



Extreme AirDefense User Guide

For Release 10.6

9037798-00
May 2023



Copyright © 2023 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Table of Contents

Preface.....	10
Conventions.....	10
Text Conventions.....	10
Terminology.....	12
Send Feedback.....	12
Help and Support.....	12
Subscribe to Product Announcements.....	13
Documentation and Training.....	13
Introduction.....	14
Scope of Documentation.....	14
Extreme AirDefense New User Experience.....	16
Login to ADSP.....	17
Logout of AirDefense.....	18
Setup Wizard.....	19
Download ADSP Toolkit.....	20
Download Toolkit from New User Interface.....	21
Launch the Old User Interface.....	22
Dashboard.....	24
View Dashboard.....	24
Set a Favorite Dashboard.....	26
Create a Dashboard.....	27
Manage Your Dashboard.....	31
Delete the Dashboard.....	33
Dashboard Widgets.....	34
WIPS Widgets.....	35
STATs Widgets.....	42
COMPLIANCE Widgets.....	47
Network View.....	49
Network Snapshot.....	49
Network Tree View.....	49
Details View.....	50
Device Details Screen.....	52
Network View - Network Snapshot.....	53
Top 5 Security Threats.....	54
Alarms and Actions.....	54
Polled Devices.....	54
Sensed Devices.....	55
Network Pane - Details View.....	55
Network Pane - Device Details.....	56

Device Details - Toolbar.....	58
Device Type Details.....	61
Alarm View.....	100
Alarms Summary.....	100
Network Tree View.....	100
Details View.....	102
Toolbar.....	103
Alarm View Drill Downs.....	104
Alarms - Alarms Summary.....	104
Alarms - Details View.....	105
Alarms Widget View.....	106
Category/Sub-category Widget.....	106
Device Classification.....	107
Rogue Activity.....	107
Alarm Severity.....	108
Alarm Details List.....	108
Alarm Actions.....	111
Configuration.....	113
Appliance Management.....	115
Appliance Settings.....	115
Backup / Restore Status.....	118
Certificate / Key Validation.....	118
Certificate Manager.....	120
Configuration Backup.....	132
Configuration Clear.....	136
Configuration Restore.....	138
Download Logs.....	139
View Performance Statistics.....	142
Language.....	142
Login / SSH Banners.....	143
Redundant Appliance Sync.....	145
Structure Configuration.....	148
Floor Plans.....	150
Triangulation Considerations	150
Policy Considerations	150
UI Scope Considerations	150
View And Manage Your Network Tree.....	151
Generate a Network Tree.....	153
Import the Network Tree.....	154
Floor Plans.....	155
Auto-Placement Rules.....	160
Auto-Placement Rules for Sensors.....	160
Auto-Placement Rules for Access Points and Switches	161
View Auto-Placement Rules.....	162
Add an Auto-Placement Rule.....	163
Edit an Auto-Placement Rule.....	165
Discovery Profile and Polling Configuration.....	166
Discovery Profile.....	167

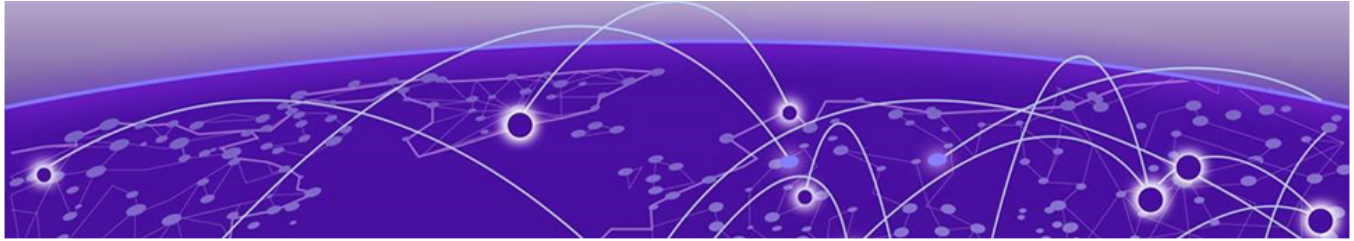
Polling Configuration.....	173
Communication Profile.....	177
Overriding Configuration Settings.....	178
View Communication Profiles	178
Add a Communication Profile.....	180
Edit the Communication Profile.....	184
Delete Communication Profiles	185
Security Profile.....	186
Overriding Configuration Settings.....	186
View Security Profile.....	187
Add a Security Profile.....	190
Edit a Security Profile.....	196
Delete a Security Profile	198
Alarm Action Manager.....	199
View Alarm Action Manager Rule Set	200
Add Alarm Action Manager Rule Set.....	203
Edit Alarm Action Manager Rule Set.....	219
Delete Alarm Action Manager Rule Set.....	220
Device Action Manager.....	221
View Device Action Manager Rule Set.....	222
Add a Device Action Manager Rule Set.....	224
Apply or Run the Device Action Manager Rule Sets.....	251
Sensor Manager.....	253
Operation Tab.....	254
Settings Tab.....	254
Overriding Configuration Settings.....	254
Operation Tab.....	255
Settings Tab.....	262
Alarm Configuration.....	268
Wired Network Monitoring	271
Network PCI Compliance Monitoring.....	272
Overriding Configuration Settings.....	273
Performance Profile.....	274
View Performance Profile.....	274
Add Performance Profile.....	275
Apply Performance Profile.....	287
Environment Monitoring.....	287
Apply Environment Monitoring Configuration.....	288
Overriding Configuration Settings.....	289
Client Types.....	289
Manage Client Types.....	290
Appliance Settings.....	291
Device Age Out.....	294
Configuration Backup.....	296
How Backups Work.....	296
View Backup Schedules.....	297
Scheduling Configuration Backup.....	298
Forensic and Log Backup.....	301
Forensic Backup Configuration.....	302

Log Backup Configuration.....	303
Configuration Restore.....	306
Download Logs.....	307
Forensic and Log Backup.....	309
Redundant Appliance Synchronization.....	311
How Synchronization Works.....	312
Synchronization Rules.....	312
.....	312
Automatic Synchronization.....	313
Appliance Replacement Considerations.....	315
Configuration Clear.....	316
Configurations.....	317
Language Settings.....	318
Change the Language.....	319
License Management.....	319
Overriding License Assignments.....	323
Auto Reassignment.....	323
Auto License Management.....	324
Add Licenses.....	326
Manage License Manually.....	327
User Management.....	330
Manage User Accounts.....	331
User Group Management.....	342
User Profile Management.....	349
Remote Profile Management	355
Add Remote Profile	355
Edit Remote Profile.....	359
Delete Remote Profile	359
System Settings.....	360
Data Format.....	361
Severity Levels.....	361
Add System Log Server IP Address.....	361
System Overview.....	363
AirDefense in Standalone Mode.....	364
System Components.....	364
System Requirements.....	365
Supported Hardware Appliances.....	365
Supported Browsers.....	366
Supported Operating Systems.....	366
Version Compatibility for Upgrade.....	366
Version 9.5.....	366
WiNG Version Compatibility.....	366
Extreme Wireless Version Compatibility.....	367
Extreme Cloud Appliance Compatibility.....	367
Connecting to Hardware Appliance.....	367
Connect a Laptop.....	367
Connect a Monitor and Keyboard.....	367
Access Appliance Remotely.....	367
Configuring the Appliance.....	368

Add-On Modules.....	368
Hardware Dependencies.....	369
System Configuration.....	369
Selecting and Deploying APs and Sensors.....	370
Supported APs.....	370
Off-Channel Scanning (OCS).....	370
Setting Up APs and Sensors.....	371
Connecting to the Network.....	371
Assigning User Interfaces.....	371
Default Login.....	372
User Accounts.....	372
User Types.....	372
System Access Limitations.....	373
Basic Navigation.....	373
Tree Structure.....	374
Device Search.....	374
Filters.....	374
Dashboard Drill Down.....	375
Alarm Time Reporting.....	375
Extreme AirDefense on Virtual Platform.....	376
Prerequisites.....	376
Required Files.....	376
Required License.....	377
Required System Configuration.....	377
Installing Extreme AirDefense 10.0 on VMware.....	377
Install Extreme AirDefense on Xen Hypervisor.....	386
Legacy Content.....	388
Menu.....	388
Installing the Toolkit.....	389
Open.....	390
Forensic Analysis-Basic.....	391
Advanced Forensic Analysis.....	395
Action Control.....	396
Reports.....	398
Report Builder.....	399
Scheduled AP Tests.....	409
Scheduled Vulnerability Assessment.....	412
Scheduled Events.....	415
Add Devices.....	417
Import and Discovery.....	423
Bluetooth Monitoring.....	433
AirDefense Dashboard.....	434
The Dashboard.....	434
Selecting Dashboard Scope.....	436
Customizing Dashboard Views.....	437
Dashboard Components.....	439
Network Tab.....	442
Select-Network View.....	443

Network Devices.....	444
Association Tree.....	451
Network Graph.....	452
Network Filters.....	454
Actions Menu.....	469
Actions Descriptions.....	470
Advanced Search.....	477
Alarms.....	480
Alarms Tab.....	480
Alarm Table.....	481
Alarm Filters.....	482
Alarm Categories and Criticality.....	490
Alarm Details.....	491
Alarm Actions.....	492
AirDefense Alarm Model.....	493
Configuration Tab.....	495
Search.....	496
Appliance Platform.....	497
Security & Compliance.....	536
Network Assurance.....	540
Operational Management.....	556
Appliance Management.....	638
Account Management.....	672
Drop-down Menu Access.....	694
Security.....	801
WIPS.....	801
Planning Your Sensor Deployment.....	802
Physical and Electromagnetic Interference.....	802
Planning Your Sensor Placement.....	805
Sensor Monitoring.....	808
Vulnerability Assessment.....	809
WEP Cloaking.....	811
ADSPAdmin.....	814
Accessing the ADSPAdmin Console.....	814
Manage System.....	815
Manage the Database.....	816
Software.....	816
Configure AirDefense.....	816
Troubleshooting.....	823
AP Testing.....	823
Connection Troubleshooting.....	823
Live RF.....	824
Forensic RF.....	825
Spectrum Analysis.....	825
Advanced Spectrum Analysis.....	826
Advanced Troubleshooting.....	828
Assurance Suite (Network Assurance).....	828
Radio Share Network Assurance.....	828
Customer Support.....	829

AirDefense Icons.....	829
AirDefense Application Icons.....	829
Wireless Client Icons.....	835



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Conventions

To help you better understand the information presented in this guide, the following topics describe the formatting conventions used for notes, text, and other elements.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings




Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions

Table 1: Notes and warnings (continued)



Icon	Notice type	Alerts you to...
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.

Table 3: Command syntax (continued)

Convention	Description
...	Repeat the previous element, for example, <i>member [member . . .]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Terminology

When features, functionality, or operation is specific to a device family, such as ExtremeSwitching, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the *device*.

Send Feedback

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, do either of the following:

- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and software compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other resources](#) such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.



Introduction

[Scope of Documentation](#) on page 14

This guide is designed to help you use the Extreme AirDefense® (AirDefense) version 10.6. AirDefense is designed to protect your network from wireless threats and attacks, maximize your wireless network performance and enforce policy compliance. As a standalone platform, AirDefense is part of a system that includes the AirDefense appliance. The AirDefense appliance comes ready with the application and all supporting software preloaded.

AirDefense enables you to administer and configure your network efficiently using our detailed dashboards and the network and alarms views. Use the floor plan configuration to locate devices in your floor plan.



Note

The old user interface is still available for use and can be launched from within the new user interface.

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 the following Extreme AirDefense features:

- AirDefense New User Experience
 - Dashboard
 - Network
 - Alarms
 - Configuration
- AirDefense Old User Interface
 - 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 *Extreme AirDefense 10.4 Appliance Installation Guide* available at the following URL:

[Extreme Networks Documentation Site](#)



Extreme AirDefense New User Experience

[Login to ADSP](#) on page 17

[Setup Wizard](#) on page 19

[Download ADSP Toolkit](#) on page 20

[Launch the Old User Interface](#) on page 22

Extreme AirDefense's upgraded user interface provides a desktop oriented workflow for managing your AirDefense monitored network . This new user interface, with its fully customizable dashboard, alarms and network views, is now enhanced with a set of configuration screens that enable you to configure your AirDefense monitored network.

AirDefense also retains the original user interface for those users who would prefer to use it. This user interface can be launched at any time from within the new user interface. When launched, the original user interface is displayed in a new browser tab and is independent of the new interface.

The following views are available:

- Dashboard
- Network View
- Alarm View
- Configuration View

The **Dashboard** view is fully customizable and provides you with a large set of widgets that you can use in your dashboards to get a deeper insight into your AirDefense managed network. You can create any number of dashboards containing only those widgets that display the data that interests you. See the topic [Dashboard](#) to learn more about AirDefense dashboards.

The **Network** view provides a deep insight into the state your network. Multiple screens enable you to drill down to view the statistics and state of individual devices that are a part of your network while retaining the ability to keep an eye on the overall state of the whole network. See the topic [Network View](#) to learn more about AirDefense's new Network view.

The **Alarm** view displays comprehensive information about alarms seen in your network. Multiple screens enable you to drill down to view details about each alarm

and to take appropriate actions to mitigate risks indicated by these alarms. See the topic [Alarms](#) to learn more about AirDefense's new Alarms view.

The **Configurations** view displays the various AirDefense parameters that can be set using this user interface. The following top level configuration settings can be managed:

- Rules / Profile Settings - You can configure *Auto Placement*, *Discovery/Polling*, and *Communication Profile* from this configuration settings menu item.
- Operational Settings - You can configure *Sensor* and its other settings from this configuration menu item.
- General Settings - You can configure AirDefense's network tree *Structure*, *License* from this configuration settings menu item. You can also create and manage *Users* from within this settings group. The *System Settings* screen enables you to configure a remote syslog server where you can record any user activity on this AirDefense instance.

See the topic [Configuration](#) to learn more about configuring your AirDefense system.

Login to ADSP

With the introduction of the new user experience, the way you login to AirDefense has been updated to reflect the style of the new interface.

To login to your AirDefense installation's web interface, enter the IP address of the AirDefense server in a browser window. The **AirDefense Login** screen displays.

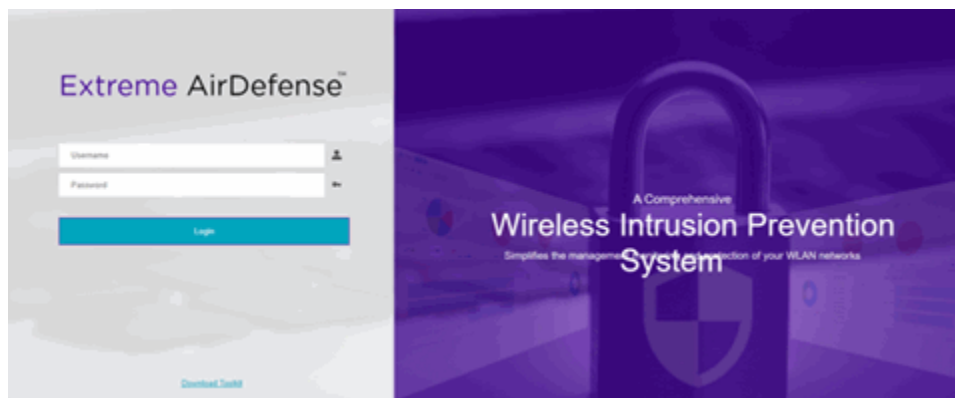
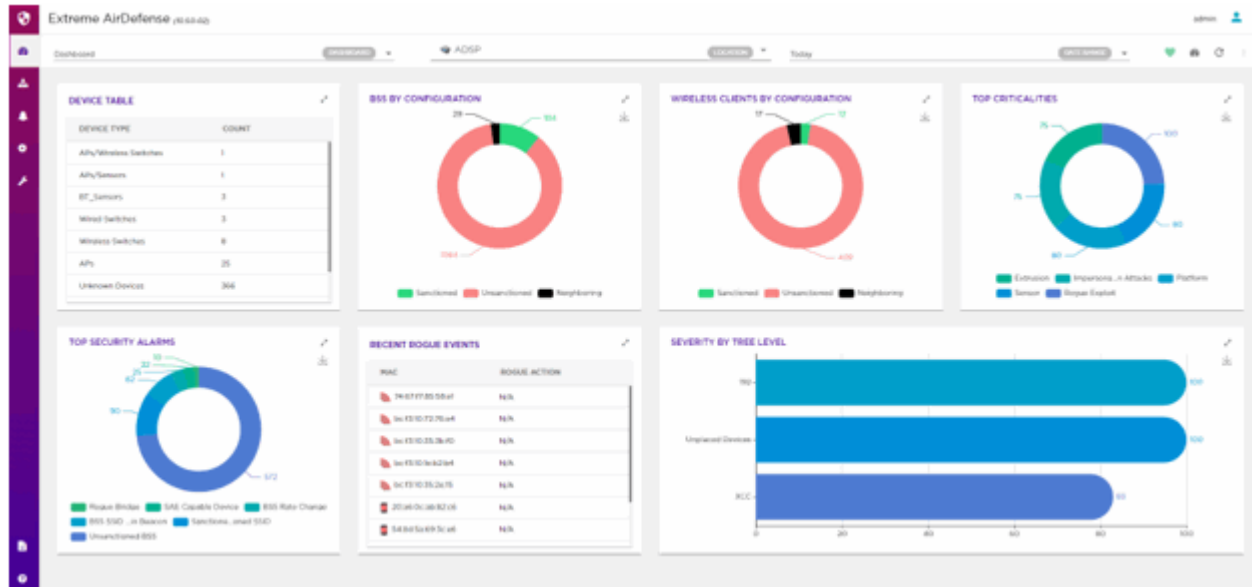


Figure 1: AirDefense Login Screen


1. Enter your username in the **Username** field.
2. Enter the password in the **Password** field. This password must be the one that is appropriate for the username entered in the **Username** field.

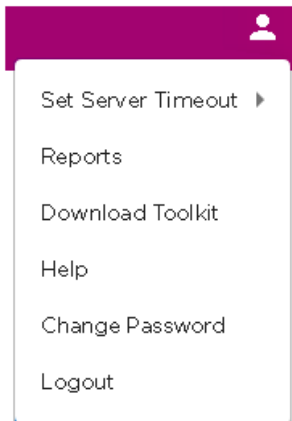
- Click the **Login** button.
On providing the correct credentials for your account, the default **Dashboard** for your account is displayed.



Logout of AirDefense

To logout of the new user interface:

- Select the  icon located to the top right of the user interface. A drop-down menu displays.

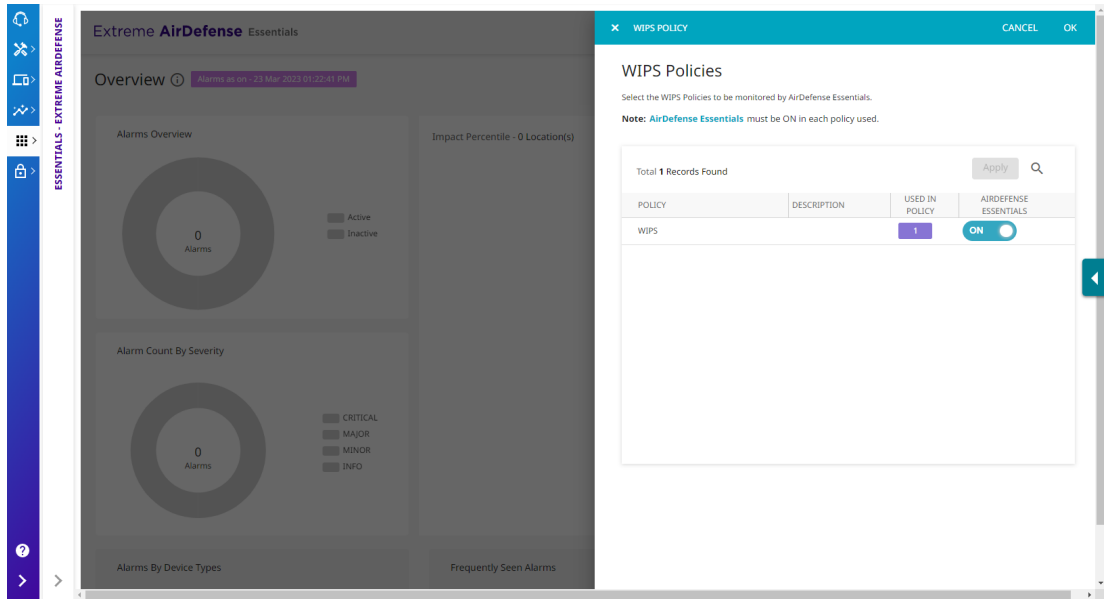


- Select the **Logout** menu item. A confirmation dialog displays.



3. Select **Yes** to exit out of the AirDefense user interface.

You are immediately logged out of the user interface and the AirDefense login screen displays.

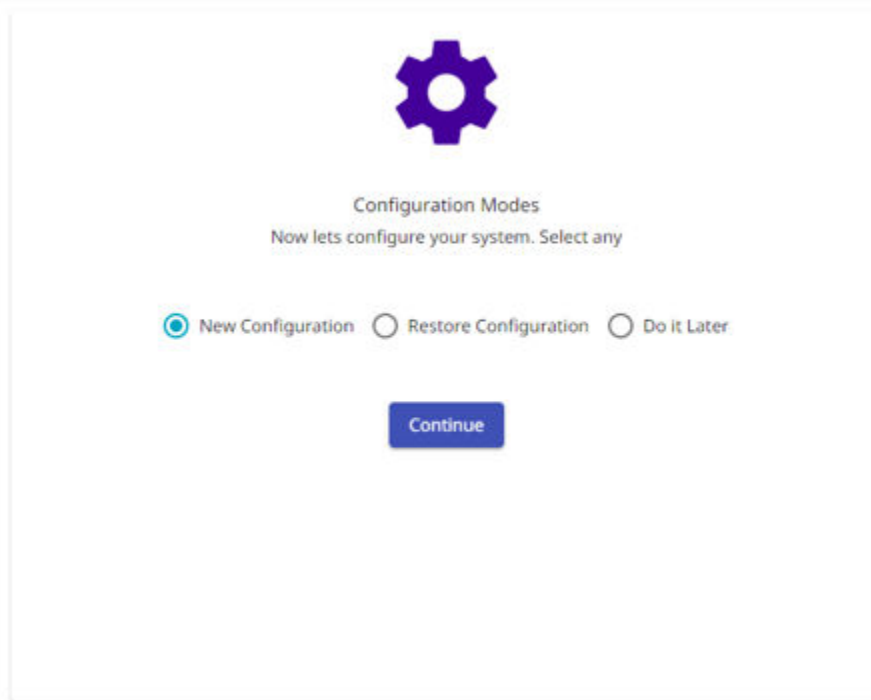


Select **No** to remain within the user interface and not logout of it.

Setup Wizard

At first login, Extreme AirDefense directs you to the setup wizard. Use the wizard to configure the system, import floor plans, and place your access points.

You can also select **Do it Later** from the **Configuration Modes** screen, which skips the wizard, letting you set up polling manually. You can also choose this option if you want to import your configuration from ExtremeCloud IQ Controller, which supports the automatic download of tree nodes, floor plans, and access point placements into AirDefense.



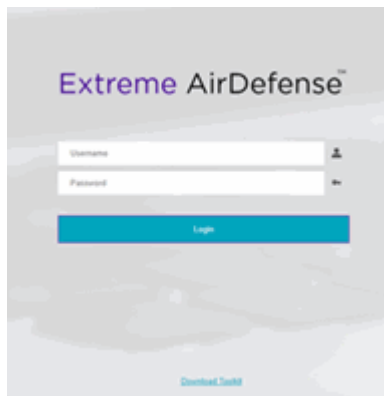
Download ADSP Toolkit

AirDefense Toolkit is a set of utilities for managing an AirDefense instance. The following operating systems can be used to install the AirDefense toolkit

- Window 7
- Windows 10 Enterprise
- Linux
- Apple Mac (Thin Client Applications only)

To download the AirDefense Toolkit:

1. From the login screen, select the **Download Toolkit** link located at the bottom of the screen.




The **Download Toolkit** dialog displays.

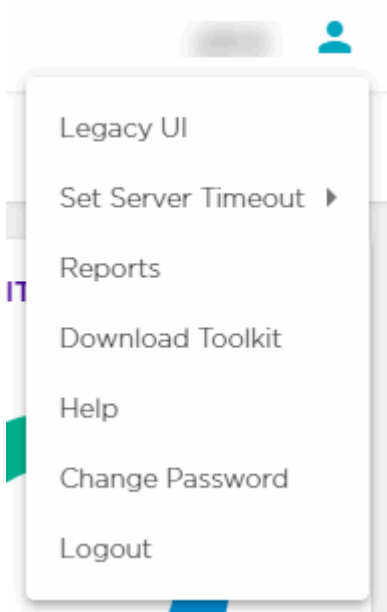


2. From the **Download Toolkit** dialog, select the appropriate download file for your operating system.
3. Once you have downloaded the toolkit and other tools from the dialog box, select the **OK** button to close the dialog.

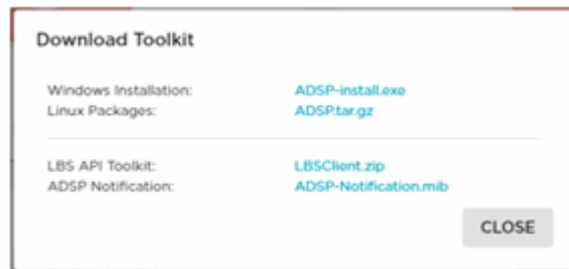
Download Toolkit from New User Interface

To download the AirDefense Toolkit from within the new user interface:

1. Select the  icon located to the top right of the user interface. A drop-down list displays.



2. Select **Download Toolkit** from the list. The **Download Toolkit** window opens.




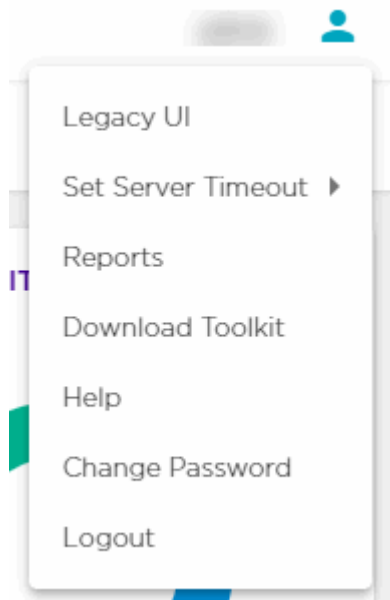
3. From the **Download Toolkit** window, select the appropriate download file for your operating system.
4. Once you have downloaded the toolkit and other tools from the dialog box, select the **CLOSE** button to close the window.

Launch the Old User Interface

AirDefense has retained the old user interface for those users who would prefer using it. This user interface is launched from within the new user interface. When launched, the old user interface displays in a new browser tab. This tab is independent of the new interface. You need not login again.

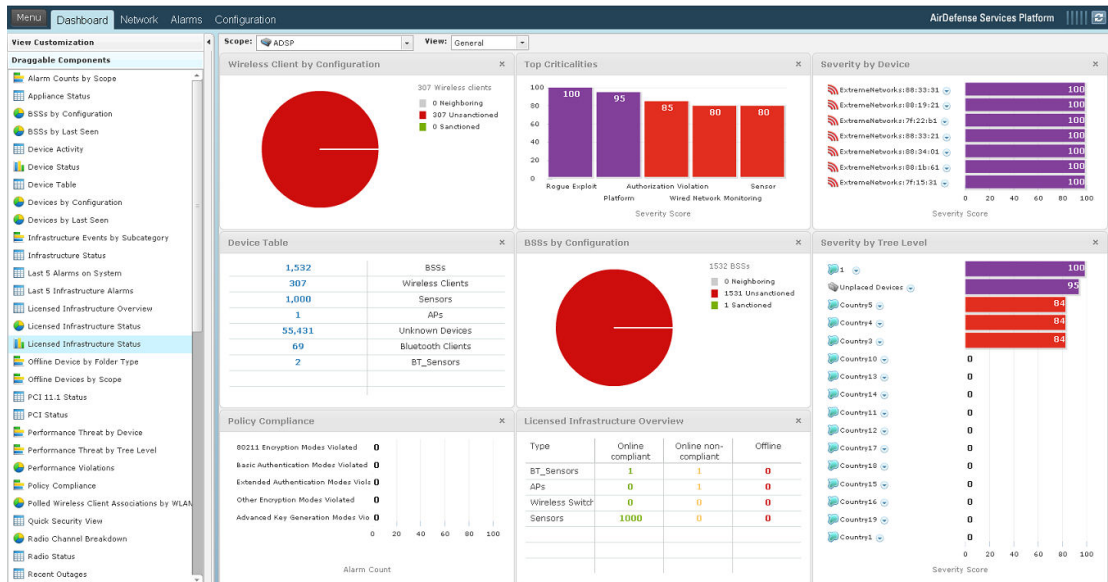
To launch the old user interface:

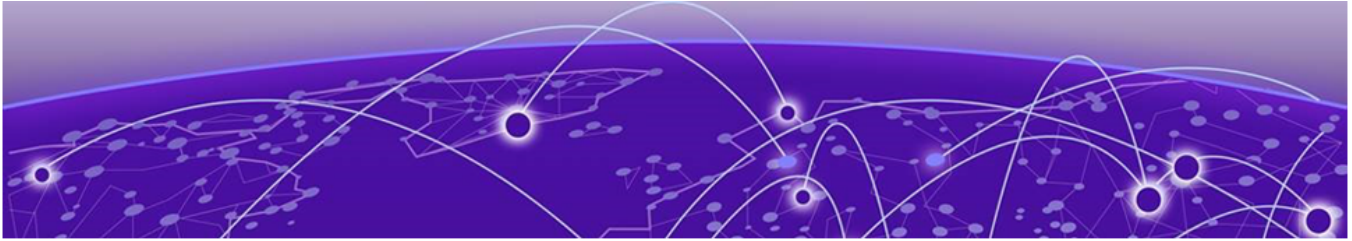
1. From within the new user interface, select the menu  icon located at the top right of your dashboard to expand the list of functions:



2. Select the Legacy UI from the menu.

A new browser tab opens and the AirDefense default **Dashboard** displays.





Dashboard


- [View Dashboard](#) on page 24
- [Create a Dashboard](#) on page 27
- [Manage Your Dashboard](#) on page 31
- [Delete the Dashboard](#) on page 33
- [Dashboard Widgets](#) on page 34

Use the fully customizable Extreme AirDefense (AirDefense) Dashboard to view various data and statistics for the sites managed through your AirDefense instance. Use the large number of built-in widgets to create customized desktops to view data and statistics. You can create any number of custom dashboards to meet your requirements.

AirDefense dashboards also includes a very powerful and fully customizable filter function to customize the data that you wish to view. You can filter the data displayed through a dashboard and its widgets by a site's location or by its site group. Further, you can also filter your data on the time duration of interest. These options, location and time, can be applied independent of each other.

View Dashboard

To load and view the **Dashboard**, select the  icon from the main toolbar to the left of the screen.

The dashboard marked as *Default* automatically loads. The default dashboard is indicated with the  icon next to its name in the **Dashboard** drop-down list.

AirDefense provides a pre-configured dashboard that displays important information. This dashboard is always named *Dashboard* and cannot be modified or deleted. When you login to your AirDefense account for the first time, this is the only dashboard that is available for immediate use.

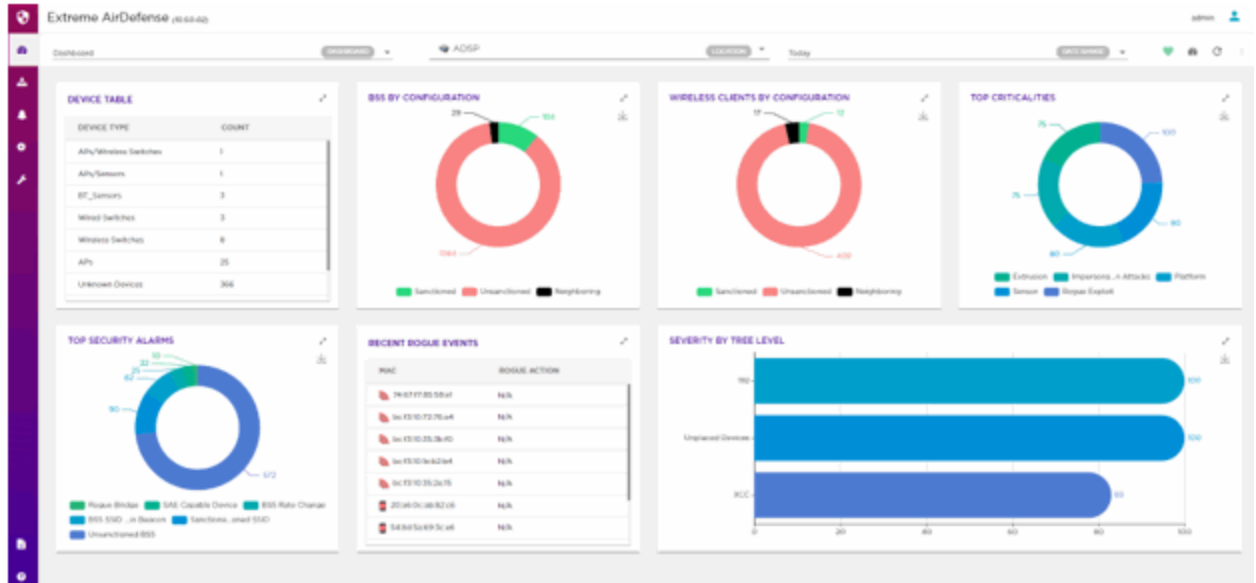




Figure 2: The Default Dashboard

To select a different dashboard, use the **Dashboard** drop-down list and select the dashboard that you want to view. The selected dashboard loads and the screen refreshes to display the latest data using the widgets placed on the dashboard.

To manually refresh the data on the screen, select the  button from  tool bar. Use this button periodically to refresh the data on the dashboard.



Note

Widgets placed on the **Dashboard** do not refresh automatically. You need to manually refresh the screen.

Use the **Location** drop-down list to select the scope of the data to show on a AirDefense dashboard. By default, data for the complete AirDefense system is displayed. When a scope is defined by using the **Location** drop-down list, the dashboard refreshes to display data for the selected site or a group of sites.

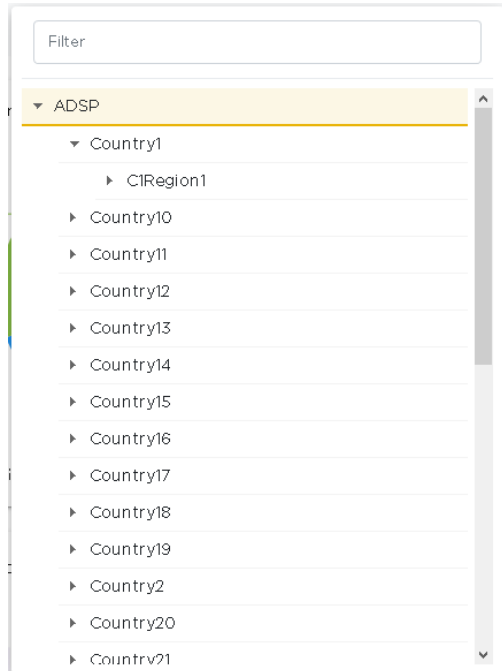


Figure 3: Location Drop-Down List

Use the **Date Range** drop-down list to select a time duration to display data for. The drop-down provides a set of pre-configured durations for filtering data. The available pre-configured durations are:

- Today - Displays the data for the current date. Excludes data for all other dates.
- Last 3 Days - Displays the data for the last 3 days prior to the current date. Includes data for the current date. Excludes data for all other dates.
- Last 5 Days - Displays the data for the last 5 days prior to the current date. Includes data for the current date. Excludes data for all other dates.



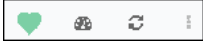

When a scope is defined using the **Date Range** control, the dashboard refreshes to display data for the selected time duration.

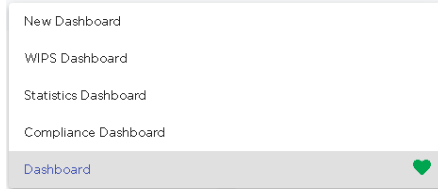
Set a Favorite Dashboard

A *Favorite* dashboard is a dashboard that you create and then customize to display the data and statistics that interests you. Every time you login to your AirDefense account, the dashboard marked as *Favorite* is always loaded.

For every account, AirDefense provides a default dashboard that is named *Dashboard*. Initially, this dashboard is also marked as the favorite dashboard for the account. This dashboard cannot be modified, deleted, or renamed.

You can create any number of dashboards for your ExtremeLocation instance. However, at any time, you can have only one dashboard as a favourite dashboard.

A favourite dashboard is indicated with the  symbol next to its name in the dashboard list and by the  icon on the  toolbar. For a normal dashboard, the same icon is displayed as .



1. Select the **Dashboard** drop-down list to display a list of available dashboards.

A default dashboard is indicated by the  icon next to its name.

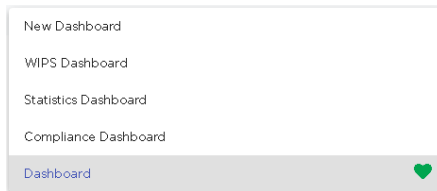




Figure 4: Default Dashboard

2. Select the dashboard that you want to mark as favourite.


The selected dashboard loads.

3. Select the  icon from the  toolbar.

The selected dashboard is immediately marked as the favourite dashboard. This dashboard loads automatically the next time you login to your AirDefense account.

Create a Dashboard

To create a new Extreme AirDefense dashboard:

1. From the main menu on the left, select the  icon to load the **Dashboard** screen. The dashboard marked as favorite automatically loads.

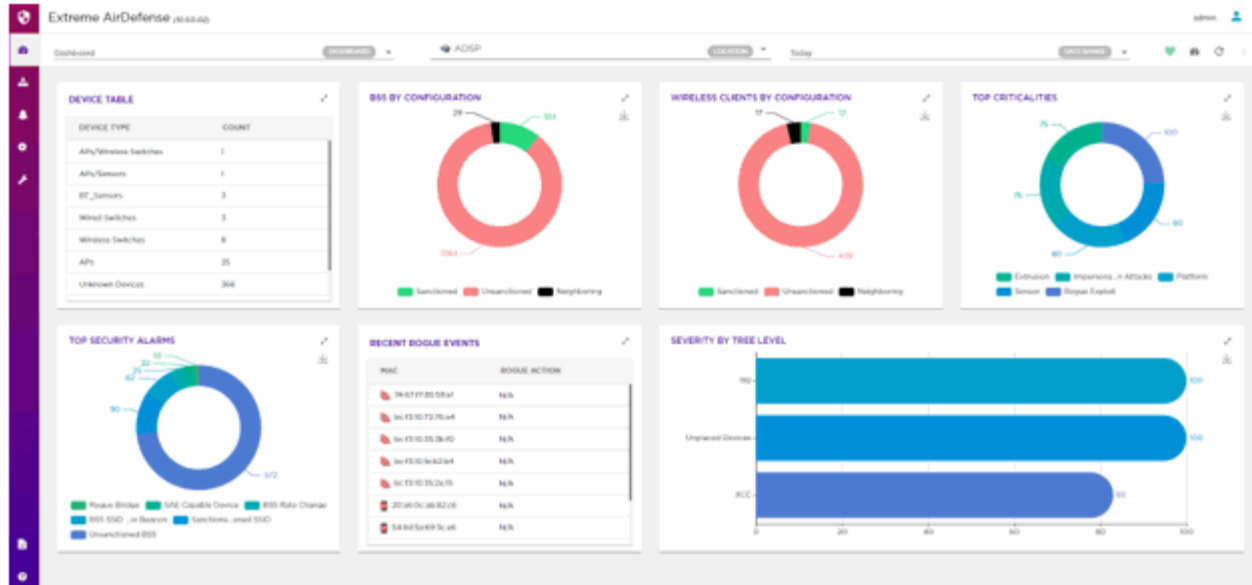


Figure 5: The Dashboard Screen

2. Select the  button from  tool bar. The button expands to display a drop-down list.

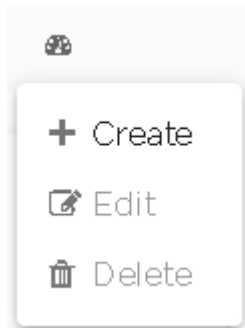


Figure 6: Manage Dashboard Options

3. Select the **Create** menu item from the drop-down list.
The following screen appears.

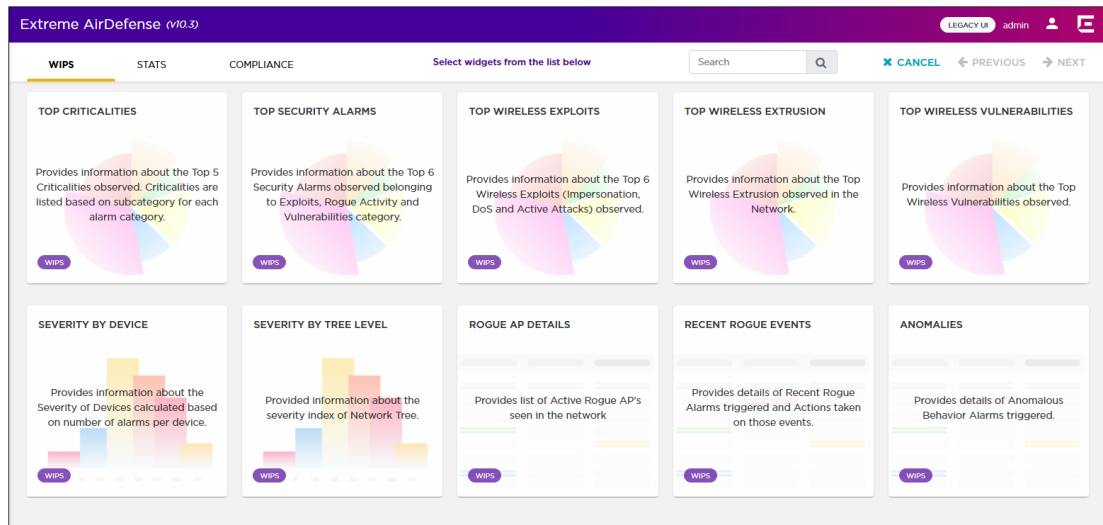


Figure 7: New Dashboard Screen

4. Select one category from the available categories. These categories classify the widgets available for use within your dashboard.

Dashboard widgets are classified into:

- **WIPS** - Use the widgets in this category to display WIPS information and statistics.
- **Stats** - Use the widgets in this category to display general statistics.
- **Compliance** - Use the widgets in this category to display PCI compliance statistics.

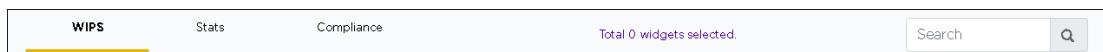


Figure 8: Widget Categories

Use the **Search** text box to drill down to the widgets of interest.



Note

You cannot have more than 14 widgets on a single dashboard. Create a new dashboard to add additional widgets.

- Click the widget to select it. At a time, you can select multiple widgets to add to the dashboard.

A green check mark appears on the top right of the selected widget.

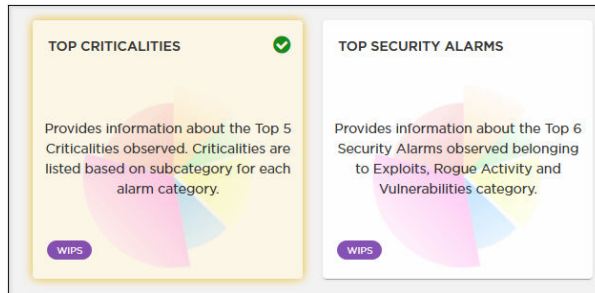


Figure 9: A Selected and an Unselected Widget

The screen also indicates the number of widgets added to this new dashboard.

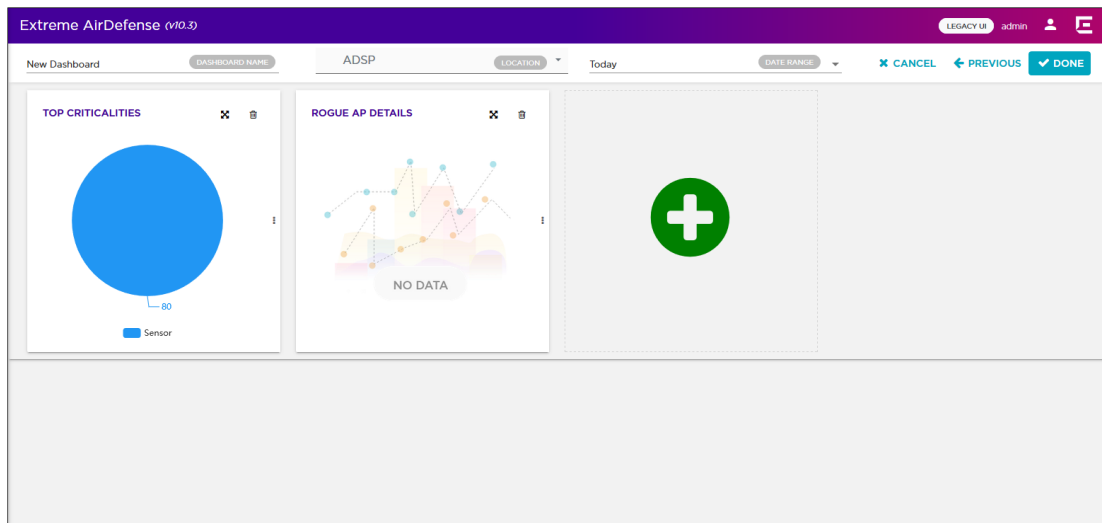



Note

To add a widget from a different widget category, select that category from the available options and continue adding widgets. You can combine widgets from all the categories to create your dashboard. You cannot, however, add more than fourteen (14) widgets to a dashboard.

- Select the **Next** button located to the top right of the screen.

The following screen appears:



To remove a widget already placed on the dashboard, use the  icon located to the top of that widget. This immediately removes the widget from the dashboard.





Note


You can also use the big green circle to add more widgets to this dashboard.


**Note**

When a widget is added to the dashboard, it will display its data even when its dashboard is being created or edited. This is by design.

- Use the  button, located to the top right of each widget, to rearrange the selected widget on the dashboard.

Hover over the widget's title. The arrow changes to . Then click and hold the primary mouse button, and drag the widget to the desired location on the dashboard. The other widgets on the dashboard are automatically rearranged to accommodate the moved widget.

