location Based Services Profiles

The LBS profile provides information that allows ADSP to track devices by location. To manage your LBS profiles, go to Configuration>Operational Management>Location Based Services to display the LBS screen.



Add a New LBS Profile

From the Location Based Services Profile screen, click the New Template button to add a new profile. Enter the Location Based Services Profile name.

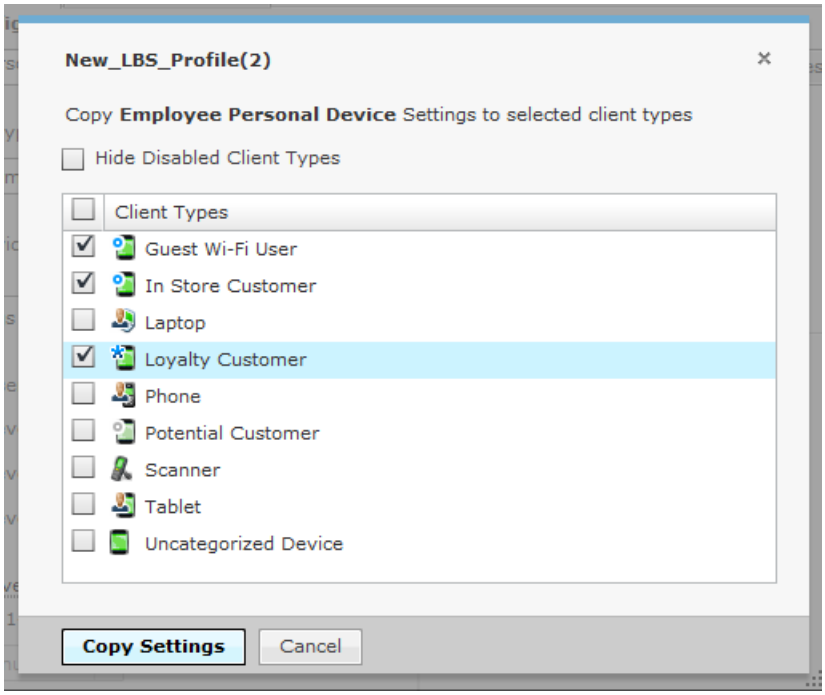


Select the **Client Based Settings** tab and define your LBS profile by following the steps outlined in the following sections.

Client Type Configuration

Copy Settings

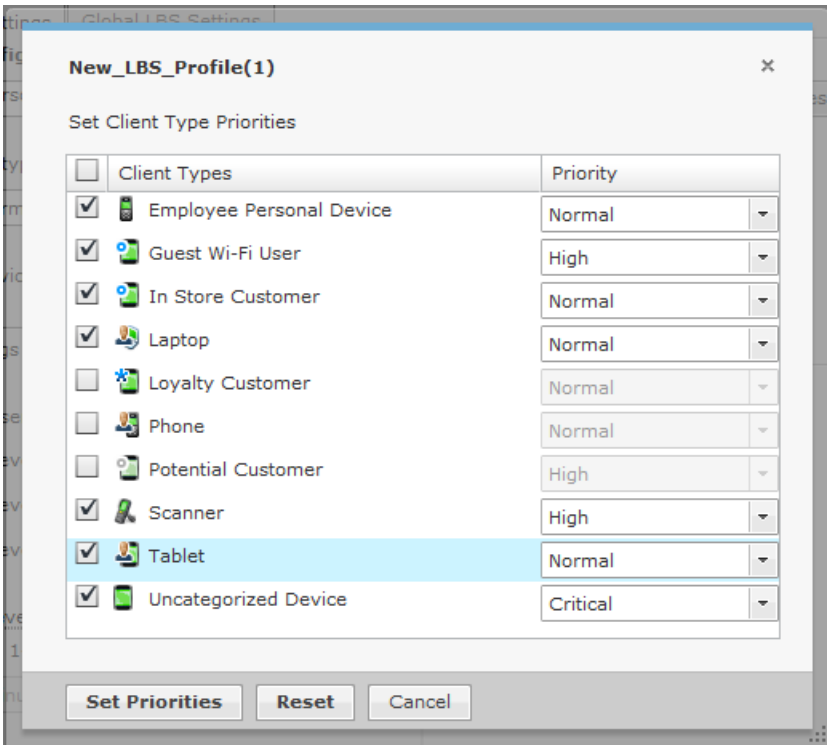
You can copy settings for the selected client type(s). Select the client type you want to copy and click the Copy Settings tab. Select the client types you want to copy the settings to by checking the checkbox.



When finished selecting, click Copy Settings to copy the settings and return to the previous dialog box.

Set Client Type Priorities

Click the **Set All Client Type Priorities** tab to display a list of client types. On this screen you can select which client types you want to track and prioritize the devices in order of importance. The choices are critical, high, normal and low. Select the checkbox of the client type you want to prioritize or select the checkbox at the top of the list for all clients' types. If you do not wish to track a certain client type, leave the checkbox blank to disable that type. See the following example.



When finished, click **Set Priorities** to set your selected priorities and return to the previous dialog box.

Select the check box for **Only track devices connected to authorized BSSs** if desired for the selected devices.

Client Based Settings

Presence 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.

Location Tracking Settings

Define the Client Based Settings for your LBS profile using the following fields found in the **Location Tracking Settings** tab:

Field	Description
Select all Sources	Select the type of source to use (**Wi-Fi Zones** or **Wi-Fi Positioning**).
Enable all Virtual Region Events	Identifies which of the available virtual region events the given device can trigger: **Enter**, **Exit**, **Proximity**, and/or **Contained**.
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.

Apply an LBS Profile

Edit LBS Profiles

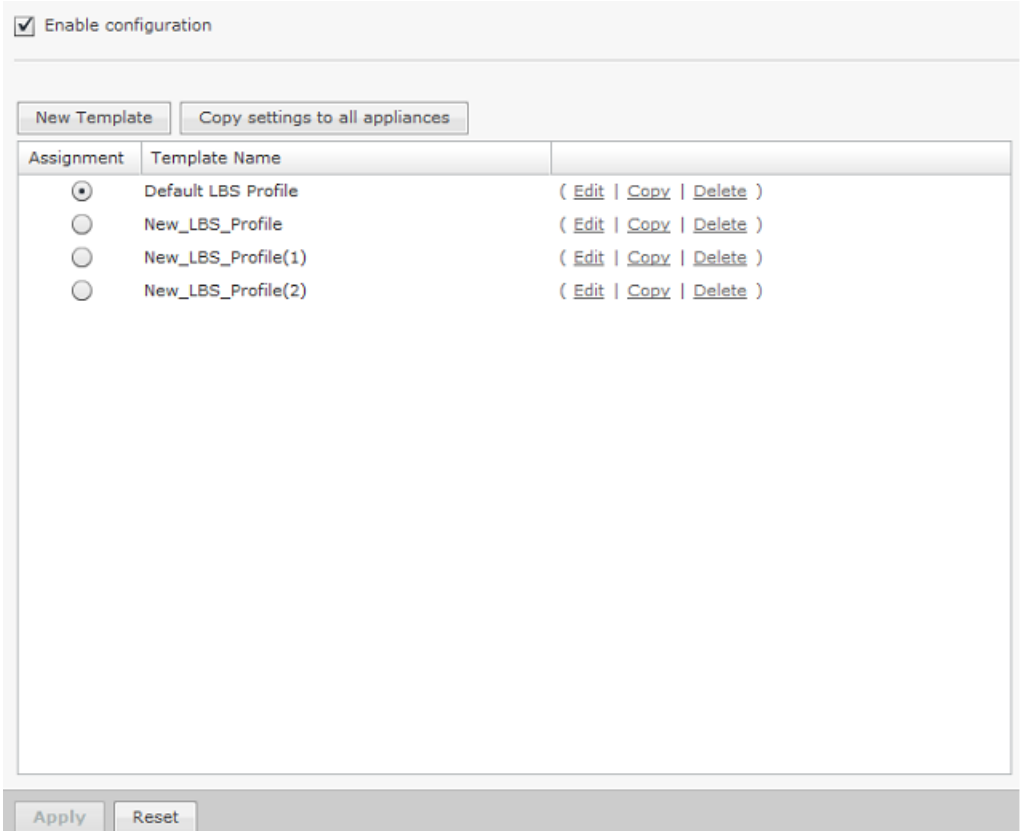
Yo have the option to edit, copy or delete the LBS profiles as needed. Follow these steps:

1. Select (highlight) the LBS profile.
2. Click the **Edit**, **Copy** or **Delete** link and make your changes.
3. Click **Save** to save your changes.

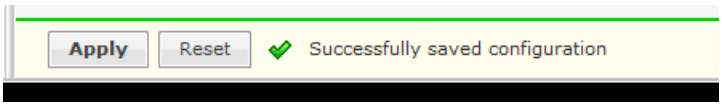
Copy Settings to all Appliances

Once you have defined an LBS profile, to use it, you must apply it to your system. You should always apply an LBS profile at the ADSP appliance level. Click Copy settings to all appliances to copy the defined LBS profile to all appliances in your system.

NOTE You must have a Central Management license in order to copy settings to all appliances.

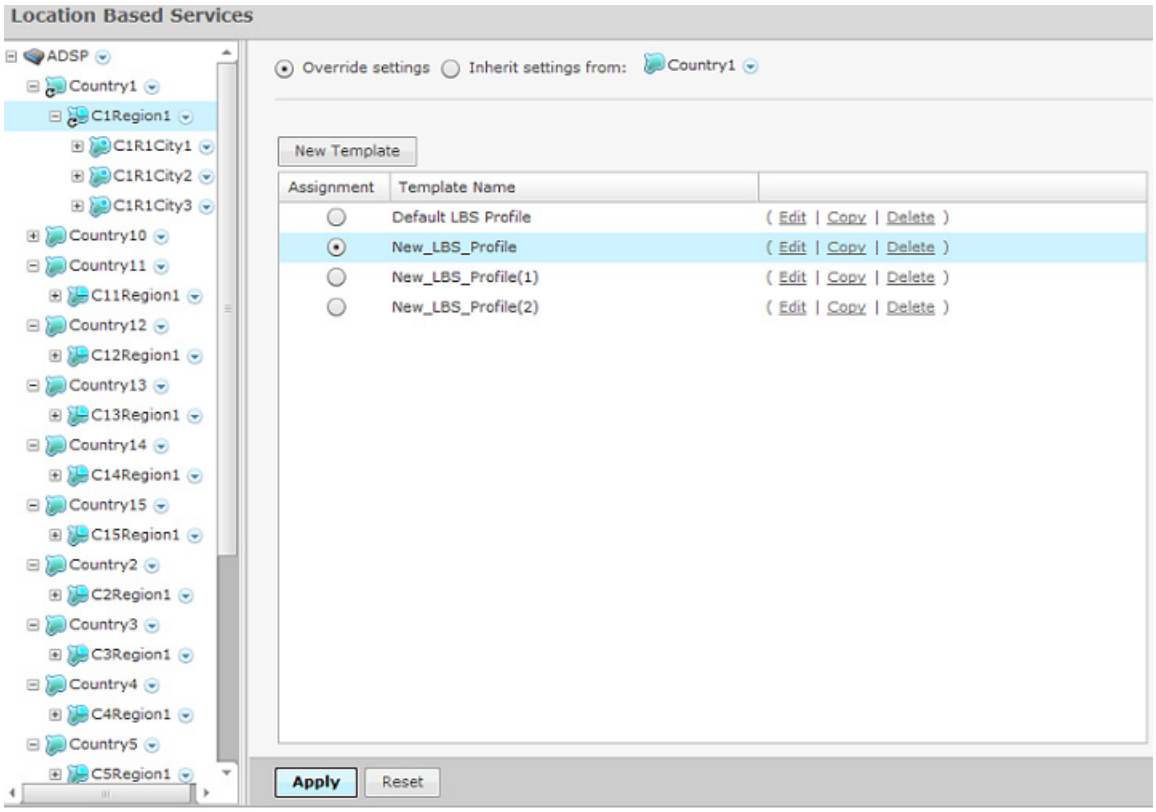


Click **Apply** to save your changes. A confirmation is displayed the bottom of the screen:



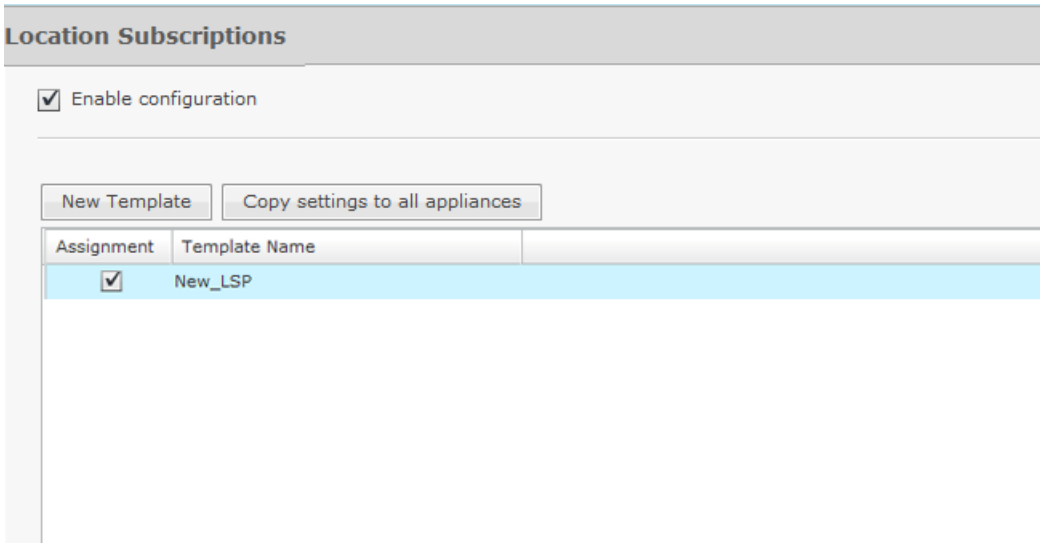
Set Different Profile

If you have a level that needs a different LBS profile, you can apply a different profile to that level. The **Override settings** option is available when you select (highlight) a network level below the appliance level. Use the **Expand**–⊞ button beside the ADSP appliance icon to reveal the other levels.



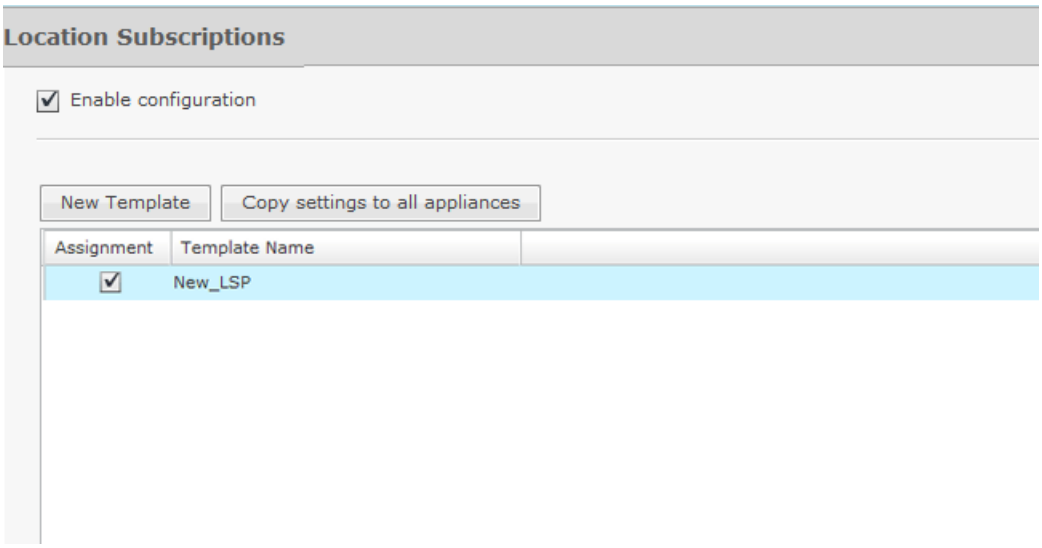
For example, in the above screen shot, the LBS profile for ADSP shows as the **Default_LBS_Profile**. In the left column you have selected the Country1 level and you can use the **Override settings** option and apply the **New_LBS_Profile** profile. Click **Apply** to save your changes.

NOTE Updates to LBS profiles are treated as jobs and are included in Job Status under Configuration > Operational Management.



Location Subscriber Profiles

Use Location Subscriber Profiles 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.

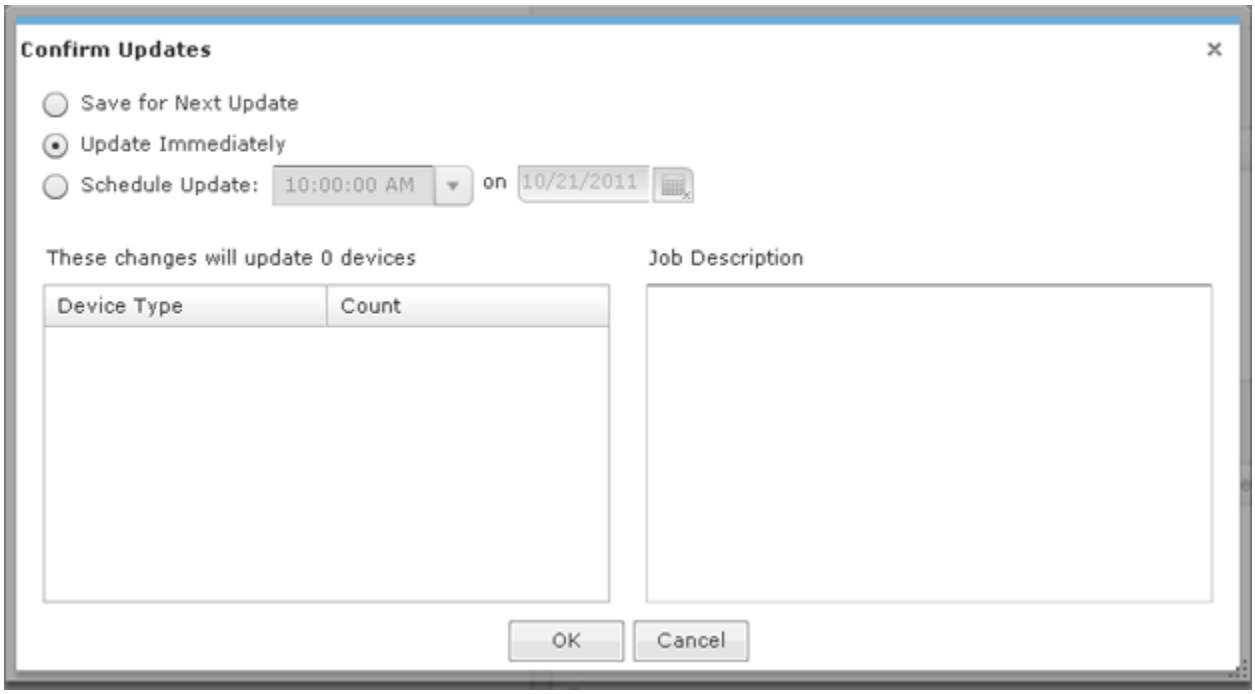


You can edit, copy or delete any selected (highlighted) profile by clicking the appropriate link. To edit or copy a profile, select (highlight) the profile, click the **Edit** or **Copy** link, and then make your changes. Click **Save** to save your changes.

The Copy settings to all appliances button will copy the defined Location Subscriber 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 **Apply** to save your additions (changes). A confirmation overlay is displayed.



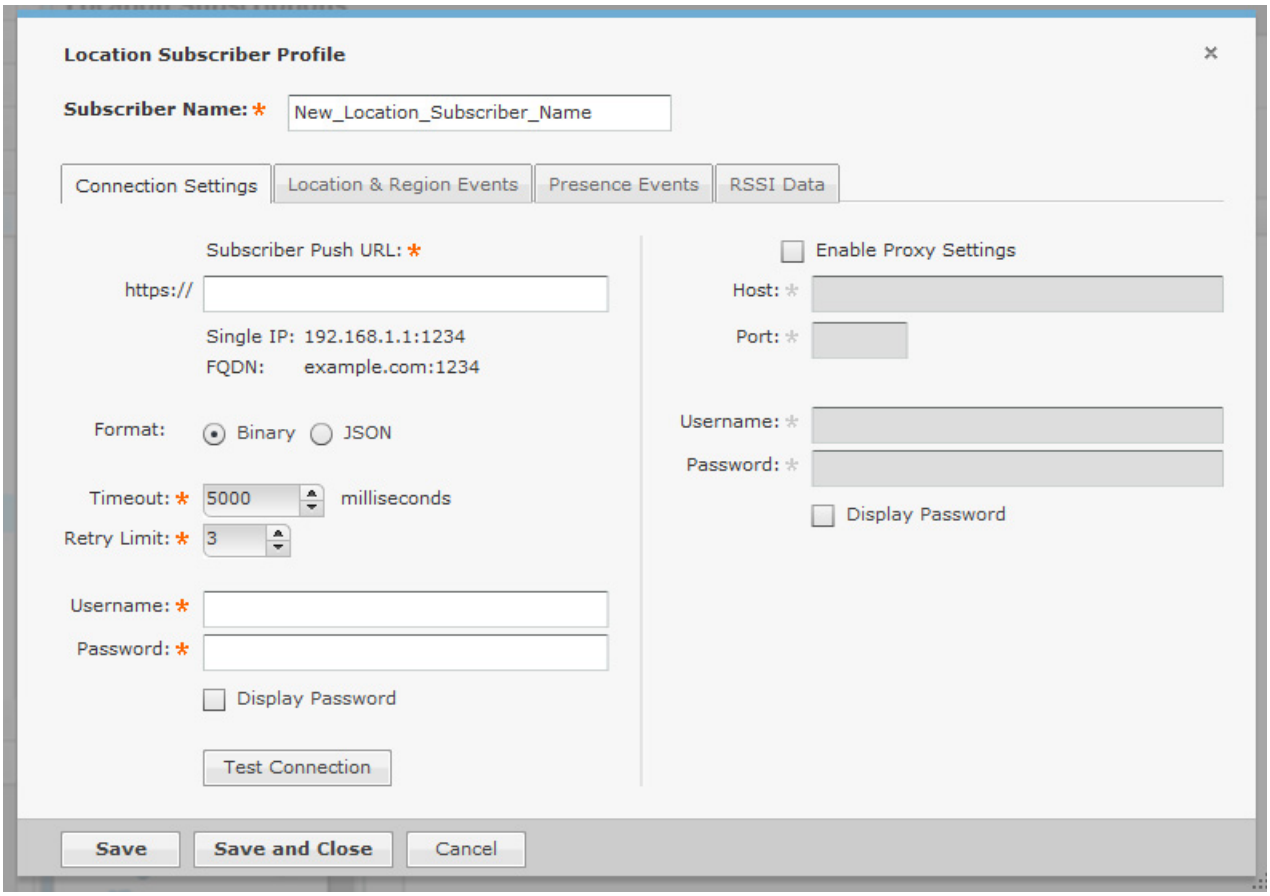
You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later. A list of device types along with the number of affected devices that will be updated is displayed. Also, if applicable, a list of unsupported settings is displayed. Click **OK** to apply changes or **Cancel** to abort.

Updates to 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 **Reset** to discard any additions (changes).

Add a New Location Subscriber Profile

Click New Template to add a new profile.



.Name your Location Subscriber Profile in the **Subscriber Name** field and use the following tabs to define the profile:

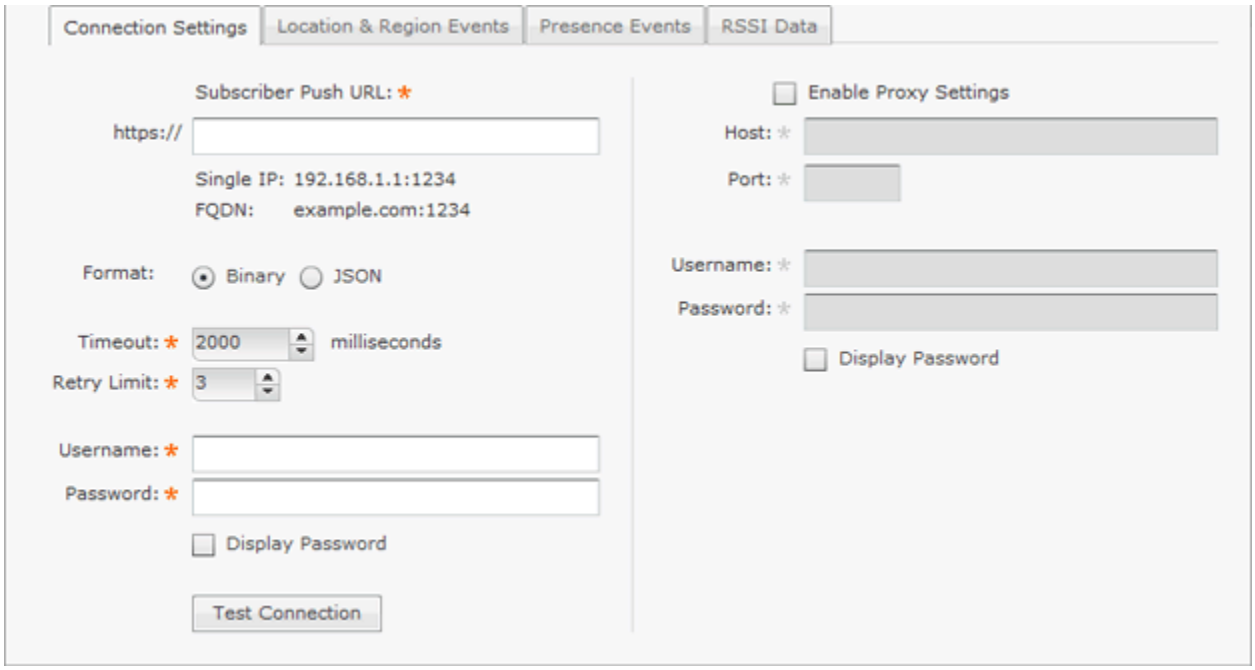
- Connection Settings
- Location & Region Events
- Presence Events
- RSSI Data.

NOTE These tabs are described in detail in the following sections.

After defining the profile, click **Save and Close** to save the profile and exit. Click **Save** to save the profile and leave it open. Click **Cancel** to cancel any changes that are not saved and exit the profile.

Connection Settings—Location Subscriber Profile

Use the Connections Settings tab to set up an secured connection to a third party application.



The Connections 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 (**Binary** or **JSON**).
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 user name used to authenticate the connection.
Password	Specifies the password of the user making a connection. You may select the Display Password checkbox to reveal the password.

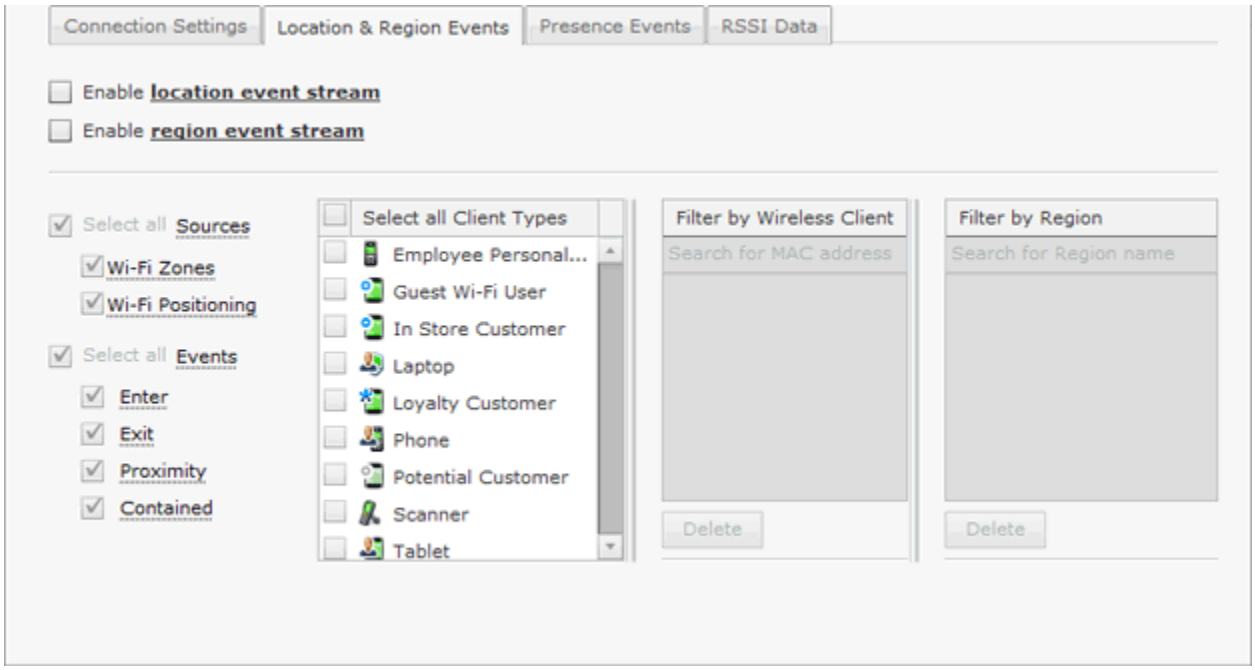
You can test the connection to see if it is working by clicking the Test Connection button.

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.
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 **Display Password** checkbox to reveal the password.

Location & Region Events—Location Subscriber Profile

Use the Location & Region Events tab to stream location and region events to a third party application.

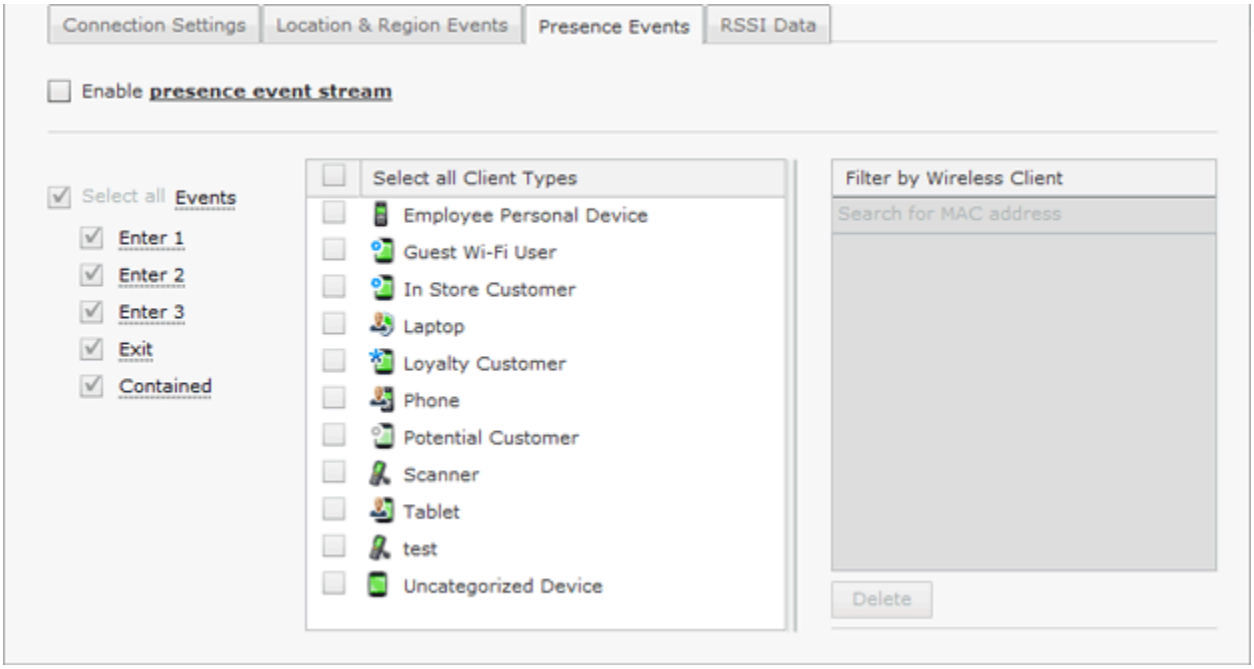


Field	Description
Enable location event stream	Select checkbox to turn on streaming location events to a third party application.
Enable region event stream	Select checkbox to turn on streaming regional events to a third party application.
Select all Sources	Select the type of source to use: Wi-Fi Zones (zone tracking) or Wi-Fi Positioning Zones (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 3rd 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 Enter, Exit, Proximity, and/or Contained. 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 Select all Client Types, 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—Location Subscriber Profile

Use the Presence Events tab to stream presence events to a third party application.

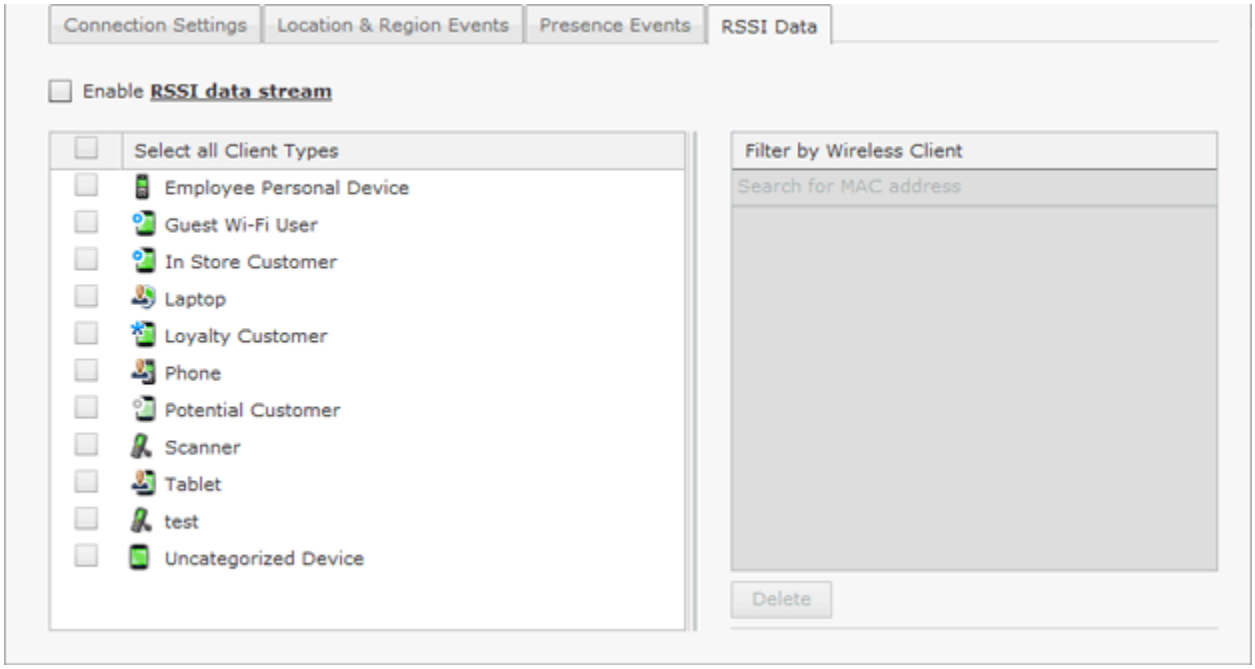


Field	Description
Enable presence event stream	Select checkbox to turn on streaming presence events to a third party application.
Select all Events	Filters streaming by events. The event triggers are Enter 1, Enter 2, Enter 3, Exit, and/or Contained. You may select all the triggers by selecting Select all Event, 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 Select all Client Types, 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—Location Subscriber Profile

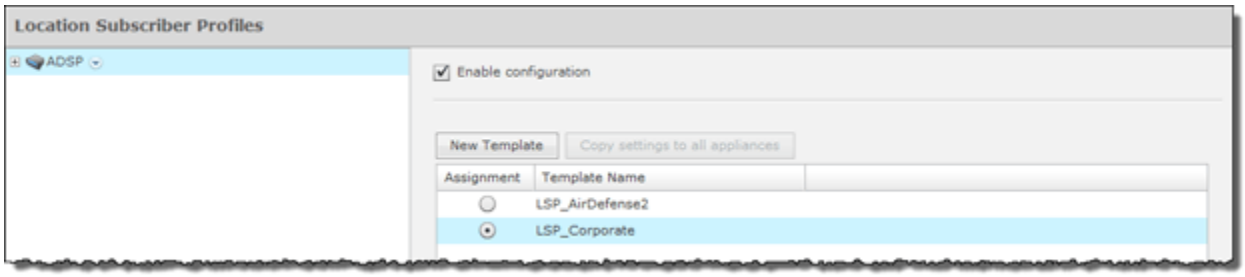
Use the RSSI Data tab to stream RSSI data to a third party application.



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 Select all Client Types, 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.

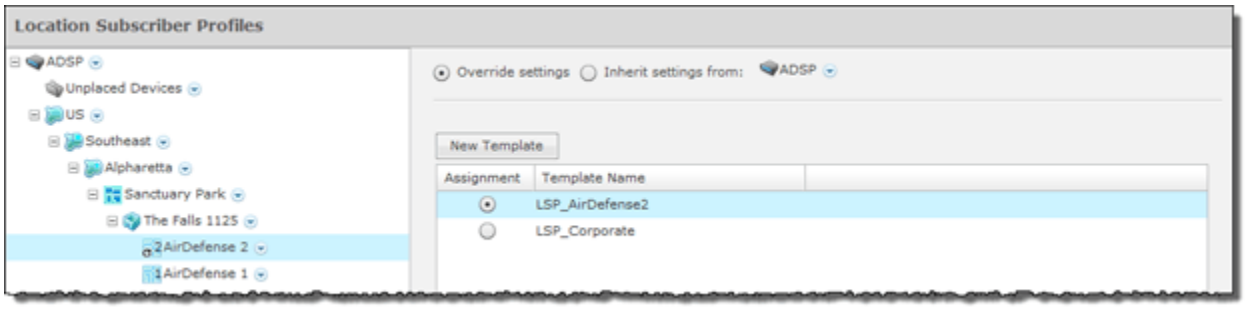
Apply an Existing Location Subscriber Profile

Once you have defined a Location Subscriber Profile, 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.

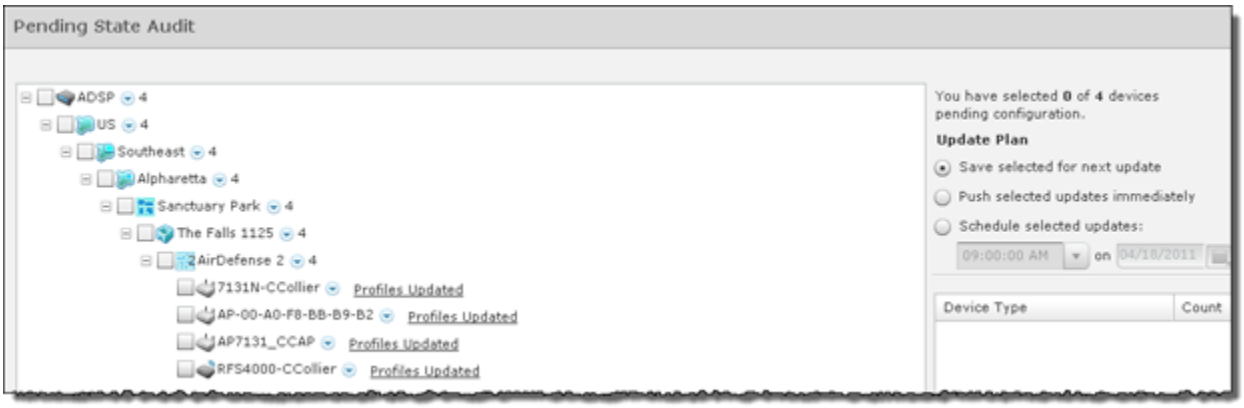


In this case, the **LSP_Corporate** profile will be accessible to corporate-wide employees and guest while the **LSP_AirDefense2** profile will be specific to employees and guests on Floor 2 of the AirDefense facilities. Click Reset to discard your changes.

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.



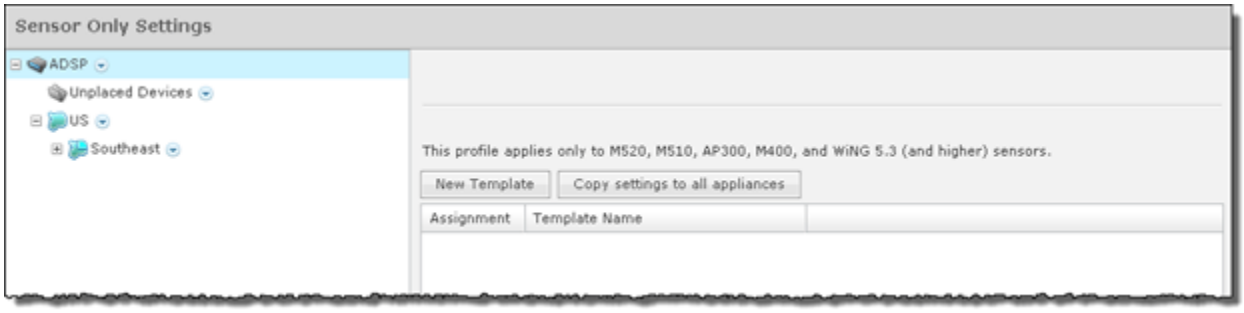
Folders with a checkmark identify that folder as having devices that in a pending state. Devices with a checkmark identify that device as a device that are in a pending state.

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 **Apply** 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 later) that are configured as a sensor only device. Legacy sensors include AP300, AirDefense M400, M510, and M520 sensors.



Existing profiles are displayed in the table below the row of buttons.

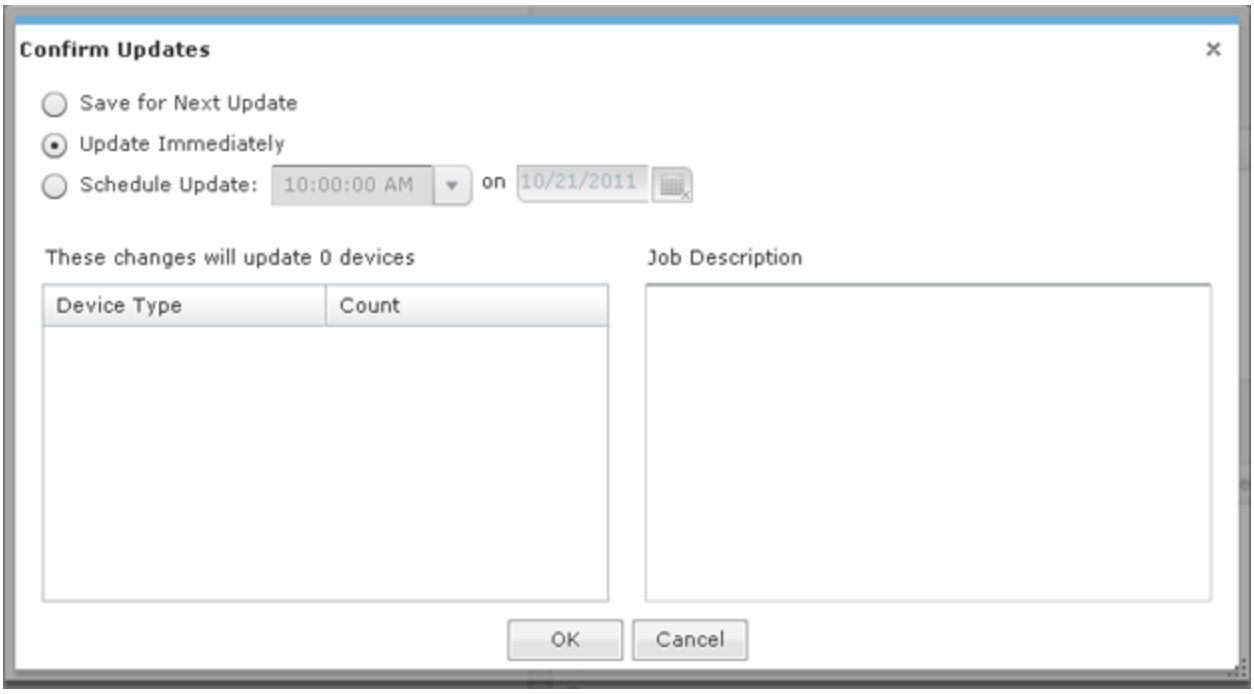
You can edit, copy or delete any selected (highlighted) profile by clicking the appropriate link.

To copy or edit a profile, select (highlight) the Sensor Only Settings profile, click the **Edit** or **Copy** link, and then make your changes. Click **Save** to save your changes.

Click **Copy settings to all appliances** to 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 **Apply** to save your additions (changes). A confirmation overlay is displayed.



In order to use Location Based Services to pinpoint a device location, a Sensor survey must be done using AirDefense Mobile 6.2 (or later.) 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.

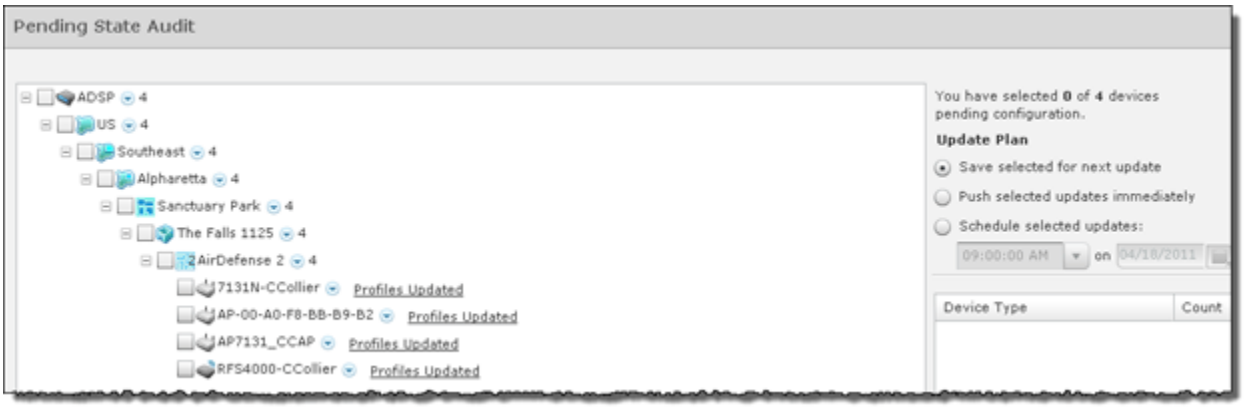
Reference Material for Location Based Services

For detailed information on location based services, see the Proximity and Analytics —Location Based Services Design and Configuration Guide. The configuration guide explains how to set up and use Location Based Services and conduct sensor surveys. To obtain a copy of the Proximity and Analytics —Location Based Services Design and Configuration Guide, go to the Support website for product manuals at the following URL: *www.zebra.com/support*

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.



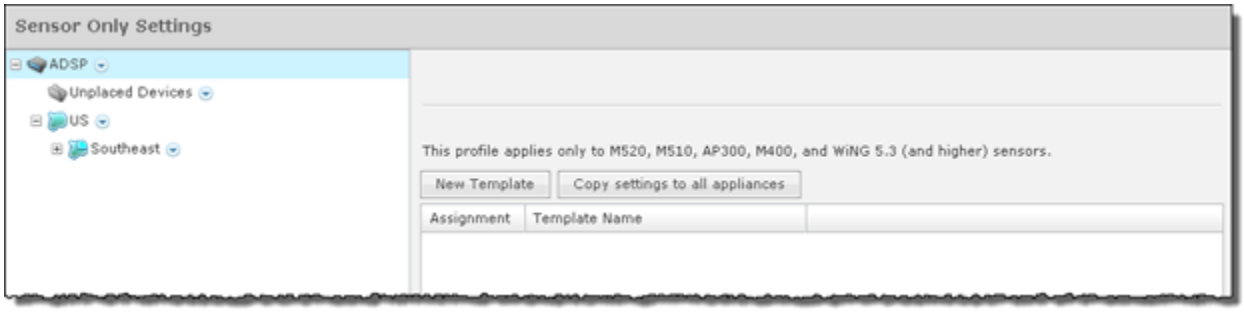
Folders with a checkmark identify that folder as having devices that in a pending state. Devices with a checkmark identify that device as a device that are in a pending state.

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 (or later) that are configured as a sensor only device. Legacy sensors include AP300, AirDefense M400, M510, and M520 sensors.



Existing profiles are displayed in the table below the row of buttons.

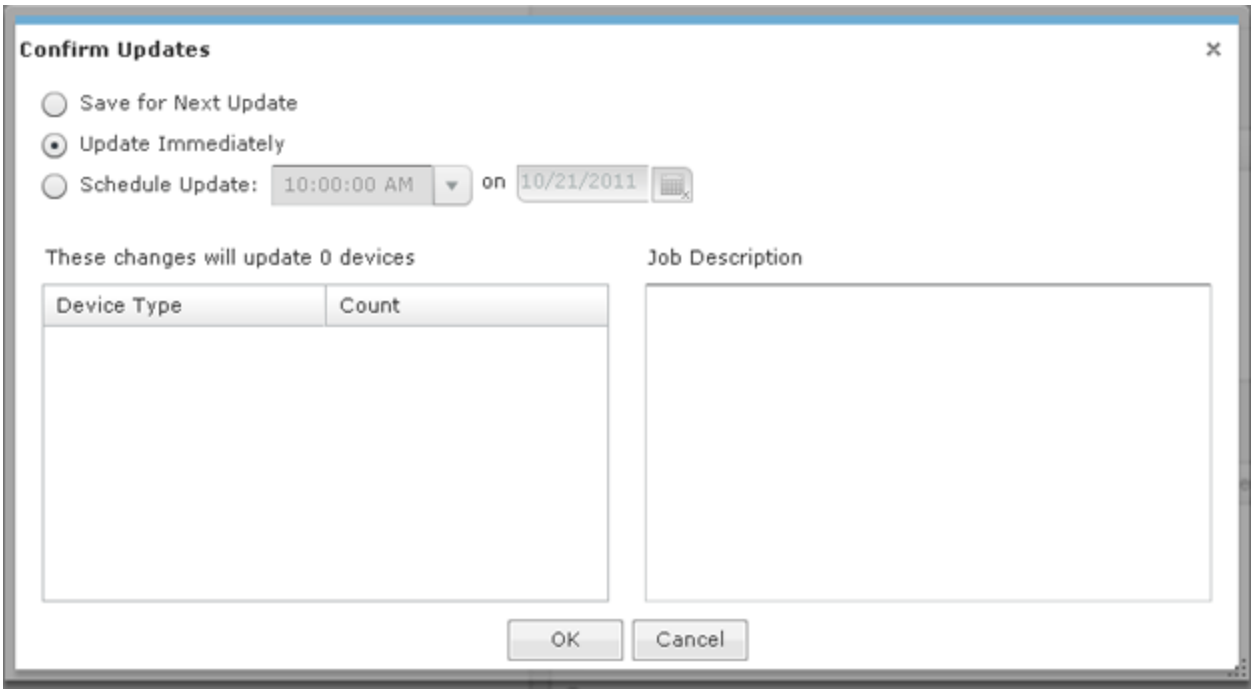
You can copy, edit or delete any selected (highlighted) profile by clicking the appropriate link.

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.

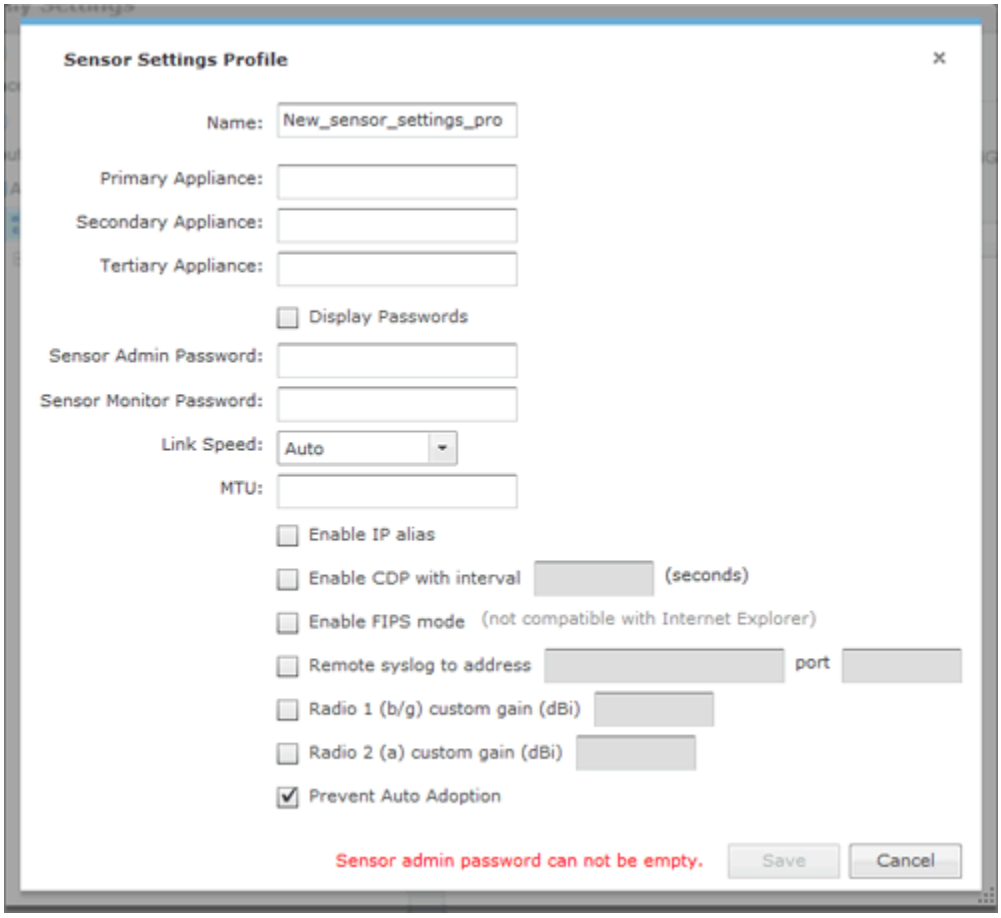


You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later. A list of device types along with the number of affected devices that will be updated 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).

Add a New Sensor Settings Profile

Click the **New Template** button to add a new profile.



Define your Sensor Settings profile using the following fields are:

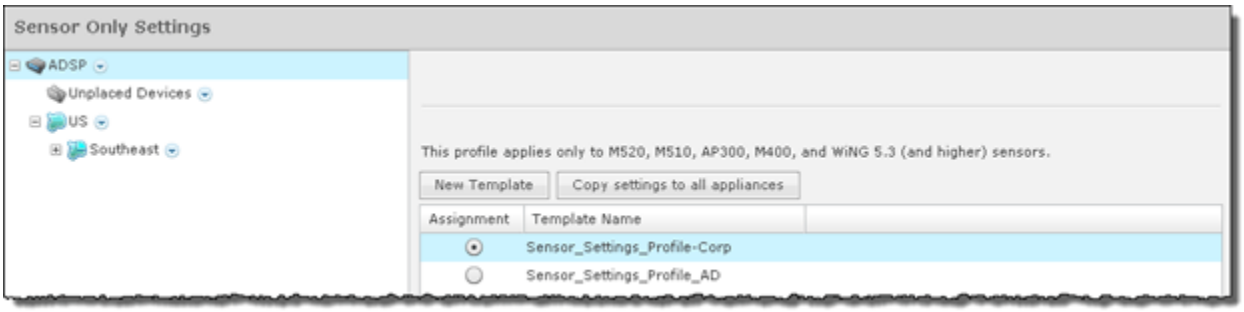
Field	Description
Primary Appliance	Specifies the IP address of the primary appliance.
Secondary Appliance	Specifies the IP address of the secondary appliance.
Sensor Admin Password	Specifies the admin password for your Sensors. Supplying this password is mandatory.
Sensor Monitor Password	Specifies 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.

Apply a Sensor Settings Profile

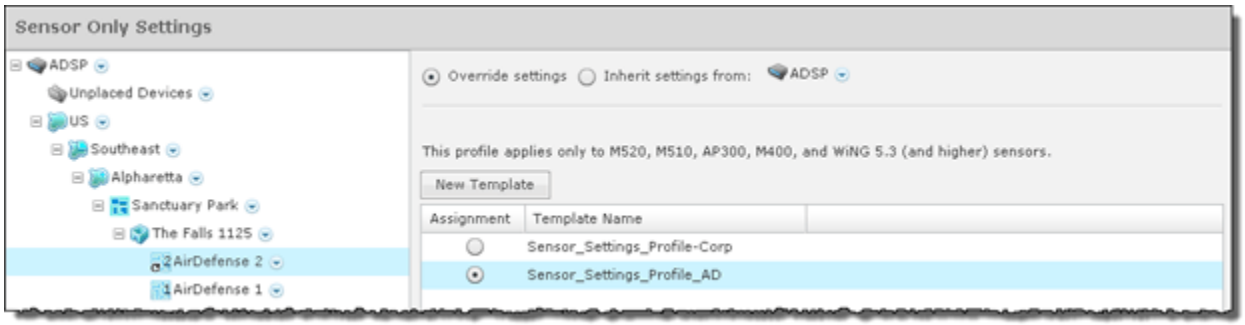
Once you have defined a Sensor Settings profile for your Sensors, you can now apply it to the Sensors in your network. A Sensor Settings profile can be applied to an appliance and all its network levels or it can be applied to a single network level. Any child network level automatically inherits the 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.



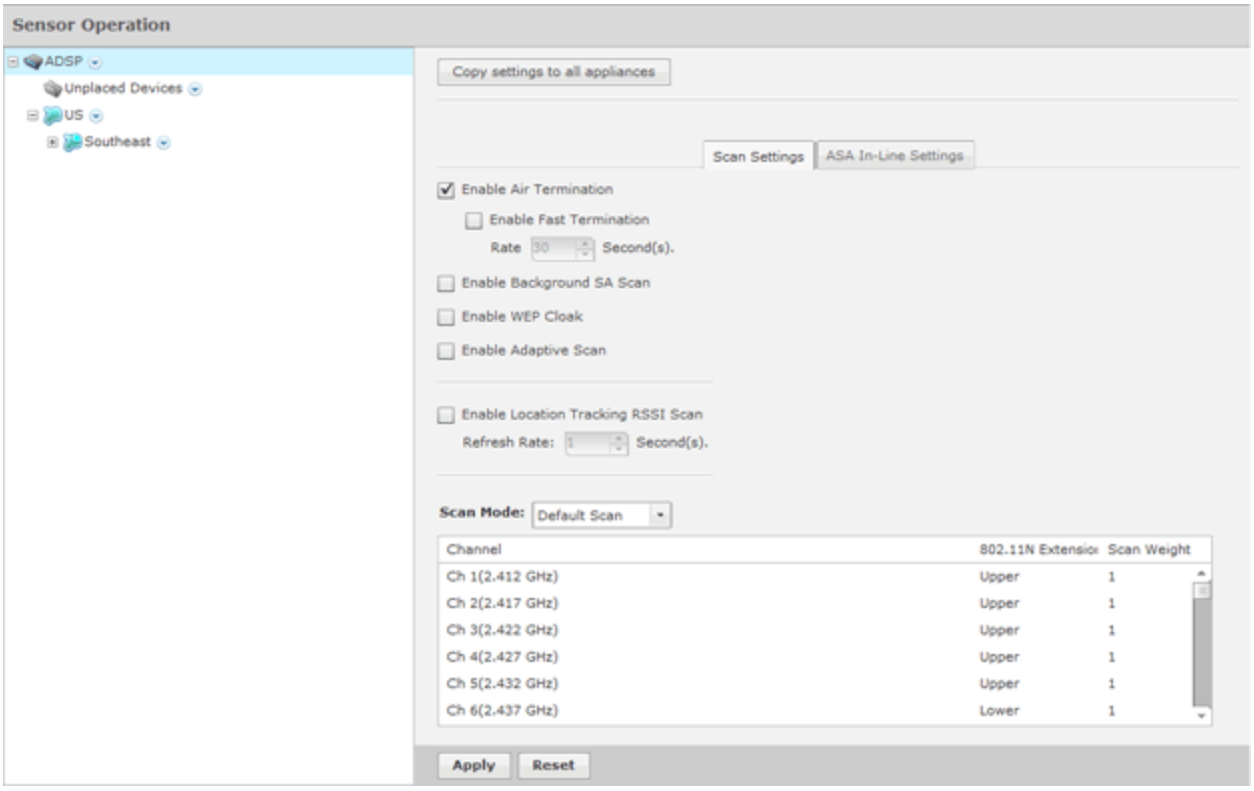
Click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

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**.



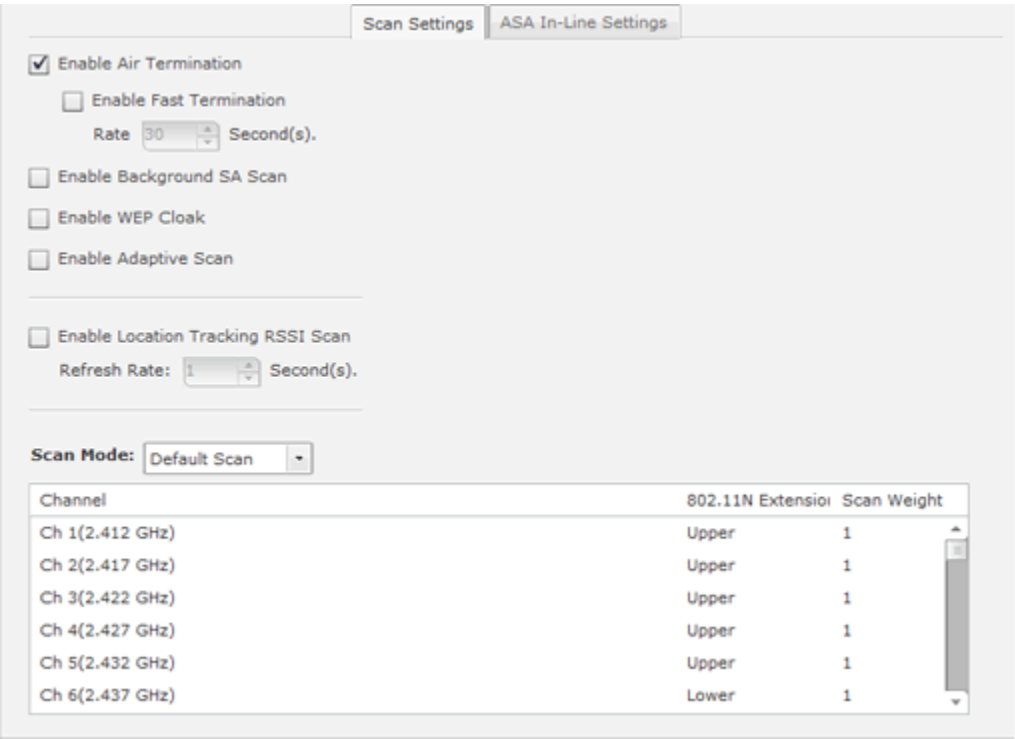
Use the **Scan Settings** and **ASA In-Line Settings** tabs to configure Sensor Operation. You can copy Sensor Operation configurations to all your appliances by clicking the **Copy settings to all appliances** button.

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

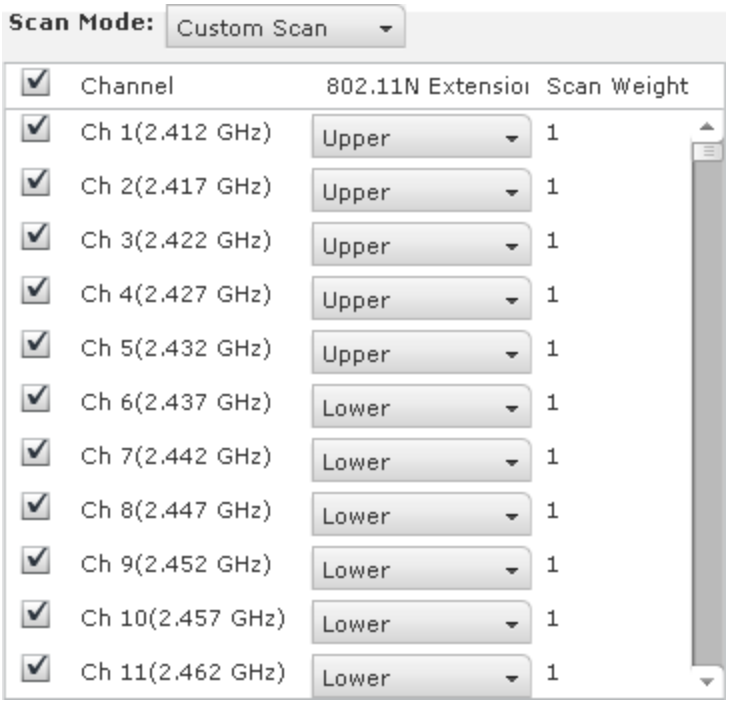
The **Scan Settings** tab is used to enable Sensor-level options and configure the Sensor scan pattern. Scan settings are configured at the appliance level of the network tree and inherited by all lower levels.



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:

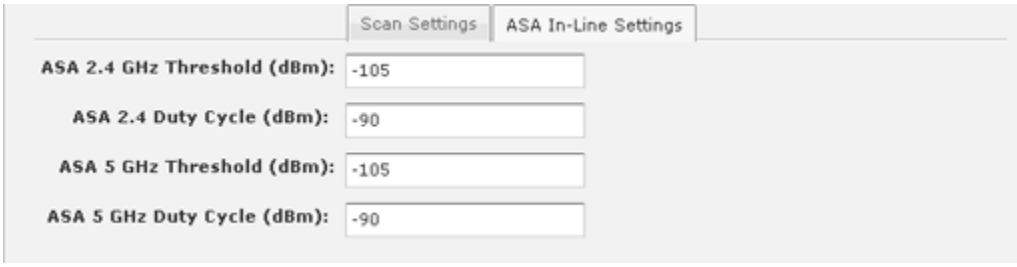
Feature/Function	Description
Enable Air Termination	Air Termination lets you terminate the connection between your wireless LAN and any or Station associated with it. By default, Air Termination is disabled. It can only be enabled in the Appliance Manager.
Enable Background SA Scan	Spectrum Analysis 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.

Feature/Function	Description
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	You can choose channels to monitor by selecting one of the following scan modes: • Default Scan—the table displays the channels that will be scanned and is not editable. • Extended Channel Scan—the table displays all standard channels plus the extended channels that will be scanned. • Extended and Emergency Channel Scan—the table displays all channels including emergency channels that will be scanned. • Custom Scan—the table displays all available channels and allows you to select channels, select the 802.11N extension, and set scan weight for each selected channel.  A scan weight of 1 specifies that the selected channel will be scanned once during each scan rotation. A scan weight of 2 specifies that the selected channel will be scanned twice and so forth. The scan sequence is determined by the specified scan weights. All selected channels are initially scanned once during the scan rotation. Any selected channels that have weights of 2 or more are then scanned again at the end of each rotation period for the number of times specified by the weight value. For example, if channels 1, 6 and 11 are assigned scan weights of 1, 2 and 2, the channel scan sequence is 1-6-11-6-11. Another example is if channels 1, 5, 6 and 11 are assigned scan weights of 2, 1, 3 and 3, the channel scan sequence is 1-5-6-11-1-6-11-6-11. • Channel Lock—used to lock a Sensor on a specific channel for scanning. A drop-down menu is displayed where you can select a channel.

ASA In-Line Settings

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



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

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

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

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**.

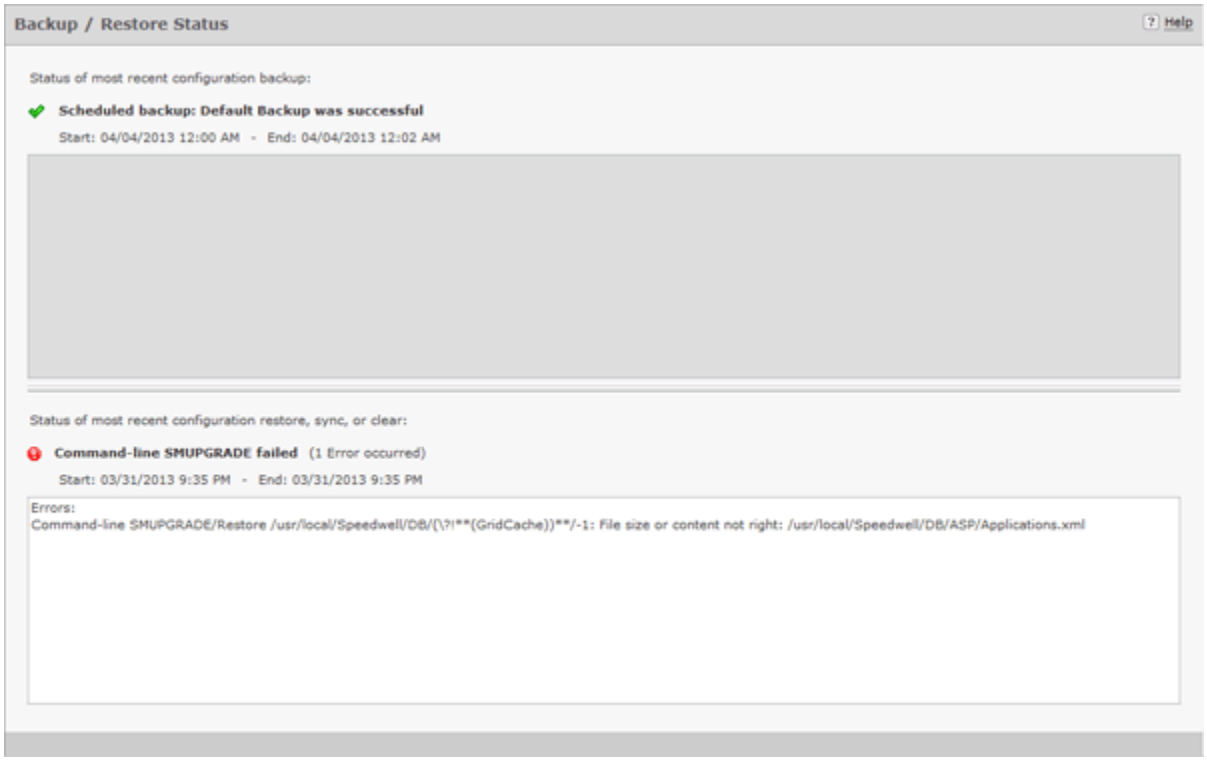
Options

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. Hint: 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 or Wireless Client. **Yes**: 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.) **No**: (Default). Click this radio button to disable AirTermination. **Hint**: If you are not an Admin User, this setting will not be visible.
Policy-based Air Termination System Enabled	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 or Wireless Client, based on alarms. **Yes**: Click this radio button to enable Policy-based Termination at the system level. **No**: (Default). Click this radio button to disable Policy-based Termination. **Hint**: If you are not an Admin User, this setting will not be visible.
Port Suppression System	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. **Yes**: Click this radio button to enable Port Suppression at the system level. See the Note, below. **No**: (Default). Click this radio button to disable Port Suppression. Note: You must have added SNMP Managed Switches and have full read and write privileges (see Adding/Importing Switches).

Function	Description
Auto-Logout Enabled	Use this feature to enable/disable the automatic logout feature, which logs a user out of ADSP after a specified amount of time. **Yes**: Click this radio button to use Auto-Logout and activate the Auto-Logout Timeout scroll list. **No**: Click this radio button to disable the Auto Logout and deactivate the Auto-Logout Timeout drop down list. Note: You must log off ADSP and then log back in before changes take effect.
Auto-Logout Timeout (Minutes)	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. Note: You must log off ADSP and then log back in before changes take effect.
Spectrum Scan Timeout	This drop-down menu allows you to set the timeout value for scanning during dedicated Spectrum Analysis. The values can be 1 - 120.
Sensor Cloaking Limit	The number amount of Sensors that can be cloaked at any one time.

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:

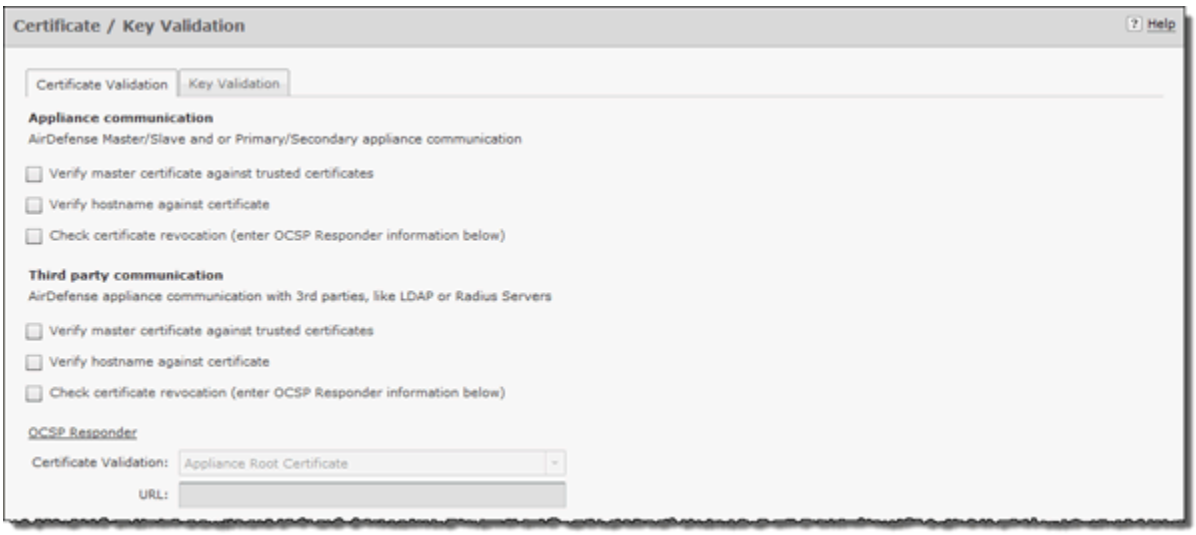
- A green checkmark– indicates that the backup/restore was successful.
- A red circle containing an exclamation mark– indicates that the backup/restore was unsuccessful.
- A start and end time is displayed to show you when the backup/restore started and when it ended.
- Any errors are displayed in the 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.



There are three types of verifications for either appliance communications or third party communications. They are:

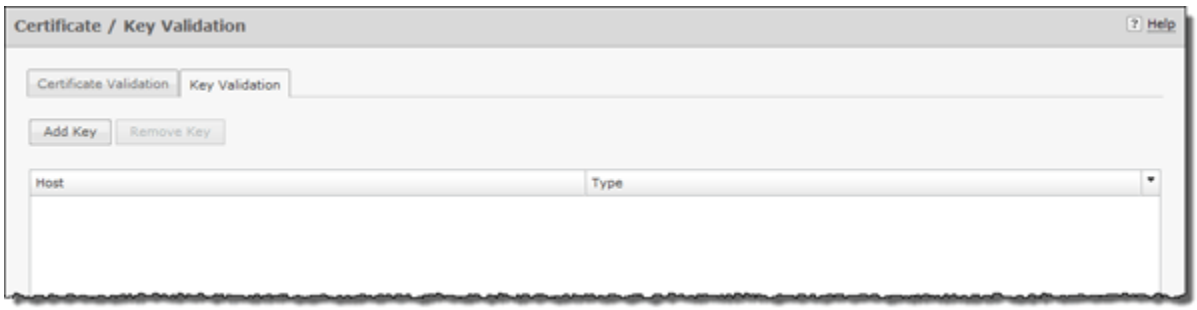
- Verify master certificate against trusted certificates
- Verify hostname against certificate
- Check certificate revocation.

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.

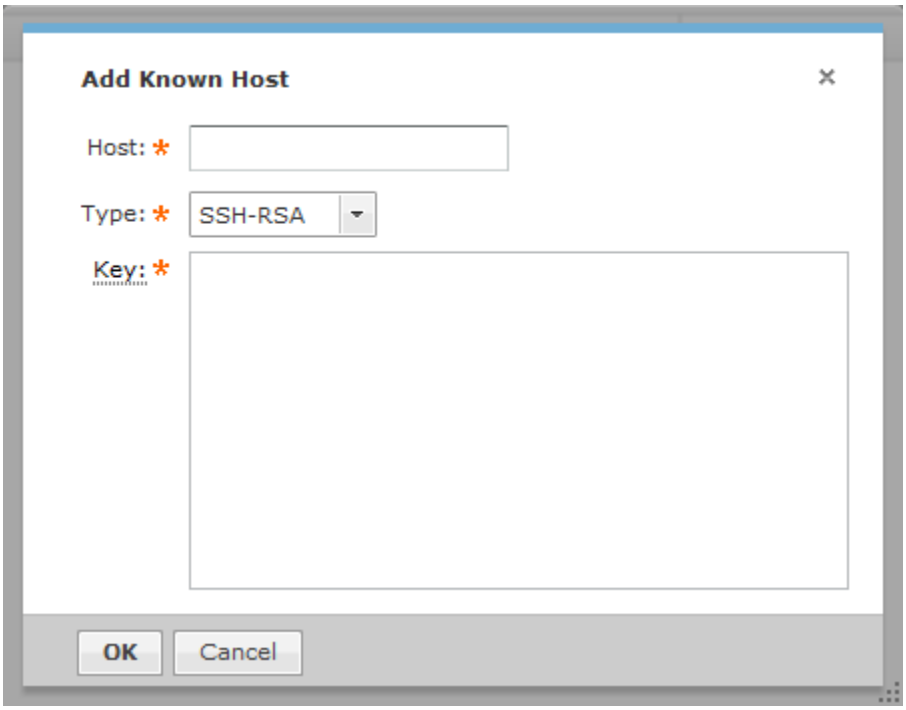
Key Validation

The **Key Validation** tab allows you to add and remove public keys for other servers.



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+YqQARTVMHfyyjisoQvBZoxvBMxf9CbXoo

VpWHBezQbm3anaav+4rEPIylcfFrIR/9o3/IdXT+arnXlrZ+7v3kBVx9SRWr5GY1

BtPFElVQi1PJz/tXTp3erWyoz4mwsb0kmoFAPc9LBrwrLtSlkrXezzrKZMa4VzB9

yK6dAQ==

---- END SSH2 PUBLIC KEY ----

copy the actual key part and paste it into the **Key** field.

AAAAB3NzaC1yc2EAAAABJQAAAIBrxx+YqQARTVMHfyyjisoQvBZoxvBMxf9CbXoo
VpWHBezQbm3anaav+4rEPIylcfFrIR/9o3/IdXT+arnXlrZ+7v3kBVx9SRWr5GY1
BtPFElVQi1PJz/tXTp3erWyoz4mwsb0kmoFAPc9LBrwrLtSlkrXezzrKZMa4VzB9
yK6dAQ==

5 Click **OK**.

To remove a public key, select (highlight) the key and then click the **Remove Key** button.

Certificate Manager

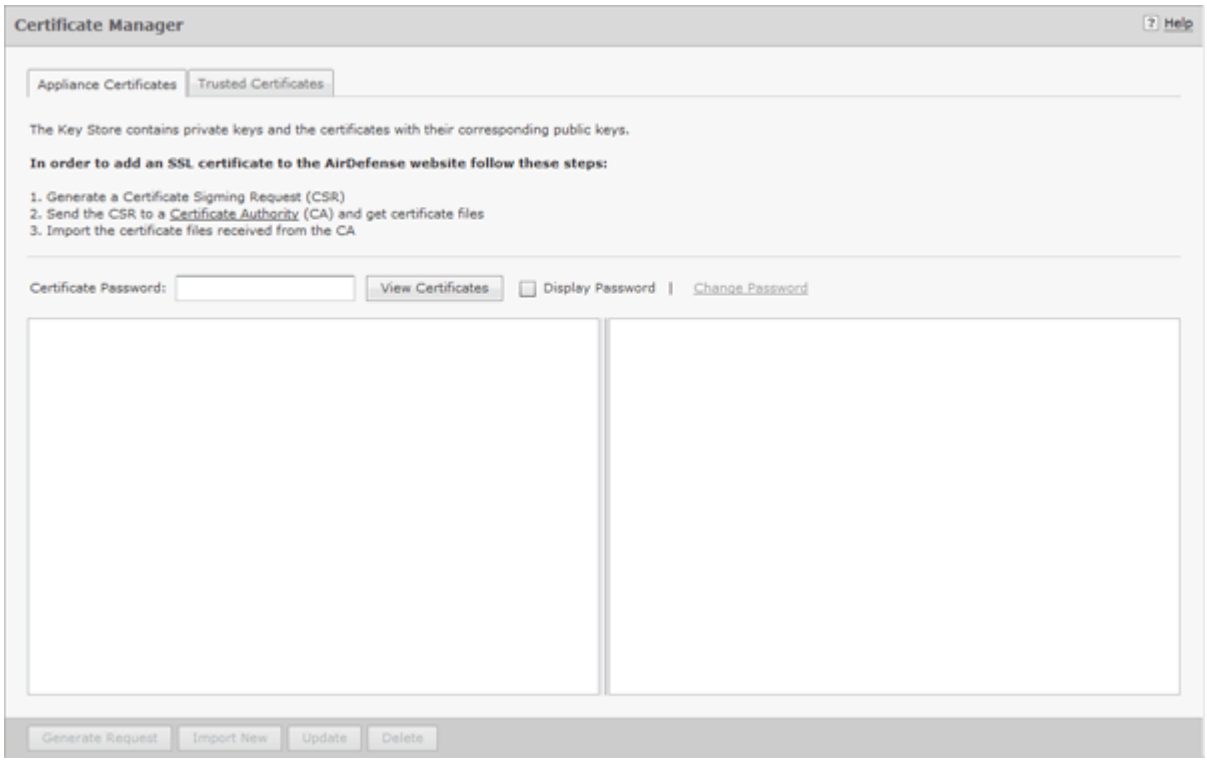
Certificates verify the authenticity of the ADSP appliance. They can prevent hijacking of sessions between your browser and the ADSP appliance, and can even alert you to physical replacement of the ADSP appliance. Certificates install into the ADSP appliance and are sent by the appliance directly to your browser.

IMPORTANT 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 ADSP with either a self-signed certificate or a root-signed certificate.

ADSP 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 an Admin User 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 ADSP 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:

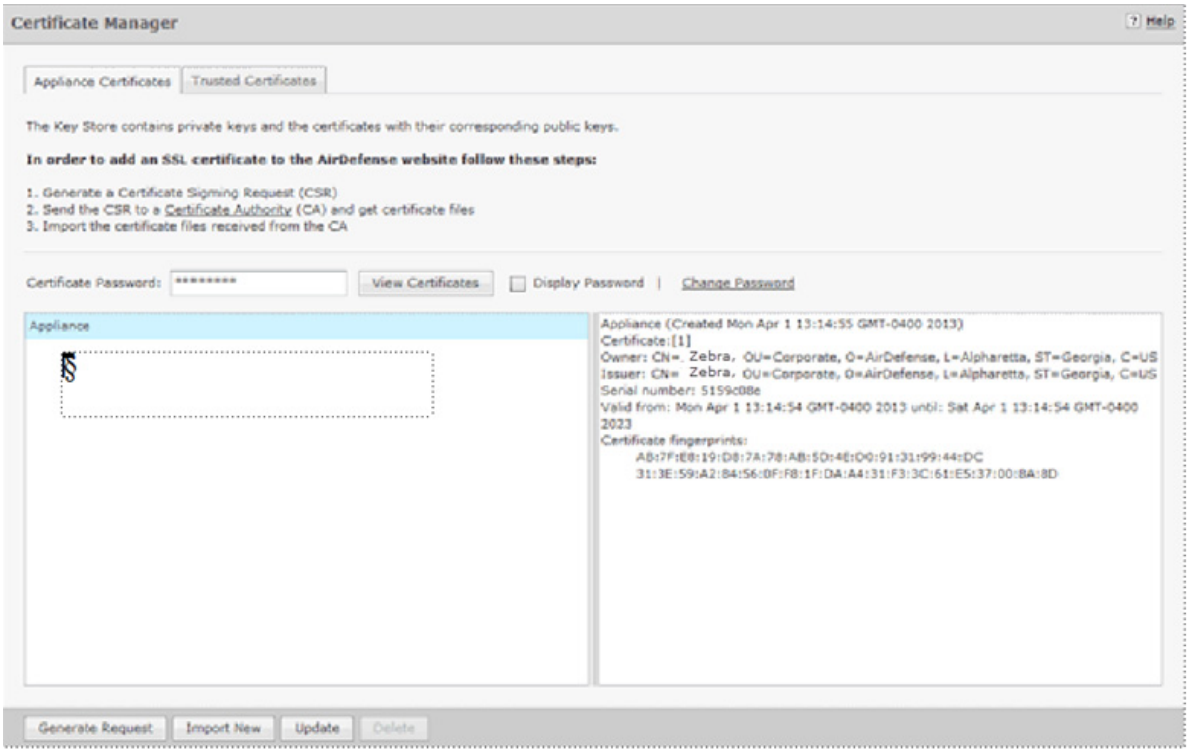
Certificate	Description
AirDefense Certificate	The AirDefense certificate represents a minimal level of security. AirDefense ships the ADSP appliance with a pre-installed security certificate. It is a working certificate that provides TLS encryption, but has not been verified and digitally signed by a root Certificate Authority (CA). The host name identified in the certificate will not match the actual host name of your ADSP appliance. Unless the certificate meets all required criteria, you will receive one or more alert screens when you open a session with ADSP.
Self-Signed Certificate	A self-signed certificate represents an intermediate level of security. 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. Unless the certificate meets all required criteria, you will receive one or more alert screens when you open a session with AirDefense.
Root-Signed Certificate	A root-signed certificate represents a high level of security. 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.
SSL Certificate	A SSL certificate represents the highest level of security. 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://.

View 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:

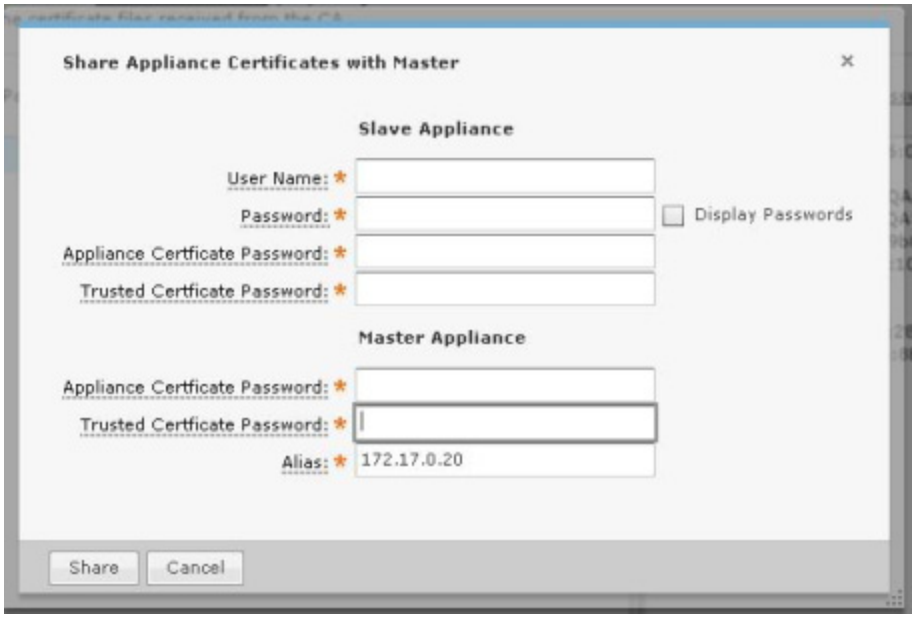
1 Access the Certificate Manager.

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:

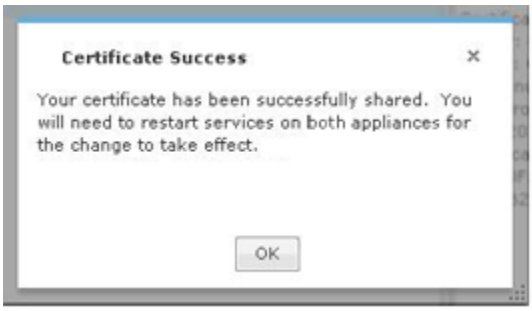
For the slave appliance:

- 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 *Add Certificates*.

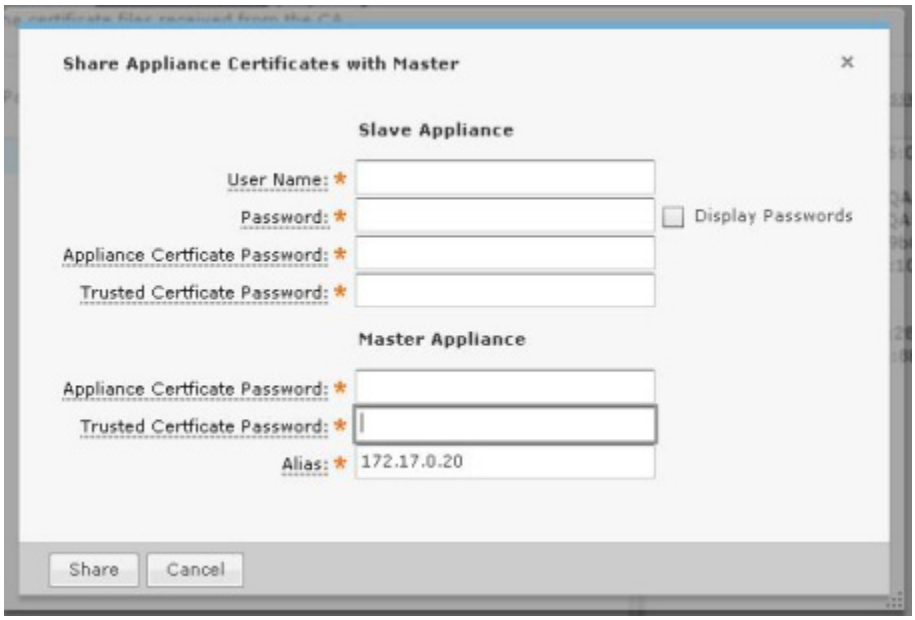
1 Access the Certificate Manager.

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**.



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.

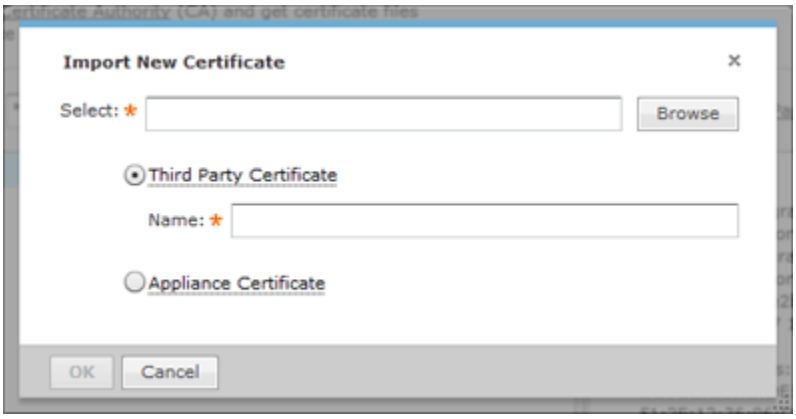
7 Click **OK**.

8 On the master appliance, access the **Trusted Certificate** tab.

9 In the **Appliance** field, select the master appliance.

10 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 through12.

16 Restart the slave appliance.

17 Check the master appliance to see that the slave appliance is now online.

Add 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).

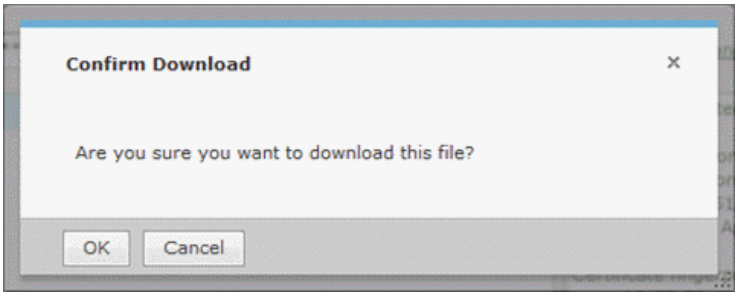
2 Send the CSR to a Certificate Authority (CA) and get certificate files.

3 Import the certificate files received from the CA.

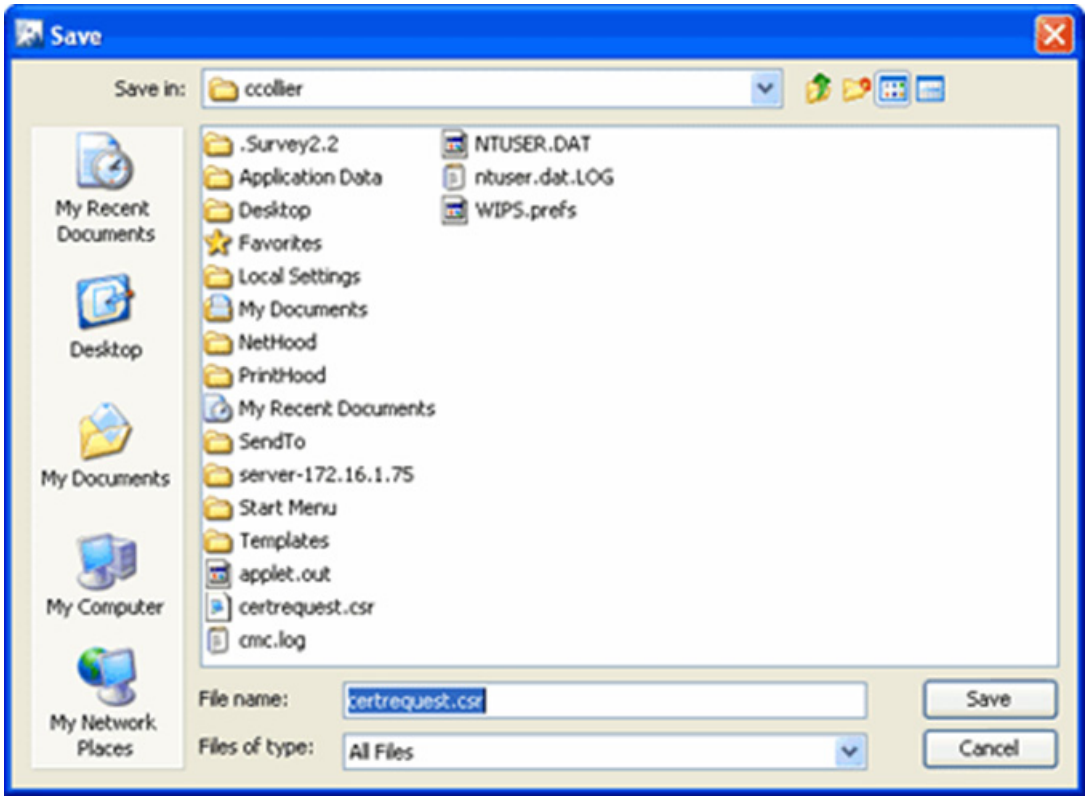
Each of these steps are discussed in the following sub-topics.

Generate Certificate Signing Request (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 **Save**.

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.

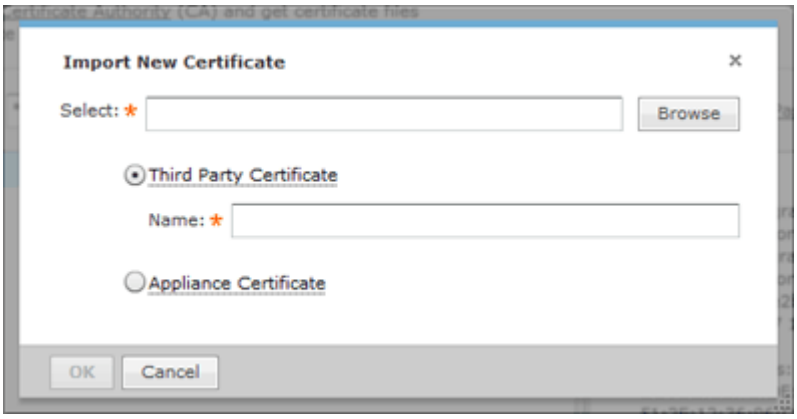
The file save in Generate a CSR has the information that a CA needs to issue certificate files. You will have to present this information to the CA in some way.

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:

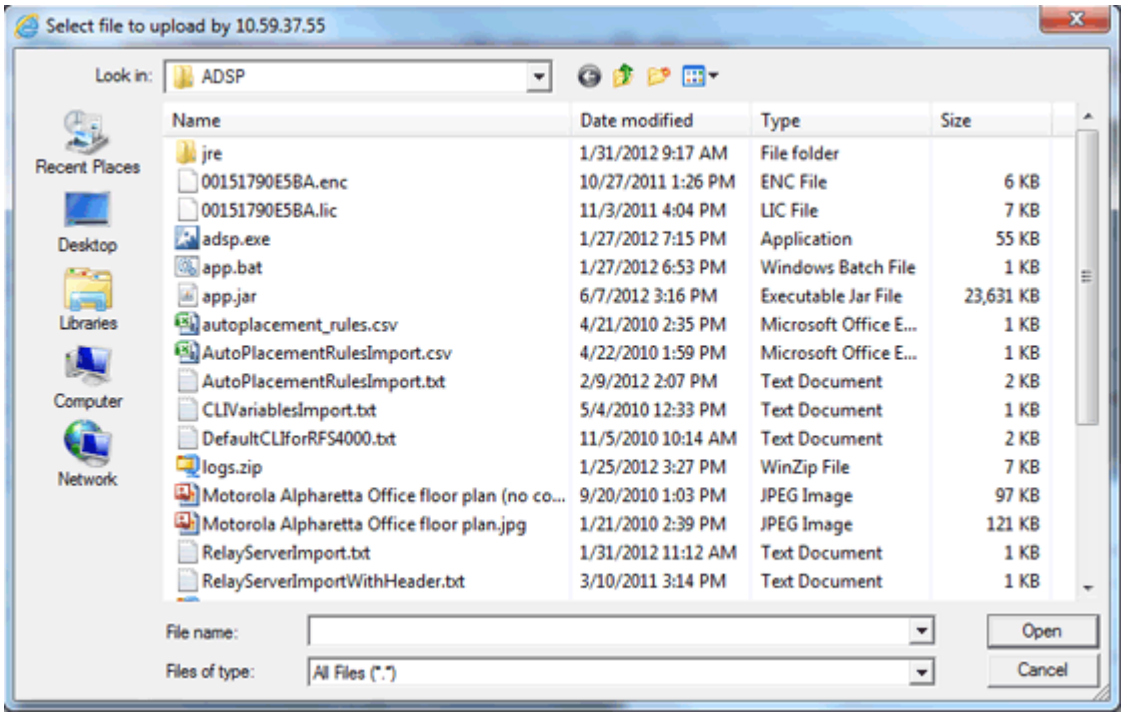
- Intermediate
- Root
- SSL which is the tomcat certificate.

Importing Certificate Files from CA

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.

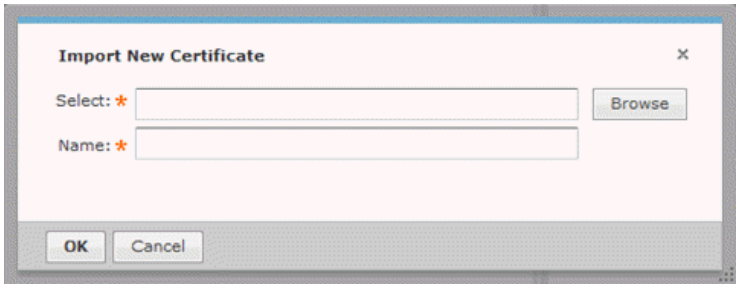
8 Click **OK**.

NOTE You will have to restart tomcat services before the certificates are activated. The tomcat services are located on your ADSP appliance.

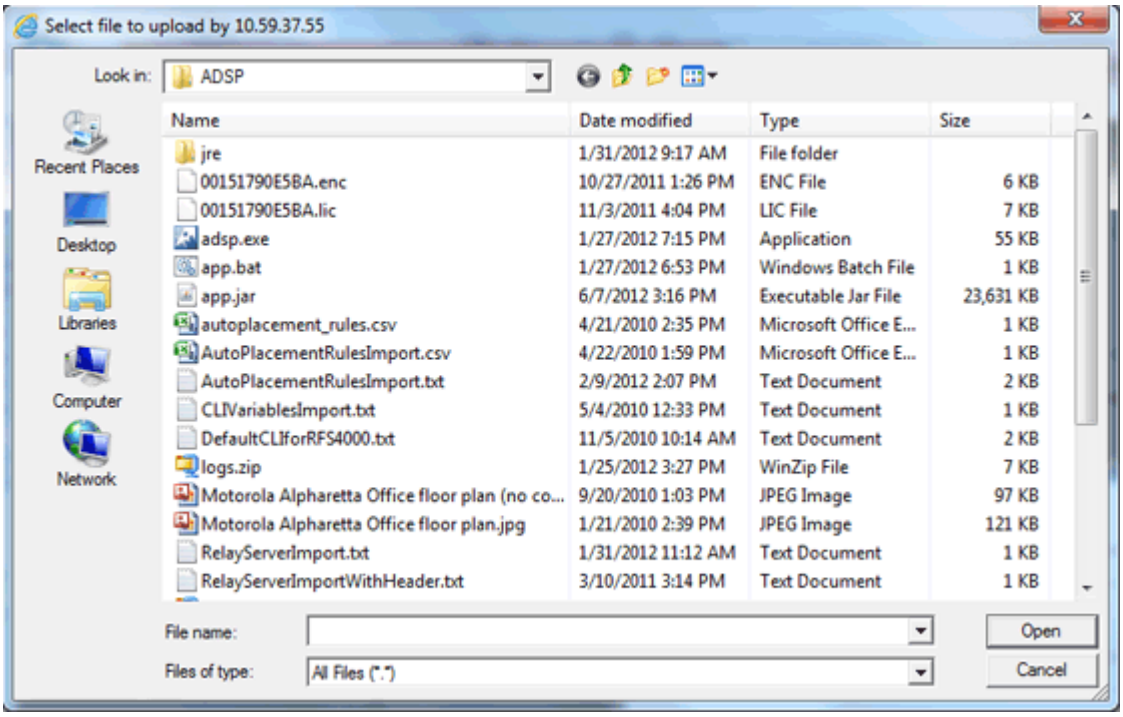
Import New Certificate

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.



2 Click the **Browse** button to open the **Select file to upload** window.



3 Navigate to the trusted 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**.

Update Certificate Information

Changing Default Information

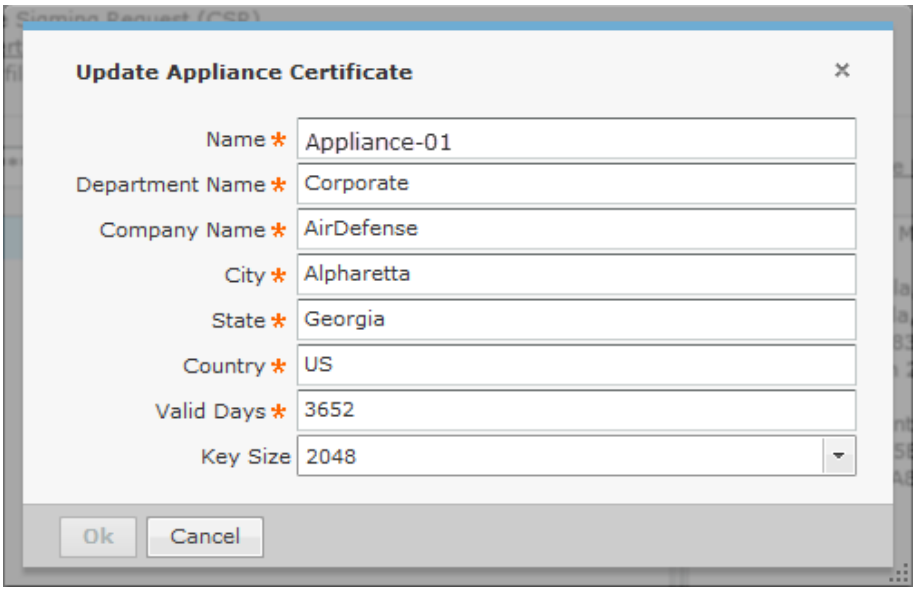
The default information is included with each certificate that you add. You may change this information if you feel it is necessary. The following information may be changed:

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.

Field	Description
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.



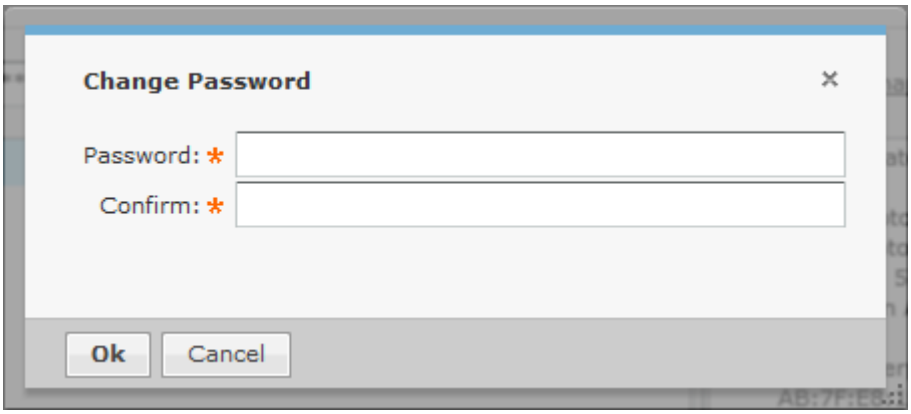
2 Change any of the information using the previous table as a guideline.

3 Click the **OK** button.

Change 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.



2 Type the new password in the **Password** field.

3 Type the new password again in the **Confirm** field.

4 Click the **OK** button.

Export 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 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.

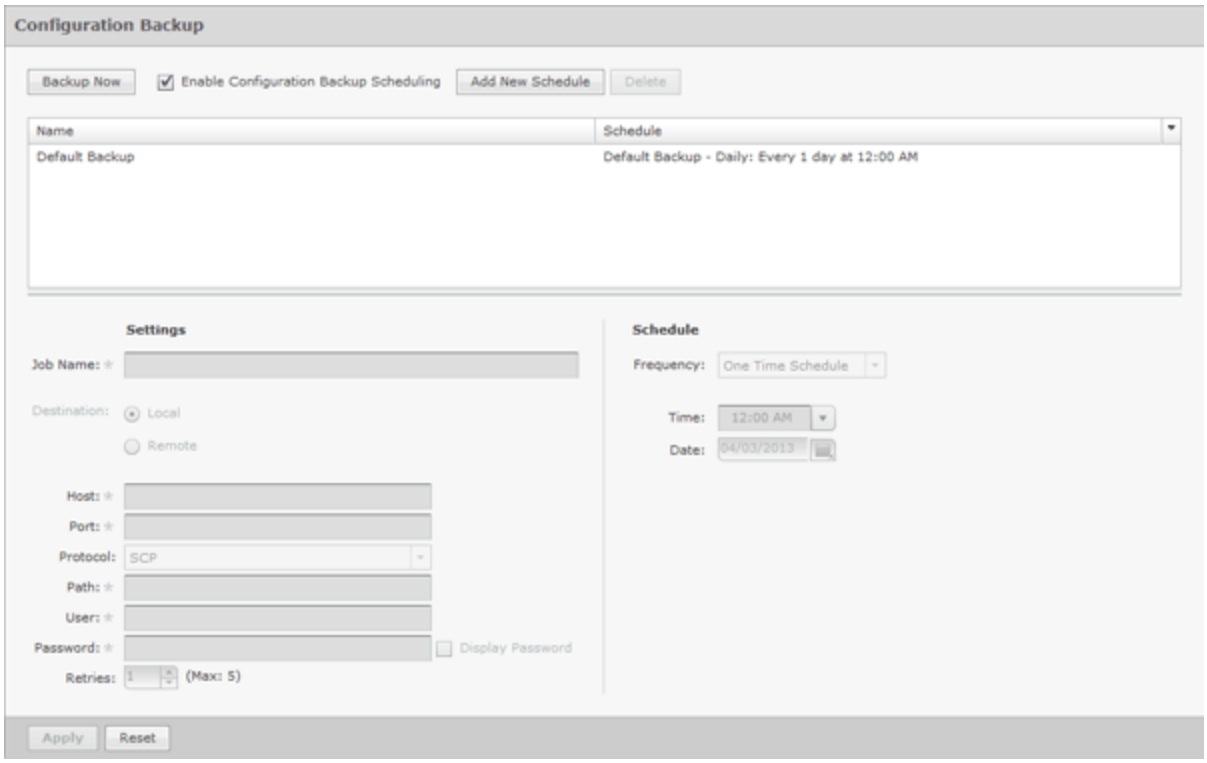
6 Select a location and specify a file name.

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.



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.

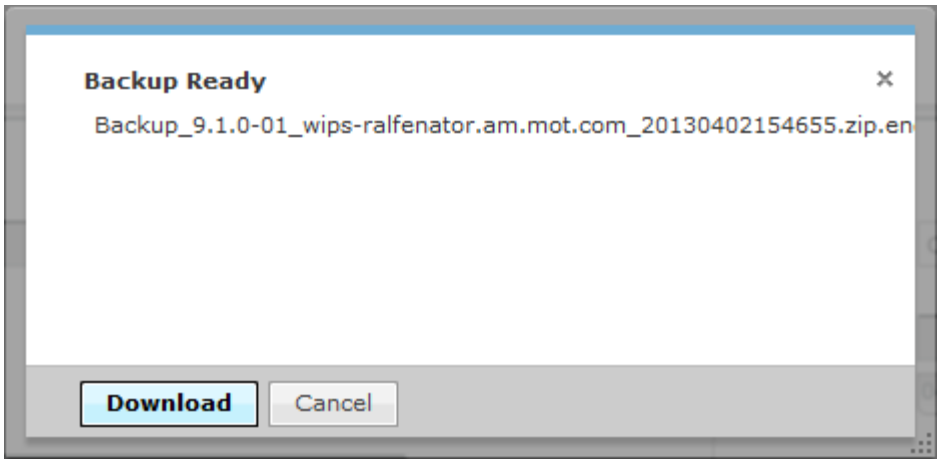
Backup Recommendations

- 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.

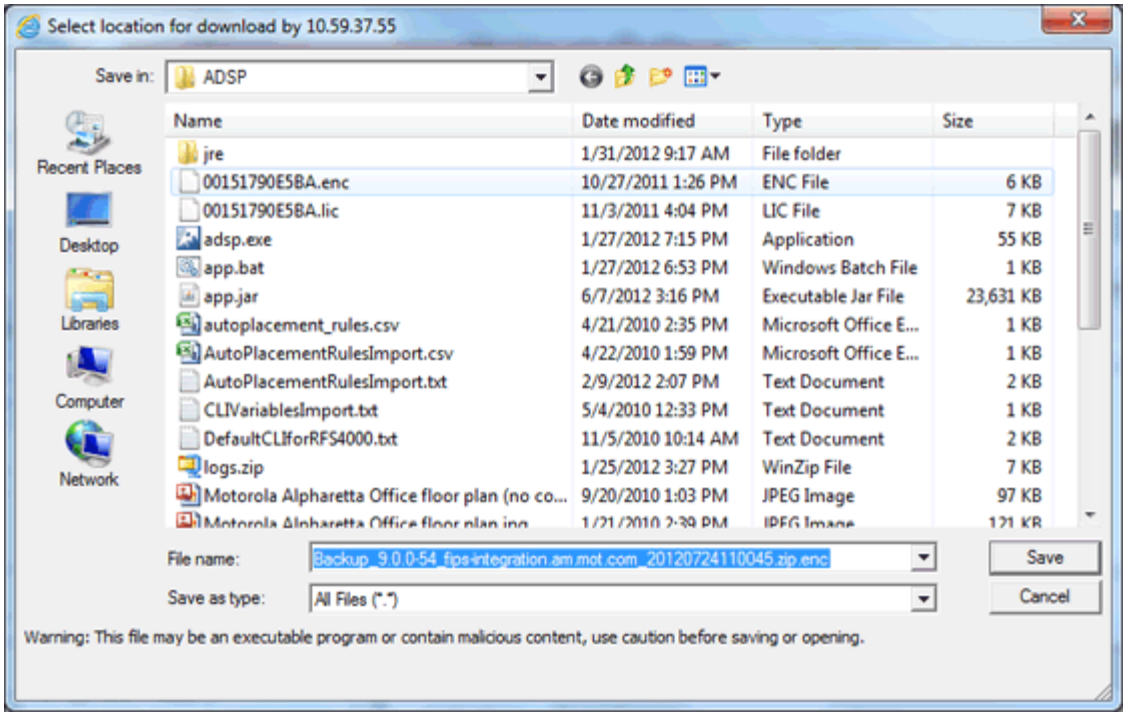
Manual Backups

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

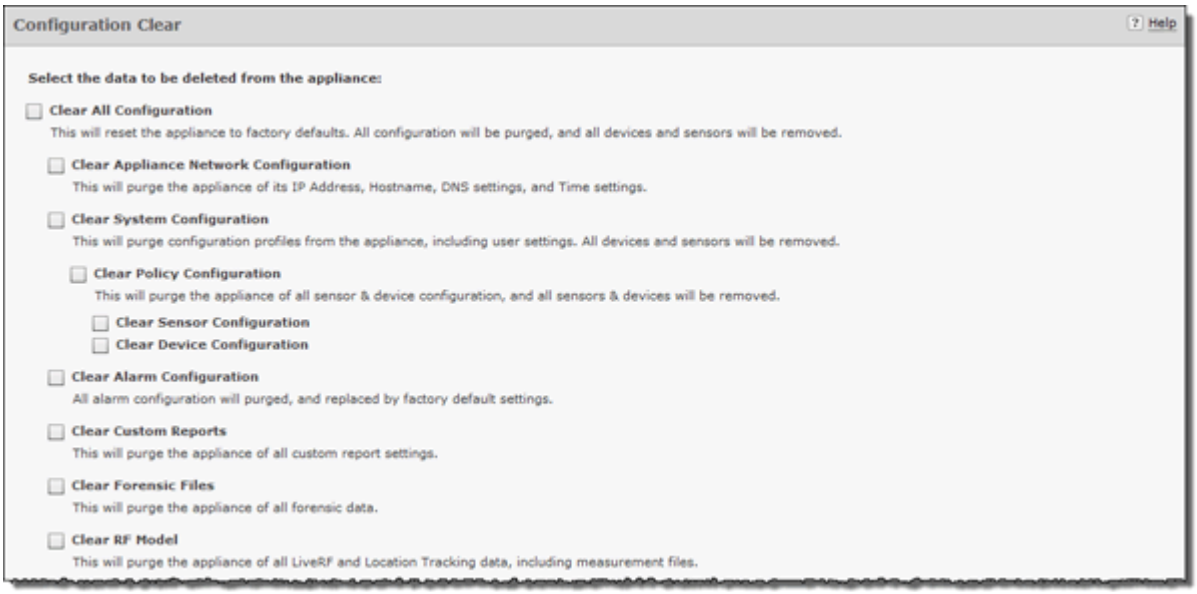
Click the **Apply** button to set the automatic backup schedule.

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 (**SCP**, **SFTP**, or **HTTPS**).
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 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:

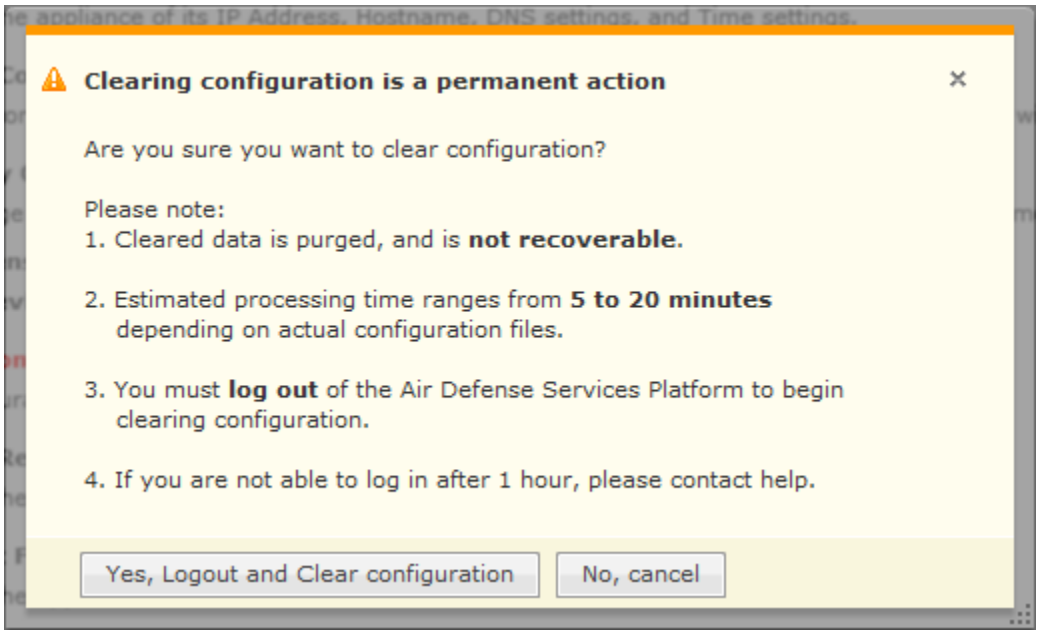
Option	Description
Clear All Configuration	Clears all configuration data, setting your server back to its original default state.
Clear Appliance Network Configuration	Clears the configuration for the appliance network. All network configuration is set back to default.
Clear System Configuration	Clears all system configuration data. This encompasses everything except what is covered by the other options. There are three other options associated with this option. • 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. • Clear Sensor Configuration—Clears all Sensor configurations that you customized. • Clear Device Configuration—Clears all device configurations that you customized.
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.



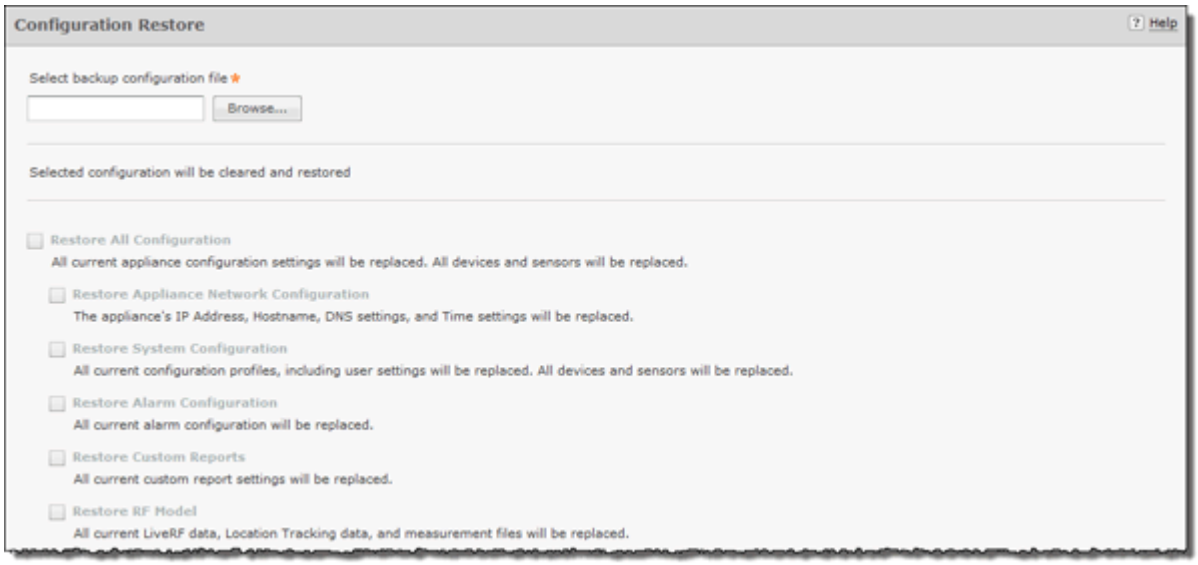
3 Select the **Yes, Logout and Clear configuration** button to confirm that you want to logout and clear the configuration data.

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** 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:

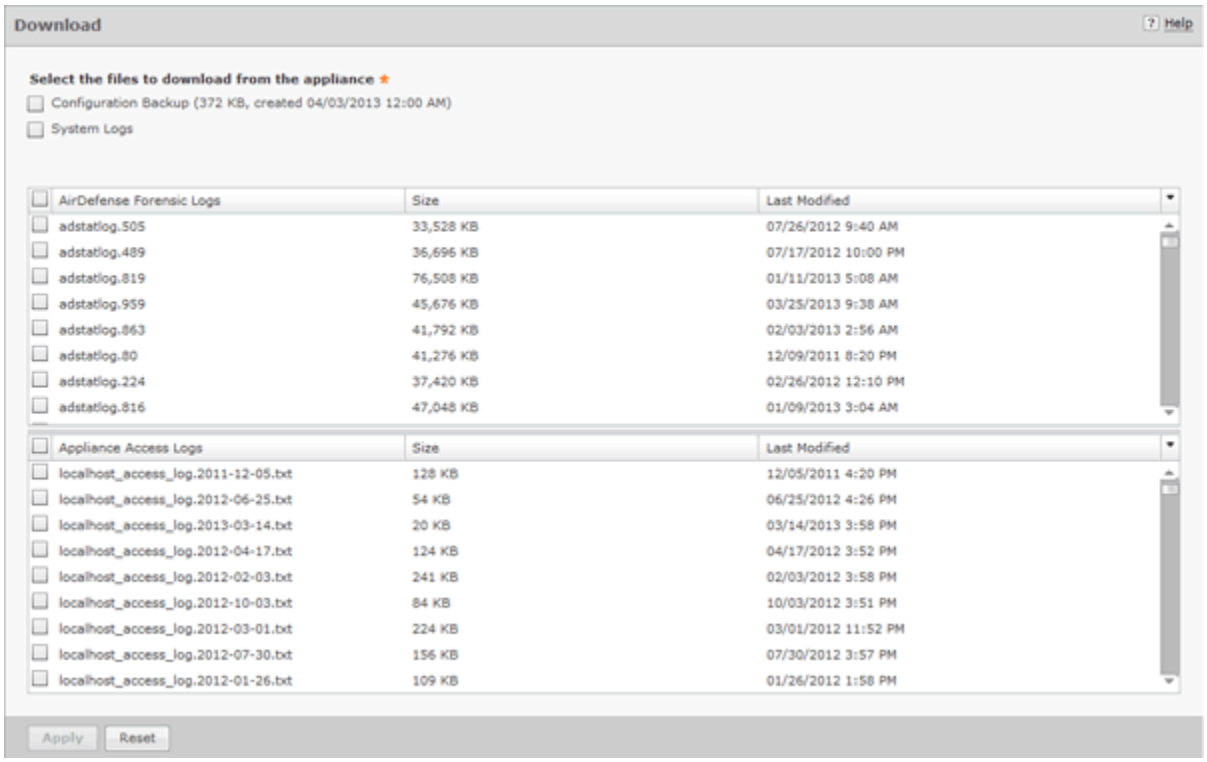
Option	Description
Restore All Configuration	Restores all configuration data from the backup file.
Restore Appliance Network Configuration	Restores the configuration for the appliance network.
Restore System Configuration	Restores all system configuration data. All Sensors and devices are replaced.
Restore 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

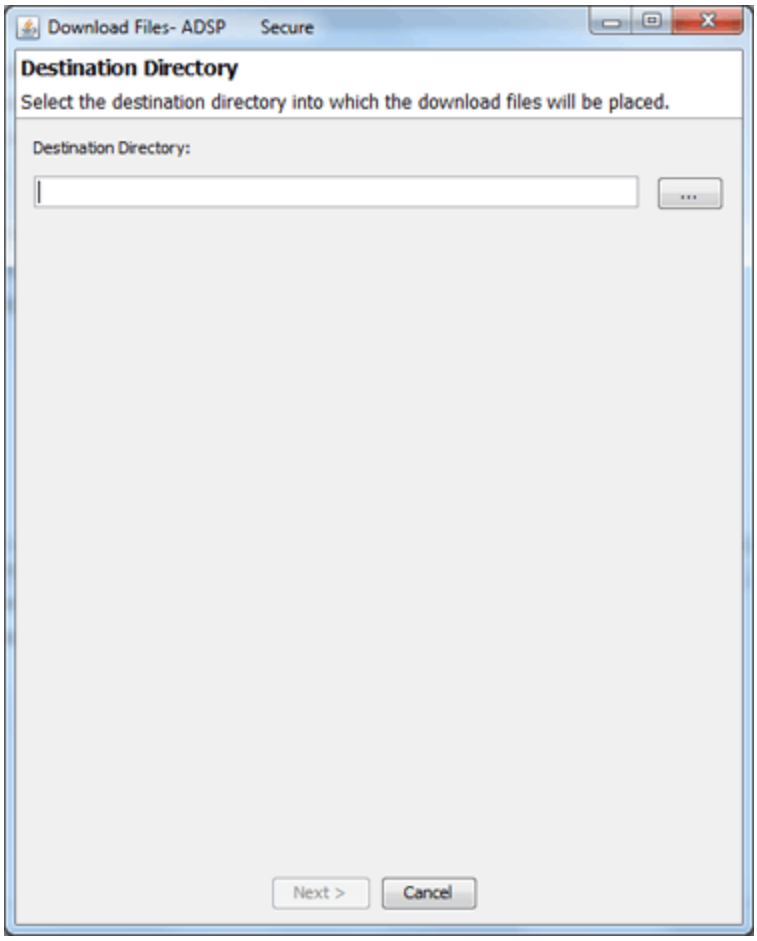
You can download configuration files that were automatically backed up to your ADSP server to your workstation. Once the backed up configuration is on your workstation, you can restore it. (See *Configuration Restore*.)



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.

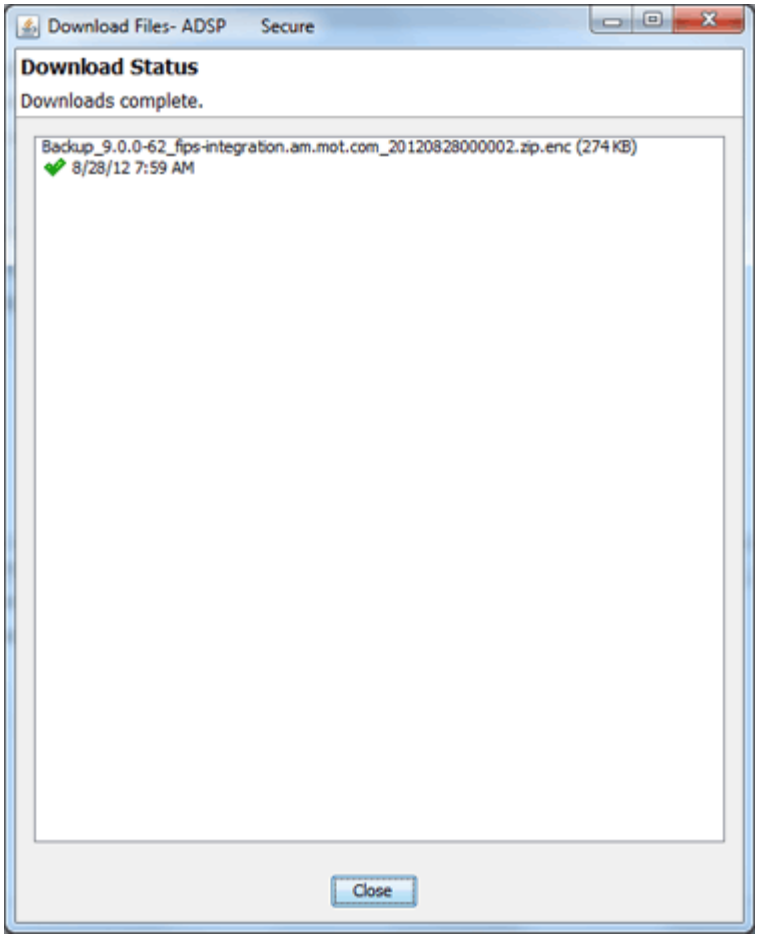


5 Click the **Browse** button to open a window where you can select your destination directory (folder).

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.

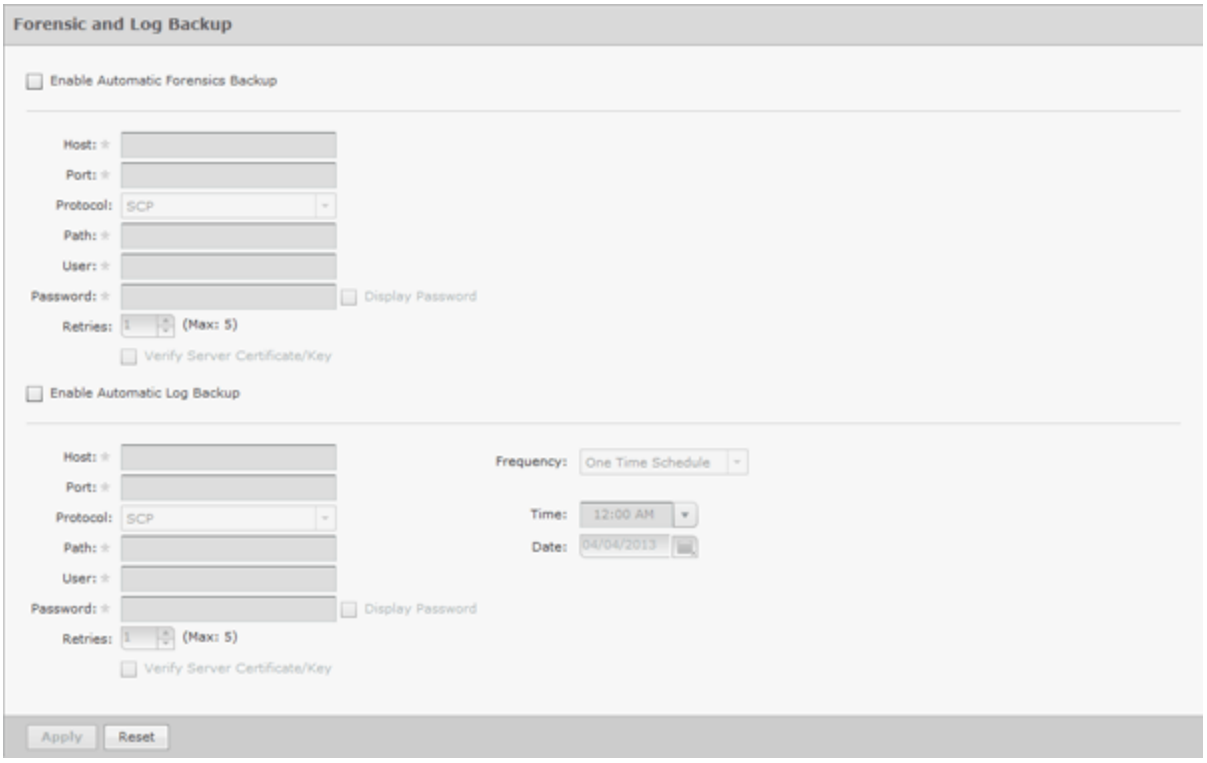
8 Click **Next**. The configuration is downloaded to the selected directory and a status window is displayed confirming the download.



9 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.

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

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.

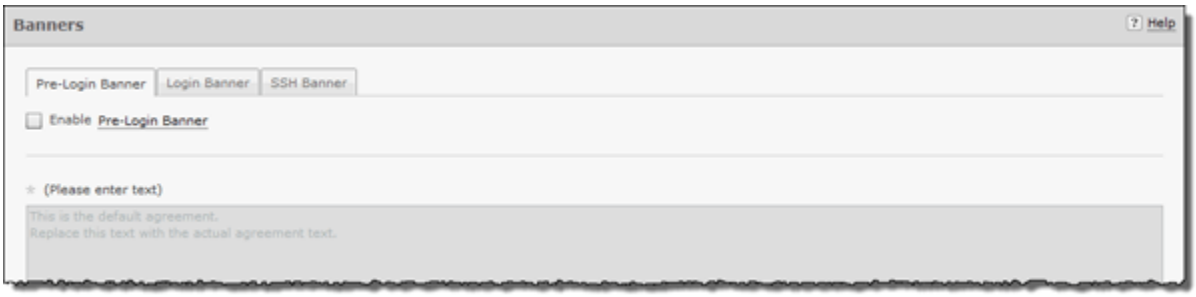
Login / SSH Banners

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.

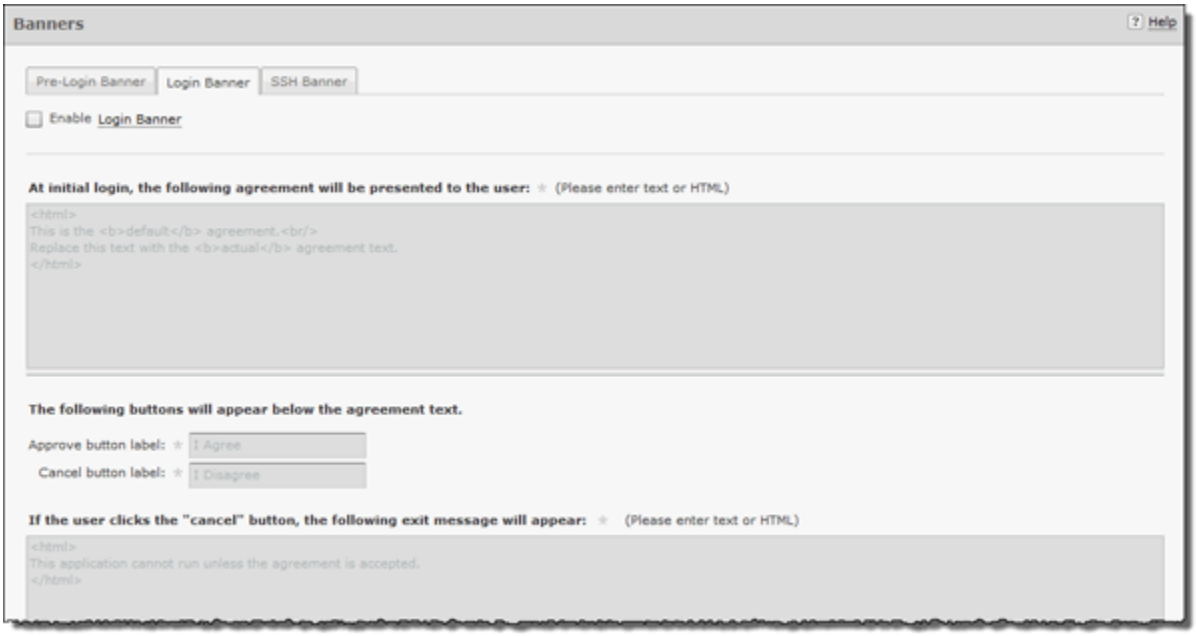
Settings

The *** (Please enter text)** field is available to enter text that users will see before logging into ADSP. Text can be entered in HTLM 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. **Note**: 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 **Startup Agreement** window. Default = **I Agree**
Cancel button label	Enter the actual text that will appear for the cancel button on the Startup Agreement window. Default = **I Disagree**
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. Note: 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 HTLM 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 **Time** drop-down menu. Then, select a day for the synchronization by clicking the **Calendar** button in the **Date** field and selecting a date.
Intra-Day Schedule	Select a time to begin the synchronization. Then, select a frequency in hours.

Interval	Action
Daily Schedule	Select a frequency in day, weekdays only, or weekends only. Then, select a time of day.
Weekly Schedule	Choose a frequency in days. Then, select a day or multiple days to conduct the 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:

- Create and modify user accounts and group accounts (**Accounts Access** feature)
- Authenticate users on the local appliance (**Local Authentication** feature)
- Change the password of the current user (**Password Reset** feature)

- Authenticate users by using the password stored on a RADIUS or LDAP server (**Remote Authentication** feature)
- Specify the user preferences that are used to set the ADSP auto refresh rate and to specify a proxy to access the server (**User Preferences**).

Account Access

You can use the Account Access feature to:

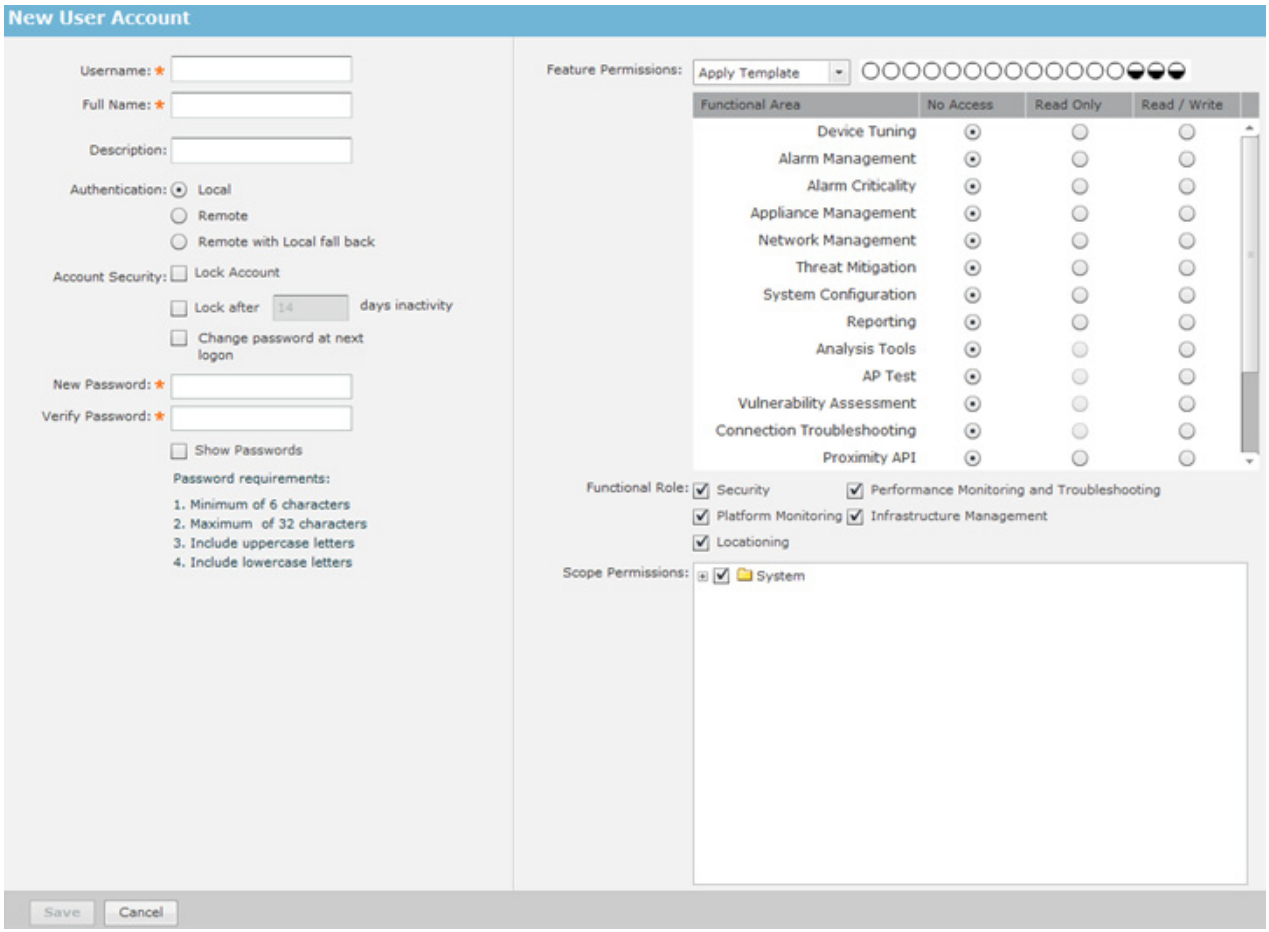
- View user account information.
- Add user accounts:
  - **New User Account** button.
  - **New Group Account** button.
- Edit user accounts (**Edit** link).
- Delete user accounts (**Delete** link).
- Synchronize user accounts (**Check Synchronization** button).

NOTE You must be an Admin User to use the Account Access feature.

To access this feature, go to **Configuration** > **Account Management** > **Account Access**.

New User Account

Select the **New User Account** option from the drop-down menu to display the **New User Account** page.



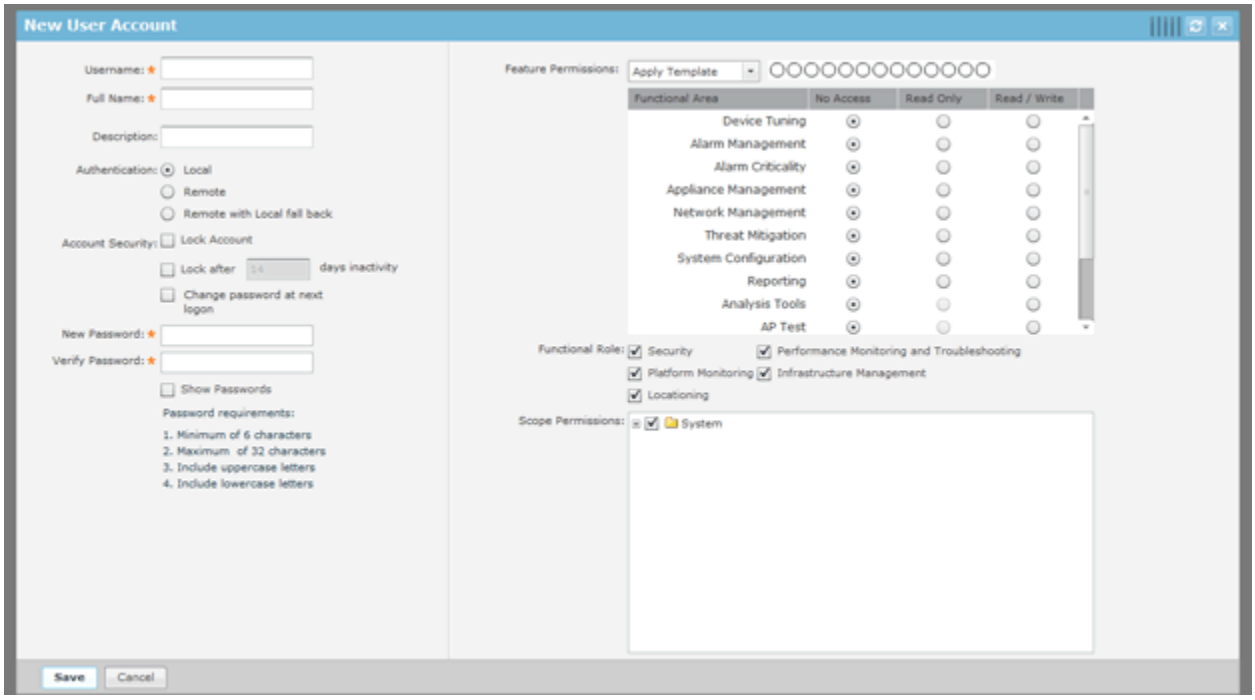
View User Information

From the left frame of the user account screen, you can view the following information about existing user accounts:

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

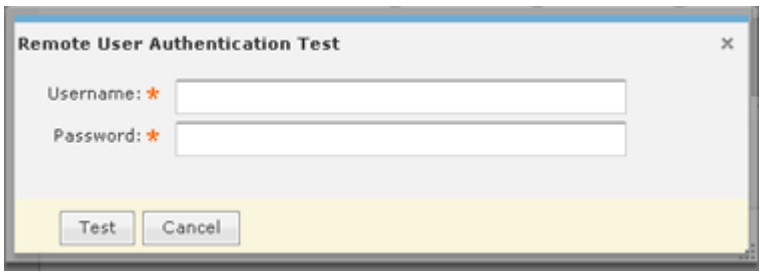
Add/Edit User Accounts

Click the **New User Account** button to access the **New User Account** overlay.



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	Select **Local** if the user will use Local Authentication. Select **Remote** if the user will use Remote Authentication. Select **Remote with local fall back** if the user will use Remote Authentication with local fall back. Note: At least one Administrator should be set to Local Authentication to avoid getting locked out of the system if a WLAN link is disconnected. When adding a remote user, *Remote Authentication* must be set up first. Once Remote Authentication is set up, select the **Remote** radio button.  You can test remote user authentication using the **Test Authentication** button.  Enter a username and password. Then, click the **Test** button. If the credentials are valid, you will receive a pass message. If the credentials are invalid, you will receive a failed message.
New Password	Enter a new password for the user. **Note**: Password must include lowercase letters and uppercase letters. Password must be 6-32 characters in length. Password may not contain spaces or tabs.
Verify Password	Enter the new password again to verify the password.
Lock Account	Check this checkbox if you want to lock the account.
Lock after x days inactivity	Check this checkbox if you want to lock the account after x amount of days of no use. Select the **Show Passwords** checkbox to reveal passwords.

Field	Description
Change password at next logon	Check this checkbox if you want to force the user to change password at the next logon. Select the **Show Passwords** checkbox to reveal passwords.
Feature Permissions	Limits users to specific functions within ADSP. Functional areas include: • Device Tuning • Alarm Management • Appliance Management • Alarm Criticality • Network Management • Threat Mitigation • System Configuration • Reporting • Analysis Tools • AP Test • Vulnerability Assessment • Connection Troubleshooting. You can apply a template or you can select individual functions for users to access. The following templates are available: • Admin—Gives users read/write permission to all functional areas. • Guest—Gives users read permission to Alarm Management, Reporting, Analysis Tools, and Connection Troubleshooting. No access is provided for the other functional areas. • Helpdesk—Gives users read/write permission to Connection Troubleshooting. No access is provided for all other function areas. • Operation Center—Gives users read/write permission to all functional areas except Appliance Management, Network Management, and System Configuration. No access is provided for these three function areas.

Field	Description
Functional Roles	Gives access to the following Functional Roles: • 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 Select the appropriate checkbox(es).
Scope Permissions	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.

Once you have configured the user options, click **Save** 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.

Change User 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.

User Roles

During installation, ADSP 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.

Default User Roles

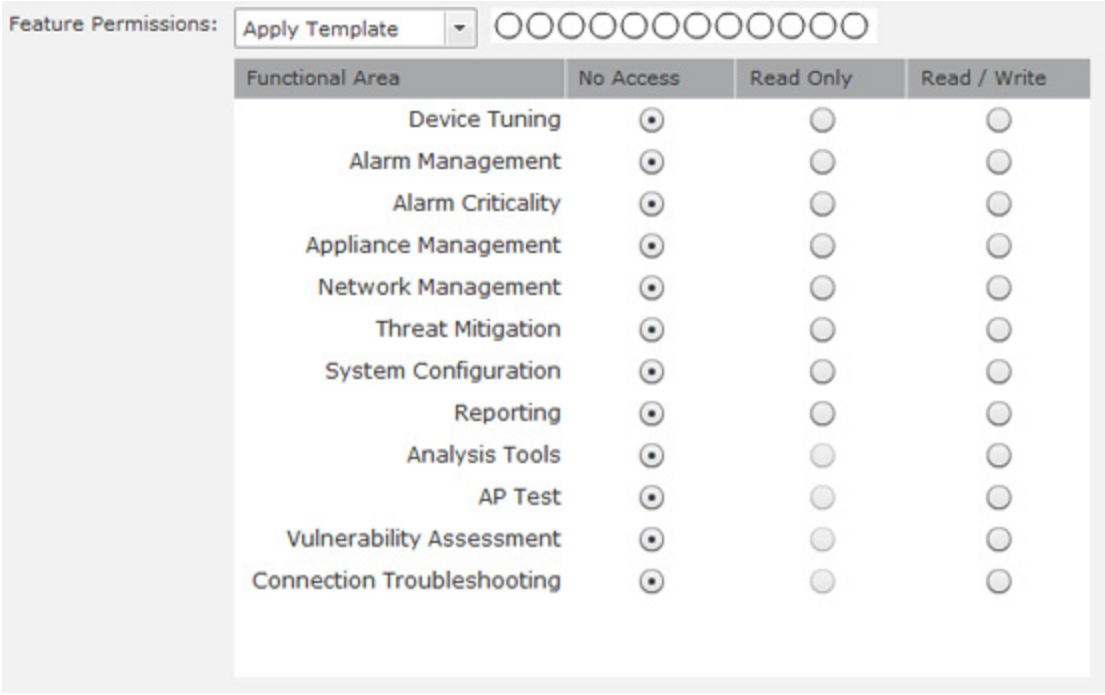
ADSP has four default role types with different levels of access to ADSP functionality.

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

The Admin User 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.

Customized User Roles

You can customize roles by giving the account no access, read only access, or read/write access to the individual functional areas.