- Use the resize bar that is displayed - when you hover over the  icon to the left of the widget - to resize the widget.

The arrow changes to . Then click and hold the primary mouse button, and drag the edge of the widget to resize it. The other widgets on the dashboard are automatically rearranged to accommodate the resized widget.

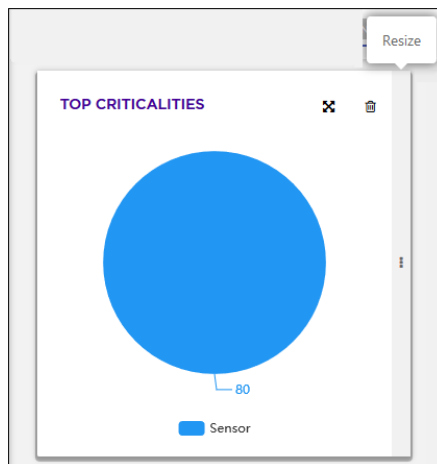


Figure 10: Widget with resize bar

**Note**

You cannot increase the height of the widget. Widget width can only be increased in fixed increments. You can only resize to the next available size.

- Enter a name for this dashboard in the **Dashboard** field located to the top left of the new dashboard.
- Select the **Done** button to save the final dashboard layout.
The dashboard is saved and displays the configured data. At any time use the **Previous** button to navigate to the previous screen. Similarly, use the **Cancel** button to exit without creating the dashboard.

Manage Your Dashboard

Use the tools provided in the **Dashboard** screen to edit any dashboard in your AirDefense account.

To edit an existing dashboard:


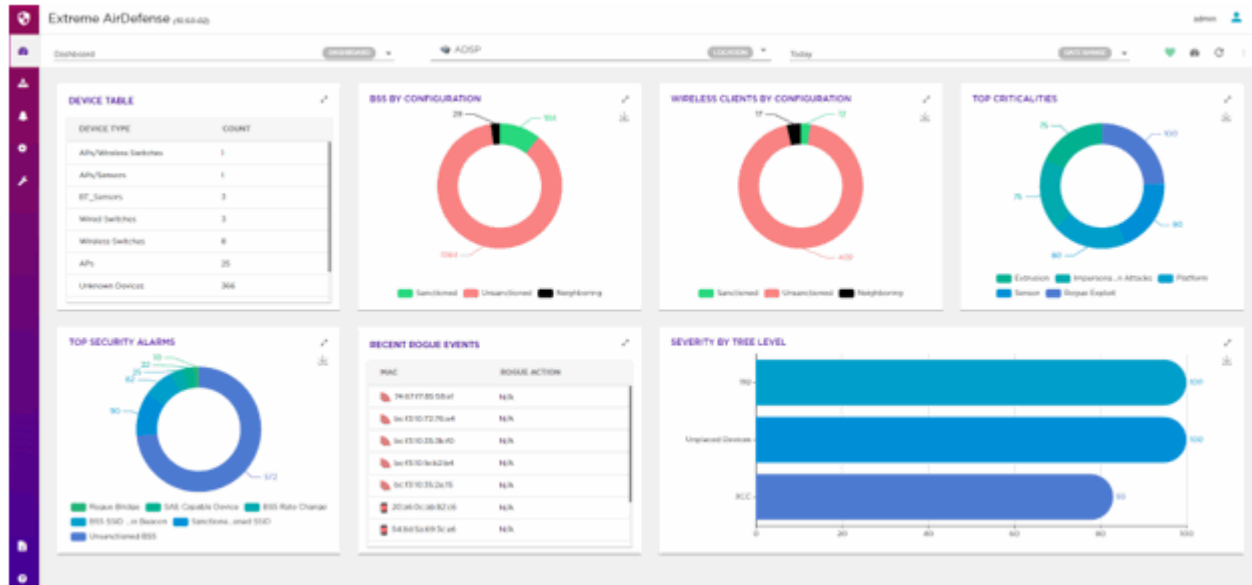
1. From the main menu on the left, select the  icon to load the **Dashboard** screen. The dashboard marked as default automatically loads.

Figure 11: The Dashboard Screen



2. Select the **Dashboard** drop-down list to expand and display the list of available dashboards for this AirDefense account.
3. From the list of available dashboards, select a dashboard.

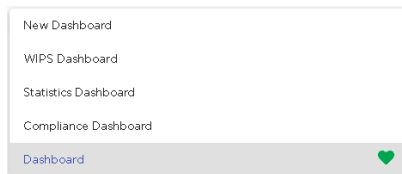


Figure 12: Dashboard List

The selected dashboard loads.

4. Select the  button from  tool bar. The button expands to display a drop-down list.

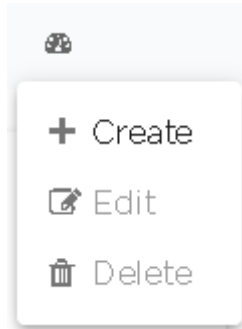


Figure 13: Manage Dashboard Options

5. Select **Edit** option from the drop-down list.
The selected dashboard is loaded in the edit mode. Use the available options to edit your dashboard.
6. After editing the dashboard, select the **Done** button to the top right of the dashboard to save the changes made to this dashboard.

Delete the Dashboard


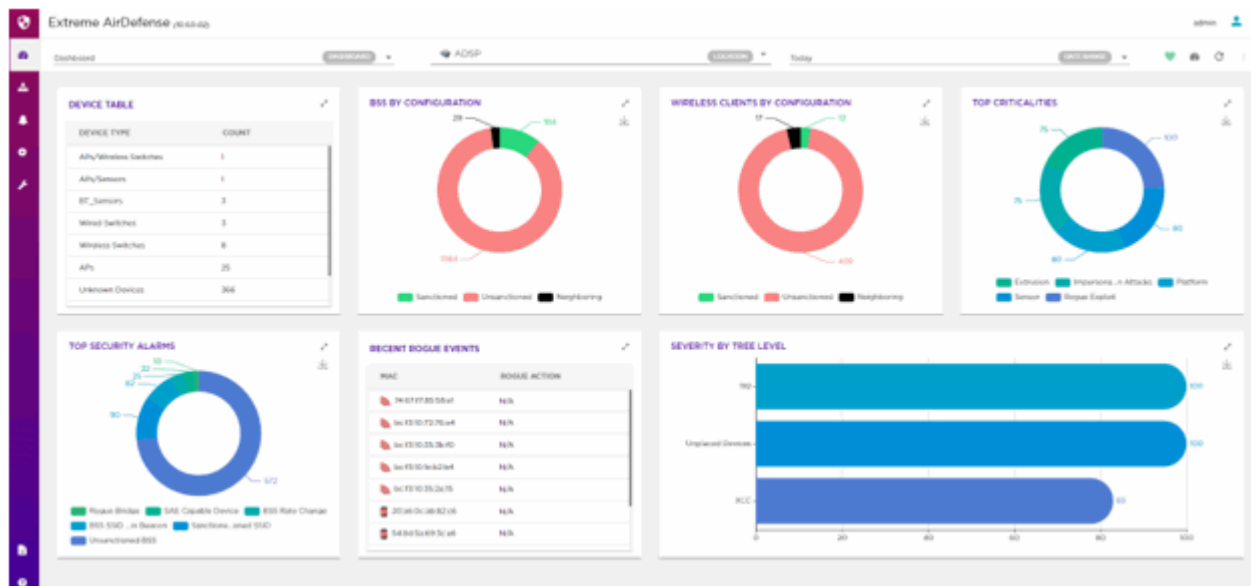
1. From the main menu on the left, select the  icon to load the **Dashboard** screen. The dashboard marked as default automatically loads.

Figure 14: The Dashboard Screen



2. Select the **Dashboard** drop-down list to expand and display the list of available dashboards for this AirDefense account.

- From the list of available dashboards, select a dashboard.

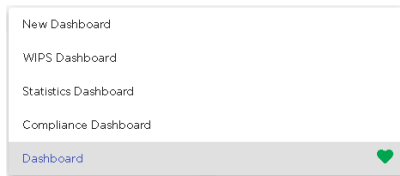


Figure 15: Dashboard List

The selected dashboard loads.

- Select the  button from  tool bar. The button expands to display a drop-down list.

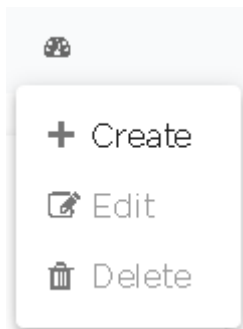


Figure 16: Manage Dashboard Options

- Select **Delete** from the drop-down list. A confirmation dialog appears.

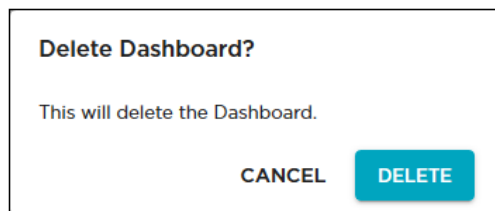


Figure 17: Delete Confirmation Dialog

- Select **Delete** to delete the dashboard. Select **Cancel** to exit this screen without deleting the selected dashboard. If **Delete** is selected, the dashboard is immediately deleted.

Dashboard Widgets

Extreme AirDefense provides a large number of widgets to enable you to customize how you view the large amount of data that it generates. These widgets displays the data of interest from Extreme AirDefense using tables and graphs. Some widgets also allow you to filter the data shown in them using filters and other elements specific to that widget.

Widgets on the **Dashboard** screen are classified into:

- **WIPS** - Use the widgets in this category to display WIPS information and statistics.
- **Stats** - Use the widgets in this category to display general statistics.
- **Compliance** - Use the widgets in this category to display PCI compliance statistics.



Figure 18: The Widget Categories

Use the **Search** text box to drill down to the widget or widgets of interest.

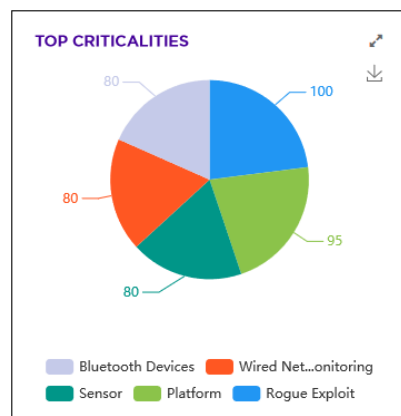
WIPS Widgets

Use the WIPS widgets to view AirDefense alarm activity and threat detection details. The following widgets are available:


- [Top Criticalities](#)
- [Top Security Alarms](#)
- [Top Wireless Exploits](#)
- [Top Wireless Extrusions](#)
- [Top Vulnerabilities](#)
- [Severity By Device](#)
- [Severity By Tree Level](#)
- [Rogue Access Points](#)
- [Recent Rogue Events](#)
- [Anomalies](#)
- [Top BT Security Alarms](#)
- [BT Security Threat By Category](#)
- [BT Security Threat By Tree Level](#)

Widget - Top Criticalities


This widget displays the top 5 criticalities observed in the AirDefense system.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

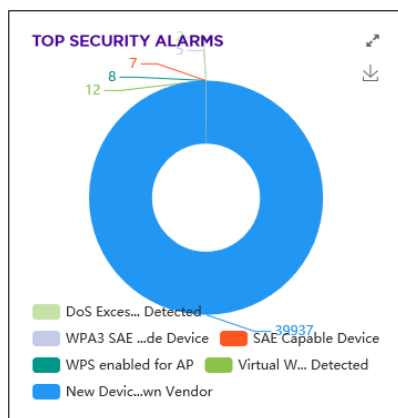
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Top Security Alarms


This widget displays the top security alarms observed in the AirDefense system. Security alarms observed in the *Exploits, Rogue Activity* and *Vulnerabilities* categories are displayed.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

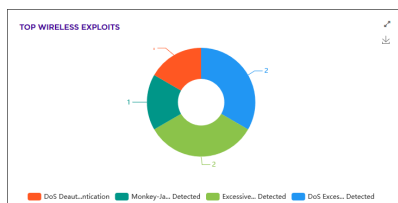
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Top Wireless Exploits


This widget displays the top 6 wireless exploits observed in the AirDefense system. Some of these exploits are *Impersonation, DoS* and *Active Attacks*.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

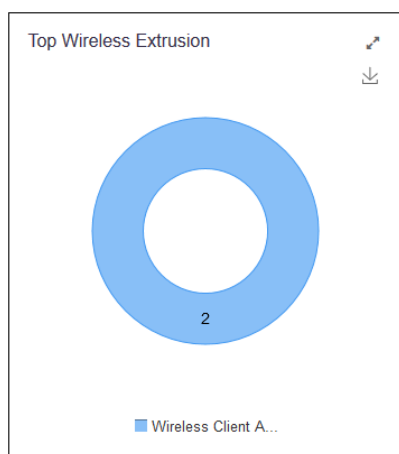
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Top Wireless Extrusions


This widget displays the top 6 wireless extrusions in your AirDefense monitored network. Extrusions happen when a sanctioned wireless station such as an access point or a sensor connects to an external unsanctioned network.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

Use the  icon to expand the widget to fill the current view.

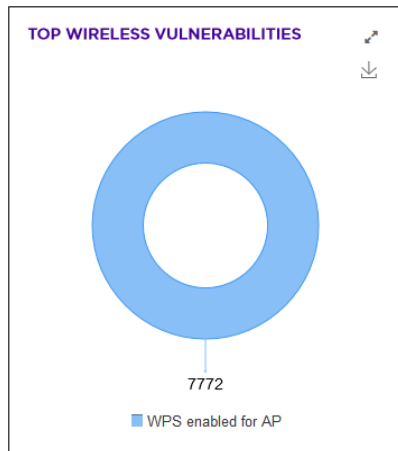
Hover on any of the widget's data points to view specific information on the selected data point. When hovering on a part of the Pie chart, the section of the chart under the mouse pointer is exploded out.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.


Widget - Top Vulnerabilities

This widget displays the top wireless vulnerabilities observed in the AirDefense system. Vulnerabilities are weaknesses that are not actively exploited, but are weaknesses that have been detected in the network. 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.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

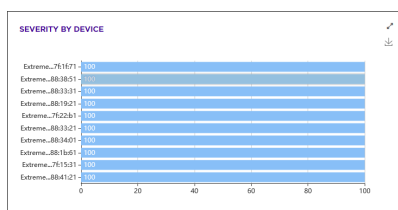
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Severity by Device


This widget displays the top devices with maximum severity identified by AirDefense.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

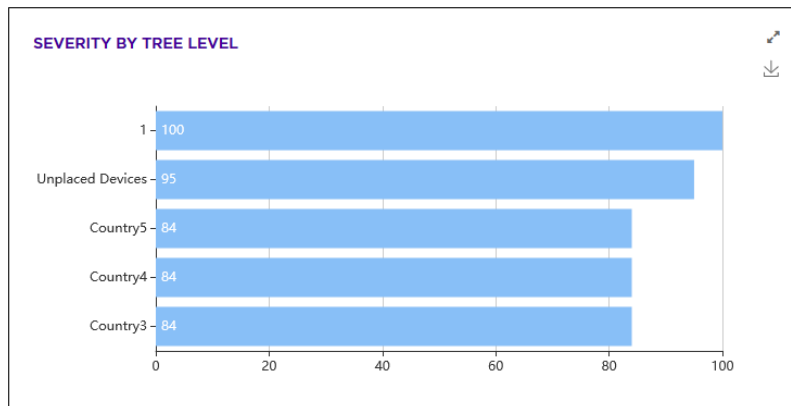
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Severity by Tree Level

This widget displays a graph for the severity index of the current selected network tree.



Use the  icon to expand the widget to fill the current view.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Rogue Access Points

This widget displays a list of all rogue access points seen by AirDefense and the location where the rogue device is found.

Scope	Rogue
Floor 1	ExtremeNetworks:7...
Floor 1	ZebraTechnologies:...
Floor 1	ZebraTechnologies:...
Floor 1	ExtremeNetworks:3...
Floor 1	ExtremeNetworks:7...
Floor 1	ExtremeNetworks:a...
Floor 1	ExtremeNetworks:d...
Floor 1	ExtremeNetworks:0...
Floor 1	ExtremeNetworks:R

The widget displays a table with the rogue access point's location and its MAC address.

Use the  icon to expand the widget to fill the current view.


Widget - Recent Rogue Events

This widget displays a list of recent rogue events identified by AirDefense. Rogue Activity includes events for devices participating in unauthorized communication in your network. Examples of the type of event included in this category are detection of a wireless device operating in your network or the detection of an unsanctioned wireless device communicating with a device in the wired network.

RECENT ROGUE EVENTS

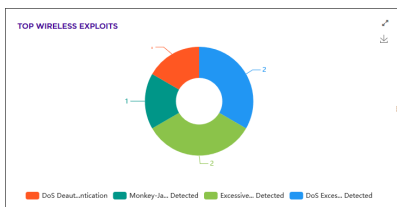
MAC	ROGUE ACTION
00:25:45:a9:5e:56	N/A
00:25:45:af:c5:02	N/A
00:25:45:b2:05:2e	N/A
00:25:45:b1:c4:ba	N/A
00:25:45:ae:19:46	N/A
00:25:45:a9:83:72	N/A

The widget displays a table with the action taken on the rogue device and the device's MAC address.


Use the  icon to expand the widget to fill the current view.

Widget - Anomalies

This widget displays the various anomalies identified in the AirDefense system. Some of these exploits are *Impersonation*, *DoS* and *Active Attacks*.

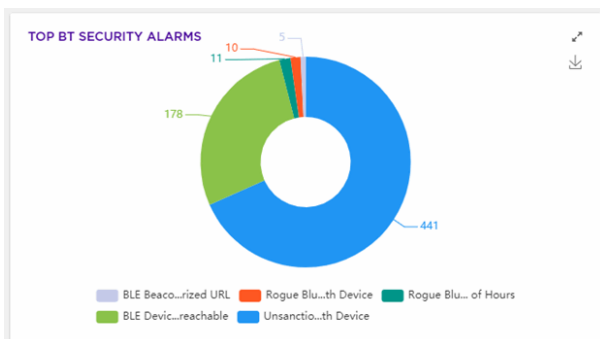


Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.


Use the  icon to expand the widget to fill the current view.

Widget - Top BT Security Alarms


This widget displays the top security alarms for Bluetooth devices observed in the AirDefense system. .



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

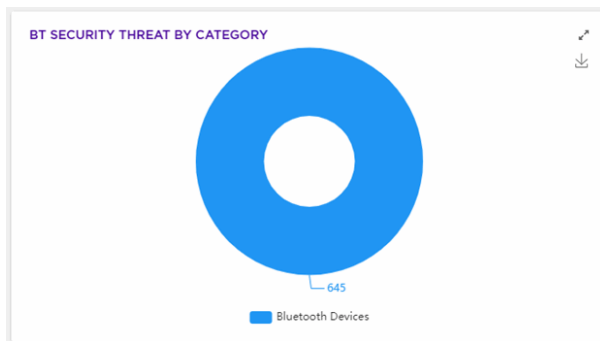
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - BT Security Threat By Category


This widget displays the top security threats by category for Bluetooth devices observed in the Extreme AirDefense system.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

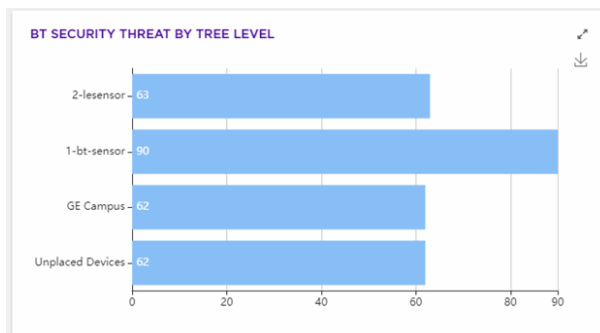
Use the  icon to expand the widget to fill the current view.


Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - BT Security Threat by Tree Level

This widget displays a graph of the security threats for Bluetooth devices in the current selected network tree.



Use the  icon to expand the widget to fill the current view.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.


STATs Widgets

Use the STATs (statistics) widgets to view AirDefense statistics. The following widgets are available:

- [Device Table](#)
- [BSS by Configuration](#)
- [Sanctioned BSS Seen in Last 5 Days](#)
- [Wireless Clients by Configuration](#)
- [Top Talkers](#)
- [BT / BLE Seen In Last 5 Days](#)
- [BT By Configuration](#)
- [BT Protocol Stack Count Comparison](#)

Widget - Device Statistics Table

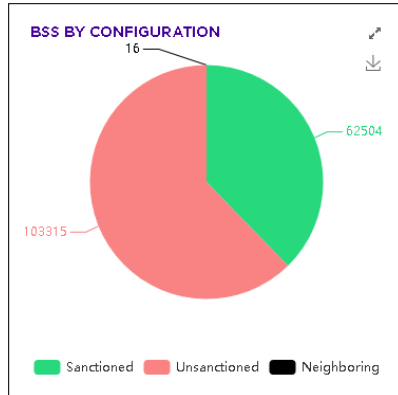
This widget displays the counts of different devices seen by AirDefense in the network.

DEVICE TABLE 	
DEVICE TYPE	COUNT
Wireless Switches	1
APs	15
Sensors	2003
BSSs	165833
Unknown Devices	217775
Wireless Clients	490497


Use the  icon to expand the widget to fill the current view.

Widget - BSS by Configuration


This widget displays the counts of BSSs seen by AirDefense in the network by classification type. The BSSs are classified as *Sanctioned*, *Unsanctioned*, and *Neighboring*



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

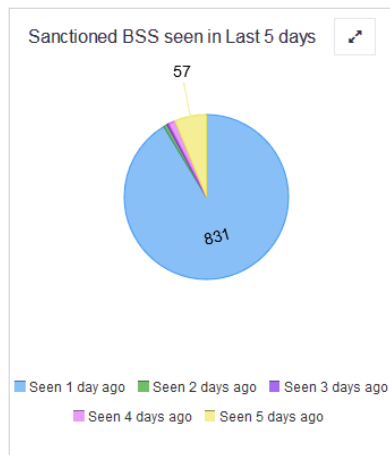
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Sanctioned BSS Seen In Last 5 Days


This widget displays the counts of sanctioned BSSs seen by AirDefense in the network during the last five (5) days.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

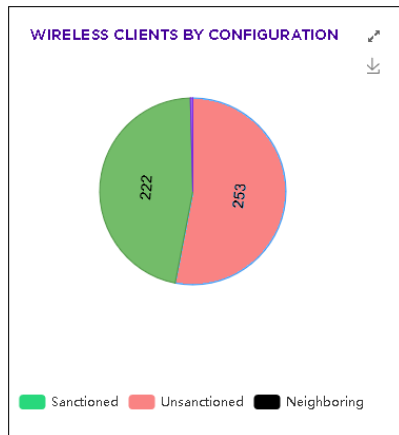
Use the  icon to expand the widget to fill the current view.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Wireless Client by Configuration


This widget displays the counts of wireless clients seen by AirDefense in the network by classification type. The wireless clients are classified as *Sanctioned*, *Unsanctioned*, and *Neighboring*



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

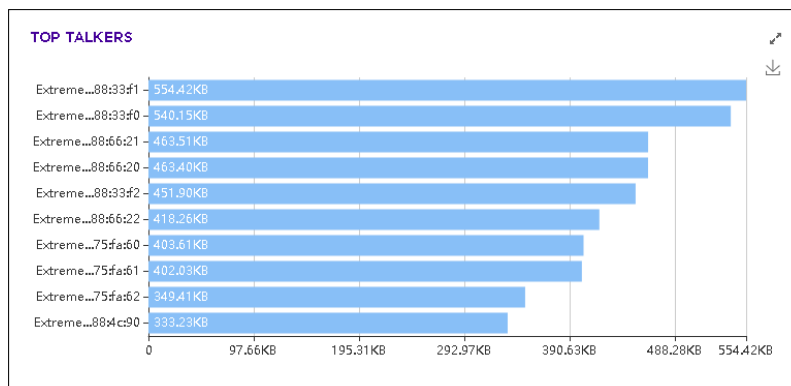
Use the  icon to expand the widget to fill the current view.


Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - Top Talkers

This widget displays a list of 10 devices that have the highest data consumption in the AirDefense monitored network. The widget also displays the exact amount of data consumed.

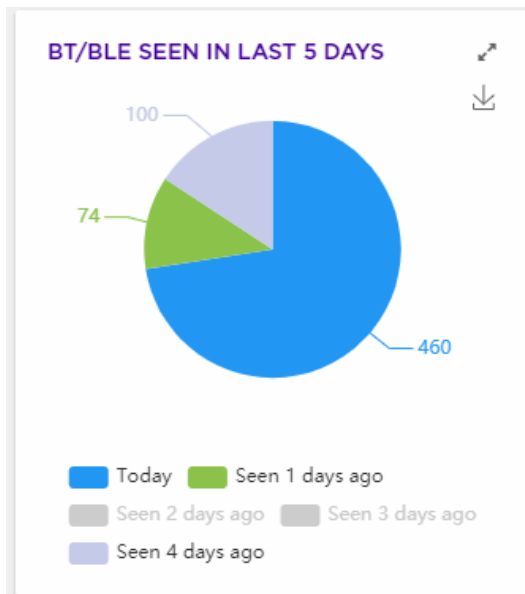



Use the  icon to expand the widget to fill the current view.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - BT/BLE Seen In Last 5 Days

This widget displays activity for Bluetooth and Bluetooth Low Energy devices that have been seen in the last five days by the Extreme AirDefense network. The colors in the piechart represent the day during which the activity had been seen. Place your cursor over a color in the pie chart to display the total number of devices with activity seen for that day, and the percentage it represents of the total number of devices seen.

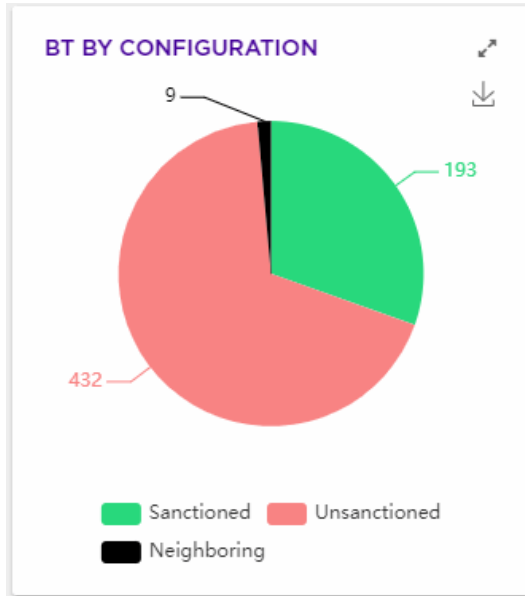


Use the  icon to expand the widget to fill the current view.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - BT By Configuration


This widget displays the counts of Bluetooth clients seen by Extreme AirDefense in the network by classification type. The Bluetooth clients are classified as *Sanctioned*, *Unsanctioned*, and *Neighboring*



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

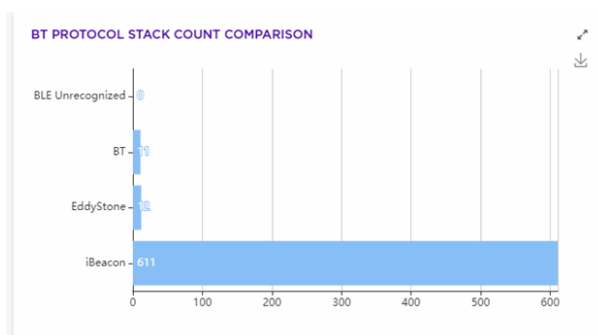
Use the  icon to expand the widget to fill the current view.


Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - BT Protocol Stack Count Comparison

This widget displays a graph that compares the protocol stack count for Bluetooth devices in the Extreme AirDefense network.



Use the  icon to expand the widget to fill the current view.

Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

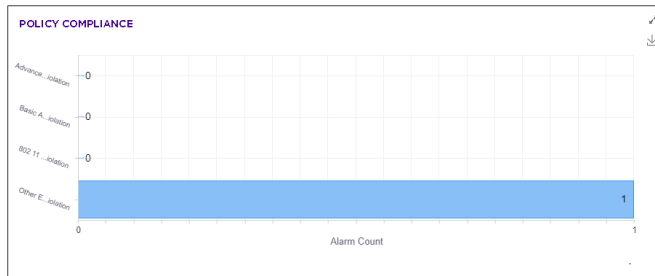
COMPLIANCE Widgets


Use the COMPLIANCE widgets to view the PCI (Payment Card Industry) Data Security Standard compliance. The following widgets are available:


- [Policy Compliance](#)
- [PCI Status](#)
- [PCI 11.1 Status](#)

Widget - Policy Compliance

This widget displays PCI policy compliance status of the AirDefense monitored network.



Use the  icon to expand the widget to fill the current view.


Use the  icon to download this widget as a image file. You can then save the downloaded image to any location on your PC.

Widget - PCI Status

This widget displays the counts of PCI Status alarms seen by AirDefense in the network.

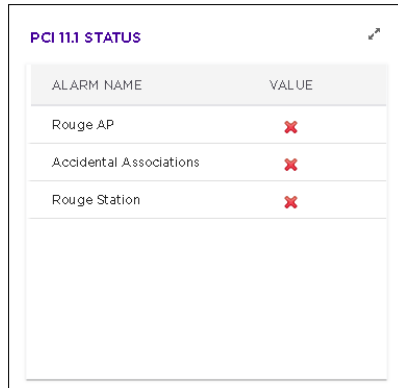
ALARM NAME	VALUE
Section 2	✘
Section 4	✘
Section 11.1	✘
Section 11.4	✔

Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

Use the  icon to expand the widget to fill the current view.


Widget - PCI 11.1 Compliance Status

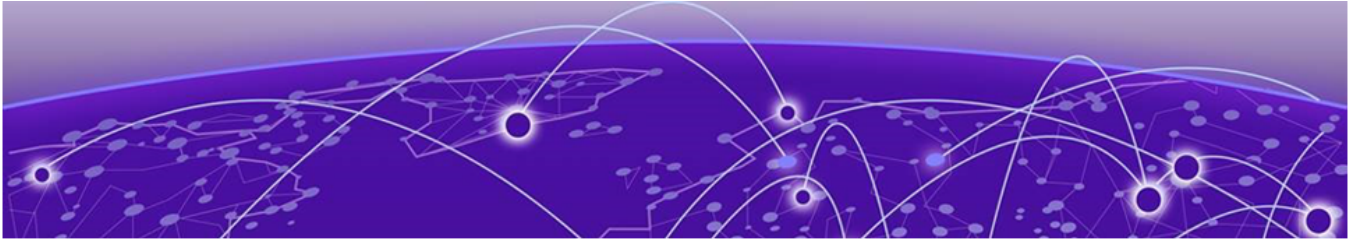
This widget displays the counts of PCI 11.1 status alarms seen by AirDefense in the network.



ALARM NAME	VALUE
Rouge AP	✘
Accidental Associations	✘
Rouge Station	✘

Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

Use the  icon to expand the widget to fill the current view.



Network View

[Network View - Network Snapshot](#) on page 53

[Network Pane - Details View](#) on page 55

The **Network View** is your main window into the Extreme AirDefense monitored network. This view provides various tools to drill down to the site/location of interest and view the state and statistics of the selected site/location in the screen's **Details** Pane.

SCOPE	DEVICE DETAILS	SEVERITY
CA 0 Alarms 0 Notifications	Sensor: 0 AP: 0 Polled	BSS: 0 WirelessClient: 0 Safe (0)
DE 0 Alarms 0 Notifications	Sensor: 0 AP: 0 Polled	BSS: 0 WirelessClient: 0 Safe (0)
Default Location 0 Alarms 0 Notifications	Sensor: 0 AP: 0 Polled	BSS: 0 WirelessClient: 0 Safe (0)
GB 0 Alarms 0 Notifications	Sensor: 0 AP: 0 Polled	BSS: 0 WirelessClient: 0 Safe (0)
NL 0 Alarms 0 Notifications	Sensor: 0 AP: 0 Polled	BSS: 0 WirelessClient: 0 Safe (0)

The **Network View** screen can be divided into:

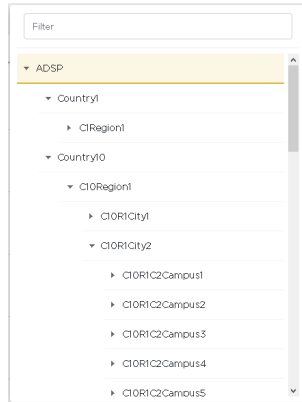
- **Network Snapshot** section - Use this section to have a quick insight into the state of your network.
- **Network Tree View** section - Use this section to select the scope of the data to view in the **Network View** screen.
- **Details** section - This section shows the data for the context (scope) selected in the **Network Tree View** section.

Network Snapshot

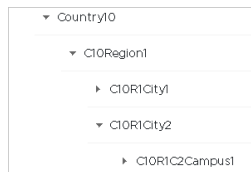
The **Network Snapshot** section of the screen provides a comprehensive insight into your network's state using widgets. For more information, see the topic [Network Snapshot](#) in this document.

Network Tree View

The **Network Tree View** section is a drop-down pane that you use to select the context or the scope of the data to display.



Use the  icon before each tree node to expand it and view its nodes. Similarly, use the  icon to collapse an expanded node.



Select the node for which you want to view the details. On selecting the node, the **Details View** pane immediately starts loading with the appropriate information. Depending on the size of the data to display, the number of devices to load and your network connection, it might take sometime for the data to be displayed.

Details View

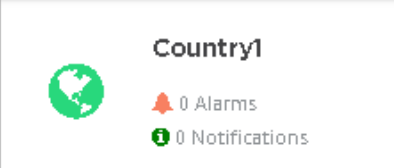






The **Details** view displays the current state of the selected site/location. This section also displays the total number of devices found at the site/location.


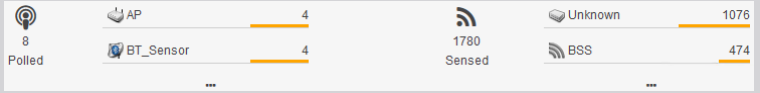

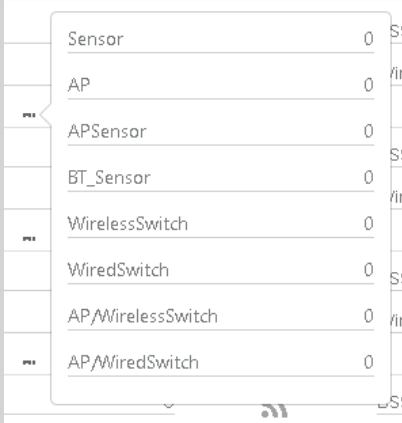




Note

Use the **Items per page** control at the bottom right of the screen to configure the number of records to display. You can also click the < and > navigation buttons located there to show more records.

The following information is displayed:

Field	Description
Scope	<p>Identifies the scope of the data being displayed (location/site/floor). The scope depends on the selection made in the My Network Tree View. Click the site/location name to view detailed statistics for it. This link is only active if there is at least 1 alarm or notification for the site/location.</p> <div data-bbox="712 516 1110 690" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p style="text-align: center;">Country1</p> <p style="text-align: center;">🚨 0 Alarms</p> <p style="text-align: center;">📢 0 Notifications</p> </div> <p>The Scope field displays the number of Alarms and Notifications generated for a site/location. The following icons indicate the severity of the site/location:</p> <ul style="list-style-type: none"> •  indicates a severity level of <i>Severe</i> which is higher than the level <i>Critical</i>. •  indicates a severity level of <i>Critical</i>. •  indicates a severity level of <i>Major</i>. •  indicates a severity level of <i>Minor</i>. •  indicates the site/location is <i>Safe</i>. •  indicates that no information is available for this site/location. <p>Select the Site Name in each row to navigate to the Device Details screen and to view details about the devices located in the selected site. If enabled, you can select the Alarms link, to launch the Alarms screen of this user interface to view the alarms raised in this site/location.</p> <p>For more information on the Device Details screen, see Network Pane - Details View on page 55.</p> <p>For more information on the Alarms screen, see Alarm View on page 100.</p>
Device Details	<p>This column displays statistics about devices identified by Extreme AirDefense in the network. Devices are broadly classified as <i>Polled Devices</i> and <i>Sensed Devices</i>. Polled Devices are those devices that are classified as <i>Network Device</i> in the main Extreme AirDefense user interface. Sensed Devices are those devices that are classified as <i>BSS, Wireless Clients, BT/ BLE, and Unknown Devices</i>.</p>

Field	Description
	<p data-bbox="711 264 1466 457">  Select the Polled icon to navigate to the Device Details screen of the user interface and to view details about the devices identified for the site. For more information on the Device Details screen, see Network Pane - Details View on page 55. </p>  <p data-bbox="711 596 1430 680"> Hover on or near the  icon to view a pop up window that displays a breakup of the various device types for the <i>Polled</i> and <i>Sensed</i> categories. </p> 
Severity	<p data-bbox="711 1167 1455 1222"> Displays a graphical representation of the site/location's health along with the current <i>Severity</i> value. </p>

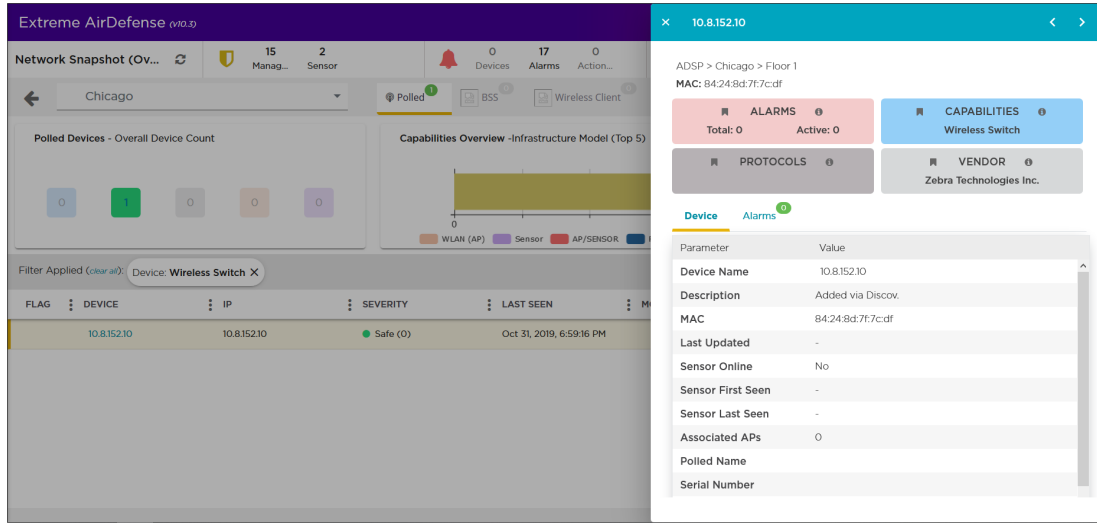
Occasionally, use the  icon to refresh the data displayed in this screen. Use the  field to change the scope of the data displayed on this screen.

Click the **Site Name** under the **Scope** column to load the **Device Details** screen. This screen displays site specific information. When you select the **Polled** icon under the **Device Details** screen, the **Device Details** screen loads to display the **Polled** tab. When you select one of the device types, the **Device Details** screen loads with the data filtered for the selected device type.

Device Details Screen

This screen displays when you select a **Site Name** in the **Details** section of the **Networks View** screen. This screen displays a list of all the devices identified as being located at the site. Use this screen to quickly analyze your overall security and performance for the selected site. This screen also enables you to drill down and

view detailed information on individual devices in your network. The following image displays a drill down view in the **Network View** window.



Network View - Network Snapshot

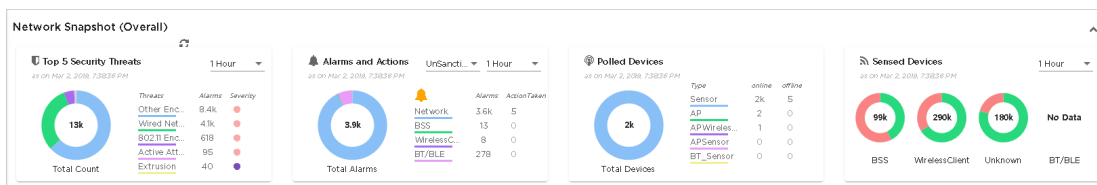
The **Network Snapshot** panel consists of four (4) widgets that provide a comprehensive insight into your network's state. These widgets are:


- [Top 5 Security Threats](#)
- [Alarms and Actions](#)
- [Polled Devices](#)
- [Sensed Devices](#)

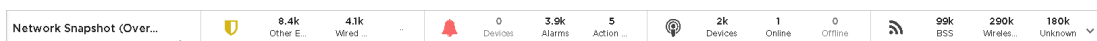


Note

This panel cannot be customized. You cannot modify the widgets in this panel.



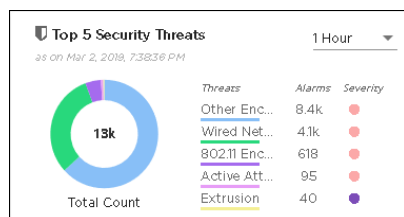
Use the  icon to collapse this panel to occupy less screen space. The same information is displayed in the collapsed panel. Use the icon in the same place to expand this panel to its full size. The expand/collapse icon is located to the top right of this panel.



Periodically use the  icon to update the data displayed in the widgets.

Top 5 Security Threats

The **Top 5 Security Threats** widget lists the top 5 security threats identified by in your network.

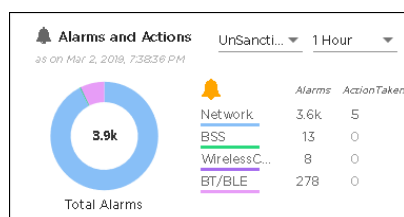


Use the drop-down list, located to the top right of this widget, to change the duration of the data that is displayed. By default, data for the last 1 Hour is displayed in the widget.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Alarms and Actions

The **Alarms and Actions** widget displays an insight into the alarms raised by all the devices in the Extreme AirDefense monitored network.



Use the drop-down list, located to the top right of this widget, to change the duration of the data that is displayed. By default, data for the last 1 Hour is displayed in the widget.

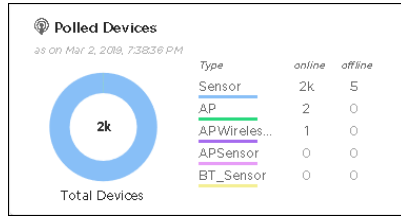
Use the **Device Type** drop-down list to select the device type of interest. Select from one of Sanctioned, Unsanctioned, and Neighboring. Unsanctioned is the default.

When a device type is selected, the data for that device type for the duration specified in the **Duration** drop-down list is displayed in the widget.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Polled Devices

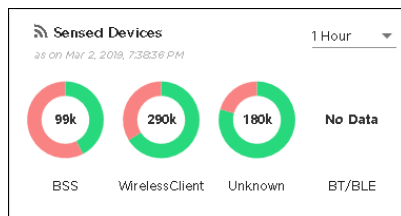
The **Polled Devices** widget displays a graph of the online/offline status of polled devices identified by Extreme AirDefense in your network. The widget displays the number of online and offline devices of major device types in your network.



Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Sensed Devices

The **Sensed Devices** widget displays the number of BSS, Wireless Clients, Unknown, and BT/BLE devices identified by Extreme AirDefense in your network.

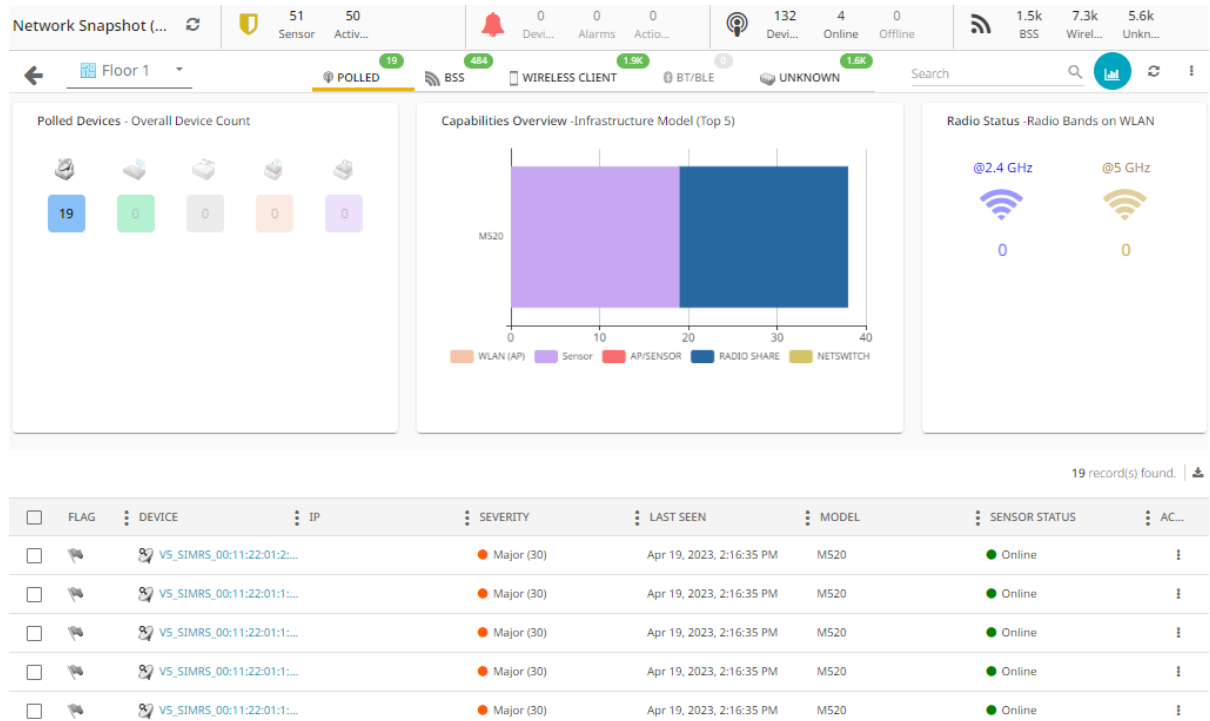


Use the drop-down list, located to the top right of this widget, to change the duration of the data that is displayed. By default, data for the last 1 Hour is displayed in the widget.

Place your cursor on any of the widget's data points to view specific information on the selected data point. Place your cursor over the pie chart to display details about each portion.

Network Pane - Details View

This screen displays in depth statistics and other details for the selected site or location. It also displays the current status of the network in the **Network Snapshot (Overall)** pane.



This screen can be divided into these sections:

- Network Snapshot (Overall) - This section provides a snapshot of the current state of your network. Use the icon to refresh the displayed data. For more information on this pane, see [Network View - Network Snapshot](#) on page 53.
- Network Scope and Tool Bar - This section provides controls that you can use to filter data displayed in this screen.
- Widgets - This section displays three (3) widgets that provide an overview about the devices in the network.
- Device Details - This section displays comprehensive data about the devices identified by Extreme AirDefense in the selected site/location. For more information, see [Network Pane - Device Details](#) on page 56.

Network Pane - Device Details


The **Device Details** pane displays comprehensive details about the devices found in the AirDefense monitored network. The data is further classified according to the identified device types. Details about each device type can be found under their own tabs.

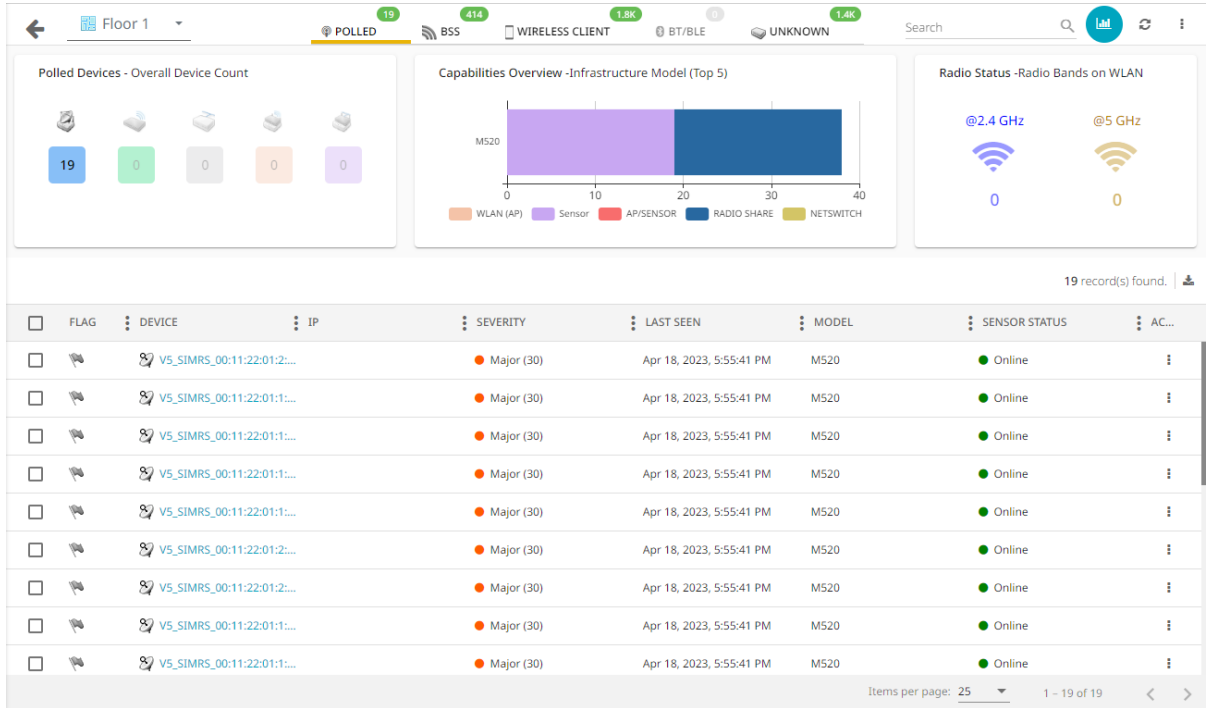
To filter the list, do either of the following:

- From the Device Details list columns, click one of the icons, select **Filter**, and choose your filter.
- Click on a graph category from the Network Snapshot area.

To apply an action to multiple devices, check the check box(es) adjacent to the relevant devices and select an action from the toolbar's Actions menu icon . You can use this

menu to select and apply a single action to one or more devices in the list. For details, see [Device Details - Toolbar](#) on page 58.

To apply an action to a single device only, you can use the toolbar Actions menu (see above) or you can use the Actions icon  that appears in the Device Details line entry for that device. For details, see the different Device Actions tables for each device type under [Device Type Details](#) on page 61.



The screenshot displays the 'Floor 1' network management interface. At the top, there are status indicators for 'POLLED' (19), 'BSS' (414), 'WIRELESS CLIENT' (1.8K), 'BT/BLE' (1), and 'UNKNOWN' (1.4K). Below these are three summary cards: 'Polled Devices - Overall Device Count' showing counts for various device types, 'Capabilities Overview -Infrastructure Model (Top 5)' with a bar chart for M520, and 'Radio Status -Radio Bands on WLAN' showing 0 devices on both 2.4 GHz and 5 GHz bands. The main area contains a table with 19 records found.

FLAG	DEVICE	IP	SEVERITY	LAST SEEN	MODEL	SENSOR STATUS	AC...
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:2:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:1:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:1:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:1:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:1:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:2:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:1:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:2:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:1:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	
<input type="checkbox"/>	V5_SIMRS_00:11:22:01:1:...		Major (30)	Apr 18, 2023, 5:55:41 PM	M520	Online	

Items per page: 25 | 1 - 19 of 19



Note

Use the **Items per page** control at the bottom right of the screen to configure the number of records to display. You can also click the < and > navigation buttons located there to show more records.

The **Device Details** pane can be divided into these panes:

Pane	Description
Toolbar	<p>The Toolbar contains a number of tools that enable you to perform several tasks on the data being displayed in the pane.</p> <p>The Toolbar displays a drop-down list that displays the hierarchy of the AirDefense system. Use this list to select the scope of the data to be displayed in this screen.</p> <p>Some of the other features are <i>Device Type</i> tabs that you can use to view specific device types, a search box that you can use to search for specific devices, and a toggle button to show or hide the charts displayed below this toolbar.</p> <p>For more information, see Device Details - Toolbar on page 58.</p>
Grid Chart View	<p>The Grid Chart View is a panel that displays the statistics for the selected device type. This data is displayed in widgets. The content of this panel is different for the different device types identified by AirDefense. For more information, see the topic Device Type Details on page 61.</p>
Device List	<p>The Device List is a table that displays a list of individual devices classified by device types. The content of this table is different for the different device type identified by AirDefense.</p> <p>For more information, see Device Type Details on page 61.</p>

Device Details - Toolbar

The **Toolbar** of the **Device Details** pane contains a set of tools that you can use to manage the devices in your network.

Table 4: Device Details Toolbar Actions









Tool	Description
	Use this icon to go back to the previous screen.
	Use this box to select the scope of the data to display in this pane. Select this pane to display a drop-down list and select the appropriate scope from this list. This drop-down list displays the AirDefense site hierarchy.
	Select each tab in this toolbar to view details about devices of the selected device type. For more information, see Device Type Details on page 61.
	Use the Search control to search for a specific device in the Device List . Hover on the field to view a list of fields that you can search on.

Table 4: Device Details Toolbar Actions (continued)

Tool	Description
	Select this icon to view or hide the Grid Chart view in this pane.
	Select this icon periodically to refresh the data displayed on this screen.
	Displays actions that you can select and apply to selected devices in the Device Details view. You can use this icon to apply a bulk action to multiple devices. For details, see the following table Device Actions - Toolbar .

Device Actions - Toolbar

Use the toolbar's Device Actions menu icon  to select and apply actions to selected devices. In the Device Details list, check the relevant devices and then use this menu to select and apply an action to the checked devices. There are also a pair of actions that you can apply to all devices in the list, and which are available only when no devices are checked. See the following table for details.

The available actions differ depending on device types and the number of checked devices. When selecting multiple devices, all selected devices must be the same device type.

**Note**


There is also a device-specific actions icon  that appears at the end of each line entry in the Device Details list (rather than in the toolbar). Use this icon to select an action for that device only. For details, see the Device Actions tables that appear for each device type under [Device Type Details](#) on page 61.

Table 5: Device Actions - Toolbar

Action	Description
Set flag	Flags the selected device(s) to indicate that attention is required.
Clear flag	Clears the flag from the selected device(s).
Classification	Use this command to classify the device into one of the following categories: <ul style="list-style-type: none"> Sanctioned (Inherit profiles) Unsanctioned Neighboring Sanctioned (Assigned profiles)

Table 5: Device Actions - Toolbar (continued)

Action	Description
Client Type	Use this command to set the client type to one of the following: <ul style="list-style-type: none"> • Employee Personal Device • Guest Wi-Fi User • In Store Customer • Laptop • Loyalty Customer • Phone • Potential Customer • Scanner • Tablet • Uncategorized Device
Audit Devices	Conducts a compliance audit on the selected device(s).
Retrieve Diagnostic Logs	Retrieves the diagnostic logs for the selected device(s).
Remove Devices	Removes selected device(s) from monitoring.
Move Devices	Place the selected device(s) on a floor.
Upgrade Devices	Upgrade the firmware for the selected device(s).
Import CLI Variables	Imports CLI Variables at the device level for the selected device(s).
Command Run and Log	Executes CLI commands for selected device(s). The results are saved in a log file.
Search Device Configuration	Allows you to search for device configurations on the selected device(s).

Table 5: Device Actions - Toolbar (continued)

Action	Description
Remove all the (filtered) Devices	<p>Use this menu item to remove all devices that are currently listed in the Device Details list from monitoring. Note the following conditions:</p> <ul style="list-style-type: none"> • This command is available only if no devices are checked in the Device Details list. If any devices are checked, the command is greyed out. • If the number of devices listed exceeds what the page displays, this action includes devices that the current query returned, but which appear off the page (see the Items per page controls to increase the number of displayed records). • The action label contains "filtered" only if you applied a filter to the list. In this case, only devices that meet the filter criteria are affected.
Classify all the (filtered) Devices	<p>Use this menu item to classify all of the listed devices into one of the following categories:</p> <ul style="list-style-type: none"> • Sanctioned (Inherit profiles) • Unsanctioned • Neighboring • Sanctioned (Assigned profiles) <p>Note the following conditions:</p> <ul style="list-style-type: none"> • This command is available only if no devices are checked in the Device Details list. If any devices are checked, the command is greyed out. • If the number of devices listed exceeds what the page displays, this action includes devices that the current query returned, but which appear off the page (see the Items per page controls to increase the number of displayed records). • The action label contains "filtered" only if you applied a filter to the list. In this case, only devices that meet the filter criteria are affected.

Device Type Details

AirDefense classifies devices into the following devices types:

- Polled
- BSS
- Wireless Clients
- Unknown
- BT/BLE

Polled Devices

Polled devices are those devices that AirDefense classifies as *Network Devices*.

Network Devices are those devices that are a part of your network and have been

assigned an IP address in your network. *Network Devices* include, switches, wireless controllers, routers, access points, and sensors. AirDefense communicates with these devices to push or pull data and configuration.

For more information on the **Polled** tab, see [Polled Devices Tab](#) on page 62.

BSS

The **BSS** screen lists all the BSSs, sanctioned or otherwise, identified by AirDefense.

For more information on the **BSS** tab, see [BSS Tab](#) on page 71.

Wireless Clients

The **Wireless Clients** tab displays a list of all wireless clients, sanctioned or otherwise, identified by AirDefense in your network.

For more information on the **Wireless Clients** tab, see [Wireless Clients](#) on page 79.

Unknown Devices

AirDefense classifies devices as **Unknown** based on the MAC address of the source or final destination of packets seen in the network. Any device with an unidentified MAC address is marked as an *Unknown Device*.

For more information on the **Unknown** tab, see [Unknown Devices](#) on page 87.

BT/BLE

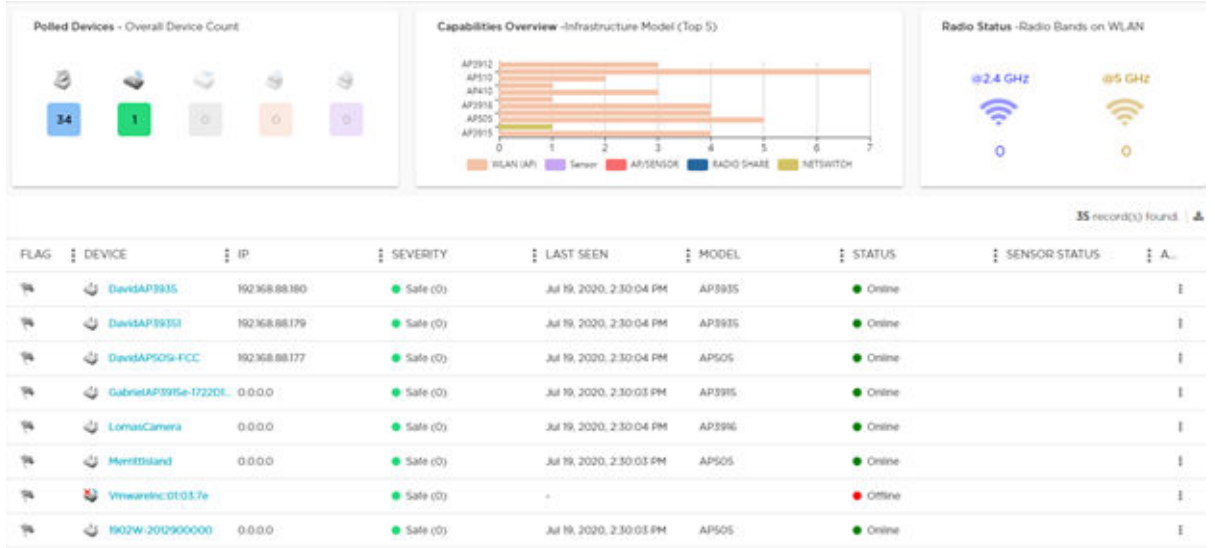
The **BT/BLE** tab displays a list of Bluetooth/Bluetooth Low Energy (BLE) devices, sanctioned or otherwise, identified by AirDefense in your network.

For more information on the **BT/BLE** tab, see [Bluetooth and Bluetooth Low Energy Devices](#) on page 94.

Polled Devices Tab

Polled devices are those devices that AirDefense classifies as *Network Devices*.

Network Devices are devices that are a part of your network and have been assigned an IP address in your network. *Network Devices* include, switches, wireless controllers, routers, access points, and sensors. These are the devices that AirDefense communicates with to push or pull data and configuration.






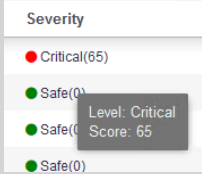
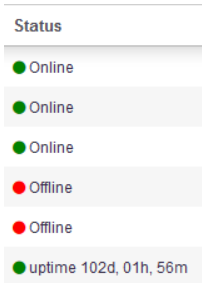



The **Polled Device** tab displays a set of widgets on the top of the display area. The widgets are:

- [Polled Devices](#)—Overall Device Count
- [Overview](#)—Infrastructure Model Overview
- [Radio Status](#)—Radio Bands on WLAN


The **Devices** table displays the following information for each Polled device:

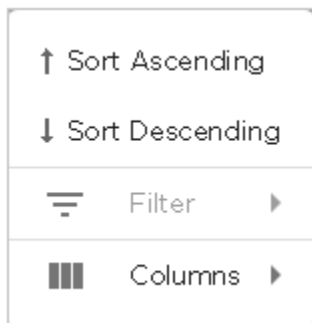
Field	Description
Flag	Select the icon to indicate that this device is considered to be of interest. The flag changes to .
Device	This column displays the device type icon and its name. Hover on the name to display more details about the device in a pop-up. The following image is a pop up that displays on hover. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Applied: Device</p> <p>MAC Address: d8:84:66:79:9c:a9 Appliance: 192.168.20.201 Manufacturer: Extreme Networks, Inc. Name: 1701Y-1208500000-sens Polled Name: 1701Y-1208500000-sens IP Address: 192.168.20.93 Model: AP3912FCCi Last Seen: 24-Jul-2018 2:57 pm Capabilities: Sensor, AP Firmware: 10.41.08.0012 Sensor Firmware: 10.41.08.0012</p> <p>Licenses: WIPS Spectrum Analysis Live RF Advanced Forensics AP Test Connection Troubleshooting WLAN Management Tracker Integration Vulnerability Assessment Advanced Infrastructure Forensics Proximity and Analytics</p> </div>

Field	Description
IP	This column displays the IP address assigned to this device.
Severity	<p>This column displays the device's threat level to your network. Hover on this value to display a threat score for this device.</p> <ul style="list-style-type: none">  Severe indicates a severity level of <i>Severe</i> which is higher than the level <i>Critical</i>.  Critical indicates a severity level of <i>Critical</i>.  Major indicates a severity level of <i>Major</i>.  Minor indicates a severity level of <i>Minor</i>.  Safe indicates the site/location is <i>Safe</i>. 
Last Seen	This column displays the date and time this device was last seen on the network.
Model	This column displays the device's model number as provided by the device. If the device does not provide its model number, the value <i>unknown</i> is displayed. Model numbers for offline devices are not displayed.
Status	<p>This column indicates the online/offline status of the device. If the device reports up-time, then this up-time value is displayed.</p> 

Field	Description
Sensor Status	This column indicates the online/offline status of a sensor device. If an access point is also a sensor, the status of the access point's sensor is indicated in this column.
	<p>Select this icon to display a context sensitive menu of actions that can be performed for this particular device. The following image displays the actions that are available for an access point.</p> <div data-bbox="712 506 1110 1199" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <ul style="list-style-type: none"> Alarms Properties Upgrade Rename Move Remove Readiness Test Device Polling ▶ <hr/> <ul style="list-style-type: none"> Action Details Port Lookup (Find this device) Forensic Analysis <hr/> <ul style="list-style-type: none"> Direct Connect <hr/> <ul style="list-style-type: none"> Copy MAC ▶ </div>

By default, only few a subset of columns are displayed in the table. Depending on the context, additional fields can be manually added to the table.

To manipulate the data display, select the  icon to the left of any column header. For example, you can sort the data, add or remove table columns, and apply a filter (when available). The following drop-down list displays.



Select the **Columns** item to view a list of columns that can be added to the table.

The following table lists the additional columns that can be added to the table.

Field	Description
Name	This column displays the name of the device if configured.
Polled Name	This column displays then polled name of the device if available.
MAC	This column displays the MAC address of the device.
First Seen	This column displays the date and time this device was first seen on the network.
Scope	This column displays the name of the site/location where this device is located as identified by Extreme AirDefense.
Floor	This column displays the floor number (in the site/location) where this device is located as identified Extreme AirDefense.
Manufacturer	This column displays the name of the manufacturer of the device.
Firmware	This column displays the details of the firmware installed on the device.
Compliant	This column indicates if the device is compliant with AirDefense's policies.
Device Actions	This column indicates if any of the following actions have taken place: <ul style="list-style-type: none"> • AP Test • Wireless Vulnerability Assessment • Termination • Dedicated Spectrum Analysis • Inline Spectrum Analysis
Associated Clients	This column displays the number of clients that are associated with the device.
Adopted APs	This column displays the number of access points that the device has adopted to.

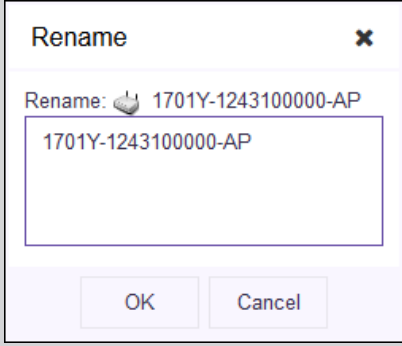
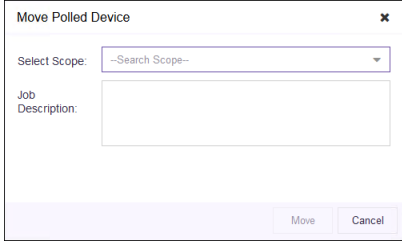
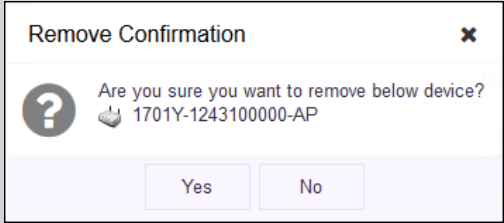
Device Actions

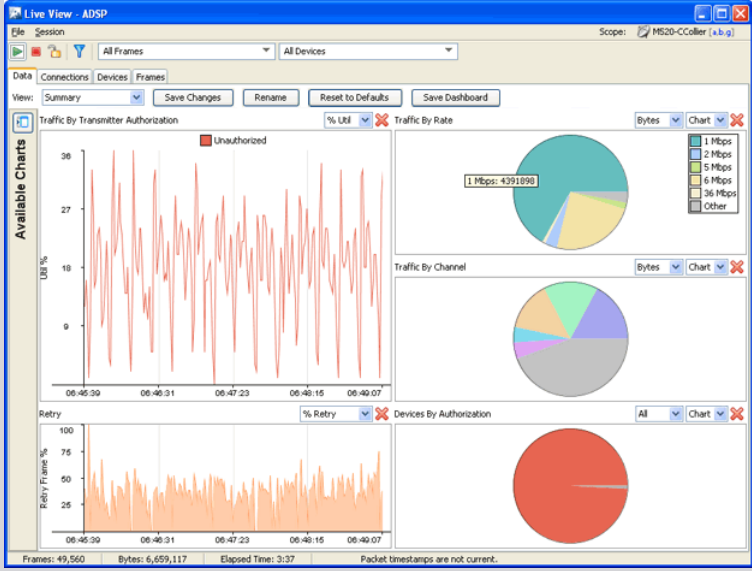
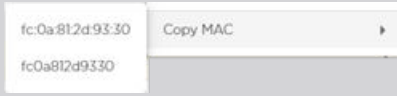
The following actions can be performed on a each device listed in the table. Select the



icon to display the list of actions that can be performed. The actions that can be performed are different for the different device types.

Action	Description
Alarms	Displays the Alarms for the device. When selected, the alarms for this device are displayed in the Alarms screen
Properties	Displays the properties of the device. Select this item to view the properties of the selected device.

Action	Description
Upgrade	Select this menu item to upgrade the selected device to the latest available firmware.
Rename	<p>Select this menu item to rename this device. Use this menu item to configure a meaningful name for this device. A small window displays. Use this Rename window to provide a name for this device.</p> 
Move	<p>Select this menu item to move this device to a different site/location in the Extreme AirDefense system. A small window displays. Use this window to provide the destination to move the device to.</p> 
Remove	<p>Select this menu item to remove the device. A small confirmation window displays. Select Yes to remove the device. Select No to exit without removing the device.</p> 
Readiness Test	Select the Readiness Test menu item to check the connections and the communication settings between Extreme AirDefense and the device. A series of test are run and the results are displayed in another window.
Device Polling	Select the Device Polling menu item to run a compliance audit on the device.
Action Details	Select the Action Details menu item to view a table listing specific actions occurring on the device.

Action	Description
Port Lookup (Find this Device)	Use the Port Lookup menu item to scan for and locate this device, in your network, using its MAC address.
Forensic Analysis	Use the Forensic Analysis menu item to analyze the device and provide detailed information on the device. Forensic Analysis returns the threat level of the device, device alarms, and device association details about the device.
Live View	<p>The Live View menu item displays the Live View window for the device where you can view the device's live status and other parameters.</p>  <p>The screenshot shows the 'Live View - ADSP' interface. It features a top navigation bar with 'File', 'Session', and 'Scope: MS20-Coller (s.b.g)'. Below this is a 'Data' section with tabs for 'Connections', 'Devices', and 'Frames'. The main area contains several charts: 'Traffic By Transmitter Authorization' (line chart showing 'Unauthorized' traffic), 'Traffic By Rate' (pie chart with a legend for 1 Mbps, 2 Mbps, 5 Mbps, 6 Mbps, 36 Mbps, and Other), 'Traffic By Channel' (pie chart), and 'Retry' (line chart showing '% Retry'). A status bar at the bottom displays 'Frames: 49,560', 'Bytes: 6,659,117', 'Elapsed Time: 3:37', and 'Packet timestamps are not current.'</p>
Direct Connect	Select the Direct Connect menu item to directly connect to the device. A new browser window or a browser tab is created for the login screen of the device.
Copy MAC	<p>The Copy MAC menu item is an ease of use feature and enables you to copy the MAC address of the device in hexadecimal or colon hexadecimal notation. Click this menu item to expand it and view MAC formats that can be copied.</p>  <p>The screenshot shows a 'Copy MAC' dropdown menu with two options: 'fc:0a:81:2d:93:30' and 'fc0a812d9330'.</p> <p>Select the MAC format to copy to your PC's clipboard.</p>

Polled Devices - Widgets

The **Polled Device** tab displays a set of widgets on the top of the display area. The widgets are:

- [Polled Devices](#)- Overall Device Count
- [Overview](#) - Infrastructure Model Overview

- [Radio Status](#) - Radio Bands on WLAN

Widget - Polled Device Tab - Polled Device

This widget displays the number of devices of each device category.

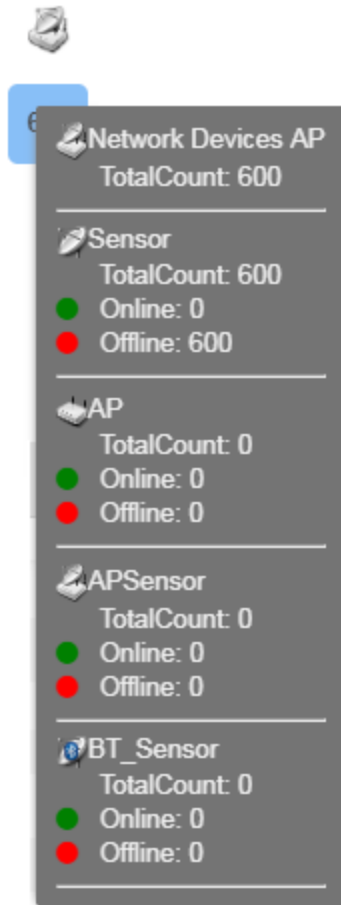
Polled Devices - Overall Device Count



The displayed device categories are:

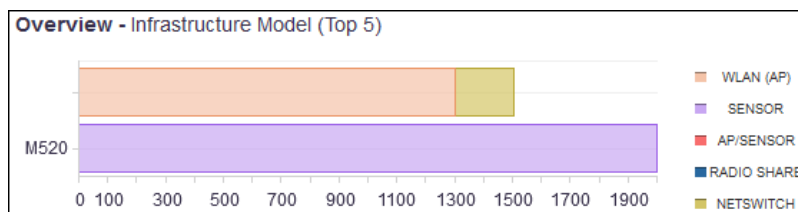
- Network Devices APs - This item includes the totals of the following device categories:
 - Sensors
 - Access Points
 - Access Points that are also sensors
 - Bluetooth Sensors
- Wireless Switches
- Wired Switches
- Wireless Access Point Switches
- Wired Access Point Switches

Hover on each of the device types to display a popup with further details of the number of devices in that device category. This popup is not displayed for those device categories that have no devices (the number of devices in that category is zero(0)).



Widget - Polled Device Tab - Infrastructure Overview

This widget displays a horizontal bar chart which displays the top 5 infrastructure devices in your AirDefense monitored network.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

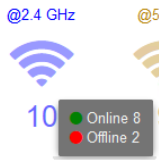
Widget - Polled Devices Tab - Radio Status

The **Radio Status** widget displays the number of radios for each radio band that have at least one WLAN configured.

Radio Status - Radio Bands on WLAN

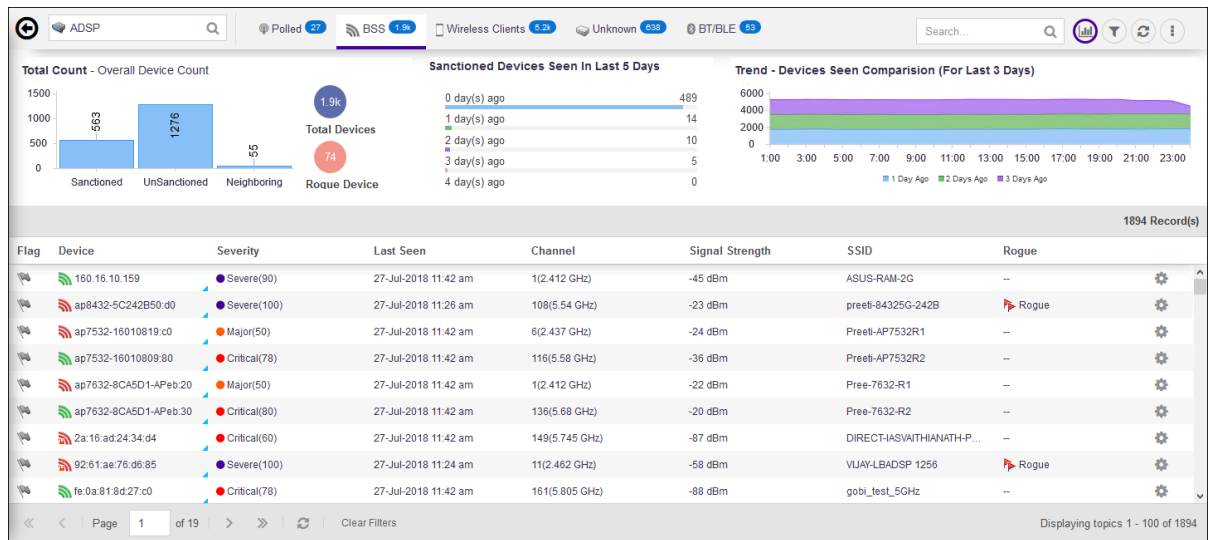


Hover on each of these radio bands to view a pop-up that displays the number of radios that are offline and online.



BSS Tab













The **BSS** tab displays a list of all *Basic Service Sets* (BSSs), sanctioned or otherwise, that were discovered by Extreme AirDefense in your network during regular scans. The tab also includes BSSs that are known about due to other methods like a controller (for example, ExtremeCloud IQ, ExtremeWireless WiNG, ExtremeCloud IQ Controller) or a CSV import.



The **BSS** tab displays a set of widgets on the top of the display area. The widgets are:

- Total Count - Overall Device Count
- Sanctioned Devices Seen in Last 5 Days
- Trend - Device Seen Comparison (For Last 3 Days)

The **BSS** table displays the following information:


Field	Description
Flag	Select the  icon to indicate that this device is considered to be of interest. The flag changes to  .
Device	<p>This column displays the device type icon and its name. Hover on the name to display more details about the device in a pop-up. The following image is a pop up that displays on hover.</p> <div data-bbox="716 569 1105 789" style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;"> <p>MAC Address: 74:67:f7:08:8a:20 Appliance: 192.168.20.201 Manufacturer: Extreme Networks, Inc. Channel: 7 SSID: Preeti-8533-R1RS Last Seen: 14-Aug-2018 6:12 pm Signal Strength: -47</p> </div> <p>Select the MAC address of the device to view its details in a separate window.</p>
Severity	<p>This column displays the device's threat level to your network. Hover on this value to display a threat score for this device.</p> <ul style="list-style-type: none"> •  Severe indicates a severity level of <i>Severe</i> which is higher than the level <i>Critical</i>. •  Critical indicates a severity level of <i>Critical</i>. •  Major indicates a severity level of <i>Major</i>. •  Minor indicates a severity level of <i>Minor</i>. •  Safe indicates the site/location is <i>Safe</i>. <div data-bbox="716 1276 914 1455" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Severity</p> <ul style="list-style-type: none">  Critical(65)  Safe(0)  Safe(0) Level: Critical Score: 65  Safe(0) </div>
Last Seen	This column displays the date and time this device was last seen actively transmitting.
Channel	This column displays the channel identified based on the last sensed transmission.
Signal Strength	This column displays the signal strength for this device.
SSID	This column displays the SSID of the network that the BSS used.
Rogue	This column indicates if a device has been flagged as a <i>Rogue</i> device. All rogue devices are flagged with this  icon.

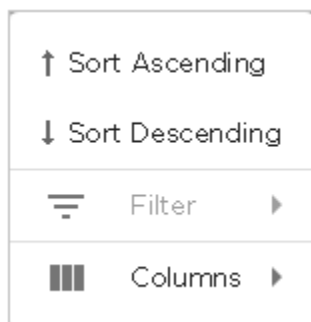
Select a device in the table to display a right-panel details window that includes the following columns:

Table 6:

Parameter	Value
Device Name	Displays the name of the device.
Description	Displays a description of the device.
Annotations	
MAC	Displays the MAC Address for the device.
Random MAC	Indicates whether the device is using Random MAC (yes) or not (no).
Observed	
First Seen	Displays date device was first seen transmitting.
Last Seen	Displays date device was last seen transmitting.
Supported b/g Channels	
Available Rates	
Associated AP	
Capabilities	
Noise	
Channel	
Associated Wireless Clients	
Polled First Seen	
Polled Last Seen	
Sensed Authentication	
Sensed Encryption	
Reported SSID(s)	Displays the SSID for the device.
Reported IP	Displays the device's IP Address
Primary Sensor	Displays the name of the primary sensor.
Signal Strength	Displays the signal strength of the device.
Protocols	
Terminating	Indicates whether the device is terminating (yes) or not (no).
Vendor	Displays name of the device's vendor.

By default, only few a subset of columns are displayed in the table. Depending on the context, additional fields can be manually added to the table.


To manipulate the data display, select the  icon to the left of any column header. For example, you can sort the data, add or remove table columns, and apply a filter (when available). The following drop-down list displays.



Select the **Filter** control (if available) to filter the data in the column based on the available filtering criteria. You can also apply a filter by clicking on graph categories within the widgets.


Select the **Columns** item to view a list of columns that can be added to the table.

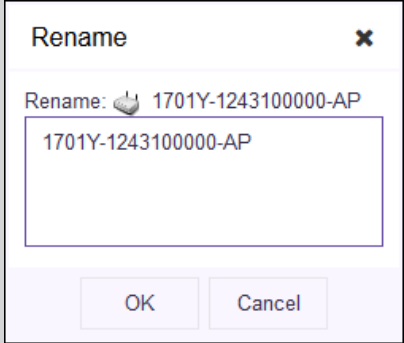
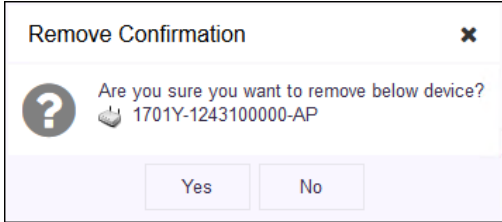
The following table lists the additional columns that can be added to the table.

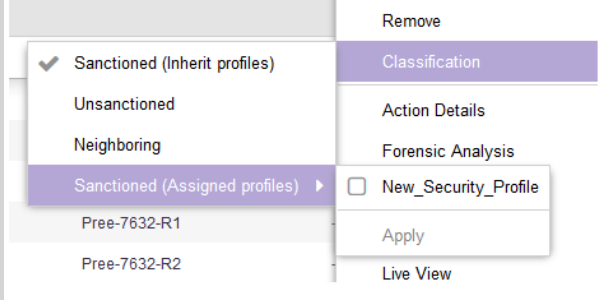
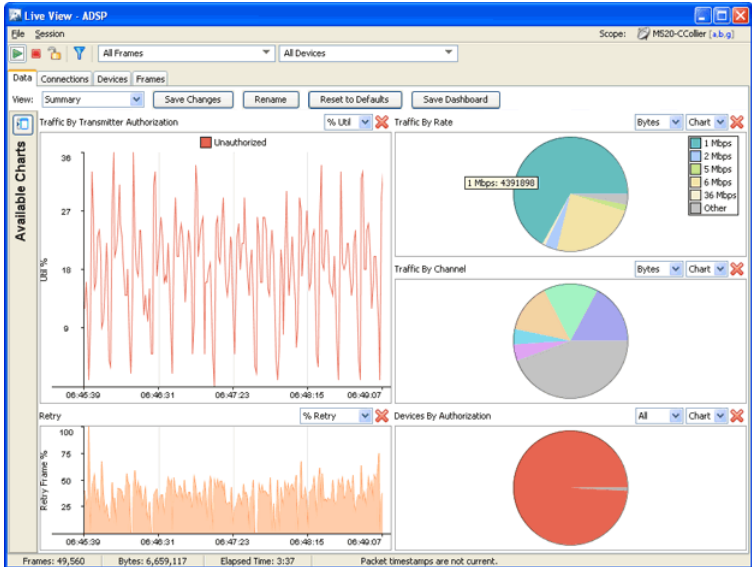
Field	Description
Name	This column displays the name of the device if configured.
IP	This column displays the IP address assigned to this device.
MAC	This column displays the MAC address of the device.
First Seen	This column displays the date and time this device was first seen on the network.
Scope	This column displays the name of the site/location where this device is located as identified by Extreme AirDefense.
Floor	This column displays the floor number (in the site/location) where this device is located as identified Extreme AirDefense.
Manufacturer	This column displays the name of the manufacturer of the device.
Classification	This column displays the device's classification as classified by Extreme AirDefense. A device can be classified as <i>Sanctioned (Inherit Profile)</i> , <i>Unsanctioned</i> , <i>Neighboring</i> , or <i>Sanctioned (Assigned Profile)</i> . You can manually set a device's classification from the  > Classification menu item from within the table.

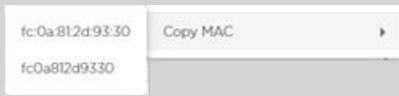
Field	Description
Sensed Authentication	This column displays the authentication scheme the device uses to authenticate.
Sensed Encryption	This column displays the encryption scheme used by the device if any.
Protocols	This column displays the various wireless protocols supported by the device.
Device Actions	This column indicates if any of the following actions have taken place: <ul style="list-style-type: none">• AP Test• Wireless Vulnerability Assessment• Termination• Dedicated Spectrum Analysis• Inline Spectrum Analysis
Associated Clients	This column displays the number of clients that are associated with the device.
Access Points	This column displays the name of the access point on which the BSS is operating.
Sensor	This column displays the name of the sensor that sees this device.
Security Policy	This column displays the security policy, if any, applied to this device.

Device Actions

The following actions can be performed on a each device listed in the table. Select the  icon to display the list of actions that can be performed. The actions that can be performed are different for the different device types.

Action	Description
Alarms	Displays the Alarms for the device. When selected, the alarms for this device are displayed in the Alarms screen
Rename	<p>Select this menu item to rename this device. Use this menu item to configure a meaningful name for this device. A small window displays. Use this Rename window to provide a name for this device.</p> 
Remove	<p>Select this menu item to remove the device. A small confirmation window displays. Select Yes to remove the device. Select No to exit without removing the device.</p> 

Action	Description
<p>Classification</p>	<p>Use this menu item to classify the device into one of <i>Sanctioned (Inherit profiles)</i>, <i>Unsanctioned</i>, <i>Neighboring</i>, and <i>Sanctioned (Assigned Profiles)</i>.</p>  <p>The <i>Sanctioned (Assigned Profiles)</i> menu item expands to show a list of available profiles that can be assigned to this device.</p>
<p>Action Details</p>	<p>Select the Action Details menu item to view a table listing specific actions occurring on the device.</p>
<p>Forensic Analysis</p>	<p>Use the Forensic Analysis menu item to analyze the device and provide detailed information on the device. Forensic Analysis brings up a new window with very detailed historical information about the device.</p>
<p>Generate Tracker File</p>	<p>Allows you to generate tracker files and save the files to a directory on your computer.</p>
<p>Locate</p>	<p>Use the Locate menu item to locate this device on your network. This opens the Location Tracking window from where you can track the device.</p>
<p>Live View</p>	<p>The Live View menu item displays the Live View window for the device where you can view the device's live status and perform remote packet captures.</p> 

Action	Description
Port Lookup (Find this Device)	Use the Port Lookup menu item to scan for and locate this device, in your network, using its MAC address.
Terminate	Use the Terminate menu item to open the Termination options window from where you can terminate this device.
AP Test	Use the AP Test action to begin an on-demand version of AP Test against the selected BSS.
Wireless Vulnerability Assessment	Use the Wireless Vulnerability Assessment window to begin an on-demand version of WVA against the selected BSS to scan your network for vulnerabilities.
Copy MAC	<p>The Copy MAC menu item is an ease of use feature and enables you to copy the MAC address of the device in hexadecimal or colon hexadecimal notation. Click this menu item to expand it and view MAC formats that can be copied.</p>  <p>Select the MAC format to copy to your PC's clipboard.</p>

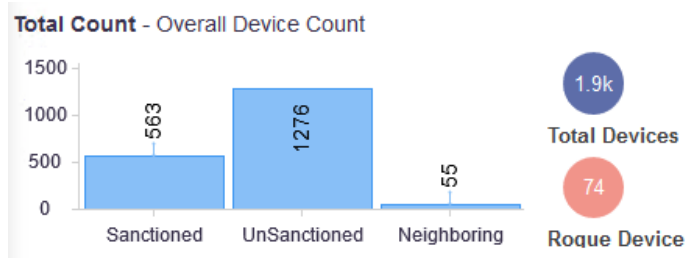
BSS Tab - Widgets

The **BSS** tab displays a set of widgets on the top of the display area. The widgets are:

- [Device Classification](#)
- [Sanctioned Devices Seen in Last 5 Days](#)
- [Trend - Device Seen Comparison \(For Last 3 Days\)](#)

Widget - BSS Tab - Device Classification

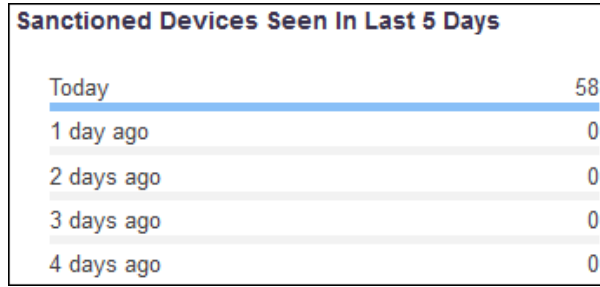
This widget displays the total number of devices, identified and classified by AirDefense. This widget shows the total count of the devices and rogues in the network. It also displays a graph of the total device segregated as *Sanctioned*, *Unsanctioned*, and *Neighboring*.



Hover on each of these device types to view more details.

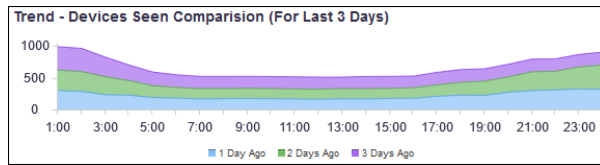
Widget - BSS Tab - Sanctioned Devices Seen in Last 5 Days

This widget displays the total number of sanctioned devices seen in the last 5 days.



Widget - BSS Tab - Trend-Device Seen Comparison (For last 3 days)

This widget displays the trend of the total number of devices seen in the network in the last three (3) days.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

Wireless Clients

The **Wireless Client** tab displays a list of wireless clients, sanctioned or otherwise, that were discovered by Extreme AirDefense in your network during regular scans.



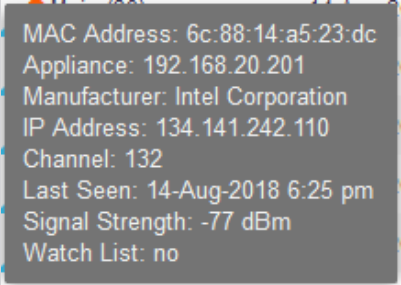





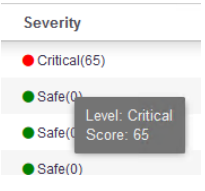
The screenshot shows the 'Wireless Clients' dashboard with the following components:


- Device Classification:** A bar chart showing 253 Sanctioned, 316 UnSanctioned, and 2 Neighboring devices.
- Total Devices:** 571 (Total), 72 (Rogue).
- Sanctioned Devices Seen in Last 5 Days:** A table showing counts for Today (58), 1 day ago (0), 2 days ago (0), 3 days ago (0), and 4 days ago (0).
- Trend - Devices Seen Comparison (For Last 3 Days):** An area chart showing device counts over a 24-hour period.
- Table of Records:** A table with 571 records, showing columns for Flag, Device, Severity, Last Seen, Channel, Signal Strength, SSID, Client Type, Rogue, and Associated BSS.

The **Wireless Clients** tab displays a set of widgets on top of the display area. These widgets are:

- [Device Classification](#)
- [Sanctioned Devices Seen in Last 5 Days](#)
- [Trend—Device Seen Comparison \(For Last 3 Days\)](#)

The **Wireless Clients** table displays the following information:

Field	Description
Flag	Select the  icon to indicate that this device is considered to be of interest. The flag changes to  .
Device	<p>This column displays the device type icon and its name. Hover on the name to display more details about the device in a pop-up. The following image is a pop up that displays on hover.</p>  <p>Select the MAC address of the device to view its details in a separate window.</p>
Severity	<p>This column displays the device's threat level to your network. Hover on this value to display a threat score for this device.</p> <ul style="list-style-type: none"> •  Severe indicates a severity level of <i>Severe</i> which is higher than the level <i>Critical</i>. •  Critical indicates a severity level of <i>Critical</i>. •  Major indicates a severity level of <i>Major</i>. •  Minor indicates a severity level of <i>Minor</i>. •  Safe indicates the site/location is <i>Safe</i>. 
Last Seen	This column displays the date and time this device was last seen actively transmitting.
Channel	This column displays the channel and the frequency on which this device was identified.
Signal Strength	This column displays the signal strength for this device.
SSID	This column displays the SSID of the network to which this device is adopted to.

Field	Description
Client Type	This column displays the device's client type as classified by Extreme AirDefense. Client Type can be one of the following types: <ul style="list-style-type: none"> • Categorized Device • Scanner • Employee Personal Device • Guest WiFi User • Laptop • Phone • Tablet • Loyalty Customer • In Store Customer • Potential Customer
Rogue	This column indicates if a device has been flagged as a <i>Rogue</i> device. All rogue devices are flagged with this  Rogue icon.
Associated BSS	This column displays the BSS this wireless client is associated with.

Select a device in the table to display a right-panel details window that includes the following columns:


Table 7:

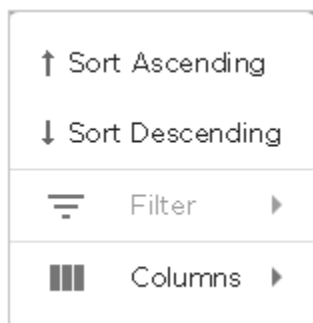
Parameter	Value
Device Name	Displays the name of the device.
Description	Displays a description of the device.
Annotations	
MAC	Displays the MAC Address for the device.
Random MAC	Indicates whether the device is using random MAC (yes) or not (no).
Observed	
Ad-Hoc	
First Seen	Displays the date the device was first seen on the network
Last Seen	Displays the date the device was last seen on the network.
Polled Authentication	
Polled Encryption	
Sensed Authentication	
Sensed Encryption	

Table 7: (continued)

Parameter	Value
Reported SSID	Displays the SSID for the device.
Reported IP	Displays the device's IP Address
Protocols	
Noise	
Signal Strength	Displays the signal strength of the device.
Channel	
Terminating	Indicates whether the device is terminating (yes) or not (no).
VLAN	
Vendor	Displays the name of the vendor of the device.