Capabilities for the individual functional areas are:

Functional Area	Capabilities (use of)
Device Tuning	• Setting annotations • Device profile configuration (existing)
Alarm Management	• Alarm configuration • View/Manage alarms that have triggered • Add notes to alarms • Acknowledge alarms • Clear alarms • Disable alarms on device
Appliance Management	• Access to all settings under current appliance management, with the exception of functional areas covered by System Configuration
Alarm Criticality	• Configure the criticality scale of alarms
Network Management	• Configure performance policy • Configure configuration policy • Configure monitoring policy • Configure infrastructure profiles • Configure sub-profiles • Action Manager use • Auto classification of devices • Network setup • Map configuration • Auto-Placement • Discovery policies • Manual modification to network tree hiearchy • Device placement • Inherited policy/profile assignment (network and device levels)
Threat Mitigation	• Manual termination • ACL • Port suppression
System Configuration	• Basically, configuration categories that affect the whole system
Reporting	• Reporting UI • Report builder

Functional Area	Capabilities (use of)
Analysis Tools	• Live View • LiveRF • Location Tracking • Spectrum Analysis • Advanced Forensics • Scope Forensics
AP Test	• On-demand or scheduled AP Test • AP Test profiles
Vulnerability Assessment	• On-demand or scheduled Vulnerability Assessment • Vulnerability Assessment profiles
Connection Troubleshooting	• Troubleshooting tools

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

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

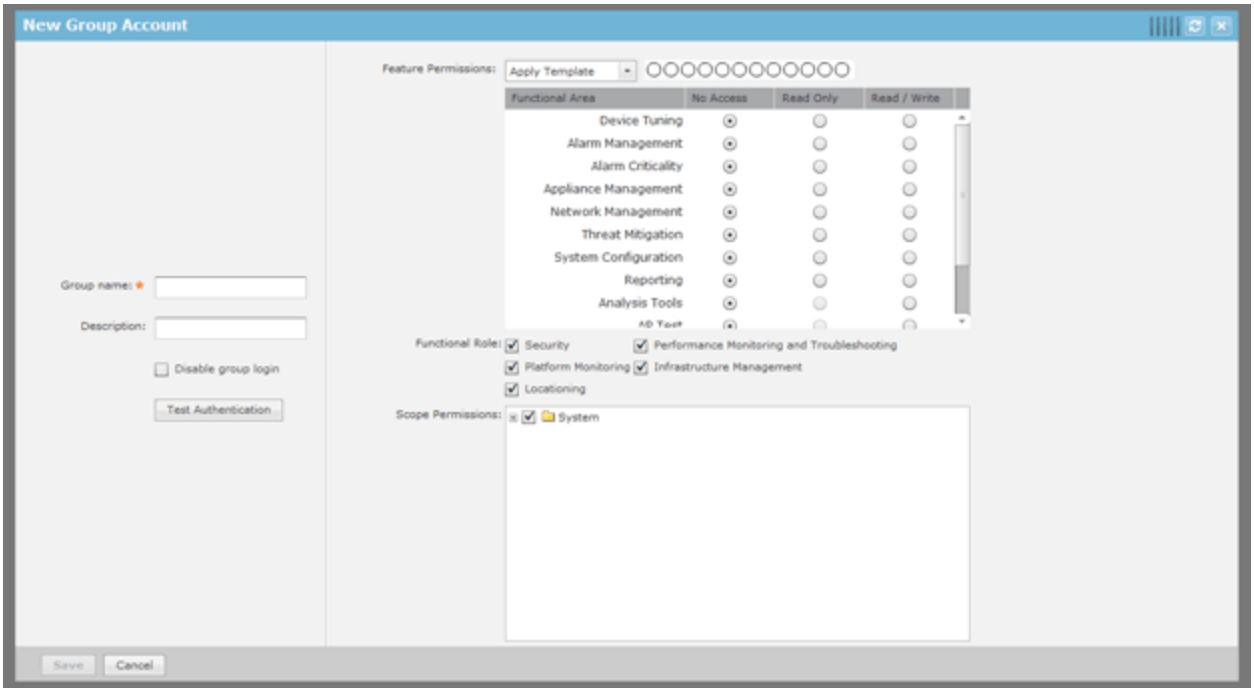
You can limit users to accessing and/or managing specific levels within the network tree. If you want users to have full access, give them permission to access the entire system. If you want users to only have access to a specific floor within a building, give them permission to access just that floor.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

Add/Edit Group Accounts

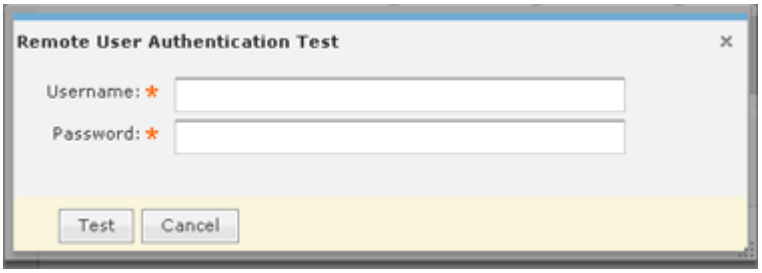
Group accounts involve a group of users set up through remote authentication (either LDAP or RADIUS). When a user attempts to log into ADSP that is a member of a group, ADSP first uses local authentication to log in the user. If the user is not part of local authentication, remote authentication is used. Upon finding the user's credential using remote authentication, the group status is check. 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	Test remote user authentication using LDAP or RADIUS.  Enter a user's username and password. Then, click the **Test** button. If the credentials are valid, you will receive a pass message. If the credentials are invalid, you will receive a failed message.

Field	Description
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 **Save** 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.

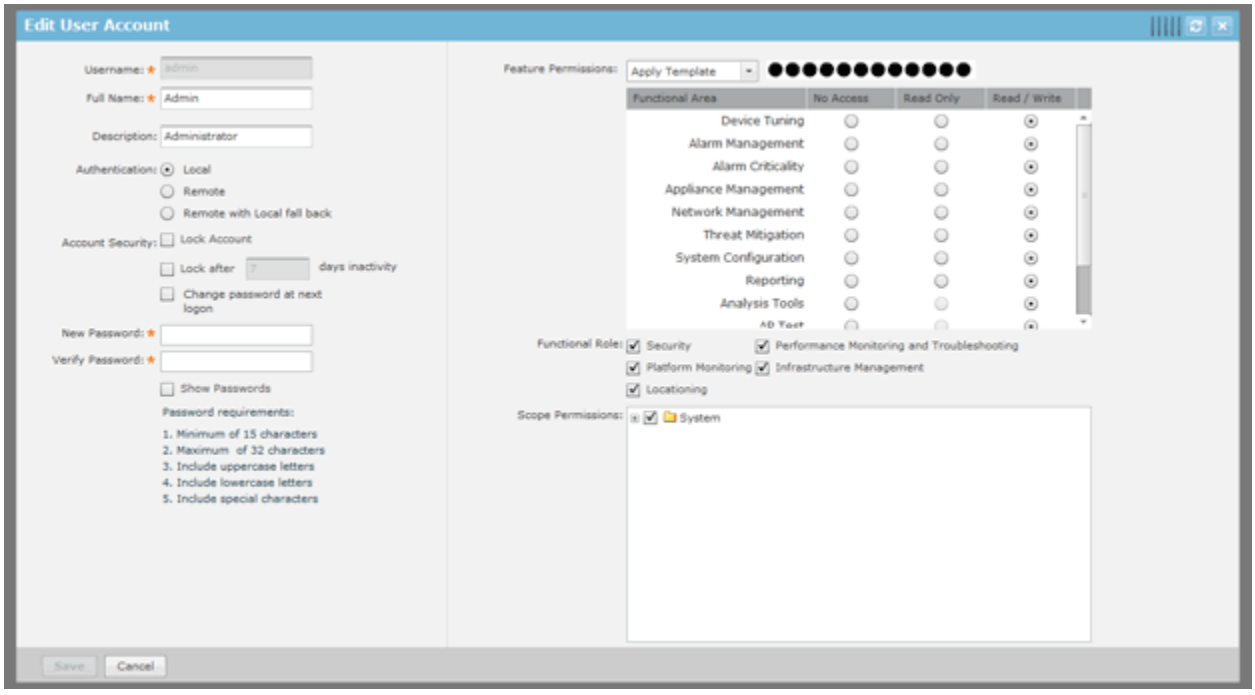
Edit, Copy, or Delete Accounts

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.

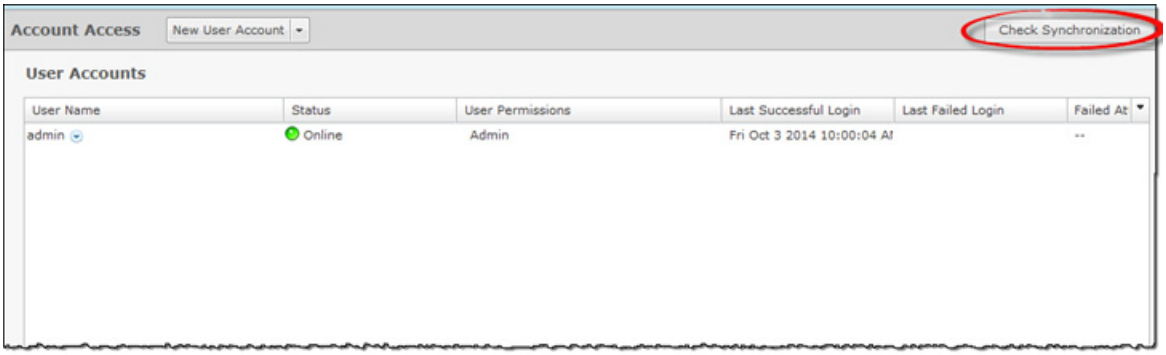


Once you have configured the user or group options, click **Save** to save the user/group account. ADSP will alert you to any errors. You can display more information about the error by clicking on the error message.

Click the **X** in the top-right corner to close the overlay panel.

Synchronize Accounts

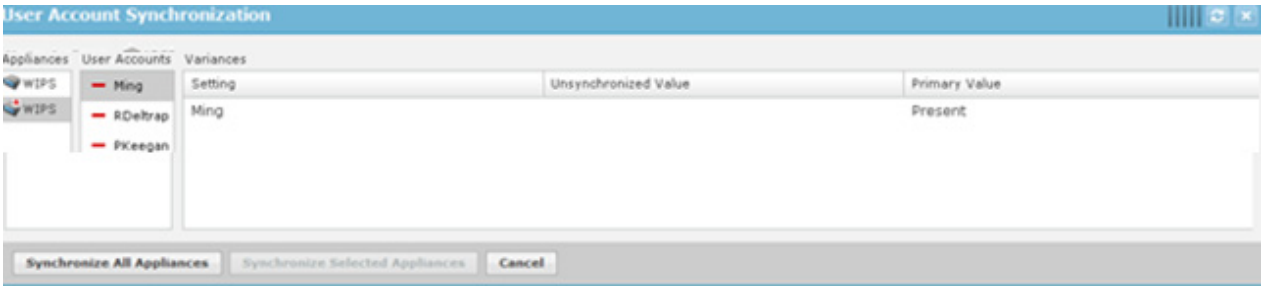
To synchronize accounts, go to **Configuration** > **Account Access** to display the **User Accounts** screen.



NOTE You must have a Central Management license in order to use the Check Synchronization feature.

With a Central Management license, you can use the **Check Synchronization** feature to check all the accounts on all your managed appliances and list the differences. You then have the option of synchronizing selected appliances or synchronizing all appliances. Click **Check Synchronization** to see if all accounts on all appliances in your system are in sync.

If an appliance is out of sync with the primary appliance, an 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.

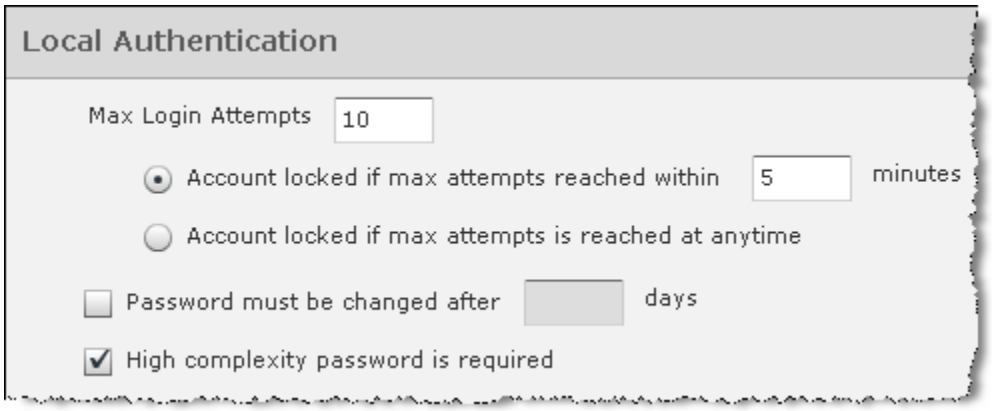


If you select (highlight) one of the user account, you will see the out of sync values.Click the **Synchronize All Appliances** button to add the missing accounts to all appliances in your system. Click the **Synchronize Selected Appliances** to add the missing accounts to the selected appliance(s).

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** > **Account 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.

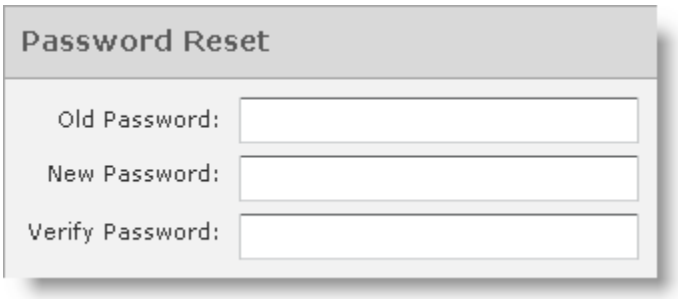
The **Check Synchronization** button is used to check all appliances in the network to ensure they are using the same Local Authentication. (The synchronization features works basically the same way wherever the feature is implemented. Synchronizing Accounts has a good example of how the synchronization 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 information for other users, you must be a user with the role of Admin. To access **Password Reset**, go to **Configuration** > **Account Management** > **Password Reset**.



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

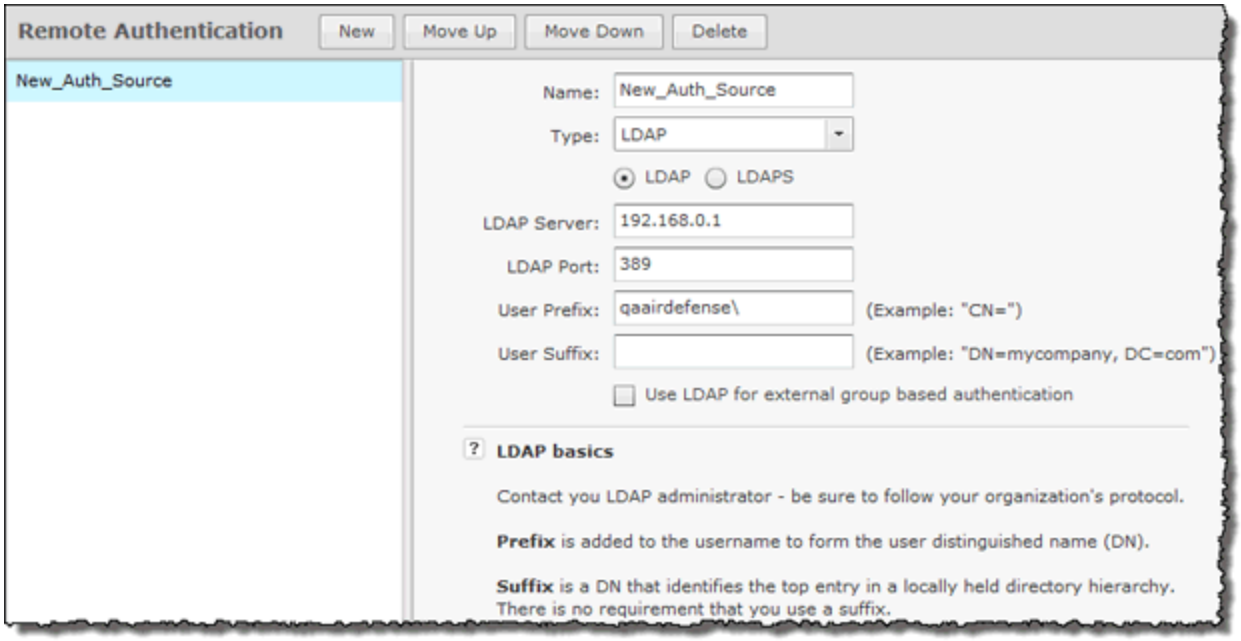
Remote Authentication is used authenticate users by using the password stored on a RADIUS or LDAP server. This reduces the cost of managing different passwords across different systems and avoids replication of password data throughout multiple databases. To access this feature, go to **Configuration** > **Account 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.

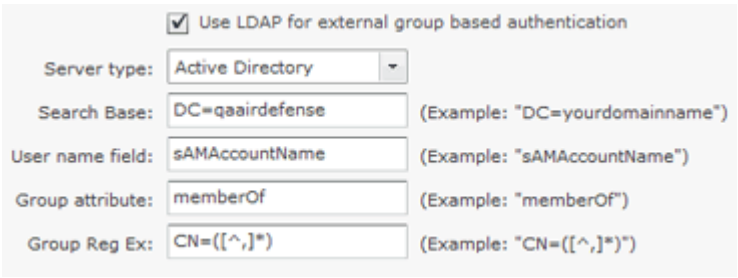
To get started, click the **New** button. Remote Authentication fields are displayed so that you can set up Remote Authentication.

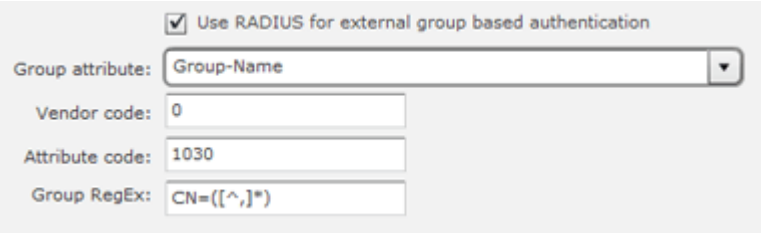


NOTE If you encounter problems, contact your LDAP administrator. He/she can advise you on how to fill in the fields. If you can, use an LDAP browser (http://www.ldapadministrator.com/download.htm) to login and browse. This will allow you to test your settings to see if they are right. There should also 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: **LDAP** or **LDAPS**. If the using a RADIUS server, the protocol type is selected from a drop-down menu. The options are **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPv2**.
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.

Field	Description
Shared Secret	Enter the shared secret password for the RADIUS server. You can make passwords viewable by selecting the **Display Passwords** checkbox. This option only displays for RADIUS servers.
Timeout	Enter a timeout value for authentication. This option only displays for RADIUS servers.
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\). **User Prefix** 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 (**User Suffix** is optional.) You can leave this field blank or you can supply a suffix.
Use LDAP for ...	This field is displayed if **LDAP** is chosen for the **Type** field. Select this checkbox if you are using external group based authentication. If checked, more fields are displayed. • Server type—For now, Active Directory is the only option. The information supplied in the other four fields are used in group identification for the Active Directory server type. • Search Base—Enter a string to find your domain name in the directory. Normally, the string is DC=yourdomainname. The **Search Base** field should be the same as the **User Prefix** field without any backslashes. • User field name—Enter a string to find your user name in the directory. Normally, the string is sAMAccountName. • Group attribute—Enter a string to find your group name in the directory. Normally, the string is memberOf. • Group Reg Ex—Enter a string that is used to strip out only unnecessary information and send what's left to ADSP for use in group identification. Normally, the string is CN=([^,]*). If the LDAP administrator changes any of the strings from what is normally used, he/she must inform you of the string to use. **Example**: 

Field	Description
Use RADIUS for ...	This field is displayed if **RADIUS** is chosen for the **Type** field. Select this checkbox if you are using external group based authentication. If checked, more options are displayed. • Group attribute—Displays a list of attributes to identify a group to ADSP. When an attribute is selected, values are inserted into the **Vendor code**, **Attribute code** and **Group RegEx** fields for ADSP to use in group identification. You should not change any of the inserted values. **Example**: 

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 *Authentication* or *User Roles*.

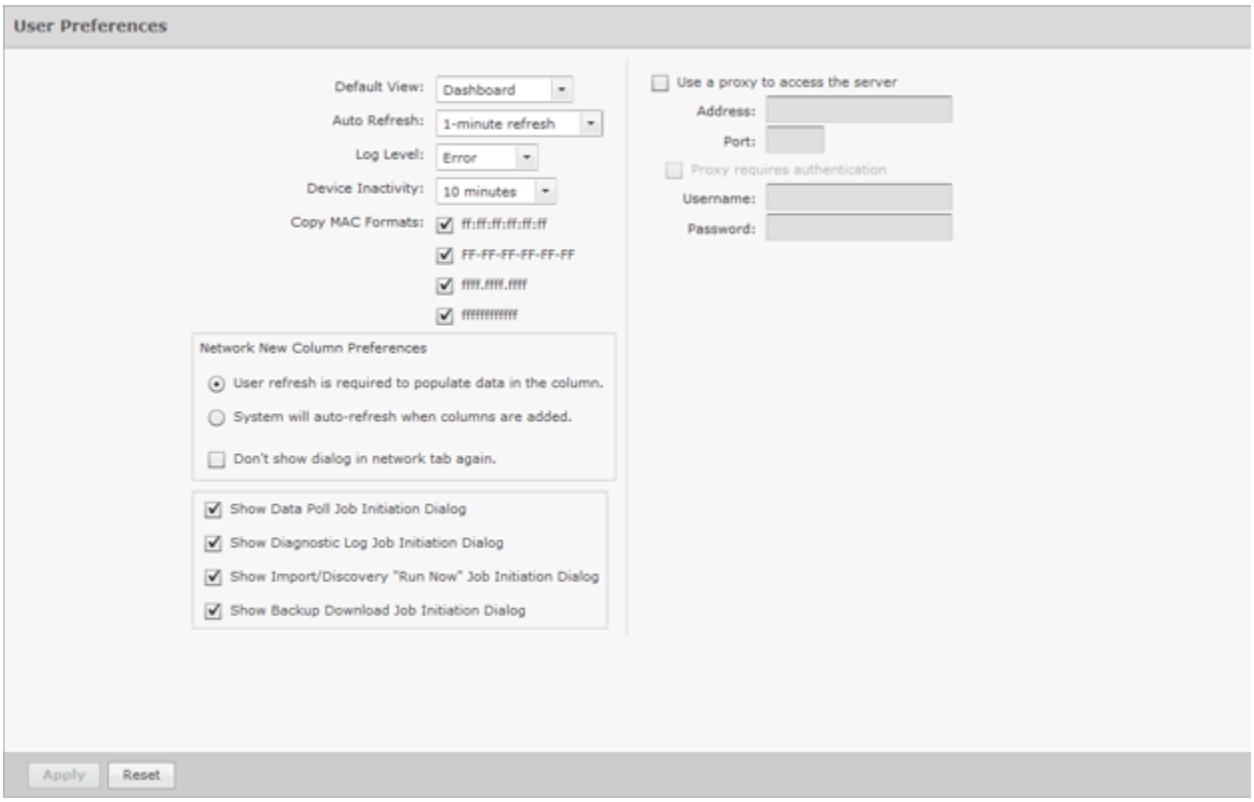
The **Check Synchronization** button is used to check all appliances in the network to ensure they are using the same Remote Authentication. (The synchronization features works basically the same way wherever the feature is implemented. *Synchronize Accounts* has a good example of how the synchronization 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.

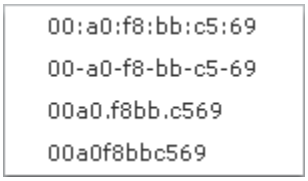
When viewing devices in the **Network** tab, the row of any device that is considered inactive will have lighter text than active devices.

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
- fffffffffff

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.

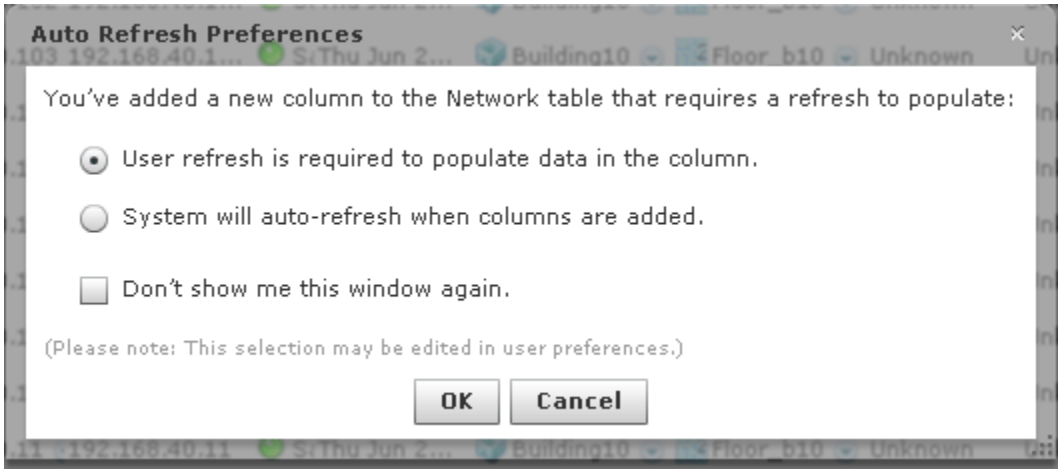
Network New Column Preferences

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.

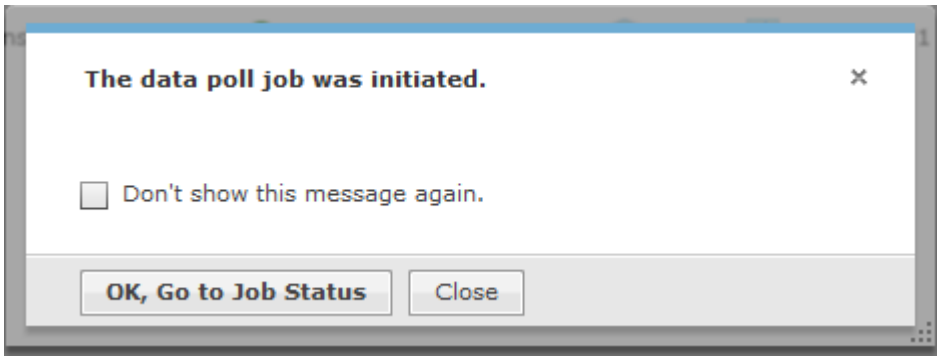


Click **OK** to save your changes.

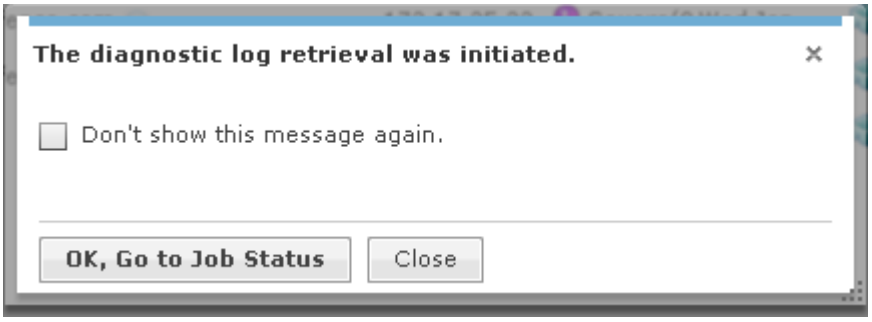
Show Job Initiation Message Dialogs

You have option of displaying a message dialog when initiating certain jobs. The different options are:

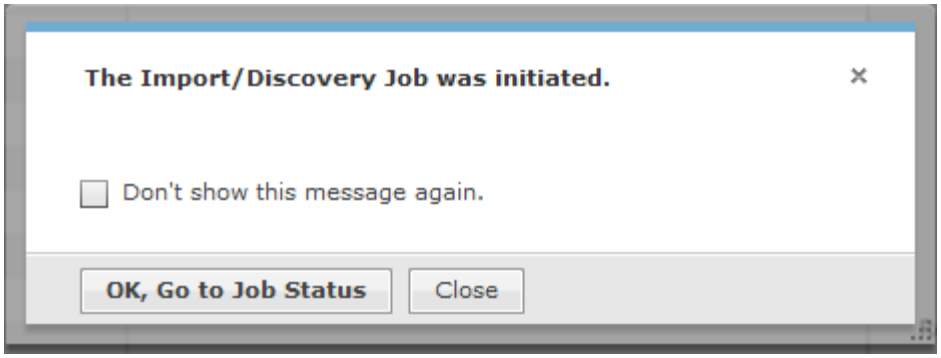
- Show Data Poll Job Initiation Message Dialog—Displays the following dialog window when a data poll is manually initiated:



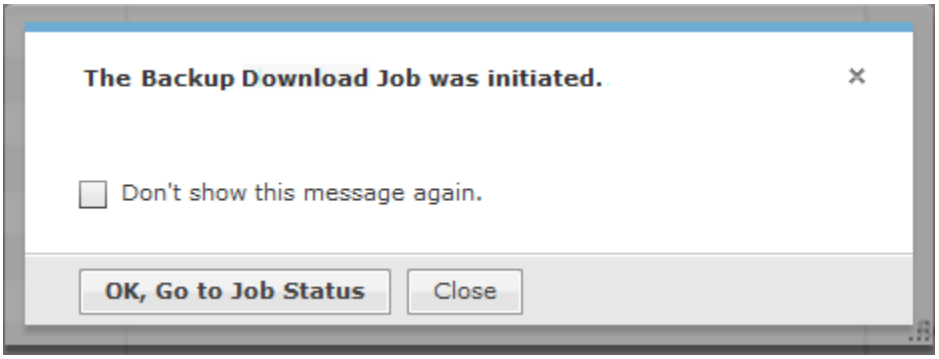
- Show Diagnostic Logs Job Initiation Message Dialog—Displays the following dialog window when manually retrieving the diagnostic log:



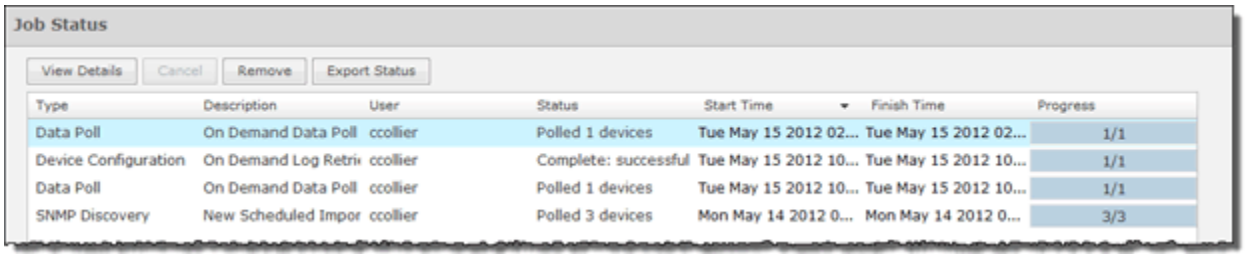
- Show Import/Discovery Job Initiation Message Dialog—Displays the following dialog window when an import/discover device is manually initiated:



- 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.



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 WLAN 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
- WLAN infrastructure running WiNG 5.2 or later
- Network with DHCP enabled
- DNS entry for the host AirDefense1 in the domain of the DHCP scope the WLAN device will be initially attached to
  - This solution does support DNS devolution

- Network which is able to route traffic and permit the following flows:
  - SNMP traps (UDP port 162) traffic from the infrastructure to the ADSP appliance
  - SNMP query traffic (UDP port 161) between ADSP and the infrastructure
  - SSH application traffic between the ADSP appliance and the infrastructure
  - SFTP or FTP traffic between the device and the Relay server (can be same system as the ADSP appliance)
  - SFTP or FTP traffic between ADSP and the external relay server when one is used.

Setup Prerequisites

1 Enable SNMP Trap reception on the ADSP appliance:

a. From the ADSPadmin utility on the appliance console, select **C** for Config then **SNMP** for Enable/Disable SNMP trap reception.

b. Select **E** for enable and save changes as shown below.

```
SNMP currently disabled


       (E) Enable SNMP

(Q) to quit (return to previous menu)     ->


Save the SNMP state as shown above? (yes/no): yes

iptables: Flushing firewall rules:                          [ OK ]
iptables: Setting chains to policy ACCEPT: filter           [ OK ]
iptables: Uploading modules:                                [ OK ]
iptables: Applying firewall rules:                          [ OK ]
iptables: Loading additional modules: ip_conntrack_tftp     [ OK ]

(Press <CR> to return to previous menu)
```

2 Verify Discovery SNMP Parameters:

a. In the appliance GUI, go to **Configuration** > **Appliance Platform** > **Communication Settings**.

b. Click on the **Unplaced Devices** folder.

NOTE When performing a discovery based on receiving a SNMP trap from a device, the system will use credentials based on the profile(s) set on the **Unplaced Devices** folder. The **Unplaced Devices** folder must have the default credentials for the device being deployed for the discovery to work successfully.

c. Uncheck default profiles for device types which will not be placed on your network.

For example, for deployments of just WiNG 5.2 devices, you would uncheck all default profiles but the 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.

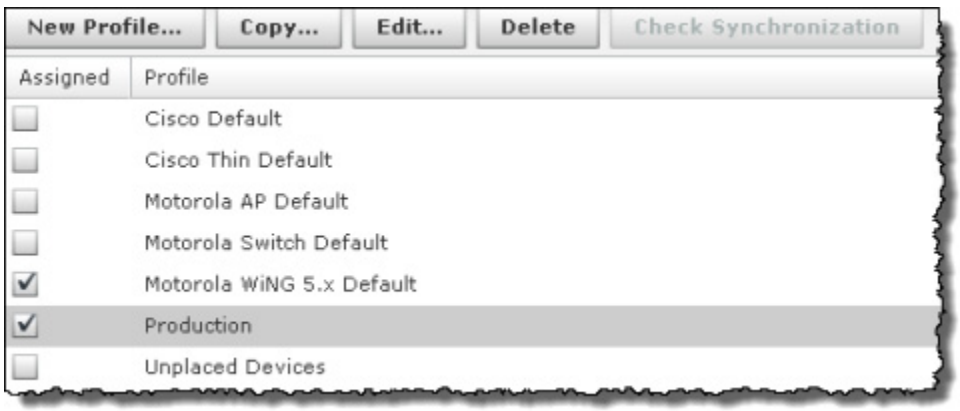
c. Uncheck default profiles for device types which will not be placed on your network.

For example, for deployments of just WiNG 5.1 devices, you would uncheck all default profiles but the 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.

d. Add a new profile which uses the non default production credentials that the infrastructure will have after completion of the zero touch configuration.

Once complete, profile assignment should look like below:

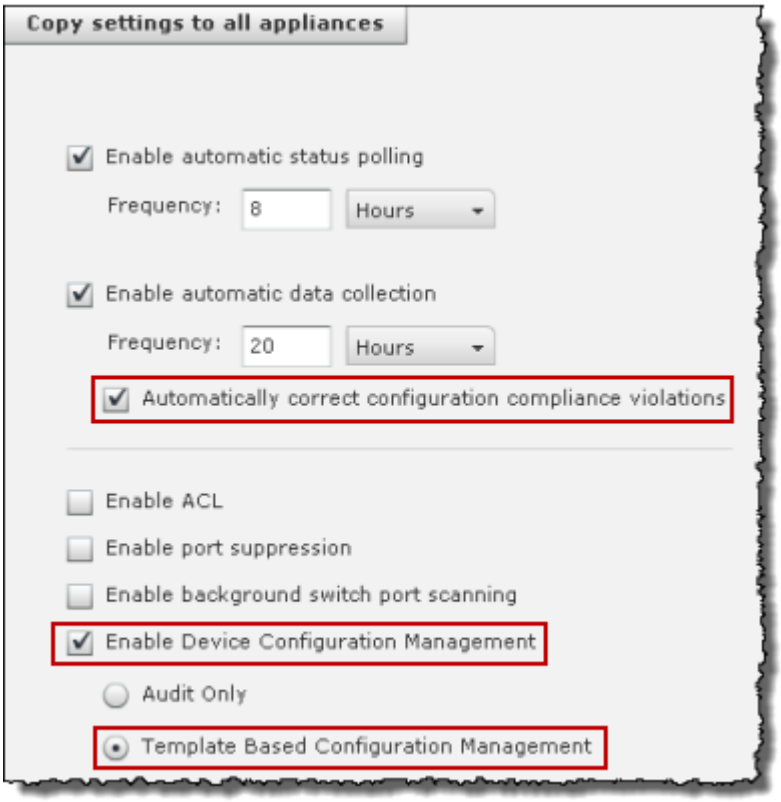


4 Setup network device configuration action:

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



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:

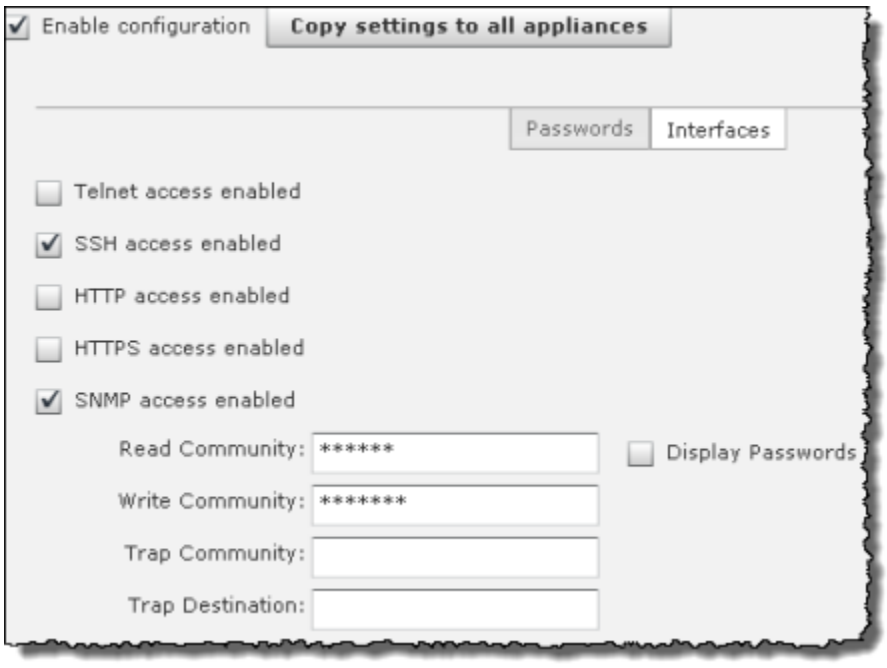
a. Some infrastructure devices require changing the administrator password at first login. The ADSP system must be setup with the credentials to use for configuring the device. The credentials can be set by going to **Configuration** > **Infrastructure Management** > **Device Access**.

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.

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.



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 AP7131 which can be used to configure other 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, the AP7131 and a static IP address are used.

1. Collect all the passwords for the AP7131 to be managed.
2. Enable SSH/Telnet if it is not enabled on the AP7131.
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 AP7131. 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 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 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 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 . 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 is managed already and something in its profile changes.
   - The 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 by selecting the scope where the floor the 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 . Now ADSP can communicate with the .

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 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.

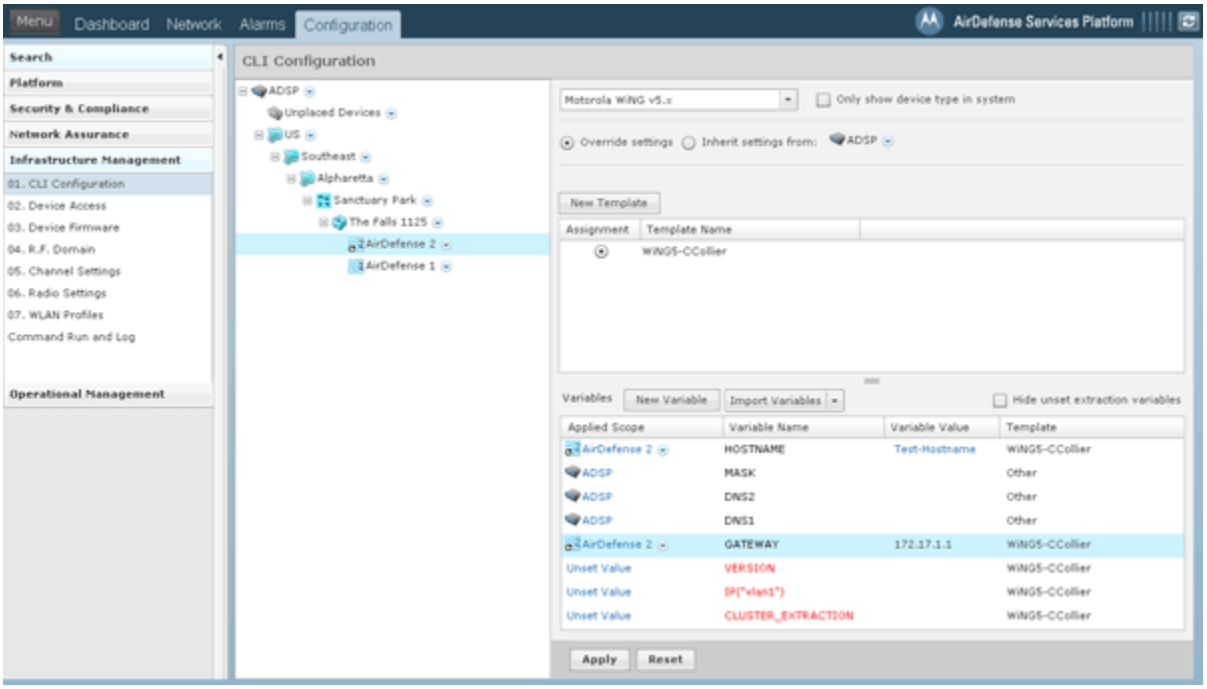
When sending variables to the device or displaying variables in the GUI, the CLI Profile variables and CLIVars Profile variables are merged (with CLIVars Profile variables taking precedence).

Scenario A

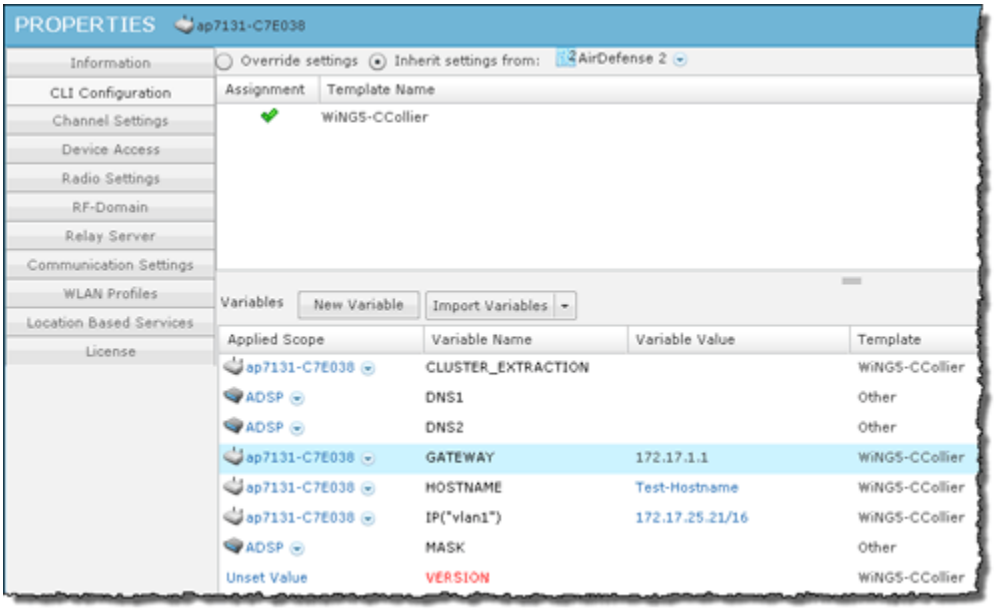
ProfileX is defined at the folder level as follows:

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.



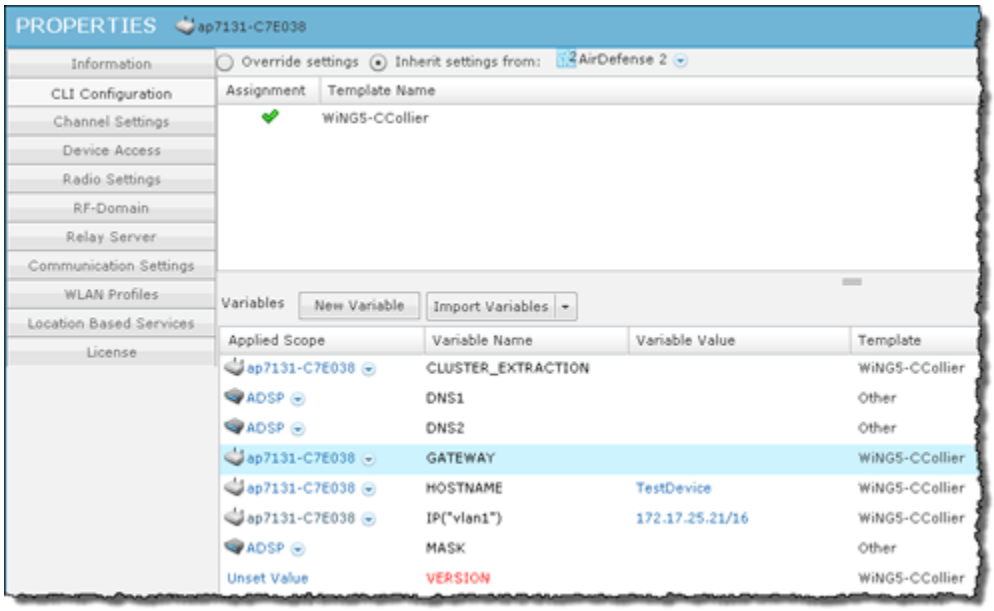
The result of this scenario is that these settings are defined at the CLI Profile level and inherited straight from their definition at the folder level.

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

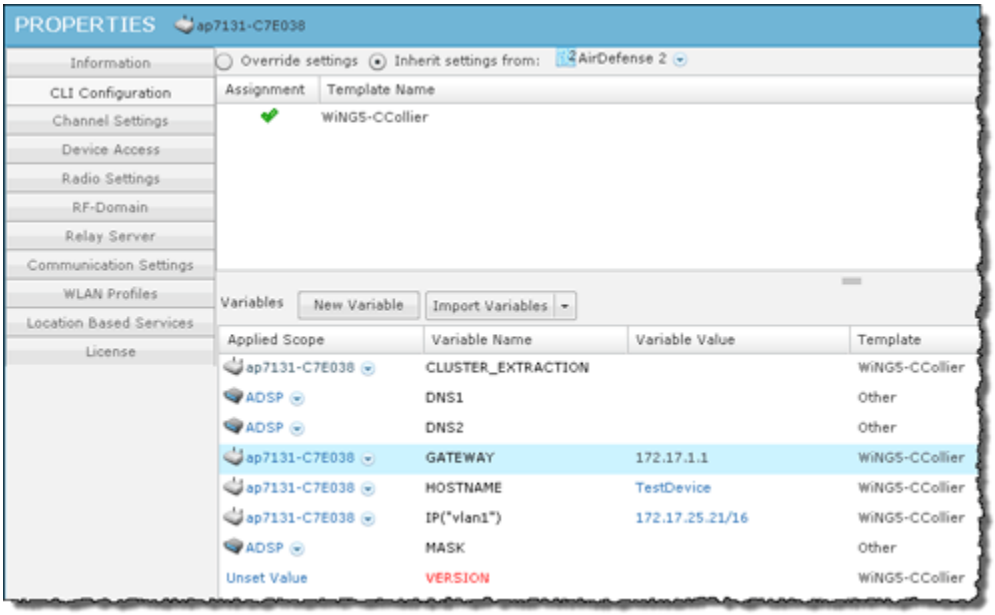
b. GATEWAY is cleared to null



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

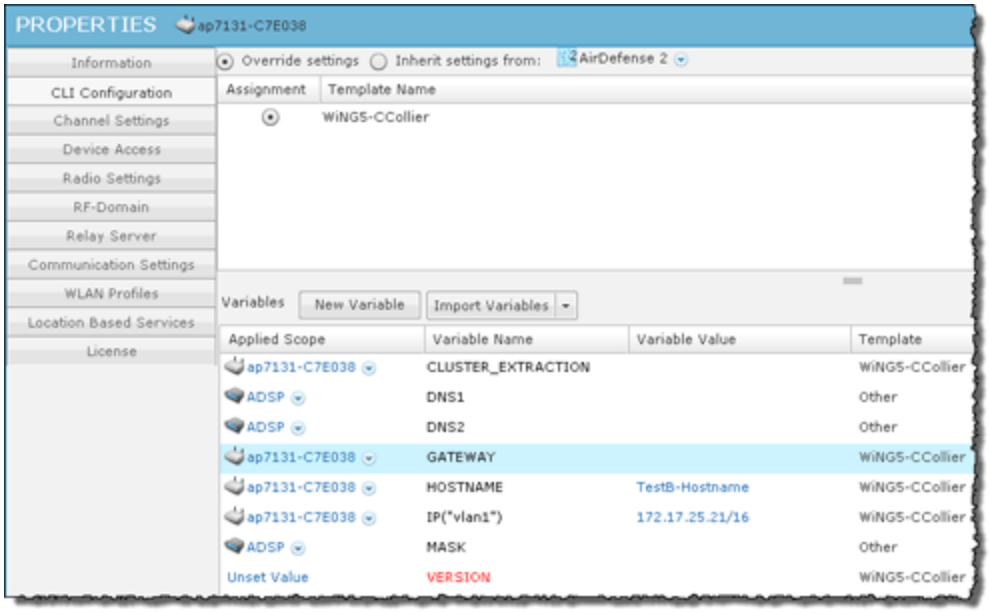


The result of this combination will result in the HOSTNAME coming from the CLIVars and the GATEWAY coming from the CLI Profile (ProfileX)

Scenario C

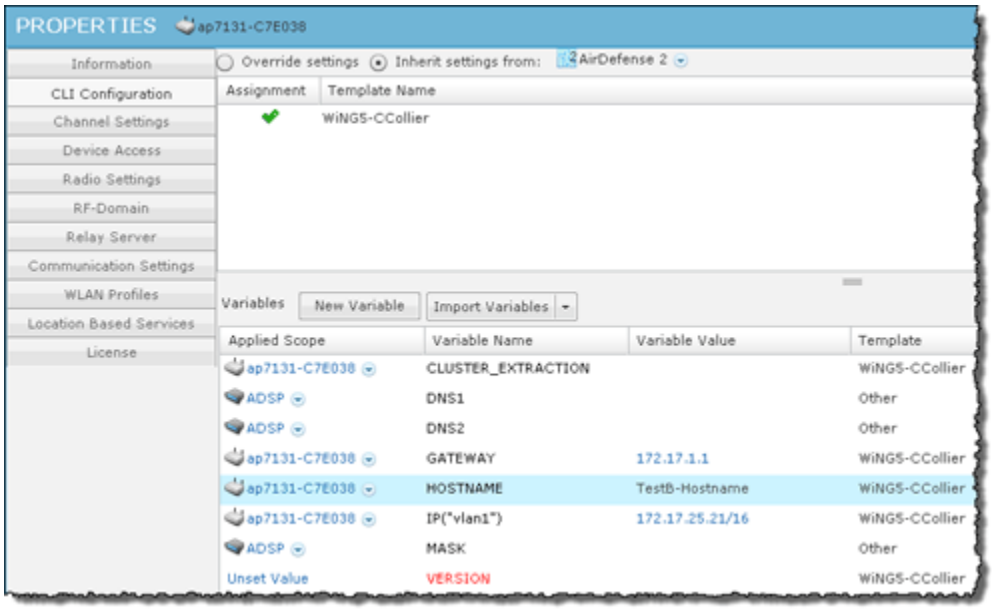
ProfileX and ProfileY are defined at the folder level but modified at the device level (override a named profile) or (inherit profile but edit variables) as follows:

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



3. Save changes.

4 Now set back to inherit either ProfileX or ProfileY (any other profile).



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.

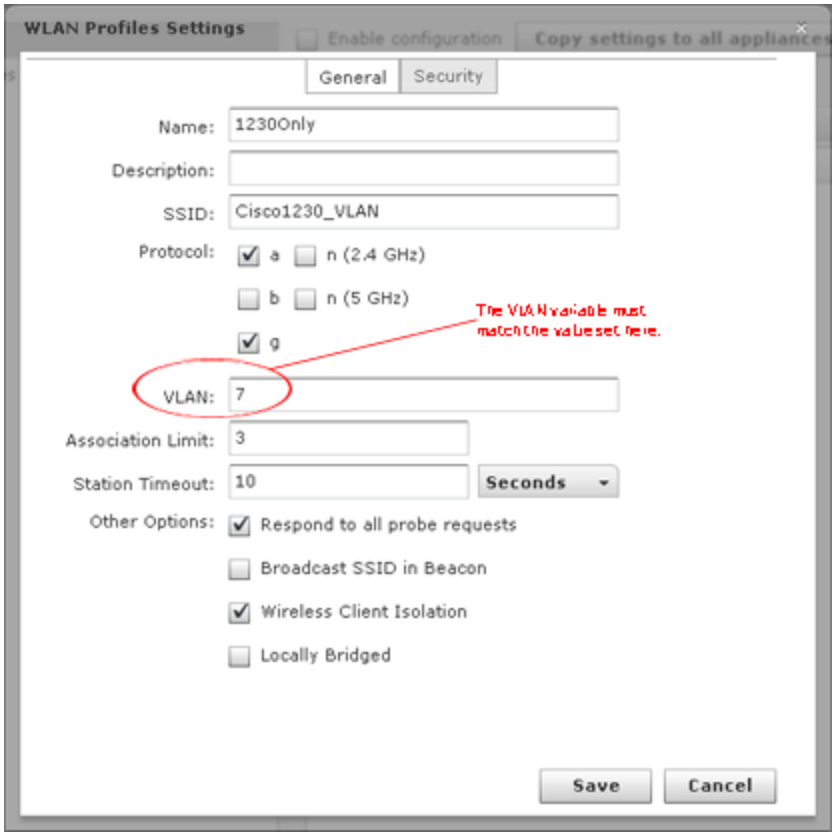
The following conditions are assumed:

- 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].

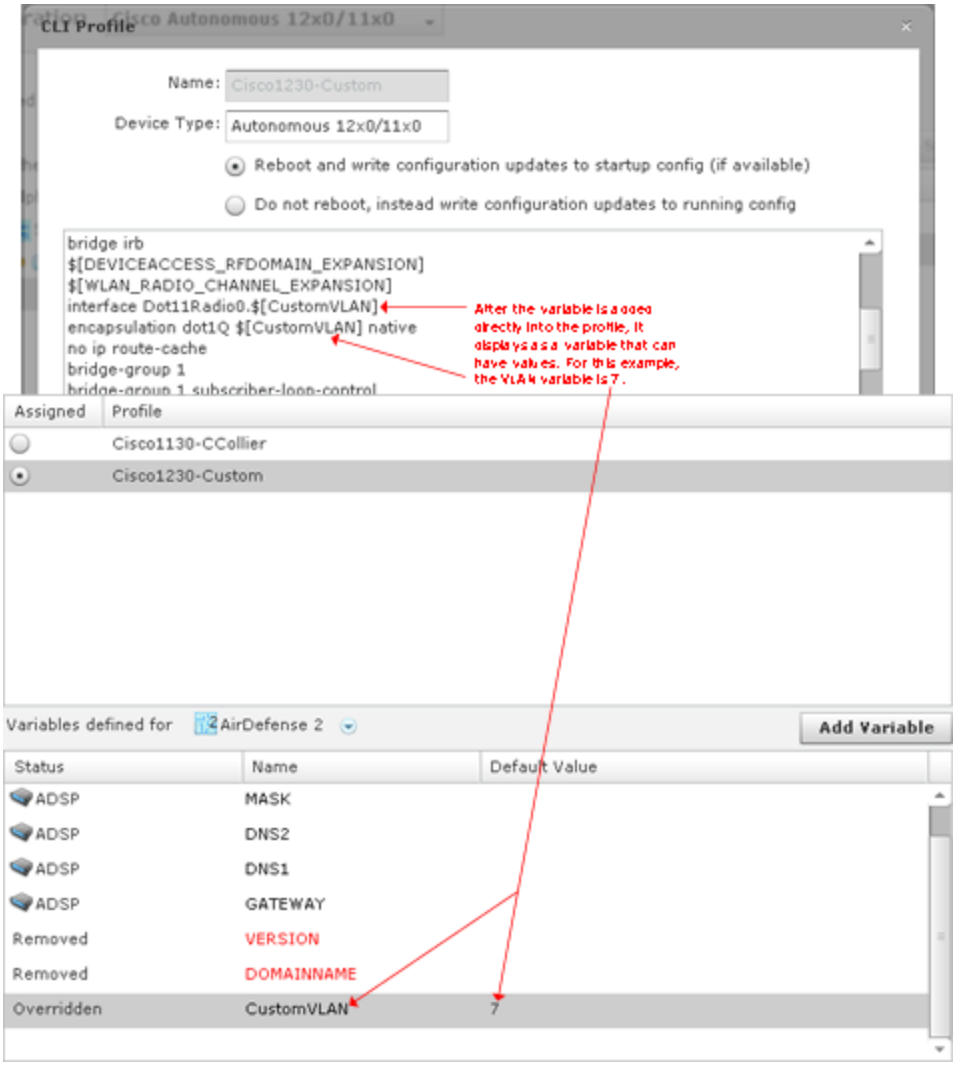
2 By inserting this variable into a CLI profile, you are able to match the non-default setting in the WLAN Profile.



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.



c. To complete this VLAN customization example for the Cisco 1230 AP, the following modifications need to be made:

i. interface Dot11Radio0.$[CustomVLAN]

ii. encapsulation dot1Q $[CustomVLAN] native

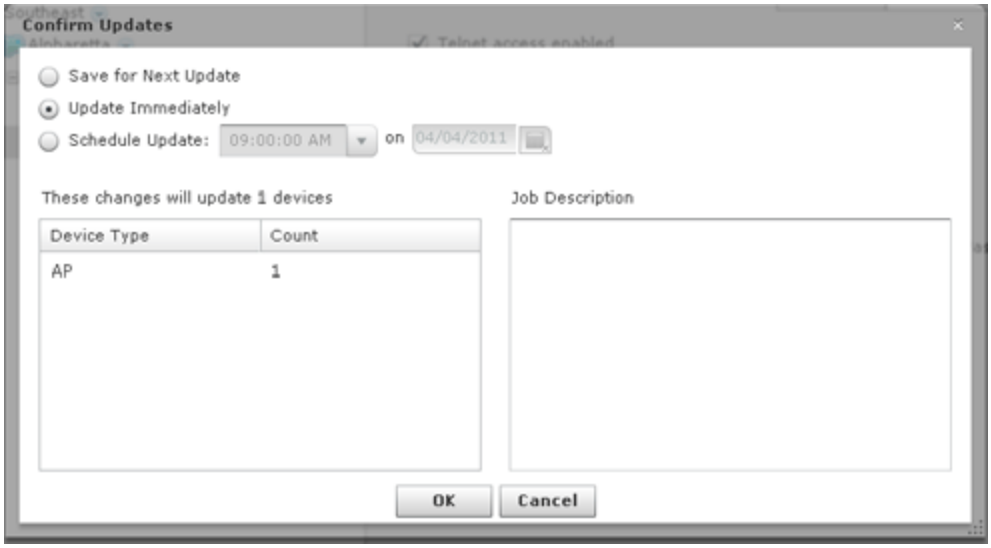
iii. interface Dot11Radio1.$[CustomVLAN]

iv. encapsulation dot1Q $[CustomVLAN] native

v. interface FastEthernet0.$[CustomVLAN]

vi. encapsulation dot1Q $[CustomVLAN] native

4 When you apply the values in the custom CLI configuration, they are applied to the configured device.



5 As with all customizations, you should test it in a lab environment before putting it into production.

Configuration Notes

ADSP 9.x WS2000 upgrade will only occur if the relay server is accessible from subnet1.

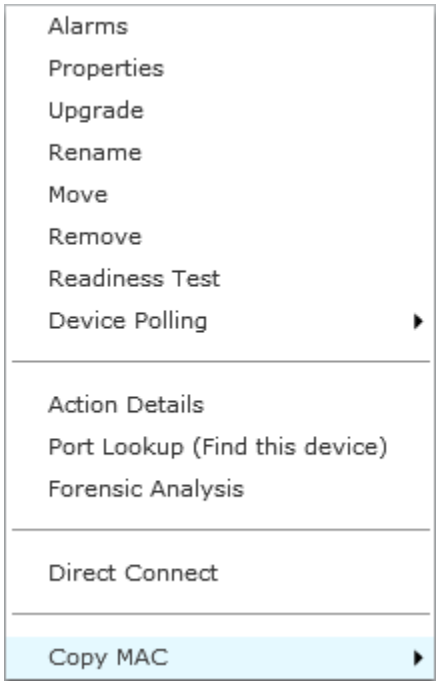
Drop-down Menu Access

Drop-down menus are located throughout ADSP. Whenever a device or network level is displayed, it has an associated drop-down menu. You can access the drop-down menu to get details on functions and properties. Click the drop-down menu button– to display information on functions that operate on a single device or group of devices.

Devices—Drop-down Menu

APs—Drop-down Menu

The APs drop-down menu contains functions that you can apply to the selected AP. Click the drop-down menu button— next to the AP name to display the drop-down menu.



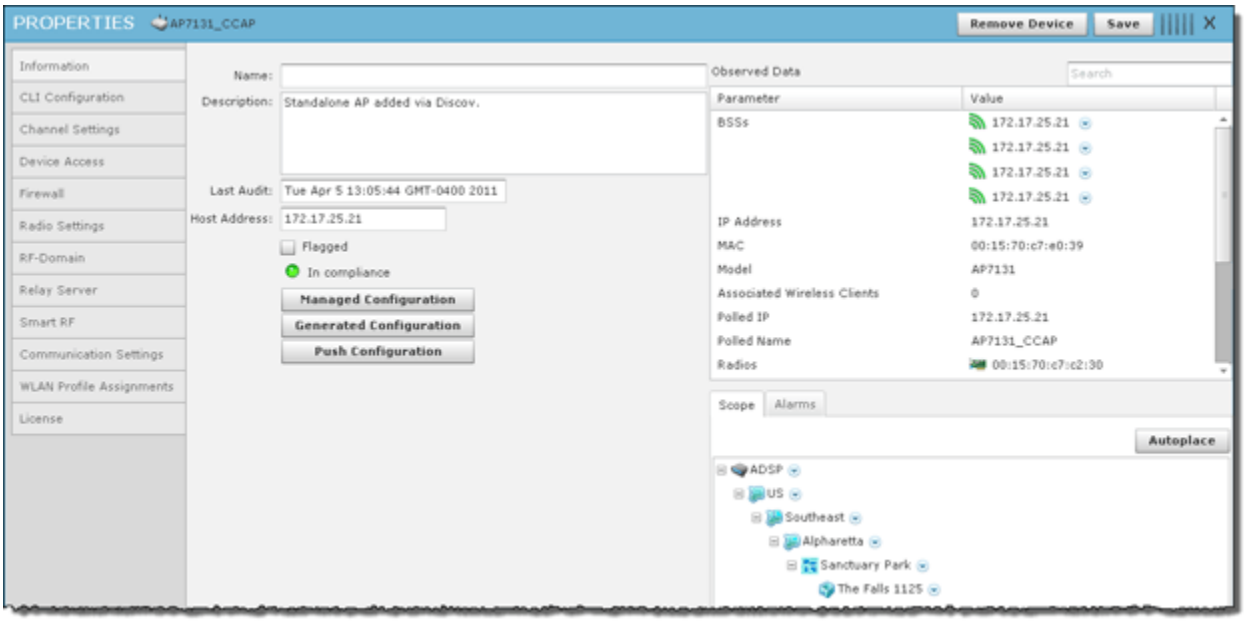
The drop-down menu for APs contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected AP.
Properties	Opens the **Properties** overlay for the selected AP.
Upgrade	• Upgrades the firmware for the selected AP. (For more information, see *Upgrade Devices* in the *Network* chapter.)
Rename	Opens a dialog window to rename the selected AP.
Move	Moves the selected AP to another network level (floor). (See *Move Devices* for more information.)
Remove	Removes the selected AP from your network. (See *Remove Devices* for more information.)
Readiness Test	Validates that the AP is management ready (that is, it can be manage through ASDP). You are alerted of problem areas. (See *Readiness Test* for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected AP. (See *Audit Devices* for more information.)

Function	Description
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup	This feature is disabled unless you have a WIPS license.
Forensic Analysis	Opens the *Forensic Analysis—Basic* window for the specified .
Direct Connect	Accesses the user interface (UI) for the selected .
Copy MAC	Copies the MAC address of the selected for later use.

Properties

You can view the properties of an AP by clicking the drop-down menu button– and clicking **Properties**.



The following information is displayed:

Field	Description
Name	The name of the AP.
Description	A description of the AP.
Last Audit	The date and time of the last audit.
Host Address	IP address of the AP.

Field	Description
Flagged	Flag an AP that you want to bring attention to.
In compliance / Not in compliance	Status of the last compliance audit. Click the **Managed Configuration** button to display the configuration. Click the **Generated Configuration** 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 **Push Configuration** button to push the existing configuration out to the .
Observed Data	Data that AirDefense Services Platform observed about the . You can filter the observed data by entering significant text in the **Search** field.

The scope of the AP is shown under the **Scope** tab. The **Autoplace** button can be used to place the AP in a network folder using Auto-Placement rules.

Alarms related to the AP 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 the AP configuration by selecting:

- *CLI Configuration*
- *Channel Settings*
- *Device Access*
- *Radio Settings*
- *RF-Domain*
- *Relay Server*
- *Communication Settings Profile*
- *WLAN Profiles*
- License—Display valid licenses for APs.

These configuration settings (or profiles) are all located in the *Configuration Tab*.

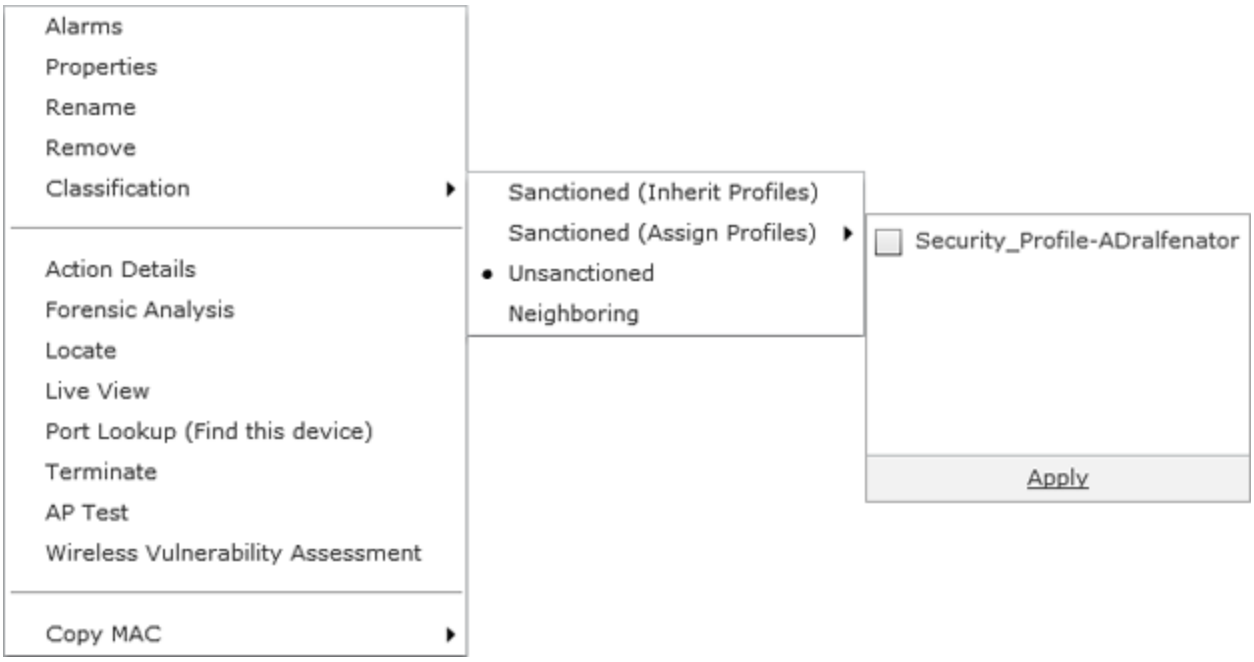
If you make changes, click **Save** to save them.

Click the **Delete Device** button to remove a device from your network.

Click the **Close** button–X to close the **Properties** overlay.

BSS—Drop-down Menu

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.



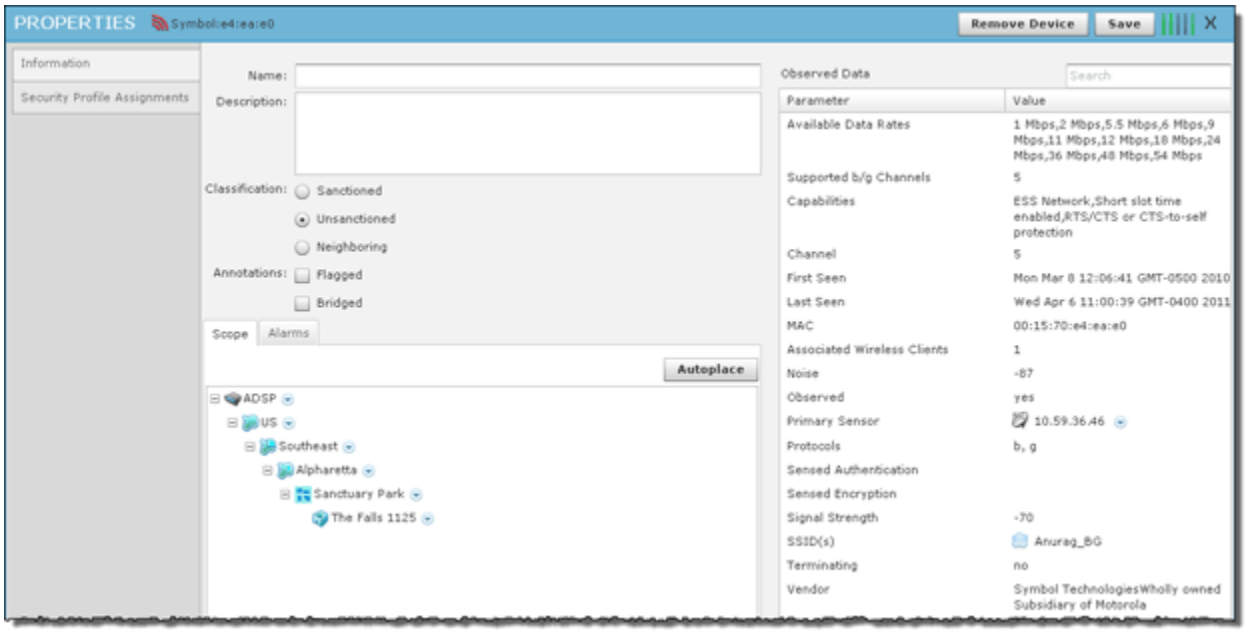
The drop-down menu for BSSs contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected BSS.
Properties	Opens the **Properties** overlay for the selected BSS.
Rename	Opens a dialog window to rename the selected BSS.
Remove	Removes the selected BSS from your network. (See *Remove Devices* for more information.)
Classification	Classifies the BSS using one of the following classifications: • Sanctioned (inherit)—Classify the selected BSS as a sanctioned device that inherits its traits from wherever its location in the network tree. • Sanctioned (override)—Classify the selected BSS as a sanctioned device using traits that override the inherited traits. For example, a security profile can be applied to a BSS that overrides the inherited traits. When using this classification, select the profile and click the **Apply** link. • Unsanctioned—Classify the selected BSS as unsanctioned. • Neighboring—Classify the selected BSS as a neighboring device.

Function	Description
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Forensic Analysis	Opens the *Forensic Analysis—Basic* window for the specified BSS.
Locate	Opens the device Location tracking window so that you can quickly locate the selected BSS.
Live View	Opens the *Live View* window for the selected BSS; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the Port Lookup window where you can locate the physical port where the BSS is accessing your network.
Terminate	Opens the Termination options so that you can terminate the connection of the BSS to your network.
AP Test	Tracks network failures from an automated or manual AP connectivity test. (See *Scheduled AP Tests* for more information.)
Wireless Vulnerability Assessment	Opens the Vulnerability Assessment window so that you can scan your wireless network for vulnerabilities. (See *On-Demand Vulnerability Assessment* 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**.



The following information is displayed:

Field	Description
Name	The name of the BSS.
Description	A description of the BSS.
Classification	The classification of the BSS: **Sanctioned**, **Unsanctioned**, or **Neighboring**.
Annotations	The annotations specified for the BSS: **Flagged** or **Bridged**.
Observed Data	Data that AirDefense Services Platform observed about the BSS. You can filter the observed data by entering significant text in the **Search** 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*.

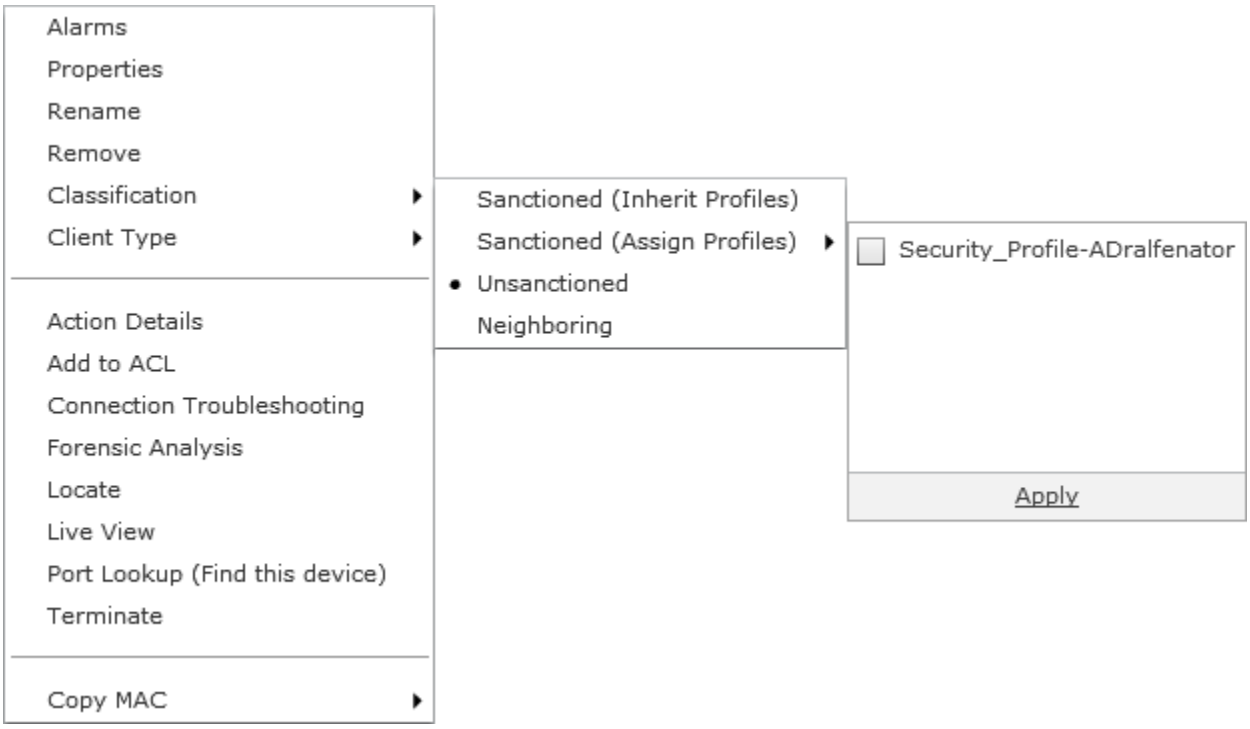
If you make changes, click **Save** to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button–X to close the **Properties** overlay.

Wireless Clients—Drop-down Menu

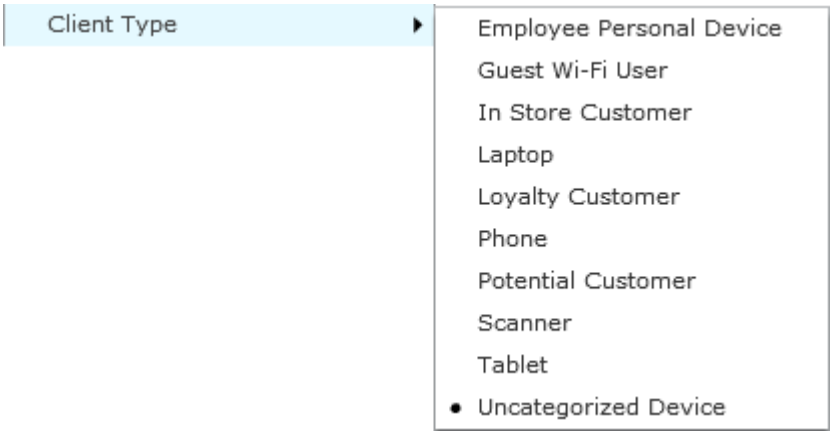
The Wireless Client drop-down menu contains functions that you can apply to the selected Wireless Client. Click the drop-down menu button– next to the Wireless Client name to display the drop-down menu.



The drop-down menu for Wireless Clients contains the following functions:

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

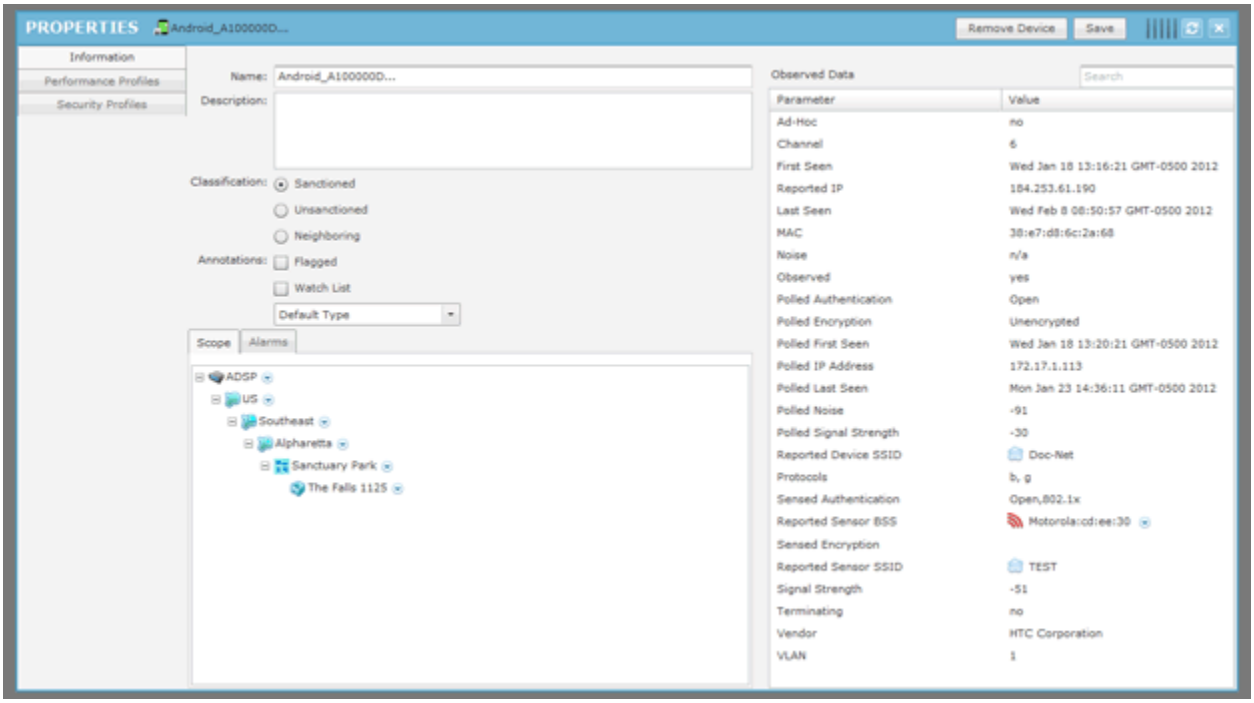
Function	Description
Classification	Classifies the Wireless Client using one of the following classifications: • Sanctioned (inherit)—Classify the selected Wireless Client as a sanctioned device that inherits its traits from wherever its location in the network tree. • Sanctioned (override)—Classify the selected Wireless Client as a sanctioned device using traits that override the inherited traits. For example, a security profile can be applied to a Wireless Client that overrides the inherited traits. When using this classification, select the profile and click the **Apply** link. • Unsanctioned—Classify the selected Wireless Client as unsanctioned. • Neighboring—Classify the selected Wireless Client as a neighboring device.

Function	Description
Client Type	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 hand-held devices from laptops in ADSP. • Employee Personal Device— • Guest Wi-Fi User— • In Store Customer— • Laptop— • Loyalty Customer— • Phone— • Potential Customer— • Scanner— • Tablet— • Uncategorized Device—  • Select the appropriate device to represent a Wireless Client and use its icon for the selected Wireless Client throughout the GUI.
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 *Connection Troubleshooting* so that you can troubleshoots a Wireless Client's ability to connect to your wireless network.
Forensic Analysis	Opens the *Forensic Analysis—Basic* window for the specified Wireless Client.

Function	Description
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.
Live View	Opens the *Live View* window for the selected Wireless Client; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the Port Lookup window where you can locate the physical port where the Wireless Client is accessing your network.
Terminate	Opens the Termination options so that you can terminate the connection of the Wireless Client to your network. (See *Terminate* 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: **Sanctioned**, **Unsanctioned**, or **Neighboring**.
Annotations	The annotations specified for the Wireless Client: **Flagged** or **Watch List**. 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 **Search** 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*.

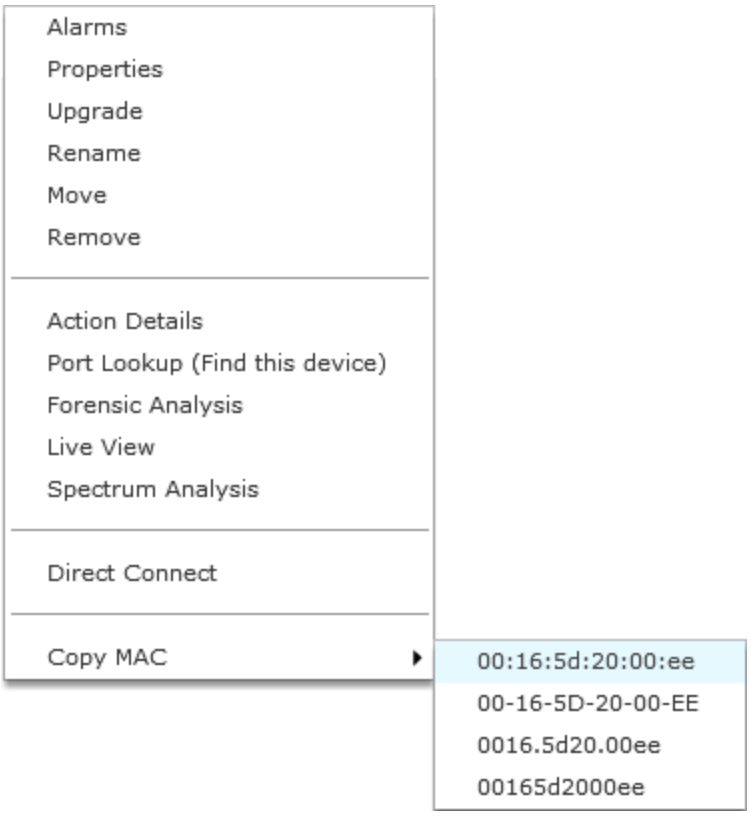
If you make changes, click **Save** to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button–X to close the **Properties** overlay.

Sensors—Drop-down Menu

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.



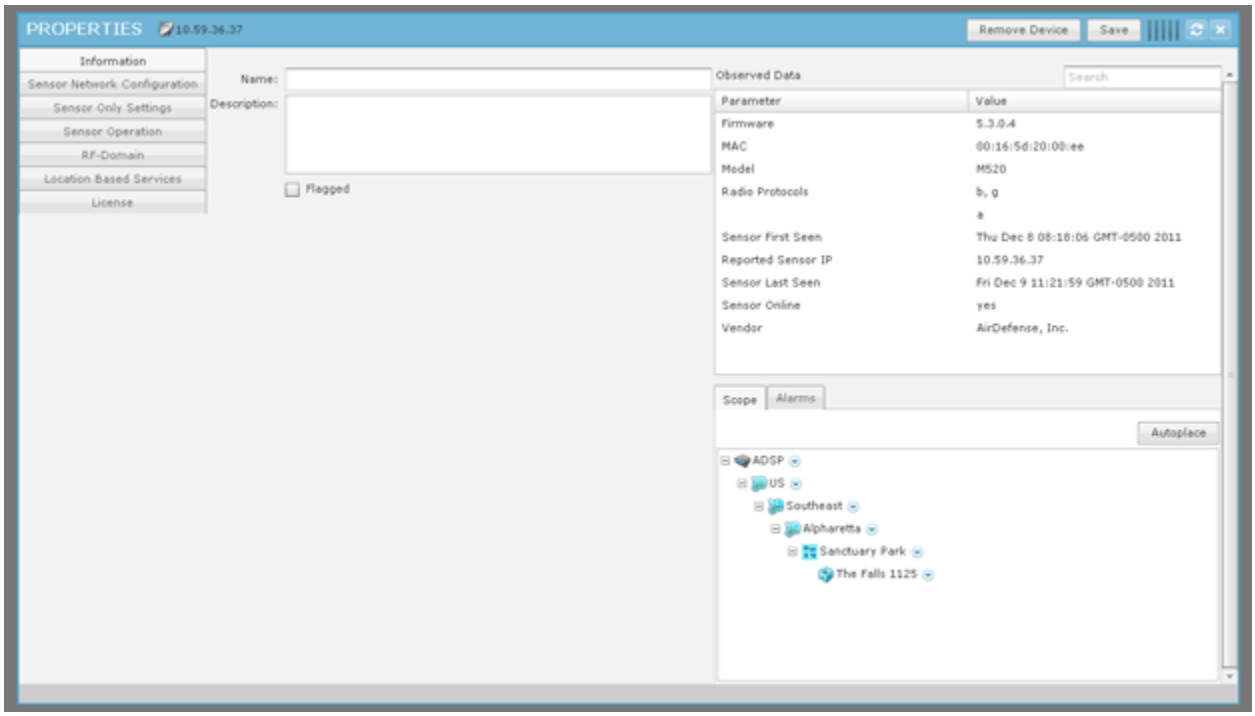
The drop-down menu for Sensors contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected Sensor.
Properties	Opens the **Properties** overlay for the selected Sensor.
Upgrade	Upgrades the firmware for the selected Sensor. (For more information, see *Upgrade Devices* in the *Network* chapter.)
Rename	Opens a dialog window to rename the selected Sensor.
Move	Moves the selected Sensor to another network level (floor). (See *Move Devices* for more information.)
Remove	Removes the selected Sensor from your network. (See *Remove Devices* 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 *Forensic Analysis—Basic* window for the specified Sensor.

Function	Description
Live View	Opens the *Live View* 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 *Spectrum Analysis* 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 **Search** 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 **Save** 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.

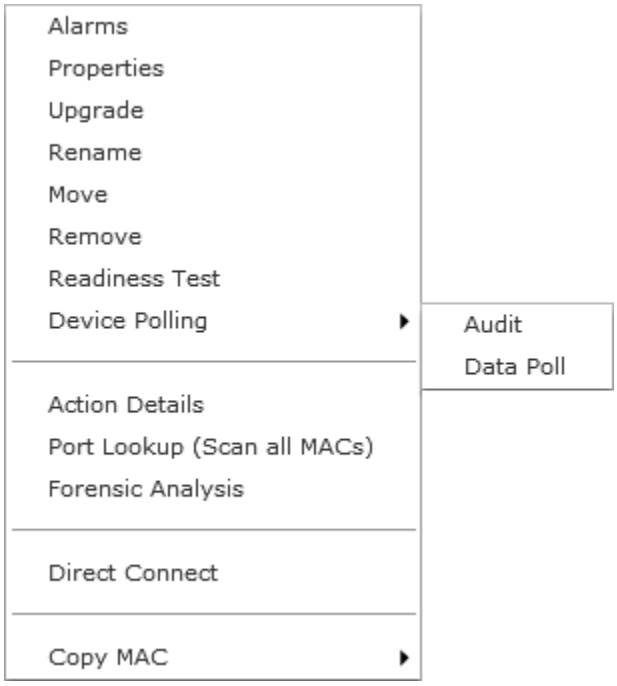
Field	Description
Use DHCP	Select the checkbox to enable DHCP.
IP Address	Manually enter a static IP address for the Sensor.
Prefix Length	Specify the static prefix length as a decimal value.
Gateway	Manually assign a valid static Gateway IP address to the Sensor.

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—Drop-down Menu

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.



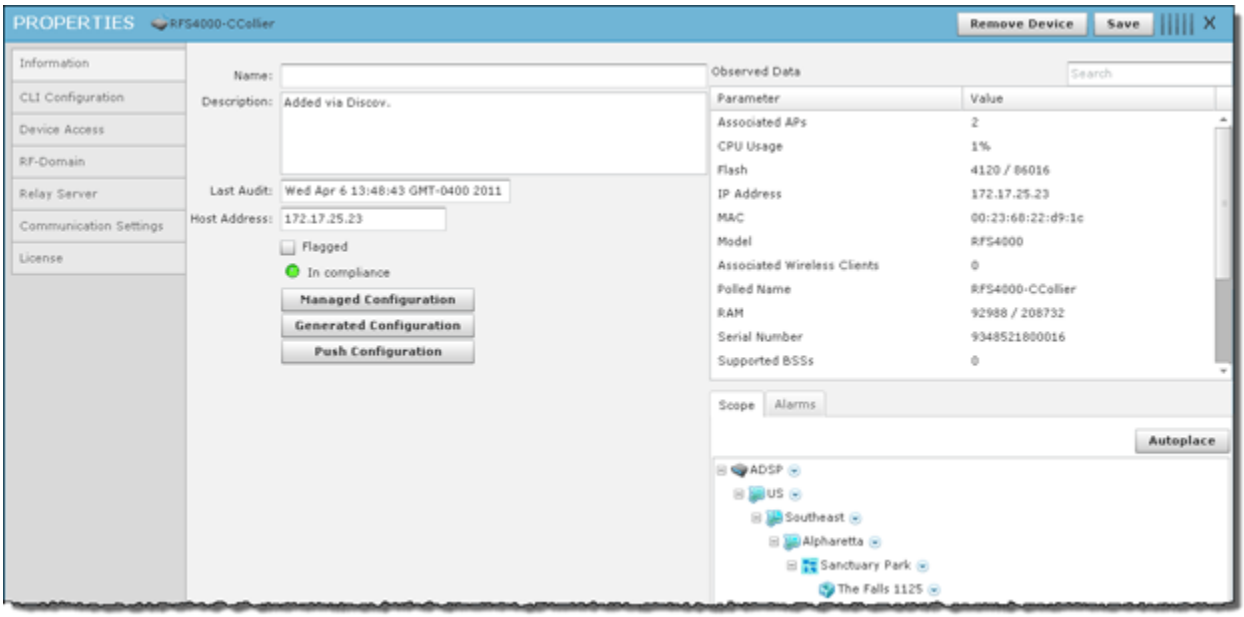
The drop-down menu for Wireless Switches contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected Wireless Switch.
Properties	Opens the **Properties** overlay for the selected Wireless Switch.
Upgrade	Upgrades the firmware for the selected Wireless Switch. (For more information, see *Upgrade Devices* in the *Network* chapter.)
Rename	Opens a dialog window to rename the selected Wireless Switch.

Function	Description
Move	Moves the selected Wireless Switch to another network level (floor). (See *Move Devices* for more information.)
Remove	Removes the selected Wireless Switch from your network. (See *Remove Devices* for more information.)
Readiness Test	Validates that the Wireless Switch is management ready (that is, it can be manage through ASDP). You are alerted of problem areas. (See *Readiness Test* for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected Wireless Switch. (See *Audit Devices* 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 *Forensic Analysis—Basic* 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 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.
Flagged	Flag a Wireless Switch that you want to bring attention to.
In compliance / Not in compliance	Status of the last compliance audit. Click the **Managed Configuration** button to display the Wireless Switch configuration. Click the **Generated Configuration** 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. Click the **Push Configuration** button to push the existing configuration out to the Wireless Switch.
Observed Data	Data that AirDefense Services Platform observed about the Wireless Switch. You can filter the observed data by entering significant text in the **Search** 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 Profile*
- License—Display valid licenses for Wireless Switch.

These configuration settings are all located in the *Configuration Tab*.

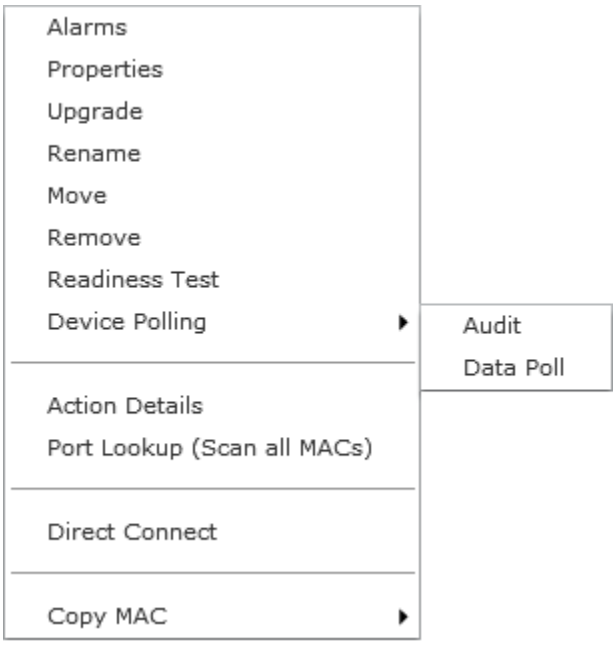
If you make changes, click **Save** to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button–X to close the **Properties** overlay.

Wired Switch—Drop-down Menu

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.



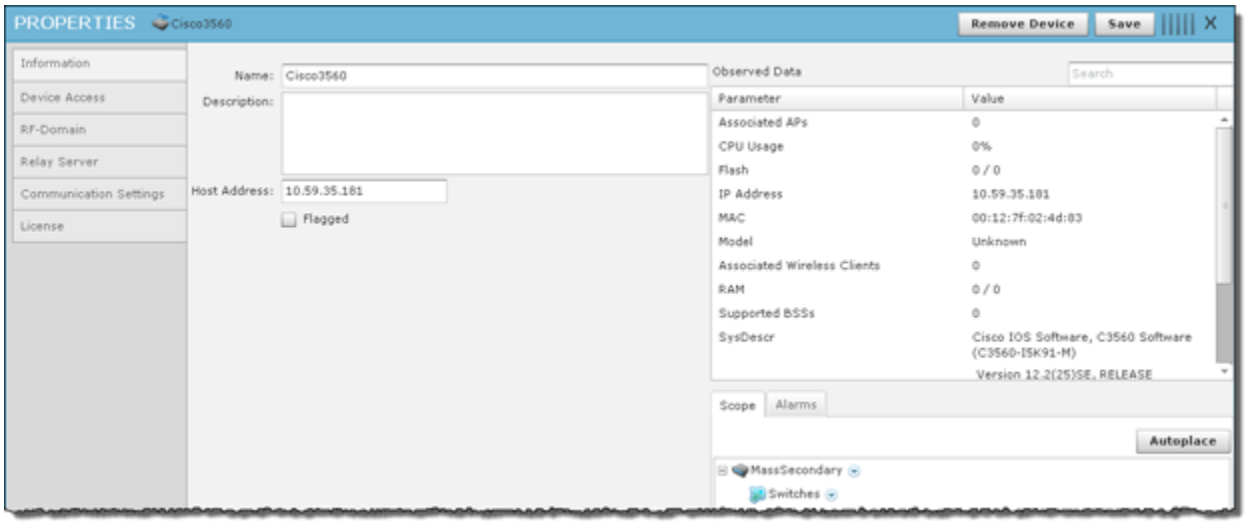
The drop-down menu for Wired Switches contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected Wired Switch.
Properties	Opens the **Properties** overlay for the selected Wired Switch.
Upgrade	Upgrades the firmware for the selected Wired Switch. (For more information, see *Upgrade Devices* in the *Network* chapter.)
Rename	Opens a dialog window to rename the selected Wired Switch.
Move	Moves the selected Wired Switch to another network level (floor). (See *Move Devices* for more information.)
Remove	Removes the selected Wired Switch from your network. (See *Remove Devices* 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 *Readiness Test* for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected Wired Switch. (See *Audit Devices* for more information.)
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.

Function	Description
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 **Search** 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 Profile*
- License—Display valid licenses for Wired Switch.

These configuration settings are all located in the *Configuration Tab*.

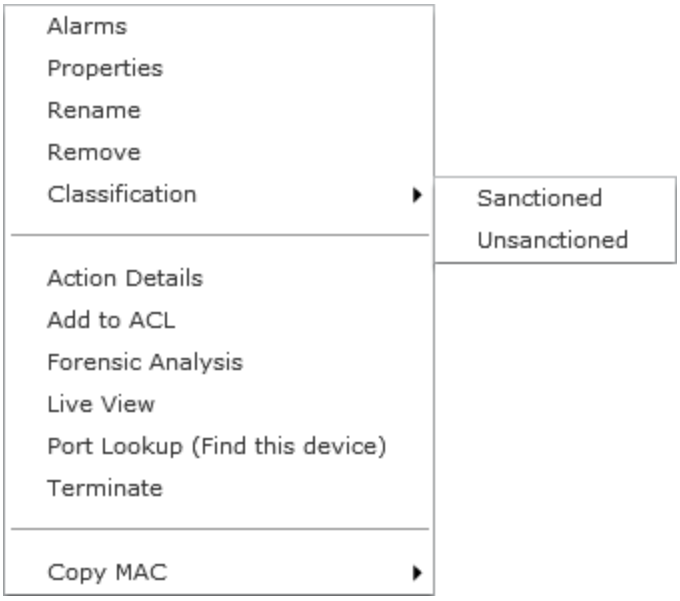
If you make changes, click **Save** to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button–X to close the **Properties** overlay.

Unknown Devices—Drop-down Menu

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.



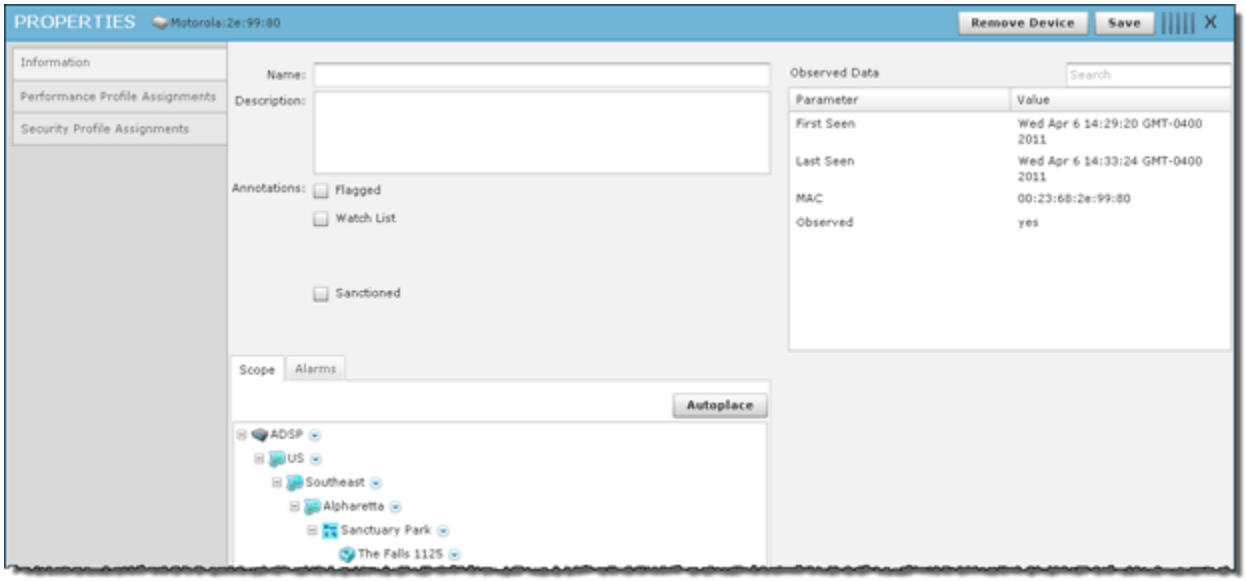
The drop-down menu for unknown devices contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected unknown device.
Properties	Opens the **Properties** overlay for the selected unknown device.
Rename	Opens a dialog window to rename the selected unknown device.
Remove	Removes the selected unknown device from your network. (See *Remove Devices* for more information.)
Classification	Classifies the unknown device as **Sanctioned** or **Unsanctioned**.

Function	Description
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Add to ACL	Adds the selected Unknown Device to the Access Control List (ACL).
Forensic Analysis	Opens the *Forensic Analysis—Basic* window for the specified unknown device.
Live View	Opens the *Live View* window for the selected unknown device; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the *Port Lookup* window where you can locate the physical port where the Unknown Device is accessing your network.
Terminate	Accesses the *Terminate* 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: **Flagged**, **Watch List**, or **Sanctioned**.
Observed Data	Data that AirDefense Services Platform observed about the Unknown Device. You can filter the observed data by entering significant text in the **Search** 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, **Save** 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—Drop-down Menu

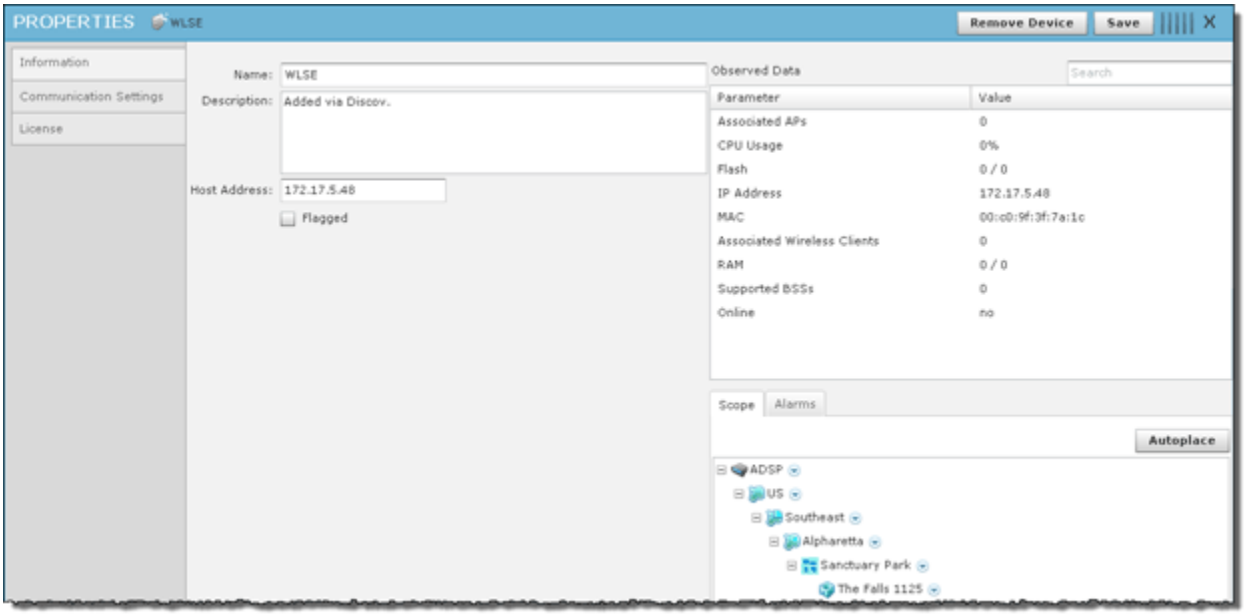
The WLSE drop-down menu contains functions that you can apply to the selected WLSE. Click the drop-down menu button– next to the WLSE name to display the drop-down menu.

The drop-down menu for WLSE devices contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected WLSE device.
Properties	Opens the **Properties** 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 *Move Devices* for more information.)
Remove	Removes the selected WLSE device from your network. (See *Remove Devices* for more information.)
Readiness Test	Validates that the WLSE device is management ready (that is, it can be manage through ASDP). You are alerted of problem areas. (See *Readiness Test* 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 **Search** 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**.

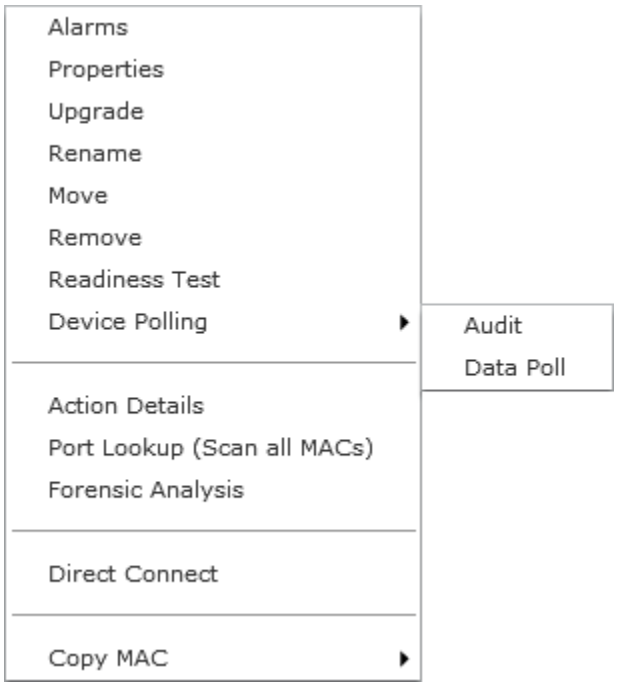
If you make changes, click **Save** to save them.

Click the **Delete Device** button to delete a device from your network.

Click the **Close** button–X to close the **Properties** overlay.

AirWave Switch—Drop-down Menu

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.



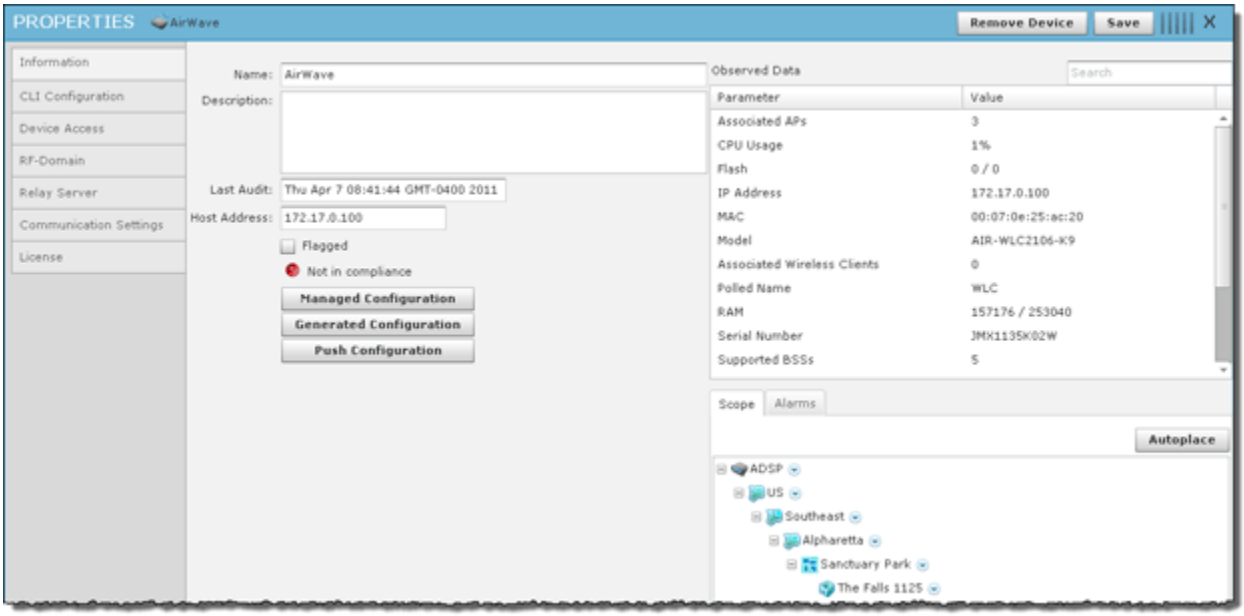
The drop-down menu for AirWave devices contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected AirWave device.
Properties	Opens the **Properties** overlay for the selected AirWave device.
Upgrade	Upgrade the firmware for the selected AirWave switch. (For more information, see *Upgrade Devices* in the *Network* chapter.)
Rename	Opens a dialog window to rename the selected AirWave device.
Move	Moves the selected AirWave device to another network level (floor). (See *Move Devices* for more information.)
Remove	Removes the selected AirWave device from your network. (See *Remove Devices* for more information.)
Readiness Test	Validates that the AirWave device is management ready (that is, it can be manage through ASDP). You are alerted of problem areas. (See *Readiness Test* for more information.)
Device Polling	Conduct a compliance audit on the selected AirWave switch. (See *Audit Devices* for more information.)
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.

Function	Description
Port Lookup (Scan all MACs)	Scan MAC addresses to view a list of switch ports.
Forensic Analysis	Opens the *Forensic Analysis—Basic* 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.

Field	Description
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 **Managed Configuration** button to display the AirWave Switch configuration. Click the **Generated Configuration** 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 **Push Configuration** 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 **Search** 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 Profile*
- License—Display valid licenses for AirWave switch.

These configuration settings are all located in the *Configuration Tab*.

If you make changes, click **Save** 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

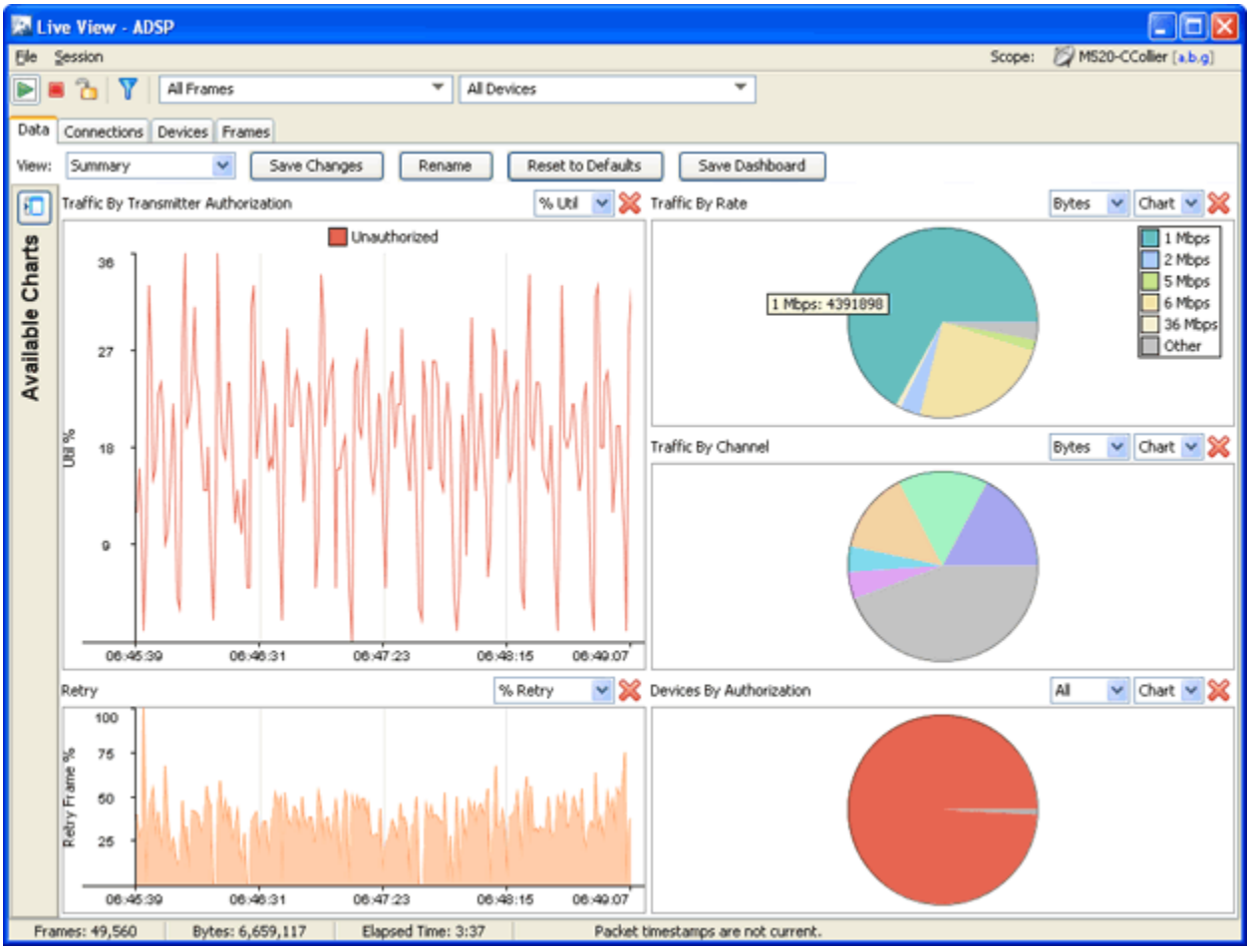
The device functions discussed here are drop-down menu functions that operate on devices and require more details on how to use them. Depending on the device, these functions may or may not appear in the drop-down menu. They are:

- Live View
- Locate
- Port Lookup
- Readiness Test
- Spectrum Analysis

- Terminate.

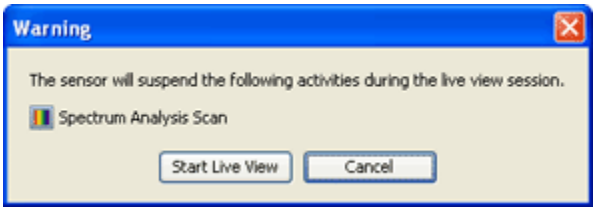
Live View

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.

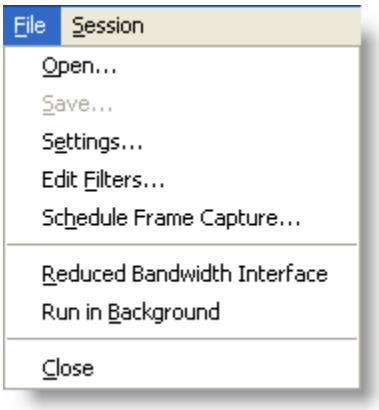
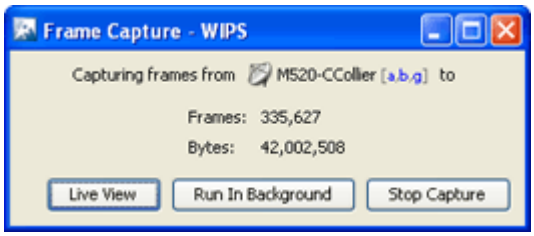
Live View consists of four main categories of information:

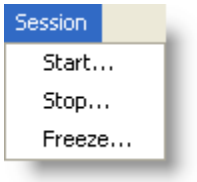
- Data
- Connections
- Devices
- Frames.

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.

Menus

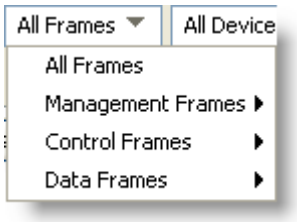
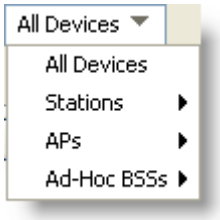
Menu	Option	Description
File 	Open	Opens a captured frame file for viewing. (See *Frame Capture Analysis* for more information.)
	Save	Opens the **Save Frame Capture** popup window where you can save the temporary capture file to a permanent file on the server or to a file on your workstation. (See *Frame Capture* for more information.)
	Settings	Opens the **Live View Settings** popup window where you can set options for your Live View sessions. (See *Live View Settings* for more information.)
	Edit Filters	Opens the Live View Filter popup window where you can set options to filter data. (See *Live View Filters* for more information.)
	Schedule Frame Capture	Schedule a Frame Capture session using the scheduler. (See Schedule Frame Capture for more information.
	Reduced Bandwidth Interface	Shrinks the **Frame Capture** window and conserves bandwidth while running Live View.  While in the reduced bandwidth state, you can: • Return to the original **Live View** window by clicking Live View. • Run live view in the background by clicking **Run in Background**. • Stop capturing Live View frames and exit Live View by clicking **Stop Capture**.
	Run in Background	Exits **Live View** window and runs Live View in the background.
	Close	Exits the Live View session and closes the **Live View** window.

Menu	Option	Description
Session 	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 **Freeze** button again to unfreeze the session.
	Opens the **Live View Filter** popup window. where you can set options to filter data. (See *Live View Filters* 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 **All Frames**.
	Acts as a quick filter to display only frames for the selected device. To view all devices, select **All Devices**.

Live View Settings

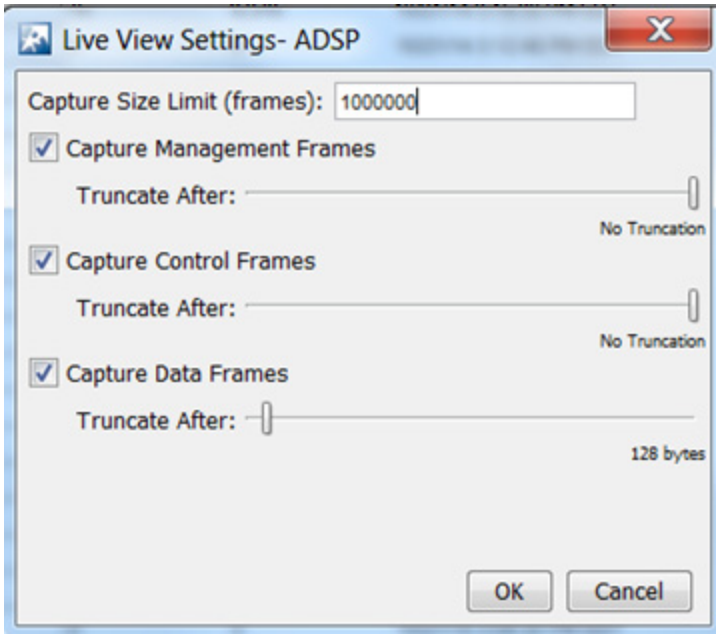
Live View has four user adjustable settings. They are:

Setting	Description
Capture Size Limit	Sets the maximum amount of frames that can be captured during any one session.

Setting	Description
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.

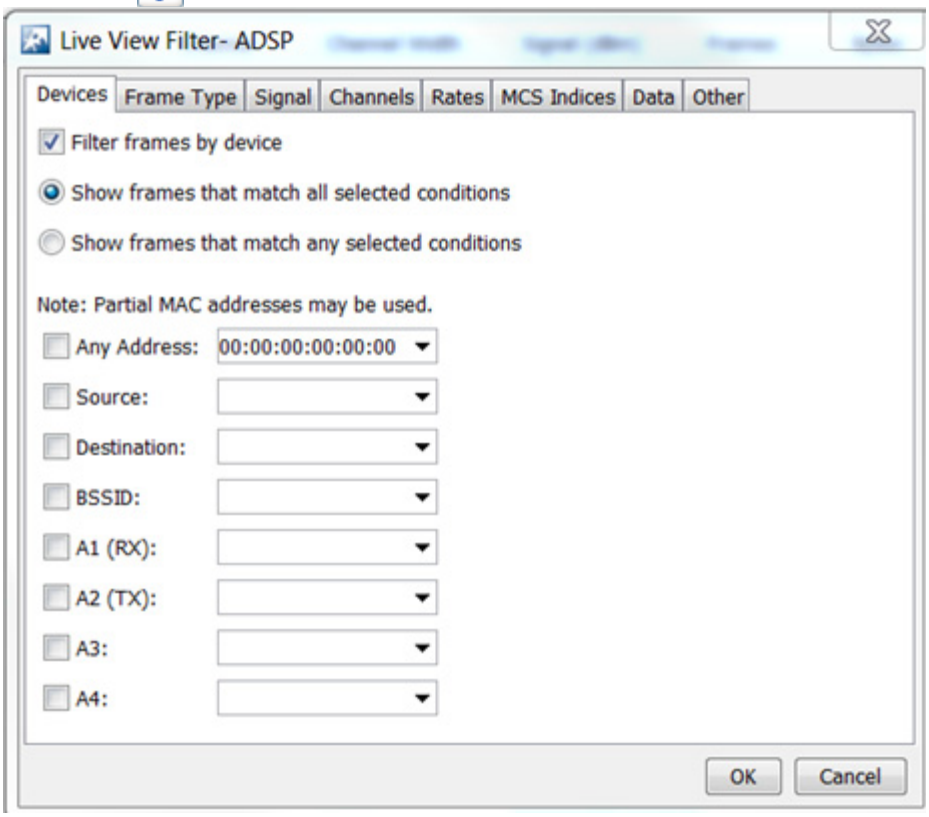


2 Make your adjustments.

3 Click **OK**.

Live View Filters

You can limit what you see in Live View through the use of filters. Select **File** > **Edit Filters** or click the **Filter–** button to display the **Live View Filter** popup window.



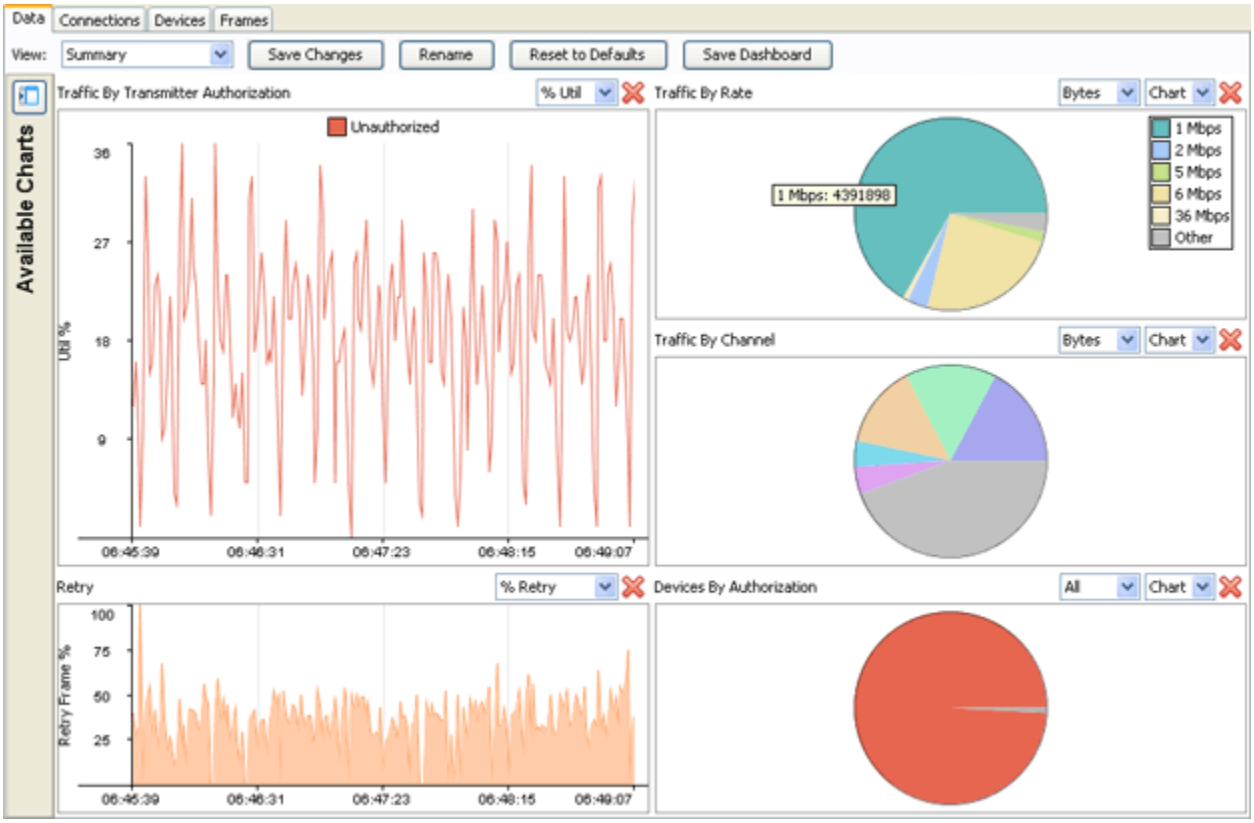
Frames may be filtered by any of the following methods:

Method	Description
Devices	To filter Live View frames by devices, go to the **Devices** tab and check **Filter frames by device**. Select any of the following conditions: • Any Address • Source • Destination • BSSID • A1 (RX) • A2 (TX) • A3 • A4 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.
Frame Type	To filter by frame types, go to the **Frame Type** tab and check **Filter frames by frame type**. Then deselect 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.
Signal Filters	To filter by signal strength, go to the **Signal** tab and check **Filter frames by signal strength**. Enter the minimum signal strength in dBm and the maximum signal strength in dBm. Live View will display only the signals within the specified range.
Channel Filters	To filter by channels, go to the **Channels** tab and check **Filter frames by channel**. Deselect the channels that you do not want to display. You may filter out a whole category of channels or individual channels.
Rates Filters	To filter by transmission rate, go to the **Rates** tab and check **Filter frames by rate**. Deselect any rate that you do not want to display.
MCS Indices	To filter by MCS Indices, go to the MCS Indices tab and check **Filter frames by MCS Index**. Deselect any index that you do not want to display.
Data Filters	To filter by data type, go to the **Data** tab and check **Filter frames by data**. Deselect any of the encryption types that you do not want to display and deselect any of the ether types that you do not want to display.
Other	To filter by other, go to the **Other** tab and check **Filter frames by other**. Enter the Mac address of the sensor you wish to filter by.

When you have set your filter criteria, click **OK** to save.

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.

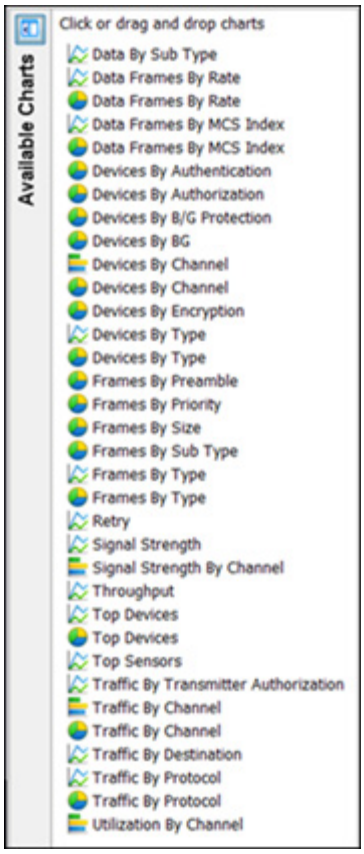


The Data tab focus can be changed by changing the view. Depending on the view that is selected different charts are displayed. There are four available views:

View	Description
Summary	Provides a summary of frame data using the following charts: • Traffic By Transmitter Authorization • Retry • Traffic By Rate • Traffic By Channel • Devices By Authorization. This is the default view.
Device Analysis	Changes the frame data focus to device information. Charts relating to device information are displayed.
Channel Analysis 2.4 Ghz (b/g/n)	Changes the frame data focus to channel information for 802.11b/g/n network traffic. Charts relating to channel information are displayed.
Channel Analysis 5 Ghz (a/n)	Changes the frame data focus to channel information for 802.11a/n 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.

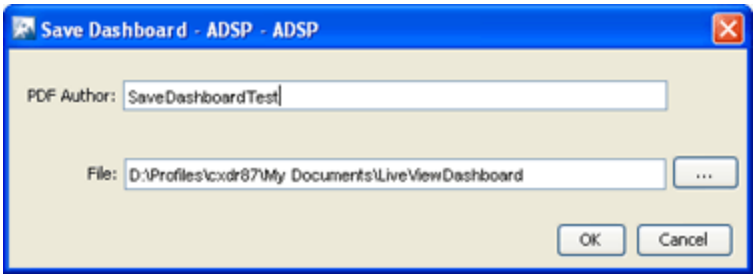
To remove a chart, click the **Remove**– button associated with the chart.

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.

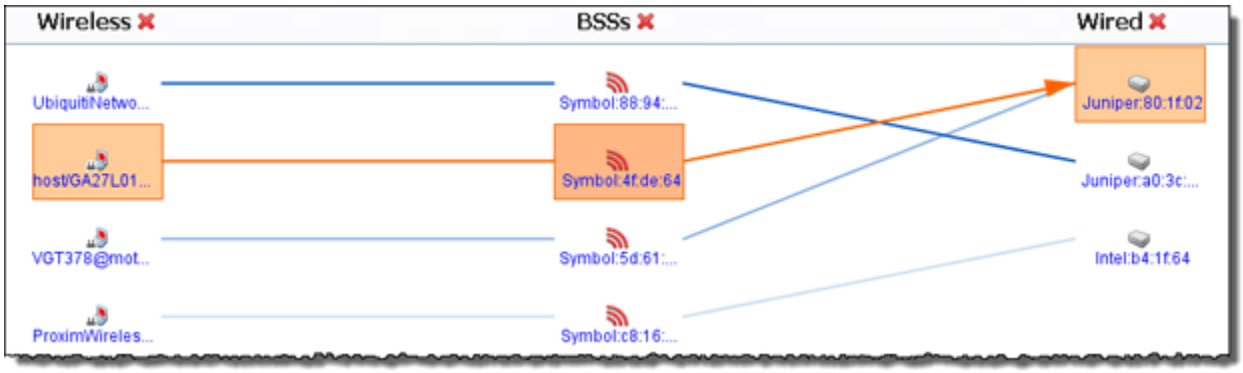
Devices are listed in three columns: Wireless (wireless devices), APs and Wired (wired devices). Device columns may be disabled or re-enabled by using the hide ( )/show ( ) button next to the

column name. For example, if the APs 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.

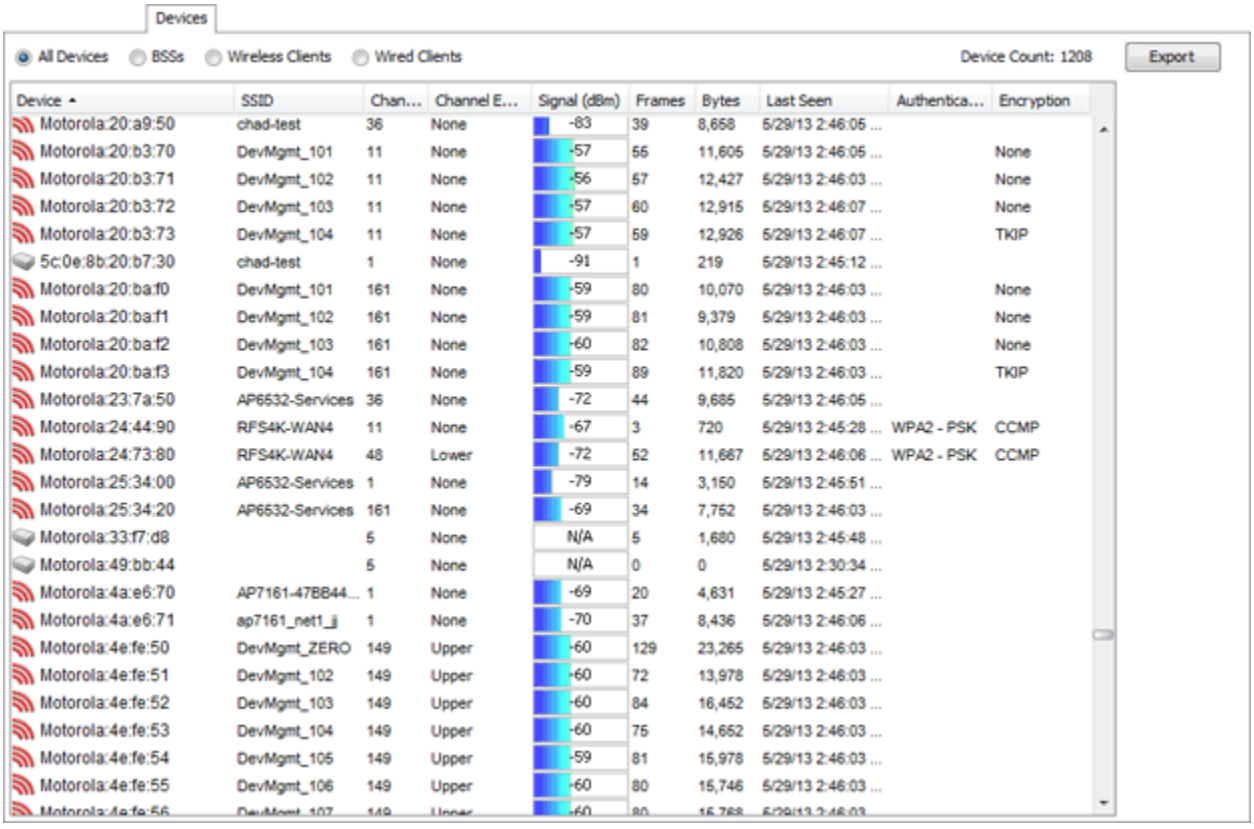


If you continue clicking on the device, the graph will cycle through the connections involving the selected device. Buttons are also provided to cycle through the connections.

The **Data Frames** and **Bytes** fields will only show the data corresponding to the selected connection.

Devices Tab

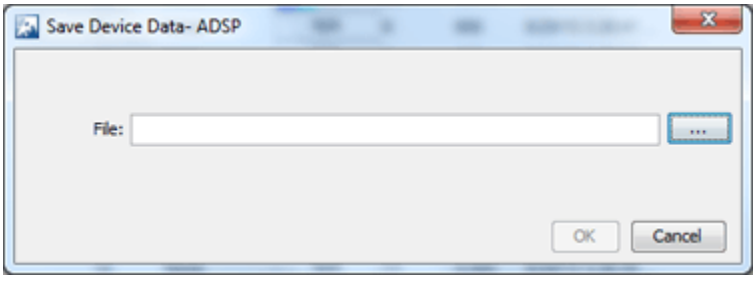
The **Devices** tab displays the devices that have been seen during a Live Monitoring session in tabular format.



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-Services	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-Services	1	None	-79	14	3,150	5/29/13 2:45:51 ...		
Motorola:25:34:20	AP6532-Services	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_ji	1	None	-70	37	8,436	5/29/13 2:46:06 ...		
Motorola:4e:fe:50	DevMgmt_ZERO	149	Upper	-60	129	23,265	5/29/13 2:46:03 ...		
Motorola:4e:fe:51	DevMgmt_102	149	Upper	-60	72	13,978	5/29/13 2:46:03 ...		
Motorola:4e:fe:52	DevMgmt_103	149	Upper	-60	84	16,452	5/29/13 2:46:03 ...		
Motorola:4e:fe:53	DevMgmt_104	149	Upper	-60	75	14,652	5/29/13 2:46:03 ...		
Motorola:4e:fe:54	DevMgmt_105	149	Upper	-59	81	15,978	5/29/13 2:46:03 ...		
Motorola:4e:fe:55	DevMgmt_106	149	Upper	-60	80	15,746	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.



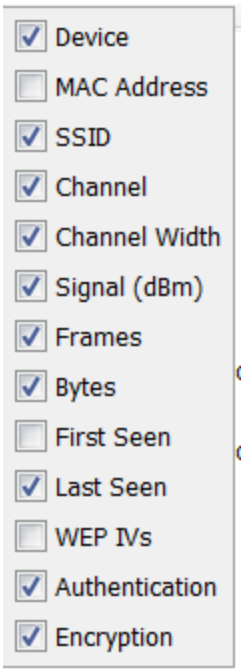
Just browse to a folder (directory) to save the file in, type in a name, and click the **Select** button. The name of the file is displayed in the **File** field. Now, click **OK** to save the file in the selected folder (directory).

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. An SSID is a 32-character unique identifier attached to the header of packets sent over a WLAN. The SSID acts as a password when a mobile device tries to connect to the BSS (Basic Service Set.)
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:

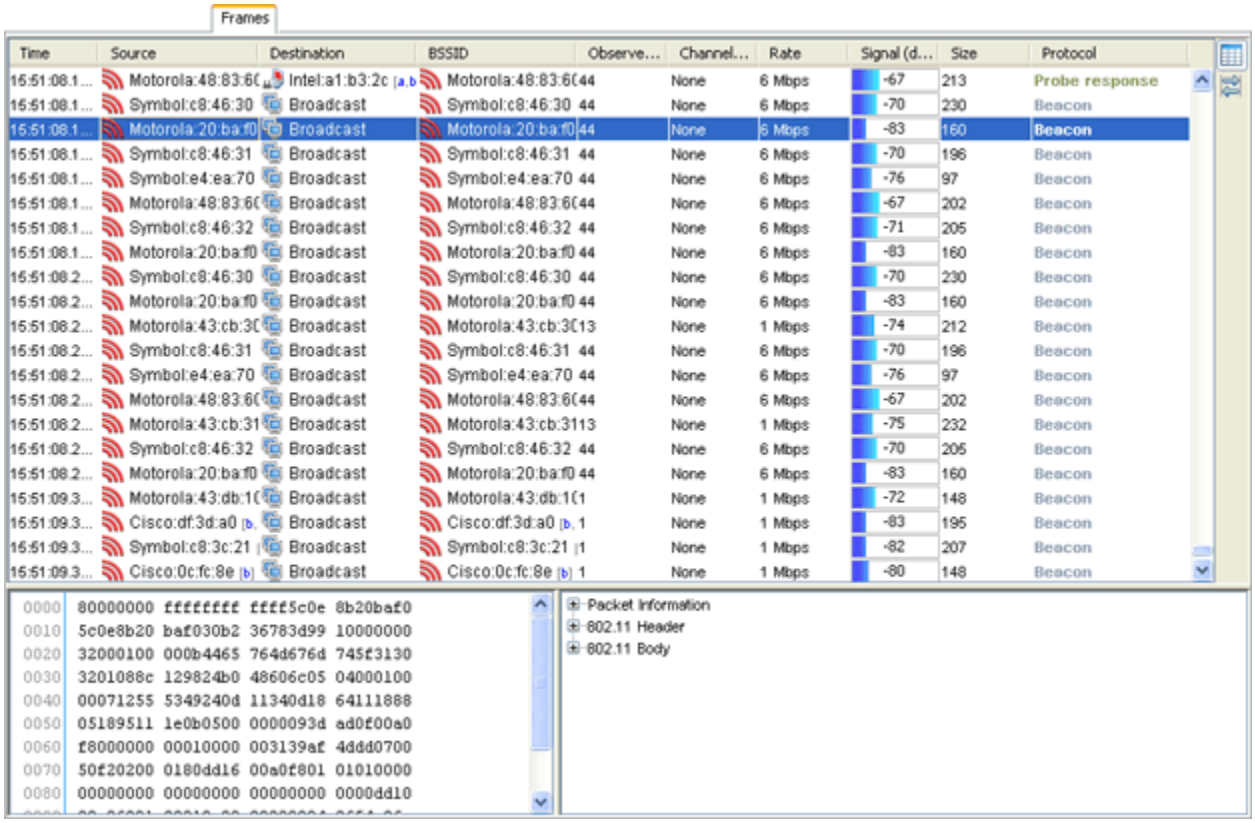
You can hide or unhide a category by right-clicking in the column heading area, and uncheck or checking the checkbox for a category (see below).



You can rearrange columns by clicking on a column heading and dragging it to a new position.

Frames Tab

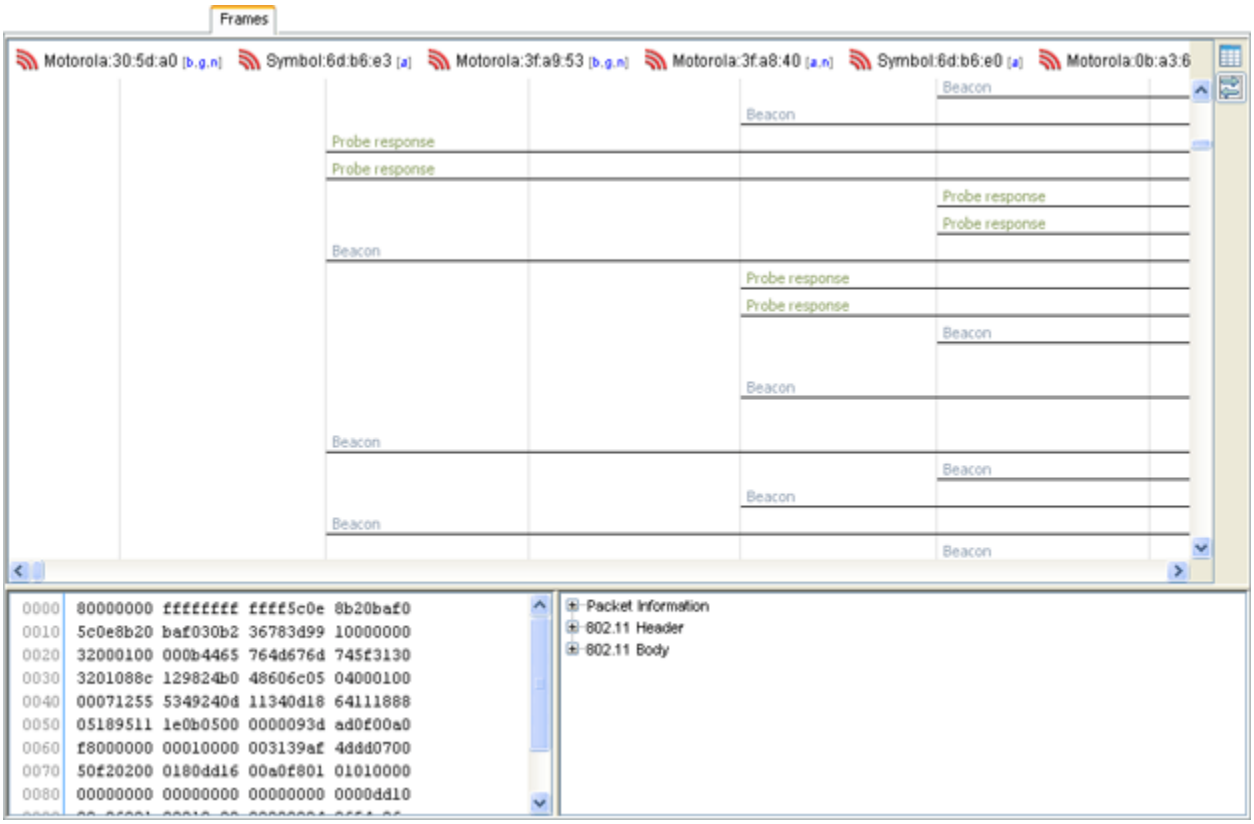
The **Frames** tab displays the frames that were captured during a Live Monitoring session.



The captured file is stored in either—or, at times, both—of the following directories:

/usr/local/smx/pcaptiures 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).

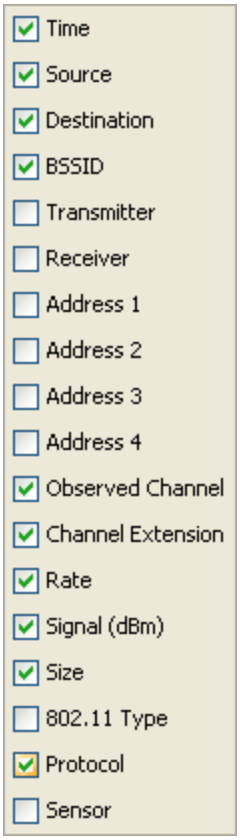
Table View

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.
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 unhide 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.

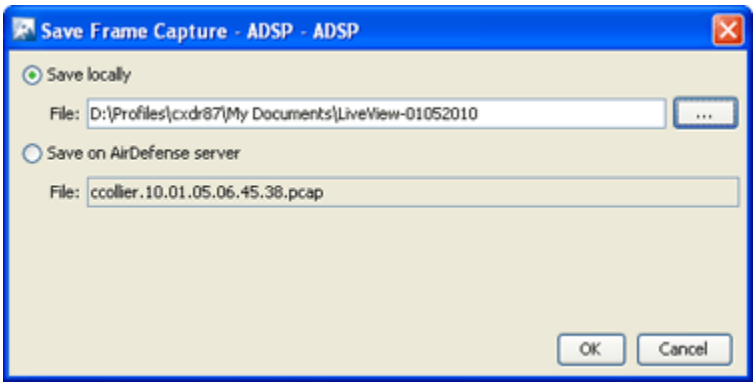
The decodes area shows the 802.11 interpretation of the frame data in a tree structure. The hex values area and decodes area are linked so that selections in one area will follow the selections in the other.

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.

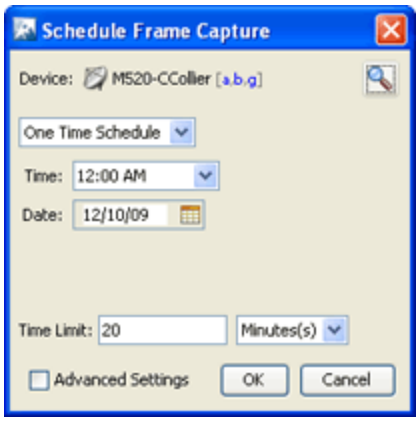
   NOTE The file name is selected automatically. You cannot change it.

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.



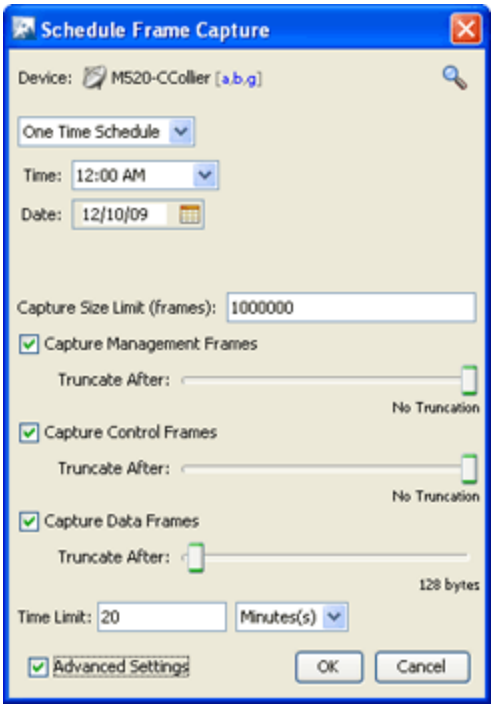
To schedule automatic frame captures, follow these steps:

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 **Time** drop-down menu. Then, select a day for the frame capture by clicking the **Calendar** button in the **Date** 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 slide-bar 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.

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 of the device as seen by at least three sensors to triangulate a position relative to the sensor locations. To use this feature, you must first import a building map and place at least three sensors on their corresponding location.

Things to Remember

- Location Tracking is not intended to be used on devices that are being terminated.
- In order to locate a device, a floor plan must already exist. (See Floor Plan.)

- 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.

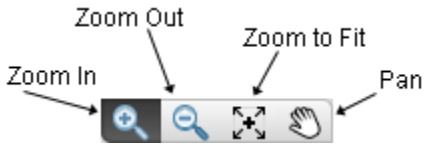
NOTE A map can only be linked to sensors on the same floor. In a multi floor building, sensors should be grouped by floors and each floor associated with its own map. At least 3 sensors per floor plan are required for location triangulation.

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

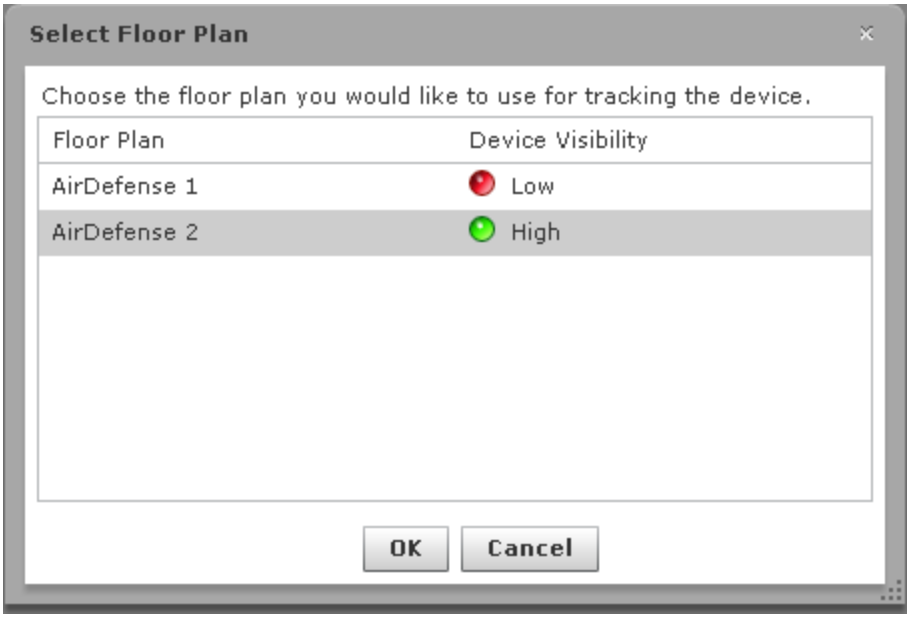
Select an empty floor and then click the **Design Floorplan** link to import a map. This will open a sub-window and you can upload the appropriate map, which can be in .gif, .jpg, or .bmp files. Select the desired floor plan and select **Open**. The map is then displayed. Scale the image as directed 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.