By default, only few a subset of columns are displayed in the table. Depending on the context, additional fields can be manually added to the table.

To manipulate the data display, select the  icon to the left of any column header. For example, you can sort the data, add or remove table columns, and apply a filter (when available). The following drop-down list displays.




Select the **Filter** control (if available) to filter the data in the column based on the available filtering criteria. You can also apply a filter by clicking on graph categories within the widgets.

Select the **Columns** item to view a list of columns that can be added to the table.

The following table lists the additional columns that can be added to the table.

Field	Description
Name	This column displays the name of the device if configured.
MAC	This column displays the MAC address of the device.

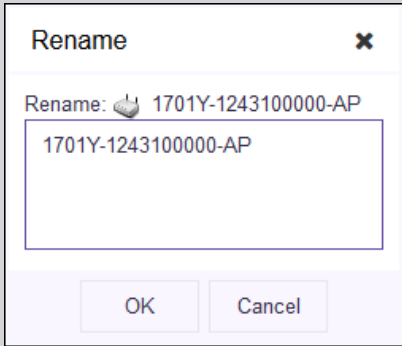
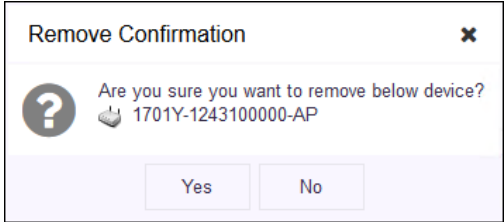
Field	Description
IP	This column displays the IP address assigned to this device.
First Seen	This column displays the date and time this device was first seen on the network.
Scope	This column displays the name of the site/location where this device is located as identified by Extreme AirDefense.
Floor	This column displays the floor number (in the site/location) where this device is located as identified Extreme AirDefense.
802.1x Name	Displays the 802.1x name of the device.
Manufacturer	This column displays the name of the manufacturer of the device.
Classification	This column displays the device's classification as classified by Extreme AirDefense. A device can be classified as <i>Sanctioned (Inherit Profile)</i> , <i>Unsanctioned, Neighboring, Or Sanctioned (Assigned Profile)</i> . You can manually set a device's classification from the  > Classification menu item from within the table.
Sensed Authentication	This column displays the authentication scheme the device uses to authenticate.
Sensed Encryption	This column displays the encryption scheme used by the device if any.
Polled Authentication	This column displays the polled authentication for this device.
Polled Encryption	This column displays the polled encryption scheme for this device.
Protocols	This column displays the various wireless protocols supported by the device.
Device Actions	This column indicates if any of the following actions have taken place: <ul style="list-style-type: none"> • AP Test • Wireless Vulnerability Assessment • Termination • Dedicated Spectrum Analysis • Inline Spectrum Analysis
Access Points	This column displays the name of the access point that sees this device.
Sensor	This column displays the name of the sensor that sees this device.
Security Policy	This column displays the security policy, if any, applied to this device.

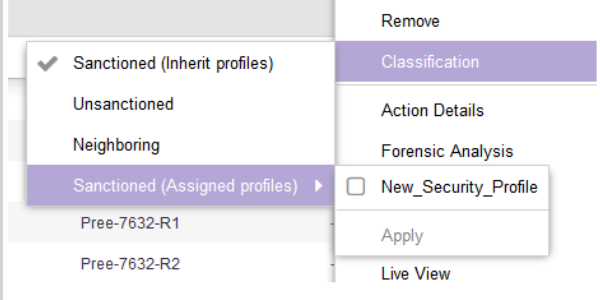
Device Actions

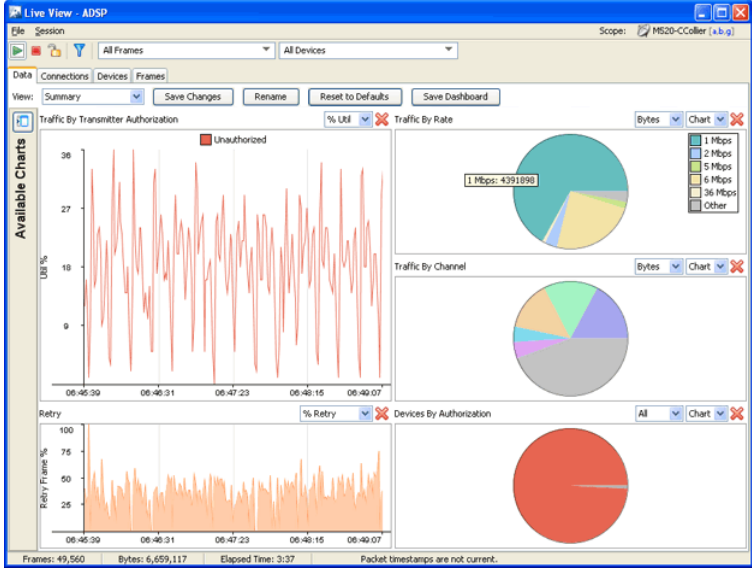
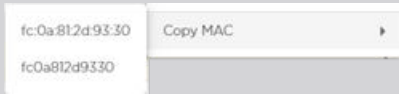
The following actions can be performed on a each device listed in the table. Select the



icon to display the list of actions that can be performed. The actions that can be performed are different for the different device types.

Action	Description
Alarms	Displays the Alarms for the device. When selected, the alarms for this device are displayed in the Alarms screen
Rename	<p>Select this menu item to rename this device. Use this menu item to configure a meaningful name for this device. A small window displays. Use this Rename window to provide a name for this device.</p> 
Remove	<p>Select this menu item to remove the device. A small confirmation window displays. Select Yes to remove the device. Select No to exit without removing the device.</p> 

Action	Description
<p>Classification</p>	<p>Use this menu item to classify the device into one of <i>Sanctioned (Inherit profiles)</i>, <i>Unsanctioned</i>, <i>Neighboring</i>, and <i>Sanctioned (Assigned Profiles)</i>.</p>  <p>The <i>Sanctioned (Assigned Profiles)</i> menu item expands to show a list of available profiles that can be assigned to this device.</p>
<p>Client Type</p>	<p>Use this menu item to select the device's correct client type when the device has not been automatically classified by Extreme AirDefense. Client Type can be one of the following types:</p> <ul style="list-style-type: none"> • Categorized Device • Scanner • Employee Personal Device • Guest WiFi User • Laptop • Phone • Tablet • Loyalty Customer • In Store Customer • Potential Customer
<p>Action Details</p>	<p>Select the Action Details menu item to view a table listing specific actions occurring on the device.</p>
<p>Add to ACL</p>	<p>Use this menu item to add this device to the Access Control List.</p> <p>Note: The ACL option is supported only with AirDefense systems that are integrated with ExtremeCloud IQ Controller management platforms.</p>
<p>Connection Troubleshooting</p>	<p>Use this menu to troubleshoot this device's ability to connect to your network. This opens the Troubleshoot Device screen in a new browser tab.</p>
<p>Forensic Analysis</p>	<p>Use the Forensic Analysis menu item to analyze the device and provide detailed information on the device. Forensic Analysis returns the threat level of the device, device alarms, and device association details about the device.</p>

Action	Description
Locate	Use the Locate menu item to locate this device on your network. This opens the Location Tracking window from where you can track the device.
Live View	<p>The Live View menu item displays the Live View window for the device where you can view the device's live status and other parameters.</p> 
Port Lookup (Find this Device)	Use the Port Lookup menu item to scan for and locate this device, in your network, using its MAC address.
Terminate	Use the Terminate menu item to open the Termination options window from where you can terminate this device.
Copy MAC	<p>The Copy MAC menu item is an ease of use feature and enables you to copy the MAC address of the device in hexadecimal or colon hexadecimal notation. Click this menu item to expand it and view MAC formats that can be copied.</p>  <p>Select the MAC format to copy to your PC's clipboard.</p>

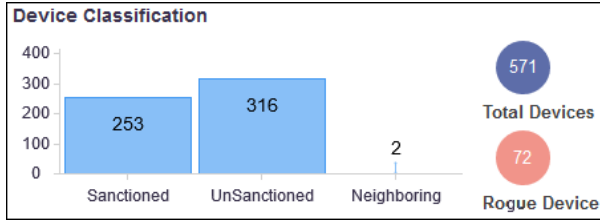
Wireless Clients - Widgets

The **Wireless Clients** tab displays a set of widgets on top of the display area. These widgets are:

- [Device Classification](#)
- [Sanctioned Devices Seen in Last 5 Days](#)
- [Trend - Device Seen Comparison \(For Last 3 Days\)](#)

Widget - Wireless Client Tab - Device Classification

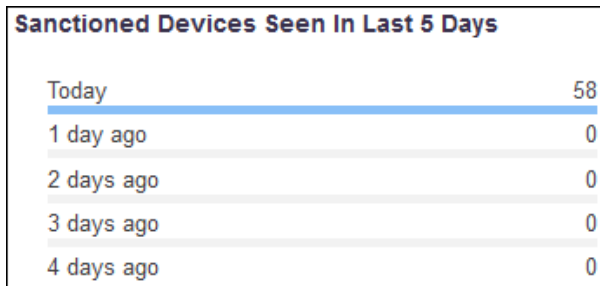
This widget displays the total number of devices, identified and then classified by AirDefense. This widget shows the count of all the devices and rogues in the network. It also displays a graph of the devices segregated as *Sanctioned*, *Unsanctioned*, and *Neighboring*.



Hover on each of these device types to view more details.

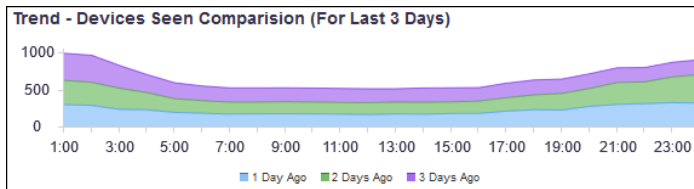
Widget - Wireless Clients Tab - Sanctioned Devices Seen in Last 5 Days

This widget displays a graph that compares the number of sanctioned wireless client devices seen within the network in the last five(5) days.



Widget - Wireless Clients - Trend—Device Seen Comparison (For Last 3 Days)

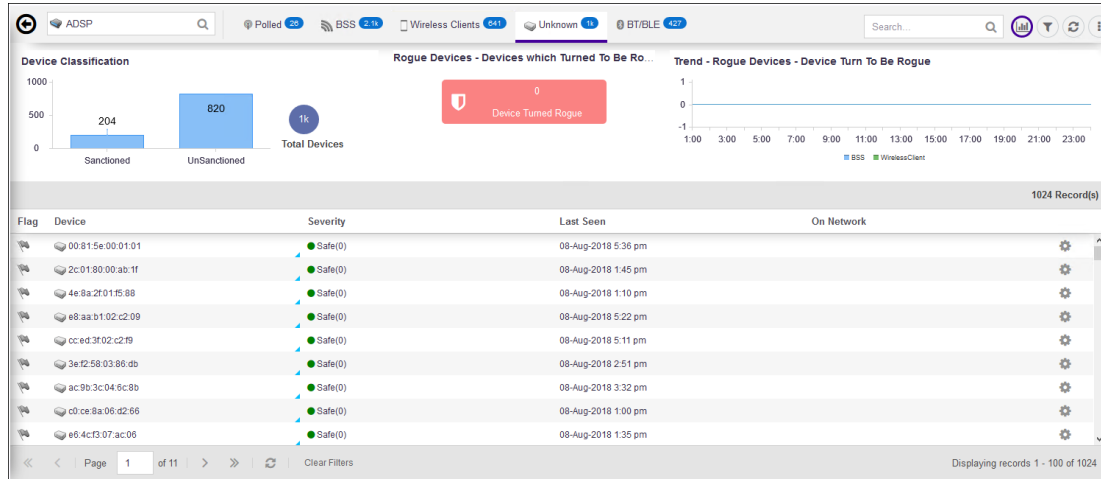
This widget displays a graph that displays the hourly trend of all wireless clients seen in the network in the last three(3) days.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

Unknown Devices



The **Unknown Devices** tab displays a list of all devices on the wired network that were discovered by Extreme AirDefense from the source or destination address in communications from or to a wireless device in your network. If Extreme AirDefense is unable to identify the MAC address listed as the ultimate source or destination, then the identified device is classified as *Unknown Device*.

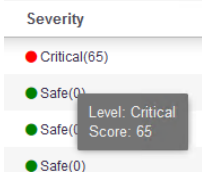


The **Unknown Devices** tab displays a set of widgets on the top of the display area. The widgets are:


- [Device Classification](#)
- [Rogue Devices - Devices which turned to be rogue](#)
- [Trend - Rogue Devices - Device turned to be rogue](#)

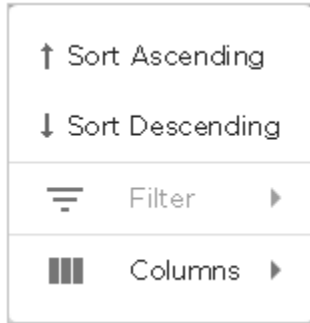
The **Unknown Devices** table displays the following information:

Field	Description
Flag	Select the  icon to indicate that this device is considered to be of interest. The flag changes to  .
Device	This column displays the device type icon and its name. Hover on the name to display more details about the device in a pop-up. The following image is a pop up that displays on hover. <div data-bbox="711 1297 1110 1751" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Applied: Device</p> <p>MAC Address: d8:84:66:79:9c:a9 Appliance: 192.168.20.201 Manufacturer: Extreme Networks, Inc. Name: 1701Y-1208500000-sens Polled Name: 1701Y-1208500000-sens IP Address: 192.168.20.93 Model: AP3912FCCI Last Seen: 24-Jul-2018 2:57 pm Capabilities: Sensor, AP Firmware: 10.41.08.0012 Sensor Firmware: 10.41.08.0012 Licenses: WIPS Spectrum Analysis Live RF Advanced Forensics AP Test Connection Troubleshooting WLAN Management Tracker Integration Vulnerability Assessment Advanced Infrastructure Forensics Proximity and Analytics</p> </div>
	Select the MAC address of the device to view its details in a separate window.

Field	Description
Severity	<p>This column displays the device's threat level to your network. Hover on this value to display a threat score for this device.</p> <ul style="list-style-type: none"> • Severe indicates a severity level of <i>Severe</i> which is higher than the level <i>Critical</i>. • Critical indicates a severity level of <i>Critical</i>. • Major indicates a severity level of <i>Major</i>. • Minor indicates a severity level of <i>Minor</i>. • Safe indicates the site/location is <i>Safe</i>. 
Last Seen	This column displays the date and time this device was last seen on the network.
On Network	<p>Identifies how ADSP obtained the MAC address of a non-wireless device. The different entries are:</p> <ul style="list-style-type: none"> • 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.

By default, only few a subset of columns are displayed in the table. Depending on the context, additional fields can be manually added to the table.

To manipulate the data display, select the  icon to the left of any column header. For example, you can sort the data, add or remove table columns, and apply a filter (when available). The following drop-down list displays.

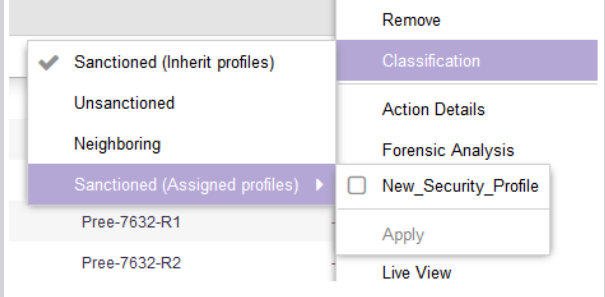


Select the **Filter** control (if available) to filter the data in the column based on the available filtering criteria. You can also apply a filter by clicking on graph categories within the widgets.

Select the **Columns** item to view a list of columns that can be added to the table.

The following table lists the additional columns that can be added to the table.

Field	Description
Name	This column displays the name of the device if configured.
MAC	This column displays the MAC address of the device.
IP	This column displays the IP address assigned to this device.
First Seen	This column displays the date and time this device was first seen on the network.
Scope	This column displays the name of the site/location where this device is located as identified by Extreme AirDefense.
Floor	This column displays the floor number (in the site/location) where this device is located as identified Extreme AirDefense.

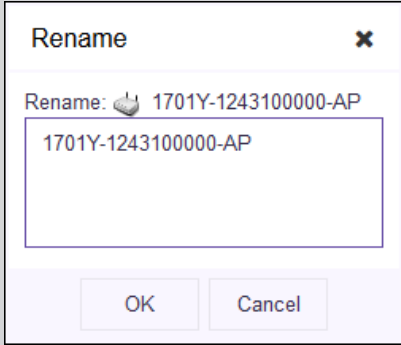
Field	Description
Manufacturer	This column displays the name of the manufacturer of the device.
Classification	<p>Use this menu item to classify the device into one of <i>Sanctioned (Inherit profiles)</i>, <i>Unsanctioned</i>, <i>Neighboring</i>, and <i>Sanctioned (Assigned Profiles)</i>.</p>  <p>The <i>Sanctioned (Assigned Profiles)</i> menu item expands to show a list of available profiles that can be assigned to this device.</p>

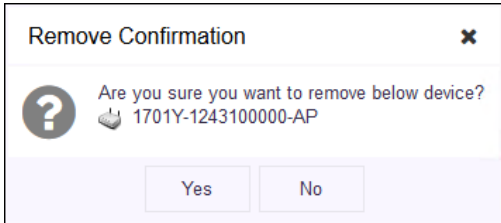
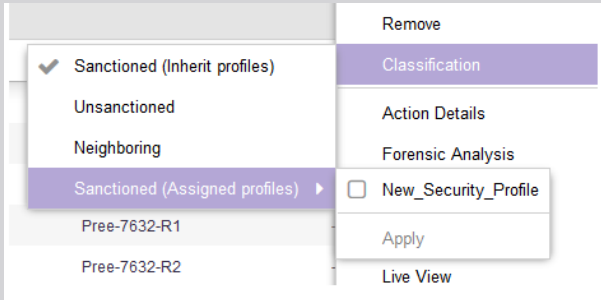
Device Actions

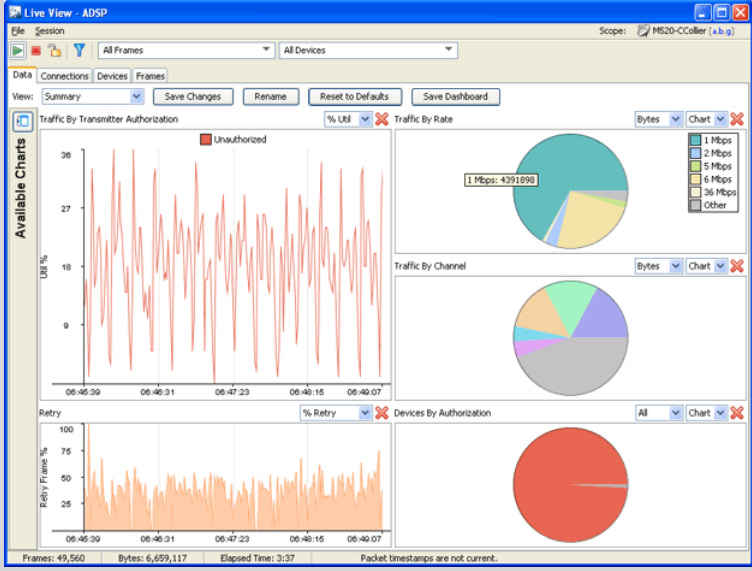
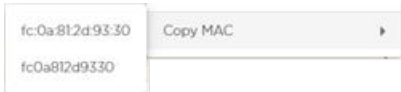
The following actions can be performed on a each device listed in the table. Select the



icon to display the list of actions that can be performed. The actions that can be performed are different for the different device types.

Action	Description
Alarms	Displays the Alarms for the device. When selected, the alarms for this device are displayed in the Alarms screen
Rename	<p>Select this menu item to rename this device. Use this menu item to configure a meaningful name for this device. A small window displays. Use this Rename window to provide a name for this device.</p> 

Action	Description
Remove	<p>Select this menu item to remove the device. A small confirmation window displays. Select Yes to remove the device. Select No to exit without removing the device.</p> 
Classification	<p>Use this menu item to classify the device into one of <i>Sanctioned (Inherit profiles)</i>, <i>Unsanctioned</i>, <i>Neighboring</i>, and <i>Sanctioned (Assigned Profiles)</i>.</p>  <p>The <i>Sanctioned (Assigned Profiles)</i> menu item expands to show a list of available profiles that can be assigned to this device.</p>
Action Details	<p>Select the Action Details menu item to view a table listing specific actions occurring on the device.</p>
Add to ACL	<p>Use this menu item to add this device to the Access Control List.</p> <p>Note: The ACL option is supported only with AirDefense systems that are integrated with ExtremeCloud IQ controller management platforms.</p>
Forensic Analysis	<p>Use the Forensic Analysis menu item to analyze the device and provide detailed information on the device. Forensic Analysis returns the threat level of the device, device alarms, and device association details about the device.</p>

Action	Description
<p>Live View</p>	<p>The Live View menu item displays the Live View window for the device where you can view the device's live status and other parameters.</p> 
<p>Port Lookup (Find this Device)</p>	<p>Use the Port Lookup menu item to scan for and locate this device, in your network, using its MAC address.</p>
<p>Terminate</p>	<p>Use the Terminate menu item to open the Termination options window from where you can terminate this device.</p>
<p>Copy MAC</p>	<p>The Copy MAC menu item is an ease of use feature and enables you to copy the MAC address of the device in hexadecimal or colon hexadecimal notation. Click this menu item to expand it and view MAC formats that can be copied.</p>  <p>Select the MAC format to copy to your PC's clipboard.</p>

Unknown Devices - Widgets

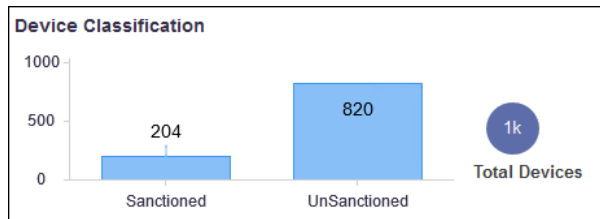
The **Unknown Devices** tab displays a set of widgets on the top of the display area. The widgets are:

- [Device Classification](#)
- [Rogue Devices - Devices which turned to be rogue](#)
- [Trend—Rogue Devices - Device turned to be rogue](#)

Widget - Unknown Devices - Device Classification

This widget displays the total number of devices, identified and then classified as *Unknown Device* by AirDefense. This widget shows the count of all the unknown

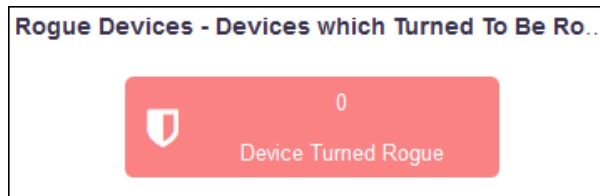
devices. It also displays a graph of the devices segregated as *Sanctioned* and *Unsanctioned*.



Hover on each of these device types to view more details.

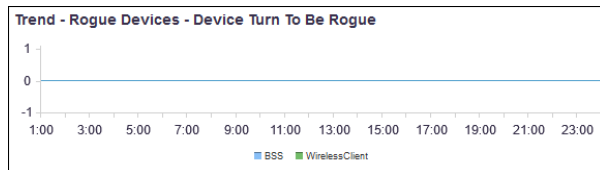
Widget - Unknown Devices - Devices which turned to be Rogue

This widget displays the number of *Unknown* devices that were identified as *Rogue* devices.



Widget - Unknown Devices - Trend - Rogue Device - Device Turn To be Rogue

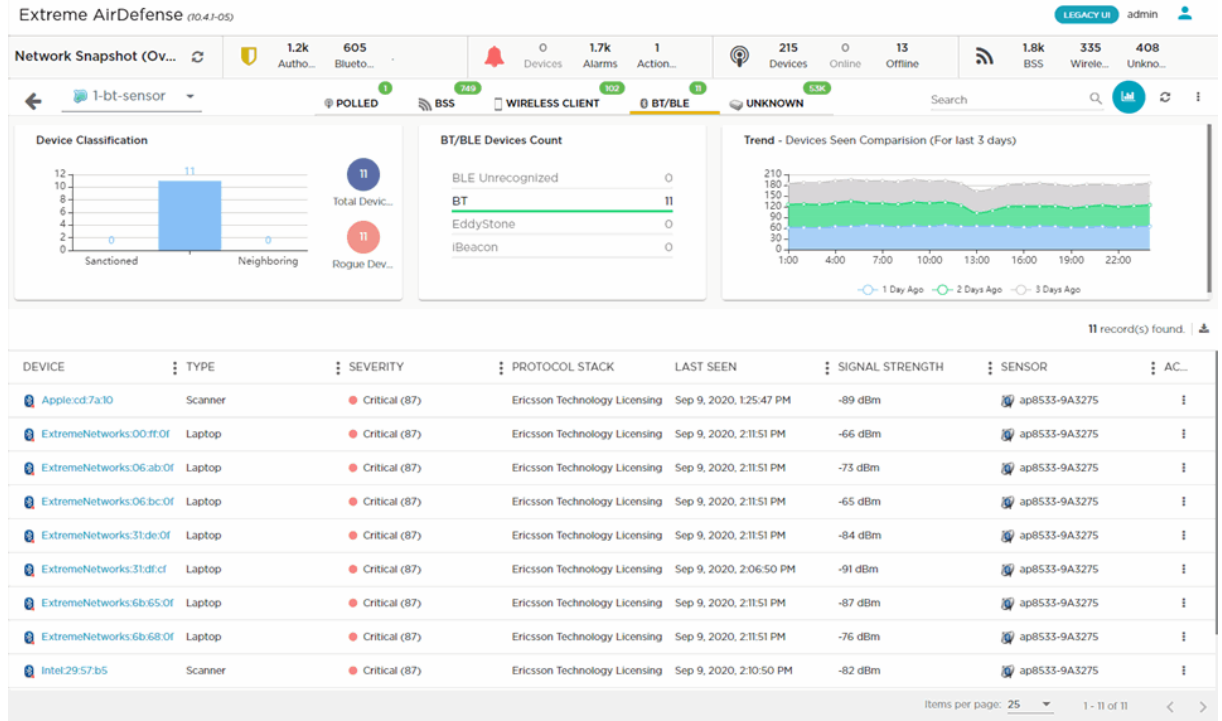
This widget displays a hourly trend of *BSS* and *Wireless Clients* that turned rogue over a period of twenty four(24) hours.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.

Bluetooth and Bluetooth Low Energy Devices

The **BT/BLE** tab displays a list of Bluetooth or Bluetooth Low Energy (BLE) clients, sanctioned or otherwise, that were discovered by Extreme AirDefense in your network during regular scans.



The **BT/BLE** tab displays a set of widgets on top of the display area. These widgets are:

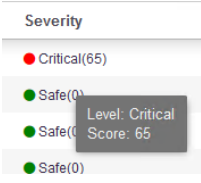
- [Device Classification](#)
- [Sanctioned Devices Seen in Last 5 Days](#)
- [Trend - Device Seen Comparison \(For Last 3 Days\)](#)

The **BT/BLE** table displays the following information for each device:


Table 8:

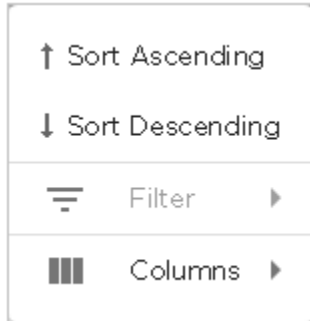
Field	Description
Device	Displays the device type icon and its name. Place your cursor on the name to display more details about the device in a pop-up: <div style="border: 1px solid gray; padding: 5px; width: fit-content; margin: 10px auto;"> MAC Address: f8:13:37:00:05:99 Appliance: 192.168.20.201 Last Seen: 15-Aug-2018 5:59 pm Signal Strength: -95 dBm </div>
Type	Displays the type of BT/BLE device as identified by Extreme AirDefense.

Table 8: (continued)

Field	Description
Severity	<p>Displays the device's threat severity to your network. Place your cursor on this value to display a threat score for the device:</p> <ul style="list-style-type: none"> • Severe indicates a severity level of <i>Severe</i> which is higher than the level <i>Critical</i>. • Critical indicates a severity level of <i>Critical</i>. • Major indicates a severity level of <i>Major</i>. • Minor indicates a severity level of <i>Minor</i>. • Safe indicates the site/location is <i>Safe</i>. 
Protocol Stack	Displays the name of the protocol in which the device is participating.
Last Seen	Displays the date and time the device was last seen on the network.
Signal Strength	Displays the signal strength for the device.
Sensor	Displays the name of the sensor that sees the device.
Action	Displays several device actions in a drop-down list, including Alarms , Remove , Classification , Live View , and Copy MAC .

By default, only few a subset of columns are displayed in the table. Depending on the context, additional fields can be manually added to the table.

To manipulate the data display, select the  icon to the left of any column header. For example, you can sort the data, add or remove table columns, and apply a filter (when available). The following drop-down list displays.




Select the **Filter** control (if available) to filter the data in the column based on the available filtering criteria. You can also apply a filter by clicking on graph categories within the widgets.

Select the **Columns** item to view a list of columns that can be added to the table.


The following table lists the additional columns that can be added to the table.

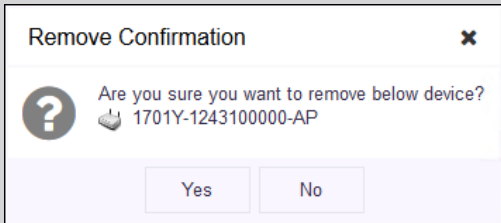
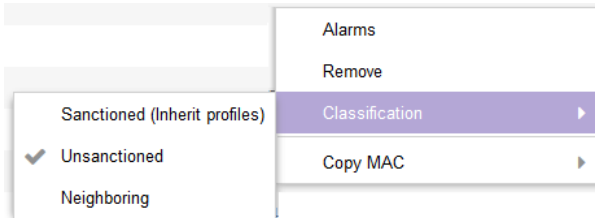
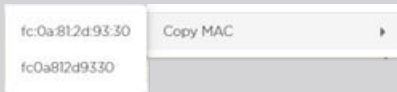
Table 9:

Field	Description
Description	Displays a brief description of the device. This information only displays when configured on the device. The column is empty if no description is configured on the device.
MAC	Displays the device's MAC address.
First Seen	Displays the date and time the device was first seen on the network.
Scope	Displays the site or location where the device is located as identified by Extreme AirDefense.
Floor	Displays the floor number at the site or location where the device is located as identified by Extreme AirDefense.
Manufacturer	Displays the name of the device's manufacturer
Classification	Displays the device's classification as classified by Extreme AirDefense. A BT/BLE device can be classified as <i>Sanctioned (Inherit Profile)</i> , <i>Unsanctioned</i> , or <i>Neighboring</i> . You can manually set a device's classification from the  > Classification menu item from within the table.

Device Actions

The following actions can be performed on device listed in the Device Details.

Select the  icon to display the list of actions that can be performed. The actions that can be performed are different for the different device types. The actions also differ depending on whether you checked specific devices in Device Details (the action applies to the checked devices) or if you checked no devices (the action applies to all of the listed devices).

Action	Description
Alarms	Displays the Alarms for the device. When selected, the alarms for this device are displayed in the Alarms screen
Remove	<p>Select this menu item to remove the device. A small confirmation window displays. Select Yes to remove the device. Select No to exit without removing the device.</p> 
Classification	<p>Use this menu item to classify the device into one of <i>Sanctioned (Inherit profiles)</i>, <i>Unsanctioned</i>, or <i>Neighboring</i>.</p> 
Copy MAC	<p>The Copy MAC menu item is an ease of use feature and enables you to copy the MAC address of the device in hexadecimal or colon hexadecimal notation. Click this menu item to expand it and view MAC formats that can be copied.</p>  <p>Select the MAC format to copy to your PC's clipboard.</p>

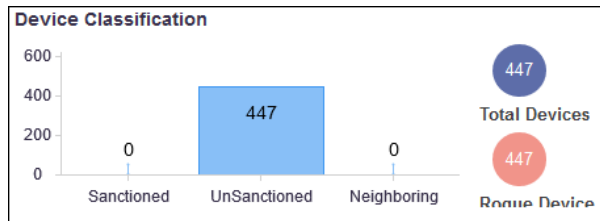
BT, BLE Devices - Widgets

The **BT/BLE** tab displays a set of widgets on top of the display area. These widgets are:

- [Device Classification](#)
- [Sanctioned Devices Seen in Last 5 Days](#)
- [Trend - Device Seen Comparison \(For Last 3 Days\)](#)

Widget - BT/BLE Devices - Device Classification

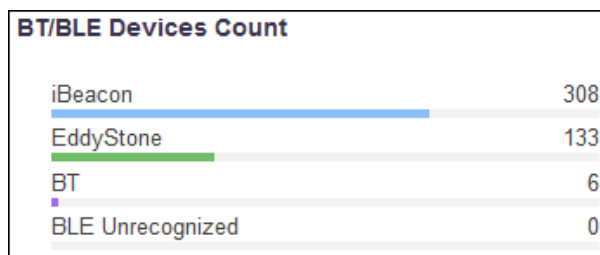
This widget displays the total number of devices, identified and then classified as *BT/BLE Device* by AirDefense. This widget shows the count of all BT/BLE devices and the number of rogue devices of this type. It also displays a graph of the devices classified as *Sanctioned*, *Unsanctioned*, or *Neighboring*.



Hover on each of these device types to view more details.

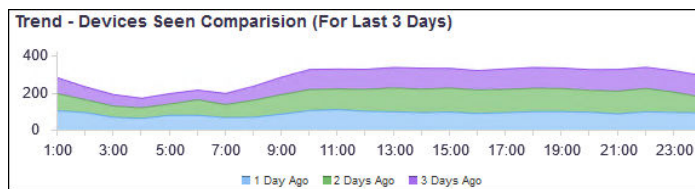
Widget - BT/BLE Devices - BT/BLE Devices Count

This widget displays the counts of different Bluetooth or Bluetooth Low Energy devices found on the network. This data is displayed as a bar graph.



Widget - BT/BLE Devices - Trend - Devices Seen Comparison (Last 3 Days)

This widget displays a graph that displays the hourly trend of all Bluetooth / Bluetooth Low Energy devices seen in the network in the last three(3) days.



Select a label to include or exclude its data in the widget. When the data for the label is excluded, the label is displayed in a lighter color.



Alarm View

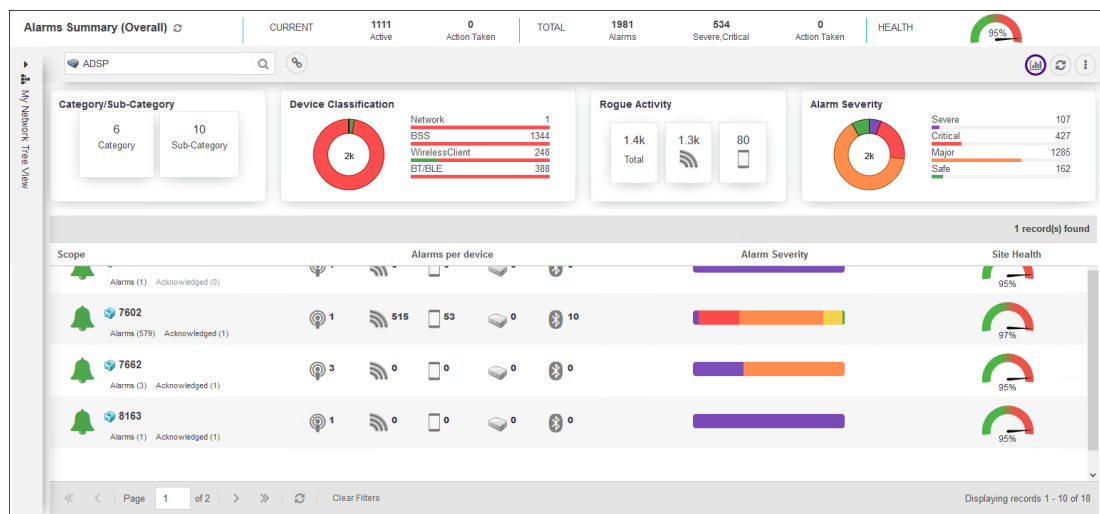
[Alarms - Alarms Summary](#) on page 104

[Alarms - Details View](#) on page 105

[Alarms Widget View](#) on page 106

[Alarm Details List](#) on page 108

Use the **Alarm View** screen to manage your alarms from AirDefense. **Alarm View** screen is a single location from where you can see the alarms raised in your network. It provides various tools to drill down to the alarms and take appropriate actions on these alarms.



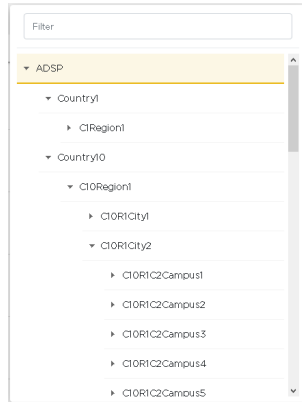
Alarms View can be divided into three sections, **Alarms Summary**, **Network Tree View** and **Details** panes. Use the **Network Tree View** pane to select the scope of the data to be display within the **Alarms View** pane. The **Details** pane displays alarms for the context(scope) selected in the **Network Tree View** pane.

Alarms Summary

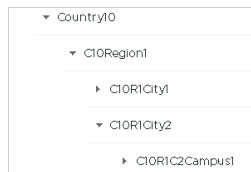
The **Alarms Summary** pane lists a count of all alarms generated in the network and also the overall health of the AirDefense monitored network. For more information, see [Alarms Summary](#).

Network Tree View

The **Network Tree View** section is a drop-down pane that you use to select the context or the scope of the data to display.









Use the  icon before each tree node to expand it and view its nodes. Similarly, use the  icon to collapse an expanded node.




Select the node for which you want to view the details. On selecting the node, the **Details View** pane immediately starts loading with the appropriate information. Depending on the size of the data to display, the number of devices to load and your network connection, it might take sometime for the data to be displayed.

Details View

The **Details View** pane displays a list of alarms generated for the selected site/location. The following information is displayed:






Column	Description
Scope	<p>This column displays the name of the site/location for which the alarm information is generated. Select the site/location name to launch the Alarm Details screen to view the alarms for the site. This option is only available for a site that has at least one alarm or notification indicated for it. For more information, see Alarms - Details View on page 105.</p>
Alarm per Device	<p>This column displays the count of alarms generated by each device category.</p> <div data-bbox="711 716 1110 764" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  </div> <p>The icons represent these device categories:</p> <ul style="list-style-type: none"> •  -Polled devices. •  -BSSs. •  -Wireless Clients. •  -Unknown devices. •  -Bluetooth/BLE devices.

Column	Description
Alarm Severity	<p>This column indicates the severity level of the alarms for this site/location as a bar graph. The graph color codes each severity type.</p>  <p>Hover on each of the color bars to view the number of alarms generated for this site/location for the selected alarm level. Select a color on this bar graph to filter and view the alarms of the selected severity. The filtered alarms are displayed in Alarm Details screen.</p>
Site Health	<p>This column indicates a calculated value that indicates the site's health and displayed on a graph. Site health is calculated using the threat index of each alarm raised in the site and includes the alarms from all the floors in the site. When calculating Site Health, the threat index of the topmost alarms in the site are used. For example, for a site where alarms of the categories <i>Severe</i>, <i>Critical</i>, <i>Minor</i> are present, only the threat indexes of all alarms of <i>Severe</i> category are considered for calculating the Site Health. Other alarms are ignored. When you acknowledge an alarm, the threat index of that alarm is no longer included when calculating the Site Health in the next iteration of Site Health calculation.</p>

Toolbar


The **Toolbar** enables you to perform specific tasks quickly.

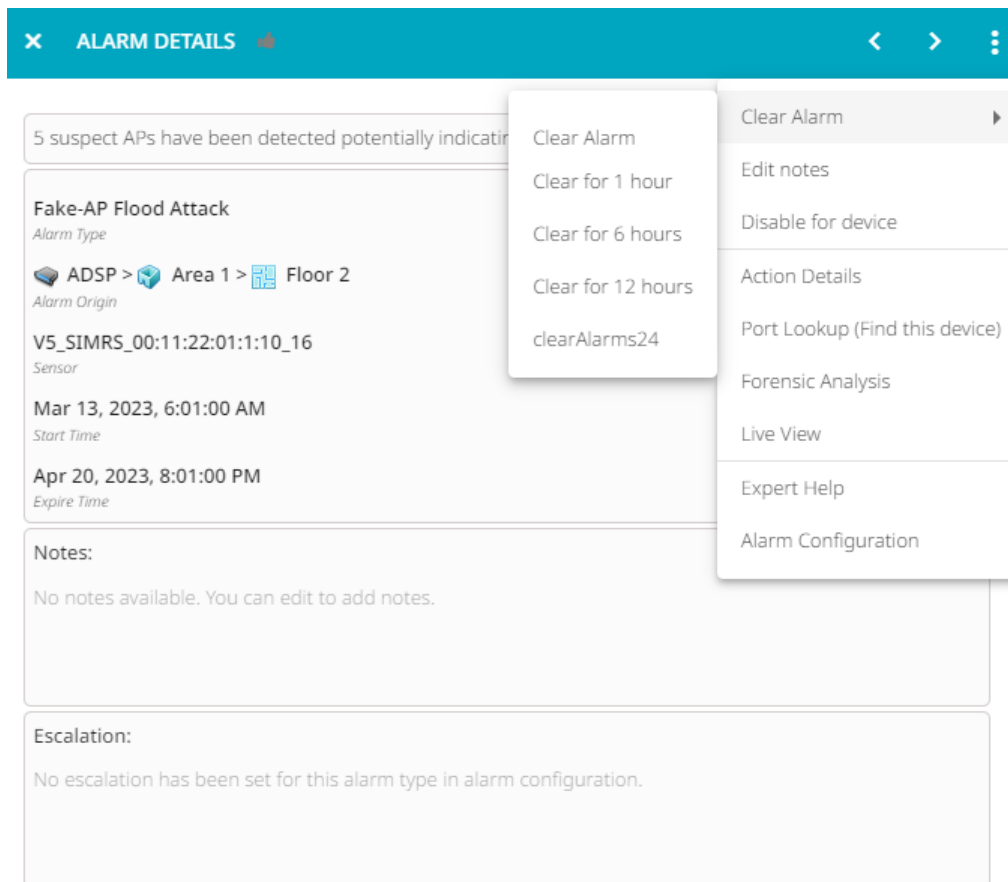
Table 10: Alarms Toolbar Actions


Tool	Description
	Use this field to select the scope of the data to display in this screen.
	Select this icon to view or hide the Grid Chart view in this pane.
	Periodically use this Refresh icon to refresh the data displayed on this screen.
	Select this icon to view a list of alarms that were raised in the last one hour.
	Displays actions that you can select and apply to the alarms in the Alarms Details view. The available actions differ depending on how many alarms were checked. For details, see Alarm Details List on page 108.

Alarm View Drill Downs

From the **Alarms Details** list, you can open the following drill downs to get more information on specific alarms and the device on which the alarm was raised:

- **Alarm Details**—For a specific alarm, click the **Alarm Type** column to open a drill down with detailed information on that alarm. Within the drill down, click the three dots  in the top right to access alarm actions that you can apply to that alarm. See the following image for an example of the drill down and the available actions.



- **Device**—For a specific alarm, click the **Device** column entry to open a drill down for the device on which the alarm was raised. Within the drill down, click the pencil icon  to edit basic device information. For more information on devices, see [Device Details Screen](#) on page 52.

Alarms - Alarms Summary

The **Alarms Summary** pane displays an up to date counts of all the alarms generated in your network.



Note

This pane cannot be modified.

The following information is displayed:

Panel	Description
Current	Displays the current total of the alarms raised in the network. This panel lists the Active alarms and the count of Action Taken on these alarms.
Total	Displays the total number of alarms raised in the network. This panel also displays a count of alarms of the categories <i>Severe</i> and <i>Critical</i> along with the count of Action Taken on these alarms.
Health	This column indicates a calculated value that indicates the health of your AirDefense monitored network. This value is calculated using the threat index of each alarm raised in the network and includes the alarms from all the sites and floors managed by AirDefense. When calculating the Health value, the threat index of the topmost alarms are used. For example, when alarms of the categories <i>Severe</i> , <i>Critical</i> , <i>Minor</i> are present, only the threat indexes of all alarms of <i>Severe</i> category are considered for calculating the Health value. Other alarms are ignored. The threat index of alarms that are acknowledged are not included when calculating the Health in the next iteration of the calculation.

Periodically use the  icon next to the pane's title to refresh the data displayed within this pane.

Alarms - Details View

This screen displays a list of all alarms raised for the selected site/location along with information required to take appropriate actions with respect to these alarms.

Extreme AirDefense (10.6.0-03) admin

Alarm Summary (Overall) **CURRENT** 67 Active 0 Action Taken **TOTAL** 115 Alarms 53 Severe,Critical 0 Action Taken **HEALTH**

← Area 1 Search

25 record(s) found.

<input type="checkbox"/>	FLAG	CRITICALITY	ALARM TYPE	DEVICE	START TIME	STATUS	SSID	SENSOR	ACKN...
<input type="checkbox"/>		Minor (20)	Wireless Client Exces...	CISCOVdigiaco.wlan	Apr 19, 2023, 1:33:00 PM	Inactive (expires in 1:46)	typhoon	VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Mar 13, 2023, 6:01:00 AM	Inactive (expires in 8:47)		VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Mar 13, 2023, 8:18:00 AM	Inactive (expires in 8:59)		VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Mar 13, 2023, 5:32:00 AM	Inactive (expires in 9:16)		VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Mar 13, 2023, 6:55:00 AM	Inactive (expires in 8:52)		VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Apr 2, 2023, 3:14:00 AM	Inactive (expires in 9:04)		VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Mar 13, 2023, 5:23:00 AM	Active		VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Mar 13, 2023, 5:26:00 AM	Inactive (expires in 7:58)		VS_SIMRS_00:11:22:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Attack	VS_SIMRS_00:11:22:...	Mar 26, 2023, 1:43:00 AM	Inactive (expires in 8:37)		VS_SIMRS_00:11:22:...	

This screen is divided into these sections:

- **Alarm Summary (Overall)** - Provides a snapshot of the current state of your network with respect to the alarms generated. Use the to refresh the displayed data. For more information on this pane, see [Alarms - Alarms Summary](#) on page 104.
- **Network Tree View** - Use this pane to select the scope of the data to display. For more information, see the section *Network Tree View* in [Alarm View](#) on page 100.
- **Toolbar** - The toolbar enables you to perform specific tasks such as hiding/showing the widgets, refreshing the screen, and performing other common actions in a single click. Use the **Search** field to filter devices listed in this screen.
- **Alarm Details List** - This pane displays a list of all alarms generated in your AirDefense managed network and in the selected site/location. For more information, see [Alarm Details List](#) on page 108.

Alarms Widget View

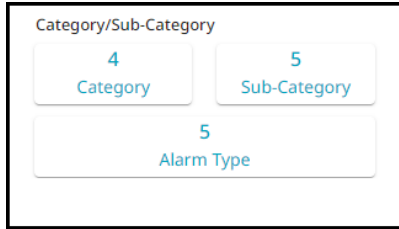
The **Alarms Widgets** pane consists of four (4) widgets that provides a comprehensive insight the alarms generated on your network. These widgets are:

- [Category/Sub-Category](#)
- [Device Classification](#)
- [Rogue Activity](#)
- [Alarm Severity](#)

Periodically use the icon to update the data displayed in the widgets.

Category/Sub-category Widget

The **Category/Sub-Category** widget displays the number of alarms raised for each alarm category, sub-category and alarm type.

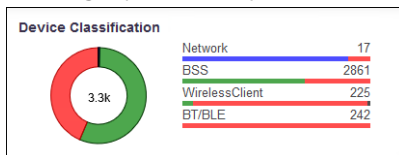


Hover over each of these category types to view the breakdown of alarms for that category. Apply a filter to the Alarms Details List by selecting any individual category name or individual alarm name. The Alarms Details list will display only the alarms that meet the filter criteria.

Category	Alarms	SubCategory	Alarms
Rogue Activity	1178	Authorization	1046
Exploits	826	Violation	816
Policy Compliance	780	Impersonation	816
Bluetooth	242	Attacks	772
Performance	154	Incorrect BSS	772
Vulnerabilities	120	Configuration Observed	772
Proximity	34	Bluetooth Devices	242
Infrastructure	11	Congestion	149
		Rogue Exploit	127
		Suspect Activity	118
		Presence	34
		Management	11
		DoS	8
		Environment	8
		Extrusion	5
		LiveRF	4
		Active Attacks	2
		Coverage	1

Device Classification

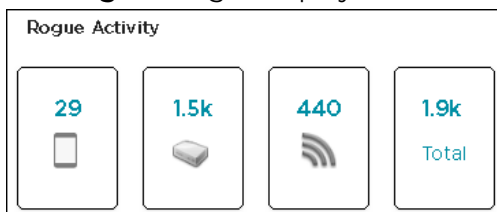
The **Device Classification** widget displays a graph of the alarms generated by the different device types. This widget displays the break up of the alarms by device type as a bar graph and a pie chart.



Hover on each of the device type labels to view a details about that particular device type. Click the device type label to launch **Alarms** detail view with the data filtered for the *Device Type*.

Rogue Activity

The **Rogue** widget displays the number of Rogue device for each device type.

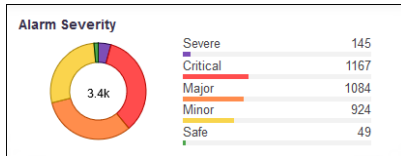


Select the number above each device type icon to launch the **Alarms** detail view with the data filtered for the *Rogue Activity* and the selected *Device Type*.

Alarm Severity

The **Category/Sub-Category** widget displays the number of alarms raised for each alarm category or sub-category.

The **Alarm Severity** widget displays graphs of the number of alarms of different severity, generated in your network, as a bar graph and a pie chart.



Click the **Severity** label to launch **Alarms** detail view with the data filtered for the *Severity* value.

Alarm Details List

The **Alarm Details List** displays details for each alarm generated in a site or location.



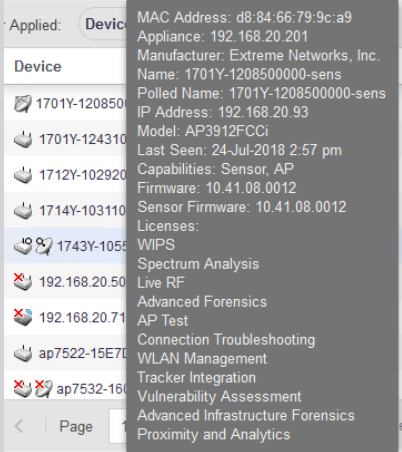
To filter the list, do either of the following:

- From the list columns, click one of the icons, click **Filter**, and choose the filter.
- Click on a graph category within the various alarm widgets.

To take action on one or more alarms, check the adjacent check box(es) and select an action from the Actions menu . For details, see [Alarm Actions](#).


<input type="checkbox"/>	FLAG	CRITICALITY	ALARM TYPE	DEVICE	START TIME	STATUS	SSID	SENSOR	ACK...
<input type="checkbox"/>		Minor (20)	Wireless Client Ex...	00:b0:00:00:44:05	Apr 18, 2023, 3:22:00 PM	Inactive (expires in 1:43)	typhoon	VS_SIMRS_00:11:...	
<input type="checkbox"/>		Minor (20)	Wireless Client Ex...	CISCOldgiaco.wl...	Apr 18, 2023, 5:20:00 PM	Inactive (expires in 2:13)	typhoon	VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 6:01:00 AM	Inactive (expires in 7:53)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 8:18:00 AM	Inactive (expires in 9:25)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 5:32:00 AM	Active		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 6:55:00 AM	Inactive (expires in 8:54)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Apr 2, 2023, 3:14:00 AM	Active		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 5:23:00 AM	Inactive (expires in 8:42)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 5:26:00 AM	Inactive (expires in 9:25)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 26, 2023, 1:43:00 AM	Inactive (expires in 9:06)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 6:24:00 AM	Inactive (expires in 9:00)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Apr 1, 2023, 4:23:00 PM	Inactive (expires in 7:55)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 5:58:00 AM	Inactive (expires in 9:30)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Apr 10, 2023, 3:29:00 PM	Inactive (expires in 8:25)		VS_SIMRS_00:11:...	
<input type="checkbox"/>		Major (30)	Fake-AP Flood Att...	VS_SIMRS_00:11:...	Mar 13, 2023, 6:13:00	Inactive (expires in		VS_SIMRS_00:11:...	

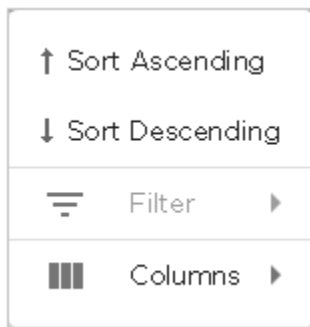
The following information is displayed:

Column	Description
Flag	Select the  to indicate that the selected alarm is considered to be of interest. The flag changes to  .
Criticality	This column displays the criticality value of the alarm. Criticality is a numerical value that indicates how critical the alarm is. The higher the value, the more critical the alarm. Each alarm has a numerical value (criticality index) pre-assigned to it. This value is used when calculating the Site Health for the site/location/system.
Alarm Type	This column displays the type of alarm generated. Each alarm is assigned a threat or criticality index. This index value is displayed in the Criticality column.
Device	<p>This column displays the device type icon and its name. Hover on the name to display more details about the device in a pop-up. The following image is a pop up that displays on hover.</p> <p>The information that the pop-up displays is different for the different device types. The following image is of a pop-up displaying data for a polled device.</p> 
Start Time	This column displays the time and date when the alarm started.
Status	This column displays the status of the alarm. Alarms are either <i>active</i> or <i>inactive</i> . Active alarms can either be acknowledged or not acknowledged. Inactive alarms are displayed till they expire after a configured time duration.
SSID	This column displays the SSID of the network to which the device -that generated this alarm- is adopted to.

Column	Description
Sensor	This column displays the name of the sensor that observed the device that generated this alarm.
Acknowledge	Use this column to mark the alarm as <i>Acknowledged</i> . This indicates that you have selected the alarm and viewed the alarm's details. Acknowledged alarms are not used when calculating a site's Site Health .

By default, only few a subset of columns are displayed in the table. Depending on the context, additional fields can be manually added to the table.

To manipulate the data display, select the  icon to the left of any column header. For example, you can sort the data, add or remove table columns, and apply a filter (when available). The following drop-down list displays.




Select the **Filter** control (if available) to filter the data in the column based on the available filtering criteria. You can also apply a filter by clicking on graph categories within the widgets.

Select the **Columns** item to view a list of columns that can be added to the table.

The following table lists the additional columns that can be added to the table.

Column	Description
Alarm ID	This column displays the unique ID assigned to this alarm when it was generated. This ID can be used to query for specific alarms.
Expire Time	Displays the date and time when the alarm expires. In case of inactive alarms, this field displays the time the alarm will be purged from the system.
Signal Strength	This column displays the signal strength of the device that triggered this alarm.
Channel	This column displays the channel and the frequency on which this device, that triggered the alarm, was identified.
Notes	This column displays the notes made for this alarm.
Summary	This column displays a brief description of the alarm.

Alarm Actions

Use the Alarm Actions menu icon  from the toolbar to select and apply an action against selected alarms.

In the Alarms Details list, check the relevant alarms and then use this menu to select the desired action. You can use this method to apply a single action against multiple selected alarms. There are also a pair of actions that apply to all alarms in the current list, and which are available only when no alarms are checked. See the following table for details.

Table 11: Alarm Actions Description



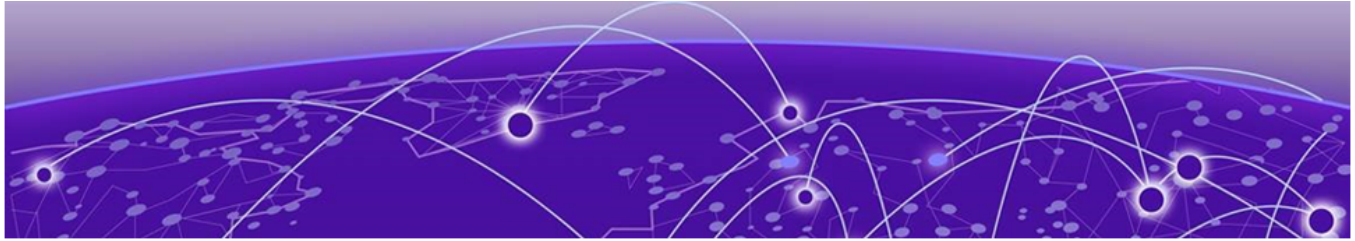
Alarm Action	Description
Clear Alarm	Use this menu item to clear the selected alarm(s). When cleared, the alarm is removed from this list. You can also temporarily clear the alarm for the duration of 1 Hour, 6 Hours, 12 Hours, or 24 Hours. Once this duration expires, the alarm is added back to this list if the conditions that generated this alarm are not cleared.
Edit Alarm Notes	Use this menu item to add more details in a note that is attached to the selected alarm(s). When selected, a dialog is displayed where you can add your notes.
Set Flag	Use this menu to set a flag for the selected alarm(s). Flags are used to indicate that the alarm requires attention. When a flag is set, it changes to  .
Remove Flag	Use this menu to unset or remove a flag set for the selected alarm(s). When unset, the flag icon changes to  .
Mark as New	Use this menu to mark the selected alarm(s) as new. When marked, the alarm is indicated in bold.
Mark as Acknowledged	Use this menu to mark the selected alarm(s) as <i>Acknowledged</i> . This indicates that you have selected the alarm and viewed the alarm's details. Acknowledged alarms are not used when calculating a site's Site Health .
Export Alarms	Use this menu to export the selected alarm(s) as a Comma Separated Value (csv) file. When prompted, provide the name and place to save the file.
Manage Cleared Alarms	Use this menu to manage alarms that you have cleared or selected to remain cleared for a set period. Use the screen to reset these cleared alarms.

Table 11: Alarm Actions Description (continued)


Alarm Action	Description
Clear all (filtered) alarms	<p>Clears all alarms that are currently listed in the Alarms List page. Note the following conditions:</p> <ul style="list-style-type: none"> • This action is available only when no alarms are checked in the Alarms List. If any alarms are checked, this action is greyed out. • If the number of alarms exceeds what the page displays, this action includes alarms that were returned by the query, but which appear off the current page (use the Items per page controls to increase the number of displayed alarms). • The action label includes "filtered" only if you have a filter applied to the list. In this case, only alarms that meet the filter criteria are affected.
Acknowledge all (filtered) alarms	<p>Acknowledges all alarms that are currently listed on the Alarms List view. Note the following conditions:</p> <ul style="list-style-type: none"> • This action is available only when no alarms are checked in the Alarms List. If any alarms are checked, this action is greyed out. • If the number of alarms exceeds what the page displays, this action includes alarms that were returned by the query, but which appear off the current page (use the Items per page controls to increase the number of displayed alarms). • The action label includes "filtered" only if you have a filter applied to the list. In this case, only alarms that meet the filter criteria are affected.



Configuration

- [Appliance Management](#) on page 115
- [Structure Configuration](#) on page 148
- [Auto-Placement Rules](#) on page 160
- [Discovery Profile and Polling Configuration](#) on page 166
- [Communication Profile](#) on page 177
- [Security Profile](#) on page 186
- [Alarm Action Manager](#) on page 199
- [Device Action Manager](#) on page 221
- [Sensor Manager](#) on page 253
- [Alarm Configuration](#) on page 268
- [Wired Network Monitoring](#) on page 271
- [Performance Profile](#) on page 274
- [Environment Monitoring](#) on page 287
- [Client Types](#) on page 289
- [Appliance Settings](#) on page 291
- [Device Age Out](#) on page 294
- [Configuration Backup](#) on page 296
- [Forensic and Log Backup](#) on page 301
- [Configuration Restore](#) on page 306
- [Download Logs](#) on page 307
- [Redundant Appliance Synchronization](#) on page 311
- [Configuration Clear](#) on page 316
- [Language Settings](#) on page 318
- [License Management](#) on page 319
- [User Management](#) on page 330
- [Remote Profile Management](#) on page 355
- [System Settings](#) on page 360

Use the **Settings** screen to configure a few of the many Extreme AirDefense settings. This screen provides configuration options that enable you to configure a few profiles, set Extreme AirDefense structure, and manage Extreme AirDefense licenses.

Select the  icon from the main menu tree on the left of the user interface to launch the configuration dashboard.

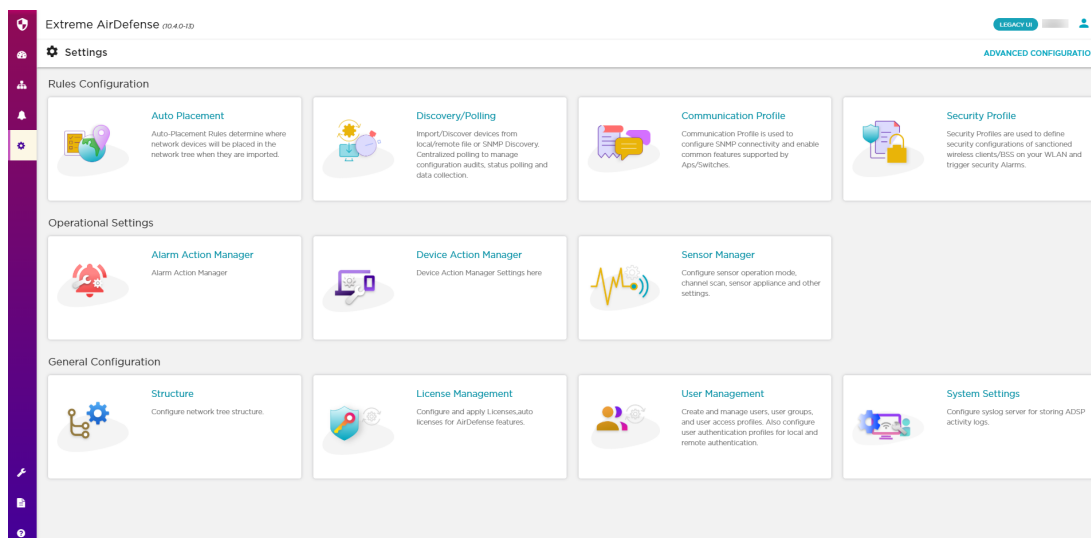


Figure 19: New User Interface - Settings Screen

The following configurations are managed from this screen.

- **Rules Configuration** - This section provides links to configure the following rules:
 - **Auto Placement** - The configurations defined within this profile determine how network devices are placed in your network hierarchy tree when imported. For more information, see [Auto-Placement Rules](#) on page 160
 - **Discovery/Polling** - The configurations defined within this profile enable you to import devices from local/remote files or to discover devices using SNMP discovery. These settings in this screen also configure centralized polling of devices for managing configuration audits, status polling, and other types of data collections. For more information, see [Discovery Profile and Polling Configuration](#) on page 166.
 - **Communication Profile** - The configurations defined within this profile enables you to set SNMP connection parameters and enable some common features supported by access points and switches. For more information, see [Communication Profile](#) on page 177.
 - **Security Profile** - The configurations defined within this profile are used to define the security configurations of sanctioned wireless devices and BSSs on your network and trigger security alarms when issues are discovered in your network. For more information, see [Security Profile](#) on page 186.
- **Operational Settings** - This section provides links to configure the different operational parameters for the Extreme AirDefense server.
 - **Sensor Manager** - Use this configuration screen to configure sensor scan patterns, set advanced spectrum analysis parameters, and enable or disable sensor-level options. The screen is also used to create and manage *Sensor Profiles* that are used to apply a set of sensor settings.

- **General Configuration** - This section provides links to configure the hierarchy of sites/location within your Extreme AirDefense network. You can also manage your licenses from within this section.
 - Structure - Use this configuration screen to set Extreme AirDefense site hierarchy. For more information, see [Structure Configuration](#) on page 148.
 - Appliance Licensing - Use this configuration screen to view and manage your licenses. For more information, see [License Management](#) on page 319.
 - User Management - Use this configuration screen to view and manage your users with respect to this Extreme AirDefense system. For more information, see [User Management](#) on page 330.
 - System Settings - Use this configuration screen to configure the remote log server to send your Extreme AirDefense system's activity logs to. For more information, see [System Settings](#) on page 360.

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**.

Appliance Settings

Port:

Mail Relay Server: (IP address or fully qualified host name)

Max Connections: (Total simultaneous application server connections)

User Session Limit of simultaneous sessions per user

Air-Termination system

Policy based Air-Termination system

Port Suppression system

Auto-Logout after minute(s)

Spectrum Scan Timeout after minute(s)

Sensor Cloaking Limit simultaneous cloaked sensors

Function	Description
Port	<p>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.</p> <p>Note: AirDefense will not allow you to choose a port already in use.</p>
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	<p>Air Termination enables you to terminate the connection between your wireless LAN and any associated authorized or unauthorized or Wireless Client.</p> <p>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.)</p> <p>No: (Default). Click this radio button to disable AirTermination.</p> <p>Note: If you are not an Admin User, this setting will not be visible.</p>

Function	Description
Policy-based Air Termination System Enabled	<p>Policy-based Air Termination is an automated version of Air Termination. This feature enables you to formulate an Action Plan to automatically terminate the connection between your wireless LAN and any associated authorized or unauthorized or Wireless Client, based on alarms.</p> <p>Yes: Click this radio button to enable Policy-based Termination at the system level.</p> <p>No: (Default). Click this radio button to disable Policy-based Termination.</p> <p>Note: If you are not an Admin User, this setting will not be visible.</p>
Port Suppression System	<p>Port Suppression enables you to turn off the port on the network switch through which a device is communicating. You can suppress the communications port for any network device, effectively shutting down the communication port for the device.</p> <p>Yes: Click this radio button to enable Port Suppression at the system level. See the Note, below.</p> <p>No: (Default). Click this radio button to disable Port Suppression.</p> <p>Note: You must have added SNMP Managed Switches and have full read and write privileges (see Adding/Importing Switches).</p>
Auto-Logout Enabled	<p>Use this feature to enable/disable the automatic logout feature, which logs a user out of AirDefense after a specified amount of time.</p> <p>Yes: Click this radio button to use Auto-Logout and activate the Auto-Logout Timeout scroll list.</p> <p>No: Click this radio button to disable the Auto Logout and deactivate the Auto-Logout Timeout drop down list.</p> <p>Note: You must log off AirDefense and then log back in before changes take effect.</p>
Auto-Logout Timeout (Minutes)	<p>This scroll list is activated when the Auto-Logout Enabled option is selected. Use the scroll button to set the number of minutes for the automatic logout feature to log users out of the system.</p> <p>Note: You must log off AirDefense and then log back in before changes take effect.</p>
Spectrum Scan Timeout	<p>This drop-down menu allows you to set the timeout value for scanning during dedicated Spectrum Analysis. The values can be 1 - 120.</p>
Sensor Cloaking Limit	<p>The number amount of Sensors that can be cloaked at any one time.</p>

Backup / Restore Status

Backup / Restore Status allows you to view the status of your configuration backups and restores.

Backup / Restore Status ? Help

Status of most recent configuration backup:

✔ **Scheduled backup: Default Backup was successful**
Start: 04/04/2013 12:00 AM - End: 04/04/2013 12:02 AM

Status of most recent configuration restore, sync, or clear:

❗ **Command-line SMUPGRADE failed (1 Error occurred)**
Start: 03/31/2013 9:35 PM - End: 03/31/2013 9:35 PM

Errors:
Command-line SMUPGRADE/Restore /usr/local/Speedwell/DB/(?!*(GridCache))*/-1: File size or content not right: /usr/local/Speedwell/DB/ASP/Applications.xml

The top section displays status information about backups. The bottom section displays status information about configuration restores, synchronization, clear information, and upgrade information.

The following status information is displayed:

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

Certificate / Key Validation

Certificate / Key Validation is where you validate certificates, and add or remove public keys.

Certificate Validation

The **Certificate Validation** tab allows you to validate certificate communications for your appliance and/or for any third party servers.

The screenshot shows the 'Certificate / Key Validation' window with the 'Certificate Validation' tab selected. It contains two sections: 'Appliance communication' and 'Third party communication', each with three checkboxes for verification options. Below these is an 'OCSP Responder' section with a dropdown menu for 'Certificate Validation' (set to 'Appliance Root Certificate') and a text field for 'URL'.

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

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

Select the appropriate checkbox for each type of verification that you want to check. If the **Check certificate revocation** checkbox is selected, the OCSP Responder fields are activated. When activated, you must select the certificate type and enter its URL.

Clicking **Apply** validates your selections.

Key Validation

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

The screenshot shows the 'Certificate / Key Validation' window with the 'Key Validation' tab selected. It features 'Add Key' and 'Remove Key' buttons at the top. Below is a table with two columns: 'Host' and 'Type'. The table is currently empty.

To add a public key:

1. Click the **Add Key** button.

2. Type in the name of the other server.
3. Select the type of public key that you want to add (SSH-RSA or SSH-DSS).
4. Paste the public key into the **Key** field.