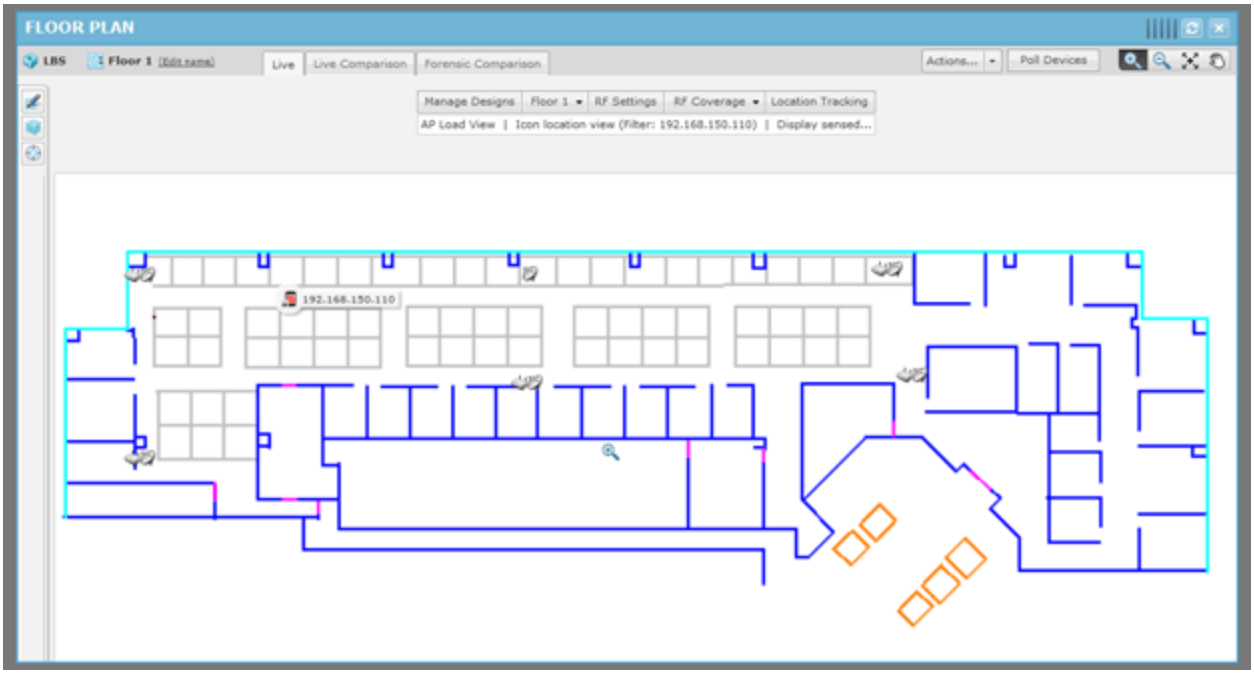
One or more maps or floor plans of the tracking coverage area are needed for this to work. You can obtain floor plans from any source, including producing your own by using drawing tools. Most applications will require multiple maps, for example, if you are setting up multiple buildings. You must supply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

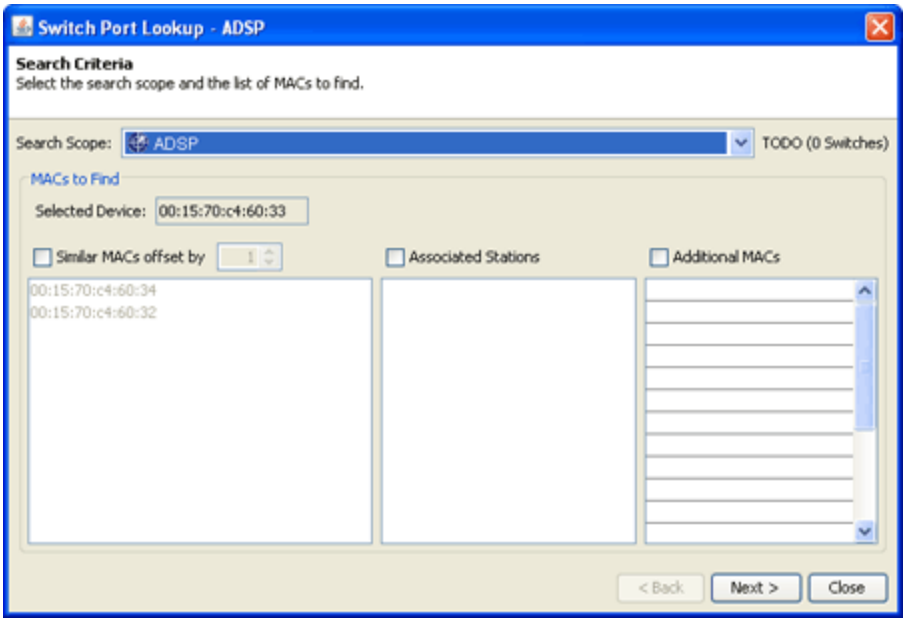
You can place your cursor over the tracked device to display statistics and information about the device.

Port Lookup

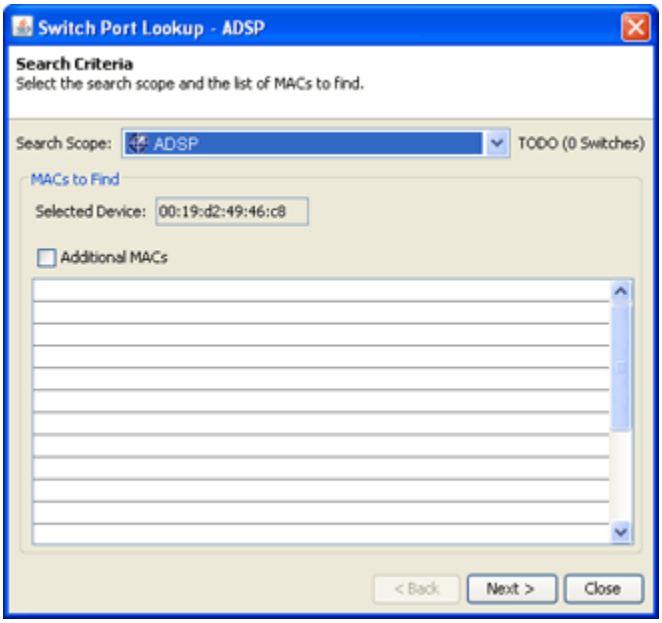
Port Lookup allows you to quickly locate the physical port that an authorized/unauthorized device is using to connect to your network. If it is determined that a rogue wireless device is connected to the network, the wired-side port can be shut off to contain the rogue device threat.

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.

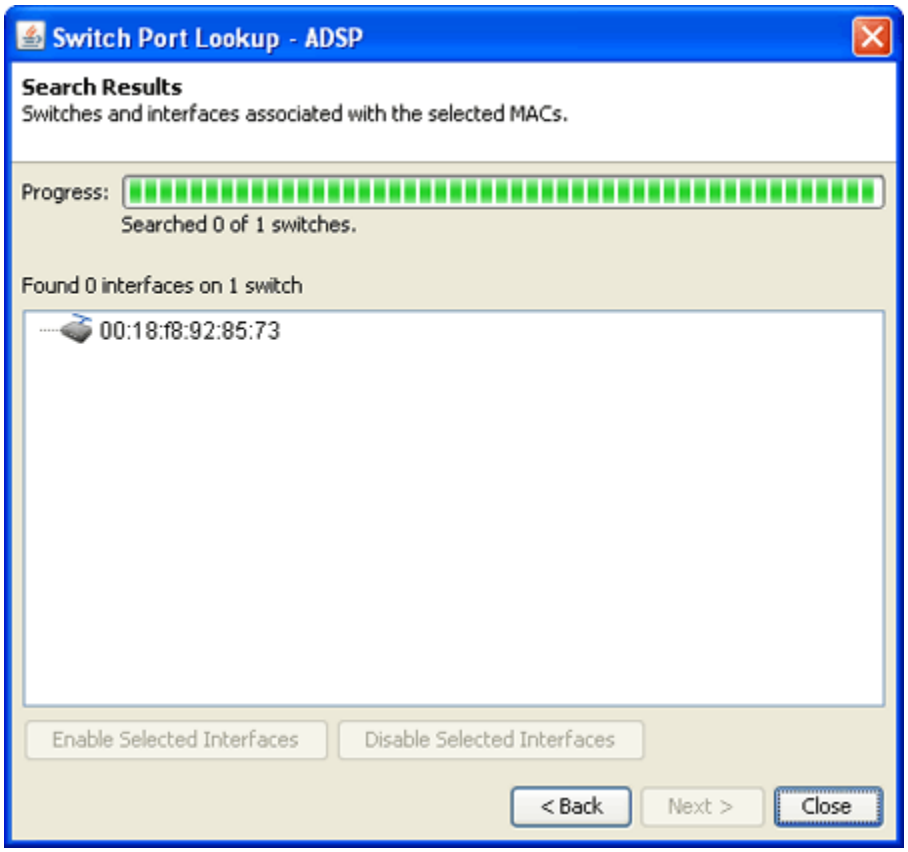
Function/Feature	Description
Search Scope	A drop-down menu that allows you to limit the scope of your search.
Selected Device	A read-only field that displays the MAC address of the selected device.

Function/Feature	Description
Similar MACs offset by	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. 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. The default offset value is 1.
Associated Wireless Clients	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.
Additional MACs	If checked, the search includes any additional MAC addresses that you specify.

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.



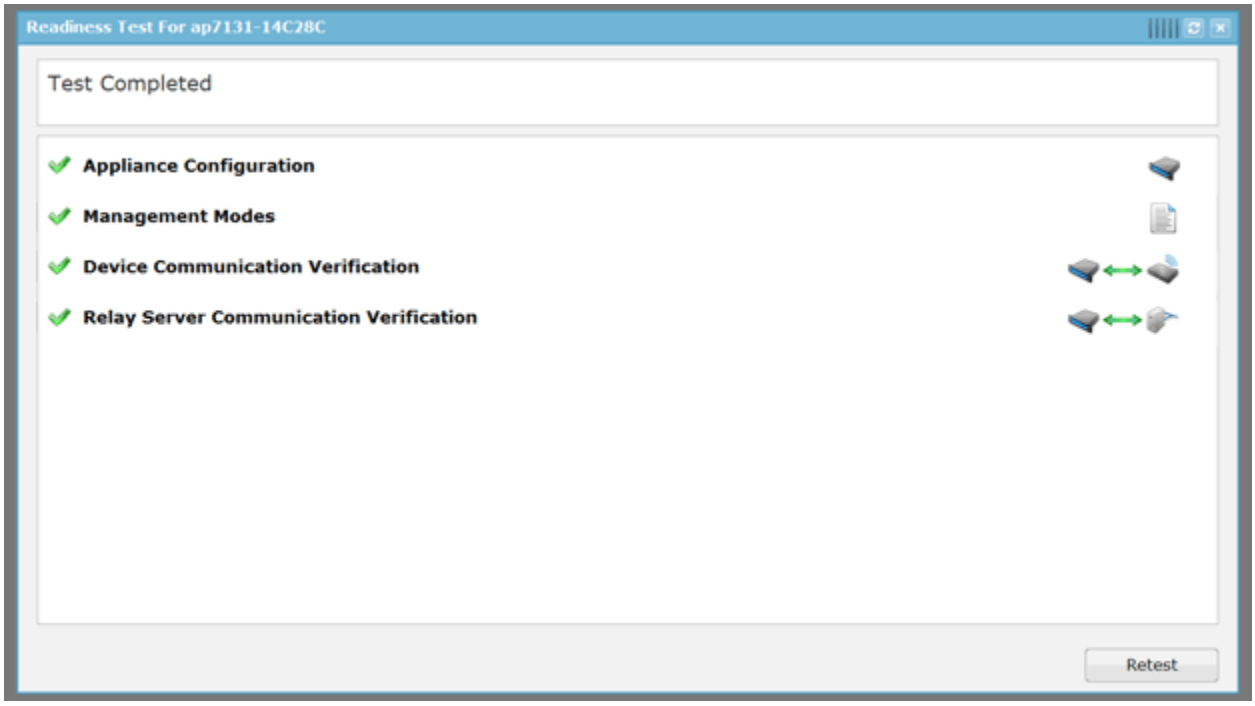
From this window, you can disable or enable a selected (highlighted) interface by clicking the appropriate button.

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 , 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: Appliance Configuration, Management Modes, Device Communication Verification, and Relay Server Communication Verification. 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 have a valid Spectrum Analysis license 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.

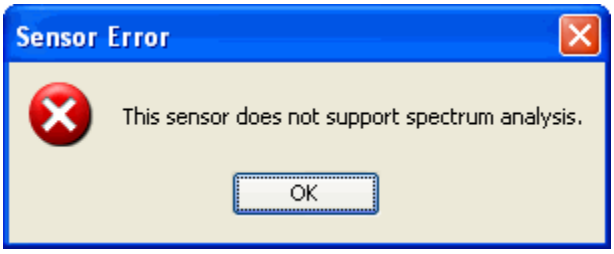
There are two ways to turn on background analysis:

- 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.

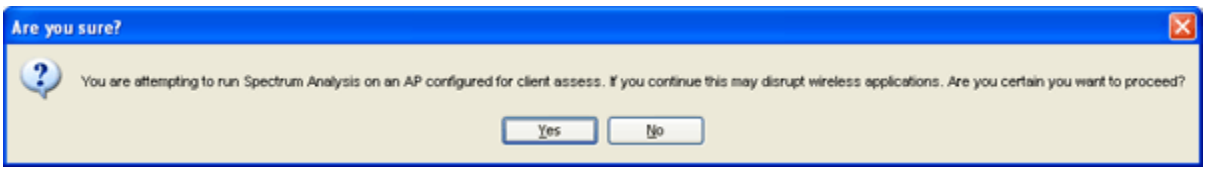
Dedicated Analysis

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:

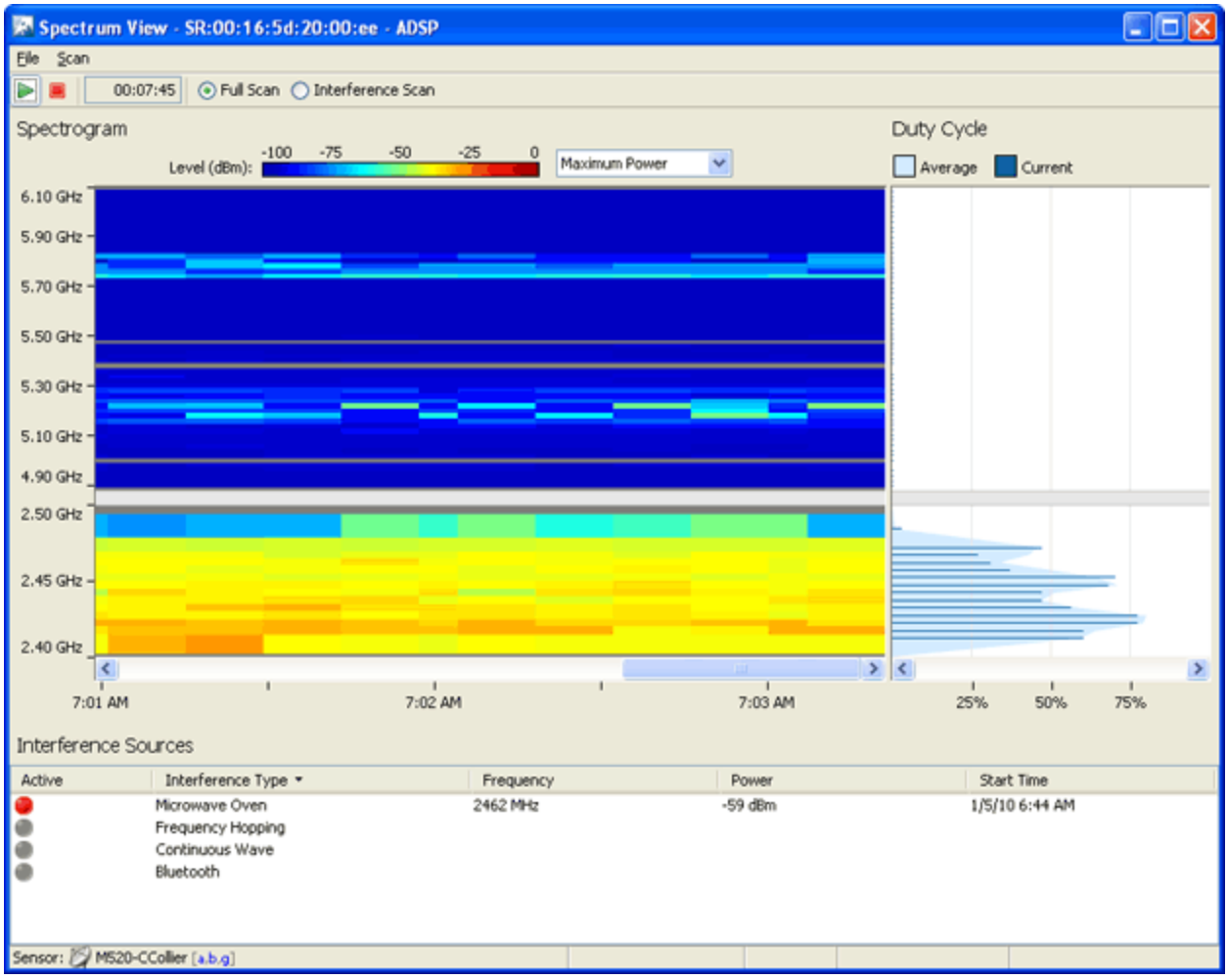


In addition, if you attempt to run Spectrum Analysis on an AP configured for client access (device configured as AP and Sensor), the following error popup may display:



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.

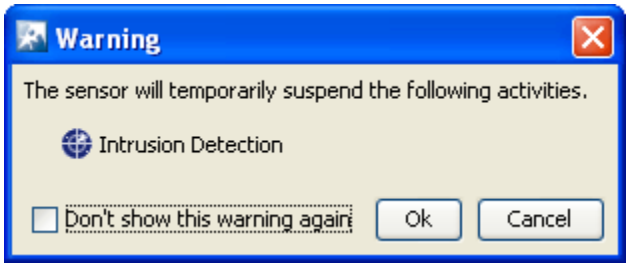
To access the **Spectrum View** window, click the drop-down menu button– for a Sensor and then select **Spectrum Analysis** from the drop-down menu.



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 temporary 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**.

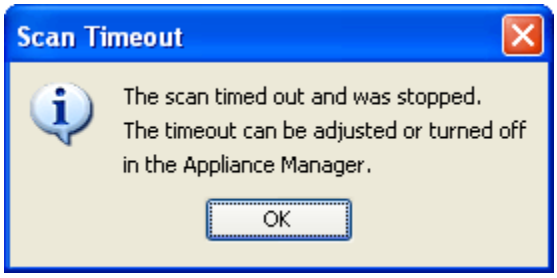
There are three conditions that may prevent a scan from starting. They are:

- 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.

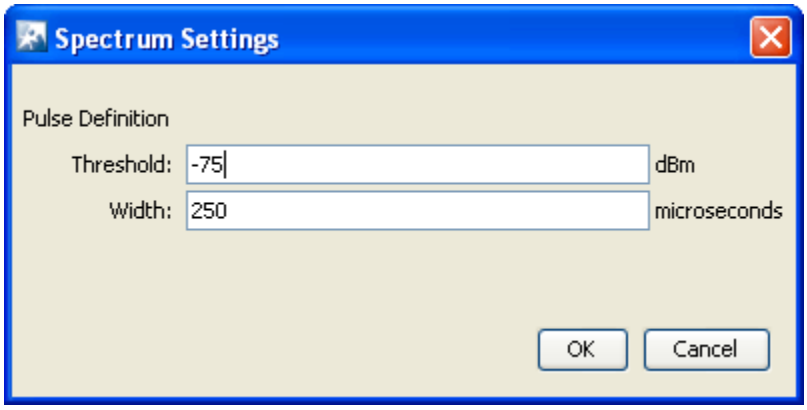
The default scanning time is 10 minutes. Scanning time can be adjusted by selecting **Configuration** > **Appliance Management** > **Appliance Settings**. If a timeout occurs, the following **Scan Timeout** popup is displayed:



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.

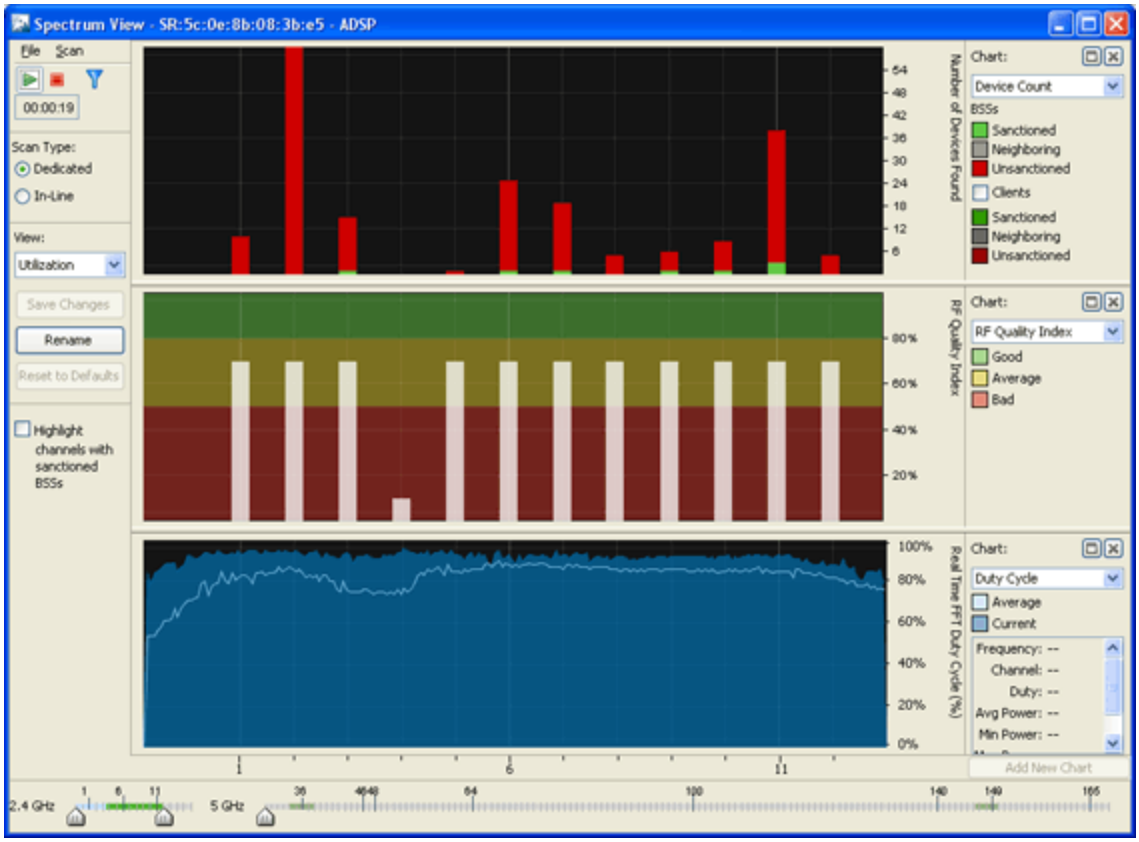
Advanced Spectrum Analysis

NOTE A Spectrum Analysis license is required to access this feature.

Advanced Spectrum Analysis is the next generation of Spectrum Analysis. Advanced Spectrum Analysis will only run on devices with the MB92 or newer chipsets. Currently, only the models 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).

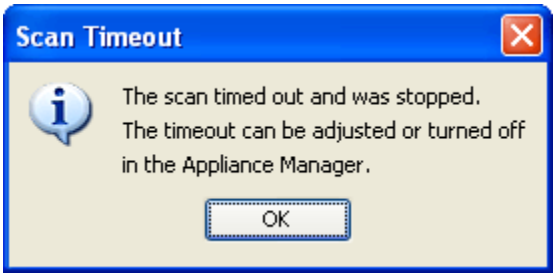
If one of these conditions exists, a warning similar to this is displayed:

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 click 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**.

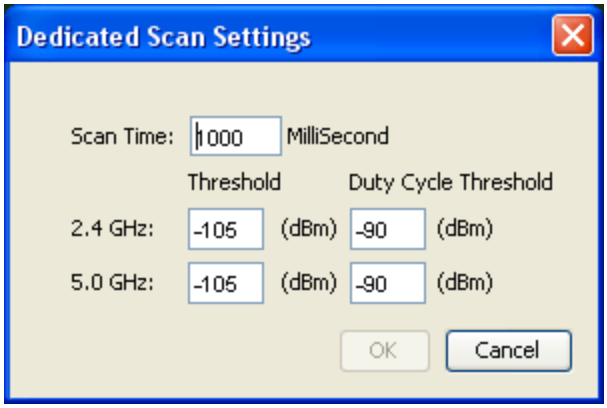
A counter is displayed next to the **Stop Scan** button to show how long the scan has been running.

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.

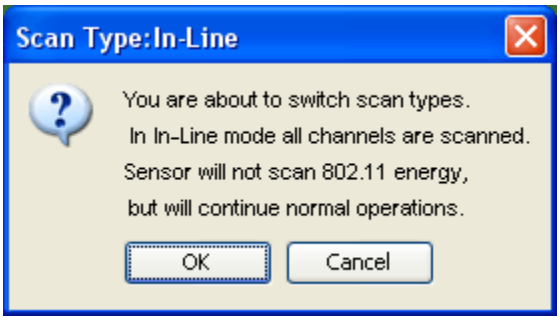
Scan Type

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 sanction BSSs in all the charts.

Chart Manipulation

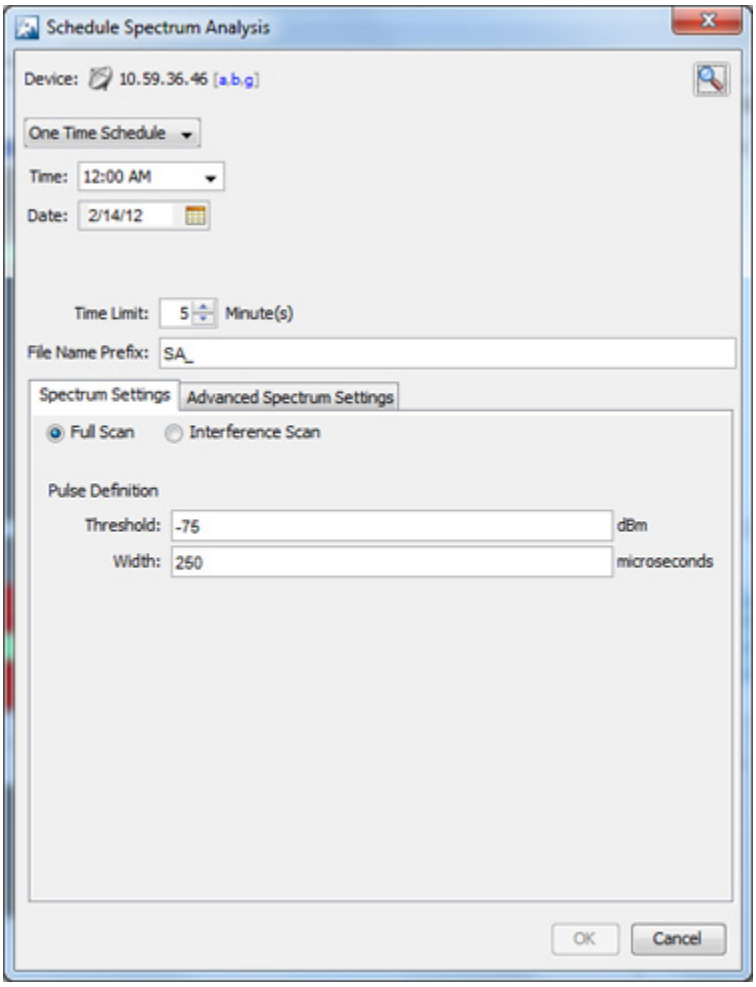
The following chart manipulations are available:

- 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

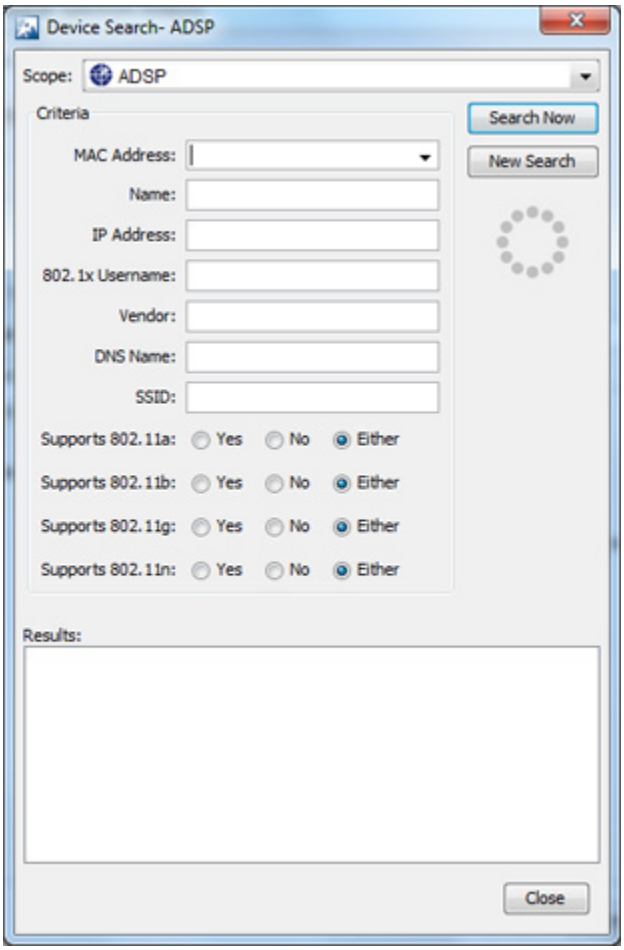
You can schedule Spectrum Analysis for regular Spectrum Analysis or Advanced Spectrum Analysis by selecting **File** > **Schedule Spectrum Analysis**.



The fields used to schedule a Spectrum Analysis are:

Field	Description
Schedule	There are five options to schedule an assessment. Depending on the option you select, you must fill in the related fields as follows: • One Time Schedule—Choose a time for the assessment by selecting a time from the **Time** drop-down menu. Then, select a day for the assessment by clicking the Calendar button in the Date field and selecting a date. • Intra-Day Schedule—Select a time to begin the assessment. 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 assessment 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 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.
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 **Menu** > **Open** > **Spectrum Analysis**.
Spectrum Settings	Only used in regular Spectrum Analysis. These are the same **Spectrum Settings** described under *Dedicated Analysis*.
Advanced Spectrum Settings	Only used in Advanced Spectrum Analysis. These are the **Dedicated Scan Settings** described under *Advanced Spectrum Analysis*.

You can switch devices by clicking **Search** button.



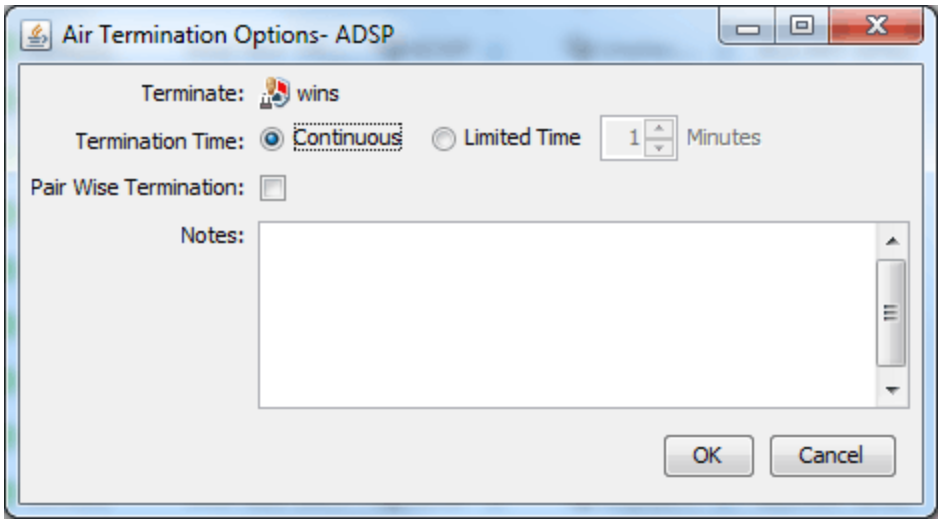
When searching, you can supply additional information such as:

- 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.



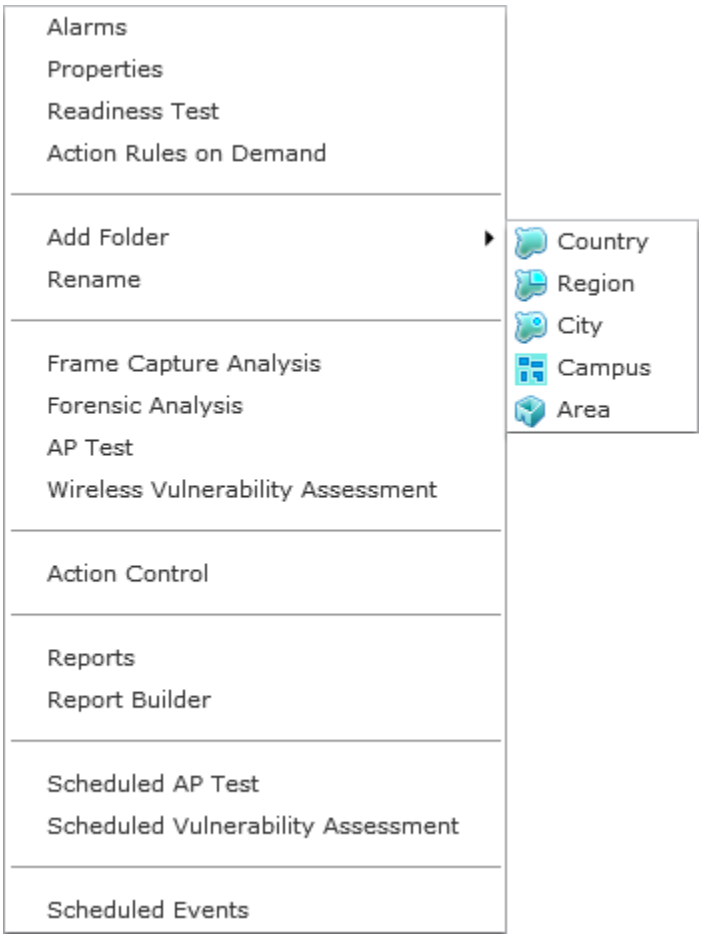
Network Level Drop-down Menus

Each network level has a drop-down menu containing functions that operate on the selected network level. You can configure the following network levels:

- Appliance
- Country
- Region
- City
- Campus
- Building
- Floor.

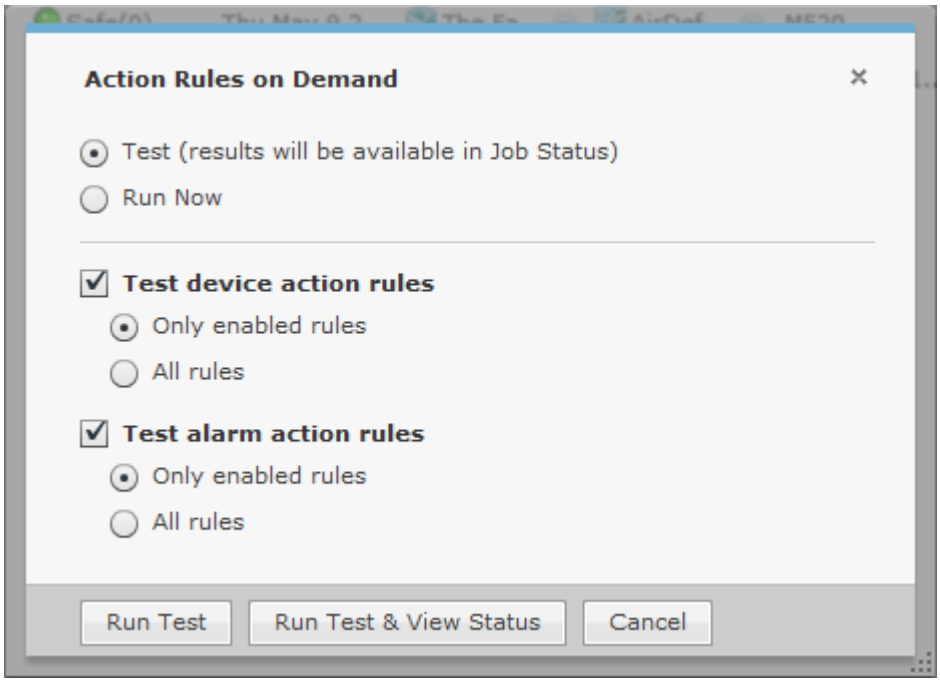
Appliance Level Drop-down Menu

The Appliance level drop-down menu contains functions that you can apply to the selected Appliance as well as the 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:

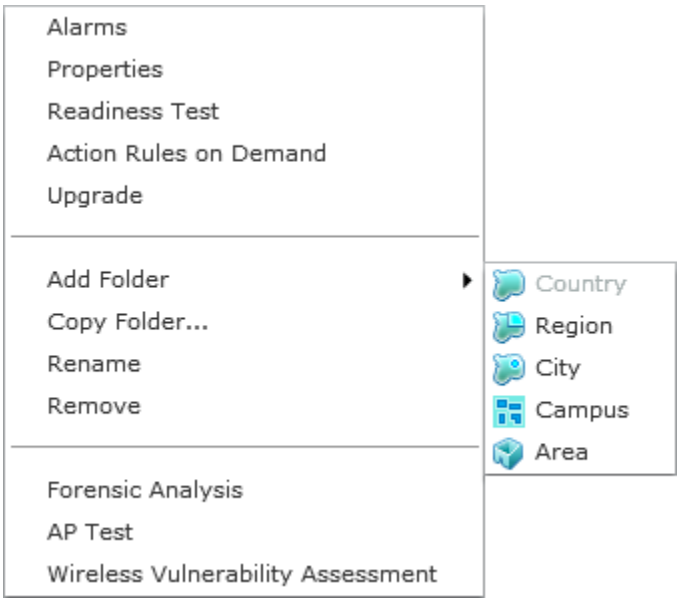
Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected Appliance.
Properties	Opens the **Properties** overlay for the selected Appliance.
Readiness Test	Validates that devices in the appliance scope are management ready (that is, devices can be manage through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

Function	Description
Action Rules on Demand	Runs an on demand test on your alarm action rules and/or device action rules.  You can run the test and view the results later in *Job Status*, or you can run the test now and view the results now. There are two options for each type of test: • Only enabled rules—run test on the enabled rules. • All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Rename	Opens a dialog window to rename the selected Appliance.
Frame Capture Analysis	Accesses *Frame Capture Analysis*.
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
AP Test	Accesses *Scheduled AP Tests*.
Wireless Vulnerability Assessment	Accesses *Scheduled Vulnerability Assessment*.
Action Control	Accesses *Advanced vs. Basic Forensic Analysis*.
Reports	Accesses Reports (*Web Reporting Interface*).
Report Builder	Accesses the Report Builder (*Report Builder*).

Function	Description
Scheduled AP Test	Accesses *Scheduled AP Tests*.
Scheduled Vulnerability Assessment	Accesses *Scheduled Vulnerability Assessment*.
Scheduled Events	Accesses *Scheduled Events*.

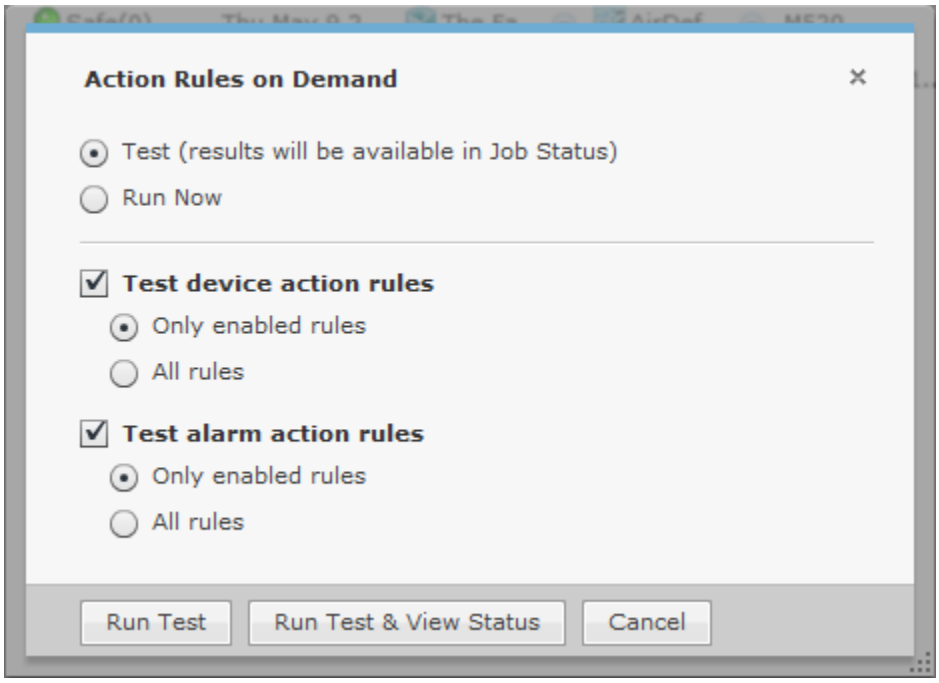
Country Level Drop-down Menu

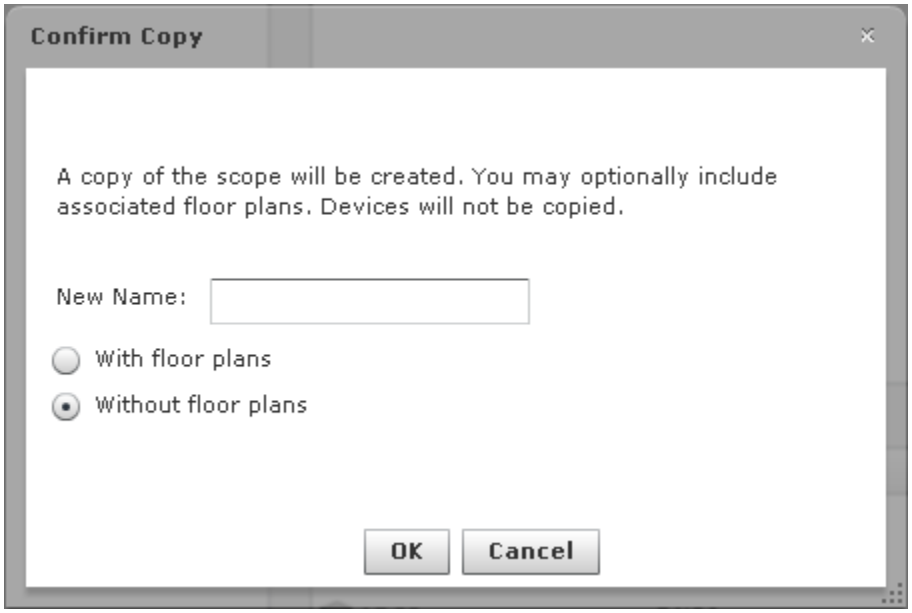
The Country level drop-down menu contains functions that you can apply to the selected Country level. Click the drop-down menu button– next to the Country name to display the drop-down menu.



The drop-down menu for countries contains the following functions:

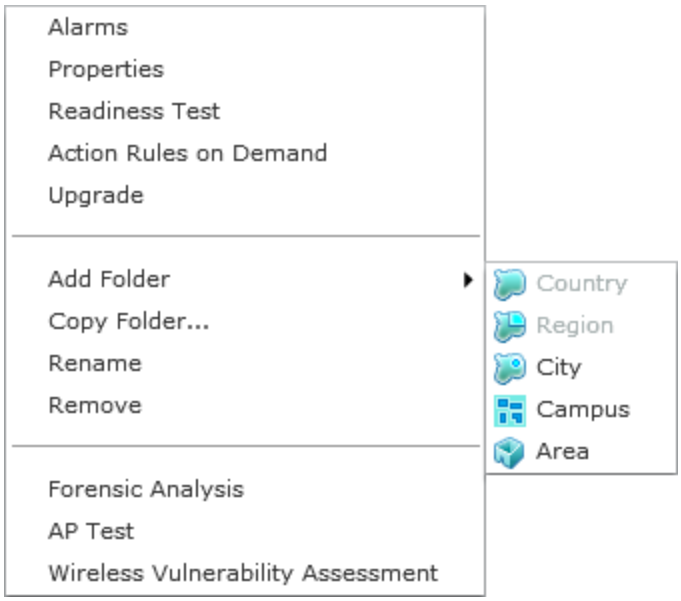
Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected Country.
Properties	Opens the Properties overlay for the selected Country.
Readiness Test	Validates that devices in the country scope are management ready (that is, devices can be manage through ASDP).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

Function	Description
Action Rules on Demand	Runs an on demand test on your alarm action rules and/or device action rules.  You can run the test and view the results later in *Job Status*, or you can run the test now and view the results now. There are two options for each type of test: • Only enabled rules—run test on the enabled rules. • All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.
Upgrade	Upgrades the firmware for devices in the selected Country. (For more information, see *Upgrade Devices* in the *Network* chapter.)
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	Copies the network scope of a Country.  Enter a name for the country, select if you want the to include the floor plans or not, and click **OK**.
Rename	Opens a dialog window to rename the selected Country.
Remove	Removes the selected Country from your network. (For more information, see *Remove Devices* in the *Network* chapter.)
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
AP Test	Accesses AP Test. (*Scheduled AP Tests*)
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment. (*Scheduled Vulnerability Assessment*)

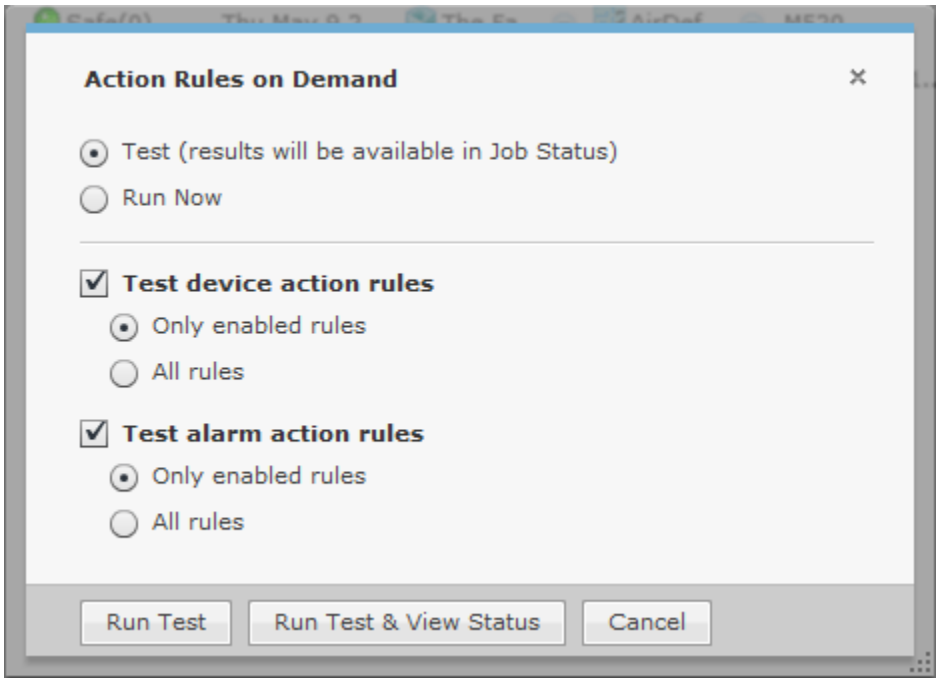
Region Level Drop-down Menu

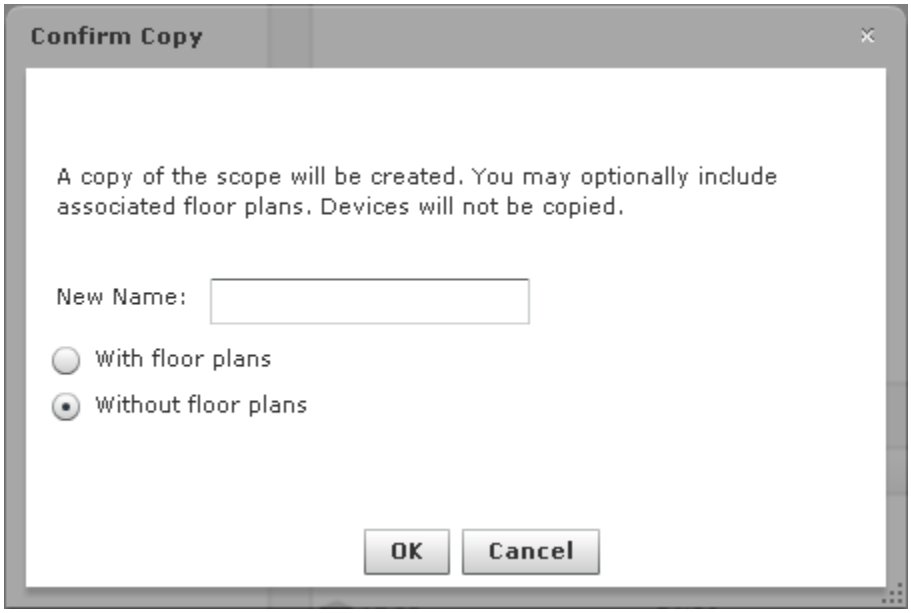
The Region level drop-down menu contains functions that you can apply to the selected Region level. Click the drop-down menu button– next to the Region name to display the drop-down menu.



The drop-down menu for regions contains the following functions:

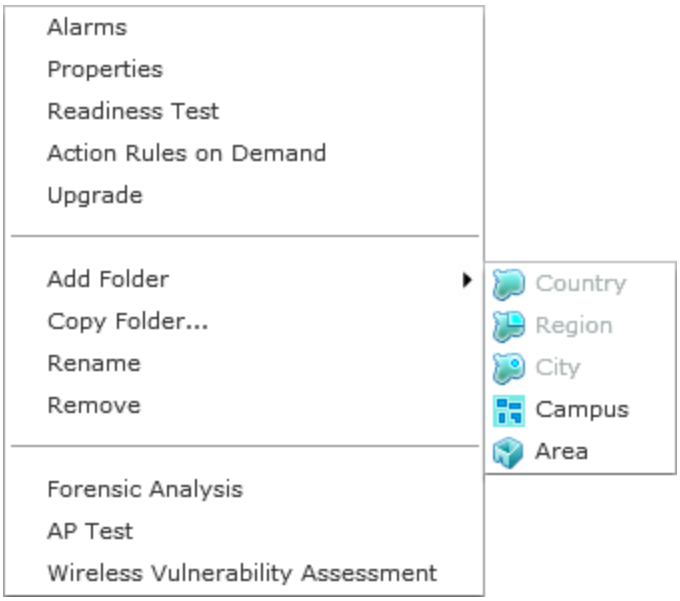
Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected Region.
Properties	Opens the **Properties** overlay for the selected Region.
Readiness Test	Validates that devices in the region scope are management ready (that is, devices can be manage through ASDP).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

Function	Description
Action Rules on Demand	Runs an on demand test on your alarm action rules and/or device action rules.  You can run the test and view the results later in *Job Status*, or you can run the test now and view the results now. There are two options for each type of test: • Only enabled rules—run test on the enabled rules. • All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.
Upgrade	Upgrades the firmware for devices in the selected Region. (For more information, see *Upgrade Devices* in the *Network* chapter.)
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	Copies the network scope of a Region.  Enter a name for the region, select if you want the to include the floor plans or not, and click **OK**.
Rename	Opens a dialog window to rename the selected Region.
Remove	Removes the selected Region from your network. (See *Remove Devices* for more information.)
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
AP Test	Accesses AP Test (*Scheduled AP Tests*).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (*Scheduled Vulnerability Assessment*).

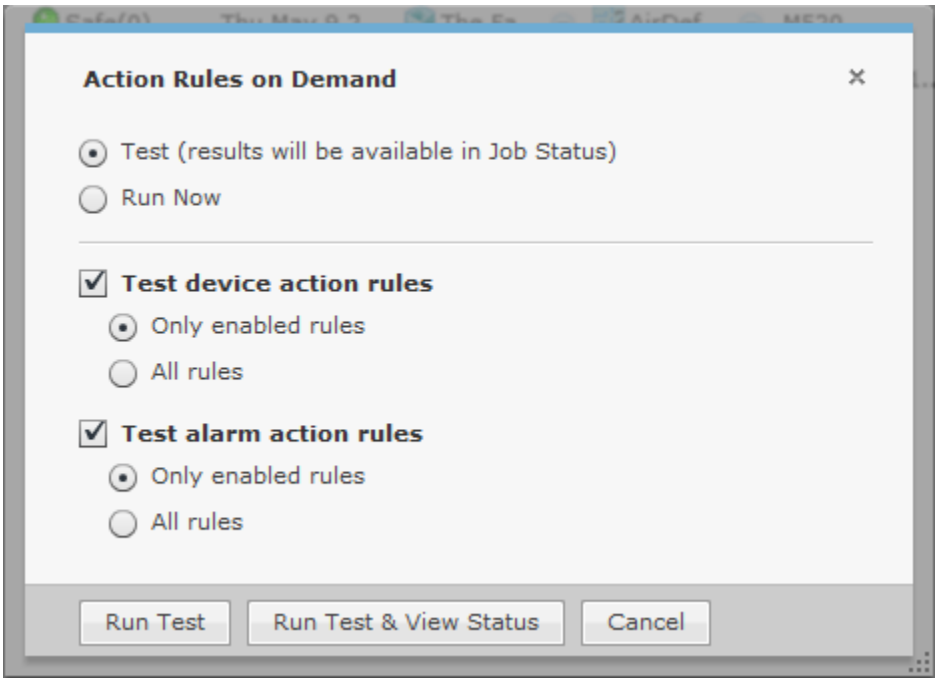
City Level Drop-down Menu

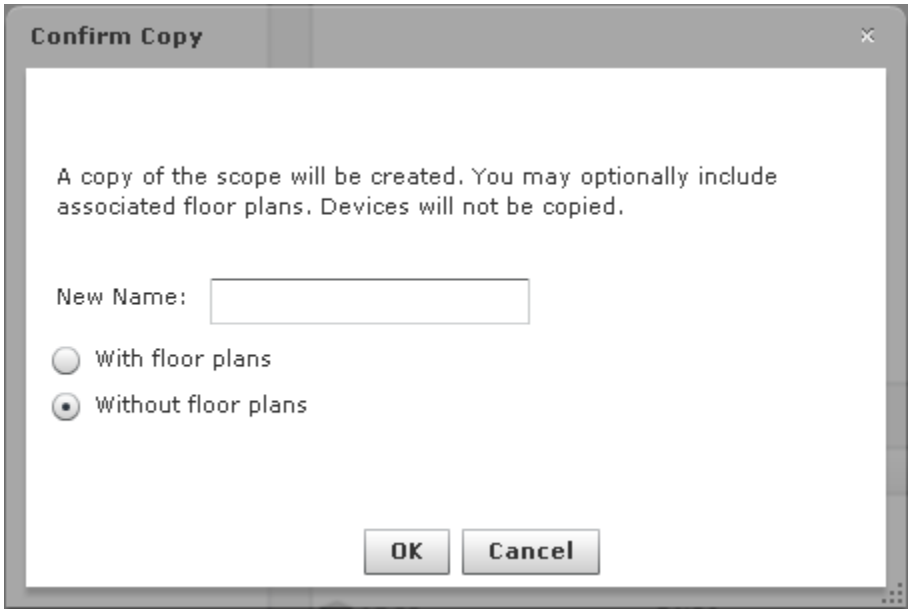
The City level drop-down menu contains functions that you can apply to the selected City level. Click the drop-down menu button– next to the City name to display the drop-down menu.



The drop-down menu for cities contains the following functions:

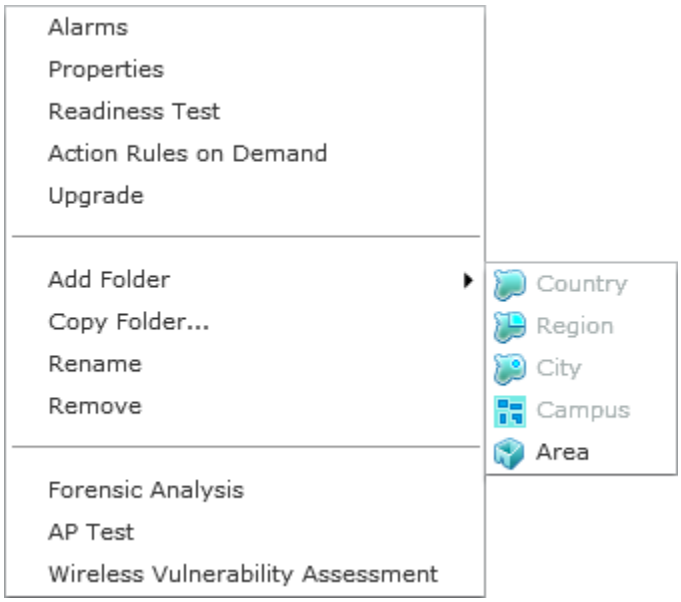
Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected City.
Properties	Opens the **Properties** overlay for the selected City.
Readiness Test	Validates that devices in the city scope are management ready (that is, devices can be manage through ASDP). You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

Function	Description
Action Rules on Demand	Runs an on demand test on your alarm action rules and/or device action rules.  You can run the test and view the results later in *Job Status*, or you can run the test now and view the results now. There are two options for each type of test: • Only enabled rules—run test on the enabled rules. • All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.
Upgrade	Upgrades the firmware for devices in the selected City. (For more information, see *Upgrade Devices* in the *Network* chapter.)
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	Copies the network scope of a City.  Enter a name for the city, select if you want the to include the floor plans or not, and click **OK**.
Rename	Opens a dialog window to rename the selected City.
Remove	Removes the selected City from your network. (See *Remove Devices* for more information.)
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
AP Test	Accesses AP Test (*Scheduled AP Tests*).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (*Scheduled Vulnerability Assessment*).

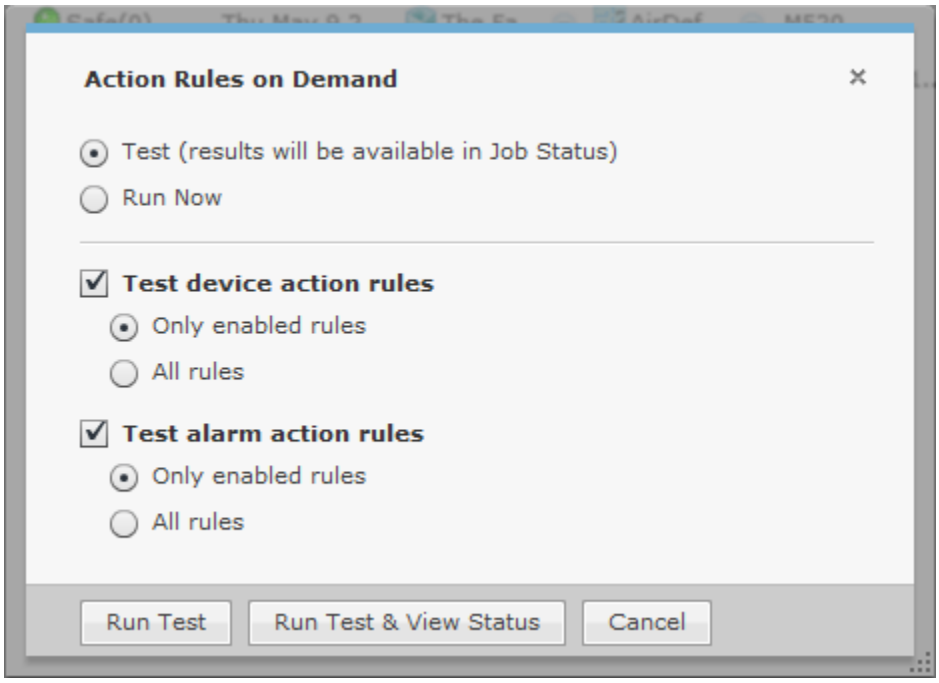
Campus Level Drop-down Menu

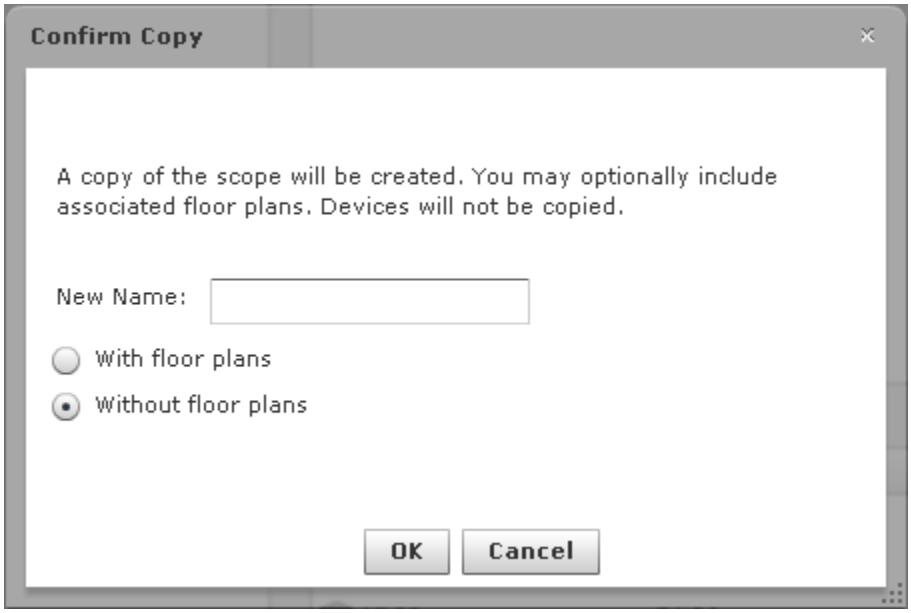
The Campus level drop-down menu contains functions that you can apply to the selected Campus level. Click the drop-down menu button– next to the Campus name to display the drop-down menu.



The drop-down menu for campuses contains the following functions:

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

Function	Description
Action Rules on Demand	Runs an on demand test on your alarm action rules and/or device action rules.  You can run the test and view the results later in *Job Status*, or you can run the test now and view the results now. There are two options for each type of test: • Only enabled rules—run test on the enabled rules. • All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.
Upgrade	Upgrades the firmware for devices in the selected Campus. (For more information, see *Upgrade Devices* in the *Network* chapter.)
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.

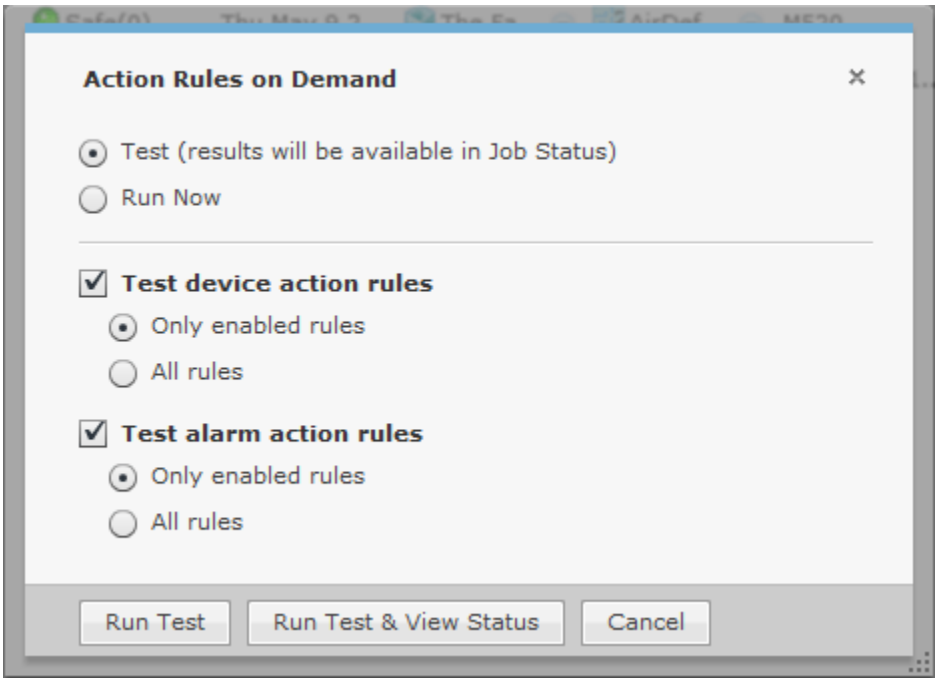
Function	Description
Copy Folder	Copies the network scope of a Campus.  Enter a name for the campus, select if you want the to include the floor plans or not, and click **OK**.
Rename	Opens a dialog window to rename the selected Campus.
Remove	Removes the selected Campus from your network.
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
AP Test	Accesses AP Test (*Scheduled AP Tests*).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (*Scheduled Vulnerability Assessment*).

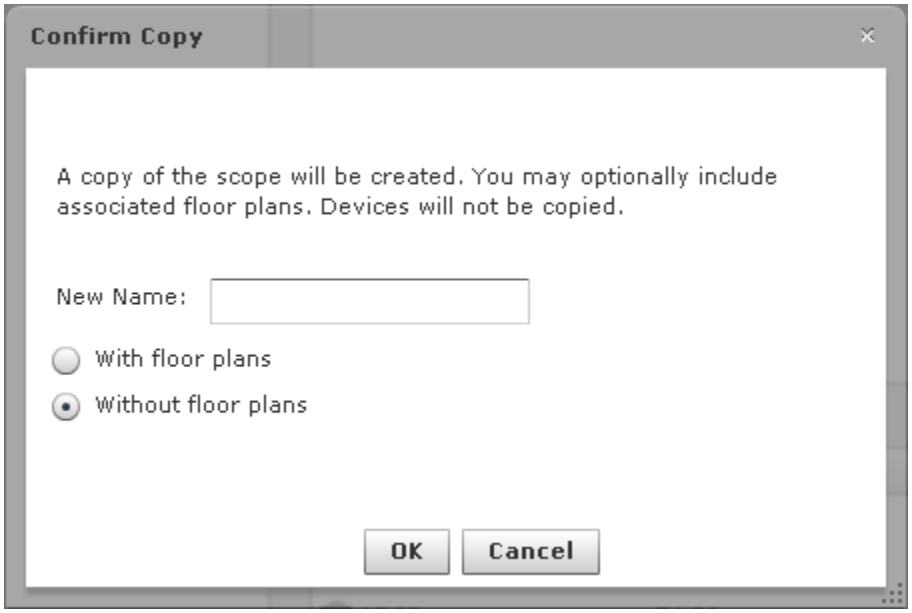
Area (Building) Level Drop-down Menu

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 **Alarms** tab where you can view the alarms for the selected Area.
Properties	Opens the **Properties** 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 *Readiness Test* for more information.)

Function	Description
Action Rules on Demand	Runs an on demand test on your alarm action rules and/or device action rules.  You can run the test and view the results later in *Job Status*, or you can run the test now and view the results now. There are two options for each type of test: • Only enabled rules—run test on the enabled rules. • All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.
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. (For more information, see *Upgrade Devices* in the *Network* chapter.)

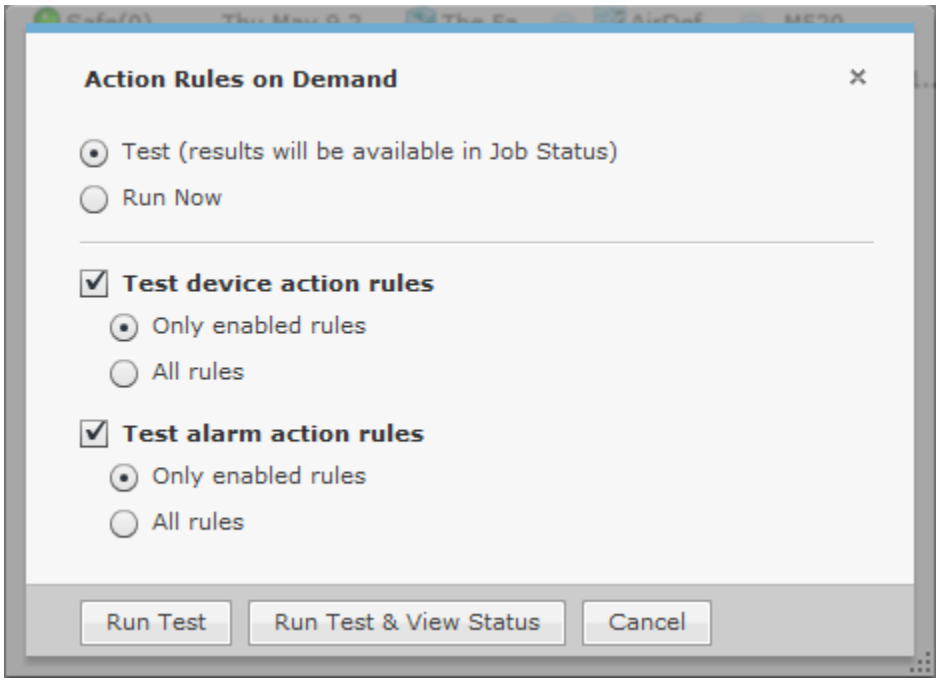
Function	Description
Copy Folder	Copies the network scope of a Area.  Enter a name for the building, select if you want the to include the floor plans or not, and click **OK**.
Rename	Opens a dialog window to rename the selected Area.
Remove	Removes the selected Area from your network.
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
AP Test	Accesses AP Test (*Scheduled AP Tests*).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (*Scheduled Vulnerability Assessment*).

Live RF/Floor Plan Level Drop-down Menu

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 **Alarms** tab where you can view the alarms for the selected Floor.
Properties	Opens the **Properties** overlay for the selected Floor.
Readiness Test	Validates that devices in the building scope are management ready (that is, devices can be managed through ASDP). You are alerted of problem areas. (See *Readiness Test* for more information.)

Function	Description
Action Rules on Demand	Runs an on demand test on your alarm action rules and/or device action rules.  You can run the test and view the results later in *Job Status*, or you can run the test now and view the results now. There are two options for each type of test: • Only enabled rules—run test on the enabled rules. • All rules—run test on all rules (enabled or not). This option is deactivated on run now tests.
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. (For more information, see *Upgrade Devices* in the *Network* chapter.)
Rename	Opens a dialog window to rename the selected Floor.
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
AP Test	Accesses AP Test (*Scheduled AP Tests*).
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (*Scheduled Vulnerability Assessment*).
Add Device	Adds devices to the AirDefense Services Platform. Add devices to the AirDefense Services Platform. (See *Add Devices*.)

Creating Floor Plans

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, and plan where to place devices on a floor for maximum coverage. To create a floor plan:

1 Upload an background image to use as a guide to insert walls, cubicles, doors, elevators, etc.

2 Add additional floors if your building contains two or more floors.

3 Use the editing tools to insert walls, cubicles, doors, elevators, etc.

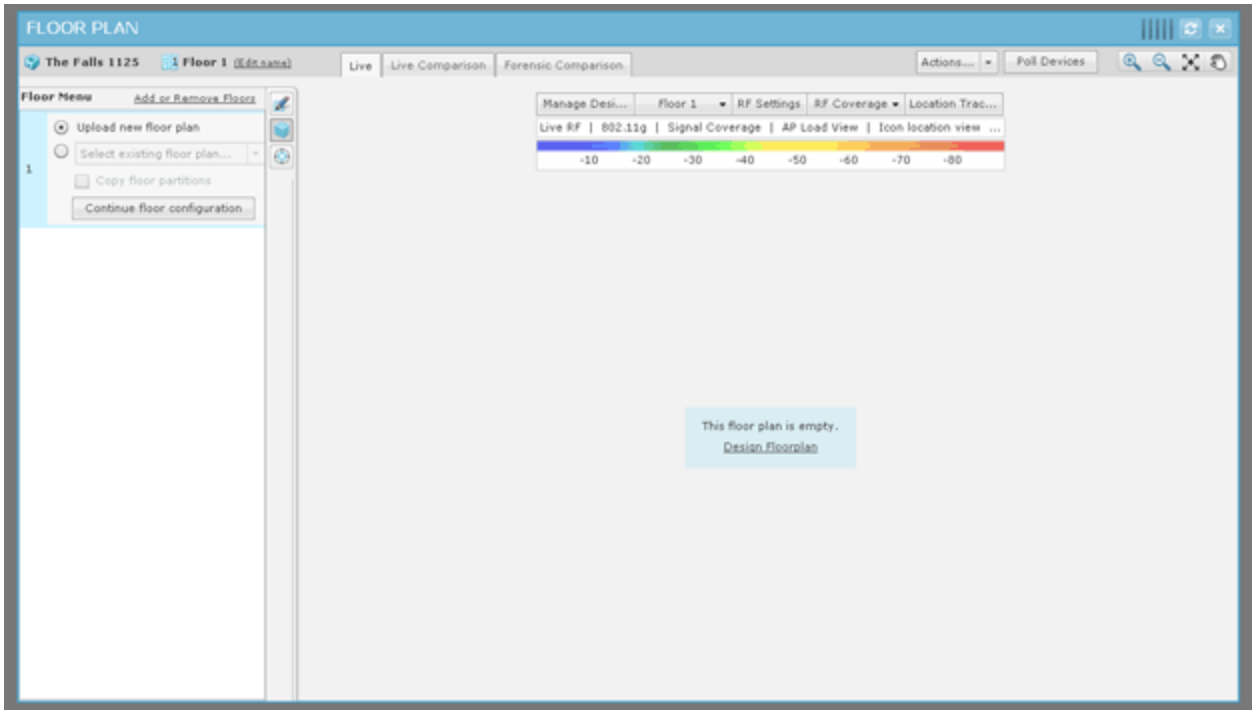
Maximum Size Allowed for a Scaled Floor Plan

There is a maximum size for the amount of territory covered in a floor plan. The maximum diagonal (line drawn from the bottom-left corner to the upper-right corner) is 1000 meters. If you scale the floor plan beyond a 1000 meter limit, regardless of the image size, the RF Modeling Engine crashes and generates an error message: “Design bounds exceeding maximum design area.”