For example, if you possess the following public key:

```
----- BEGIN SSH2 PUBLIC KEY -----
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**.
6. To remove a public key, select (highlight) the key and then click the **Remove Key** button.

Certificate Manager

Certificates verify the authenticity of the AirDefense appliance. They can prevent hijacking of sessions between your browser and the AirDefense appliance, and can

even alert you to physical replacement of the AirDefense appliance. Certificates install into the AirDefense appliance and are sent by the appliance directly to your browser.



Important

AirDefense recommends using a security certificate for every AirDefense appliance in your network. Furthermore, we recommend that you replace the pre-installed security certificate from AirDefense with either a self-signed certificate or a root-signed certificate.

AirDefense supports the X.509 ITU-T (ITU Telecommunication Standardization Sector) standard for certificates. The supported encryption key lengths are 2048, 4096, and 8192. More information about the X.509 ITU-T standard can be found by searching the Internet.

Use the Certificate feature to view and create security certificates for the AirDefense 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 iCertificates feature by following these steps:

View Certificate Details

To view certificate details:

1. Navigate to **Configuration > Appliance Management > Certificate Manager**.

The screenshot shows the 'Certificate Manager' web interface. At the top, there are two tabs: 'Appliance Certificates' (selected) and 'Trusted Certificates'. Below the tabs, a message states: 'The Key Store contains private keys and the certificates with their corresponding public keys.' This is followed by instructions: 'In order to add an SSL certificate to the AirDefense website follow these steps:' and a numbered list: 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. Below the instructions, there is a 'Certificate Password' field, a 'View Certificates' button, a 'Display Password' checkbox, and a 'Change Password' link. The main content area is currently empty. At the bottom, there are four buttons: 'Generate Request', 'Import New', 'Update', and 'Delete'.

2. Enter your certificate password.



Note

The first time you access Certificates use the default password (security). Immediately change the default password to one that is more secure. Do not continue to use the default password.

3. Click the **View Certificates** button.

Certificate Types

Every AirDefense appliance comes with an AirDefense certificate. However, there are three other certificates available; each represents a different level of security.

- Self-signed certificate
- Root-signed certificate
- SSL certificate.

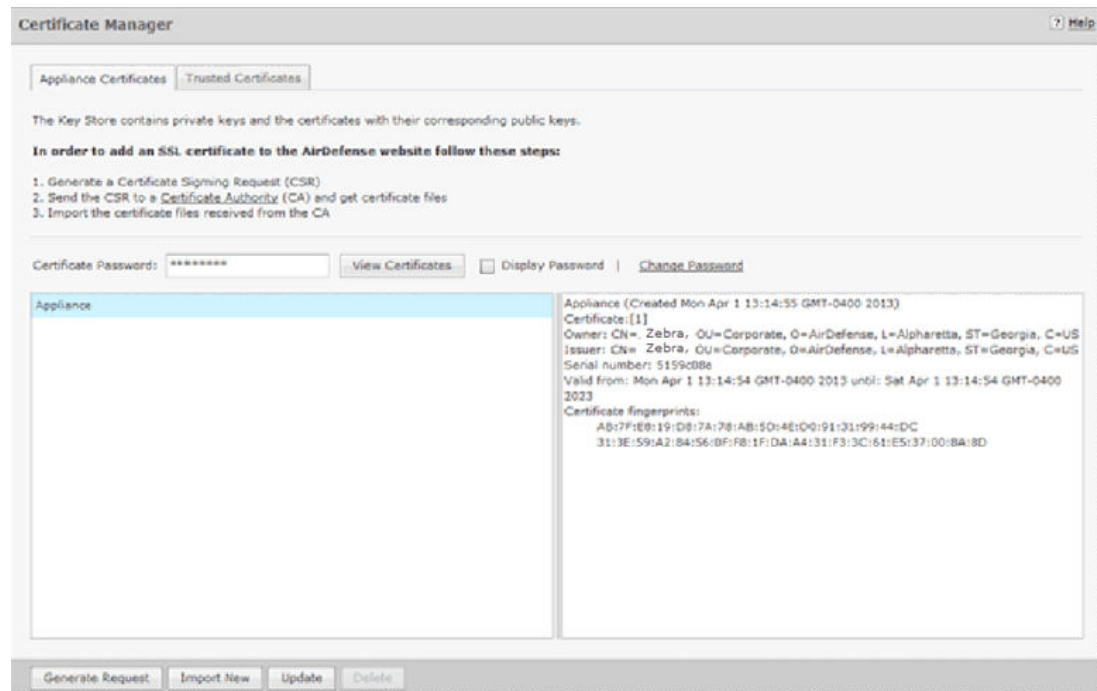
The following table describes each of the certificate types:

Certificate	Description
AirDefense Certificate	The AirDefense certificate represents a minimal level of security. AirDefense ships the AirDefense 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 AirDefense appliance. Unless the certificate meets all required criteria, you will receive one or more alert screens when you open a session with AirDefense.
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

AirDefense 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 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

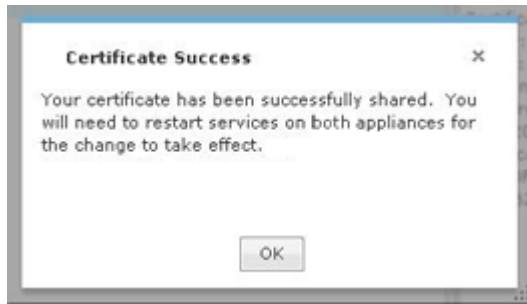
The **Share Appliance Certificate** button is only visible after adding the slave appliance with **Add Devices**.

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.



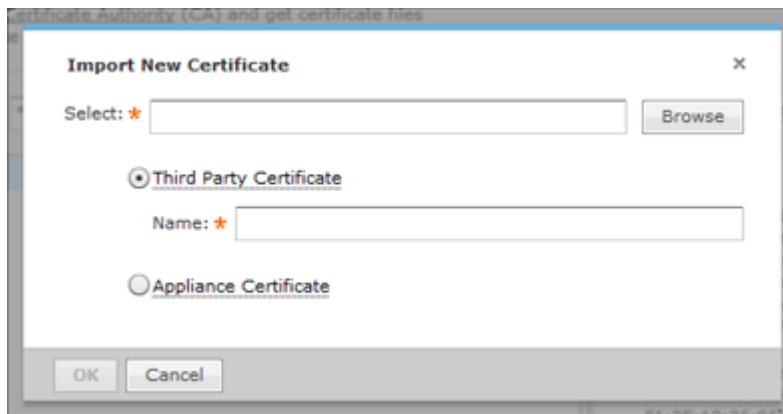
7. Click **OK**.

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 through 13.

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

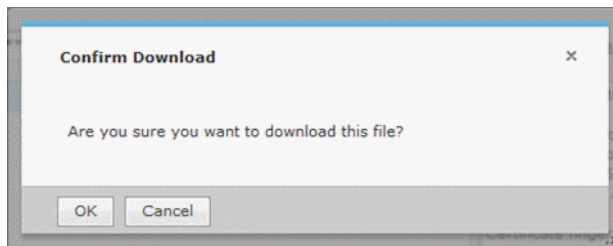
The Appliance Certificates store private keys and the certificates with their corresponding public keys. There are three main steps to adding an appliance certificate. They are:

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.

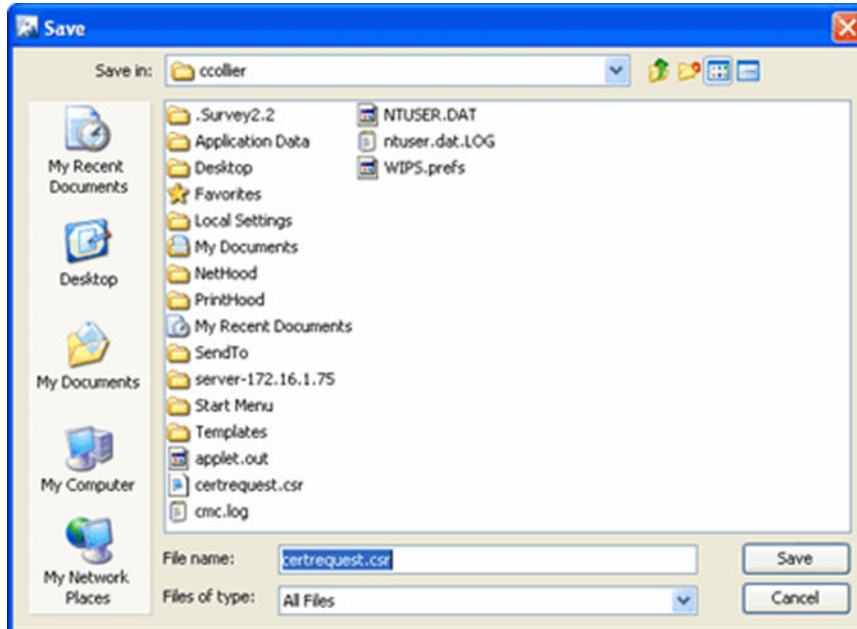
Generate Certificate Signing Request

To generate a Certificate Signing Request (CSR), do the following:

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.

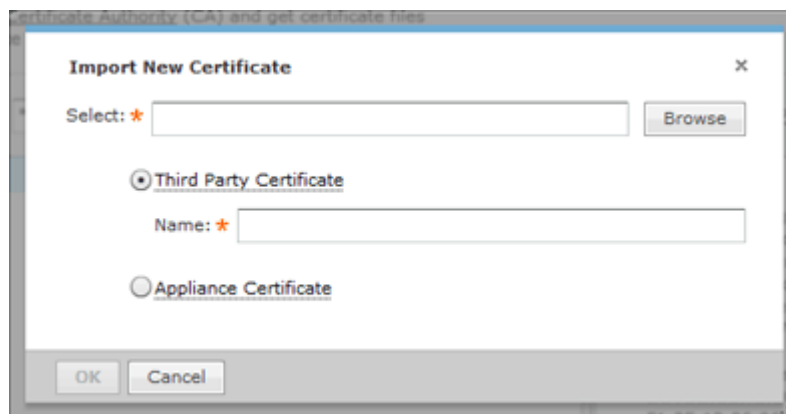
The file save in Generate a CSR has the information that a CA needs to issue certificate files. You will have to present this information to the CA in some way.

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.

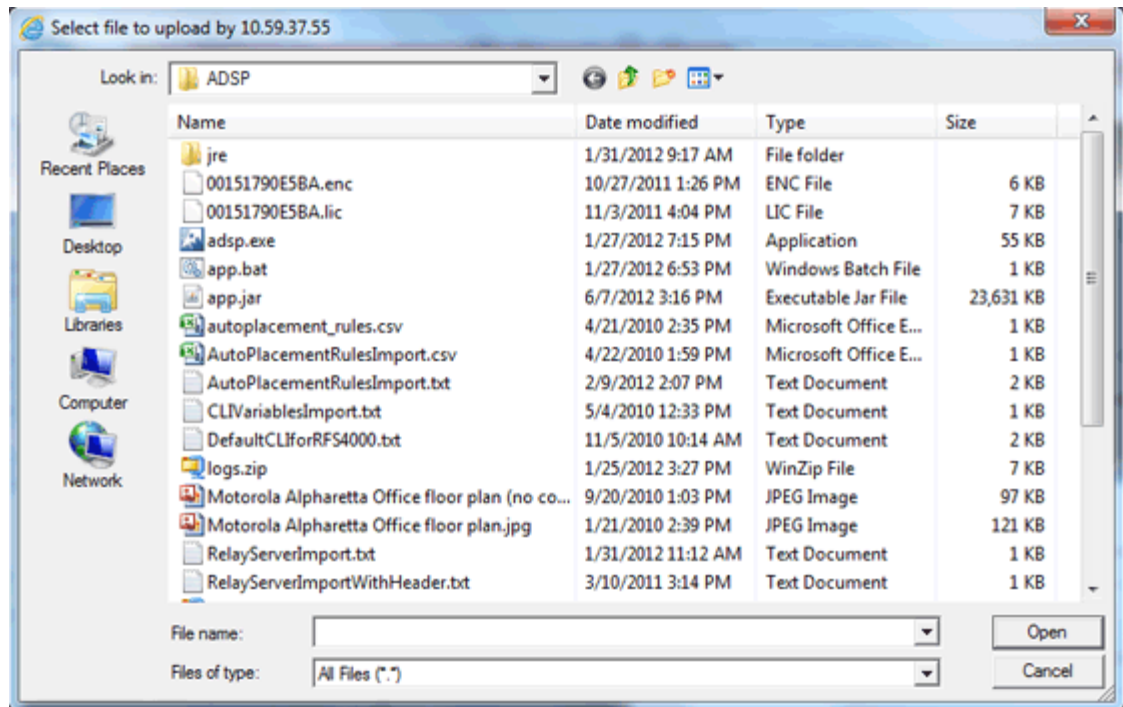


- Click the **Browse** button to open the **Select file to upload** window.



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.



- Navigate to the Intermediate certificate, select (highlight) it, and then click the **Open** button. The file name should now display in the **Select** field.
- Type in a name for the certificate.
- Click **OK**.
- Repeat Steps 1 to 5 to import the Root certificate.
- 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.

- Click **OK**.



Note

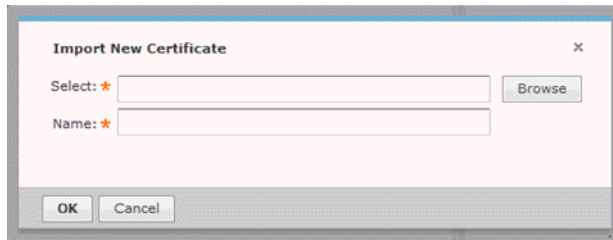
You will have to restart tomcat services before the certificates are activated. The tomcat services are located on your ADSP appliance.

Import New Certificate

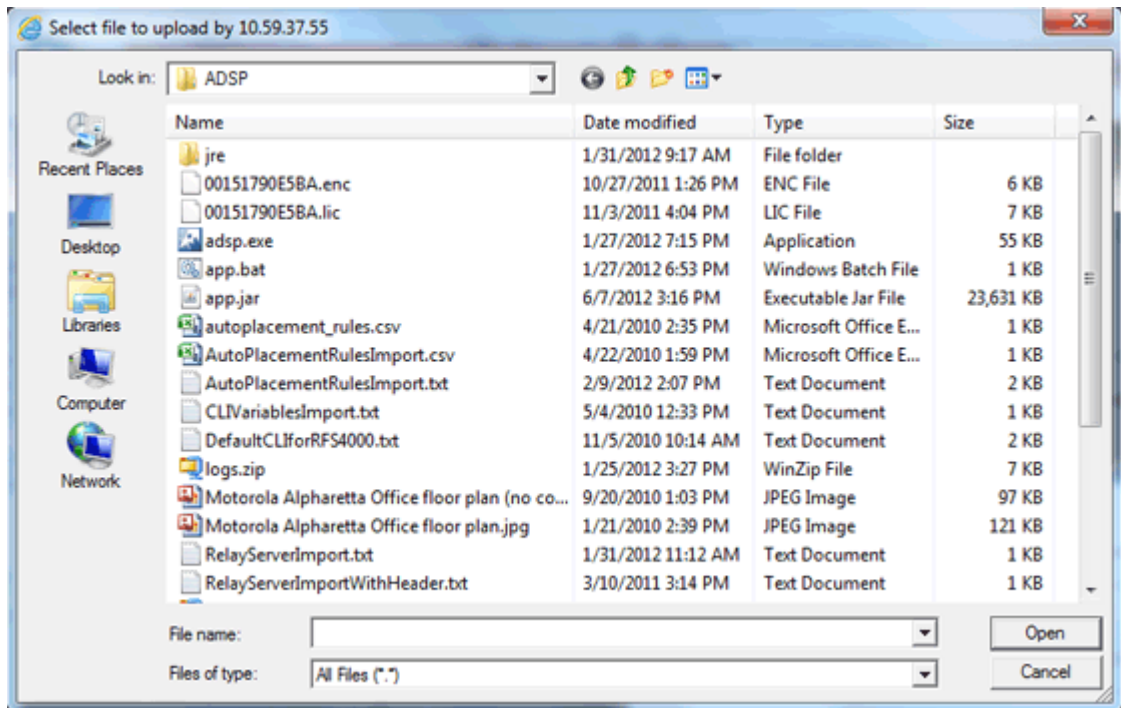
The Trusted Certificates store contains certificates from other parties (like AirDefense kAppliances, LDAP or Radius Servers) that you expect to communicate with, or from

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

This topic discusses the process to update certificate information for certificates already stored in your appliance.

Changing Default Information

A certificate's default information is included with each certificate that you add.

To change the certificate's default information:

1. Click the **Update** button to display the **Update Appliance Certificate** window.

The screenshot shows a dialog box titled "Update Appliance Certificate" with a close button (X) in the top right corner. The dialog contains the following fields:

- Name * (text input): Appliance-01
- Department Name * (text input): Corporate
- Company Name * (text input): AirDefense
- City * (text input): Alpharetta
- State * (text input): Georgia
- Country * (text input): US
- Valid Days * (text input): 3652
- Key Size (dropdown menu): 2048

At the bottom of the dialog are two buttons: "Ok" and "Cancel".

The following table describes the certificate information fields that can be modified:

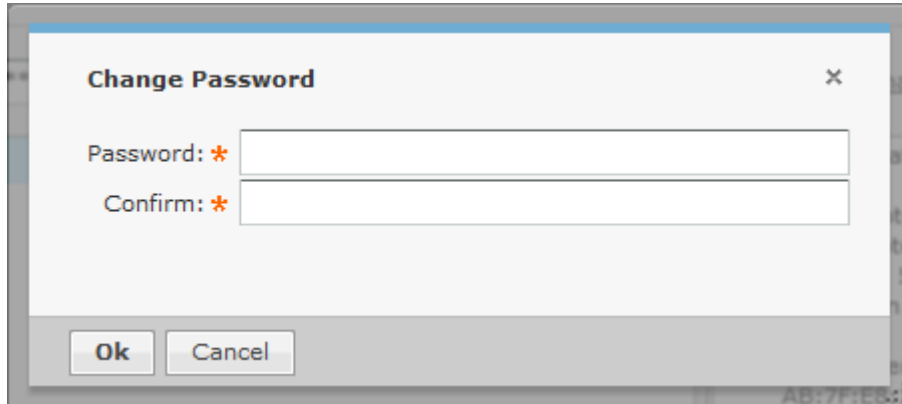
Field	Description
Name	The hostname you assigned the AirDefense appliance.
Department Name	The department in which the AirDefense administrator is a member.
Company Name	The name of your company.
City	The city in which your company is located.
State	The State (full name - not abbreviated) in which the company is located.
Country	The two-character country code for the country in which the company is located.
Valid Days	The number of days a certificate is valid once you add it.
Key Size	The certificate encryption key length. Supported encryption key lengths are 2048, 4096, and 8192.

2. Once done, 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 local computer.



Note

This information is required for Managed Services Provider (MSP) integration.

Depending on your browser, follow one of these procedures:



Note

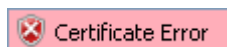
Procedures for Internet Explorer and Firefox are included here. Other browsers will have similar buttons/links that allow you to export a certificate.

- [For Internet Explorer](#) on page 131
- [For Firefox](#) on page 132

For Internet Explorer

To export certificates using Microsoft™ Internet explorer:

1. Click **Certificate Error** near the top of Internet Explorer window.




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. Select a location on the local PC 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

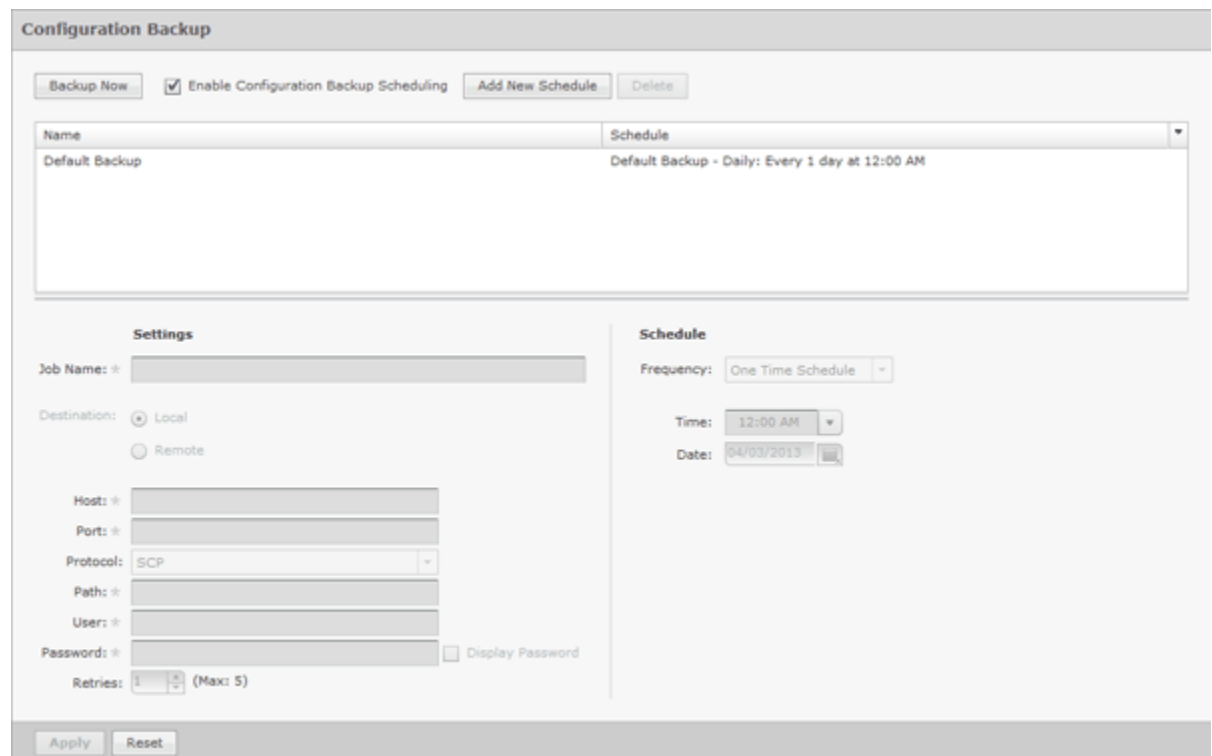
To export certificate using Mozilla™ Firefox:

1. Click the area with the appliance ID located near the top the Firefox window.

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](#)



Configuration Backup

Backup Now Enable Configuration Backup Scheduling

Name	Schedule
Default Backup	Default Backup - Daily: Every 1 day at 12:00 AM

Settings

Job Name: *

Destination: Local Remote

Host: *

Port: *

Protocol: SCP

Path: *

User: *

Password: * Display Password

Retries: 1 (Max: 5)

Schedule

Frequency: One Time Schedule

Time: 12:00 AM

Date: 04/03/2013

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 the `/usr/local/smx/backups` folder.
- 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.

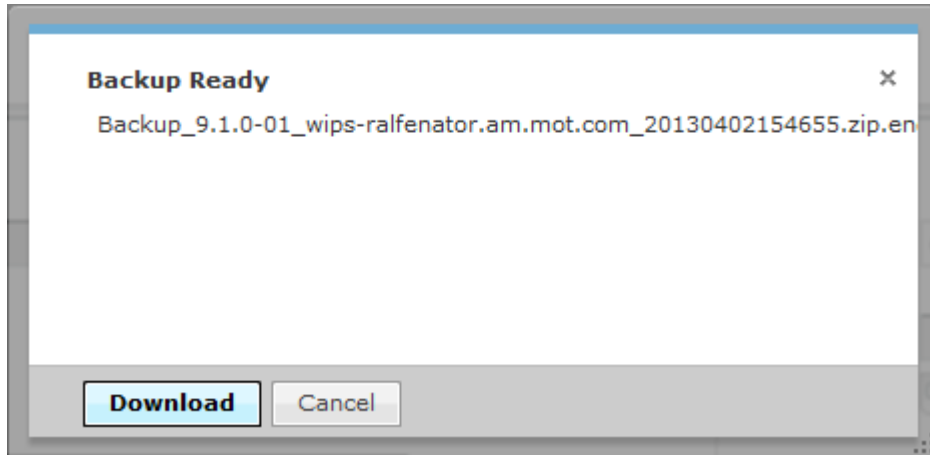
Backup Recommendations

- 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.

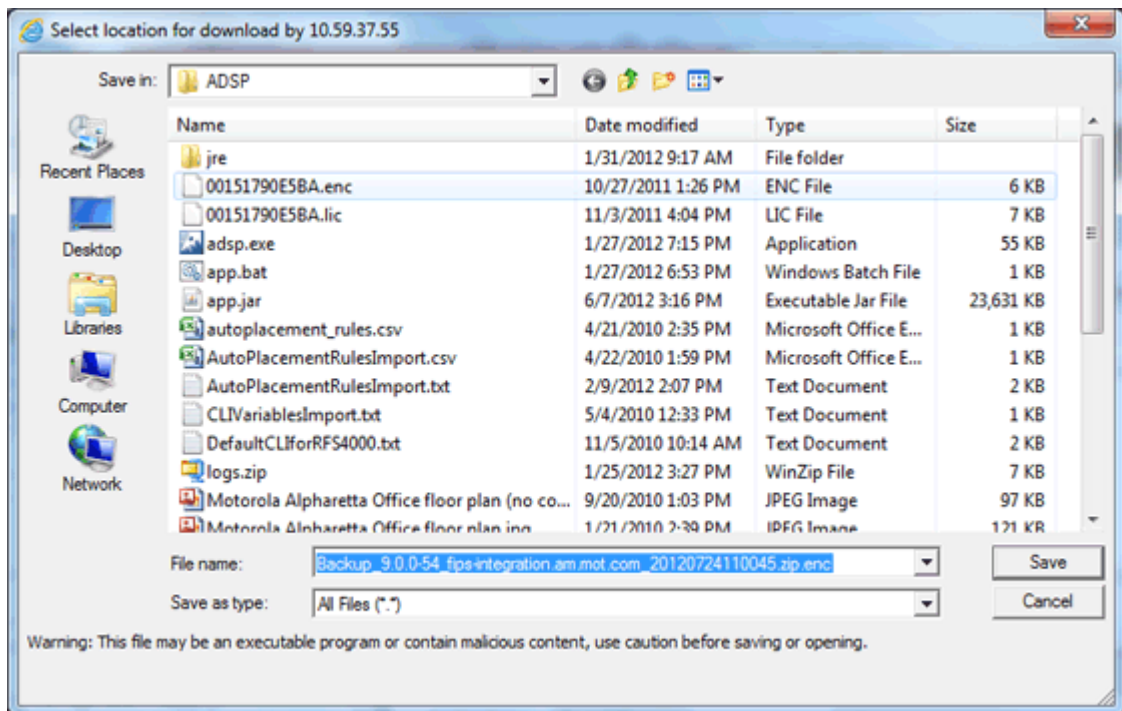
Manual Backups

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.



Note

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 in the **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.

5. Click the **Apply** button to set the automatic backup schedule.
6. During an automatic backup, you can 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).

Field	Description
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.

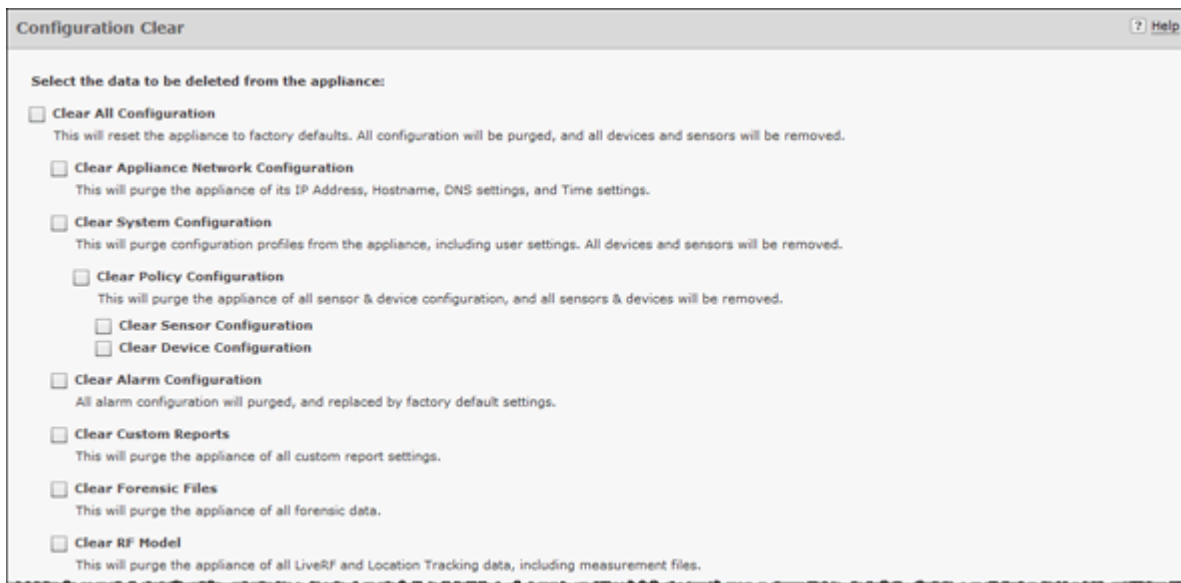
Configuration Clear

Use the Configuration Clear option to clear configuration data and set your appliance back to its default state when your system was first delivered.

You can either clear the complete configuration data and reset the system as it was first delivered or can clear specific configuration data.

The available options are:

1. Navigate to **Configuration > Appliance Management > Configuration Clear**.

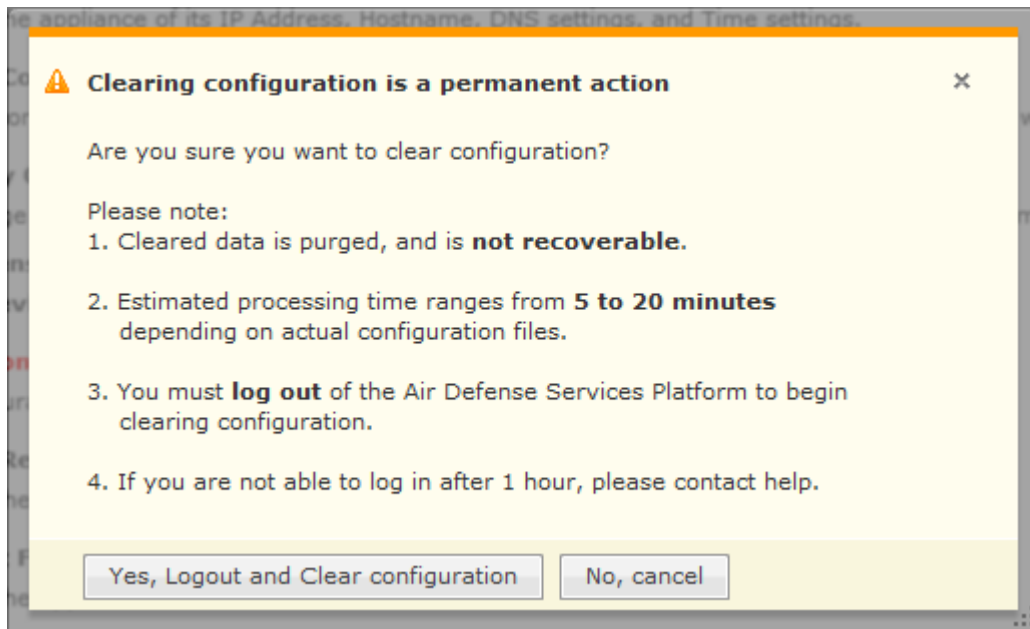


2. You can select from the following configuration options:

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.

Option	Description
Clear System Configuration	Clears all system configuration data. This encompasses everything except what is covered by the other options. There are three other options associated with this option. <ul style="list-style-type: none"> • 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.
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.

3. Select one or more options by placing a checkmark in the checkbox.
4. After selecting your options, click the **Next** button. A confirmation window is displayed.



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



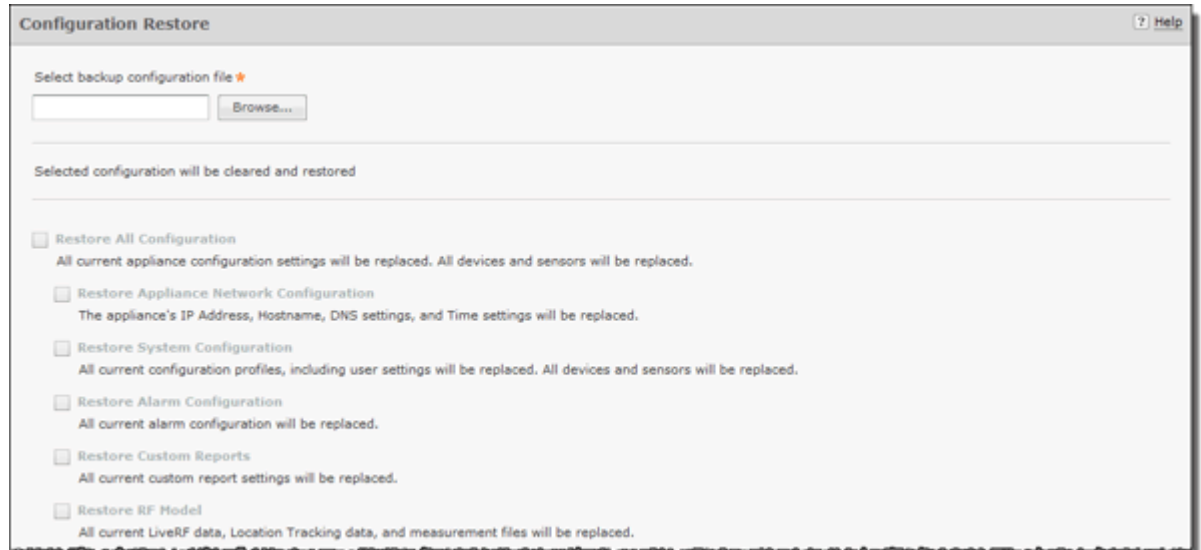
Note

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 AirDefense server.

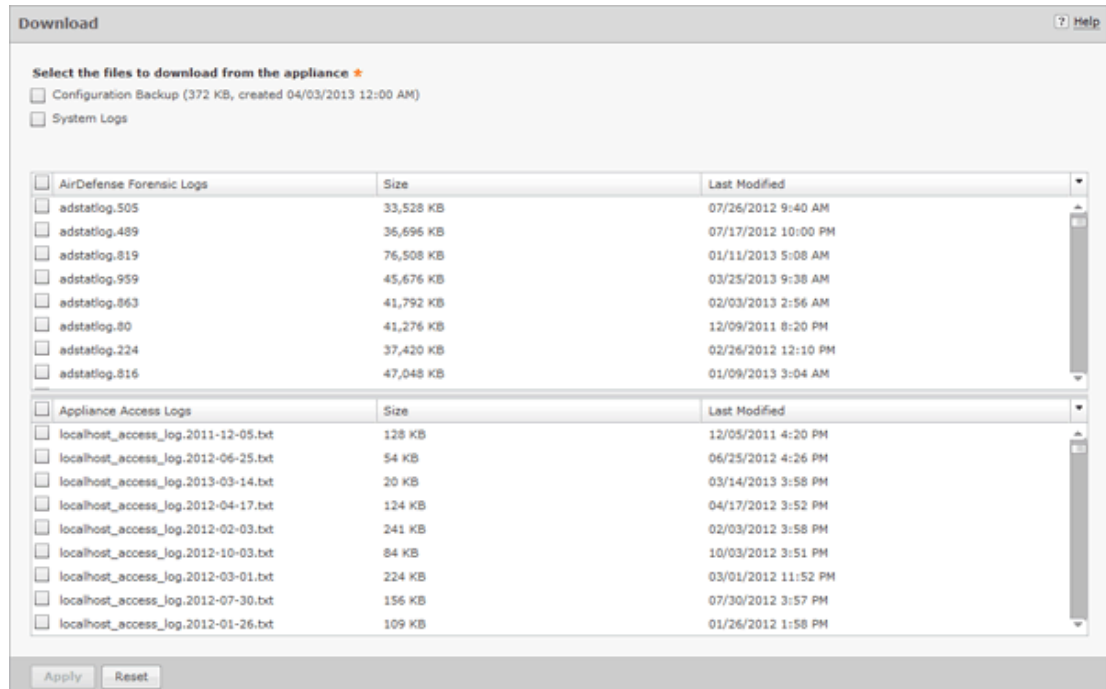
If you want to restore a configuration that was automatically backed up to your AirDefense server, you can download it to your workstation. (See [Download Logs](#).)

Download Logs

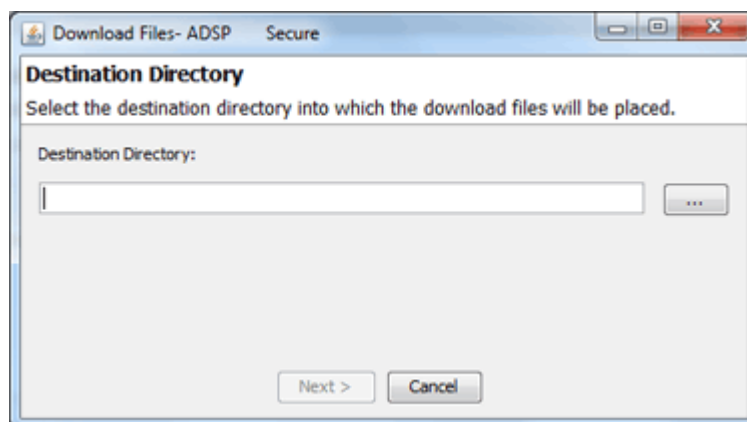
You can download configuration files that were automatically backed up to your ADSP server to your workstation. Once the backed up configuration is on your workstation, you can restore it. (See [Configuration Restore](#).)

To download a configuration, follow these steps:

1. Navigate to **Configuration > Appliance Management > Download Logs**.

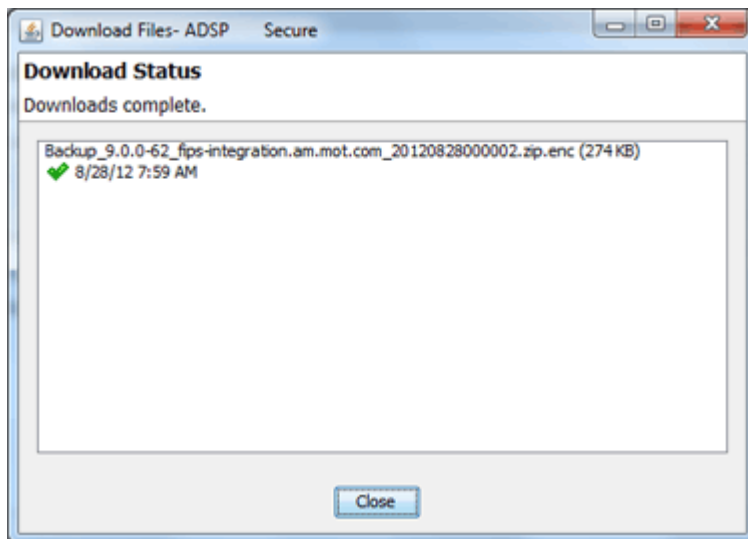


2. Select if you want to download a backup that exists on your appliance and/or the system logs.
3. You can download all forensic logs or all appliance access logs. Alternatively, you can pick and choose the forensic logs or appliance access logs that you want to download.
4. Click **Apply**. A destination 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

To enable 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.

You can automatically back up forensics data and log files by navigating to **Configuration > Appliance Management > Forensic and Log Backup**.

Forensic and Log Backup

Enable Automatic Forensics Backup

Host:

Port:

Protocol:

Path:

User:

Password: Display Password

Retries: (Max: 5)

Verify Server Certificate/Key

Enable Automatic Log Backup

Host:

Port:

Protocol:

Path:

User:

Password: Display Password

Retries: (Max: 5)

Verify Server Certificate/Key

Frequency:

Time:

Date:

Field	Description
Host	The name of the server where you want to back up forensics or log files. This can be an IP address or a DNS name defined by your DNS server.
Port	The port number to use during the backup.
Protocol	The file transfer protocol to use for backing up forensics or log files.
Path	The directory (folder) where to place the backup on the destination server.
User	The username used to log in on the destination server.
Password	The password used to log in on the destination server.
Verify Server Certificate/Key	Verifies that the server certificate (HTTPS connections) or server key (SCP and SFTP connections) is valid.
Retries	The number of times to retry the forensic backup if a failure occurs. The maximum number is 5.

You can schedule the backups for system and access logs. Select an interval and then fill in the related fields using the following table:

Interval	Action
One Time Schedule	Choose a time for the backup by selecting a time from the 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.

View Performance Statistics

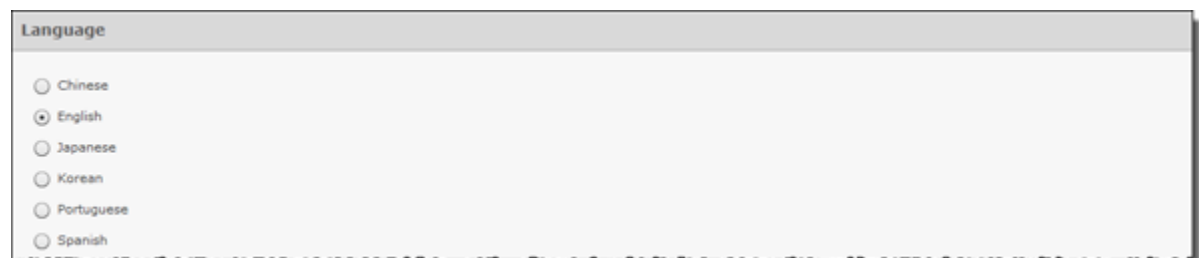
You can view AirDefense appliance performance statistics for the last day, the last week, or the last month.

In a web browser, go to one of the following locations, depending on whether you want to view daily, weekly, or monthly statistics:

- https://<AirDefense_ip_address>:8543/wireless/stats_day.html
- https://<AirDefense_ip_address>:8543/wireless/stats_week.html
- https://<AirDefense_ip_address>:8543/wireless/stats_month.html

Language

AirDefense 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](#)
- [Login Banner](#)
- [SSH Banner](#)

Pre-Login Banner

The **Pre-Login Banner** tab is provided for AirDefense deployments who wish to display their own customized banner before allowing users to log into AirDefense. You could use this banner to force user to accept "Terms and Conditions".



To activate, select **Enable Pre-Login Banner** checkbox.

The * **(Please enter text)** field is available to enter text that users will see before logging into AirDefense. Text can be entered in HTML or text format.

Click **Apply** to save the pre-login banner.

Login Banner

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

To activate, select **Enable Login Banner** field.

The following configuration options are available for customizing the Login Banner.

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 AirDefense users who wish to add their own customized text for users accessing the AirDefense appliance through SSH.



To activate, select **Enable SSH Banner** field.

The following configuration option is available for customizing the SSH Banner.

The **At initial login...** field is available to enter text that users will see when accessing the AirDefense appliance through SSH. Text can be entered in HTML or text format.

Click **Apply** to save the SSH banner.

Redundant Appliance Sync

AirDefense 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`.
- 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:



Note

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.

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.
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.

5. 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.

Structure Configuration

AirDefense requires you to create and maintain the hierarchy of sites and locations in your network for it to work as intended. This hierarchy, called the *Network Tree*, is a representation of how the sites are arranged within your network.

Your network tree can be arranged as:

- Country
- Region
- City
- Campus
- Building or Area
- Floor

In the above list, *Country* is the highest level in your hierarchy and *Floor* is the lowest.

The following image is of the **Structure Configuration** pane that displays your network tree.

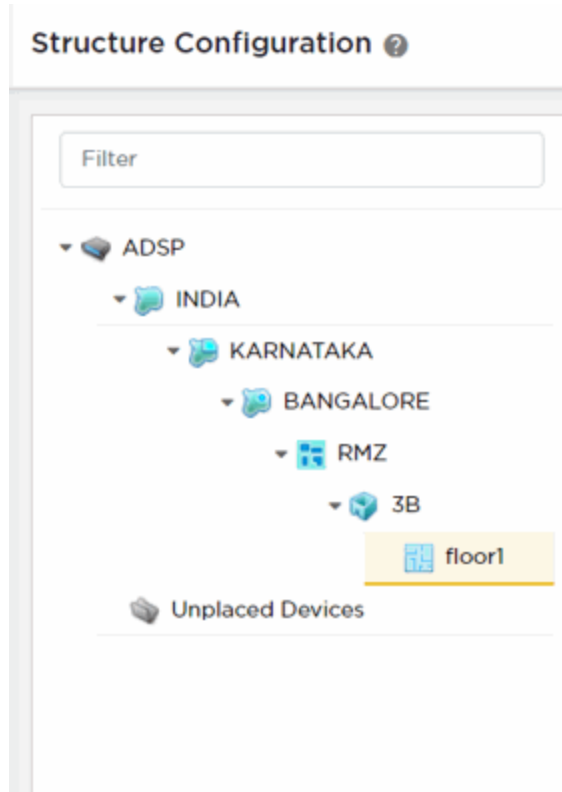



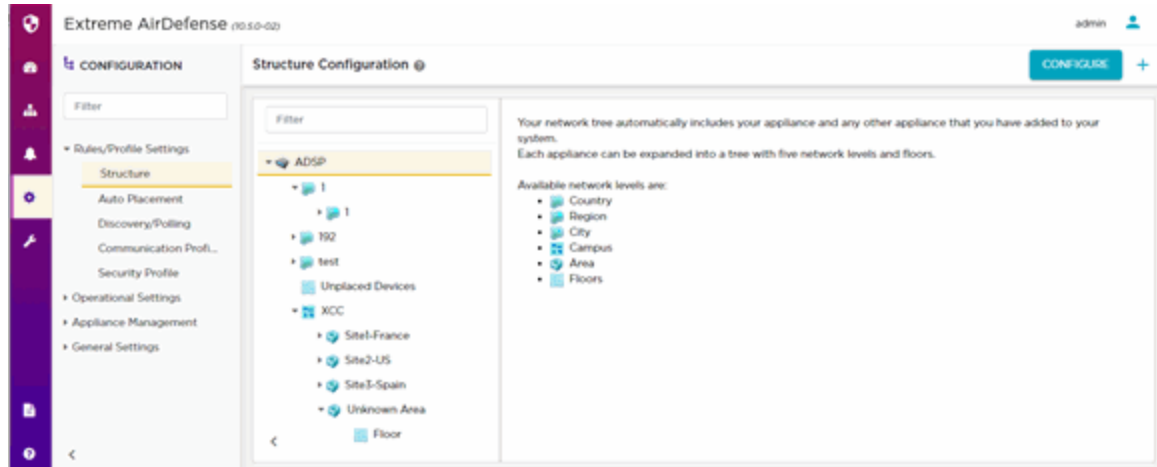
Figure 20: Network Tree


Your network tree automatically includes your appliance and any other appliance that you have added to your AirDefense system. Each appliance can be included into and then expanded within the hierarchy tree.

Deciding how to structure your network tree depends on the following decisions:

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

Launch the **Structure Configuration** screen from the  > **Structure** menu path. The following screen displays.



Use the  icon to regenerate your network structure.

Floor Plans

Extreme AirDefense has different options for assigning floor plans:

- **Configure floor plan in Extreme AirDefense**—You can create a detailed floor plan map from the **Structure Configuration** window. For details, see [Floor Plans](#) on page 155.
- **Import floor plan from Extreme IQ Controller**—If you have already configured your floor plan in ExtremeCloud IQ Controller, there is no need to create a floor plan in Extreme AirDefense. You can create a discovery profile in AirDefense that points to ExtremeCloud IQ Controller. During polling, AirDefense imports the floor plans, access points, and placements automatically. See [Add a Discovery Profile](#) on page 169 for information about how to configure a discovery profile.

Triangulation Considerations

To use triangulation, you must load AirDefense 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 (AirDefense) 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.

View And Manage Your Network Tree

You can view your network tree from the **Structure Configuration** panel wherever available.

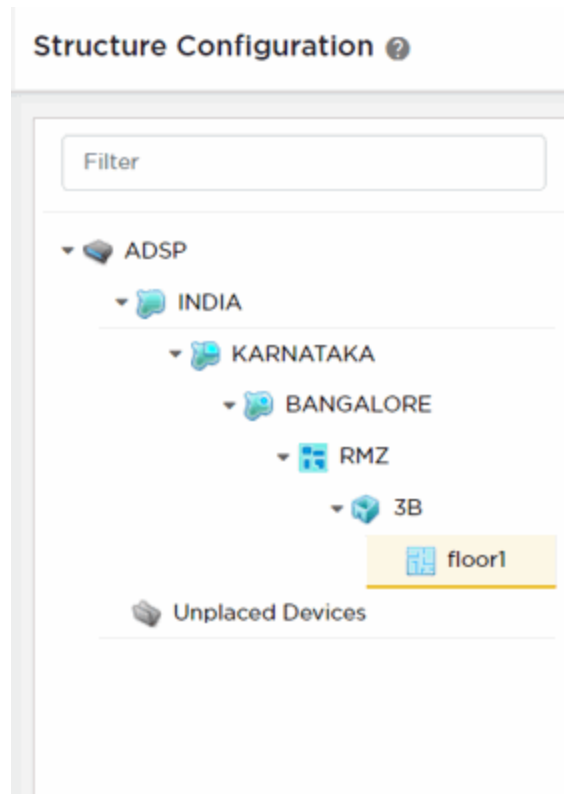
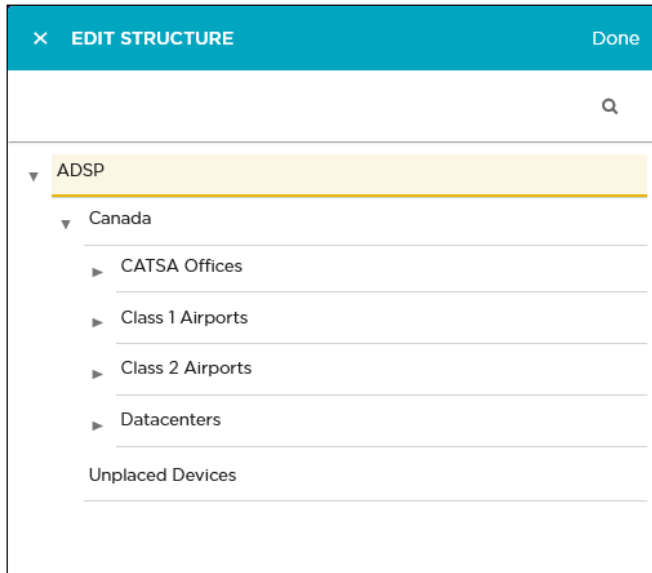


Figure 21: Structure Configuration Panel

Use the icons next to each node on the network tree to expand or contract it. The topmost node for the network tree is the *Appliance* node. The inner most node is the *Floor* node. You can create a detailed floor plan map from the Floor node (for details, see [Floor Plans](#) on page 155).

Use the **Filter** text area to filter the devices to view specific terms in the **Structure Configuration** pane.

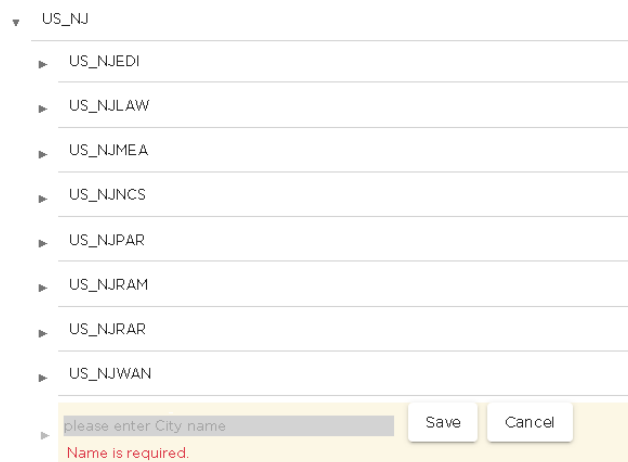
To edit the network tree, select the  icon located to the top left of the pane. The **Edit Structure** dialog displays.



Place your cursor over a node on this tree to view the actions that can be performed at that level. The following actions can be performed:

- Add a tree node as a next level node (sub-node) in the hierarchy. Use the **+** icon to add a node to the tree.


When you add a node, it is always added as a sub-node of the node where this action was performed. If the main node has sub-nodes, the new node is always added as the last sub-node.



- Edit the node. The only action that can be performed is renaming the node. Use the **✎** icon to edit the node.


The node name is edited in place. Use the **Save** button to save the edited node name. Use the **Cancel** button to retain the node's existing name.



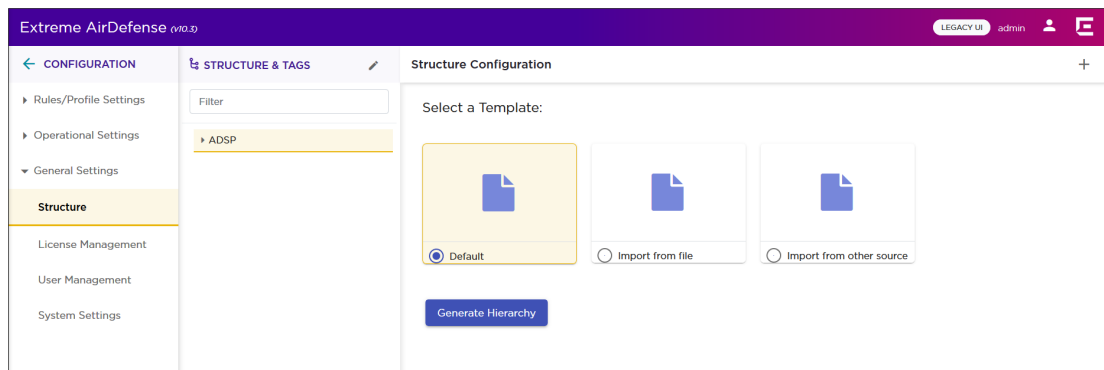
- Delete the node and if it has sub-nodes, then this command deletes the sub-nodes too. Use the  icon to delete the node. The node and its sub-nodes are immediately deleted.

Generate a Network Tree

Before you can use a new installation of AirDefense, you must define the network structure of the sites that the system must manage. On first use, you must generate the system's network tree.

1. Select the  icon located to the top right of the screen.

The **Structure Configuration** screen displays.

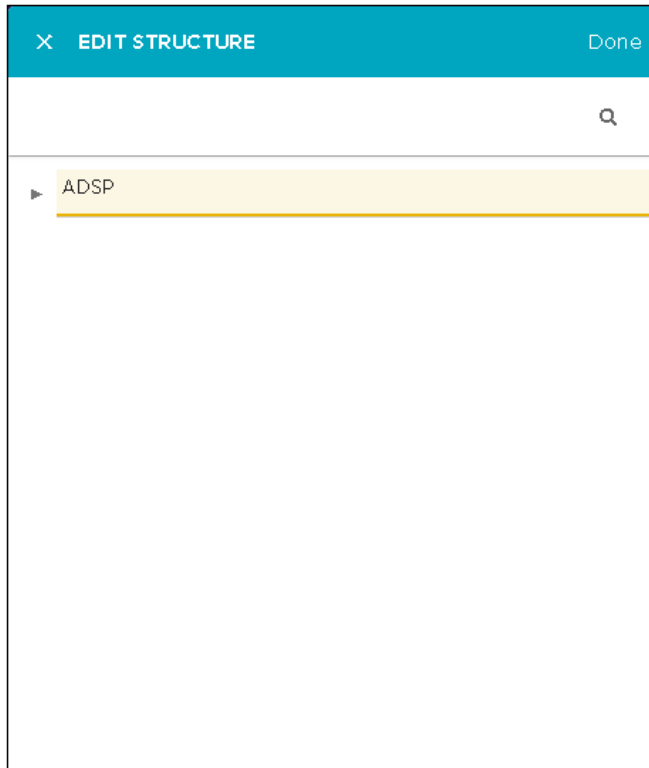


A blank network tree is generated from the **Structure Configuration** screen.

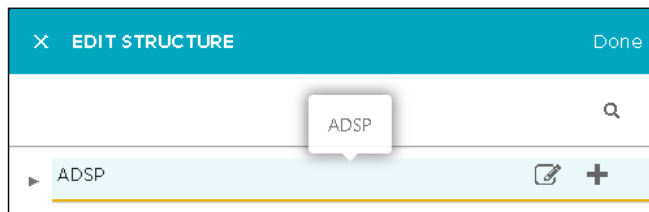
2. From the **Structure Configuration** screen, select the **Default** button.

3. Select the **Generate** button.

A blank network tree is created with the top level node named as *ADSP*.



4. Hover on this level to display the action buttons for this level.



5. Use the **+** icon to add a sub-node to this top level node.

The **Edit Structure** dialog displays.

For more information on viewing and managing nodes, see the topic [View And Manage Your Network Tree](#) on page 151.

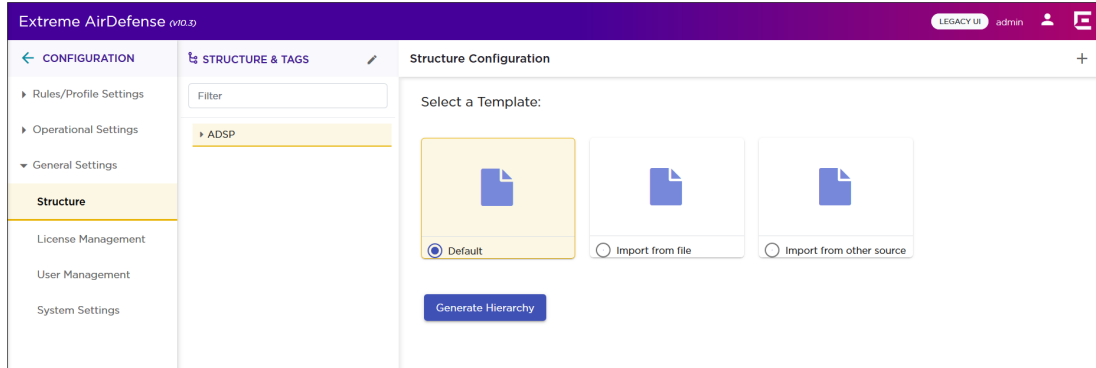
6. Once you have completed populating all the nodes in your network tree, select the **Done** button located on the top right of this dialog.

The **Edit Structure** dialog is closed and the **Structure Configuration** screen displays.

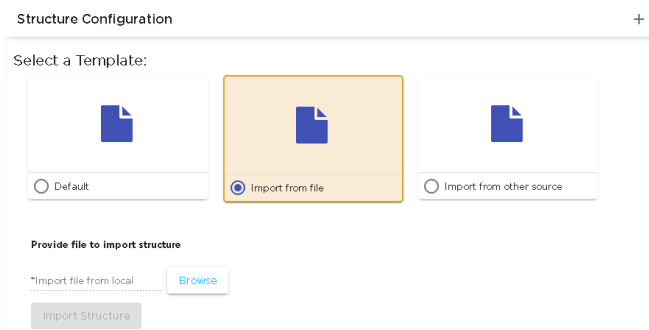
Import the Network Tree

AirDefense's network tree can also be imported from an external file.

You can import network tree from the **Structure Configuration** screen.



1. From the **Structure Configuration** screen, select the **Import from File** button. The screen changes to the following:

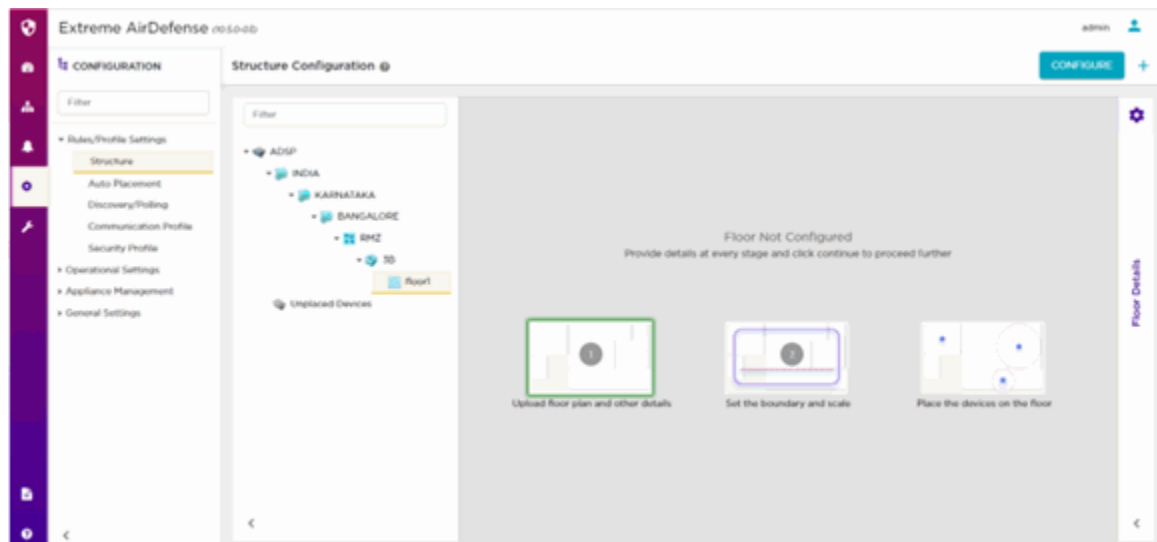


2. Select the **Browse** button to launch the operating system's **File Upload** window.
3. Use the operating system's file upload window and navigate to the location where your import file is located and select the appropriate button to upload your file. On successful import, the AirDefense network tree is updated.

Floor Plans

This task describes how to create a detailed floor plan of your network and devices.

You can create a detailed floor plan map of your network and devices from the **Structure Configuration** window:



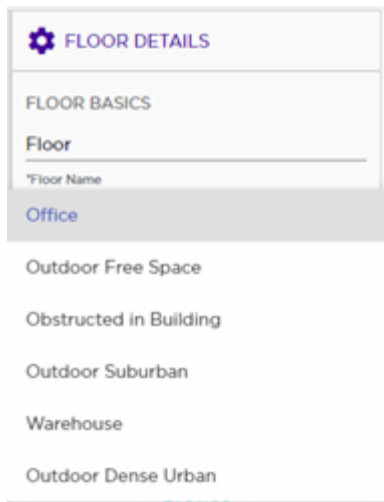
To map your floor plan:

1. From the **Structure Configuration** tree on the **Configuration** tab, select the Floor level.
2. To configure your floor plan, select the **Configure** button at the top right corner of the panel.

The **Floor Details** window displays.

- To select the type of environment that your floor plan represents, select the down arrow to expand the drop-down list:

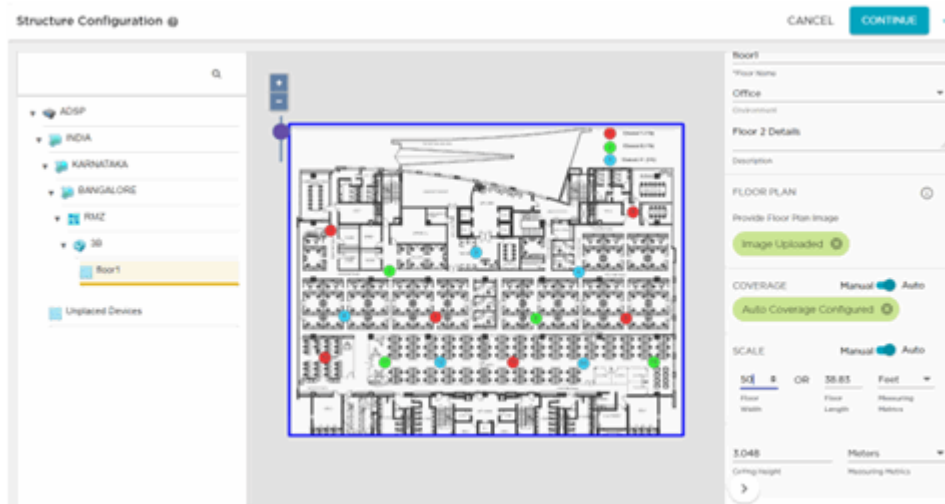
The **Environment** drop-down list displays.



- To upload an image of your floor plan, select the **Browse** button and choose the file to upload.



- Use the Coverage panel in the right-hand Floor Details window to set the boundaries for your floor plan map. Select **Auto** to configure the map using default coverage boundaries. Select **Manual** to configure the boundaries manually.



Note

If you select **Auto** to use the default coverage option, changes and variations in the proximity of your mapped devices may occur. Use the **Manual** option to set your coverage to prevent these issues.

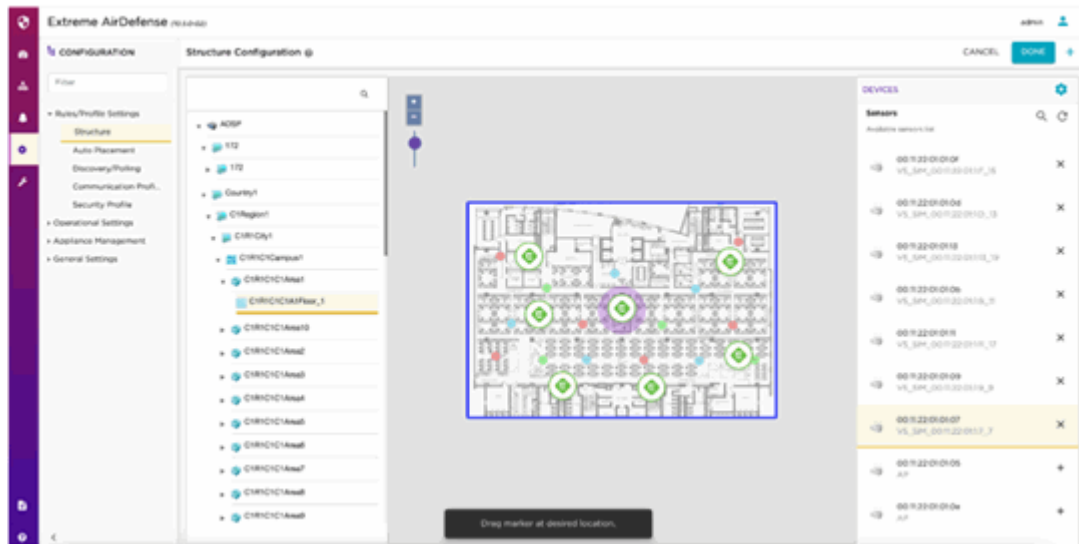
- Use the **Scale** panel in the right-hand Floor Details window to set the scale for your floor plan map. Select **Auto** to configure the map using default scaling. Select **Manual** to configure the scale manually.



Note

If you select **Auto** to use the default scale option, changes and variations in the proximity of your mapped elements may occur. Use the **Manual** option to set your scale to prevent these issues.

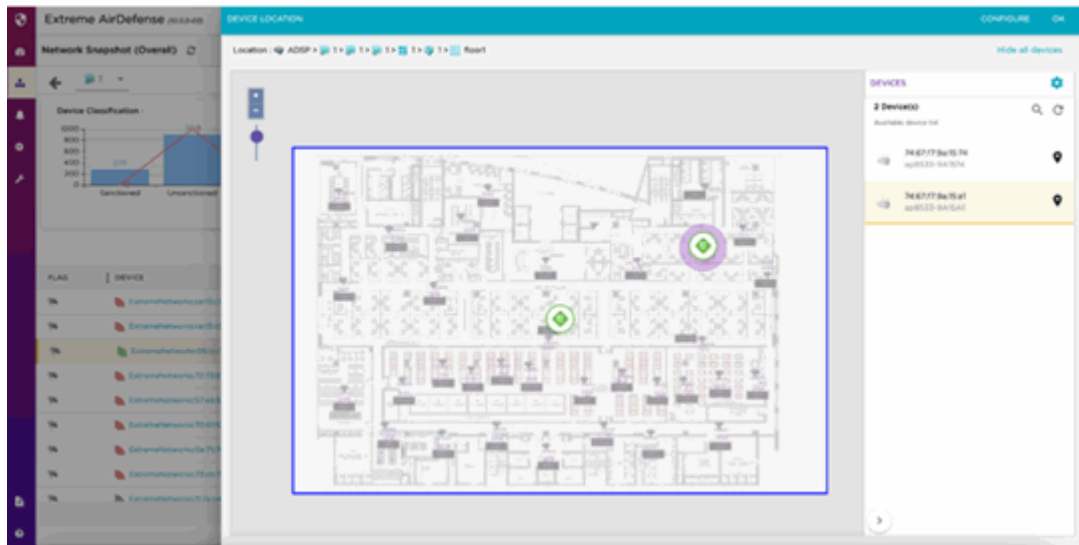
- To add a device to your floor plan map, select it from the right-hand list of devices and drag and drop it on the map.



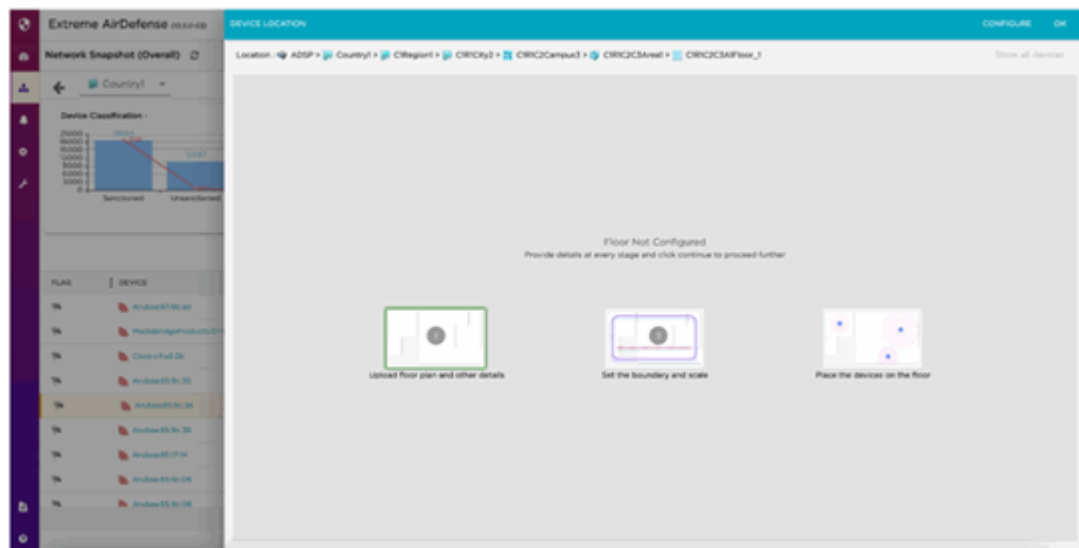
- To view Device Locations, navigate to the Network Snapshot tab and select any BSS, Wireless Client, or BT/BE device type. If the device type is configured for a floor plan, the Device Location window opens



9. Select Show All Devices to display all the the devices and APs:



10. If a floor plan is not configured, you can configure a floor plan from this window:



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 are applied differently based on the device type that are discovered in your network. The rules are different for sensors when compared to rules for access points and switches.

Auto-Placement Rules for 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.

Auto-Placement Rules for Access Points and Switches

Auto-Placement rules for APs and switches are applied when APs or switches are manually added or 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 access points 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 AirDefense.
 - The first IP address on the list is the Devices Management IP Address. This is the IP address that AirDefense 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 AirDefense 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 AirDefense for this purpose and is not saved by AirDefense. It is not used as a configured or managed IP address for the device, and it will not be displayed by AirDefense.
 - 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 AirDefense to communicate with the switch. It may NOT be the switch's configured IP address.

RULE NAME	DESTINATION
ST020	ADSP > Even > ST020 > Floor 1
ST022	ADSP > Even > ST022 > Floor 1
ST026	ADSP > Even > ST026 > Floor 1
ST030	ADSP > Even > ST030 > Floor 1
ST032	ADSP > Even > ST032 > Floor 1
ST034	ADSP > Even > ST034 > Floor 1
ST036	ADSP > Even > ST036 > Floor 1
ST042	ADSP > Even > ST042 > Floor 1
ST044	ADSP > Even > ST044 > Floor 1
ST046	ADSP > Even > ST046 > Floor 1
ST048	ADSP > Even > ST048 > Floor 1
ST050	ADSP > Even > ST050 > Floor 1

View Auto-Placement Rules

Use the **Auto-Placement Rules** screen to view a list of auto-placement rules configured for this AirDefense managed network. These rules determine where devices are placed in the network tree when they are imported into the network.

TOTAL RECORDS : 126		Search
RULE NAME	DESTINATION	
ST020	ADSP > EVEN STORES > ST020 > Floor 1	
ST022	ADSP > EVEN STORES > ST022 > Floor 1	
ST026	ADSP > EVEN STORES > ST026 > Floor 1	
ST030	ADSP > EVEN STORES > ST030 > Floor 1	
ST032	ADSP > EVEN STORES > ST032 > Floor 1	
ST034	ADSP > EVEN STORES > ST034 > Floor 1	
ST036	ADSP > EVEN STORES > ST036 > Floor 1	
ST042	ADSP > EVEN STORES > ST042 > Floor 1	

Figure 22: Auto-Placement Rules

The screen displays the following information:

Field	Description
Rule Name	This field displays the name of the auto-placement rule.
Destination	This field displays the destination configured for this rule. This is the location where a device that matches the auto-placement rule is placed in.
Action	The icons in this field enable you to view, edit or delete auto-placement rules. Use the icon to view the rule's configuration in a different dialog. Use the to delete the selected auto-placement rule. Similarly use to edit the auto-placement rule. For more information, see Edit an Auto-Placement Rule on page 165.

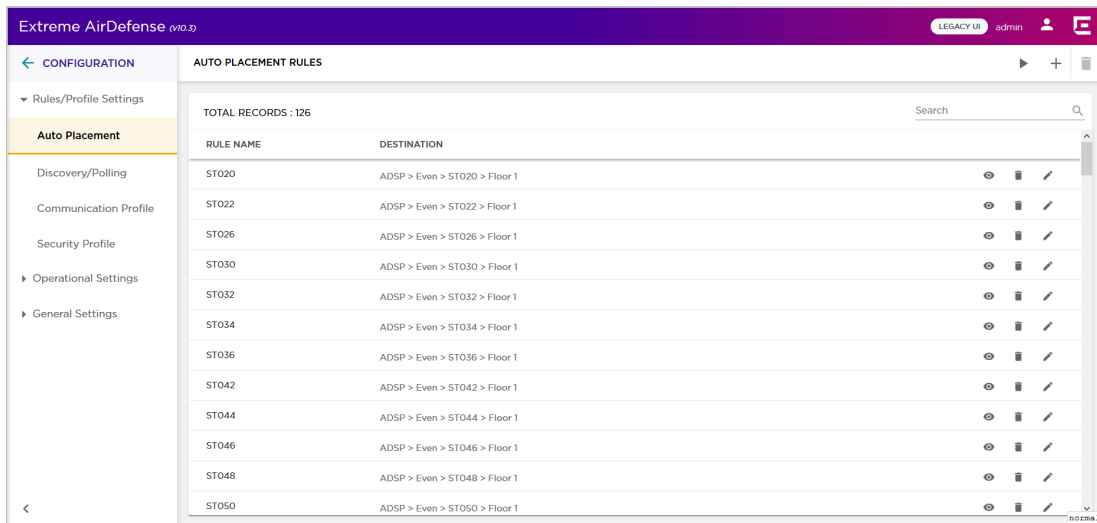
Use the area to search for a particular auto-placement rule.

The **Auto-Placement Rules** screen has a provision to manually run the auto-placement rules listed in this screen. By default AirDefense runs the auto-placement rules periodically. To force AirDefense to run the auto-placement rules on demand, select the icon located to the top right of this screen. When selected, all the rules configured in this screen are run immediately on the devices listed in the **Unplaced Devices** screen.

To add more auto-placement rules, use the icon located to the top right of this screen. For more information, see [Add an Auto-Placement Rule](#) on page 163.

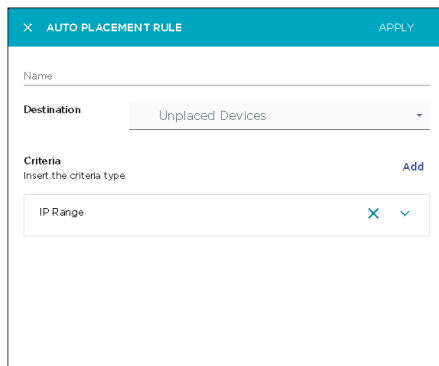
Add an Auto-Placement Rule

Auto-Placement rules configure where devices are placed when they are imported into the AirDefense managed network.

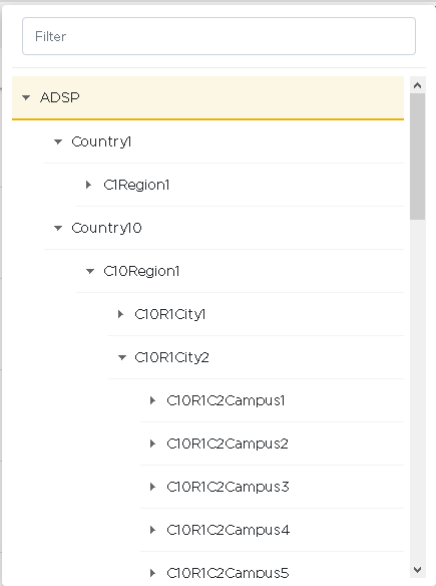


To add a new auto-placement rule:

1. From the **Auto-Placement Rules** screen, select the **+** icon. The **Auto Placement Rule** dialog displays.





2. Provide the following information to create a new auto-placement rule:

Field	Description
Name	Provide a meaningful name for the auto-placement rule. You should name your rules such that they are easy to identify from among similar rules.
Destination	<p>Use the Destination drop-down list to select the floor on which the devices meeting this auto-placement rule are to be placed.</p>  <p>Select the <i>Unplaced Devices</i> option from the drop-down list to indicate that the device is not placed. Unplaced devices appear in the Unplaced Devices tab of the Auto-Placement Rules screen.</p>
Criteria	<p>By default, a new rule has the following criteria selected:</p> <ul style="list-style-type: none"> • IP Range <p>Use this field to configure the range of IP address that is used as a selection criteria for this auto-placement rule.</p> <p>The following additional fields are available:</p> <ul style="list-style-type: none"> • MAC Address <p>Use this field to configure the device's MAC address that is used as a selection criteria for this auto-placement rule. You can configure a range of MAC addresses that is then used to place the devices. To use a single MAC address, enter the same address in both the Start MAC Address and End MAC Address fields.</p> <ul style="list-style-type: none"> • DHCP

Field	Description
	<p>Use this field to specify whether or not DHCP is used (True or False) as a selection criteria for this auto-placement rule. This parameter only works with sensors not with access points and switches.</p> <ul style="list-style-type: none"> • Network Address <p>Use the field to configure the device's network address that is used as a selection criteria for this auto-placement rule.</p> <ul style="list-style-type: none"> • DNS Server <p>Use this field to specify the DNS server or servers the devices are using and use that information as a selection criteria for this auto-placement rule. This parameter only works with sensors not with access points and switches.</p> <ul style="list-style-type: none"> • Device Name <p>Use this field to specify the device name that is used as a selection criteria for this auto-placement rule.</p> <ul style="list-style-type: none"> • Device Model <p>Use this field to specify the device model .This information is then used as a selection criteria for this auto-placement rule.</p> <ul style="list-style-type: none"> • Firmware <p>Use this field to specify the device's installed firmware version. This information is then used as a selection criteria for this auto-placement rule.</p> <ul style="list-style-type: none"> • Serial Number <p>Use this field to specify the device's unique serial number.This serial number is then used as a selection criteria for this auto-placement rule.</p>



Note

Select the  icon to expand each selection criteria. To delete a selection criteria, use the  icon.


3. Select the **Apply** button located to the top right of this dialog to save the auto-placement rule.
4. Select the small 'x' icon to the top left of the dialog to close it.

Edit an Auto-Placement Rule

Auto-Placement rules configure where devices are placed when they are imported into the AirDefense managed network.

RULE NAME	DESTINATION
ST020	ADSP > Even > ST020 > Floor 1
ST022	ADSP > Even > ST022 > Floor 1
ST026	ADSP > Even > ST026 > Floor 1
ST030	ADSP > Even > ST030 > Floor 1
ST032	ADSP > Even > ST032 > Floor 1
ST034	ADSP > Even > ST034 > Floor 1
ST036	ADSP > Even > ST036 > Floor 1
ST042	ADSP > Even > ST042 > Floor 1
ST044	ADSP > Even > ST044 > Floor 1
ST046	ADSP > Even > ST046 > Floor 1
ST048	ADSP > Even > ST048 > Floor 1
ST050	ADSP > Even > ST050 > Floor 1

To edit an existing auto-placement rule:

1. From the **Auto-Placement Rules** screen, select the auto-placement rule to edit.
2. Select the  icon to edit the selected auto-placement rule. The **Auto Placement Rule** dialog displays.

3. Modify the required fields.
For more information on the fields in this screen, see [Add an Auto-Placement Rule](#) on page 163.
4. Select the **Apply** button located to the top right of this dialog to save the auto-placement rule.
5. Select the small 'x' icon to the top left of the dialog to close it.

Discovery Profile and Polling Configuration

Use the **Discovery/Polling** configuration menu item to configure the following AirDefense parameters:

- **Discovery and Import** - Use this configuration option to configure how devices are imported or are discovered. For more information, see [Discovery Profile](#) on page 167
- **Polling** - Use this configuration option to set the various parameters for managing configuration audits, status polling, and data collections from a single window. For more information, see [Polling Configuration](#) on page 173

Use the **Configuration > Discovery/Polling** menu to launch the **Discovery Profiles** screen.

Discovery Profile

Discovery profiles are used to configure how devices are discovered or imported from various sources into the AirDefense managed network. Use the configurations in **Discovery/Polling** screen to set periodic imports and discovery of the devices into your network.

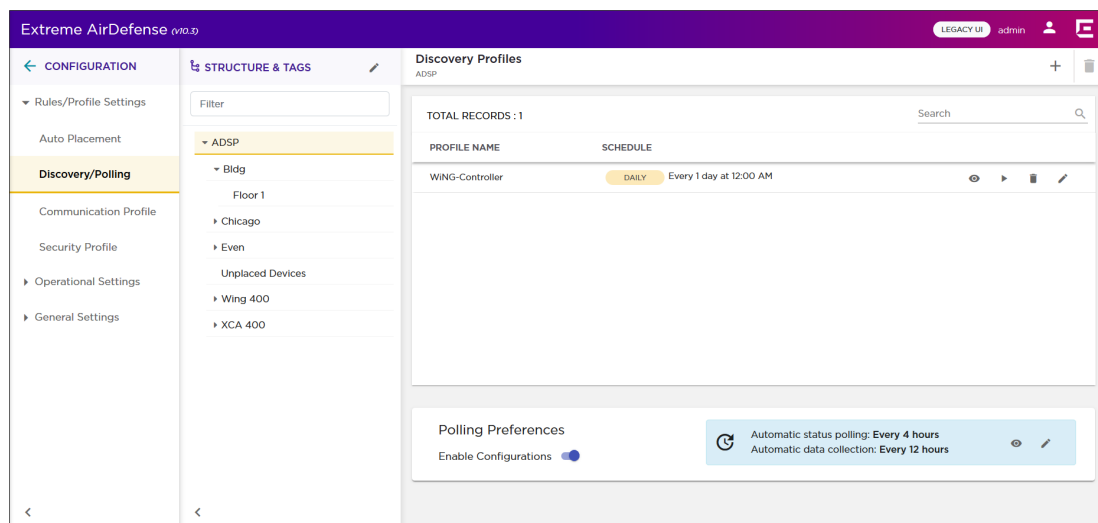
Devices can be imported or discovered from one of the following sources:

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

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

Discovery Profiles Screen

The **Discovery Profile** screen enables you to add and manage the profiles configured for your AirDefense system.



This screen is divided into the following sections:

- **Structure & Tags** - This section is used to set the scope of the *Polling Preferences* configuration. It is not used when configuring *Discovery Profiles*.
- **Discovery Profiles** - This section is used to add and manage your discovery profiles in the AirDefense system.

The **Discovery Profiles** area of the **Discovery/Polling** screen lists all the discovery profiles configured for your AirDefense system. Use the controls provided within this area to add and manage discovery profiles. You can add a new profile, modify or delete an existing profile. If required, you can also manually run a profile.

View Discovery Profiles

Use the **Discovery/Polling** screen to view a list of discovery profiles configured for this Extreme AirDefense managed network. These profiles determine how devices are discovered by Extreme AirDefense and how devices are imported into the system.

PROFILE NAME	SCHEDULE	JOB TYPE	ACTION
XIQ-Dev_polling	DAILY Weekdays at 12:00 AM	XIQ Import	View Run Delete Edit
XCA Import	DAILY Weekdays at 12:00 AM	XCA Import	View Run Delete Edit
x590 Switch	DAILY Weekdays at 12:00 AM	SNMP Discovery	View Run Delete Edit
XCA Import	INTRA DAY Every 5 hrs at 6:10 PM	XCA Import	View Run Delete Edit
remoteFile	DAILY Weekdays at 12:00 AM	Remote File	View Run Delete Edit
XCA RestAPI Import	DAILY Weekdays at 12:00 AM	XCA Import	View Run Delete Edit
XIQ-1	DAILY Weekdays at 12:00 AM	XIQ Import	View Run Delete Edit
XIQ Import	DAILY Weekdays at 12:00 AM	XIQ Import	View Run Delete Edit
WING-Controller	DAILY Every 1 day at 12:00 AM	SNMP Discovery	View Run Delete Edit

Figure 23: Discovery Profiles

The screen displays the following information:

Field	Description
Profile Name	The name of the discovery profile.
Schedule	The schedule for running this discovery profile.
Job Type	The method by which AirDefense is discovering or importing device information.
Action	The icons in this field enables you to edit, delete, run the discovery profile. Use the icon to view the details for this discovery profile in a separate dialog. Use the icon to run this discovery profile manually. Use the icon to delete the selected discovery profile. Similarly use the icon to edit the auto-placement rule.

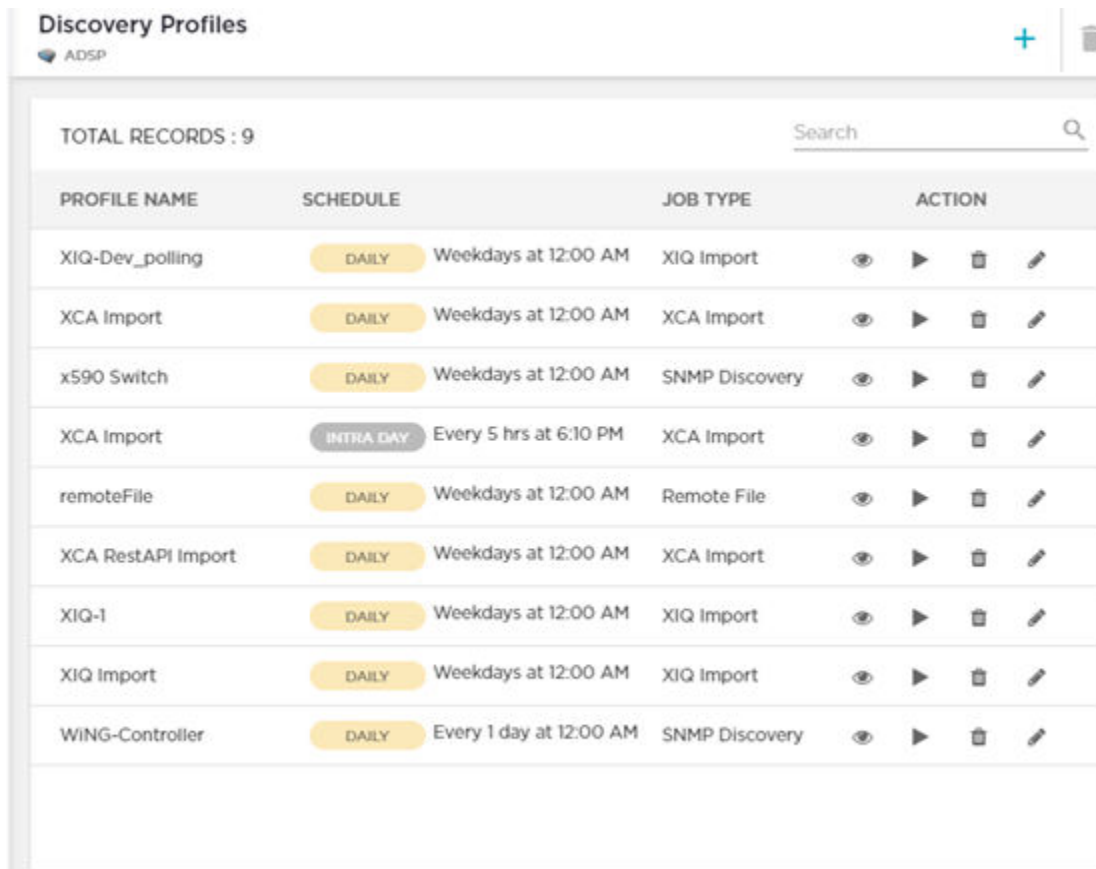
Use the area to search for a particular discovery profile.

The **Discovery Profiles** screen has a provision to manually run the profiles listed in this screen. By default Extreme AirDefense runs the discovery profile based on its schedule. To force Extreme AirDefense to run a discovery profile on demand, select the ▶ icon.

To add more discovery profiles, use the + icon located to the top right of this screen. For more information, see [Add a Discovery Profile](#) on page 169.

Add a Discovery Profile

Discovery profiles configure how devices are discovered or imported into the Extreme AirDefense managed network.



The screenshot shows the 'Discovery Profiles' interface. At the top, there is a header with 'Discovery Profiles' and 'ADSP' on the left, and a '+' icon and a trash icon on the right. Below the header, it says 'TOTAL RECORDS : 9' and has a search bar. The main content is a table with the following columns: PROFILE NAME, SCHEDULE, JOB TYPE, and ACTION. The table contains 9 rows of profiles.

PROFILE NAME	SCHEDULE	JOB TYPE	ACTION
XIQ-Dev_polling	DAILY Weekdays at 12:00 AM	XIQ Import	▶
XCA Import	DAILY Weekdays at 12:00 AM	XCA Import	▶
x590 Switch	DAILY Weekdays at 12:00 AM	SNMP Discovery	▶
XCA Import	INTRA DAY Every 5 hrs at 6:10 PM	XCA Import	▶
remoteFile	DAILY Weekdays at 12:00 AM	Remote File	▶
XCA RestAPI Import	DAILY Weekdays at 12:00 AM	XCA Import	▶
XIQ-1	DAILY Weekdays at 12:00 AM	XIQ Import	▶
XIQ Import	DAILY Weekdays at 12:00 AM	XIQ Import	▶
WING-Controller	DAILY Every 1 day at 12:00 AM	SNMP Discovery	▶

To add a new discovery profile:

1. From the **Discovery Profiles** screen, select the + icon. The **Discovery Profile** dialog displays.

2. In the **Discovery Profile Name** field, change the default value from *New Scheduled Import* to a name that describes this discovery profile.
3. Expand the **Job Type** field using the icon.
4. Select the method through which Extreme AirDefense imports device information:

Option

SNMP Discovery	Configure device imports through <i>SNMP Discovery</i> .
Local File	Import devices via a local file.
Remote File	Import devices via a remote file.
XCC Import	Import device information from Extreme AirDefense.
XIQ Import	Import device information from ExtremeCloud IQ.

From the **Network Criteria selection** drop-down list, select the criteria used to select the device.

Wild Card

Enter an IP address including a wild card. For example, 10.9.*.100.

Single IP

Enter a single IP address. For example, 192.168.12.23.

IP Range

Enter a range of IP addresses. For example, 192.168.10.10–192.168.10.35.

Network Address

Enter a Network Address. For example, 192.168.10.0/24.

FQDN

Enter a fully qualified domain name. For example, www.example.com.

Use the **Communication Profile** field to select an existing communication profile. From the drop-down list, you can select a existing communication profile, or you can create a new profile. You can also select the *Manual Entry* option from this list to create a communication profile that is unique to this SNMP host.



Note

A communication profile is a set of parameters that enables you to connect to a remote server. For more information on communication profiles, see [Communication Profile](#) on page 177.

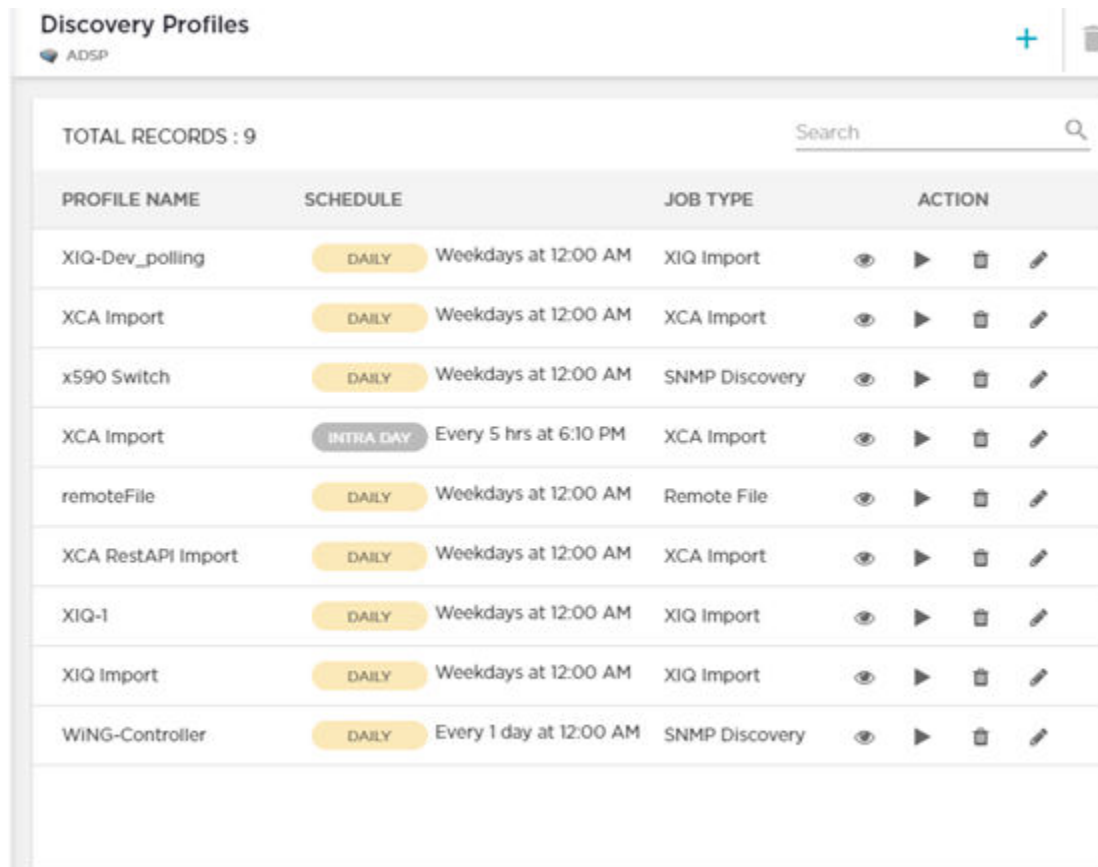
5. Use the **Schedule** field to schedule the frequency that discovery of the device occurs. Select **Daily**, **Monthly**, **One Time**, and **Intra-Day** (which is more than one time per day) from the drop-down list. You can also select the time that the device is discovered.
6. Use the **Placement Rules** field to configure the placement of the devices.
7. To configure device imports through a *Remote File*, select the **Remote File** button. Provide the following information:

Field	Description
Host	Provide the host name or IP address of the remote server where the import file is located.
Protocol	From the drop-down list, select the protocol to use when communicating with the remote host.
Path	Enter the full path to the import file on the remote host. The path must also include the full name of the import file. For example /home/localadmin/temp/importlist.list
User	Enter the username to be used when connecting to the remote host.
Password	Enter the correct password for the username entered in the User field.
Verify Server Certificate	Select this option to force Extreme AirDefense to verify the remote server's security certificate for validity.

8. Select the **APPLY** button located to the top right of this dialog to save the device discovery profile.
9. Select the small 'x' icon to the top left of the dialog to close it.


Edit a Discovery Profile

Discovery profiles configure how devices are discovered or imported into the AirDefense managed network.



PROFILE NAME	SCHEDULE	JOB TYPE	ACTION
XIQ-Dev_polling	DAILY Weekdays at 12:00 AM	XIQ Import	View Play Delete Edit
XCA Import	DAILY Weekdays at 12:00 AM	XCA Import	View Play Delete Edit
x590 Switch	DAILY Weekdays at 12:00 AM	SNMP Discovery	View Play Delete Edit
XCA Import	INTRA DAY Every 5 hrs at 6:10 PM	XCA Import	View Play Delete Edit
remoteFile	DAILY Weekdays at 12:00 AM	Remote File	View Play Delete Edit
XCA RestAPI Import	DAILY Weekdays at 12:00 AM	XCA Import	View Play Delete Edit
XIQ-1	DAILY Weekdays at 12:00 AM	XIQ Import	View Play Delete Edit
XIQ Import	DAILY Weekdays at 12:00 AM	XIQ Import	View Play Delete Edit
WING-Controller	DAILY Every 1 day at 12:00 AM	SNMP Discovery	View Play Delete Edit

To edit an existing discovery profile:

1. From the **Discovery Profiles** screen, select the discovery profile to edit.
2. Select the  icon to edit the select discovery profile.

The **Discovery Profile** dialog displays.

DISCOVERY PROFILE APPLY

*Discovery Profile Name
test

Job Type ^

Job Type
SNMP Discovery

Network Criteria * Wild Card *
Wild Card 192.168.*.100 X
e.g.: 192.168.*.100

Communication Profile *
Extreme WING 5.x Default

Extreme WING 5.x Default ✎

SNMP CONSOLE HTTP

Schedule v

DAILY Weekdays at 12:00 AM

Placement Rules v

Add to appliance: ADSP, Place devices in a single folder: ADSP > Old > 3 > Floor

Show all X

3. Modify the required fields.
For more information on the fields in this screen, see the topic [Add a Discovery Profile](#) on page 169.
4. Select the **APPLY** button located to the top right of this dialog to save the device discovery profile.
5. Select the small 'x' icon to the top left of the dialog to close it.

Polling Configuration


AirDefense uses a centralized polling feature to manage configuration audits, status polling, and data collections from a single location.

Polling preferences are configured from the **Discovery Profile** screen. Use the **Polling Preferences** area of the **Discovery Profiles** screen to configure your polling profiles.

PROFILE NAME	SCHEDULE	SCHEDULE	JOB TYPE	ACTION
XIQ-Dev_polling	DAILY	Weekdays at 12:00 AM	XIQ Import	View, Play, Delete, Edit
XCA Import	DAILY	Weekdays at 12:00 AM	XCA Import	View, Play, Delete, Edit
x590 Switch	DAILY	Weekdays at 12:00 AM	SNMP Discovery	View, Play, Delete, Edit
XCA Import	INTRA DAY	Every 5 hrs at 6:10 PM	XCA Import	View, Play, Delete, Edit
remoteFile	DAILY	Weekdays at 12:00 AM	Remote File	View, Play, Delete, Edit
XCA RestAPI Import	DAILY	Weekdays at 12:00 AM	XCA Import	View, Play, Delete, Edit
XIQ-1	DAILY	Weekdays at 12:00 AM	XIQ Import	View, Play, Delete, Edit
XIQ Import	DAILY	Weekdays at 12:00 AM	XIQ Import	View, Play, Delete, Edit
WING-Controller	DAILY	Every 1 day at 12:00 AM	SNMP Discovery	View, Play, Delete, Edit

You can configure different polling preferences for each node in your AirDefense hierarchy. To do so, you must select the correct node in the **Structure & Tags** area of the **Discovery Profiles** screen. After selecting the scope, you can apply the polling preferences to the scope.

View the current Polling Preference details

Use the  icon in this control to view the current polling preference values. This information is displayed in a separate window.

Basic Settings	
Automatic Status Polling	Enabled
Automatic Status Polling Frequency	4 Hours
Automatic Data Collection	Enabled
Automatic Data Collection Frequency	12 Hours
Extended Settings	
ACL	Disabled
Port Suppression	Disabled
Background Switch Port Scanning	Enabled
Device Configuration	Disabled

Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to *ON*. The top

most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from** : control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.


Edit Polling Preferences

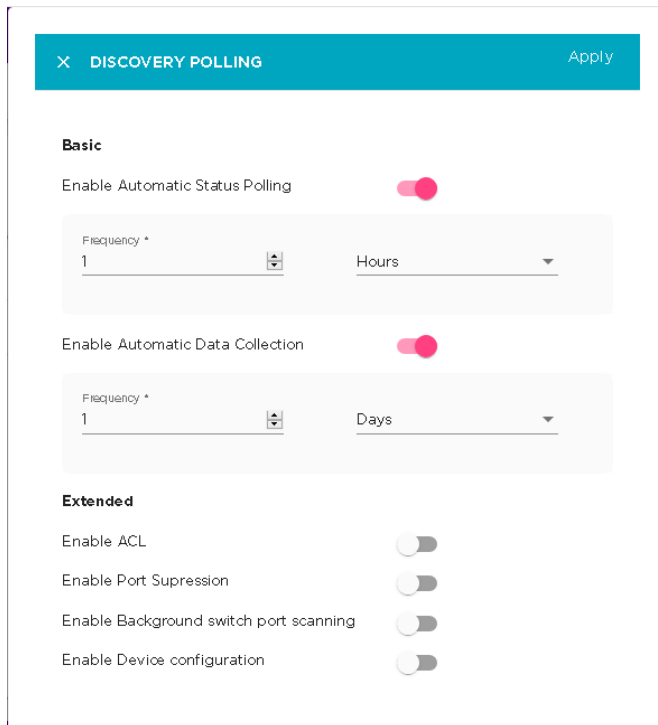
AirDefense uses a centralized location where you can configure polling preferences. These preferences are used to manage configuration audits, status polling, and data collections from a single location.

Polling Preferences

Select the **Enable Configurations** switch to toggle enabling polling preferences. The current configuration is displayed as under.



1. Use the **Structure & Tags** tree to select the scope for configuring polling preferences. It is possible to configure polling preference for each level of the AirDefense tree structure. However, it is recommended that you configure a polling preference for the top level of this tree. When configured, this preference is applied to every level in the AirDefense structure. You can then fine tune this configuration at each level of the tree.
2. Use the  icon to edit the current polling preference. The **Discovery Polling** dialog displays.



3. Select the **Enable Automatic Status Polling** switch to toggle it. When enabled, AirDefense automatically polls for device network status at an interval defined by the frequency values configured for this field.

Set the following frequency parameters for this field:

Field	Description
Frequency	Use the spinner control to set the duration value.
Frequency Format	Use the drop-down list to select the format for the frequency. Select from one of <i>Days, Hours, or Minutes</i> .

4. Select the **Enable Automatic Data Collection** switch to toggle it.

Each device model has an associated data collection profile which identifies the list of attributes collected from it. When this option is enabled, these SNMP attributes are collected from the devices at a frequency configured for this field.

Set the following frequency parameters for this field:

Field	Description
Frequency	Use the spinner control to set the duration value.
Frequency Format	Use the drop-down list to select the format for the frequency. Select from one of <i>Days, Hours, or Minutes</i> .

5. Set the following **Extended** parameters.

Field	Description
Enable ACL	When enabled, this parameter enables you to carry out the ACL action from the Device Action Manager or Alarm Action manager profile. This action would enable the Access Control List on switches that meet the conditions defined in the filter of Alarm Action Manager or Device Action Manager.
Enable Port Suppression	When enabled, this parameter enables you to carry out the Port Suppression action from the Device Action Manager or Alarm Action manager profile. This action is used to suppress communications between unauthorized devices and switches on your network.
Enable Background Switchport Scanning	When enabled, this parameter will allow generation of all alarms related to a switch.
Enable Device Configuration	When enabled, this parameter enables you to manually perform audit operations on the imported devices.

6. Select the **APPLY** button located to the top right of this dialog to save the polling preferences for the selected scope.
7. Select the small 'x' icon to the top left of the dialog to close it.
- Repeat the above steps for configuring polling preferences for a different scope by selecting it from the **Structure & Tags** pane.

Communication Profile

A *Communication Profile* is a set of configurations that enables you to use the same settings for connecting to various devices in your AirDefense managed network.

A communication profile consists of the following:

- SNMP Configuration - Use the settings under the **SNMP** tab to configure SNMP connection parameters.
- Console Configuration - Use the settings under the **Console** tab to configure console access parameters.
- HTTP Configuration - Use the settings under the **HTTP** tab to configure the parameters to access devices using HTTP protocol.

The main advantage of creating a communication profile is its capability to use the same credentials across multiple devices in the AirDefense managed network. This enables ease of configuration management and reduces its complexity.

You can create multiple communication profiles and apply them to individual sections of your AirDefense tree structure. However, it is suggested that you create a few global communication profiles and apply them for the whole system. You can then create new profiles that can be applied for various nodes in your structure. This provides a great amount of granularity of configuration across your AirDefense managed network.

Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to *ON*. The top most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

View Communication Profiles

Use the **Communication Profiles** screen to view a list of these profiles configured for your AirDefense managed network. A Communication Profile is a set of configurations that enables you to use the same settings for connecting to various devices in your AirDefense managed network.

A communication profile consists of configuration for the following:

- SNMP - Use the settings under this tab to configure SNMP connection parameters.
- Console - Use the settings under this tab to configure console access parameters.
- HTTP - Use the settings under this tab to configure the parameters to access using HTTP protocol.

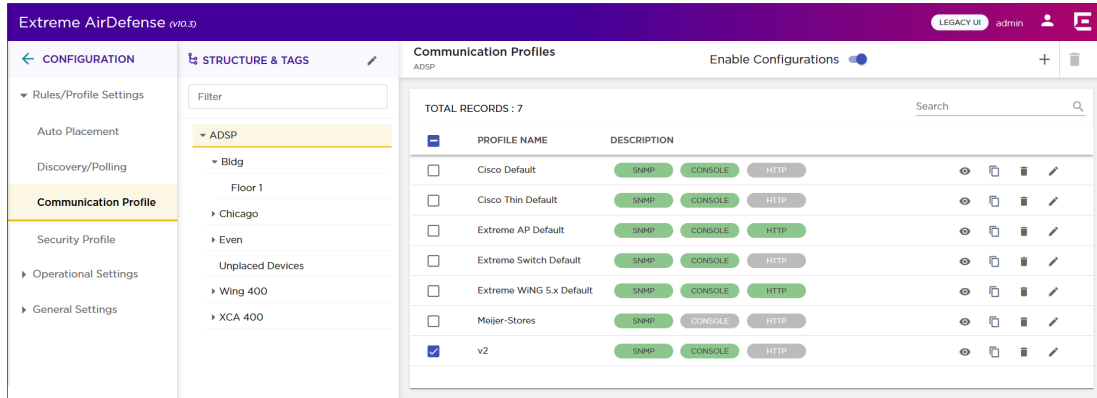






Figure 24: Communication Profiles

The screen displays the following information for each communication profile:

Field	Description
Profile Name	Displays the name of this communication profile.
Description	This field indicates which communication settings are active. An active setting is indicated in green and an inactive setting in grey.
Action	<p>The icons in this field enable you to manage your communication profiles. You can edit your profile, create a new profile by creating a duplicate of the profile, and delete the profile.</p> <p>The following actions can be performed:</p> <ul style="list-style-type: none"> • View Profile - Use the  icon to view the selected communication profile in a separate window. • Duplicate Profile - Use the  icon to create a duplicate of the selected profile. A new profile is created and the configuration dialog displays for the newly created communication profile. • Delete Profile - Use the  icon to delete the selected communication profile. • Edit Profile - Use the  to edit the communication profile. A configuration dialog displays where you can update the communication profile. For more information, see Edit the Communication Profile on page 184.

To apply one or more communication profiles to a particular scope (location), select the context from the **Structure & Tags** area. If permissions for this level are inherited from it's parent, change the Override Inherit from: ADSP control to **Override**. Select the check-box next to each selected communication profile to enable it for the selected scope (location). Click the **APPLY** button to apply the override for the selected context.

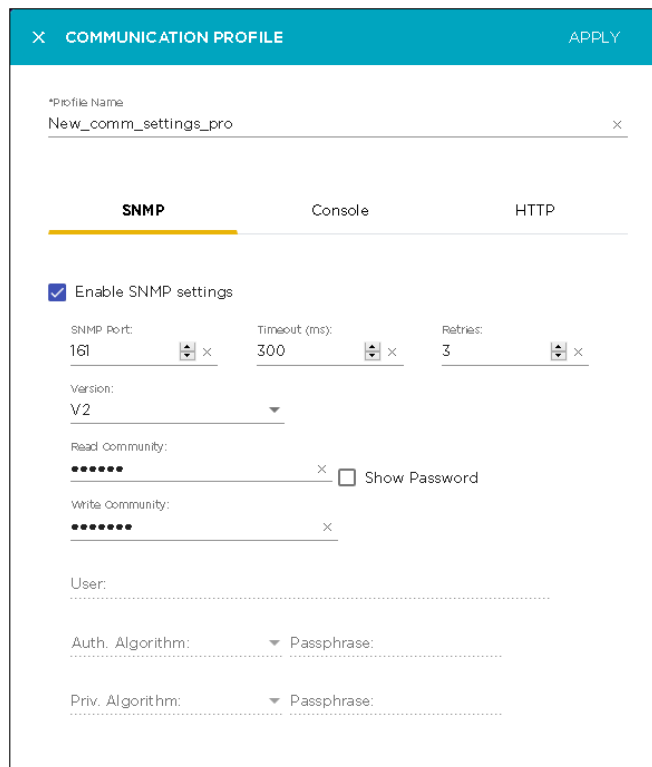
To add more communication profiles, use the **+** icon located to the top right of this screen. For more information see [Add a Communication Profile](#) on page 180.

Add a Communication Profile

A *Communication Profile* is a set of configurations that enables you to use the same settings for connecting to various devices in your AirDefense managed network.

To add a new communication profile:

1. From the **Communication Profile** screen, select the **+** icon.
The **Communication Profile** dialog displays.



The screenshot shows the 'COMMUNICATION PROFILE' dialog box with an 'APPLY' button in the top right corner. The 'Profile Name' field contains 'New_comm_settings_pro'. Below this are three tabs: 'SNMP' (selected and highlighted with a yellow underline), 'Console', and 'HTTP'. Under the 'SNMP' tab, there is a checked checkbox for 'Enable SNMP settings'. Below this are three input fields: 'SNMP Port' (161), 'Timeout (ms)' (300), and 'Retries' (3). A 'Version' dropdown menu is set to 'V2'. There are two password fields: 'Read Community' and 'Write Community', both masked with dots. A 'Show Password' checkbox is next to the 'Read Community' field. Below these are 'User:', 'Auth. Algorithm:', 'Passphrase:', 'Priv. Algorithm:', and 'Passphrase:' fields, all of which are currently empty.

By default, the **SNMP** configuration tab displays.

2. Provide a meaningful name for the communication profile. You should name your profiles such that they are easy to find among similar profiles.

3. Provide the following information for configuring SNMP settings:

Field	Description
Enable SNMP Settings	Select this switch to enable SNMP settings.
SNMP Port	Use the spinner to set the SNMP port for the device. The default port number is 161.
Timeout (in ms)	Use the spinner to set the timeout value in milliseconds to connect to the device.
Retries	Use the spinner to set the maximum number of retries that can be made while attempting to connect to the device.
Version	Use the drop-down to select the SNMP version number to use. AirDefense supports SNMP version 1 (V1), version 2 (V2), and version 3 (V3).
Read Community	Enter the Read Community string. This string is used for SNMP authentication. You also have an option to display passwords while typing them.
Write Community	Enter the Write Community string. This string is used for the SNMP authentication.
User	Enter the name of the SNMP V3 user. This user is configured on the switch for SNMP V3 access. Note: This field is only available when SNMP version is V3.

Field	Description
Auth. Algorithm	Use the drop-down list to select the authentication algorithm. This selection must match what is set on the device. The available algorithms are <i>MD5</i> , <i>SHA</i> , and <i>None</i> . You must supply a pass-phrase which must also match what is set on the device. Note: This field is only available when SNMP version is V3.
Priv. Algorithm	Use the drop-down list to select the privacy algorithm. This selection must match what is set on the device. The available algorithms are <i>DES</i> , <i>3DES</i> , <i>AES128</i> , <i>AES192</i> , <i>AES256</i> , and <i>none</i> . You must also supply a pass-phrase which must also match what is set on the device. Note: This field is only available when SNMP version is V3.

4. Select the **Console** tab to configure the settings for console access.

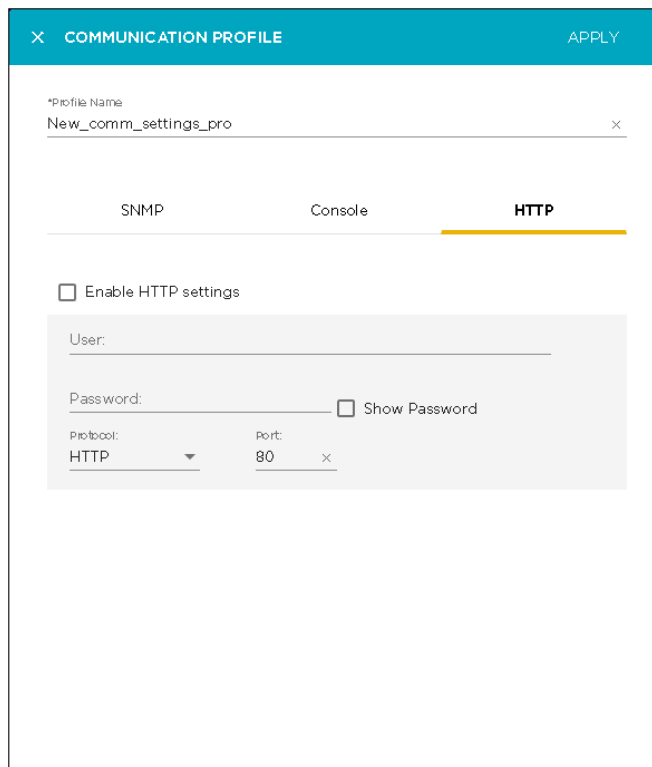
The screenshot shows the 'COMMUNICATION PROFILE' configuration interface. At the top, there is a teal header with 'X COMMUNICATION PROFILE' on the left and 'APPLY' on the right. Below the header, the 'Profile Name' is set to 'New_comm_settings_pro'. There are three tabs: 'SNMP', 'Console' (which is selected and highlighted with a yellow underline), and 'HTTP'. Under the 'Console' tab, there is a checkbox labeled 'Enable Console settings'. Below this, there is a 'User' field with the value 'admin'. A 'Password' field is shown with masked characters and a 'Show Password' checkbox. There is also an 'Enable Password' checkbox. At the bottom, there are 'Protocol' and 'Port' fields. The 'Protocol' is set to 'SSH' and the 'Port' is set to '22'.

Provide the following information:

Field	Description
Enable Console Settings	Select this switch to enable Console settings.
User	Use this field to enter the user name used to log in to the device.

Field	Description