NOTE The maximum total amount of territory (real estate) for a scaled floor plan is determined by a diagonal line from the two furthest corners of the diagram. This line can be no longer than 1000 meters (3280 ft.) For a perfectly square floor plan, this represents a single side of no greater than 707.1 meters (2320 ft.) and a total area of 50,000 sq meters (538,196 sq ft.)

Uploading Background Image

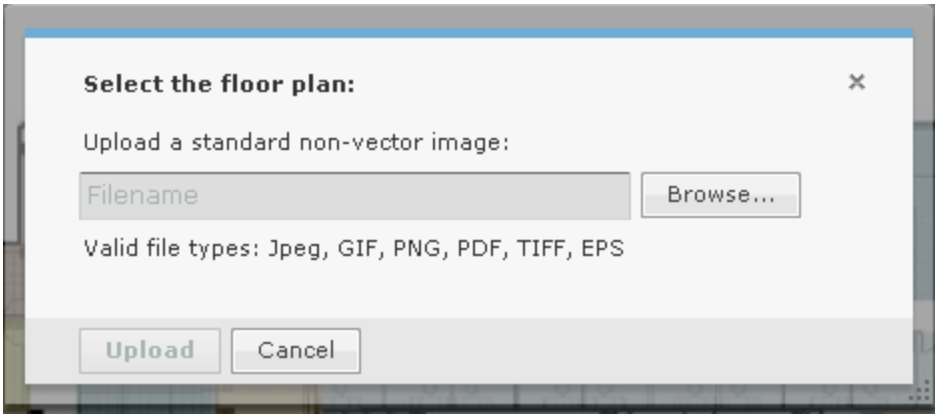
The first time that you access a Floor Plan, you will need to upload a background image for your first floor. If you are accessing a Floor Plan from an area (building), the first floor is selected. If you are accessing a Floor Plan from a floor, that floor is selected.



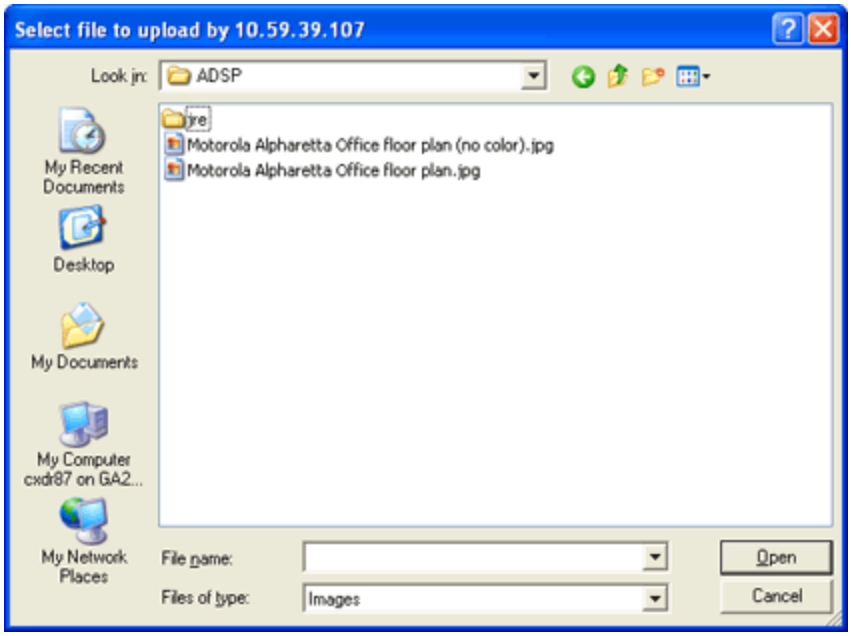
When the floor plan is complete, you will need to click the Close button–X to save and close. The Floor Plan can then be viewed throughout ADSP, and can be used to locate devices in your network and display Live RF data.

To upload a background image, click the **Continue floor configuration** button or the **Design Floorplan** link to get started.

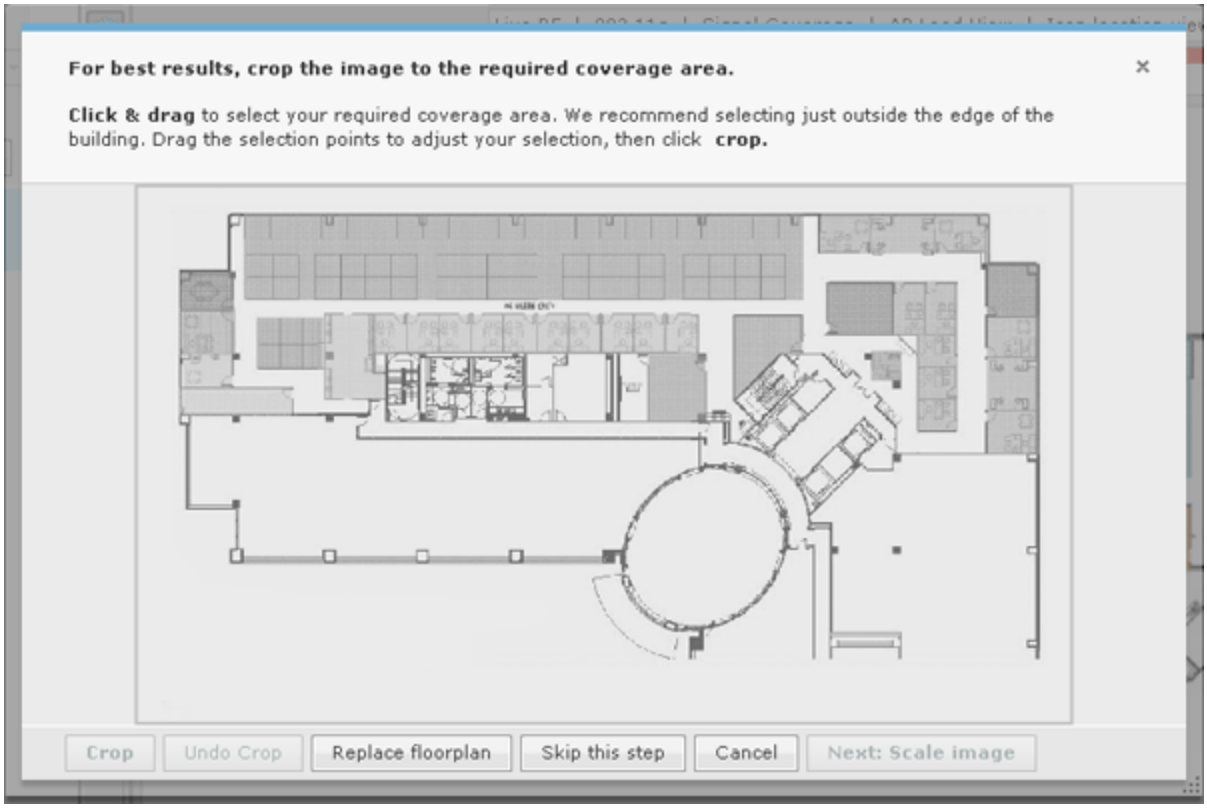
NOTE The Floor Plan single dimension limit (width or height) is 8192 pixels while the total pixel count (width x height) limit is 8,000,000 pixels. If the appliance has at least 2GB of memory, the total pixel count may be as high as 16,777,215 pixels but the single dimension limit is still 8192 pixels.



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:

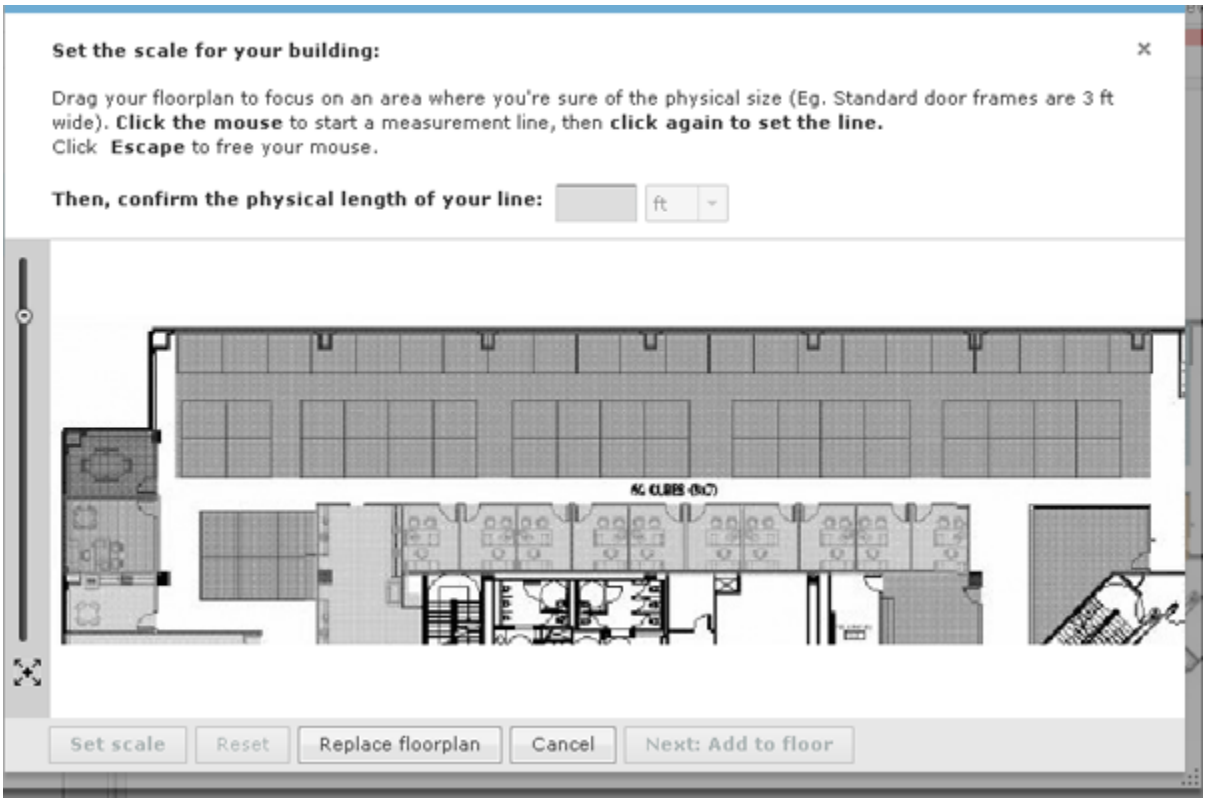
a. Clicking on a point in the image.

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.

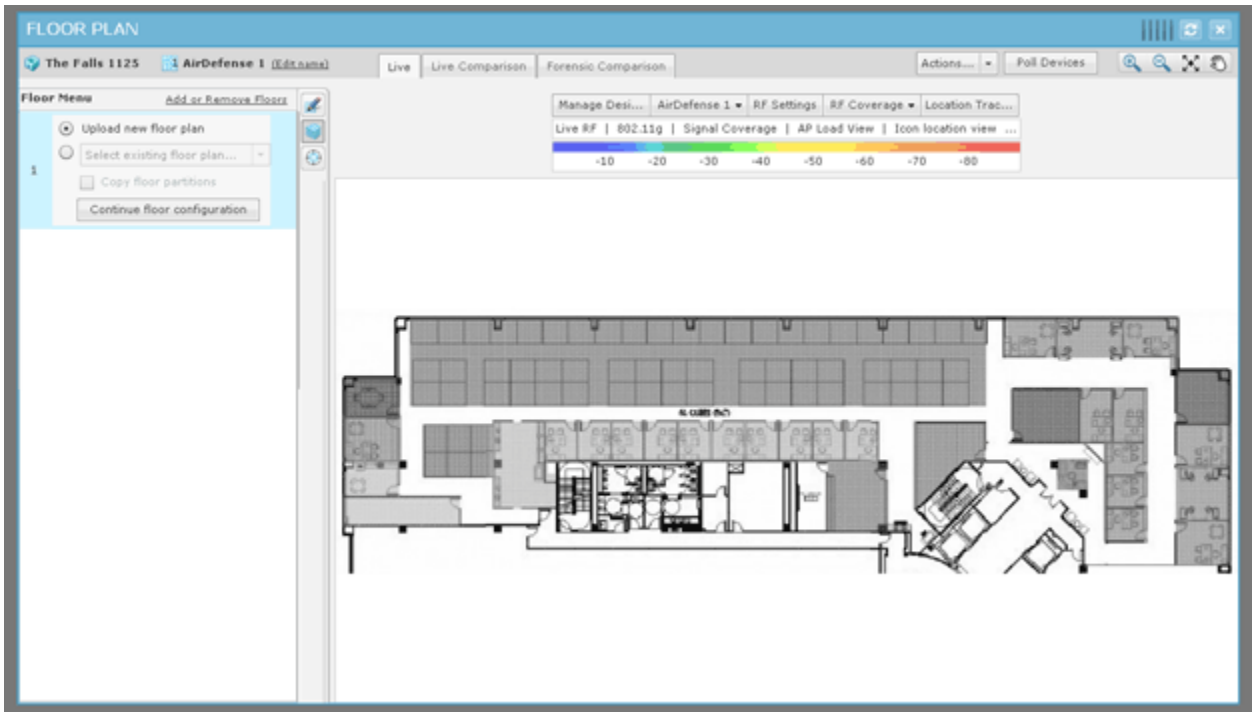


6 Scale your image by clicking on a point in the image, draw a line, and then click an end point. Enter the distance of the line which represents the actual length of the physical space in feet or meters. The **Set scale** button is activated. Click it to complete scaling.

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:

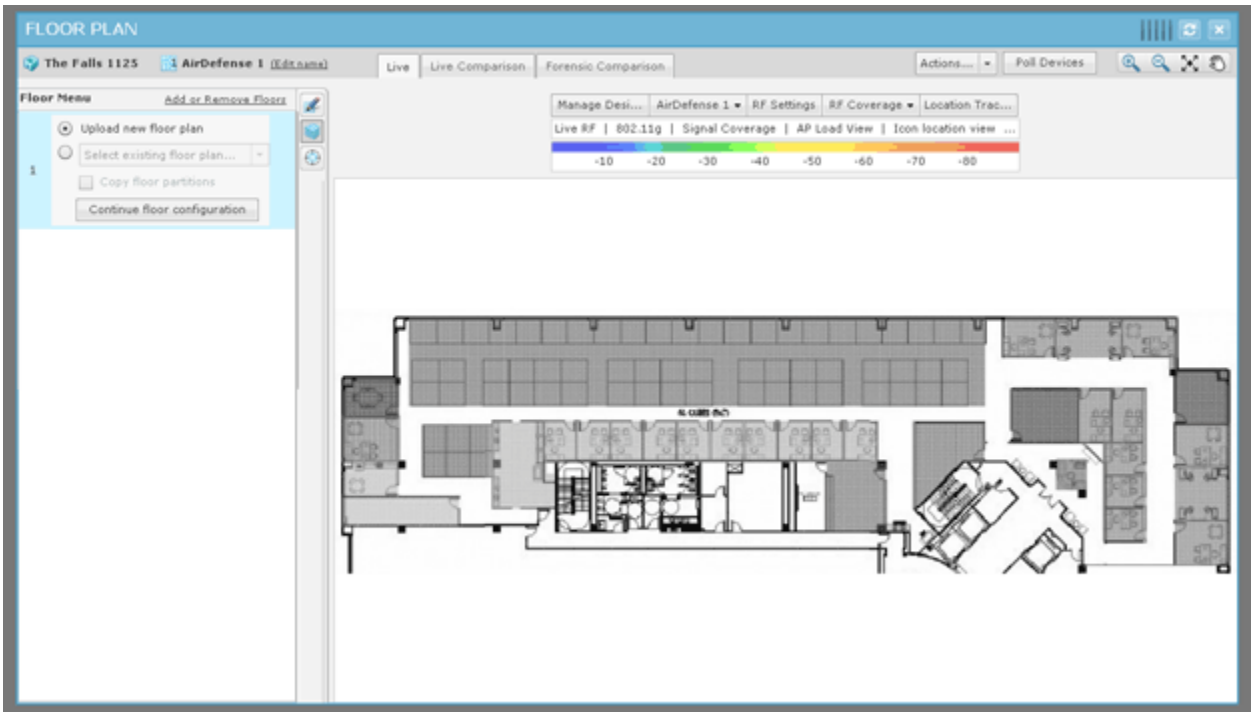


You can now use the editing tools to add walls, cubicles, doors, elevators, etc. This allows you to account for building obstacles when ADSP does calculations to locate devices and/or to display Live RF data.

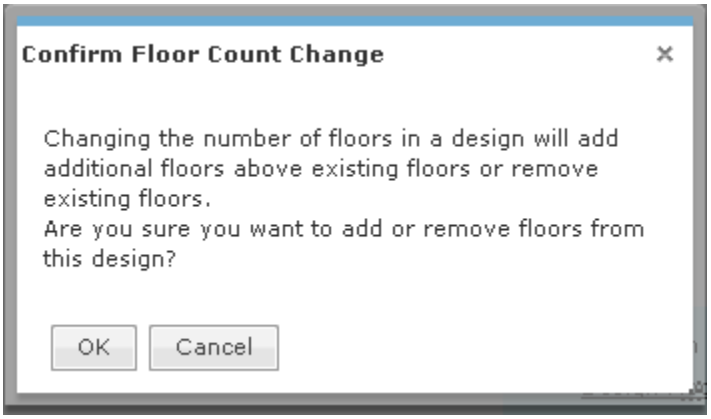
Add Additional Floors

To add an additional floor to your building, first reveal the existing floors by clicking anywhere on the **Floor Plan Toolbar**.

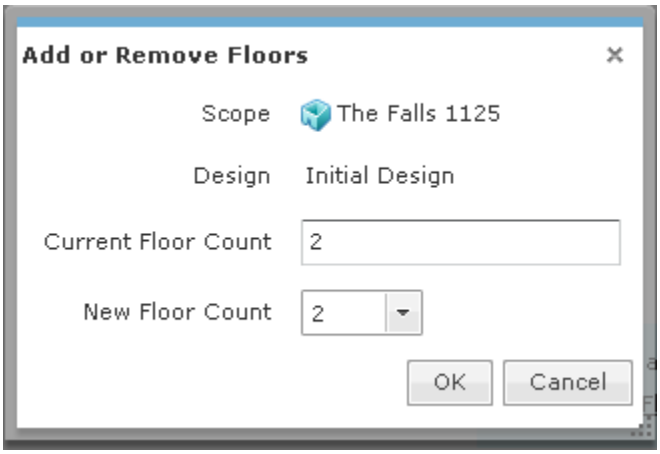
NOTE Clicking the **Floor Plan Toolbar** also removes floor selection from view.



Click the **Add or Remove Floors** link. The following dialog box is displayed:

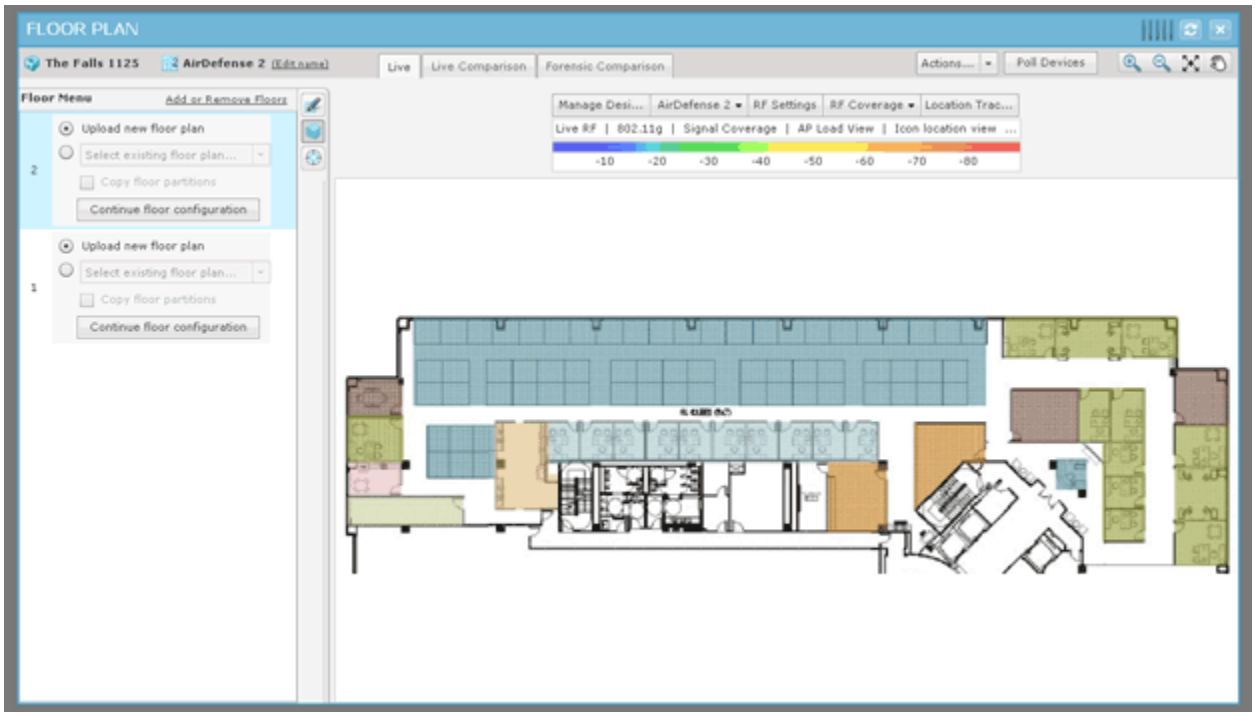


Click **OK** to continue to the following dialog box:



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:



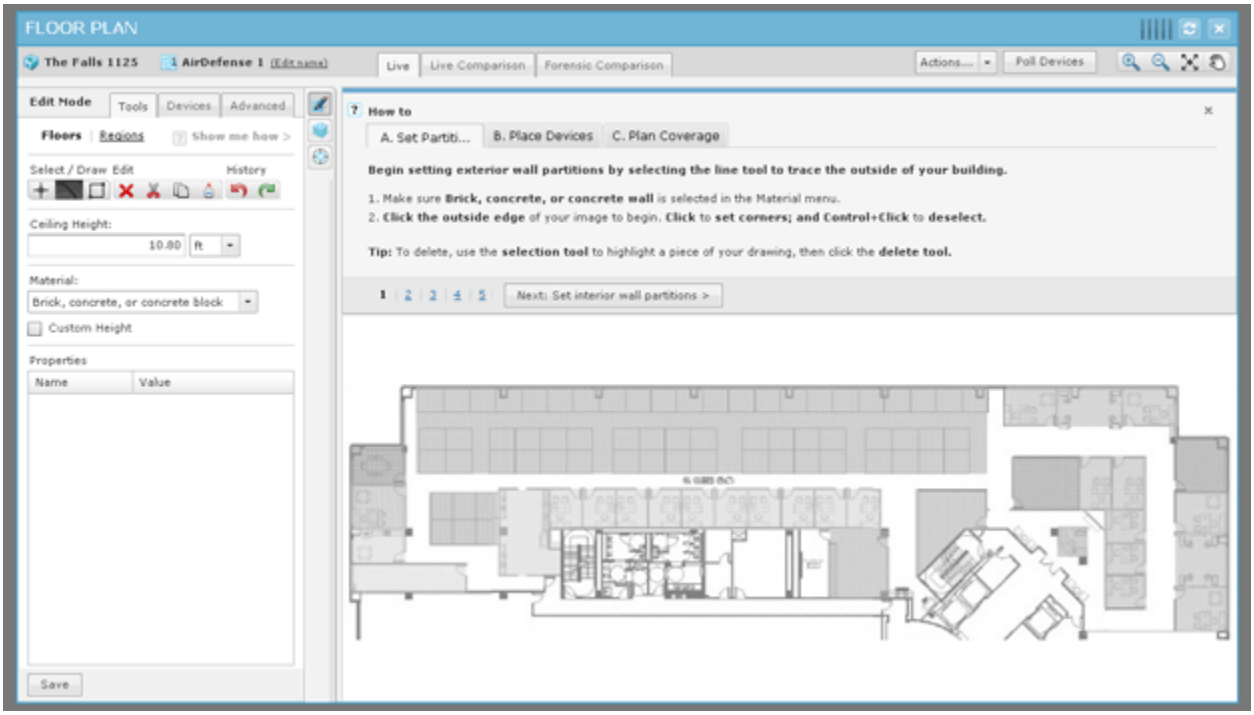
To access the different floors within a building, click the thumbnail image for the floor located in the left pane.

Edit 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 *Floor Plan 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.

Click **Save** to save any changes.

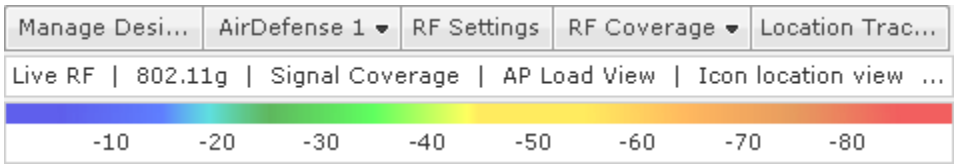
Global Tools

Global tools are tools that are available on all Floor Plan pages. They are:

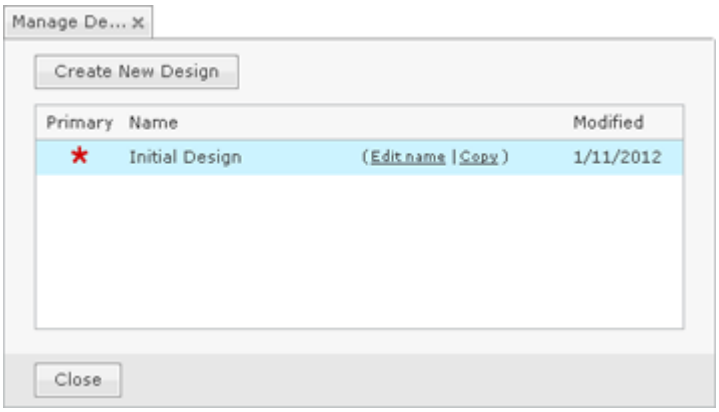
- Context Label
- Actions
- Floor manipulation.

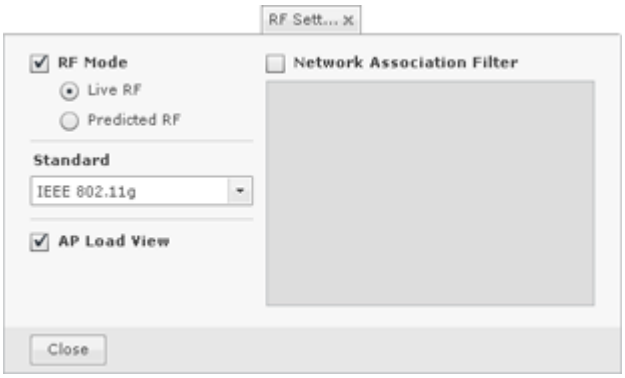
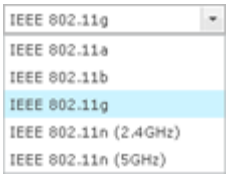
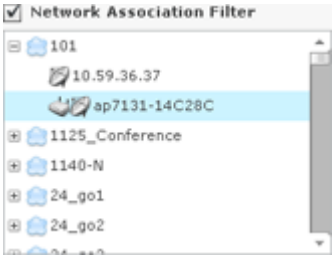
Context Label

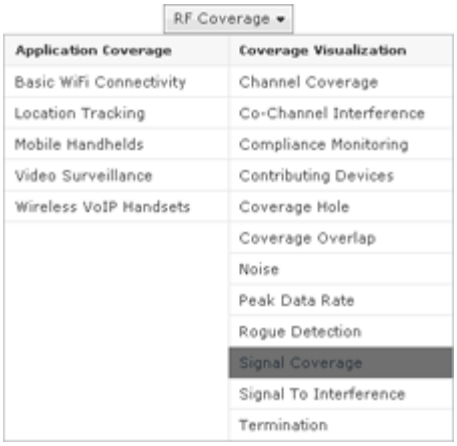
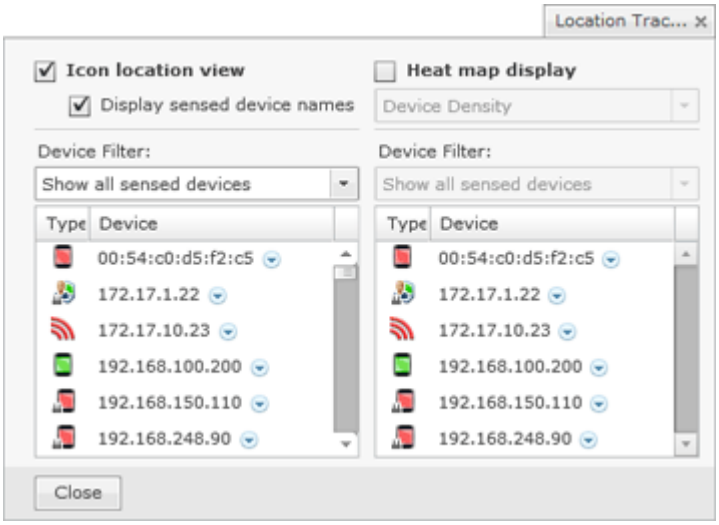
The **Context Label**, located near the top-center of the Floor Plan, controls the context of the Floor Plan.

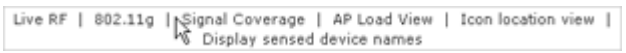


The **Context Label** shows you the following information:

Field	Description
Manage Designs	When this field is clicked, a list of existing designs is displayed:  You can edit or add to the list using the following actions: • Click the **Primary** field for a design to make it the primary design. • Click on the **Edit name** link to change the name. • Click the **Copy** 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 **Edit name** link. • Click the **Remove**–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. • Click the **Create New Design** button to create a new design. A name for the new design is auto-generated and can be changed using the **Edit name** link. Click **Close** to exit the design manager.
Floor Selection	This field shows the selected floor. If you click the field, you can select another floor to view. 
RF Settings	RF Settings includes: • RF Mode setting • Protocol setting • AP Load View setting • Network Association Filter.

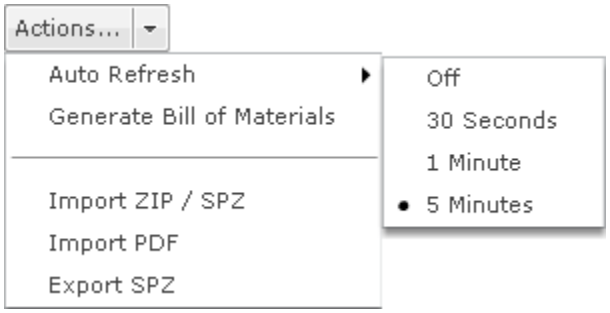
Field	Description
• RF Mode Setting	The **RF Mode** setting determines if your heat maps display no RF data (deselected), Live RF data (selected), or Predicted RF data (selected). 
• Protocol Setting	The **Protocol** setting allows you to filter RF data according to the selected protocol. 
• AP Load View Setting	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.  Click on the smaller circle to display all the associated Wireless Clients in a table. 
• Network Association Filter Setting	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	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.  Visualizations and applications are configured in **Configuration** > **Network Assurance** > **Live RF Settings**.
Location Tracking	This field displays a list of devices being tracked grouped by device type.  If a device in the list is selected (highlighted) it is highlighted in the floor plan map. Location Tracking has two views: **Icon location view** and **Heat map display**. The **Icon location view** displays the most likely location for selected devices as an icon for each device. The **Heat map display** displays the most likely locations for the selected device as a color gradient ranging from red (most likely) to blue (least likely) locations.

Field	Description
Current Settings	This field gives you a quick view of the settings that have been set via the **Context Label**.  Three dots (...) at the end of the **Current Settings** indicate there are more settings that have been configured. Moving your mouse over the **Current Settings** will reveal the additional settings. 
Color Chart	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). 

Floor Plan Actions

The Floor Plan Actions feature contains a set of tools for generating a bill of materials and importing/exporting floor plan data.



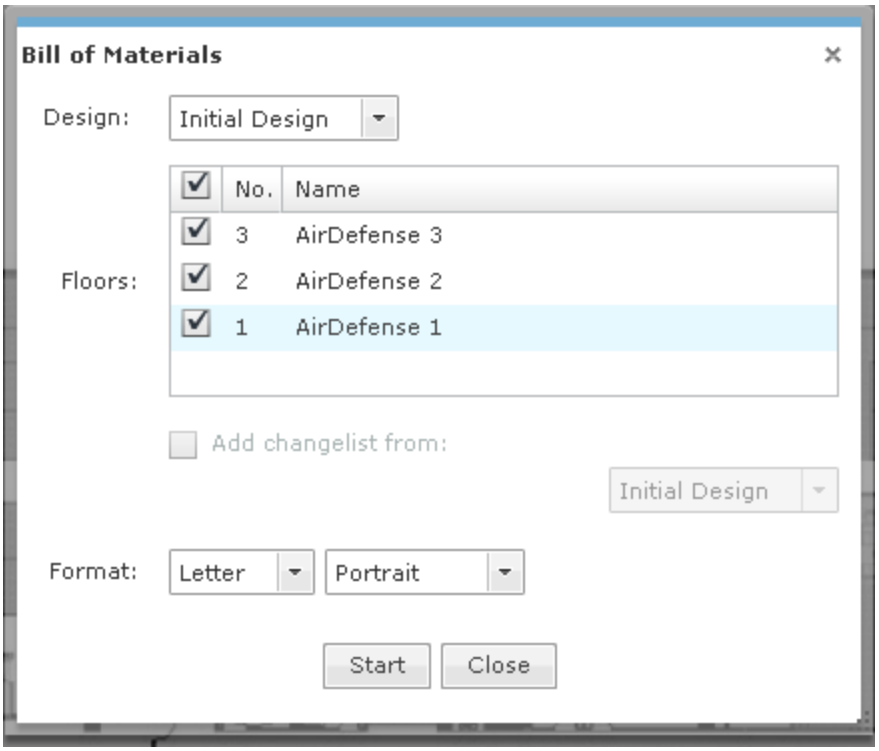
Auto Refresh

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:

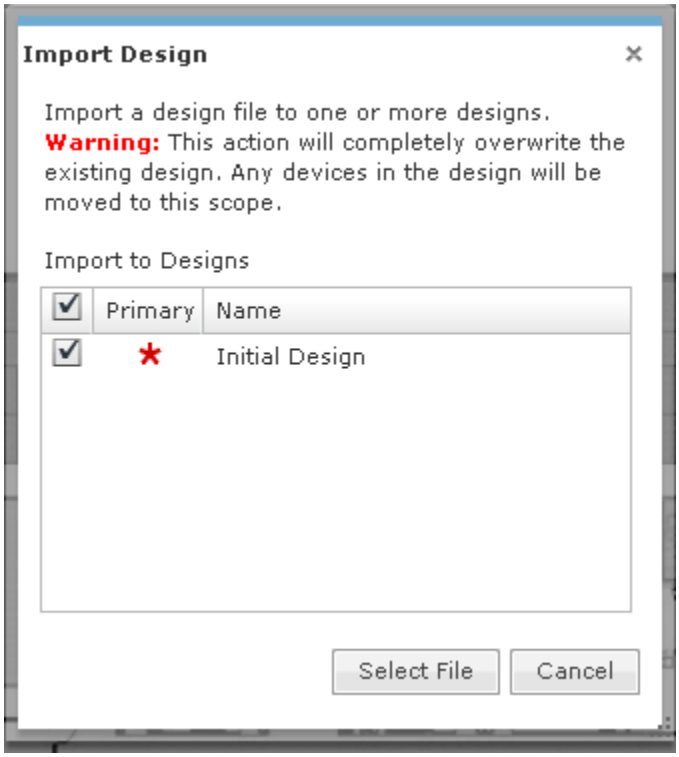
Field	Description
Design	Selects the design to use when generating the bill of materials.
Floors	Selects the floors of the design to use when generating the bill of materials. A checkmark selects the floors. The top checkbox, when checked, will select or deselect all of the floors.
Add changelist from	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.

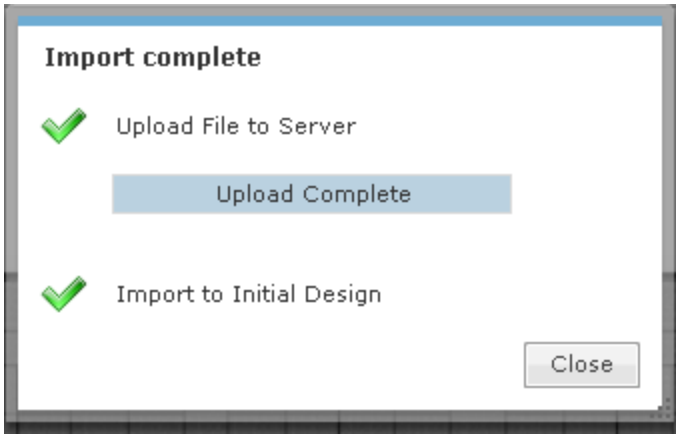
Import ZIP / SPZ

LAN Planner

You can import a LAN Planner (or Outdoor Planner) design that has been exported to a ZIP file, a speedwell (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.

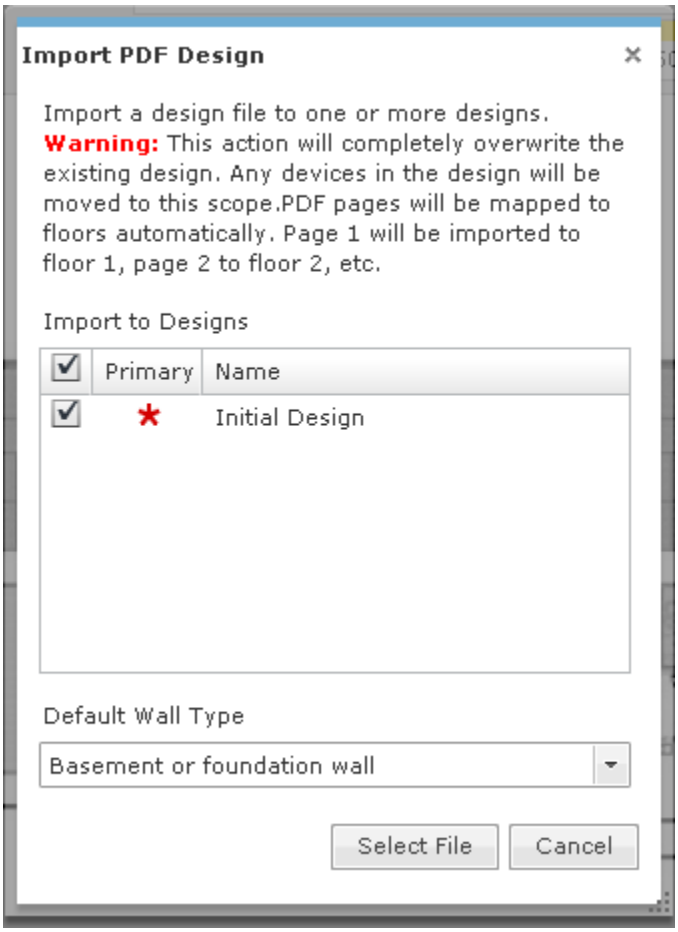


Click the **Close** button to return to the Floor Plan.

NOTE LAN Planner and Outdoor Planner are legacy products that are no longer available for purchase. However, If you have the application, ADSP will support it.

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:

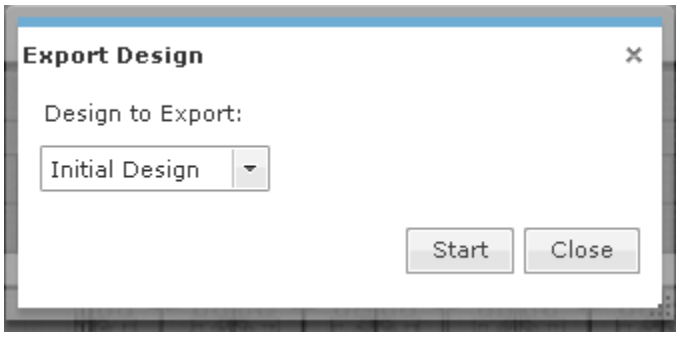
- You can choose the default wall type with Import PDF as follow: Basement or foundation wall
- Brick, concrete, or concrete block
- Cubicle wall
- Drywall or sheetrock
- Elevator or metallic obstacle
- Glass door or window, no tint
- Metallic rack
- Wooden door.

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.

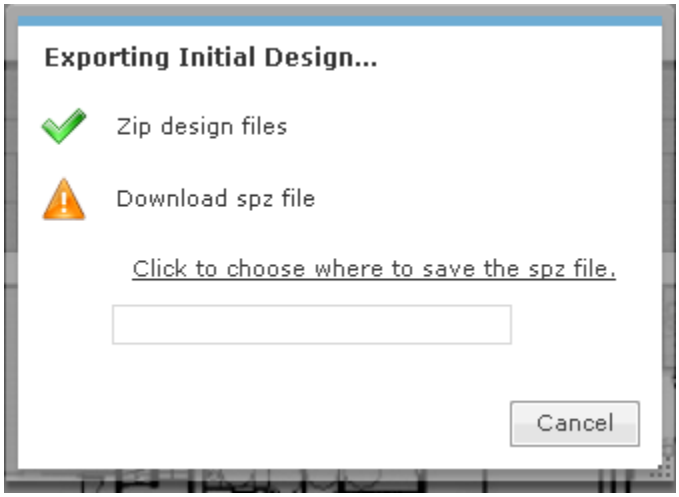
Export Floor Plan to ZIP File

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.



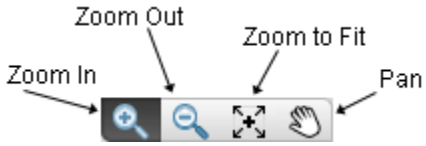
To begin, select a design from the drop-down menu and then click **Start**. A checklist is generated to indicate success or not.



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 Tools

The floor manipulation tools (located near the top-ride 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:

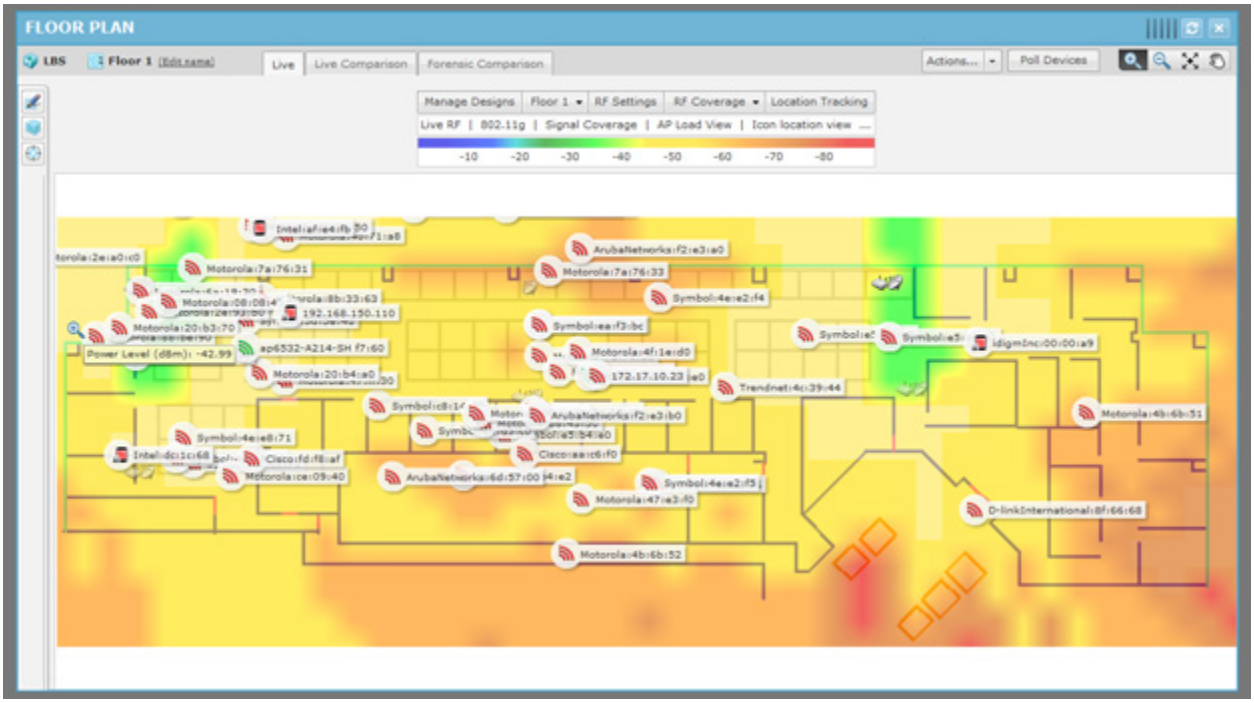
Tool	Description
	Click this tool to zoom in (enlarge the size) a floor plan image. Each click will zoom into another level.
	Click this tool to zoom out (reduce the size) a floor plan image. Each click will zoom out to another level.

Tool	Description
	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.

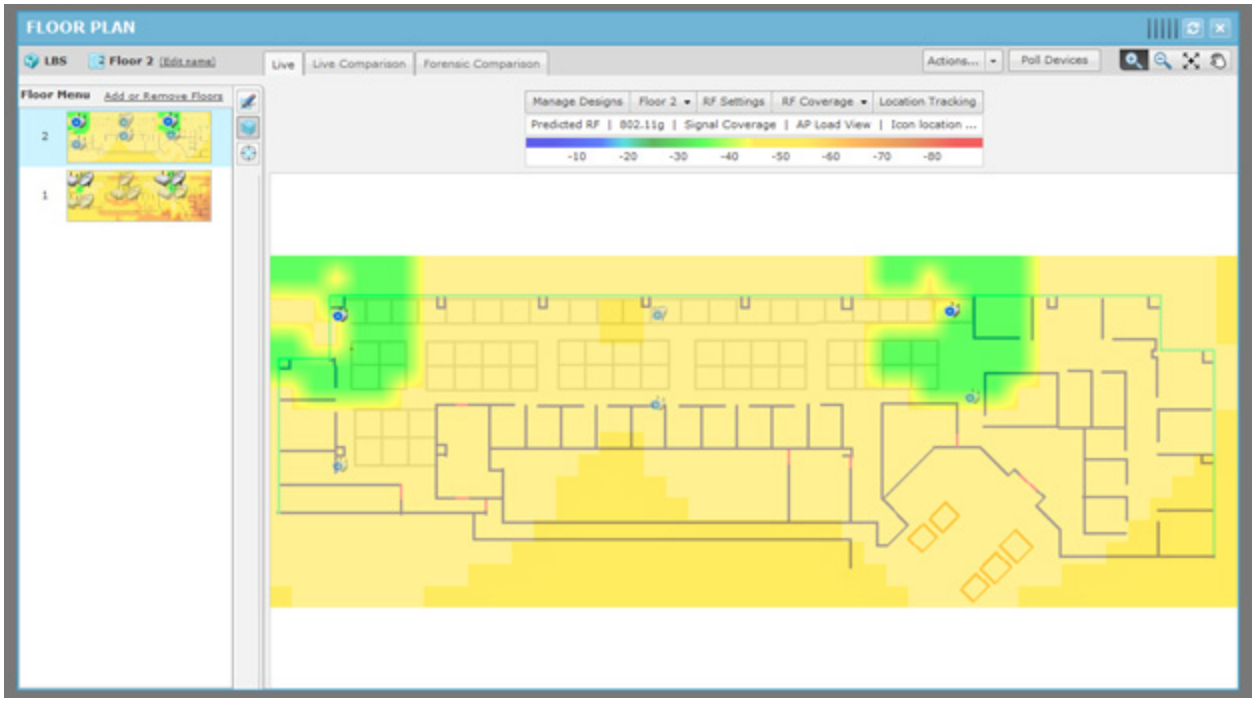


Live RF data is available on all Floor Plan pages. When the Floor Plan is refresh (manually or automatically), RF data is updated using the latest data (radio, power, channel, live status, etc.) about the devices. This data comes from the last polling cycle for the devices. If the **Poll Devices** button is clicked, the devices are refreshed first by ADSP and then the RF data is updated and displayed in the Floor Plan.

Predictive RF

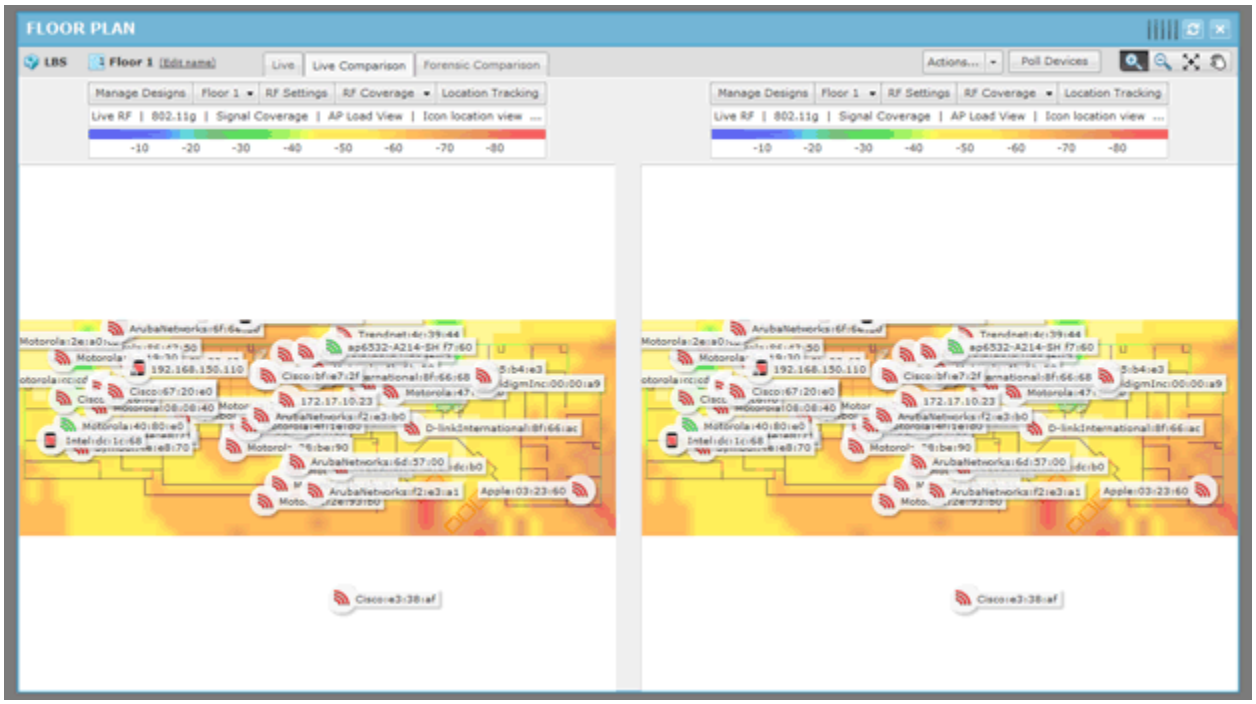
The Floor Plan also displays a Predictive RF heat map that represents predicted coverage for planned devices placed on a Floor Plan. You must first place planned devices on the Floor Plan

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.

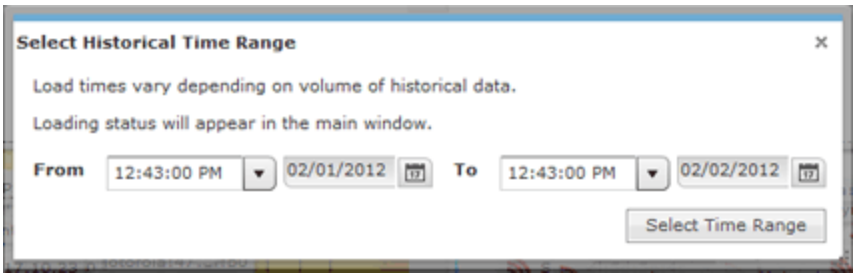


You have access to the Context Label where you can manipulate one or both of the images.

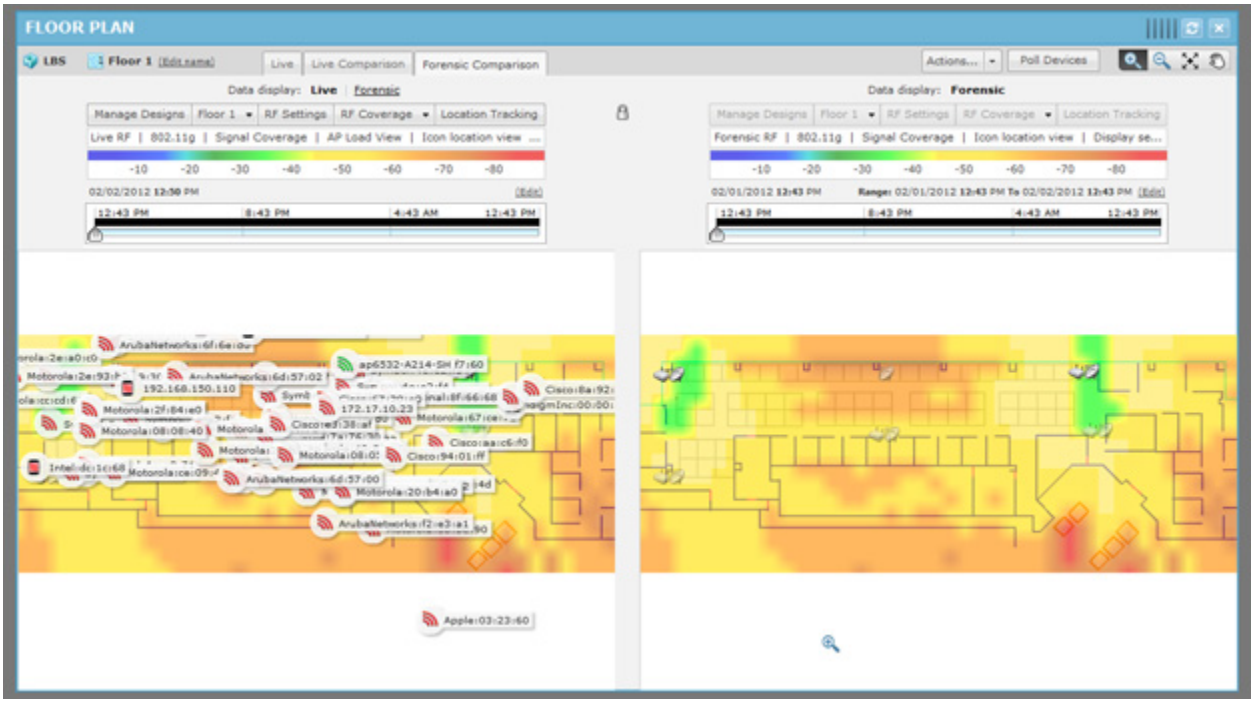
The floor manipulation tools are available so that you can zoom in/out or pan the images.

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.

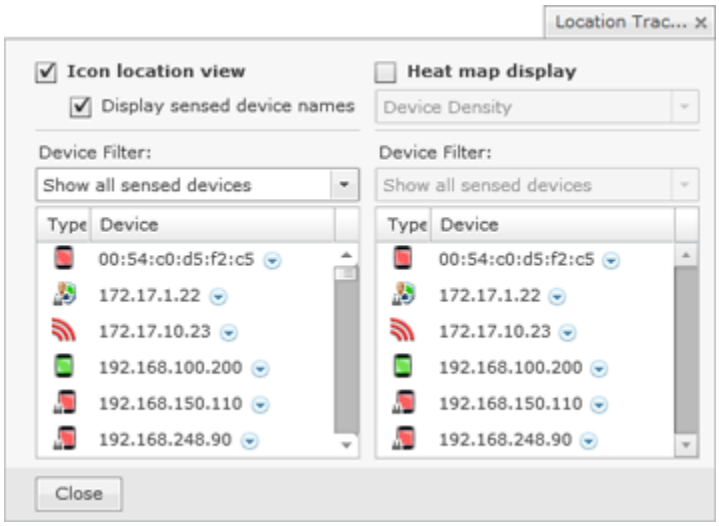
Tracking Rogue Devices

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:

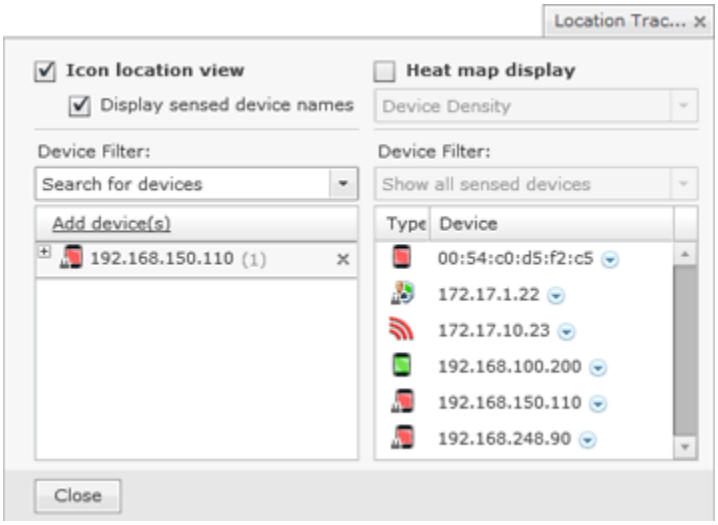
- **Icon location view** displays the devices on the map by its icon and device name.
- **Heat map display** displays the likely location for a tracked device as a color gradient ranging from red (most likely) to blue (least likely) locations. The device icon is displayed on the map at the most likely 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.

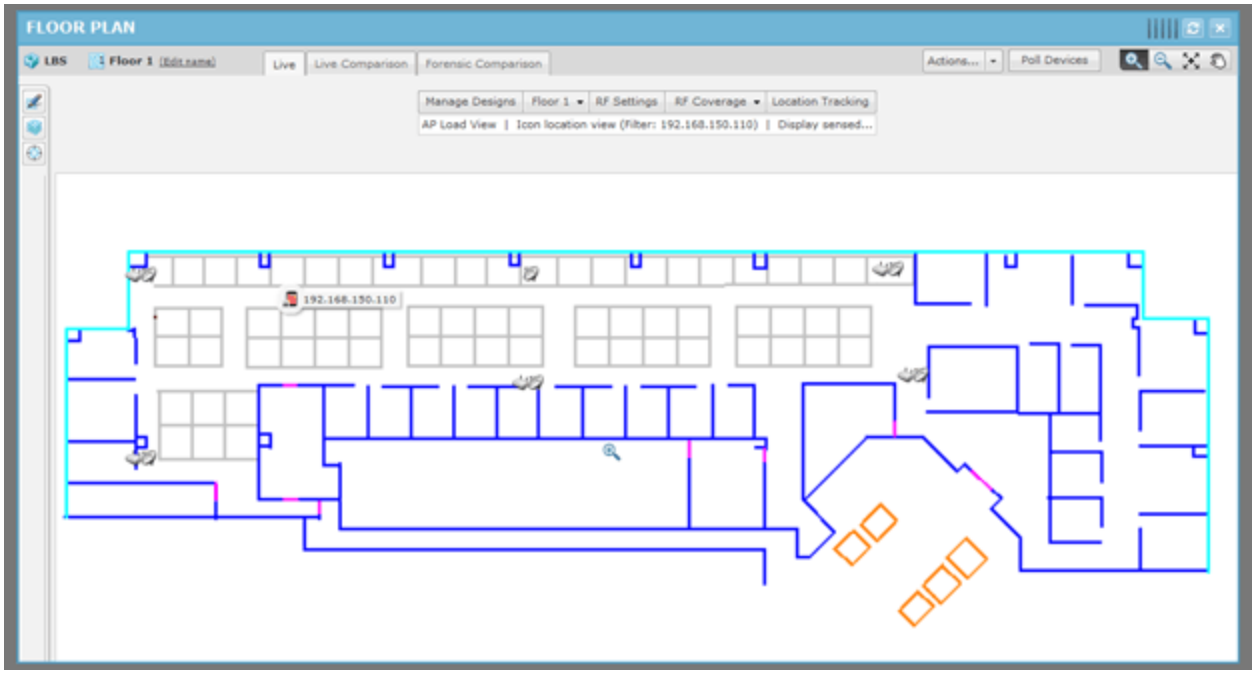
NOTE The **Advanced** link is used to open a search dialog that gives you more options to find devices.

When you see the device listed, click on it and then click **Track Device**. The device is displayed in the tracked device list.



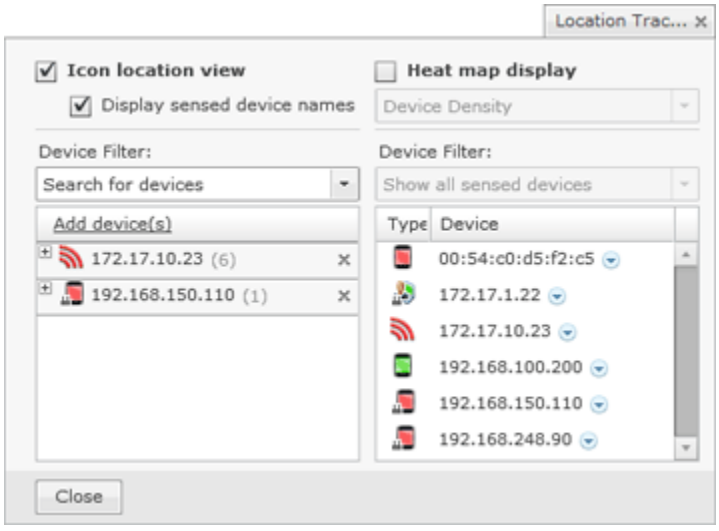
NOTE You may select more than one device using the <Shift> key or the <Ctrl> key.

Click the **Close** button or anywhere outside the Location Tracking dialog to display the device in the Floor Plan.

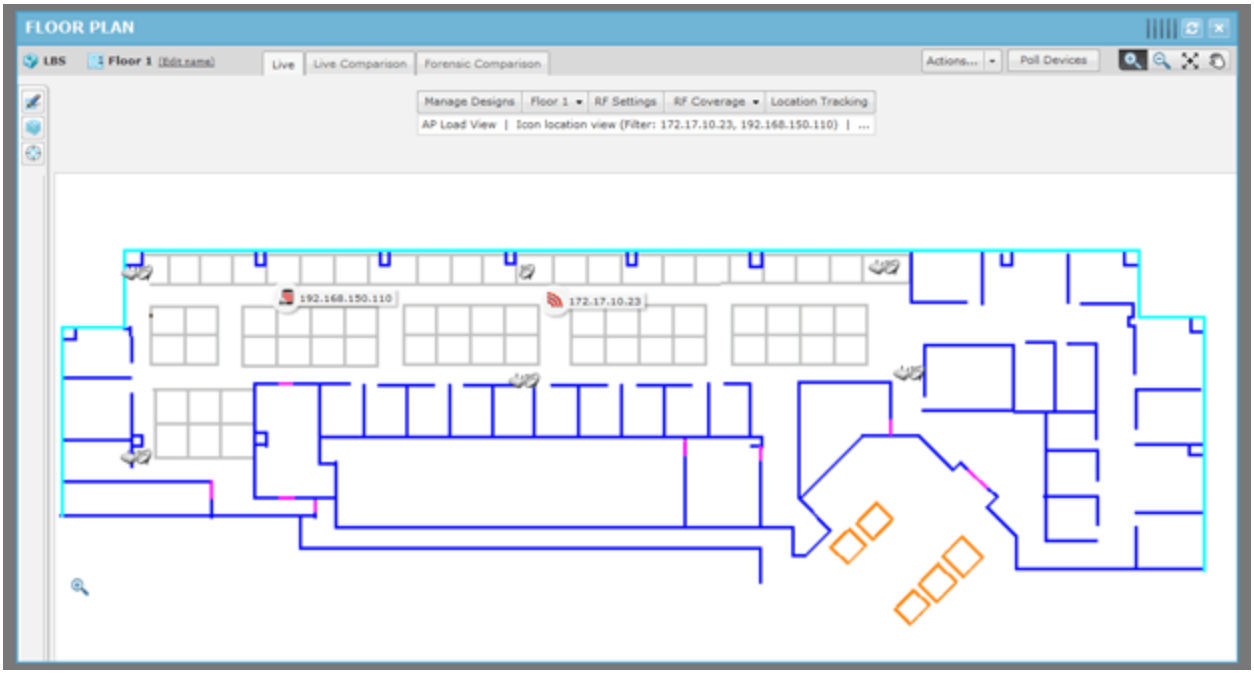


The Floor Plan shows the device being tracked. Click the **Refresh** button to refresh the image. If the device has moved, you will see its current position in the floor plan.

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 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 controller infrastructure. The 4.x version of 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

In order to activate Wireless Client tracking, you must enable the Enhanced Probe table on the RFSX000 controller. This allows an AP to forward an MU probe request data to the controller.

You must manually enter the MAC address for each Wireless Client that you wish to track into the preferred Wireless Client (MU) list. If you want to track multiple rogue Wireless Clients, you have to input the MAC of each Wireless Client (MU) into the switch, and then wait until it is pushed into ADSP. Follow these steps:

1 Log in to 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.

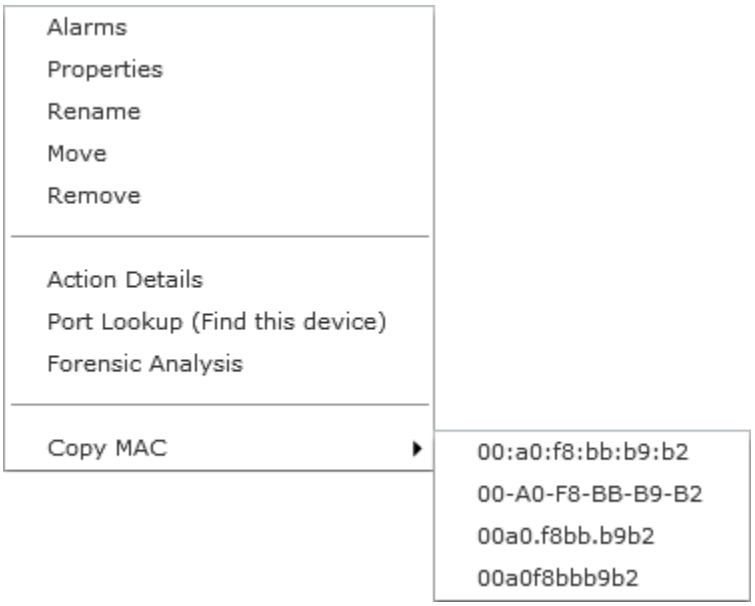
11 Click **Apply**.

12 Repeat steps 9 – 11 for the A radio.

13 Restart the controller.

Unplaced Devices Level Drop-down Menu

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.



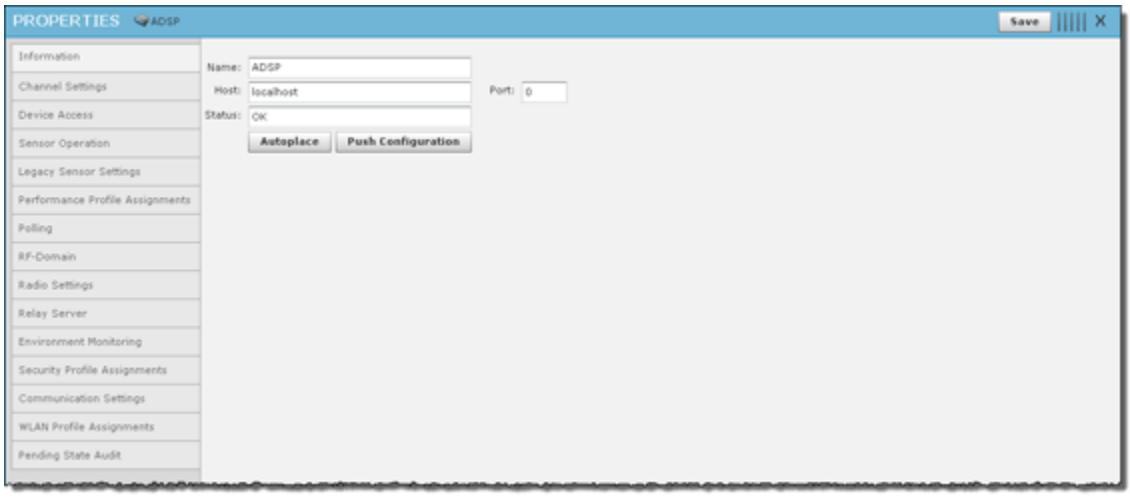
The drop-down menu for unplaced devices contains the following functions:

Function	Description
Alarms	Accesses the **Alarms** tab where you can view the alarms for the selected Unplaced Devices level.
Properties	Opens the **Properties** overlay for the selected Unplaced Devices level.
Rename	Opens a dialog window to rename the selected unplaced device.
Move	Moves the selected unplaced device to another network level (floor). (See *Move Devices* for more information.)
Remove	Removes the selected unplaced device from your network. (See *Remove Devices* 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 *Port Lookup* window where you can locate the physical port where the unknown device is accessing your network.
Forensic Analysis	Accesses *Forensic Analysis—Basic*.
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 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.

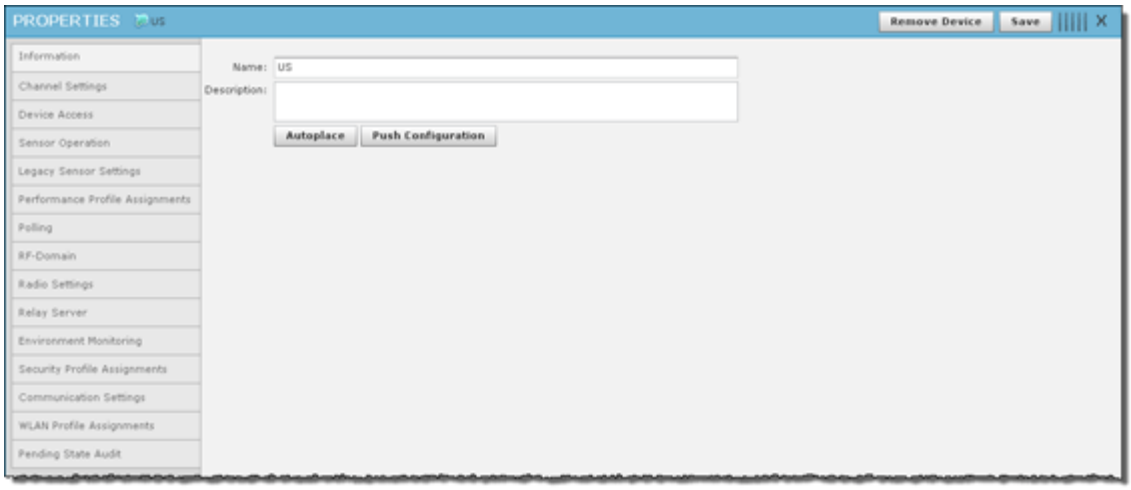
You can view and/or override an appliance's configuration by selecting:

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

- *Environment Monitoring*
- *Security Profiles*
- *Communication Settings Profile*
- *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 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 Profile*
- *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 8 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 AirDefense.

NOTE Each of these modules require a separate license.

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/mis-configured 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 enable 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 s 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).

Device Placement Considerations

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.

The sensors should be separated by at least 10 feet from any installed APs to avoid radio defense. 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 Requirements per Area

While a single ADSP 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 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 s 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 and Placement

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, contact Support for guidance 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.

Planning Your Sensor Placement

Sensor Placement using ADSP

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

You will need the following documents to help determine sensor placement:

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

You will need the following tools:

- A laptop running AirDefense Mobile 4.0, or later, or 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.
- Access to all areas to be monitored is required during the survey.

Procedure

Follow these steps to plan your sensor placement:

1. Obtain Maps/Layouts of the facility and determine the traversal plan.
2. Start AirDefense Mobile.
3. Turn on the target device (, soft , or laptop/PDA with wireless client card). AirDefense Mobile should detect the target device.
4. 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.
5. Use AirDefense Mobile Options to Lock On the channel on which the target device is discovered.
6. Right-click select the device in the Dashboard tree; select LiveView.
7. Focus on “Signal Strength” in the **Decode** tab in LiveView. Verify that the target device is being tracked by AirDefense Mobile.
8. 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 . The peaks are indicative of the effective signal strength relative to AirDefense Mobile.
9. Move the target device to the anticipated fringe where a neighboring sensor would become primary.
10. At the fringe of coverage, signal strength should be no less than -70 dBm to assure termination ability.
11. 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.

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 s and wireless clients they are protecting.

  For this requirement, you should leverage any site surveys you conduct or have conducted for placement of s as aids to sensor placement decisions. Another option is using a WLAN simulation tools such as 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 s 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 APs, or more specifically three 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. 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. To achieve accurate results, follow these guidelines:

- Place at least three independent sensors on the same floor plan so the system can capture the RSSI values.
- Place a sensor in each area where accurate resolution is required or to increase overall sensor density to ensure high RSSI values.

Considerations

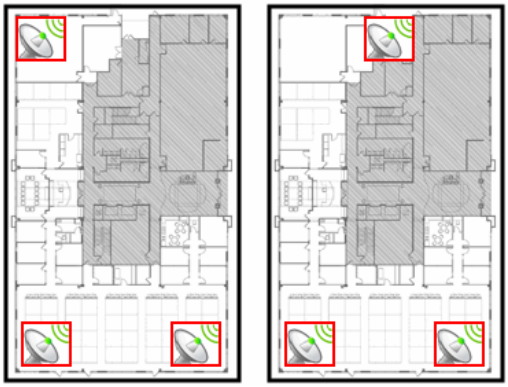
Every site is unique in terms of actual sensor coverage; this section merely describes sensor placement and respective coverage in a simplified way. Actual signal propagation is a very complex issue due to environmental factors like the reflection/absorption properties of materials (walls, furniture),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

Intrusion Detection System



With Location Tracking

Example 1

You have a small office of 10,000 sq. ft. For Wireless IDS/IPS you would only need 1 sensor; to maximize the coverage it makes sense to place the sensor in the center of the building. When location tracking is need 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:

NOTE Sensor monitoring profiles are described in detail in Chapter 7, *Configuration*, or in the **Configuration** tab (online Help).

- **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**

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.

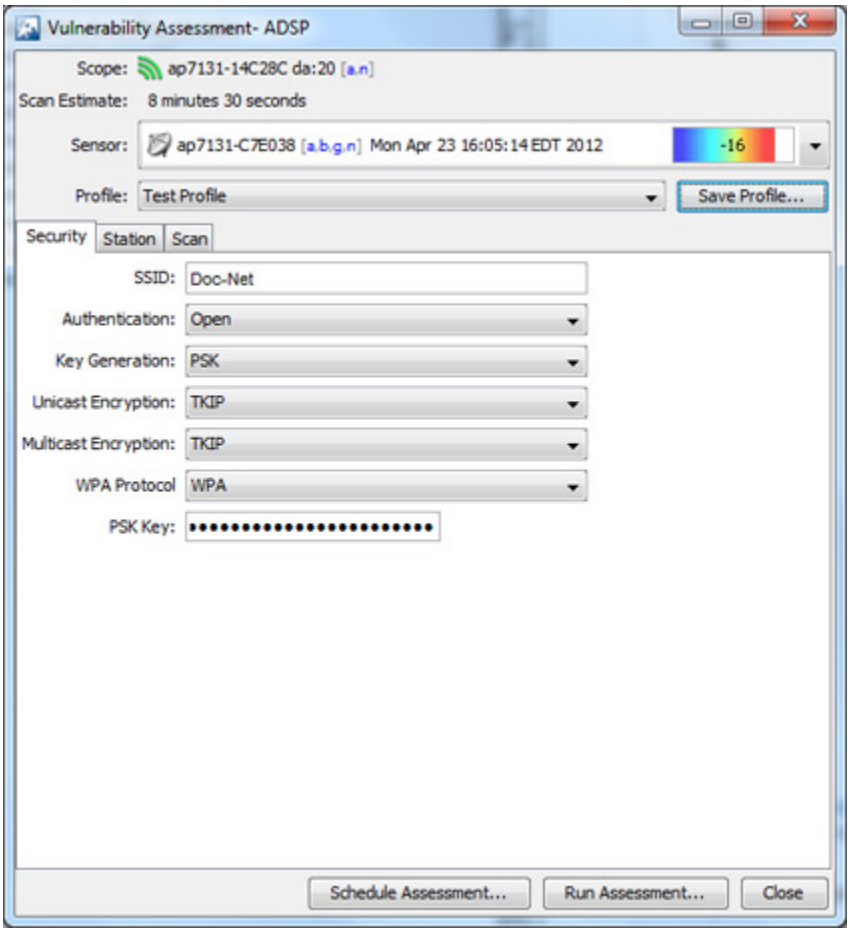
The assessment is accomplished by using deployed sensors as a wireless client to connect to an AP and scan network resources. Vulnerability Assessment can be run automatically or manually, providing proactive notification that network resources may be compromised.

NOTE Vulnerability Assessment is only supported on the legacy sensors M510 and M520 with firmware version 5.3 or later installed. Vulnerability Assessment is also supported on the AP650 and AP7131 sensors with WiNG 5.1 or later 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 drop-down menu button– for a BSS or network level, and select **Wireless Vulnerability Assessment**.

NOTE When the scope is network level, all APs in the scope are assessed.

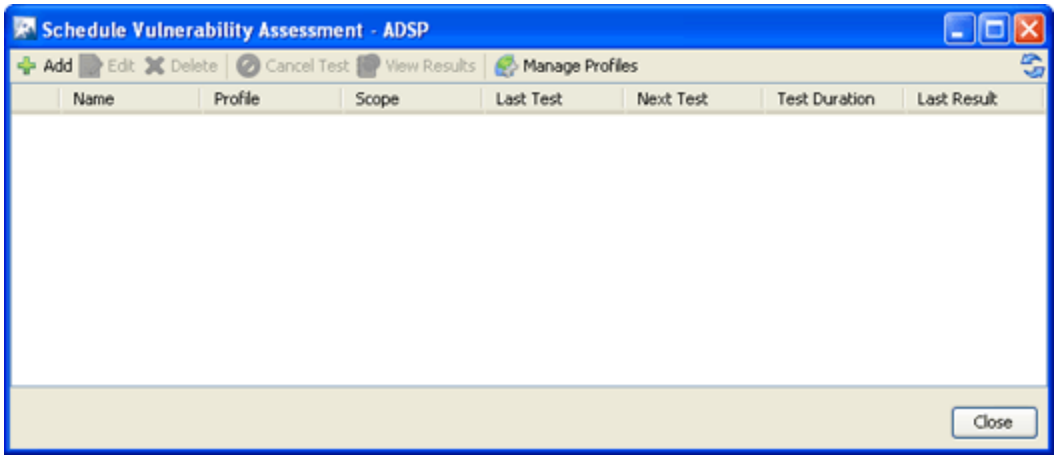


The **Vulnerability Assessment** window allows you to configure and run the assessment. After you have configured an assessment, you can save it as a profile. A profile can be selected later to run test on a similar scope.

For details on how to set up and run Vulnerability Assessments on demand, see the section on *On-Demand Vulnerability Assessment*.

Scheduled Vulnerability Assessment

Scheduled Vulnerability Assessments must be scheduled using the **Schedule Vulnerability Assessment** window. Navigate to **Menu** > **Scheduled Vulnerability Assessment**.



The **Scheduled Vulnerability Assessment** window displays a list of all scheduled assessments. From this 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.

For details on how to schedule Vulnerability Assessments and use the Schedule Vulnerability Assessment window, see the section *Scheduling AP Test or Vulnerability Assessment*.

WEP Cloaking

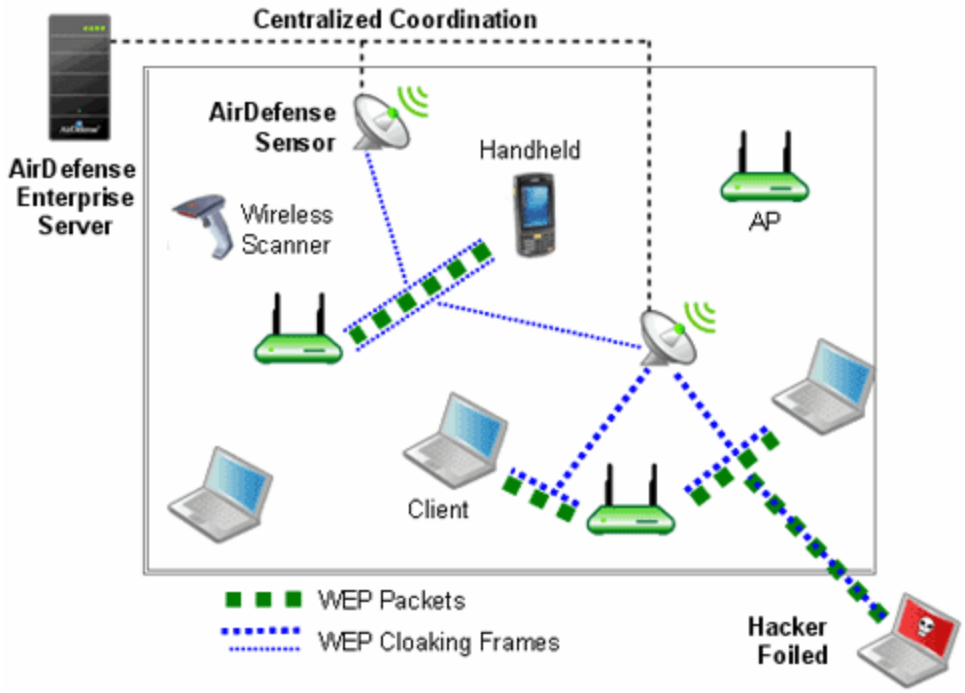
In order to extend the life of some older legacy equipment that only supports WEP encryption, AirDefense has implemented a feature known as WEP Cloaking. This technology injects “noise” into a WEP-protected environment by transmitting frames that appear to be sourced from valid devices but are encrypted 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 s it is protecting.

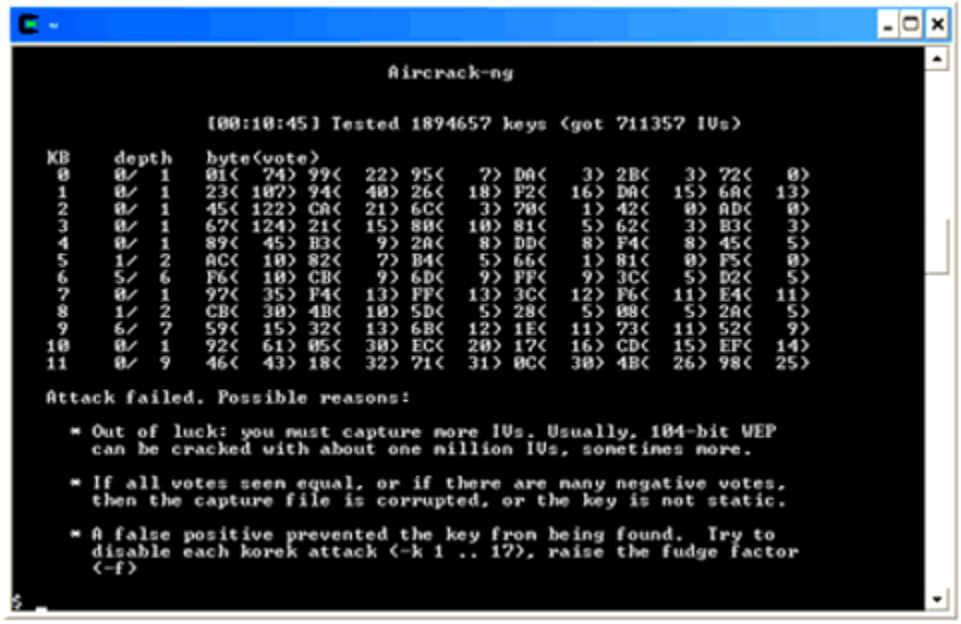
WEP Cloaking Overview

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.



Ongoing Cloaking Ability

In the event of a wired network outage, even 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.

Recommendations

- You should use a layered security approach to fortify your wireless network. 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 s 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 allowed data rates for each AP to ensure that unnecessary distant wireless associations do not provide wireless client access to the network through the AP. This would result in a low negotiated data rate.
  - If the AP is 802.11b/g and the WEP wireless clients require 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.

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**.

The 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 9 WLAN MANAGEMENT

Introduction

WLAN Management gives you the tools to configure wireless infrastructure devices regardless of device type or vendor. WLAN Management simplifies the WLAN configuration process by providing the same configuration interface for all wireless infrastructure devices, eliminating the need to understand the individual syntax for multiple vendors/device types.

A WLAN Management license gives you access to:

- Perform Device Configuration
- Automate Configuration Audit & Correction
- Monitor Device Health
- Receive Infrastructure Faults
- Collect Network Traffic Statistics
- Visualizing Network Topology
- Maintaining Consistent Configuration
- Monitoring and Prioritizing Critical Events
- Reporting on Network Health and Utilization.

In the **Configuration** tab of the GUI, the following **Infrastructure Management** features/functions are activated (unlocked):

- Device Firmware
- Channel Settings
- Radio Settings
- WLAN Profiles
- CLI Configuration.

Also, in the **Configuration** tab of the GUI, the Pending State Audit and the Relay Server features are activated, and added to the **Operational Management** and **Appliance Platform** categories.

Infrastructure Management

Infrastructure Management is used to configure devices so that they can communicate on your network.

Device Firmware

Device Firmware configuration allows you to upload new AP or sensor firmware from a workstation to a network server. Once the firmware is uploaded, you can upgrade your APs and/or sensors using ADSP.

Uploaded firmware images are listed by device type, version number, and image file name.

Use the **Upload Firmware Image** button to upload firmware.

Channel Settings

Use Channel Settings to select power and channel settings for the B/N/G radio and the A/N radio. The settings are applied to APs and wireless switches.

By default, Channel Settings are enabled, and are set for maximum power and automatic channel selection. The configuration fields for each radio are:

Setting	Description
Power (dBM)	Enter the maximum power value (in dBm) that APs and wireless switches must have. Default setting is 20 dBm.
Channel Selection	Select one of three options: • Automatic—ADSP automatically sets which channel is used. • Manual—Select a channel to use from the drop-down menu and then select the extension range (none, upper, or lower). • Random—ADSP randomly sets the channel Default setting is automatic.

Radio Settings

Radio Settings allow you to specify the radio settings used in your network. Using ADSP, you specify the supported rates and other settings for each radio. If a radio in your network is detected operating outside the set specifications, ADSP issues an alarm.

The settings apply to APs and wireless switches. You may also define a radio as a sensor. There are three possible radio configurations:

- B/G/N Radio
- A/N Radio
- 3rd Radio.

By default, Radio Settings are enabled, and all data rates are selected for both 2.4 and 5ghz radio settings. Use the individual radio tabs to configure each radio.

The configuration fields for each B/G/N Radio and the A/N Radio are:

Field	Description
Function	Defines the radio as a sensor or an infrastructure device (AP or wireless switch). You can also disable the radio.
Data Rates	Sets the data rates for the radios. You can set rates for 802.11 a/b/g as a group or 802.11 n.
DTIM Period	Specifies the supported Delivery Traffic Indication Message (DTIM) interval. The default value is 1.
RTS Threshold	Specifies the supported Request to Send (RTS) threshold. This can be a value between 0 and 2339 bytes. The default value is 2312.
Max Retries	Specifies the supported number of RTS retries. This can be a value between 1 and 128. The default value is 32.
Preamble	Specifies that the preamble is short or long.
Beacon Period	Specifies the supported beacon interval (period) in 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.

You may also specify the frame aggregation as A-MSDU, A-MPDU, or both.

WLAN Profiles

WLAN Profiles are used to configure the WLAN settings for devices utilizing your network. After creating a WLAN Profile using the **New Profile** button, it can be applied by selecting the profile and clicking the **Apply** button. When a WLAN Profile is applied to your system, if the WLAN thresholds for that profile are exceeded, a security alarm is generated. If there are no WLAN Profiles applied to your system, no alarms are generated. There are two tabs associated with WLAN Profiles: **General** and **Security**.

General Tab

The **General** tab is where you name your WLAN Profile and specify the general settings not related to security. Available fields are:

Field	Description
Name	Specifies the profile name.
Description	Allows you to specify a short description of the profile.
SSID	Specifies the Service Set Identifier (SSID) for devices.
Protocol	Specifies the protocol that the device can use [a, b, g, n (2.4 GHz), or n (5 GHz)].
VLAN	Specifies the Virtual Local Area Network (VLAN) the device is authorized to use.
Association Limit	Specifies the number of associations allowed per device.
Station Timeout	Specifies the number of seconds or minutes that a device has to become a sanctioned device.
Other Options	Specifies which of the following options may a device perform: • Respond to all probe requests • Broadcast SSID in Beacon • Wireless Client Isolation • Locally Bridged.

Security Tab

The **Security** tab is where you define the security aspects of your WLAN Profile. Available fields are:

Field	Description
Authentication	Specifies the type of authentication devices may use (**Open**, **Shared**, **WPA**, **WPA PSK**, **WPA2**, **WPA2 PSK**, or **Legacy EAP**).
Encryption	Specifies the type of encryption devices may use (**Static WEP**, **WEP64**, **WEP128**, **TKIP**, **CCMP**, or **Keyguard**). You may select one or more encryption types.

Field	Description
PSK	Specifies a pre-shared key (PSK) / password used by devices. The PSK may be ASCII or HEX.
WEP Keys	Specifies the WEP keys used to connect to the network. The WEP key may be ASCII or HEX. You may also elect to transmit the WEP key.
RADIUS Servers	NOTE This field is displayed only when the authentication method is WPA, WPA2, or Legacy EAP. Lists any RADIUS servers used in authentication. You can edit or delete a highlighted server by clicking the appropriate button. New servers may be added to the list by clicking the **New Server** button. You must supply the following information: • A name for the RADIUS Server Profile. • The IP address or host name of the RADIUS server. • The RADIUS server port used for communications. • The shared password of the RADIUS server. Select the **Display Passwords** checkbox if you wish the password to be displayed while typing it. • A protocol selected from the drop-down menu (**PAP**, **CHAP**, **MSCHAP**, or **MSCHAPv2**). • A timeout value and a time interval selected from the drop-down menu (**Seconds** or **Minutes**). • The maximum number of retries to connect to the RADUIS server.

CLI Configuration

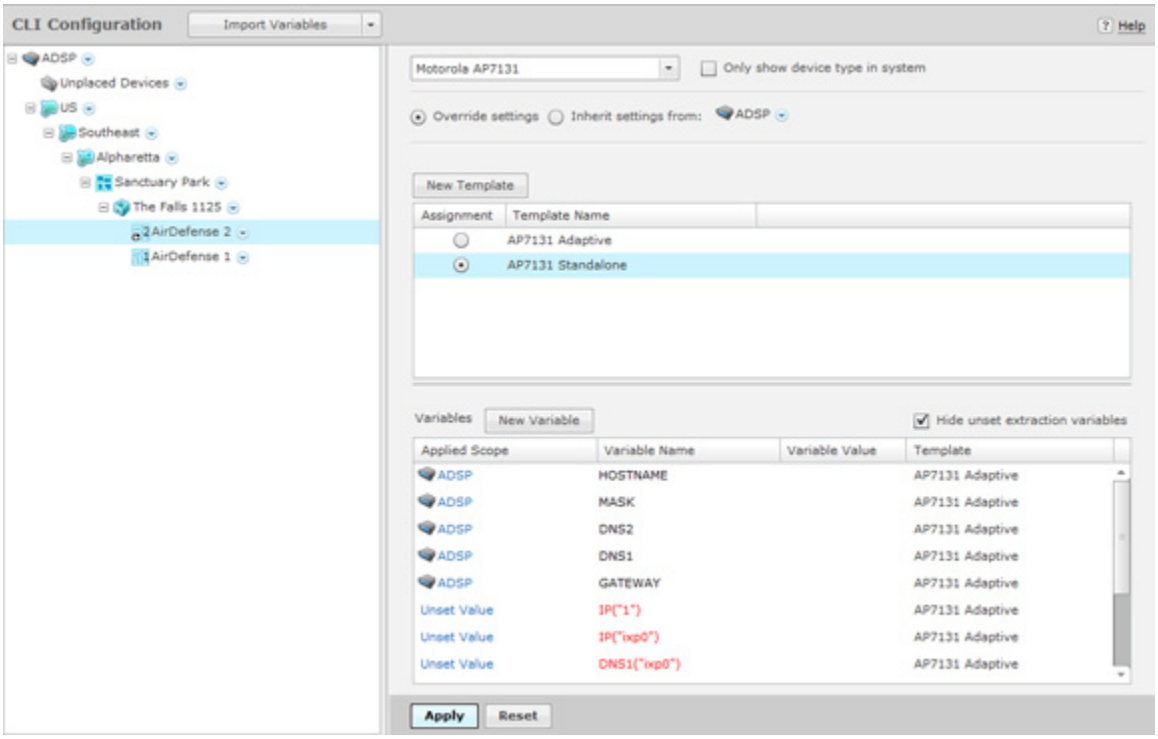
The Command Line Interface (CLI) for devices is a powerful tool that gives you direct access to APs and switches. The CLI commands can be used to configure and control how devices interface with your network.

AirDefense Services Platform uses the CLI to construct device profiles that can be used to control and manage devices in your network. You can push the CLI profiles out to devices in your network that ensure all devices in your network conform to your company policies.

AirDefense Services Platform creates and updates device configurations by revising the configuration files and their CLI command set. CLI profiles are created using configuration templates that you can use as is or change to meet the configuration requirements of your devices. Once a profile is created, you can apply it to any or all of the devices in your network. Devices are typically s and switches. The following devices are currently supported:

- Brocade BR v5.x
- Brocade BR51X1
- Brocade BR71X1
- Brocade BRX000
- Cisco Airespace

- Cisco Autonomous 12x0/11x00
- Extreme Networks AP35X0
- Extreme Networks AP47X0
- Extreme Networks EX v5.x
- Extreme Networks WM2000
- Extreme Networks WM3X00
- AP51X1
- AP650
- AP7131
- AP7181
- CB3000
- RFSX000
- WiNG v5.x
- WS2000
- WS5100.



Add a CLI Profile

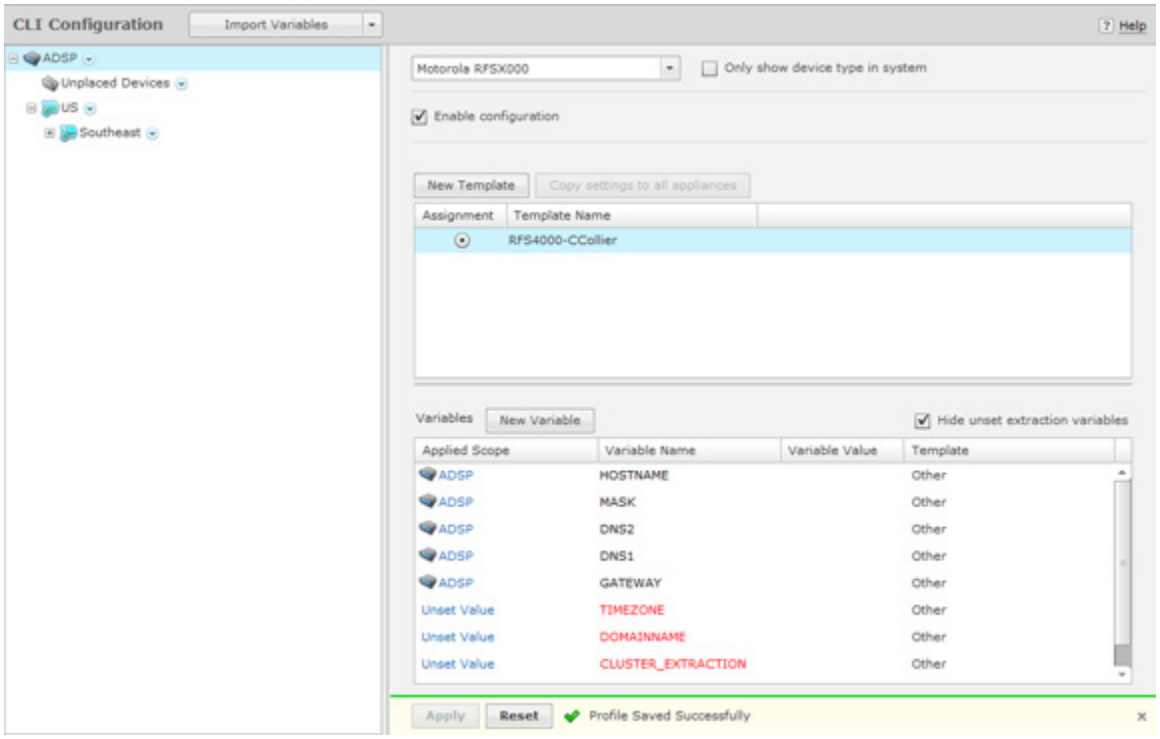
To create a new profile, select a device from the **CLI Configuration** drop-down menu and then click the **New Template** button. The following fields are available:

Field	Description
Name	This field is used to name your new profile.
Device Type	This field displays the device that was selected from the CLI Configuration drop-down menu. You cannot change the device once it has been chosen.
CLI Commands	Displays the CLI commands that are part of the selected template. These commands are editable. Be very careful when making changes. Only make changes to CLI commands if you have knowledge about the commands for the device associated with the template.

Apply a CLI Profile

After creating a CLI Profile, you must apply the profile to your network. Usually, you will have a CLI profile that can be used on a large majority of devices in your network. However, there will be times where you may need a special profile for a specific building or even a specific floor within a building.

If you have a CLI profile that works on a large majority of devices in your network, you should apply it at the appliance level. Then, if you have a special profile that fits the needs of a specific building or a specific floor in a building, you can override the appliance level profile and apply it to a lower network level.



To apply a CLI profile to a device type, select a device type from **CLI Configuration** drop-down menu.

If you want to apply the CLI profile to the appliance level, select the appliance level and then select the **Enable configuration** checkbox. Next, select the profile from the list of profiles. If there is only one profile, it is selected automatically. Click **Apply** to apply the selected profile to devices in the appliance level.

If you want to apply the CLI profile to a specific lower network level, select the lower network level and then select the **Override settings** radio button. Next, select the profile from the list of profiles. If there is only one profile, it is selected automatically. Click **Apply** to apply the selected profile to devices in the selected network level.

If you have a Central Management license and you want to use the same configuration on other ADSP appliances, you can copy configuration settings to all your managed appliances by clicking **Copy settings to all appliances**.

CLI Variables

Variables can be used in the CLI commands to get information (values) from other sources. They are global in nature and can be assigned to any network level. There are three types of variables: user-defined variables, extraction variables, and expansion variables.

User-defined variables are displayed in the **Variables** section. You can edit user-defined variables by selecting a network level from the tree and assigning values to one or more variables.

Use the **Variables** section to define configuration variances unique to the specific device parameters listed. For example, highlight the “Gateway” parameter and click under the **Device Value** column to display a field used to assign a unique Gateway address to this specific profile. Select and assign new default values as needed for each available profile.

New user-defined variables can be added to the **Variables** section by adding a variable in the CLI Commands section when creating a new profile or editing an existing profile. Use the following format:

$[VARIABLE_NAME]

Once a variable is added to the CLI Commands section and the profile is saved, its name is displayed in the **Variables** section with an empty default value. Only the following characters are supported in user-defined variables:

A-Z, a-z, 0-9, and _

Below is a list of current extraction variables and the associated device types they are applicable for:

- IP(iface)— All
- MASK(iface)—5131, 7131, WS2K, CiscoThick
- MASK—5131, 7131, WS2K
- GATEWAY—All
- GATEWAY(iface)—5131, 7131, WS2K
- HOSTNAME—All
- DOMAINNAME—RFS*, WS5100, CiscoThick
- DOMAINNAME(iface)—5131, 7131, WS2K
- DNS1—5131, 7131, RFS*, WS2K, WS5100

- DNS1(iface)—5131, 7131, WS2K
- DNS2—5131, 7131, WS2K
- DNS2(iface)—5131, 7131, WS2K
- WINS(iface)—5131, 7131, WS2K

Expansion variables are used to include information from profiles that are configured in ADSP. An expansion variable will always end with _EXPANSION. For example, $[WLAN_RADIO_CHANNEL_EXPANSION] is an expansion variable that includes configuration information from WLAN Profiles, Radio Settings, and Channel Settings.

The Status column displays the status of the variable (inherited, overridden, or removed).

- **Inherited**—Variable is inherited from a higher network level. The inherited level is displayed in this field.
- **Overridden**—Variable is overridden at the current network level.
- **Removed**—Variable is not used at the current network level. Removed variables are displayed in red text.

Operational Management

Pending State Audit is added to Operational Management as part of the WLAN Management module.

Pending State Audit

Pending State Audit is used to identify any devices that are in a pending state. Devices in a pending state have been scheduled or need to be scheduled for configuration.

Folders with a checkmark identifies that folder as having devices that in a pending state. Devices with a checkmark identifies that device as a device that are in a pending state.

You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later using **Job Status** under **Device Monitoring**. A list of device types along with the number of affected devices that will be updated is displayed. Also, if applicable, a list of unsupported settings is displayed.

Appliance Platform

Relay Server is added to Appliance Platform as part of the WLAN Management module.

Relay Server

Define or update the Relay Servers used to access managed devices. Relay Servers are FTP/TFTP servers that devices access to fetch configuration, firmware, and provisioning information. Use the Relay Server to set the configurations of both the Device Relay and Appliance Relay Servers.

NOTE You can use your appliance as the relay server. To do so, select the **Internal Relay Server** option.

Set the following values for **Device Relay Server (download)**:

- Enter the **Host** name of the relay server ADSP uses to access and fetch device configurations. Normally, this is the IP address of the relay server. This can be an internal relay server (your appliance) or an external relay server.
- Select a protocol from the drop-down menu (**FTP**, **TFTP**, **SFTP**, **SCP**, **HTTP**, or **HTTPS**). If you are using your appliance as the relay server, you can only use **FTP** or **SFTP**.
- Specify the **Path** ADSP uses to download information. You should either leave the path blank or use root (/). Use /pub if you are using your appliance as a relay server.
- Define the **Port** ADSP uses to connect to the Device Relay Server. If you are using your appliance as the relay server, use port 21 when **FTP** is the selected protocol or port 22 when **SFTP** is the selected protocol.
- Enter the **Username** needed to update the Device Relay Server used by ADSP.
- Enter the **Password** required to update the Device Relay Server used by ADSP.

If different than the Device Relay, set the following values for **Appliance Relay Server (upload)**:

NOTE Use the **Same as Device Relay Server** option if the Relay Server connection address and login credentials will always be the same for both the ADSP appliance and the device. The option to unsynchronized these configuration fields will only be needed in cases where the address of the Relay Server will depend upon whether it is being accessed by the device or the ADSP appliance. This type scenario will be encountered in network deployments where NAT'ing is utilized in such a way that the relay server address will depend upon where the accessing device is located on the network.

- Enter the **Host** name of the relay server ADSP uses to access and fetch device configurations. Normally, this is the IP address of the relay server. This can be an internal relay server (your appliance) or an external relay server.
- Select a protocol from the drop-down menu (**FTP**, **TFTP**, **SFTP**, **SCP**, **HTTP**, or **HTTPS**). If you are using your appliance as the relay server, you can only use **FTP** or **SFTP**.
- Specify the **Path** ADSP uses to upload information. You should either leave the path blank or use root (/). Use /pub if using your appliance as a relay server.
- Define the **Port** ADSP uses to connect to the Appliance Relay Server. If you are using your appliance as the relay server, use port 21 when **FTP** is the selected protocol or port 22 when **SFTP** is the selected protocol.
- Enter the **Username** needed to update the Appliance Relay Server used by ADSP.
- Enter the **Password** required to update the Appliance Relay Server used by ADSP.

Import Relay Server Information

You can import relay server information using the **Import Parameters** button. Comma delimited files are used to import relay server information. The format of the file is:

relay_params,server,folderpath,deviceHost,deviceProtocol,devicePath,devicePort,deviceUsername,
devicePassword,applianceHost,applianceProtocol,appliancePath,appliancePort,applianceUsername,
appliancePassword

NOTE Although the above format is shown on multiple lines, each import entry must be one line with no line breaks or carriage returns.

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

Things to Remember:

- The first field for importing relay server information must be relay_params.
- At this time, the only valid server name is localhost.
- Servers must be specified in pairs. You must specify a Device Relay Server and an Appliance Relay Server in one entry.
- If the server information is the same, you still must enter information for both servers. Also, if the information for both relay servers match, the **Same as Device Relay Server** checkbox is selected in the GUI after the import.
- Normally, you will supply a username and password. However, when using the TFTP protocol, the username and password fields can be left blank with no blank space between the commas (i.e., ,,).
- deviceHost designates the IP address of the host.
- deviceProtocol designates the protocol to use for communications. Valid protocols are FTP, TFTP, SFTP, SCP, HTTP, or HTTPS. These are the same protocols listed in the Protocol drop-down menu of the GUI.
- folderpath designates the network level path and must included a slash (/) at the beginning of the path and between network levels. Also, the path must already be present in the existing network tree. To specify an appliance level, just enter the appliance name.
- devicePath and appliancePath designate the path where the configuration file is located on the individual servers.
- devicePort and appliancePort designate the port to use for communications.

Examples:

relay_params,localhost,/ADSP,172.17.0.80,ftp,/,21,anonymous,anonymous,172.17.0.80,ftp,/,21,anonymous,anonymous

relay_params,localhost,/US/Southeast/AirDefense,172.17.0.80,ftp,/,21,anonymous,anonymous,172.17.0.80,ftp,/,21,anonymous,anonymous

relay_params,localhost,/relay_test,172.17.0.80,tftp,/,69,,,172.17.0.85,ftp,/,21,anonymous,anonymous

If you have a Central Management license, you can copy the Relay Server configuration to all your appliances.

CHAPTER 10 CENTRAL MANAGEMENT CONSOLE

Introduction

The Central Management Console (CMC) is a centralized management system that allows you to administer multiple AirDefense appliances from one location. CMC can be used to ensure that configurations are the same across multiple appliances. You no longer have to configure each appliance separately.

The CMC application is bundled with the Enterprise application but runs as a separate client-side application. CMC has its own login interface that is separate from the Air Defense Enterprise.

Configuring Master/Slave Servers

You should designate one server as the master server and then add the slave servers. You can then maintain configuration changes from the master server and have them take effect across all server appliances. You can make changes to:

- Alarm Configurations
- User Accounts
- Authorized Stations.

Things to Remember

- All the configuration is done on the master server. No configuration is necessary for the slave server(s).
- Changes made to a master server will be automatically synchronized with the slave servers; however, changes made to slave servers are not synchronized with the master server.
- Any changes made to configurations using CMC will override configuration settings on the slave devices.

Sharing Certificates

In order for the slave server to work properly, you must share the Central Management license from the master server to the slave server(s) by following these steps:

1. From the master server ADSP dashboard, right-click the slave server and select the **Share Certificates** option. A pop-up displays.
2. Fill in the required fields and click on **Share**.
3. When you have completed these steps, restart both the master and the slave servers.

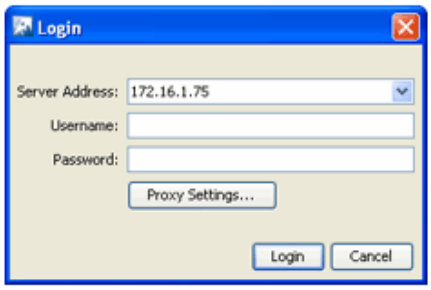
NOTE The default password is “security” for both the master and slave appliances.

Sometimes the slave appliance will show as off-line even after a restart of the ADSP processes. In this case, remove the slave appliance and try adding it again.

Log in to CMC

Follow these steps to log in to the CMC:

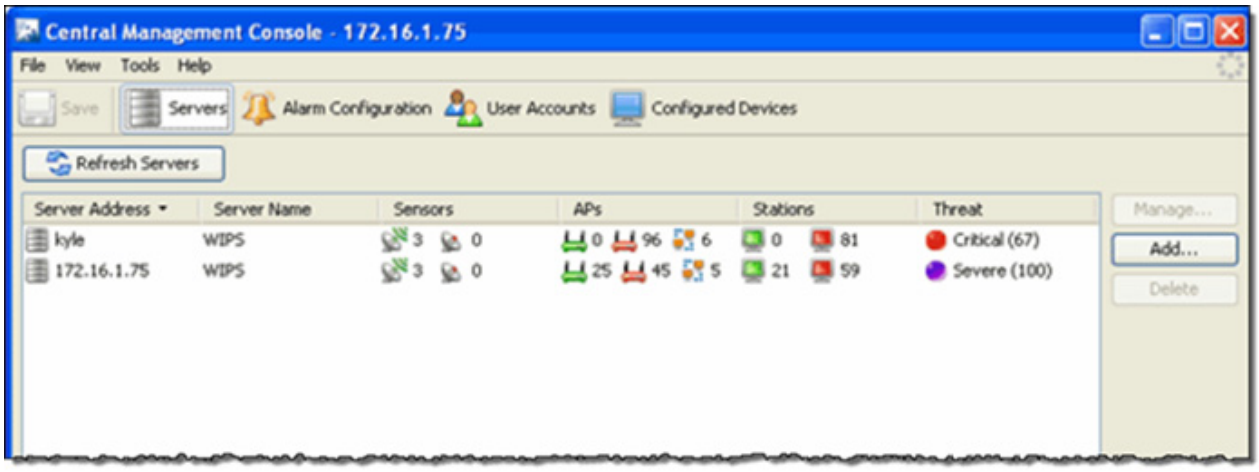
1. Using windows explorer, navigate to c:\Program Files\AirDefense\Enterprise.
2. Double-click on the Air DefenseCMC.exe file. The Login window displays:



3. Type in your server address (or DNS name). If your server address is displayed, you do not need to type it. Also, if it is listed in the drop-down menu, just select it.
4. Type in your Username and Password.

NOTE You must be a user with administrative privileges to log in to CMC.

5. Click **Login**. Once you have successfully logged in, the CMC main window displays.



Menus

File Menu

Table 10-1

Menu Option	Description
Save	Saves configuration changes that have not been applied to the managed servers.
Exit	Closes and exits out of the AirDefense CMC.

View Menu

Table 10-2

Menu Option	Description
Task Status	Opens the *Task Status Window* where you can view status history.
Servers	Opens the CMC view for *Servers* where you can configure servers that you want to manage.
Alarm Configuration	Opens the CMC view for *Alarm Configuration* where you can configure alarms.
User Accounts	Opens the CMC view for *User Accounts* where you can configure user accounts.
Configured Devices	Opens the CMC view for *Configured Devices* where you can configure devices.

Tools Menu

Table 10-3

Menu Option	Description
Search Devices	Searches your managed servers for devices.
Compare Policies	Compares policies on your managed servers to check for differences.
Retrieve Logs	Retrieves log files from your managed servers and saves them to a local directory (folder) on your work station.
Upload Service Module	Uploads Enterprise Service Modules to your managed servers.

Help Menu

Table 10-4

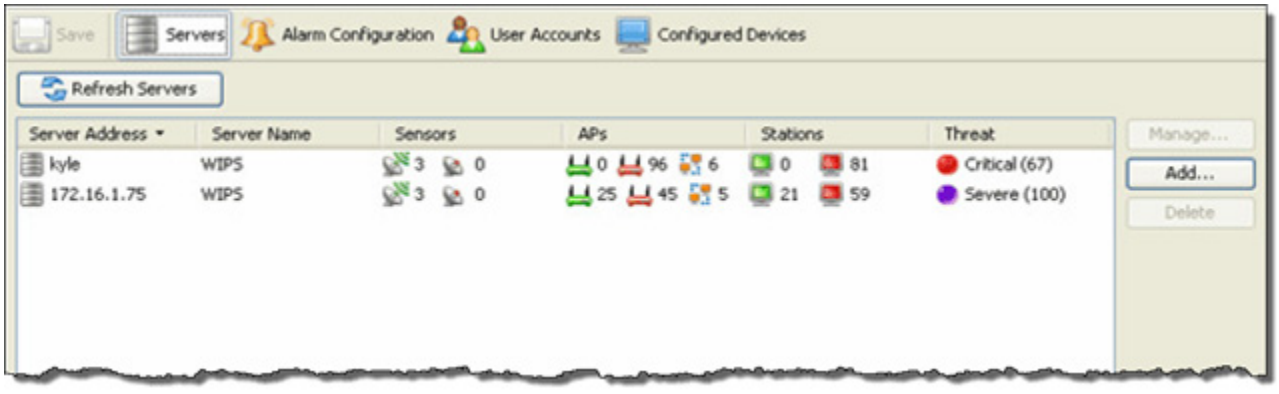
Menu Option	Description
Help contents	Opens the AirDefense CMC online help.
Icon Key	Opens a PDF document that consolidates icon graphics used in AirDefense into one convenient source.
Glossary	Opens a PDF document that lists computer and wireless Internet terminology and acronyms that pertain to AirDefense Enterprise.
About	Opens the About this Application sub-window and lists the Enterprise build version number.
Support	Opens the Support sub-window and provides the following information: • Hyperlink to the support center to open or view known issues and cases • Call Center Support phone numbers • Email address • Home website for Air Defense.

Configuration Views

The CMC has four configuration views: servers, alarm configurations, user accounts, and configured devices. (These are described in details in the following sections.) Using the configuration views you can change configurations for all your servers from one location.

Servers

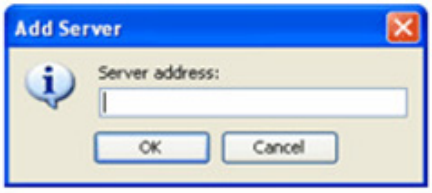
This view of CMC displays a list of servers managed by CMC. From this screen you can add servers, delete servers or manager server configurations.



Adding a Server

To add a server to the list, follow these steps:

1. Click **Add**. The **Add Server** pop-up window displays.



2. Type in the server address (or valid DNS name) and click **OK**. The server now appears ion the list of servers.

Deleting a Server

To delete a server from the list, select (highlight) the server and click **Delete**, or right-click on a highlighted server name and click **Remove Server**.

Managing Server Activities

The server view also gives you a snapshot of certain activities on the server. The following information is displayed:

Table 10-5

Column	Description
Server Address	The IP address of the server or DNS name as described by your DNS server.
Server Name	The name of the server.
Sensors	The number of active and inactive sensors that are configured for the server.
APs	The number of authorized and unauthorized APs that the sensors on a particular server have detected in your network.
Stations	The number of authorized and unauthorized stations detected on your network, and the number of Ad-Hoc networks detected.
Threat	The aggregated threat level detected.

You can access the Enterprise GUI for a server by selecting (highlighting) the server and clicking **Manage**. You can also right-click on the highlighted server name and select **Manage Server** from the list of options.

Refreshing a Server

To refresh a server, select (highlight) the server name(s) and click **Refresh Servers**, or right-click and select **Refresh Servers** from the list of options.

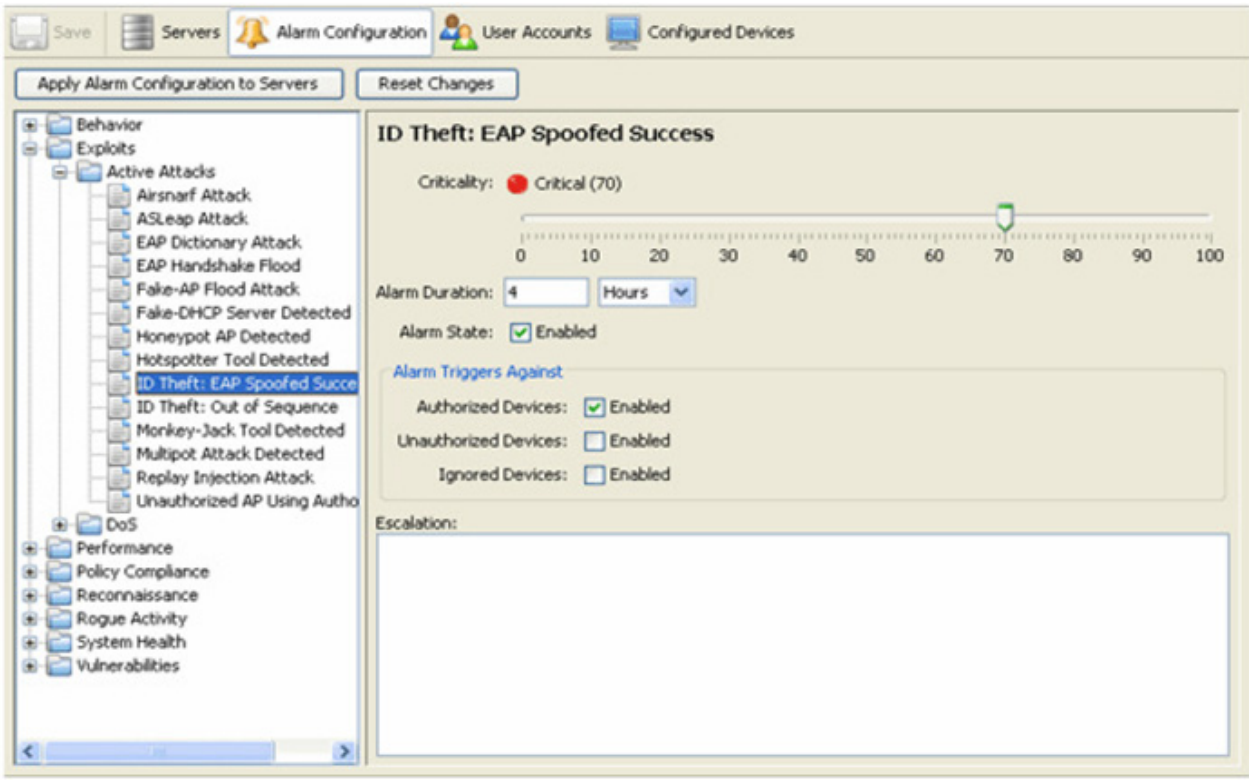
Server Errors

There are times when you will get a server error. See the following example:

Notice the first server. It has an orange **x** in the bottom right corner of the server icon. This indicates an error. If you move your cursor over the server icon, you will see an error message; in this case, the message is “Software version mismatch.” No data is displayed for this server. Also you can open the *Task Status Window* and look at the task history to see the error.

Alarm Configuration

This view of CMC allows you to edit and push alarm configurations to your managed servers.



The following alarms can be configured:

Table 10-6

Criteria (Field)	Description
Criticality	Adjusts the criticality level of the alarm from 0 to 100 (low to severe). The higher the number, the higher the criticality level. Use the slider to adjust the level.
Alarm Duration	Specifies how long an alarm will last (in minutes and hours). Type in a value and then select **Minutes** or **Hours** from the drop-down menu.
Alarm State	Enables or disables the alarm state. A checkmark indicates the alarm is enabled.
Authorized Devices	Enables or disables an alarm trigger for authorized devices. A checkmark indicates the alarm is enabled.
Unauthorized Devices	Enables or disables an alarm trigger for unauthorized devices. A checkmark indicates the alarm is enabled.
Ignored Devices	Enables or disables an alarm trigger for ignored devices. A checkmark indicates the alarm is enabled.
Escalations	Describes the escalation procedure to follow if the alarm occurs.

To change a configuration:

1. Use the tree to drill down to the alarm.
2. Select the alarm by highlighting it.
3. Change the criteria as described in the above table.
4. Click **Apply Alarm Configuration to Servers**.

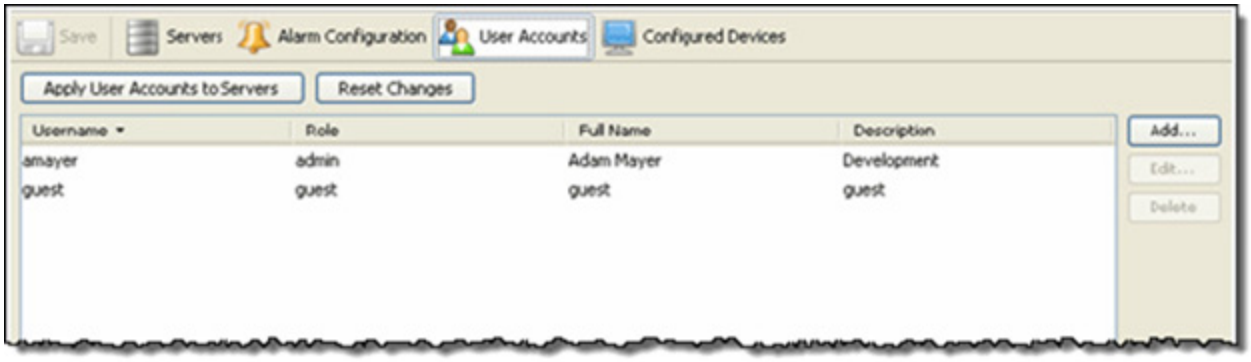
NOTE You can reset the configuration to it previous settings by clicking **Reset Changes**.

If you are making extensive changes and you want to apply the changes later, click **Save**. This will save your changes until your are ready to apply them, even if you close CMC. You can return later and finish making changes, and then click **Apply Alarm Configuration to Servers**.

NOTE If you make changes and do not apply or save them, you are prompted to save your changes when you exit CMC.

User Accounts

This view of CMC allows you to edit and push user account information to your managed servers.



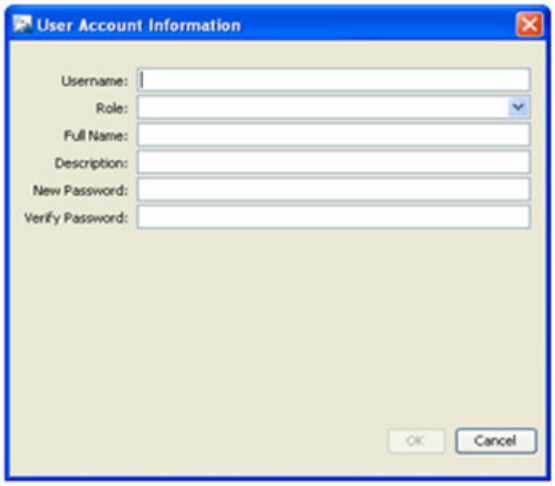
The following account information is displayed and can be configured:

- Username—user account name.
- Role—role of the user.
- Full Name—full name of the user.
- Description—description to help identify the user.

NOTE AirDefense recommends that you do not user CMC to manage user accounts in conjunction with user domains.

Add a User Account

From the **User Accounts** screen, click **Add** to add a new user account. The **User Account Information** window displays.



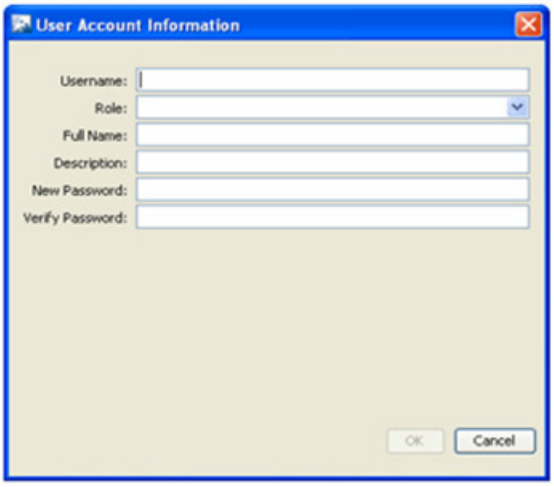
1. Type in the Username, Role, Full Name and Description.
2. Type in a new password and then enter it again in the **Verify Password** field.
3. Click **OK**. The user account now appears in the list of user accounts.

4. Click **Apply User Accounts to Servers** to apply your changes to your managed servers.

NOTE You can reset the configuration to its previous settings by clicking **Reset Changes**.

Editing a User Account

From the **User Accounts** screen, select the user account by highlighting it. Click **Edit**, or right-click the highlighted user account and select **Edit Account**. The **User Account Information** window displays.



1. Make any necessary changes.
2. Type in the password and then enter it again in the **Verify Password** field.
3. Click **OK**. The changed information is displayed in the user account(s).
4. Click **Apply User Accounts to Servers** to apply your changes to your managed servers.

Deleting a User Account

To delete a user account, select (highlight) the user account name and click **Delete**, or right-click on a highlighted user account and click **Delete Account.** You will be prompted to reaffirm your deletion.

Configured Devices

This view of CMC allows you to edit and push device configuration information to your managed servers. The devices are limited to wireless stations, as these are more likely to move to other locations managed by a different WIPS server.

The following account information is displayed and can be configured:

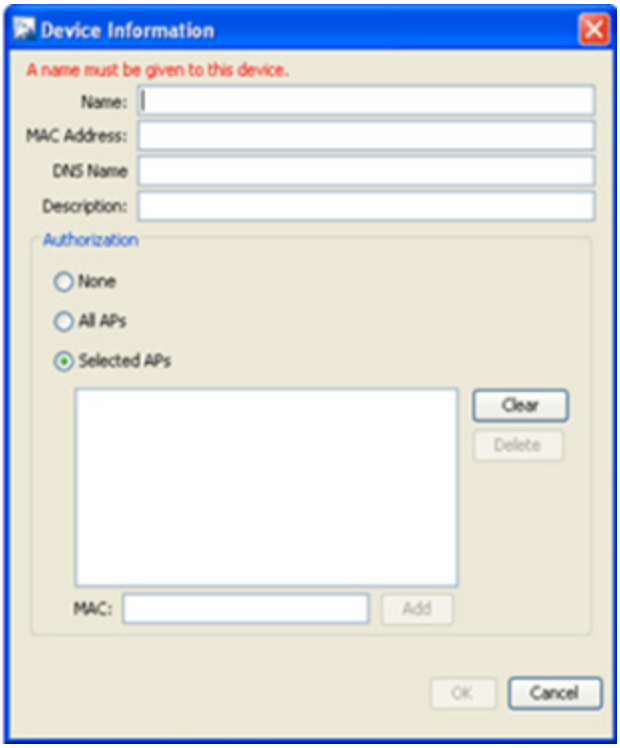
- Name—Name of the device.
- MAC—MAC address of the device.
- DNS Name—Name if the device as described by the DNS server.
- Authorization—List of APS that Station is authorized to access.
- Description—Description to help identify the device.

Add a Device

When adding a device, 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 master and slave appliances are able to connect with each other through the network.
- Ensure that master and slave appliances do not have a time lag of more than 10 minutes when connecting.
- 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.

From the **Apply Configured Devices to Servers** screen, click **Add**. The Device Information window displays.



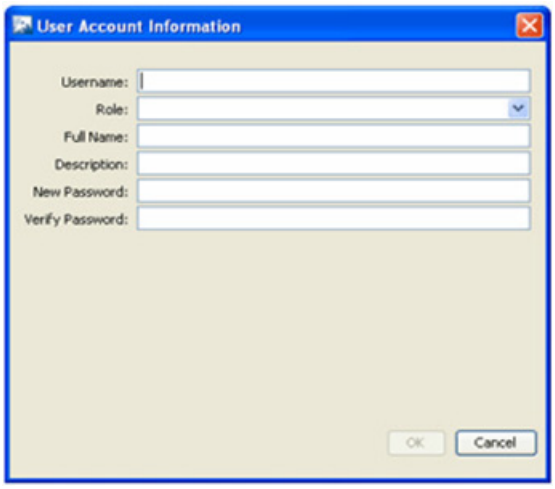
1. Type in the Name, MAC Address, DNS Name and Description.
2. If the device is a Station, select one of the following options: **None**, **All APs** or **Selected APs**.
   - None
   - All APs
   - Selected APs
3. Click **OK**. The device now appears in the list of devices.
4. Click **Apply Configured Devices to Servers** to apply your changes to your managed servers.

NOTE You can reset the configuration to its previous settings by clicking **Reset Changes**.

Editing Device Information

From the **Apply Configured Devices to Servers** screen, select the device by highlighting it.

Click **Edit**, or right-click the highlighted device and select **Edit Device**. The **User Account Information** window displays.



1. Change the criteria as necessary.
2. Type in the password and then enter it again in the **Verify Password** field.
3. Click **OK**. The changed information is displayed in the user account(s).
4. Click **Apply User Accounts to Servers** to apply your changes to your managed servers.

NOTE You can reset the configuration to its previous settings by clicking **Reset Changes**.

Deleting a Device

To delete a device from the list, select (highlight) the device and click **Delete**, or right-click on the selected device and click **Delete Device**. You will be prompted to confirm your deletion.

Importing a Device

A station definition file can be used to import multiple stations into the CMC. You must use a specific file format for importing wireless stations. Any file that is not in the correct format will be rejected. Follow these steps to import a station definition file:

1. Click **Import**. A Windows Explorer window displays.
2. Navigate to the folder where your station definition file is located.
3. Select (highlight) the station definition file and click **Open**. The device information is imported into the CMC and is displayed in the list of devices.
4. Click **Apply Configured Devices to Servers** to apply your changes to your managed servers.

Save Option

If you are making extensive changes and you want to apply them later, click **Save** to save your changes until you are ready to apply them. Even if you close CMC, you can return later and finish making changes. When all changes are complete, click **Apply User Accounts to Servers**.

NOTE If you make changes and do not apply them you will be prompted to save your changes when you exit CMC.

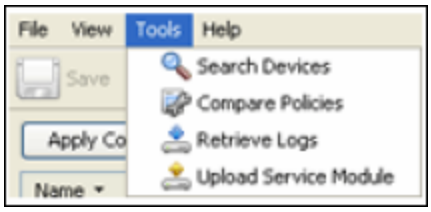
CMC Tools

The CMC includes the following tools.

- *Searching for Devices*
- *Comparing Policies*
- *Retrieving Logs*
- *Uploading the Service Module.*

For more information on each tool, click the link shown above.

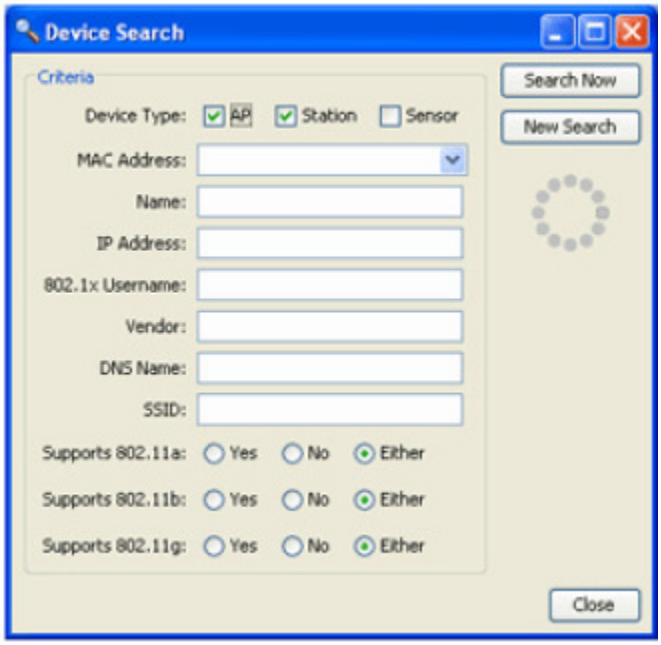
You can find the tools in the Tools menu.



Each tool is discussed in detail under the Tools folder.

Searching for Devices

The Search Devices tool lets you search for devices on any of your managed servers. Click **Tools** > **Search Devices** to access this tool. The **Device Search** window displays.



You can search for a device by the following criteria:

Table 10-7

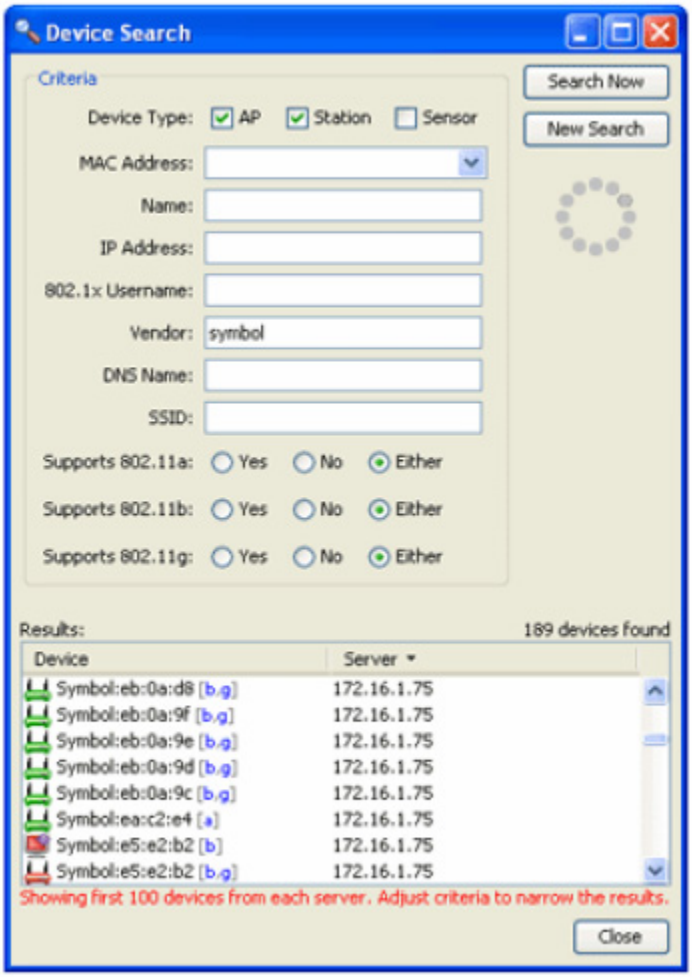
Criteria	Description
Device Type	Search for any combination of APs, stations or sensors.
MAC Address	Search for a particular device by MAC address. Select an address from the drop-down list.
Name	Search for a specific device by a user-selected name.
IP Address	Search for a specific device by IP address.
802.1x Username	Search for a specific device by its 802.1x username.
Vendor	Search for a specific device by its manufacturer.
DNS Name	Search for a specific device by DNS name, if you are using a DNS server (optional.)
SSID	Search for a specific device by its SSID.

Table 10-7

Criteria	Description
Supports 802.11a	Select one of the following options: • **Yes** if the device supports the 802.11a protocol. • **No** if the device does not support the 802.11a protocol. • **Either** if it does not matter.
Supports 802.11b	Select one of the following options: • **Yes** if the device supports the 802.11b protocol. • **No** if the device does not support the 802.11b protocol. • **Either** if it does not matter.
Supports 802.11g	Select one of the following options: • **Yes** if the device supports the 802.11g protocol. • **No** if the device does not support the 802.11a protocol. • **Either** if it does not matter.

To execute a search, set one or more of the search criteria and then click **Search Now**. The following image shows the results of a search using the following criteria:

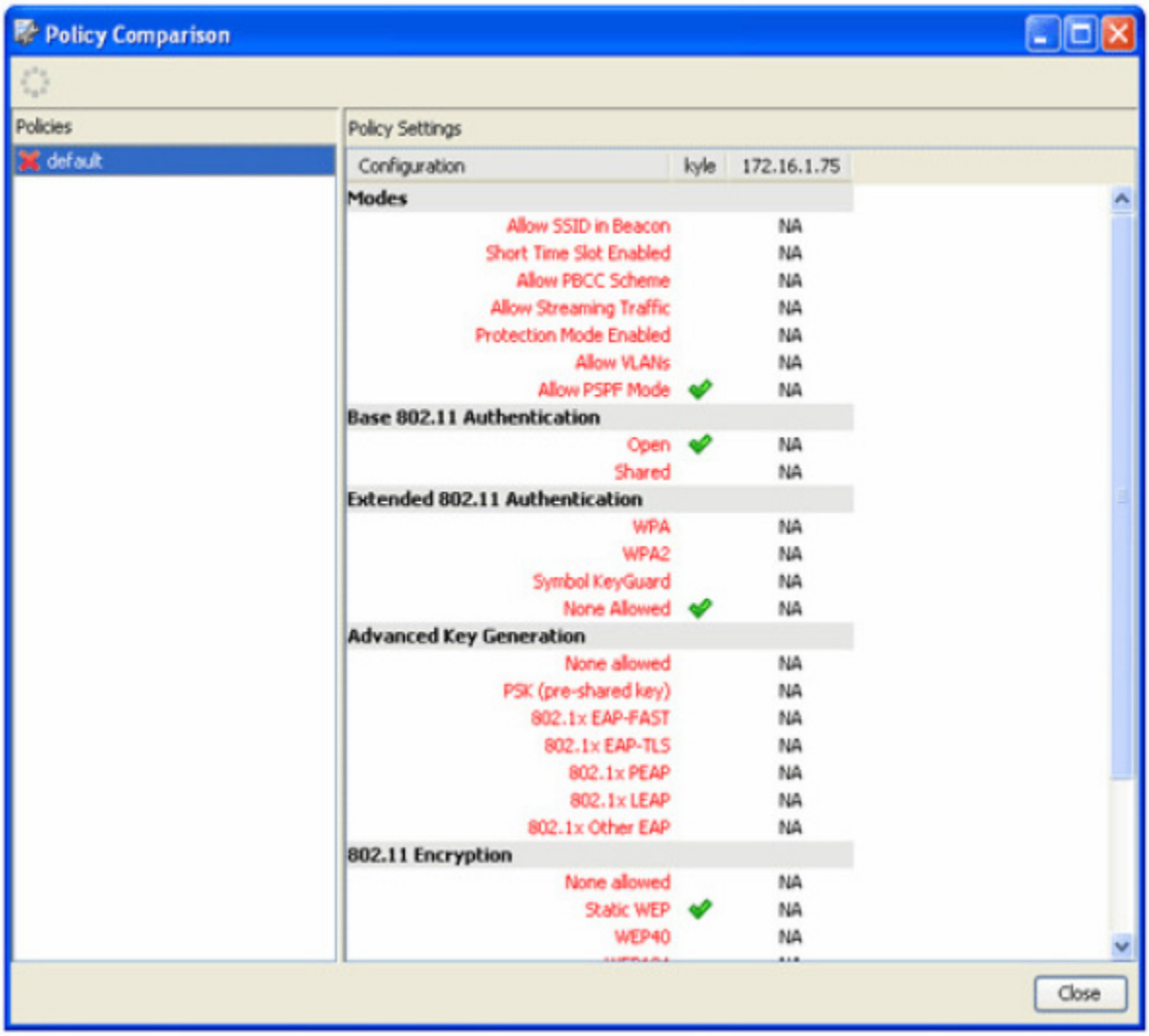
- Device Type: **AP** and **Station**
- Vendor: **Symbol**
- Supports 802.11a: **Either**
- Supports 802.11b: **Either**
- Supports 802.11g: **Either**



The Results window displays all devices that fit the search criteria. You can click **New Search** to reset the fields and enter new criteria. Click **Close** to exit the Device Search window.

Comparing Policies

The Compare Policies tool loads all configuration policies for your managed servers and checks to see if there are any discrepancies in wireless policy settings between different managed servers. Once you know which policies are different, you can use the Configured Devices view to make the policies the same across all your managed servers. Click **Tools** > **Compare Policies** to access the tool. The **Policy Comparison** window displays.

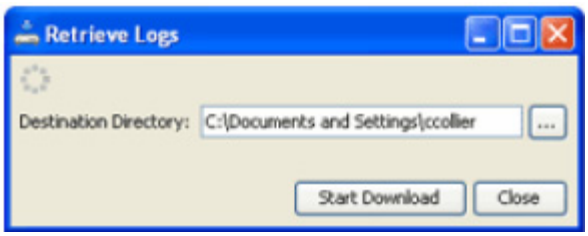


A red ***x*** indicates that you have discrepancies in wireless policy settings among your managed servers. A green checkmark ✔ indicates that there are no discrepancies in wireless policy settings. Click **Close** to exit the Policy Comparison window.

Retrieving Logs

The Retrieve Logs tool gives you a means to download log files from your managed servers to a local directory (folder) on your workstation. Once you have the files in a local folder you can view

them at your leisure. Click **Tools** > **Retrieve Logs** to access the tool. The Retrieve Logs pop-up displays.



You can save the log files to the default location displayed or you can click ... to open Windows Explorer and navigate to a directory (folder). Once you have selected a directory (folder), click **Open** to place the directory name in the Destination Directory field. Click **Start Download** to download the log files.

NOTE Since you are retrieving log files from all the your managed servers, it may take some time to complete the download. You can check the Task History in the Task Status Window to monitor the progress of the download.

The log files will be placed in a ZIP file (logs.zip) in a directory (Folder) located in your download directory. The directory name will have the format server IP address. Any errors can be viewed in the cmc.log file in the default Destination Directory.

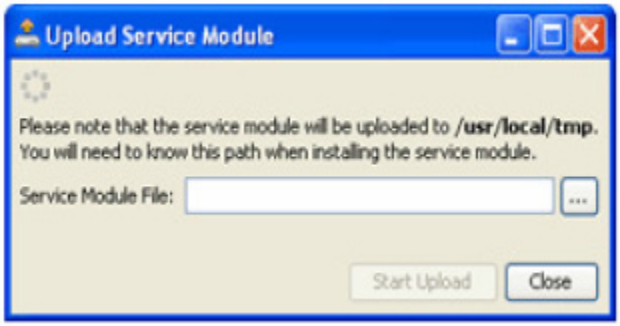
Click **Close** to exit the Retrieve Logs pop-up.

Uploading the Service Module

The Upload Service Module tool lets you upload an Enterprise Service Module to all your managed servers at once.

NOTE Once the service module is uploaded, you will still have to install it on each server individually.

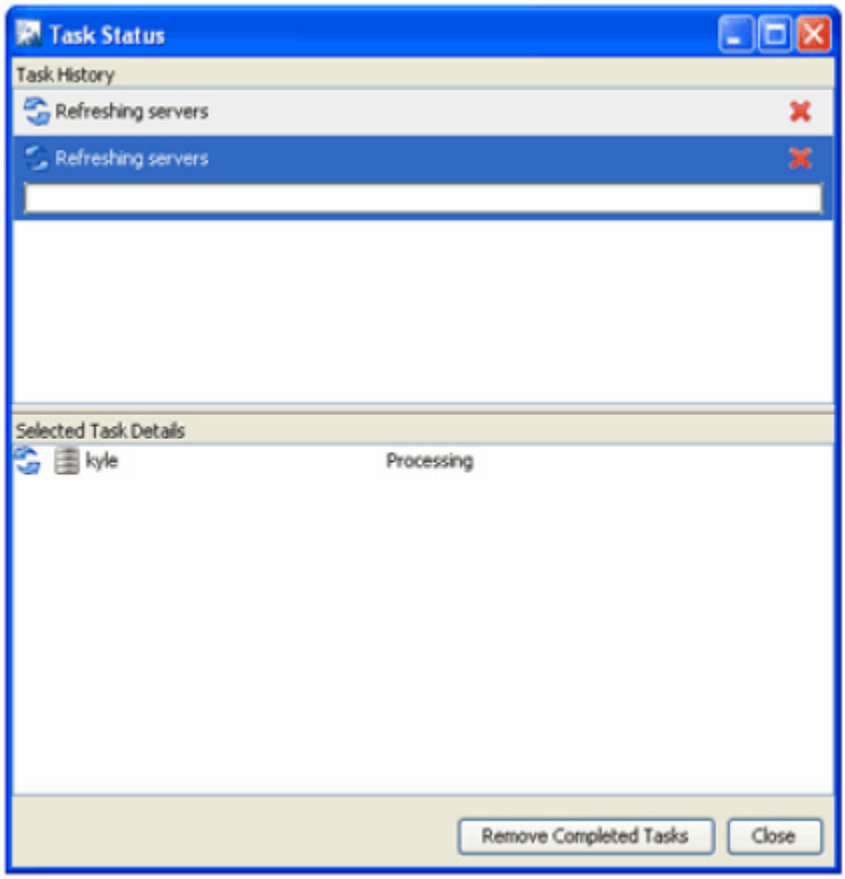
Click **Tools** > **Upload Service Module t**o access this tool. The Upload Service Module window displays.



Click on the navigation button ... to open a window where you can navigate and select the service module that you wish to upload. Once the service module is selected, click **Open** to place the file in the **Service Module File** field. Click **Start Upload** to upload the service module. The service module is uploaded to /usr/local/tmp on your managed servers.

Task Status Window

Some of the tasks that you initiate in the CMC may take some time to complete, depending on appliance and network activities. The Task Status window gives you task status information so you can track when the tasks are complete. To display the Task Status window from any view, click the Task Status button or click **Views** > **Task Status**. The Task Status window displays.



To see a task status, select (highlight) a task in the Task History. The status is shown in the Selected Task Details window. You can cancel a task by clicking the red ***x*** to the right of the task.

Completed tasks will remain in Task History until you exit the CMC. You can remove a completed task by selecting (highlighting) the task and then clicking **Remove Completed Tasks**.

Click **Close** to exit the Task Status window.

CHAPTER 11 ADSPADMIN

Introduction

When you are performing the initial ADSP configuration, you will need to use the **ADSPadmin** utilities in the Command Line Interface (CLI). Once ADSP is set up, use the GUI for ongoing configuration. The functions provided in ADSPadmin are:

- Manage
- Dbase
- Software
- Config.

Using ADSPadmin to Configure ADSP

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 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.

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.

1. Type **netport**, then press <**Enter**> at the prompt. The **Netport configuration** screen opens, displaying the current network interface configuration.
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.
2. 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.)
3. Press <**Enter**>. You are prompted to enter a time in 24-hour HHMM or HHMMSS format.
4. Press <**Enter**>. You are prompted to save your changes.
5. 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 changes.
4. Type **yes** and press <**Enter**> to save your changes (or **no** to disregard your changes). 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. 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 changes.
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. An 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 changes.
4. Type **yes** and press <**Enter**> to save your changes (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 changes.
4. Type **yes** and press <**Enter**> to save your changes (or **no** to disregard your changes).
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	Resets the administrator password back to the system default.
PASSWD	Change the password of a Command Line User (**smxmgr** and **smxarchive**).
RESTART	Restart ADSP processes (*not a full reboot!*)
REBOOT	Reboot ADSP appliance (*full reboot.*)
HALT	Halt ADSP (*stop processes.*)

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.

CHAPTER 12 TROUBLESHOOTING AND CUSTOMER SUPPORT

Introduction

ADSP provides modules and solution packages to assist you in troubleshooting your network. The individual modules are:

- AP Testing
- Connection Troubleshooting
- Live RF
- Spectrum Analysis.

The available solution packages are:

- Advanced Forensics
- Advanced Troubleshooting
- Assurance Suite (Network Assurance).

AP Testing

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.

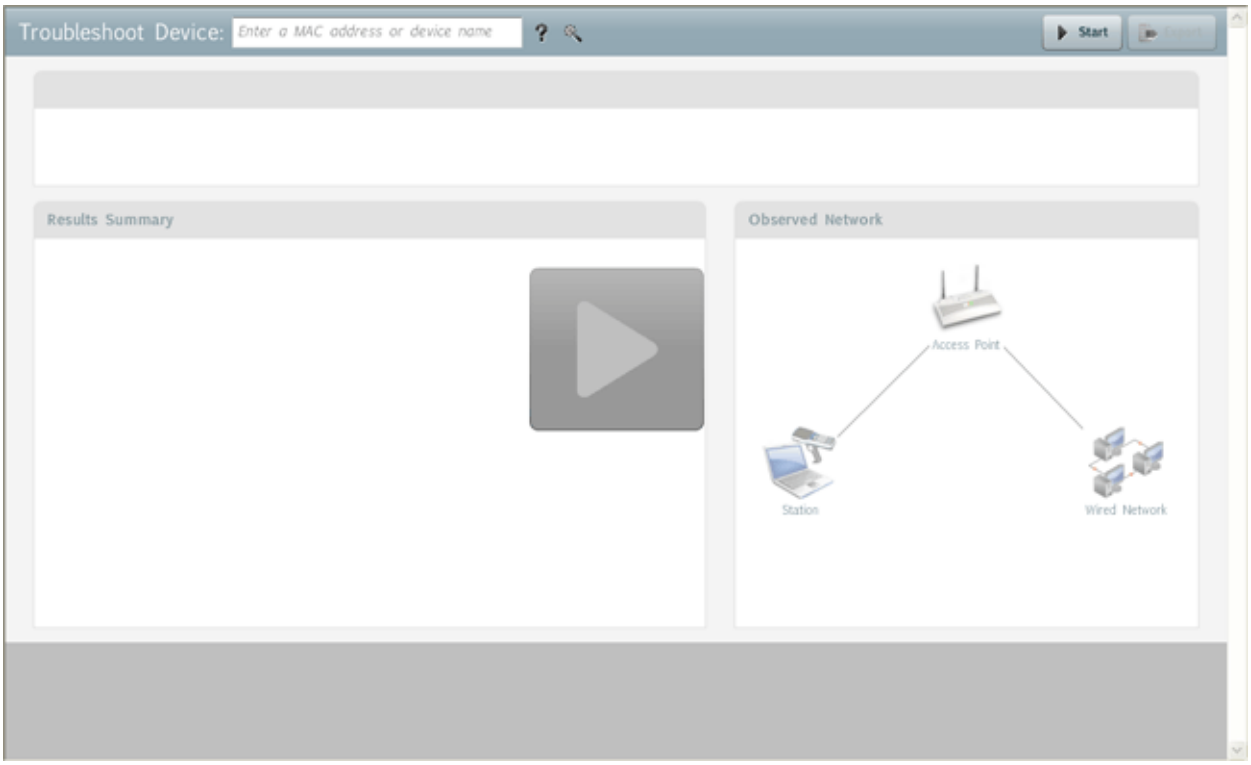
NOTE AP testing is supported on the legacy sensors M510 and M520 with firmware version 5.3 or higher installed, and on APs configured as sensors with WiNG version 5.1 or later installed.

See the *AP Testing* topic in *The Menu* chapter for details on how to schedule both automated and on-demand tests for APs.

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.

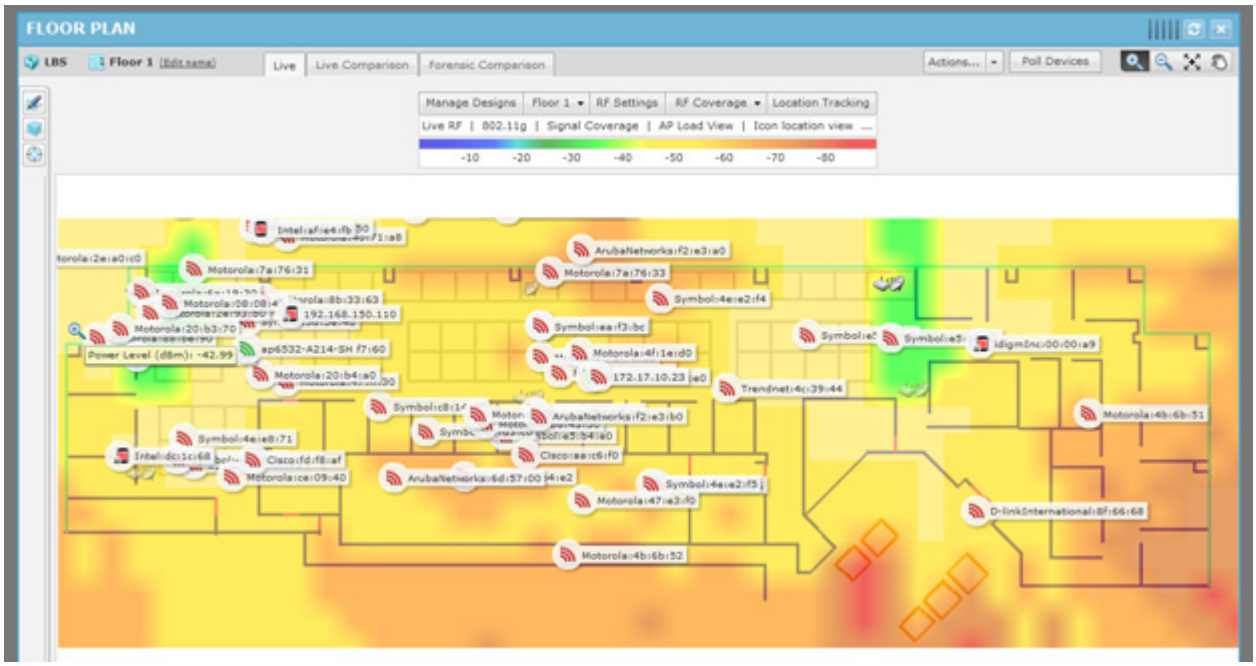
The Troubleshooting tool is accessed through the ADSP GUI.



The *Connection Troubleshooting* topic in *The Menu* chapter 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.

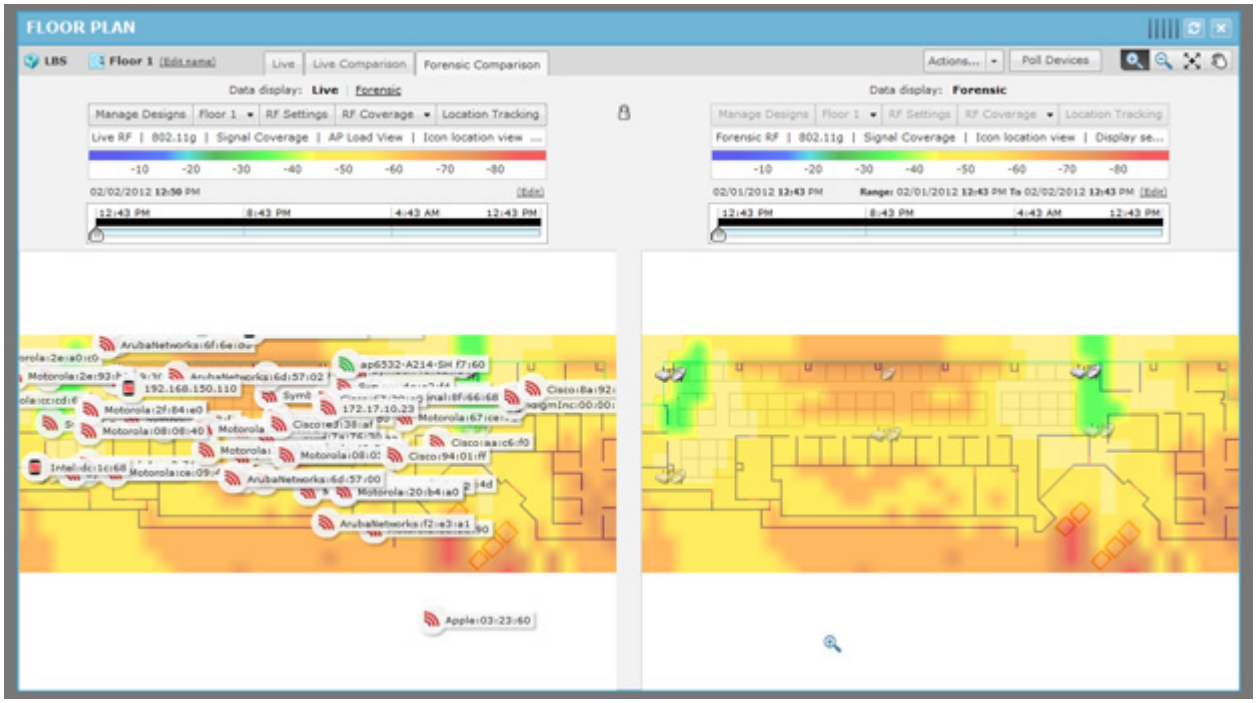
The heat map can be filtered according to:

- 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 RF Settings* topic in the *Configuration* chapter fully explains how to use Live RF.

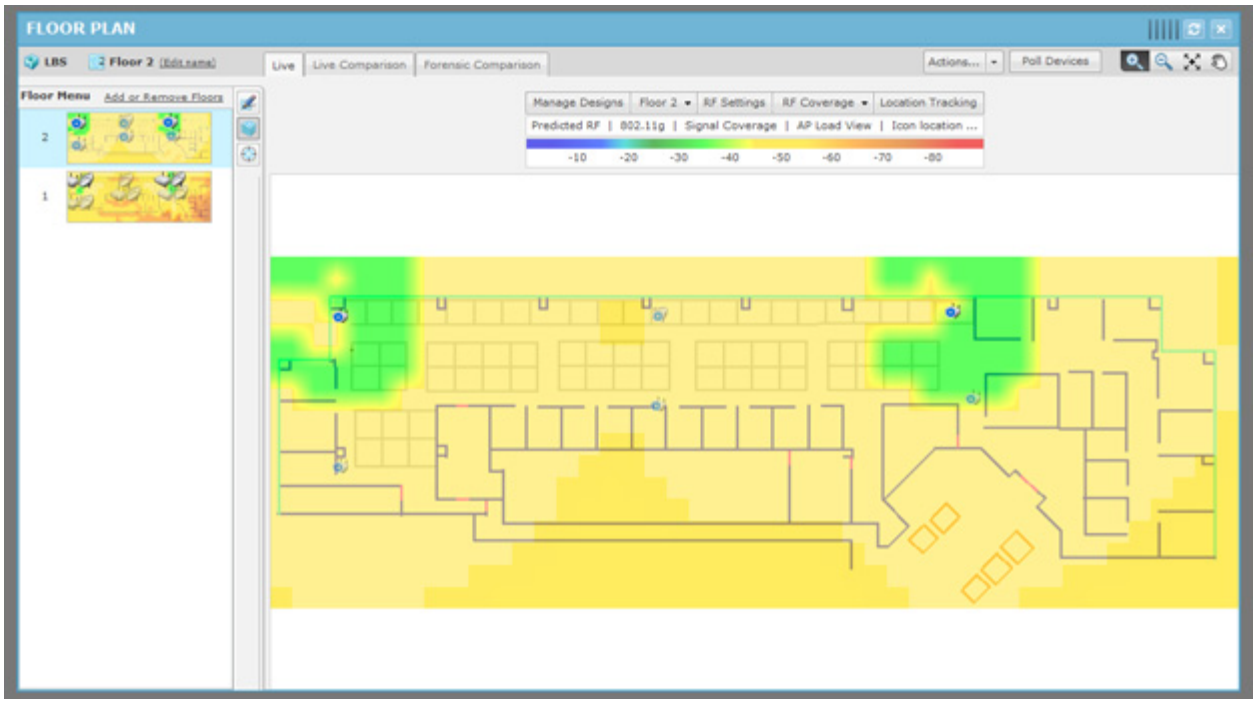
Forensic RF

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

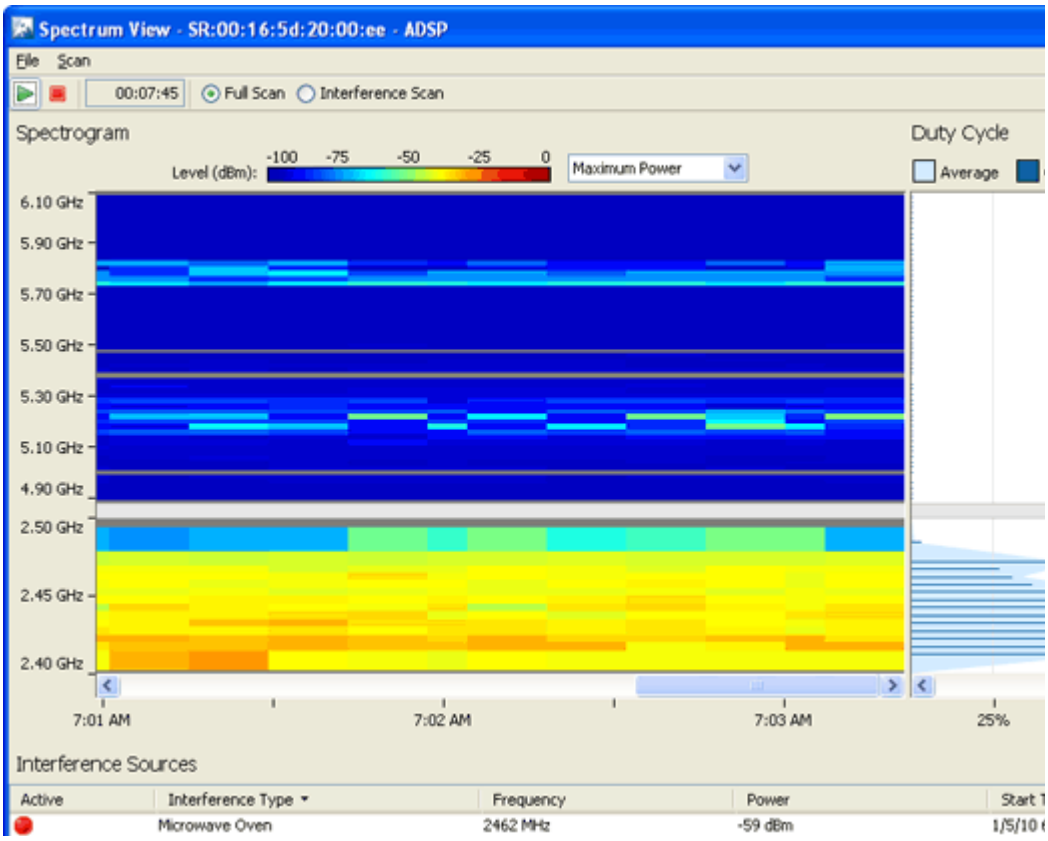
The Spectrum Analysis module gives you a tool to identify and locate interference sources on your wireless network. The analysis is conducted using only ADSP software; no extra hardware is required.

NOTE You must have a valid Spectrum Analysis license 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)

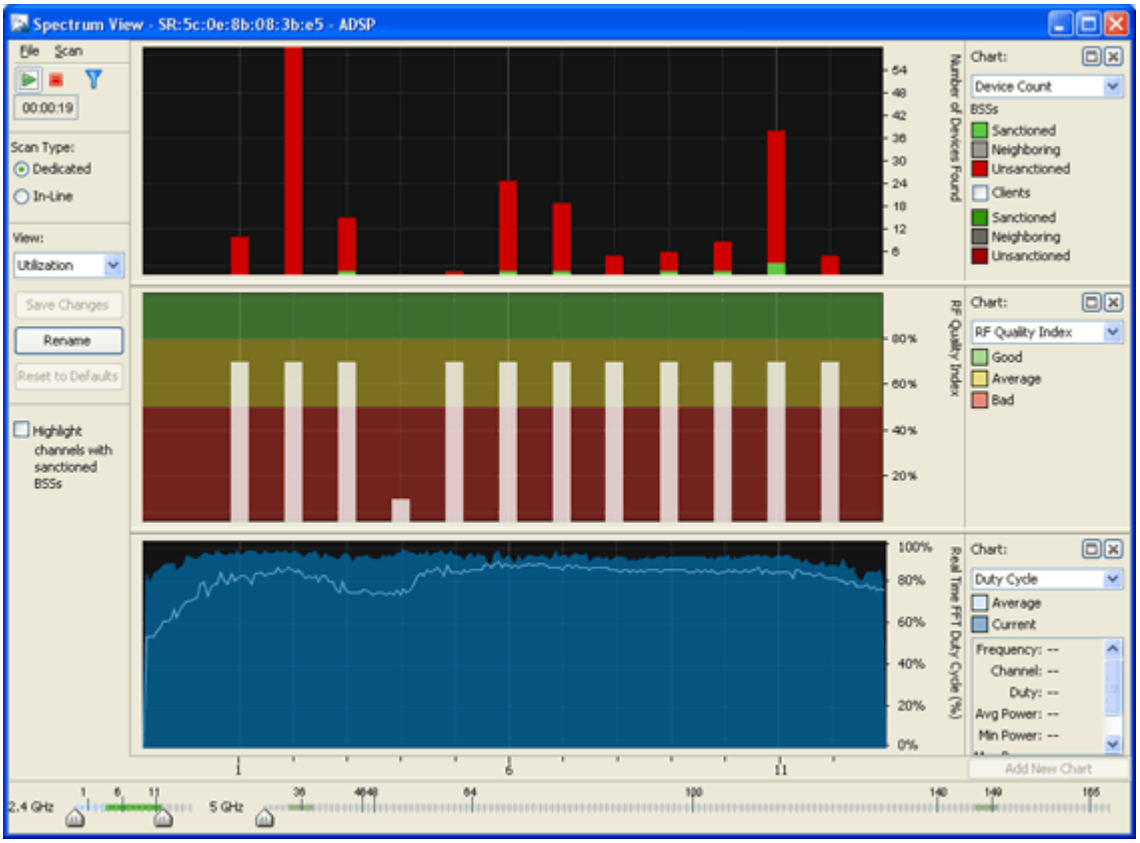
- Dedicated Spectrum View
  - Sensor temporarily dedicated to Spectrum Analysis
  - While in Spectrum View the sensor provides no protocol analysis (after user-configured time period, sensor defaults back to WIPS)
  - Scanning options:
    - Full Scan Mode - scan full 2.4-2.5 GHz and 4.9-6.1 GHz spectrum 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 in *The Menu* chapter fully explains how to use Spectrum Analysis.

Advanced Spectrum Analysis

Advanced Spectrum Analysis (ASA) is the next generation of Spectrum Analysis. ASA 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.

NOTE APs 7522 and 7532 do not support Spectrum Analysis or Advanced Spectrum Analysis when running in RadioShare mode. When the APs are configured as dedicated sensors, both SA and ASA are enabled and fully functional.

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 s 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)

The Network Assurance solution 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 an 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 sharing. With a Radio Share Network Assurance license, you receive the following modules:

- Radio Share Testing
- Radio Share Advanced Forensics
- Radio Share Client Connectivity Troubleshooting
- Radio Share Spectrum Analysis.

Customer Support

Customer Support Center

If you have a problem with your equipment, contact the support center for your region. The Customer Support Center provides product support and issue resolution for products that are under warranty or covered by a service agreement. Contact the support center at:

- North America: 1-800-722-6234
- International: +1-631-738-5200

When contacting Customer Support, please provide the following information:

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

The Customer Support Center responds to calls by email or telephone within the time limits set forth in your support agreement. If you purchased your business product from a business partner, contact that business partner for support.

Support Website

The Support Website, located at *www.zebra.com/support,* provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Product Manuals

Product manuals, including the AirDefense User Guide and Installation Guide, are available at *www.zebra.com/support*

CHAPTER 13 ADSP ICONS

Introduction

The following Icons are used in the ADSP application. They are organized into the following categories:

- Dashboard Icons
- Tree Icons
- Network Navigation Icons
- Alarm Icons
- Appliance Icons
- Switch Icons
- Sensor Icons
- Icons
- BSS Icons
- Wireless Client Icons
- Unknown Device Icons
- Manager Icons
- SSID Icon.

The following symbols are used in conjunction with the device icons to help identify them:

Symbol	Description
	Offline device
	Unlicensed device
	Device on wired network
	Device on wireless network

Symbol	Description
	Unmanaged device
	Part of a bridged network
	Associated to a network
	Participating in an Ad-Hoc network
	Wi-Fi Direct device

Dashboard Icons

Icon	Description
	Displays Dashboard components as a pie chart.
	Displays Dashboard components as a column chart.
	Displays Dashboard components as a bar chart.
	Displays Dashboard components as a table.
	Displays Dashboard components as a line chart.

Tree Icons

Icon	Description
	This is the highest level in the tree. It represents the entire system.
	This is the second highest level in the tree. It represents an appliance.
	This is the third highest level in the tree. It represents the country.
	This is the fourth highest level in the tree. It represents a region
	This is the fifth highest level in the tree. It represents a city.
	This is the sixth highest level in the tree. It represents a campus.

Icon	Description
	This is the seventh highest level in the tree. It represents an area or building.
	This is the lowest level in the tree. It represents a floor.
	This represents an unplaced device. It has not been placed in any tree level.

Alarm Icons

Icon	Description
	Alarm—Icon for individual event.
	Behavior—(Anomalous Behavior) Indicates device is operating outside normal expectations.
	Exploits—Events caused by a potentially malicious user actively interacting on your Wireless LAN.
	Infrastructure—Events related to Infrastructure Management and Infrastructure Faults.
	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—Events which indicate devices are not in compliance with the defined policy.
	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.
	Vulnerability—Devices that are detected to be susceptible to attack.

Appliance Icons

Icon	Description
	Online ADSP appliance.
	Offline ADSP appliance.

Switch Icons

Icon	Description
	A managed online switch seen on your wired network that has been configured for polling.
	An online switch seen on your wired network that is not managed by ADSP.
	A managed offline switch seen on your wired network that has been configured for polling.
	A managed online switch that you are planning to add to your wired network.
	A managed online switch seen on your wireless network that has been configured for polling.
	An online switch seen on your wireless network that is not managed by ADSP.
	A managed offline switch seen on your wireless network that has been configured for polling.
	A managed online switch that you are planning to add to your wireless network.

Sensor Icons

Icon	Description
	A Sensor that is functioning normally and is communicating with the ADSP Server. To be online, the Sensor must be connected to the ADSP Server.
	A Sensor that is not communicating with the ADSP Server. If you did not intentionally take a Sensor off-line, check the Sensor's configuration settings.
	A Sensor that is not licensed with the ADSP Server. Use the Licenses feature of the Appliance Manager to check the license status.
	A Sensor that is in the auto-connect mode. Note: The Sensor auto-connect mode is the fourth phase of zero touch. After 5 minutes of attempting zero touch discovery and an AP is not adopted by a switch or the default password has been changed, a Sensor will enter the auto-connect mode and attempt to connect the AP to the ADSP appliance.

Icon	Description
	A planned Sensor as seen in adding planned devices to a floor plan.
	A Sensor that is in radio share mode. Note: If the Sensor appears in a Java applet (standalone feature) and is in radio share mode, the ap_radioShare icon displays (not a Sensor icon).
	A Sensor that is in radio share mode and is not communicating with the ADSP Server. If you did not intentionally take the Sensor off-line, check the Sensor's configuration settings.

Icons

Icon	Description
	An online AP that is managed by ADSP.
	An online AP that is not managed by ADSP.
	An offline AP that is managed by ADSP.
	A planned as related to adding planned devices to a floor plan.
	An AP that has a Sensor in radio share mode.

BSS Icons

Icon	Description
	Sanction BSS—BSS that has been sanctioned by ADSP.
	Unsanctioned BSS—BSS that has not been sanctioned by ADSP.
	Neighboring BSS—BSS that is on a neighboring network.
	Ad-Hoc BSS—An ad-hoc network with one or more Wireless Clients connected to it.
	Not Observed BSS—BSS that has not been seen by a Sensor.
	Bridge Sanction BSS—Two or more BSSs that have been bridged and sanctioned by ADSP.
	Bridge Unsanctioned BSS—Two or more BSSs that have been bridged and are not sanctioned by ADSP.

Icon	Description
	Bridge Neighboring BSS—Two or more BSSs that are bridged and on a neighboring network.
	Wi-Fi Direct Sanctioned BSS—Wi-Fi Direct BSS that has been sanctioned by ADSP.
	Wi-Fi Direct Unsanctioned BSS—Wi-Fi Direct BSS that has not been sanctioned by ADSP.
	Wi-Fi Direct Neighboring BSS—Wi-Fi Direct BSS that is on a neighboring network.

Wireless Client Icons

There are various types of Wireless Clients. Each type has its own set of icons to identify the Wireless Clients throughout the ADSP GUI. The different types are:

- Default (used to identify Wireless Clients that have not been associated with a specific type)
- MCDs
- VoIP Phones
- Laptops
- Employee Laptops
- Employee Phones
- Employee Devices
- High Priority Visitor Devices
- Visitor Devices
- Low Priority Visitor Devices.

Default (Uncategorized) Devices

Icon	Description
	A Wireless Client that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Wireless Client that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Wireless Client on a neighboring network that is currently “probing” but is not associated to a BSS.
	A Wireless Client that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.

Icon	Description
	A Wireless Client that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Wireless Client that is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Wireless Client on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more Wireless Clients that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more Wireless Clients that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more Wireless Clients on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct Wireless Client that is sanctioned by ADSP.
	A Wi-Fi Direct Wireless Client that is not sanctioned by ADSP.
	A Wi-Fi Direct Wireless Client on a neighboring network.

MCDs

Icon	Description
	A MCD that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A MCD that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A MCD on a neighboring network that is currently “probing” but is not associated to a BSS.
	A MCD that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	A MCD that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A MCD that is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A MCD on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more MCDs that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more MCDs that are not sanctioned by ADSP forming an Ad-Hoc network.

Icon	Description
	One or more MCDs on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct MCD that is sanctioned by ADSP.
	A Wi-Fi Direct MCD that is not sanctioned by ADSP.
	A Wi-Fi Direct MCD on a neighboring network.

VoIP Phones

Icon	Description
	A VoIP Phone that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A VoIP Phone that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A VoIP Phone on a neighboring network that is currently “probing” but is not associated to a BSS.
	A VoIP Phone that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	A VoIP Phone that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A VoIP Phone is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A VoIP Phone on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more VoIP Phones that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more VoIP Phones that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more VoIP Phones on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct VoIP Phone that is sanctioned by ADSP.
	A Wi-Fi Direct VoIP Phone that is not sanctioned by ADSP.
	A Wi-Fi Direct VoIP Phone on a neighboring network.

Laptops

Icon	Description
	A Laptop that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Laptop that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Laptop on a neighboring network that is currently “probing” but is not associated to a BSS.
	A Laptop that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	A Laptop that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Laptop is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Laptop on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more Laptops that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more Laptops that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more Laptops on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct Laptop that is sanctioned by ADSP.
	A Wi-Fi Direct Laptop that is not sanctioned by ADSP.
	A Wi-Fi Direct Laptop on a neighboring network.

Employee Laptops

Icon	Description
	An Employee Laptop that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	An Employee Laptop that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	An Employee Laptop on a neighboring network that is currently “probing” but is not associated to a BSS.

Icon	Description
	An Employee Laptop that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	An Employee Laptop that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	An Employee Laptop is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	An Employee Laptop on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more Employee Laptops that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more Employee Laptops that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more Employee Laptops on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct Employee Laptop that is sanctioned by ADSP.
	A Wi-Fi Direct Employee Laptop that is sanctioned by ADSP.
	A Wi-Fi Direct Employee Laptop on a neighboring network.

Employee Phones

Icon	Description
	An Employee Phone that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	An Employee Phone that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	An Employee Phone on a neighboring network that is currently “probing” but is not associated to a BSS.
	An Employee Phone that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	An Employee Phone that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	An Employee Phone is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	An Employee Phone on a neighboring network that is currently “probing” and is associated to a BSS.

Icon	Description
	One or more Employee Phones that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more Employee Phones that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more Employee Phones on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct Employee Phone that is sanctioned by ADSP.
	A Wi-Fi Direct Employee Phone that is not sanctioned by ADSP.
	A Wi-Fi Direct Employee Phone on a neighboring network.

Employee Devices

Icon	Description
	An Employee Device that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	An Employee Device that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	An Employee Device on a neighboring network that is currently “probing” but is not associated to a BSS.
	An Employee Device that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	An Employee Device that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	An Employee Device is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	An Employee Device on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more Employee Devices that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more Employee Devices that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more Employee Devices on a neighboring network forming an Ad-Hoc network.

Icon	Description
	A Wi-Fi Direct Employee Device that is sanctioned by ADSP.
	A Wi-Fi Direct Employee Device that is not sanctioned by ADSP.
	A Wi-Fi Direct Employee Device on a neighboring network.

High Priority Visitor Devices

Icon	Description
	A High Priority Visitor Device that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A High Priority Visitor Device that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A High Priority Visitor Device on a neighboring network that is currently “probing” but is not associated to a BSS.
	A High Priority Visitor Device that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	A High Priority Visitor Device that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A High Priority Visitor Device is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A High Priority Visitor Device on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more High Priority Visitor Devices that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more High Priority Visitor Devices that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more High Priority Visitor Devices on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct High Priority Visitor Device that is sanctioned by ADSP.
	A Wi-Fi Direct High Priority Visitor Device that is not sanctioned by ADSP.
	A Wi-Fi Direct High Priority Visitor Device on a neighboring network.

Visitor Devices

Icon	Description
	A Visitor Device that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Visitor Device that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Visitor Device on a neighboring network that is currently “probing” but is not associated to a BSS.
	A Visitor Device that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	A Visitor Device that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Visitor Device is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Visitor Device on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more Visitor Devices that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more Visitor Devices that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more Visitor Devices on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct Visitor Device that is sanctioned by ADSP.
	A Wi-Fi Direct Visitor Device that is not sanctioned by ADSP.
	A Wi-Fi Direct Visitor Device on a neighboring network.

Low Priority Visitor Devices

Icon	Description
	A Low Priority Visitor Device that is sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Low Priority Visitor Device that is not sanctioned by ADSP and is currently “probing” but is not associated to a BSS.
	A Low Priority Visitor Device on a neighboring network that is currently “probing” but is not associated to a BSS.

Icon	Description
	A Low Priority Visitor Device that has not been seen by a Sensor and is currently “probing” but is not associated to a BSS.
	A Low Priority Visitor Device that is sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Low Priority Visitor Device is not sanctioned by ADSP and is currently “probing” and is associated to a BSS.
	A Low Priority Visitor Device on a neighboring network that is currently “probing” and is associated to a BSS.
	One or more Low Priority Visitor Devices that are sanctioned by ADSP forming an Ad-Hoc network.
	One or more Low Priority Visitor Devices that are not sanctioned by ADSP forming an Ad-Hoc network.
	One or more Low Priority Visitor Devices on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct Low Priority Visitor Device that is sanctioned by ADSP.
	A Wi-Fi Direct Low Priority Visitor Device that is not sanctioned by ADSP.
	A Wi-Fi Direct Low Priority Visitor Device on a neighboring network.

Unknown Device Icons

Icon	Description
	Unknown device detected in your wireless traffic.
	Non-wireless device marked as a wired resource.

Manager Icons

Icon	Description
	Wired Manager
	Wireless Manager

SSID Icon

Icon	Description
	This is the Service Set Identifier to which the BSSs belong.

CHAPTER 14 GLOSSARY

Wireless Terms and Definitions

Term	Definition
ACL	An Access Control List (ACL) allows the system administrator to grant or restrict access rights to a network device by specifying a MAC address or range of MAC addresses. It also defines which operations are allowed on a given device.
Action Manager	Rules that can be applied to define a response to an event/alarm. Setting these rules within the action manager can reduce the need for physical management as the system will respond.
Active Scan	The process by which stations attempt to locate APs by broadcasting probe request frames containing a specific Service Set Identifier (SSID). This is also used in AD-Hoc mode to locate other stations.
Ad Hoc Network	An ad hoc network exists when two or more wireless devices associate with each other without the use of an intermediary . The software that controls the functionality of wireless network adapters typically provides the ability, configured manually, to accomplish this. The software creates a session ID-much like the MAC address of an -which the devices use to communicate with each other.
Ad Hoc Wireless Client	An ad hoc station is a Wireless Client that is connected to one or more other Wireless Clients without using an AP. Ad hoc networking is a function of most standard 802.11 network client cards. Wireless Clients that are connected in this manner do not need a wireless infrastructure, and therefore represent a security threat, especially when one or more Wireless Clients in the ad hoc network also connect to a wired network.
Adjacent Non-Overlapping Channel	RF channels in sequence with sidebands that do not share the same frequencies.

Term	Definition
Alarms	ADSP generates alarms to signify certain events or conditions that have occurred within a wireless LAN that violate a policy or performance threshold. There are nine alarm categories ranging from device behavior to rogue activity and vulnerabilities to policy compliance to platform health.
A-MPDU	Aggregate MAC Protocol Data Unit (A-MPDU): a method of frame aggregation allowing separate destinations and encryptions for each of the MPDUs contained causing more overhead than A-MSDU due to the individual MAC headers and trailers used inside.
A-MSDU	Aggregate MAC Service Data Unit (A-MSDU): a method of frame aggregation in which the headers and trailers of multiple MSDUs are removed then the MSDUs are combined in to a single 802.11 frame for transmission wrapped with a single header and trailer.
Antenna Diversity	The use of two or more antennae to mitigate the effects of Multipath and Scattering on a single radio. This can be transmit diversity, receive diversity or both dependent upon the antenna technologies deployed.
AP	An Access Point is a small device (usually smaller than a laptop or CD carrying case) that transmits and receives network traffic over fourteen radio channels, as specified by the 802.11 protocol (only 11 channels are authorized for wireless network use within the U.S.). An AP physically connects to your network via a standard Ethernet cable connection, and acts as a hub for nearby laptops and workstations that are configured with wireless network adapters. APs may use a variety of antenna configurations, with each antenna offering specific functionality, such as 360 degree accessibility, line-of-sight accessibility, high gain (strong signal strength), etc.
Appliance	64-bit appliance hardware that enables AirDefense applications.
API	Application Programming Interface (API) is typically used to provide a set of routines, protocols and tools for building applications for devices to interact with each other. For example, mobile phones can interact with wireless networks and applications can be developed and customized to provide location information through the wireless environment.
AP Testing	AirDefense module that allows proactive identification of problems impacting wireless applications by periodically performing end-to-end network testing of the wireless path a device uses to connect.
ARP	Address Resolution Protocol (ARP) is a TCP/IP protocol used to obtain the physical address of a node. A client station broadcasts an ARP request onto the network with the IP address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted. ARP returns the layer 2 address for a layer 3 address. ARP requests are broadcast onto the network, requiring every station in the subnet to process the request.

Term	Definition
ATIM	Announcement Traffic Indication Message (ATIM) is used in ad-hoc networks to let an awaking station know that it has traffic buffered on the station sending the ATIM. This keeps the station active long enough for the traffic to be delivered. Once all traffic is received and the corresponding ACKs are sent, the station may close again.
Authentication	A process by which a station or users credentials are verified prior to the station being allowed to associate with the SSID.
Authentication Modes	You can configure AP configuration policies to accept either non-authenticated network connections and/or shared key authentication. You select authentication modes when you set up a configuration policy for the AP. Placing an authentication mode in your AP policy definition ensures that the authentication mode is being deployed and used by both the AP and its associated Wireless Clients. AirDefense generates an alarm if it detects that an AP has allowed a Wireless Client to associate with it without correct authentication, or if the AP or Wireless Client is improperly configured.Some authentication modes are Open, Shared Key, WEP, LEAP, 802.1x, PEAP, WPA, AirFortress, and VPN.
Beacon	A broadcast frame sent out by an AP or station containing information about the device and service set. They also contain management information and control information such as the TIM, DTIM and ATIM as well as the beacon interval.
Beam Forming	A signal processing technique used in Sensor arrays for directional signal transmission or reception achieving spatial selectivity by using adaptive or fixed receive/transmit beam pattern.
Block Acknowledgment	Allows the acknowledgment of several frames with a single ACK frame rather than one for each frame received.
Bridge	Ordinarily, each AP is physically connected to the wired network via standard Ethernet cable. There may be instances in which the Extended Service Set is so large (in terms of physical space) that the wired network is several APs away. In this case, two or more APs serve as relays to the wired network. Unlike regular APs, bridges do not have an Ethernet connection to the physical network. They are configured to transmit data they receive to a specific - either another bridge or to a wired AP.
BSS	Basic Service Set (BSS) is the term that describes the footprint of a single and all Wireless Clients associated with it. The BSS is a footprint in that only Wireless Clients within a certain radius of the will be able to transmit to, and receive data from the AP. Further away, the radio signals will be too weak for successful data transmission. Each BSS has an ID (or identifier). This is the MAC address of the wireless network adapter on that .
Channel	A contiguous grouping of frequencies of which the center frequency is used to define the grouping and is assigned a sequential number for identification within a given frequency range.

Term	Definition
Channel Bonding	The simultaneous use of two Non-Overlapping channels for transmission to transmit data used in 802.11n and legacy “Super G” environments.
Channel Width	The range of radio frequency allocated to specific RF channels. DSSS channels are 22MHz wide while OFDM channels are only 20MHz wide.
Co-Channel interference	This occurs when RF devices from different service sets are on the same center frequency (Channel) and occupy the same physical airspace increasing the size of the contention domain.
Contention Domain	A shared medium in which devices use a non-guaranteed communication method forcing each node to negotiate with the other nodes using the medium for an opportunity to transmit.
CRC	Cyclic Redundancy Check: a common technique for detecting data transmission errors. Transmitted messages are divided into predetermined lengths that are divided by a fixed divisor. According to the calculation, the remainder number is appended onto and sent with the message. When the message is received, the computer recalculates the remainder and compares it to the transmitted remainder. If the numbers do not match, an error is detected.
CSR	Certificate Signing Request
Denial-of-Service Attack	A Denial-of-Service (DoS) is an external attack on your wireless LAN that can cripple the network. A DoS attack can come from any direction. Because 802.11x wireless LANs operate on the unregulated 2.4 GHz radio frequency that is also used by microwave ovens and cordless telephones, commonly available consumer products can give hackers the tools for a simple and extremely damaging DoS attack. For example, unleashing large amounts of noise from these other devices can jam the airwaves and shut down a wireless LAN.
DoS Attack / Malicious Disassociation	Hackers can launch more sophisticated DoS attacks—called malicious disassociation—by configuring a Wireless Client to operate as an AP. As an AP, the hacker can flood the airwaves with persistent ‘disassociate’ commands that force all Wireless Clients within range to disconnect from the wireless LAN. In another variation, the hacker sends malicious broadcasts every few minutes. This causes a situation where Wireless Clients are continually kicked off the network, reconnected, and kicked off again.
DoS Attack / EAP Manipulations	Hackers can abuse the Extensible Authentication Protocol (EAP) to launch DoS attacks. The ‘Unofficial 802.11 Security Web Page’ at http://www.drizzle.com/~aboba/IEEE/ lists forms of DoS attacks from various ways hackers can manipulate EAP protocols by targeting Wireless Clients and APs with log-off commands, start commands, premature successful connection messages, failure messages, and other modifications of the EAP protocol.

Term	Definition
DoS Attack / Rogue AP	Some DoS attacks exploit improperly configured wireless LANs or rogue APs to target the entire enterprise network. When an AP is attached to an unfiltered segment of the enterprise network, the AP broadcasts 'Spanning Tree' (802.1D) packets. This opens the door to attacks that take down all wireless equipment and spur a meltdown of the entire internal networking infrastructure, including the hubs, routers, switches, etc. that are connected behind the wireless LAN. In normal operation, the Spanning Tree algorithm ensures the existence of a loop-free Ethernet topology in networks that contain parallel bridges and multiple Ethernet segments. A loop occurs when there are alternate routes between hosts. If a loop exists in an extended network, bridges may forward traffic indefinitely to false or wrong Ethernet hosts, which can result in increased traffic and degradation in network performance to a point where they no longer will respond or operate. A hacker can launch a DoS attack by intentionally inserting this loop on the network. The hacker goes through the wireless LAN to maliciously replay an altered Spanning Tree session back to the enterprise. A rogue sniffer can initiate this by attack echoing a manipulated replay Spanning Tree session back to the wireless LAN AP, which in turn echoes the manipulated Spanning Tree packets to other internal hosts with a devastating domino effect. Spanning Tree attacks will typically render the intelligent hubs, bridges, routers, and switches completely inoperative and usually require rebooting or reconfiguration of these devices to make them operative again. Any rogue AP plugged into a port on a hub or into a switch or router that is not filtered by a firewall can open a network to this most damaging DoS attack.
Device	A Sensor, AP, or Wireless Client in an AirDefense wireless LAN.
DHCP	Dynamic Host Configuration Protocol (DHCP) provides a means to allocate an IP address dynamically to computers on a LAN. It eliminates the need to assign permanent IP addresses manually. DHCP software runs on servers and can be found in network devices (such as routers) that allow multiple users to access the Internet. Microsoft® introduced DHCP on their Windows® NT server in 1994. Newer DHCP servers will dynamically update DNS servers after assigning the addresses.
DIFS	Distributed Coordination Function Interframe Spacing (DIFS) is used by all stations in Distributed Coordination Function (See DCF) for media access.
DNS	Domain Name System (DNS) is the name of a web address, as opposed to its actual IP address.Web sites are actually located by their IP addresses. So, when you type in http://www.airdefense.net, the computer doesn't immediately know that it should look for the AirDefense, Inc. web site. Instead, it sends a request to the nearest DNS server, which matches an IP address to the domain name and then connects you to the server with that IP number.

Term	Definition
Domain Name	This is the name that identifies a website. For example, *apple.com* is the domain name of the Apple website. A single web server may have more than one domain name, but a single domain name points to only one device. For example, www.apple.com, support.apple.com, and store.apple.com could be served on one to three devices. It is also possible, and quite common, for a domain name to be registered, but not be connected to an actual device. The reason for this is usually so that a company or group can have email addresses at a certain domain without having to maintain a web site. In these cases, there still must be a device to handle the mail of the listed domain name.
DTIM	Delivery Traffic Indication Message (DTIM) is used to alert an awaking station that an AP has buffered multicast or broadcast traffic for that station. This keeps the station activated long enough for the awaiting traffic to be delivered. Once all traffic is received and the corresponding ACKs are sent the station may dose again.
Dual CTS Protection	Allows both RTS/CTS and CTS to Self protection modes for both legacy and HT devices within the same contention domain that may or may not be part of the same service set.
Dynamic SM Power Save	Similar to SM Power Save but the AP is allowed to trigger a station to power up additional radios by using an RTS/CTS exchange initiated by the AP thus powering up the stations radios more rapidly.
EIFS	Extended Interframe Spacing used after collisions or errors in transmissions.
Extended Service Set / Service Set ID (ESS/SSID)	Logical groupings of one or more APs (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs. Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the APs in an Extended Service Set be in physical proximity to each other, or for example, are all on the same floor of a building. The grouping of APs into a wireless network is at the discretion of the network administrator. When a Wireless Client wishes to use the services of an , it must broadcast a probe request announcing the Extended Service Set it wishes to become a part of. The nearest in that ESS authenticates the Wireless Client and allows network connectivity through the Wireless Client to take place.
Fragmentation	Reducing the size of transmitted frames. Each fragment is assigned the same frame ID but a different fragment ID for reassembly at the receiver. The threshold triggering fragmentation is user definable.
Frame	A packet which has been encoded for transmission over a particular link.
Frame Aggregation	Combining multiple frames into a single frame for transmission.
Free Space Path Loss	The reduction of signal amplitude due to the natural propagation or expansion of the signal wave front.

Term	Definition
Fresnel Zone	This is an area centered upon the visual line of site between transmitting and receiving antenna, the size of which is determined by the frequency used, distance between antenna and power used.
Gain	Amplification of the signal. This can be active gain, the introduction of a powered amplifier between the transmitter and the antenna, or passive gain the use of an antenna or shortening of cable runs in the system resulting in lower attenuation.
Greenfield HT	An environment containing only HT (802.11n) devices not only in the service set but within the contention domain as well (no legacy devices are present i.e. no 802.11a/b/g radios in the area) also called Greenfield mode.
Groups	Groups denote clusters of individual Sensors, with each Sensor monitoring the activity of one or more APs.
Guard Interval	A period of time that allows for late arriving symbols over long paths used in OFDM transmissions.
Hidden Node	A station that is not detected by another station due to blockage of the signal and or being out of signal range from each other. Both stations may be within range of the but not be able to receive the others transmissions resulting in collisions.
Host Name	This is the name of a computer that acts as a server for other computers on the network. It can be a web server, an email server, an FTP server, etc. For instance, a web host is what provides the content of web pages to the computers that access it.
HT Protection Modes	Mode 0 = only HT radios in use no legacy radios present. Mode 1 = HT non-member protection allows the HT service set containing all HT devices to be co-located with non-HT devices which are in the same service set. Mode 2 = HT 20MHz protection mode allows 20 MHZ HT stations to be part of a 20/40 MHz HT service set. Mode 3 = one or more non-HT stations are associated with the HT and are part of the service set.
IBSS	Independent Basic Service Set. The SSID of an ad-hoc network.

Term	Definition
Identity Theft	Identity theft (also known as MAC spoofing) is a serious external threat to your wireless LAN. Identity theft is the theft of an authorized user's identity. Service Set Identifiers (SSIDs) that act as crude passwords and MAC addresses that act as personal identification numbers are often used to verify that clients are authorized to connect with an . Because existing encryption standards are not foolproof, knowledgeable hackers can use software tools, such as Kismet or Ethereal, to steal the authorized SSIDs and MAC addresses of an authorized user. The hacker can then assume the identity of that user by asserting the stolen MAC address as his own and connect to the wireless LAN as an authorized user. Once connected, the hacker can steal bandwidth, corrupt or download files, and wreak havoc on the entire network. Using these methods, a hacker can easily change the MAC address of a Wireless Client or AP to change its identity and defeat MAC address-based authentication. An enterprise can detect MAC spoofing by monitoring the airwaves of their wireless LAN and identifying when more than one MAC address is simultaneously on the network. Wireless LAN intrusion detection systems can also identify when a MAC address is spoofed by analyzing the vendor fingerprints of the wireless LAN card, whereby the IDS can see when, for example, an Orinoco® wireless LAN card connects to the network using the MAC address of a Cisco® wireless LAN card.
IP Address	A numeric address that is given to a device that is connected to the Internet, through which other devices and servers can find and identify the device. The IP address also applies to servers and users connected to the Internet. For servers, it is translated into a domain name, by a Domain Name Server (DNS). For users, it is assigned by the Internet Service Provider (ISP) when the user goes online. This IP address might be the same number each time you log on (called a static IP), or it might be a newly assigned number each time you connect, based on what is available.
Locations	Locations are the top-level descriptors in the AirDefense GUI program tree. Depending on the size of your wireless network, Locations (represented by a globe icon) can denote a cluster of buildings, or even a city, and can contain any number of offices. Below Locations on the hierarchy are Groups (represented by an icon of multiply-connected Sensors).
Loss	Attenuation of the signal being transmitted, caused by cables, connectors, free space path loss, impedance mismatch, or a purposeful attenuation device being placed in-line prior to the antenna.
MAC Address	The MAC (media access control) address is the network address used by the 802.11 protocol to identify the physical address of a device. Each 802.11 Wireless Client and AP ship with a unique MAC address.

Term	Definition
Man in the Middle Attack	One of the more sophisticated attacks, a man-in-the-middle is a potentially crippling external attack on your wireless LAN that can break a secure VPN connection between an authorized Wireless Client and an AP. By inserting a malicious Wireless Client between the victim Wireless Client and the AP, the hacker becomes the “man in the middle” as he tricks the Wireless Client into believing he is the AP and tricks the AP into believing he is the authorized Wireless Client. This attack preys upon a CHAP implementation to randomly force a connected Wireless Client to re-authenticate with the AP. The Wireless Client must respond to a random challenge from the AP, and the AP must respond to a successful challenge response with a success packet. To begin this attack, the hacker passively observes the Wireless Client as it connects to the AP, and the hacker collects the authentication information, including the username, server name, client and server IP address, the ID used to compute the response, and the challenge and associate response. The hacker then tries to associate with the AP by sending a request that appears to be coming from the authenticated Wireless Client. The AP sends the VPN challenge to the authenticated Wireless Client, which computes the required authentic response, and sends the response to the AP. The hacker observes the valid response. The hacker then acts as the AP in presenting a challenge to the authorized Wireless Client. The Wireless Client computes the appropriate response, which is sent to the AP. The AP then sends the Wireless Client a success packet with an embedded sequence number. Both are captured by the hacker. After capturing all this data, the hacker then has what he needs to complete the attack and defeat the VPN.The hacker sends a spoofed reply with large sequence number, which bumps the victim’s Wireless Client off the network and keeps it from re-associating. The hacker then enters the network as the authorized Wireless Client. Only 24x7 monitoring and a highly capable wireless IDS can detect this type of attack on a wireless LAN. An effective security solution must first keep a constant watch over the wireless LAN while it analyzes the activity it observes. A wireless IDS should be able to detect this type of attack based on its signature as well as the simultaneous use a single MAC address and user name by both the authorized Wireless Client and the hacker.
Mbps	Megabits per second: the speed of data transfer. (1 Mbps = 1,000,000 bits per second)
MCD	An MCD is a hand-held communications device.
MCS	Modulation Coding Schemes (MCS) defines the modulation technique used to achieve specific data rates in 802.11 transmissions.

Term	Definition
MIB	A management information base (MIB) is a formal description of a set of network objects arranged in a hierarchical format much like that of a Domain Naming Service (DNS) structure, that can be managed using the Simple Network Management Protocol (SNMP).
MIMO	Multiple-Input/Multiple-Output (MIMO): the use of multiple antennae on the transmit and receive sides of a radio chain.
MISO	Multiple-Input/Single-Output (MISO): the use of multiple antennae on the receive side and a single antenna on the transmit side of a radio chain.
Modulation	Any of several techniques for combining user information with a carrier signal from a transmitter.
MSP	Managed Services Provider (MSP): Typically an information technology (IT) services provider, who manages a defined set of services for their clients.
MTU	Maximum Transmission Unit. The MTU is a limit, in bytes, on the size of data sent over a network. It is the maximum size of a single unit (e.g., an Ethernet frame) of digital communications.
MTBA	Multiple Traffic ID Block Acknowledgment (MTBA) is used with A-MPDUs to allow acknowledgments of the individual MPDUs contained in the A-MPDU because the individual MPDUs must be acknowledged.
NAT	Network Address Translation (NAT): the process of modifying IP address information in the IP packet header while transmitting data.
NAV	Network Allocation Vector. A timer used in wireless transmission which contains the contents of the duration field.
Near Far	This problem is due to one station being closer to the than another and gaining more time on the AP because of higher power being detected by the AP. To reduce the effect, increase the power setting on the Far node and decrease the power setting on near node.
Null Probe	This is a probe request sent by a station looking for any SSID to join. A null probe contains no SSID in the probe request and is considered to be a form of active scanning.
NX7500	The NX 7500 is a multi-service platform that brings advanced wireless LAN (WLAN) performance and single point of control simplicity to the mid-size WLAN.Designed for mid-size enterprises and campus environments, the NX 7500 offers comprehensive management of up to 2,048 network elements.
NX9500	The NX9500 controller is a 2U large size appliance for large wireless environments that expect aggressive growth, supporting up to 2500 sensors. The 9500 runs standalone or unified mode versions of the ADSP software.
NX9510	The NX9510 controller is a 2U large size appliance for large wireless environments that expect aggressive growth, supporting up to 2500 sensors. The 9510 runs standalone or unified mode versions of the ADSP software. The 9510 system has an encryption card, which is the only way it differs from the NX9500.

Term	Definition
Overlapping Adjacent Channel	RF channels with sidebands in the same frequency, also called adjacent interfering channels.
Passive Scan	A process by which stations try to locate APs by listening on each channel for specific periods of time until a beacon is detected containing a SSID that the station may use to begin the authentication and association process. This may be done using a Null Probe or not depending upon the tools used.
Phased Coexistence Operation (PCO)	An alternate operational mode that alternates between 20MHz and 40MHz transmissions as a protection mechanism.
PIFS	Point Coordination Functions Interframe Spacing used by an to take control of the media in Point Coordination Function (PCF) mode.
Ping	The main purpose of a ping is to test a server on the Internet to see if it is working. Pinging a server can also test and record the response time of servers and other computers connected to the Internet. This is helpful in finding Internet bottlenecks, so that data transfer paths can be re-routed the most efficient way. Also, a good way to make sure you do not get disconnected from your ISP for being idle is to send a ping every 5 minutes or so. There are a number of shareware Ping programs that will do this for you.
Plenum (spaces)	Plenum spaces are used to circulate air, heating, and air conditioning throughout buildings and are often found above false ceilings or under floors. Because this plenum space often runs uninterrupted around large buildings, it is sometimes used to route computer network cable and can also be used for installing wireless APs, especially where network managers want to hide the AP from view. Like all computer or electrical cables, wireless APs installed in the plenum airspace should be plenum rated, which means that they should not emit toxic gases if the equipment does catch fire. The US National Electric Code “UL 2043” specification is one of the regulations designed to reduce fire hazards from electrical equipment in offices, schools, factories, and other buildings. The UL 2043 plenum rating determines if an AP can safely be placed in the plenum airspace.
Probe Requests	A frame sent by stations to locate APs or other stations during active scanning.
Probe Response	A frame sent to a station from an or station in answer to a probe request.

Term	Definition
Protocols	Beside each icon in AirDefense is a letter designation (a,b,g), representing the protocol of the device. AirDefense supports three protocols for 802.11 traffic: 802.11a, 802.11b, and 802.11g. Protocols differ in their frequency range, radio channels, and data rates. Multi-protocol support threads through the entire user-interface structure for both the AirDefense Server and Sensors. In all GUI programs in which Device Identifiers appear, AirDefense labels the protocol for each device that it detects in your wireless WLAN. Additionally, you can use the filtering that is available in Navigation Trees in Dashboard, Manage Alarms, Sensor Manager, Policy Manager, and Reports to isolate devices using any single or combination of protocols. In the Sensor UI, you can set and apply operational settings to Model 400 Sensors for both 802.11b/g or 802.11a protocols.
PSK	Pre-Shared Key (PSK) is a password (key) that is shared by devices on a wireless network.
QoS	Quality of Service (QoS) standards are used to insure that the application in use receives enough bandwidth for the intended use, often combined with bandwidth control mechanisms.
Radio Chain	Set of two or more antennae and a radio used in multiples for MIMO transmissions.
RIFS	Reduced Interframe Space (RIFS): a new Interframe Space defined in 802.11n with a duration of only 2usec (microseconds) supported only in Greenfield HT environments between HT radios.
Roaming	The ability of a Wireless Client to move from one Basic Service Set to another. This may or may not be seamless. Although there is an industry standard for roaming, support issues like mobile IP still exists. Also, most manufacturers are currently implanting roaming in a proprietary manner.
Rogue	A rogue AP is connected to, and is communicating with your internal network. It is highly likely that one or more Wireless Clients are attached to this AP.
Rogue Device	A rogue device is any wireless device that is unauthorized to operate in your wireless LAN, and that is connected to, or is attempting to connect to, your internal network.
Rogue Wireless Client	A rogue Wireless Client is connecting to and is communicating with your internal network.
RSSI	Received Signal Strength Indicator (RSSI) is a mechanism by which the receiving device evaluates the incoming transmissions strength. This can be viewed in dBm or as a percentage value. There is no defined industry standard to measure RSSI values. They can be measured on quality, available bandwidth, strength, or any combination of indicators. RSSI is implemented in vendor proprietary methods.

Term	Definition
RTS/CTS	Request To Send / Clear To Send is an optional feature of the IEEE 802.11 Standard that allows a station (STA) to reserve the media to reduce collisions in crowded air space and reduces the effect of the Hidden Node Problem.
Sensor Group	A sensor group is a cluster of individual sensors, with each sensor monitoring the activity of one or more APs.
Sensor Location	A Sensor Location is a top-level descriptor in AirDefense GUI program trees. Depending on the size of your wireless network, Locations (represented by a globe icon) can denote a cluster of buildings, or even a city, and can contain any number of offices.Below Locations on the hierarchy are Sensor Groups (represented by an icon of multiple-connected Sensors).
SIFS	Short Interframe Spacing (SIFS) is used prior to priority transmission tasks such as ACKs (acknowledgment frames) and CTS (clear to send frames).
SIMO	Single-Input/Single-Output (SIMO) is the use of a single antenna attached at both the transmitter and the receiver of a radio chain.
Spatial Multiplexing Power Save (SM Power Save)	A power saving scheme introduced in 802.11n that allows a MIMO AP to power down all but one radio.
Spatial-OFDM	The combination of sending multiple independent streams and spatial diversity using multiple channels and sub -carriers also referred to as Spatial-Multiplexing using OFDM allowing multiple data streams to be used as part of a single signal.
SSID	Service Set Identifier (SSID) is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other.
SSL	Secured Sockets Layer (SSL) is a protocol-a form of channel encryption that delivers server authentication, data encryption, and message integrity. SSL is layered beneath application protocols, such as http, SMTP, Telnet, FTP, Gopher, and NNTP; it is layered above the connection protocol TCP/IP. SSL operates without depending on the Internet application protocols. With SSL implemented on both the client and server, your Internet communications are transmitted in encrypted form. Information you send can be trusted to arrive privately and unaltered to the server you specify, and no other.
Threat Analysis	Threat Analysis provides active alarm information in scope-based forensic analysis.
TIM	Traffic Indicator Map (TIM) is used to notify a station awaking from Power Saving Poll Mode that there are frames buffered at the AP for it. This keeps the station activated long enough for the awaiting traffic to be delivered. Once all traffic is received and the corresponding ACKs are sent the station may dose again.

Term	Definition
TxBF	The Transit Beam Forming (TxBF) is also called a Smart Antenna system or Phased Array Antenna system. It allows MIMO devices to focus the transmission beams in a coordinated method.
Unauthorized Device	An unauthorized device is any wireless device that does not have permission to operate in your wireless LAN, but is connected to, or is attempting to connect to, your internal network. Also see Rogue Device.
VLAN	Virtual LAN (local area network) is a logical grouping of network nodes that act as if they are connected to a single, shared-media network.
VPN	Virtual Private Network (VPN) is a secure private network that transmits data using the public telecommunications infrastructure. You can use a VPN for both extranets and wide area intranets. A VPN uses encryption and authentication to encrypt all data that passes between two Internet points, providing both privacy and security. To use a VPN service, you need a static IP number, a dedicated connection to the Internet, and a router (or switch) that supports VPN protocol.
WDS	Wireless Distribution System (WDS) is an example of which is a bridged network connection.
WIDS	Wireless Intrusion Detection System (WIDS) is a monitoring system dedicated to anomalous activity monitoring and reporting.
WIPS	Wireless Intrusion Prevention System (WIPS) is a monitoring system dedicated to anomalous activity monitoring and reporting that also takes pro active steps to disallow any unauthorized use of the wireless media.
Wireless Client	A Wireless Client is any network device that associates with an AP. (To associate with an AP is to be authorized as a valid user, though some APs may be configured to not require authorization.)
Wireless LAN	The wireless local area network (wireless LAN) refers to that portion of your enterprise network whose medium for data transfer is the radio airwave using the fourteen channels specified by the 802.11 protocol (only eleven channels are authorized for wireless LAN use within the U.S.).
WLSE®	WLSE® is an acronym for Wireless LAN Solution Engine, which is a core component of Cisco Systems' CiscoWorks® WLSE technology, a centralized, systems-level solution for managing a Cisco Aironet® wireless LAN infrastructure.
Zone Tracking	Zone tracking uses the RSSI information to determine the associated zone by how close the client device is to a specific sensor in a monitored environment, providing more granular detail than presence.

802.11 Terms and Definitions

Term	Definition
AC	Access Category (AC): The levels of priority in EDCA (see *EDCA*) are called access categories (ACs). The contention window (CW) can be set according to the traffic expected in each access category, with a wider window needed for categories with heavier traffic.
ADDTS	Add Traffic Stream (ADDTS) is used to carry the Transmit Specification (TSPEC) and optionally the Traffic Classification (TCLAS) information between a Quality of Service AP (QAP) and a Quality of Service Wireless Client (QSTA) when creating or maintaining a Traffic Stream (TS).
Adjacent Non-Overlapping Channel	RF channels in sequence with sidebands that do not share the same frequencies.
AGC	Automatic Gain Control (AGC): Technology allowing an automatic increase in power for an incoming signal based upon the strength of the incoming signal giving more power to weaker signals and less power to stronger signals in an effort to normalize signal strength.
AIFS	Arbitration Interframe Space (AIFS): The time a station (STA) differs before attempting to access the medium based upon the access category (AC) assigned to the frame in a Quality of Service (QoS) service set, AIFS are used when transmitting all data frames and (MPDUs), all management frames (MMPDUs), and the following control frames: Power Saving Poll (PS-Poll), Request to Send (RTS), Clear to Send (CTS) (when not transmitted as a response to the RTS), Block Acknowledgment Request (BlockAckReq), and Block Acknowledgment (BlockAck) (when not transmitted as a response to the BlockAckReq).
AID	Association Identifier (AID): A value assigned to a station (STA) by an access point (AP) within the service set upon station association from the allowed range of 1 to 2007 within the 16 bit AID field.
AKMP	Authentication and Key Management Protocol (AKMP) is used to distribute and manage keys to various nodes or networking devices.
A-MPDU	Aggregate MAC Protocol Data Unit (A-MPDU) is a method of frame aggregation allowing separate destinations and encryptions for each of the MPDUs. This causes more overhead than an A-MSDU due to the individual MAC headers and trailers used inside.
A-MSDU	Aggregate MAC Service Data Unit (A-MSDU) is a method of frame aggregation in which the headers and trailers of multiple MSDUs are removed then the MSDUs are combined in to a single 802.11 frame for transmission wrapped with a single header and trailer.

Term	Definition
Antenna Diversity	The use of two or more antennae to mitigate the effects of Multipath and Scattering on a single radio. This can be transmit diversity, receive diversity or both dependent upon the antenna technologies deployed.
APS	Asynchronous Power Save (APS) is a power saving scheme within ad-hoc WLAN deployments.
APSD	Automatic Power Save Delivery (APSD) is an enhanced version of the 802.11 power saving scheme that allows the station (STA) to create a schedule for the delivery of frames based upon a pattern and specified number of beacon frames.
ATIM	Announcement Traffic Indicator Message (ATIM) is used in ad-hoc WLANs to indicate that a member has buffered traffic for another member that may be in power save mode (dozing), similar to the TIM in a beacon frame found in infrastructure networks.
Barker Coding	Used in Direct Sequence Spread Spectrum (DSSS) as a coding method derived from a set of N values and positive and/or negative ones associated with the lower data rates of 1 and 2 Mbps.
Beam Forming	A signal processing technique used in Sensor arrays for directional signal transmission or reception achieving spatial selectivity by using adaptive or fixed receive/transmit beam pattern.
BER	Bit Error Rate (BER) is the ratio of bits received to the number of bits sent.
Block Acknowledgment	Allows the acknowledgment of several frames with a single ACK frame rather than one for each frame received.
BPSK	Binary Phase Shift Keying (BPSK) is a modulation type using two distinct carrier phases to signal ones and zeros, the simplest form of phase shift keying.
BSS	Basic Service Set (BSS) is the basic building block of an 802.11 wireless LAN. In infrastructure mode, a BSS is a single AP and its associated stations (Wireless Clients).
CCK	Complementary Code Keying (CCK): Part of 802.11b that replaces Barker coding to allow data rates of 5.5 and 11 Mbps.
CCMP	Counter mode with Cipher-block Chaining Message (CCMP) is a robust encryption mechanism that is part of 802.11i and replaces the use of legacy encryptions Authentication Code Protocol in modern Robust Security networks RSNs.
Channel	A contiguous grouping of frequencies of which the center frequency is used to define the grouping and is assigned a sequential number for identification within a given frequency range.
Channel Bonding	The simultaneous use of two Non-Overlapping channels for transmission to transmit data used in 802.11n and legacy “Super G” environments.

Term	Definition
Channel Width	The range of radio frequency allocated to specific RF channels. DSSS channels are 22MHz wide while OFDM channels are only 20MHz wide.
Co-Channel interference	This occurs when RF devices from different service sets are on the same center frequency (Channel) and occupy the same physical airspace increasing the size of the contention domain.
Contention Domain	Contention Domain is A shared medium in which devices use a non-guaranteed communication method forcing each node to negotiate with the other nodes using the medium for an opportunity to transmit.
Contention Free Burst	Contention Free Burst (CFB) may be used if a Quality of Service station (QSTA) has time remaining in a Transmit Opportunity (TXOP) and has additional data to send rather than contending for the media again.
Contention Window	Contention Window (CW): The levels of priority in EDCA (see *EDCA*) are called access categories (see *AC*.) The contention window (CW) can be set according to the traffic expected in each access category, with a wider window needed for categories with heavier traffic.
DBPSK	Differential Binary Phase Shift Keying (DBPSK) is a modulation scheme using the difference between successive phases rather than the bit pattern to set the phase of a wave used with Barker coding to achieve the 1 Mbps data rate in 802.11 transmissions.
DCF	The basic 802.11 MAC layer uses the distributed coordination function (DCF) to share the medium between multiple stations.
Destination Address	The final address to which a frame is sent that can be on either the LAN or WLAN.
DFS	Dynamic Frequency Selection (DFS) is used to avoid interference with other systems—most commonly radar systems—by detecting another device on the same channel and then moving to a clear channel that is part of 802.11h.
DIFS	Distributed Interframe Space (DIFS): The time period that a station (STA) waits before transmitting after the medium has been determined to be idle.
DLS	Direct Link Setup (DLS) is a process defined by 802.11e that allows Quality of Service Wireless Clients (QSTAs) to communicate directly with each other once associated through the same AP.
DPSK	Differential Phase Shift Keying (DPSK) is a modulation technique that uses each 1 bit to trigger a phase shift of 180 degrees, but does not use the 0 bits resulting in their having no effect.
DQPSK	Differential Quadrature Phase Shift Keying (DQPSK) is used in 802.11 networks to obtain the 2 Mbps having twice the data rate as Differential Phase Shift Keying (DPSK) while using the same signaling rate.
Distribution System	Distribution System (DS) is a network to which a WLAN connects that if more than one WLAN attaches becomes an Extended Service Set (ESS).

Term	Definition
Dual CTS Protection	Allows both RTS/CTS and CTS to Self protection modes for both legacy and HT devices within the same contention domain that may or may not be part of the same service set.
Dynamic SM Power Save	Similar to SM Power Save but the AP is allowed to trigger a station to power up additional radios by using an RTS/CTS exchange initiated by the AP thus powering up the stations radios more rapidly.
EDCA	Enhanced Distributed Channel Access (EDCA) is a prioritized collision avoidance mechanism used by Quality of Service Wireless Clients (QSTAs) within a Quality of Service Basic Service Set (QBSS). (Also see *AC*.)
EIFS	Extended Interframe Space (EIFS) is used before transmission, when a station determines that the medium is idle following reception of a frame believed to contain PHY errors.
EIRP	Equivalent Isotropically Radiated Power (EIRP) is the total output of a wireless system measured against an isotropic radiator comprised of the transmitting radios power and all gain and or loss introduced into the system.
EOPS bit	An End of Service Period (EOPS) bit is a bit used in a frame transmitted by the Hybrid Coordinator (HC) to notify Quality of Service Wireless Clients (QSTAs) that the frame is the end of a service period.
ERP	Extended Rate Physical (ERP): A clause 19 extension of the PHY that was used previously in both clause 15 and clause 18 Direct Sequence Spread Spectrum (DSSS) networks allowing higher data rates and modulation techniques.
ESS	Extended Service Set (ESS): One or more Basic Service Sets (BSS) that are interconnected and appear as a single BSS at the Logical Link Control sub-layer of the Data Link layer to any station associated with any of the connected service sets.
EVM	Error Vector Magnitude (EVM) is a measure of how far constellation points have deviated from ideal locations in digital transmissions and receptions used in performance measurements of transmitters and receivers.
FCS	Frame Check Sequence (FCS): A checksum value added to a frame for error detection that in generated using the same manner for both 802.3 and 802.11 frames.
FFT	Fast Fourier Transform (FFT) is an algorithm used in calculating the Discrete Fourier Transform (DFT) as part of converting data between time, space and frequency used largely by the Wi-Fi industry within Multiple Input Multiple Output (MIMO) and Multiple Input Single Output (MISO) transmissions.
Frame Aggregation	Combining multiple frames into a single frame for transmission.
GFSK	Gaussian Frequency Shift Key (GFSK): The modulation type used with Frequency Hopping Spread Spectrum to achieve data rates of 1 and 2 Mbps.

Term	Definition
Greenfield HT	An environment containing only HT (802.11n) devices not only in the service set but within the contention domain as well (no legacy devices are present i.e. no 802.11a/b/g radios in the area) also called Greenfield mode.
GTK	Group Temporal Key (GTK) is used to decrypt and encrypt broadcast and multicast traffic in an Extensible Authentication Protocol (EAP) protected network.
Guard Interval	A period of time that allows for late arriving symbols over long paths used in OFDM transmissions.
HC	Hybrid Coordinator (HC): A type of coordinator used in the Quality of Service (QoS) facility that implements the frame exchange sequences and medium access control service data unit (MSDU) handling rules defined by the hybrid coordination function (HCF).
HR/DSSS	High Rate Direct Sequence Spread Spectrum is the extended PHY specified in the 802.11b amendment that allows 5.5 and 11 Mbps data rates.
HT Protection Modes	Mode 0 = only HT radios in use no legacy radios present Mode 1 = HT non-member protection allows the HT service set containing all HT devices to be co-located with non-HT devices which are in the same service set. Mode 2 = HT 20MHz protection mode allows 20 MHZ HT stations to be part of a 20/40 MHz HT service set. Mode 3 = one or more non-HT stations are associated with the HT and are part of the service set.
LBT	Listen Before Talk (LBT)—also called Listen Before Transmit—requires a device to sense the medium to make sure it is idle prior to transmissions as a method of avoiding collisions.
Modulation	Any of several techniques for combining user information with a carrier signal from a transmitter.
MCS	Modulation Coding Schemes (MCS) define the modulation technique used to achieve specific data rates in 802.11 transmissions.
MISO	Multiple Input Single Output (MISO) is a system with two or more receivers and only one transmitter.
MTBA	A Multiple Traffic ID Block Acknowledgment (MTBA) is used with A-MPDUs to allow acknowledgments of the individual MPDUs contained in the A-MPDU because the individual MPDUs must be acknowledged.
NAV	A Network Allocation Vector (NAV) is a logical timer used in contention that sets the value to be decremented prior to transmission equal to the value found in the duration field of a frame detected while performing the Clear Channel Assessment (CCA).
OFDM	Orthogonal Frequency Division Multiplexing (OFDM) is a modulation technique used in the 5 GHz Spectrum with mandatory data rates of 6, 12, and 24 Mbps and optional rates of 9, 18, 36, 48 and 54 Mbps.

Term	Definition
Overlapping Adjacent Channel	RF channels with sidebands in the same frequency, also called adjacent interfering channels.
PBCC	Packet Binary Convolutional Coding (PBCC): A technique used to allow transmissions of 22 and 33 Mbps in 2.4 GHz as part of what was once called 802.11b+ or Super b.
PC	Point Coordinator (PC) is that part of an AP that performs the point coordination function for the service set, a service absent in ad-hoc networks.
PCF	Point Coordination Function (PCF) is an optional coordination function that allows contention free transmissions within the service set.
PCO	Phased Coexistence Operation (PCO): An alternate operational mode that alternates between 20MHz and 40MHz transmissions as a protection mechanism.
PER	Packet Error Rate (PER): A ratio of failed packet deliveries compared to the total number of packets sent to the intended receiver.
PIFS	Priority Interframe Space (PIFS) is the timing used by an AP in a Point Coordination Function (PCF) mode network during the contention free period (CF) to gain control of the medium to transmit beacons and retransmit frames for which it has not received an acknowledgment (ACK) frame.
PLCP	Physical Layer Convergence Protocol (PLCP) is a sub-layer of layer one that is responsible for handing off to layer two and receiving from layer two the frames to be transmitted or received.
PMD	Physical Media Dependent (PMD): A sub-layer of layer one that is responsible for sensing the medium as part of the clear channel assessment (CCA) and placing frames on the medium as well as retrieving them from the medium.
PMK	Pairwise Master Key (PMK) is a key used to derive lower level keys as part of an extensible authentication protocol (EAP) exchange.
PMKID	Pairwise Master Key Identifier (PMKID): Used in a key exchange to identify the association key as defined in 802.11i section 8.5.1.2.
PMKSA	Pairwise Master Key Security Association (PMKSA): The result of a successful IEEE 802.IX exchange, pre-shared PMK information, or PMK cached via some other mechanism as part of a key exchanged as defined in 802.11i.
PSDU	Physical Layer Convergence Protocol Services Data Unit (PSDU) is the information passed to and from the Media Access Control (MAC) sub-layer.
PSK	A Pre-shared Key (PSK) is a static key distributed to multiple devices.

Term	Definition
PS_POLL	Power Saving-Poll (PS_POLL) is a frame sent to an AP by a station (STA) upon awakening from power save mode or “dosing” that hears its identifier in the Traffic Indication Message (TIM), Delivery Traffic Information Message (DTIM), or Asynchronous Traffic Indication Message (ATIM) signaling that the AP has traffic buffered for the station (STA) that indicates to the AP that the station is awake and ready to receive that traffic.
PTK	Pairwise Transient Key (PTK): Developed locally by stations in a four way handshake as part of 802.11 authentication and not sent across the network this is a value that is derived from the Pairwise Master Key (PMK), Authenticator address (AA), Supplicant address (SPA), Authenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK).
Radio Chain	A set of two or more antennae and a radio used in multiples for MIMO transmissions.
RIFS	Reduced Interframe Space (RIFS) is a new Interframe Space defined in 802.11n with a duration of only 2usec (microseconds) supported only in Greenfield HT environments between HT radios.
RFC1042	A standard for the transmission of IP datagrams over IEEE 802 networks.
Spatial-Multiplexing	Spatial-Multiplexing is a power saving scheme introduced in 802.11n that allows a MIMO AP to power down all but one radio.
Spatial-OFDM	Spatial-OFDM is the combination of sending multiple independent streams and spatial diversity using multiple channels and sub-carriers also referred to as Spatial-Multiplexing using OFDM allowing multiple data streams to be used as part of a single signal.
TKIP	Temporal Key Integrity Protocol (TKIP) is a security protocol used in the IEEE 802.11 wireless networking standard.
TxBF	Transmit Beam Forming (TxBF) is also called Smart Antenna system or Phased Array Antenna system). It allows MIMO devices to focus the transmission beams in a coordinated method.
WEP	Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks.
WPA	Wi-Fi Protected Access (WPA) is a security protocol developed by the Wi-Fi Alliance to secure wireless computer networks.

Term	Definition
Xen Cloud Platform	Xen Cloud Platform (XCP) is a hypervisor (Host OS) using a micro-kernel design, providing services that allow multiple virtual (Guest OS) computer operating systems to execute on the same computer hardware concurrently.
Xen Hypervisor	Xen Hypervisor is also known as the Host Operating System which uses a micro-kernel design, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.
Zone Tracking	Uses the RSSI information to determine the associated zone by how close the client device is to a specific sensor in a monitored environment. It provides more granular detail than presence.

INDEX

A

B

C

D

L

M

N

O

P

R

S

T

U

V

W

Z

Zebra Technologies Corporation.
Lincolnshire, IL 60069 USA

MN000090A01 Revision F December 2015