Password	Use this field to enter the password for the above user name. Use the Show Password checkbox to view the password entered in this field.
Enable Password	Use this field to enter the <i>Enable</i> password. This password is required to enter the enable mode on the device.
Protocol	Use the drop-down list to select the protocol to use for console access. Select from <i>SSH</i> or <i>Telnet</i> .
Port	Use this field to enter the port number that is used for communications. By default port 22 is used used.

5. Select the **HTTP** button to configure the settings for devices that support configuration through a web user interface using HTTP.



Provide the following information:

Field	Description
Enable HTTP Settings	Select this switch to enable HTTP settings.
User	Use this field to enter the user name used to log in to the device.
Password	Use this field to enter the password for the above user name.

Field	Description
Protocol	Use the drop-down list to select the protocol to use for HTTP access. Select from <i>HTTP</i> or <i>HTTPS</i> .
Port	Use this field to enter the port number that is used for communications. By default port 80 is used used.

6. Select the **Apply** button located to the top right of this dialog to save the communication profile.
7. Select the small 'x' icon to the top left of the dialog to close it.

Edit the Communication Profile

Use the **Communication Profiles** screen to view a list of communication profiles configured for your AirDefense managed network. A Communication Profile is a set of configurations that enables you to use the same settings for connecting to various devices in your AirDefense managed network.

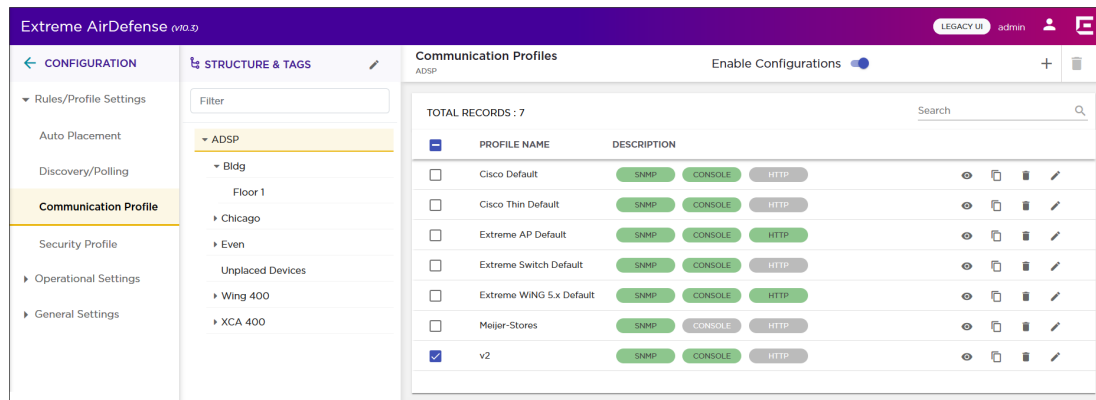

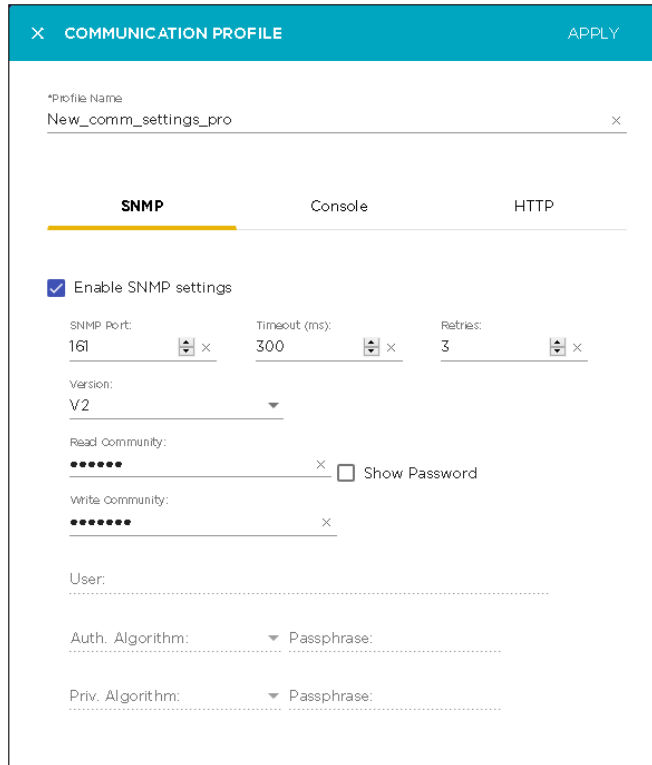


Figure 25: Communication Profiles

To edit a communication profile:


1. From the **Communication Profile** screen, select the communication profile to edit.
2. Select the  icon to edit the selected communication profile.
The **Communication Profile** dialog displays.

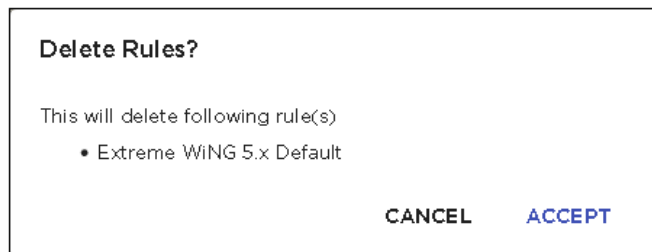


3. Modify the configuration settings for the different tabs in this dialog.
For more information on the fields in this dialog, see [Add a Communication Profile](#) on page 180
4. Select the **Apply** button located to the top right of this dialog to save the communication profile.
5. Select the small 'x' icon to the top left of the dialog to close it.

Delete Communication Profiles

To delete a communication profile:

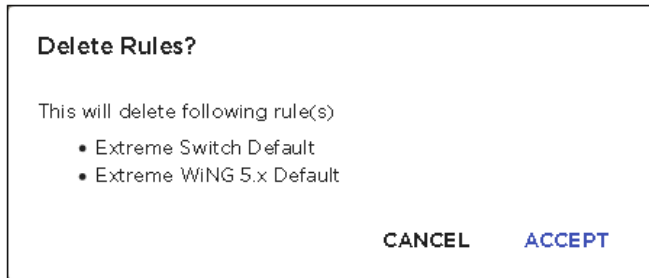
1. Select the  icon for the profile that you wish to delete.
The **Delete Rules** dialog displays.



2. Review the rule to delete.
3. Select **ACCEPT** button to delete the selected communication profile.
4. To delete multiple communication profiles, use the [CTRL]+Click key combination to select the profiles that you want to delete.

5. Select the  icon located to the top right of the screen to delete the selected communication profiles.

The **Delete Rule(s)** dialog displays.

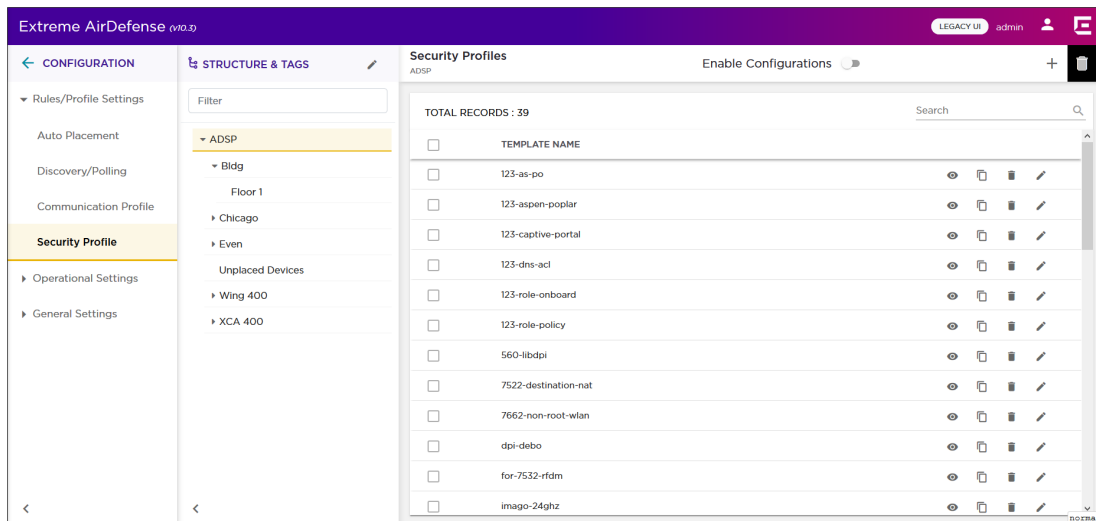


6. Review the communication profiles to delete.
7. Select **ACCEPT** button to delete the selected communication profile.

Security Profile

Security profiles are used to define the security configurations of the sanctioned wireless clients on your Extreme AirDefense managed wireless LANs. When a Security Profile is applied to your Extreme AirDefense system, and 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.

Security profiles are configured from the **Configuration > Security Profile** menu path. The **Security Profiles** screen displays. Existing security profiles are listed in the right pane of this window.



Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to **ON**. The top

most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

View Security Profile

Use the **Security Profile** screen to view a list of these profiles configured for you Extreme AirDefense managed system. A security profile is set of configurations that control how your alarms are generated.

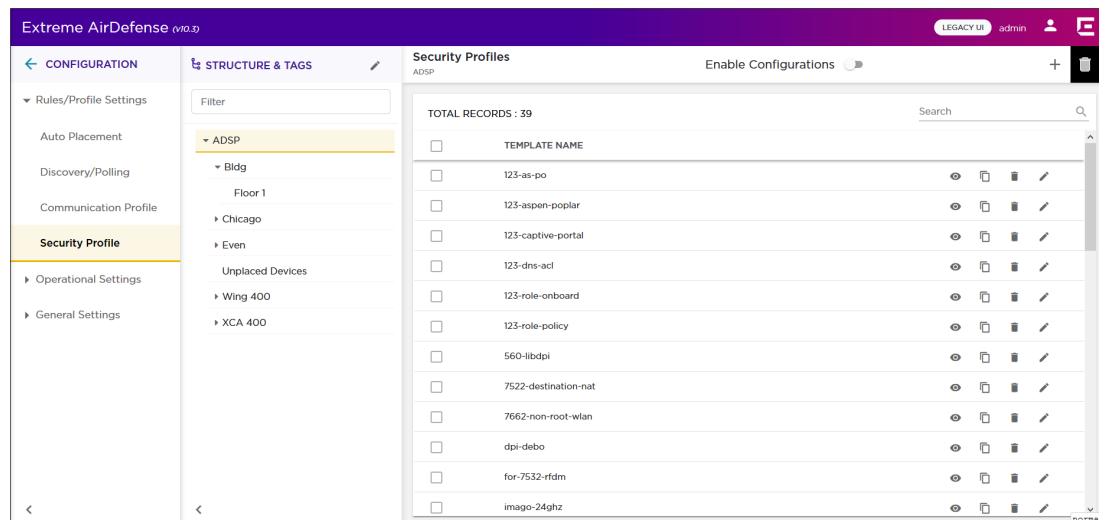







Figure 26: Security Profile Screen


The screen displays the following information:

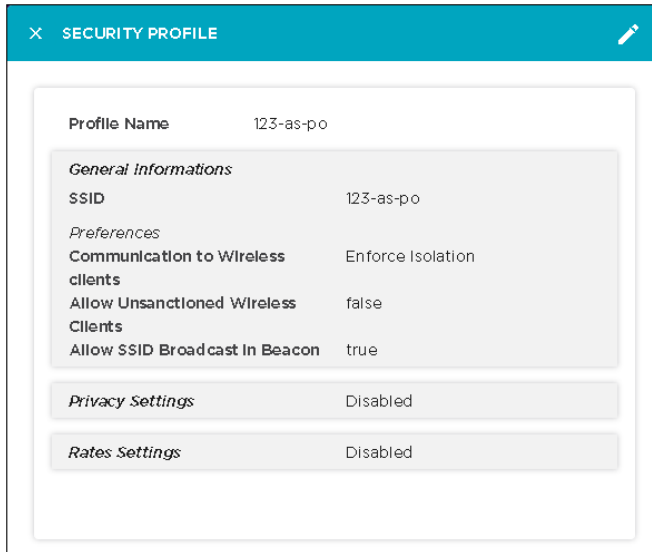
Field	Description
Template Name	The name of the security profile.
Action	<p>The actions that can be performed on the security profile. The icons in this field enable you to manage your security profile. You can edit your profile, create a new profile by creating a duplicate of the profile, or delete the profile.</p> <p>The following actions can be performed:</p> <ul style="list-style-type: none"> • View Profile - To view a security profile, use the  icon for the profile. The details for this profile is displayed in a separate dialog. • Duplicate Profile - Use the  icon to create a duplicate of the selected profile. A duplicate of this profile is created and the configuration dialog displays the newly created security profile. Customize the duplicate profile to meet your requirements. • Delete Profile - Use the  icon to delete the selected security profile. • Edit Profile - Use the  to edit the security profile. A configuration dialog displays where you can make changes to the selected security profile. For more information, see Edit a Security Profile on page 196.

To apply one or more security profiles to a particular scope (location), select the context from the **Structure & Tags** area. If permissions for this level are inherited from its parent, change the Override Inherit from: ADSP control to **Override**. Select the check-box next to each selected security profile to enable it for the selected scope (location). Click the **APPLY** button to apply the override for the selected context.

To add more security profiles, use the  icon located to the top right of this screen. For more information see [Add a Security Profile](#) on page 190.

View a Security Profile


Use the  icon for a security profile to view its details. A configuration dialog displays all the details about this security profile.



The following information is displayed for each security profile.

Field	Description
Profile Name	The name of this security profile.
General Information	<p>The General Information field displays the following information for this security profile.</p> <p>SSID The SSID that is covered by this security profile.</p> <p>Communication to Wireless clients The permissions set for enabling wireless clients to communicate with each other. Displays <i>Enforce Isolation</i> if the wireless clients are not allowed to communicate with each other.</p> <p>Allow Unsanctioned Wireless Clients The permission to allow unsanctioned Wireless Clients. Displays <i>false</i> if unsanctioned wireless clients are not allowed.</p> <p>Allow SSID Broadcast in Beacon The status of allowing SSID to be broadcast in the beacon. Displays <i>false</i> if SSID cannot be broadcast in the beacon.</p>

Field	Description
Privacy Settings	<p>The privacy setting configured for this security profile. When privacy settings are configured, this field displays <code>Enabled</code>. The following additional configuration information is also displayed.</p> <p>Base 802.11 Authentication The Base 802.11 authentication in use with this security profile. Displays <code>Open</code> or <code>Shared</code>.</p> <p>Extended 802.11 Authentication The Extended 802.11 authentication used with this security profile. Displays <code>WPA</code>, <code>WPA2</code>, or <code>Symbol KeyGuard</code>.</p> <p>Advanced Key Generation The key generation algorithm used with this security profile.</p> <p>802.11 Encryption The 802.11 encryption system used with this security profile.</p> <p>Other Encryption Other encryption schemes used with this security profile.</p>
Rate Settings	The configured rate settings used with this security profile. Selects the transmit and receive data rates for the BSSs to use.

Use the  icon located to the top right of this screen to edit the settings for the current security profile. For more information, see [Edit a Security Profile](#) on page 196

Add a Security Profile

A Security Profile is set of configurations that control how your alarms are generated. Use the **Security Profile** screen to view a list of these profiles configured for you Extreme AirDefense managed system.

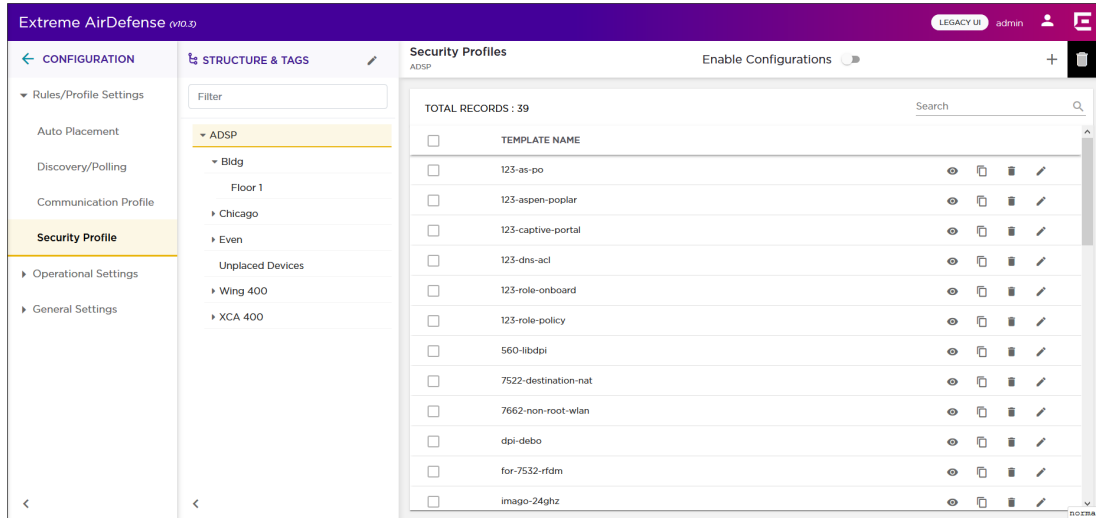


Figure 27: Security Profile Screen

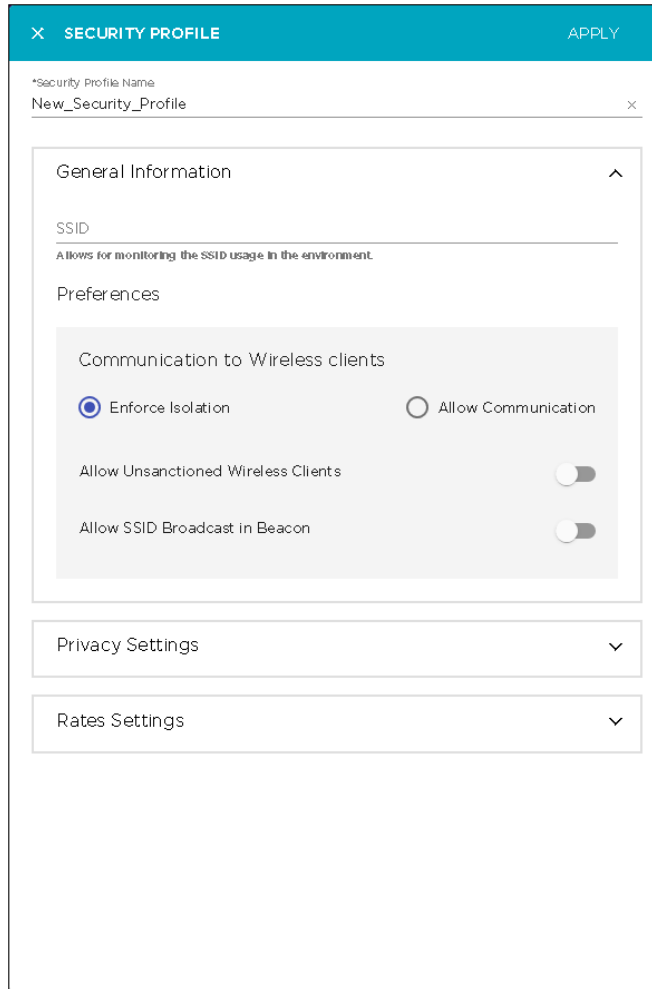
A complete security profile consists of the following configurations:


- General Configuration - This set of parameters configure settings related to wireless clients.
- Privacy Configuration - This set of parameters enable you to monitor privacy settings.
- Rate Settings - This set of parameters select the specific rates that you need to monitor.

The **Enable Configuration** switch must be set to ON for security profiles to be applied throughout your Extreme AirDefense monitored network. This setting is only available at the topmost level of your Extreme AirDefense network tree.

To add a new security profile:


1. From the **Security Profile** screen, select the **+** icon. This icon is located to the top right of this screen.
The **Security Profile** screen displays.



2. Select the  icon next to the **General Settings** field if the field is not expanded. In the **SSID** field, provide the SSID that the security profile applies to. This must be a valid SSID used in your Extreme AirDefense system.

Configure the following preferences for this security profile:


Field	Description
Communication to Wireless Clients	Select one of the following options: Enforce Isolation Select this option to isolate wireless clients within your network. Allow Communication Select this option to enable communications between wireless clients in your network.
Allow unsanctioned Wireless clients	Select this switch to allow or prevent unsanctioned wireless clients access to your system.
Allow SSID broadcast in Beacons	Select this switch to allow the BSS SSID to be broadcast in its beacon. SSIDs are not passwords. Many BSSs allow their SSIDs to broadcast by default.

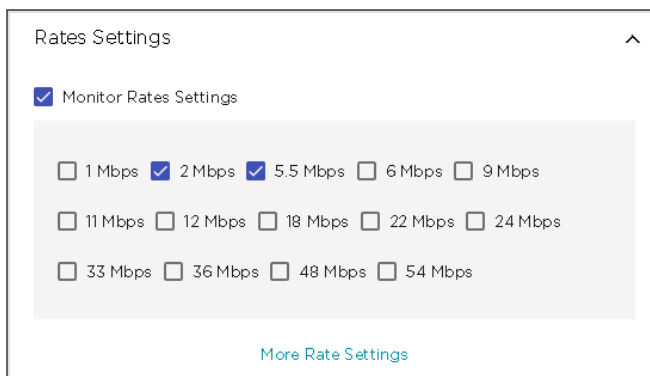
3. Expand the **Privacy Settings** field using the  icon if the field is not expanded. This field configures the settings related to transmission privacy.
4. Select the **Monitor Privacy Settings** option to enable this feature. Provide the following additional configuration information:

Field	Description
Extended 802.11 Authentication	<p>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.</p> <p>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.</p> <p>Symbol KeyGuard When this checkbox is selected, it activates Symbol KeyGuard authentication protocols, which is provided by Symbol Technologies.</p>
802.11 Encryption	<p>AES (CCMP) When selected, causes the BSS to advertise support for Advanced Encryption Standard (AES-CCMP).</p> <p>Unencrypted Allowed Select this checkbox to allow unencrypted wireless traffic.</p> <p>TKIP When selected, this enables the BSS to advertise support for Temporal Key Integrity Protocol (TKIP).</p>

Field	Description
Advanced Key Generation	<p>802.1x EAP-FAST When selected, it keys 802.1X EAP Flexible Authentication via Secure Tunneling.</p> <p>802.1x EAP-TLS When selected, it keys EAP Transport Level Security.</p> <p>802.1x EAP-TTLS When selected, it keys EAP Tunneled Transport Layer Security.</p> <p>802.1x EAP-GTC When selected, it keys EAP Generic Token Card.</p> <p>802.1x RSA/PKA When selected, it keys EAP RSA Public Key Authentication Protocol.</p> <p>802.1x RSA/SID When selected, it keys EAP RSA SecurID.</p> <p>802.1x PEAP When selected, it keys any 802.1X Protected Extensible Authentication Protocol (PEAP).</p> <p>802.1x LEAP When selected, it keys EAP Lightweight Extensible Authentication Protocol.</p> <p>802.1x Other EAP Keys any 802.1x EAP authentication/key distribution mechanism other than the types previously mentioned.</p> <p>PSK (preshared key) When selected, it activates the Pre-shared Key authentication.</p>

Field	Description
Base 802.11 Authentication	<p>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 controller).</p> <p>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 controller over a secure channel that is independent of 802.11. In practice, the shared key authentication secret is manually distributed and typed.</p>
Other Encryption	<p>AirFortress When selected enables AP usage of Layer 3 AirFortress encryption.</p> <p>Other Ethertypes allowed When selected, enables AP usage of other Layer 3 encryption mechanism which is not specified within this list.</p> <p>Cranite When selected, enables AP usage of Layer 3 Cranite encryption.</p> <p>IP-Sec When selected, enables AP usage of Layer 3 IP security protocol as encryption.</p>

- Expand the **Rate Settings** field using the  icon if the field is not expanded. This field configures the transmit and receive data rates for BSSs to use.
- Select the **Monitor Rate Settings** field to enable it. The field expands to display a set of default rates.



From the list of rates, select the ones that you want to apply.

Select the **More Rate Settings** button to expand this list to include more rates that you can apply.

More Rate Setting

1SS 2SS 3SS 4SS

> 20Mhz,1

6.5 - 7.2 Mbps 13 - 21.7 Mbps 26 - 43.3 Mbps

52 - 72.2 Mbps 78 - 86 Mbps

> 40Mhz,1

13.5-15 Mbps 27 - 45 Mbps 54 - 90 Mbps

108 - 150 Mbps 162 - 200 Mbps

> 80Mhz,1

29-32 Mbps 58 - 97 Mbps 117 - 195 Mbps

234 - 325 Mbps 351 - 433 Mbps

Select the rates that you want to apply to this security profile.

7. Select the **APPLY** button located to the top right of this dialog to save the security profile.

The new security profile is added to the list of active profiles for this Extreme AirDefense monitored networks.

8. Select the small **X** icon located to the top left of the dialog to close it. Your changes will not be saved when you use this method to close the dialog.

Edit a Security Profile

Use the **Security Profile** screen to view a list of these profiles configured for you AirDefense managed system. A Security Profile is set of configurations that control how your alarms are generated.

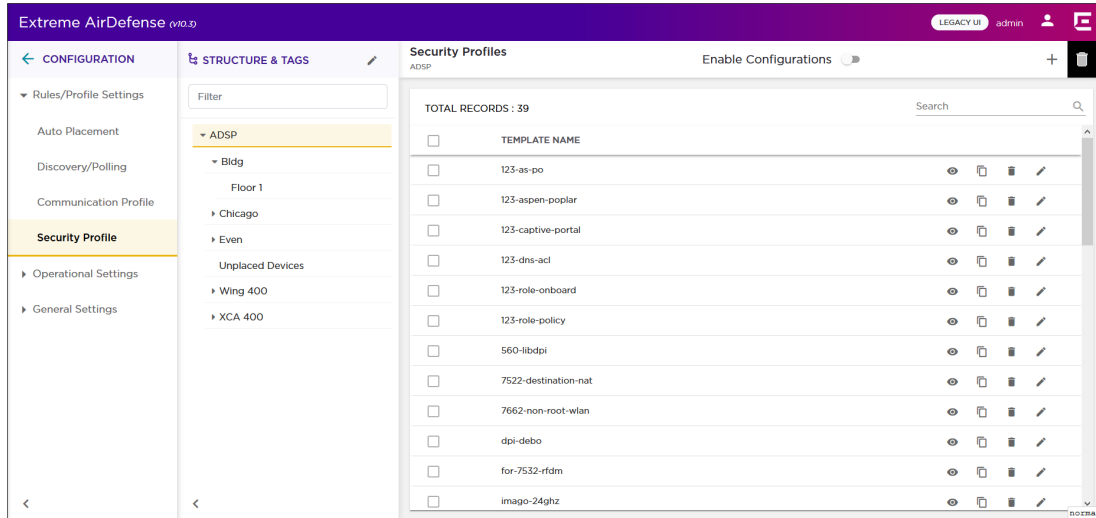



Figure 28: Security Profile Screen

A complete security profile consists of the following configurations:

- General Configuration - This set of parameters configure settings related to wireless clients.
- Privacy Configuration - This set of parameters configure enable you to monitor privacy settings.
- Rate Settings - This set of parameters configure the specific rates that you need to monitor.

To edit an existing security profile:

1. From the **Security Profile** screen, select the  icon for the security profile that you wish to edit.
The **Security Security Profile** dialog displays.

X SECURITY PROFILE **APPLY**

*Security Profile Name
New_Security_Profile

General Information ^

SSID
Allows for monitoring the SSID usage in the environment.

Preferences

Communication to Wireless clients

Enforce Isolation Allow Communication

Allow Unsanctioned Wireless Clients

Allow SSID Broadcast in Beacon

Privacy Settings v

Rates Settings v


2. Modify the required fields.

For more information on the fields of this dialog, see [Add a Security Profile](#) on page 190


3. Select the **APPLY** button located to the top right of this dialog to save the security profile.
4. Select the small 'x' icon to the top left of the dialog to close it.

Delete a Security Profile

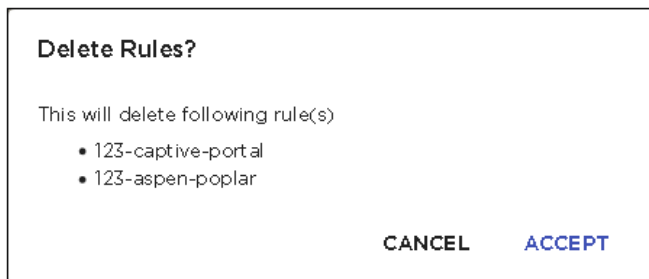
To delete a security profile:

1. Select the  icon for the profile that you wish to delete.
The **Delete Rule** dialog displays.



2. Review the rule to delete.
3. Select **ACCEPT** button to delete the selected rule.
4. To delete multiple security profiles, use the [CTRL]+Click key combination to select the profiles that you want to delete.
5. Select the  located to the top right of the screen to delete the selected security profiles.

The **Delete Rule(s)** dialog displays.



6. Review the rules to delete.
7. Select **ACCEPT** button to delete the selected rules.

Alarm Action Manager

Alarm Action Manager enables you to automatically respond to alarms in your Extreme AirDefense managed network with predetermined actions configured using alarm rules. Automating your response to the alarms enables you to focus on other critical administrative tasks.

An Alarm Action Manager rule set consists of lists of Alarms, Filters, and Actions. The list of Alarms contains those alarms for which you need to take specific action. The list of Filters contain a set of conditions that filters for a specific sub-set of alarms from those raised. The list of Actions contains the actions that will be automatically taken for these alarms.

An Alarm Action Manager rule can contain one or more of Alarms, Filters, and Actions. You may define as many Alarm Action Manager rules as required.

Alarm Action Manager rules are configured from the **Alarm Action Manager** screen. This screen is launched by selecting the **Configuration > Operational Settings > Alarm Action Manager** menu path.

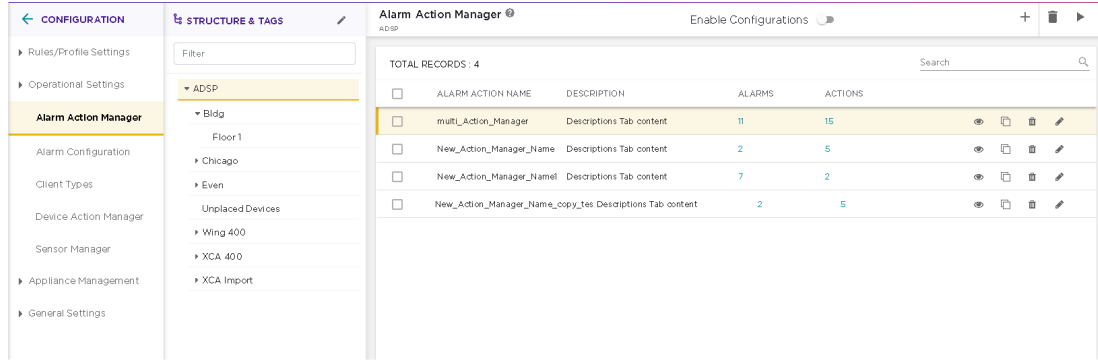


Figure 29: Alarm Action Manager Rule Set Screen

View Alarm Action Manager Rule Set

Use the **Alarm Action Manager** screen to view a list of these rules sets configured for your Extreme AirDefense managed system. An Alarm Action Manager Rule Set is a set of configurations that perform certain actions depending on the alarms that are raised in your network.

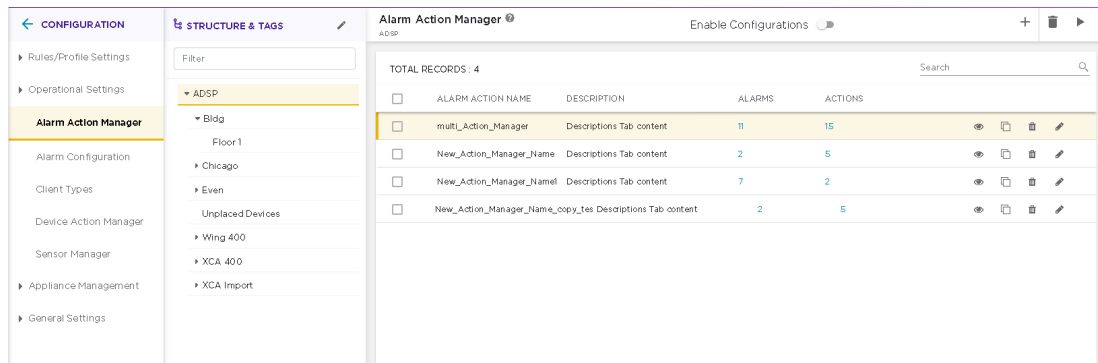







Figure 30: Alarm Action Manager Screen

The screen displays the following information:

Field	Description
Alarm Action Name	The name of the Alarm Action Manager rule set.
Description	A description about the Alarm Action Manager rule set and its actions.
Alarms	The number of alarms included in the Alarm Action Manager rule set.

Field	Description
Actions	The number of actions to be performed when the conditions specified within this rule set is met.
Actions	<p>The actions that can be performed on the Alarm Action Manager rule set. The icons in this field enable you to manage your Alarm Action Manager rule set . You can edit the rule set, create a new one by creating a duplicate of an existing rule set, or delete the rule set.</p> <p>The following actions can be performed:</p> <ul style="list-style-type: none"> • View - To view an Alarm Action Manager rule set, use the  icon for the rule set. The details for this rule set is displayed in a separate dialog. • Duplicate - Use the  icon to create a duplicate of the selected rule set. A duplicate of this rule set is created and the configuration dialog displays the newly created Alarm Action Manager rule set. Customize the duplicate rule set further to meet your requirements. • Delete - Use the  icon to delete the selected Alarm Action Manager rule set. • Edit - Use the  to edit the Alarm Action Manager rule set. A configuration dialog displays where you can make changes to the selected Alarm Action Manager rule set. For more information, see Edit Alarm Action Manager Rule Set on page 219.

To apply one or more Alarm Action Manager rule sets to a particular scope (location), select the context from the **Structure & Tags** area. If the permissions for this level are inherited from its parent, change the Override Inherit from: ADSP control to **Override**. Select the check-box next to each selected Alarm Action Manager rule set to enable it for the selected context.

To add more Alarm Action Manager rule sets, use the  icon located to the top right of this screen. For more information, see [Add Alarm Action Manager Rule Set](#) on page 203.

View Alarm Action Manager Rule Set

Use the  icon for an Alarm Action Manager rule set to view its details. A configuration dialog displays all the details about this Alarm Action Manager rule set.

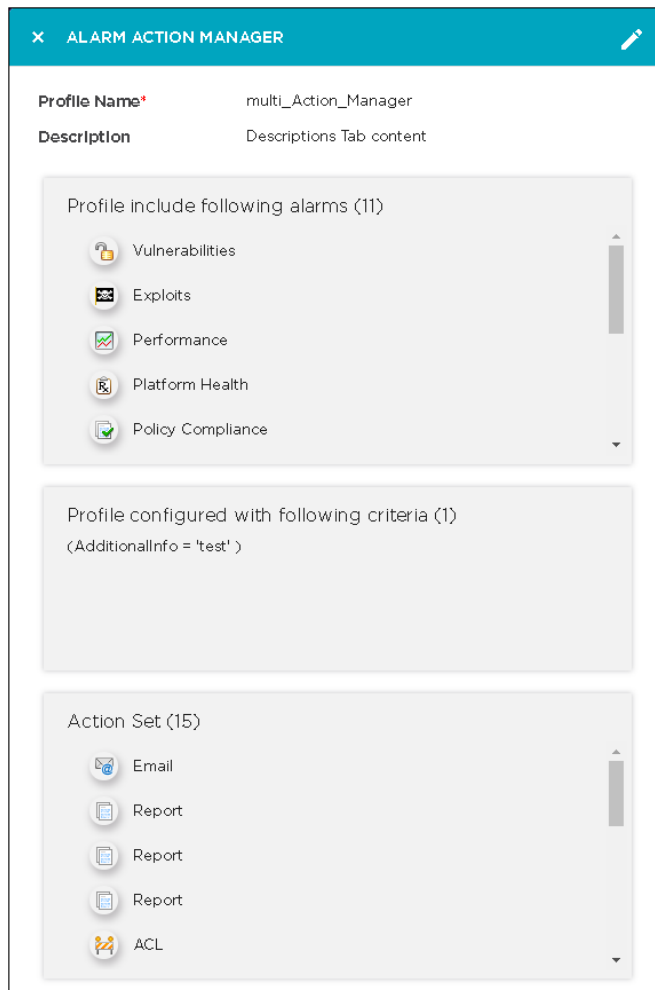



Figure 31: Alarm Action Manager Rule Set View Dialog


The following information is displayed for each Alarm Action Manager rule set.

Field	Description
Profile Name	The name of this Alarm Action Manager rule set.
Description	A description about the Alarm Action Manager rule set and its actions.
Profile include following alarms	This field lists the individual alarms included within this Alarm Action Manager rule set. The field name also lists the total number of alarms that are included within this rule set.
Profile configured with the following criteria	This field lists the filtering criteria used by this Alarm Action Manager rule set. The field name also lists the total number of filtering criteria used within this rule set.
Action Set	This field lists the actions that need to be performed by this rule set. The field name also lists the total number of individual actions that are configured for this Alarm Action Manager rule set.

You can directly edit the rule set from within this dialog. Click the  icon located to the top right of the dialog to edit it.

Add Alarm Action Manager Rule Set

An Alarm Action Manager profile is a set of rules that govern the automatic actions that can be performed when certain alarms are raised. These actions can be performed based on which alarms are monitored and other filtering criteria.

New Alarm Action Manager rule sets are created from the **Alarm Action Manager Rule Set Screen**. Use the  icon to add a new Alarm Action Manager Rule Set. The same screen is also used to edit an existing rule set of the same type.

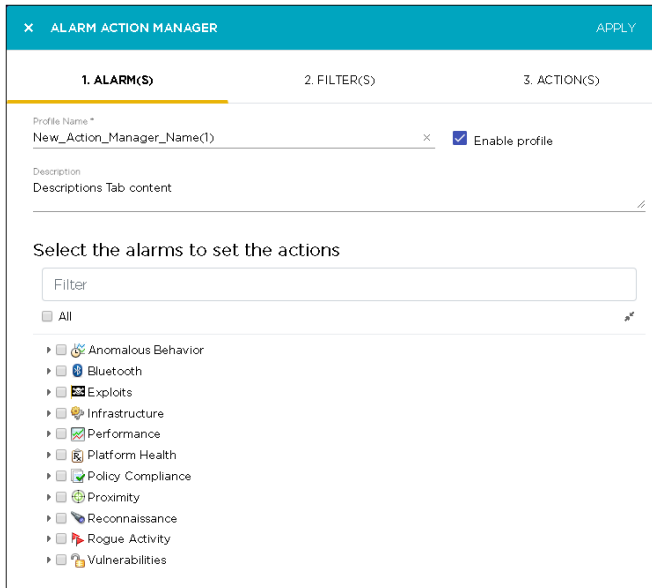


Figure 32: Add an Alarm Action Manager Rule Set

To create a new Alarm Action Manager rule set, you need to do the following:

1. Assign a name to your Alarm Action Manager rule set. Use the **Profile Name** field that is located in the **Alarms** tab of this screen.
2. Select the individual alarms or group of alarms from the **Alarms** tab.
3. Create at least one filter for the rule set. You can add up to twenty five (25) filters for every Alarm Action Manager rule set. Filtering enables you to remove data that does not interest you.
4. Create at least one action that needs to be performed for this Alarm Action Manager rule set.

Select Alarms

The **Alarms** tab of the **Alarm Action Manager** dialog lists all alarms that are raised by the AirDefense system. These alarms are classified under eleven (11) major categories with many sub-categories for each of them. The major categories of alarms are:

- Anomalous Behavior - This is a collection of all alarms that indicate behavior that is different from the normal behavior of a device within the AirDefense system.
- Bluetooth - This is a collection of all alarms that are related to Bluetooth and BLE devices.
- Exploits - This is a collection of all alarms that indicate attempted exploits on your AirDefense system.
- Infrastructure - This is a collection of all alarms that indicate issues with the infrastructure devices of the AirDefense system.
- Performance - This is a collection of all alarms that indicate performance issues with your AirDefense system.
- Platform Health - This is a collection of all alarms that indicate the current issues found within your AirDefense system.
- Policy Compliance - This is a collection of all alarms that indicate issues with compliance with various policies configured within the AirDefense system.
- Proximity - This is a collection of all alarms that are raised for various proximity events within your AirDefense system.
- Reconnaissance - This is a collection of all alarms that indicate presence of various tools that enable reconnaissance of your AirDefense system.
- Rogue Activity - This is a collection of all alarms that indicate rogue activity within your AirDefense system.
- Vulnerabilities - This is a collection of all alarms that indicate all vulnerabilities found during routine scanning of your AirDefense system.

Use the check-box next to each alarm or alarm group to select that item. When you select an alarm group, all its sub-groups and their alarms are also selected.

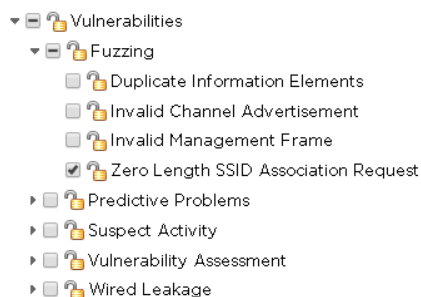


Figure 33: Selected Alarm

When an alarm group is selected, all its sub-groups and their alarms are also selected.

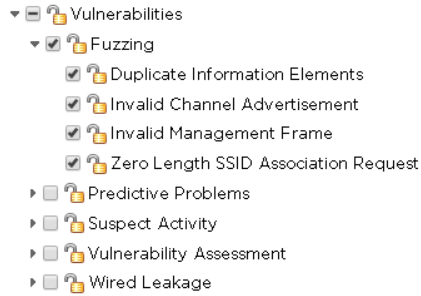


Figure 34: Selected Alarm Group

Configuring Filters

Configure your filters by using logical constructs of AND, OR, and NOT that are available for use when creating and adding multiple filter criteria to your rule. These logical constructs are explained below.

- AND - All the conditions defined for this rule must be met for the actions to be triggered.
- OR - One or more of the conditions defined for this rule set must be met for the actions to be triggered.
- NOT (AND) - This is the opposite condition of the AND construct. None of the selected conditions should meet for the action to be triggered.
- NOT (OR) - This is the opposite condition of the OR construct. One or more of the specified filter conditions must not be met for the action to be triggered.

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

**Important**

In the Alarm Action Manager, the order of filters within the rule defines how the filters are applied. For example, if you want create a rule to sanction only BSSs, the first filter should be defined as *DeviceType=Include BSS* before defining other rules such as *DeviceManufacturer* or *DeviceSSID*. Setting the *DeviceType=Include BSS* as the first filter will cause all wireless client devices to be ignored.

Selecting Filters

Select a filter to add to this Alarm Action Manager rule set by clicking the **Filters** tab. By default the **Basic** option is selected.

Click the **+** icon within the **Filters** tab to add a new filter rule to this rule set.

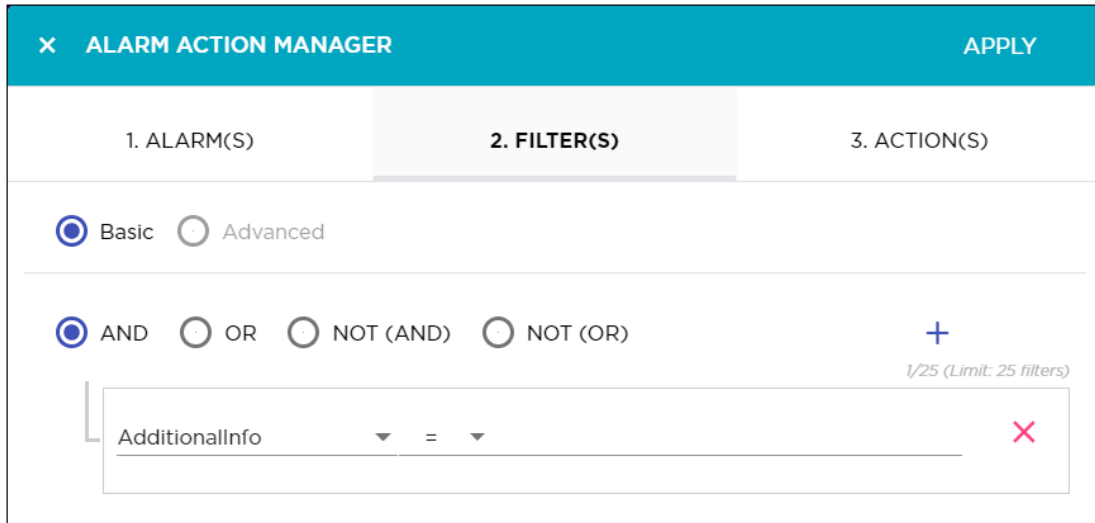


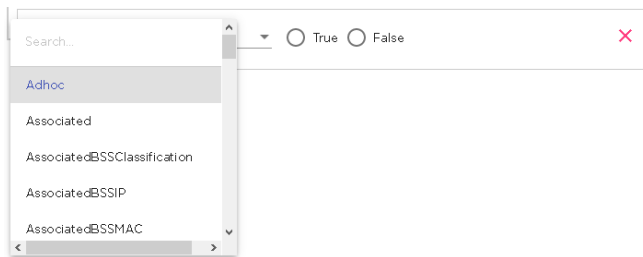
Figure 35: New Filter

Use the **AND**, **OR**, **NOT (AND)**, and **NOT (OR)** logical constructs to create your rule. You can add up to twenty five (25) filter rules to this Alarm Action Manager rule set.

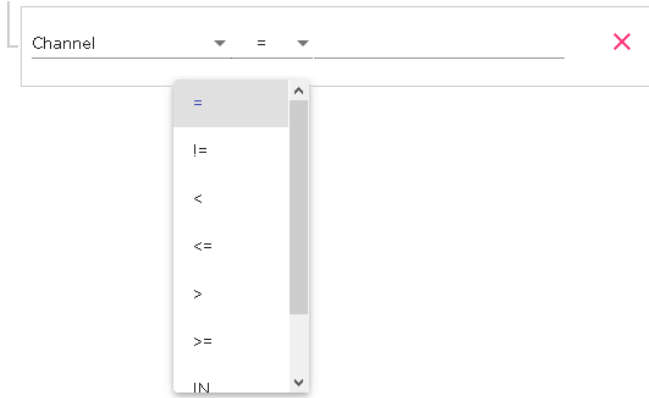
The following logical constructs are available for use:

- **AND** - All the conditions defined for this rule must be met for the actions to be triggered.
- **OR** - One or more of the conditions defined for this rule set must be met for the actions to be triggered.
- **NOT (AND)** - This is the opposite condition of the AND construct. None of the selected conditions should meet for the action to be triggered.
- **NOT (OR)** - This is the opposite condition of the OR construct. One or more of the specified filter conditions must not be met for the action to be triggered.

Use the **Filter** drop-down list to select the rule to apply.



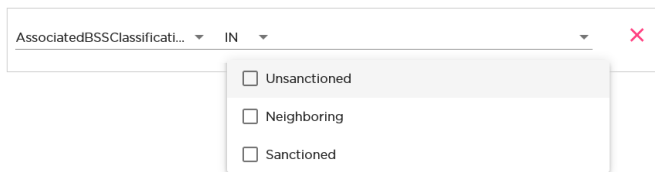
Next, use the **Comparison Criteria** drop-down list to select the comparison operator for this filter rule. The operator indicates the relationship between the filter and a value that you specify.



The selection in this list will vary with the filter selected in the **Filter** field. Some of the most common comparison operators are:

=	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)

For each filter, there will be one or more values that you compare for taking action. The kind and number of value or values will depend on the filter that you have selected. Enter a value that is appropriate for the filter criteria. Any errors that you make will be flagged immediately.



To remove a rule that you have configured, select the red **X** icon located to the right of each rule. When you click this icon, the rule is immediately deleted from this rule set.

Add Actions

Actions are configured from the **Actions** tab. You can specify one or more (up to five (5)) actions that can be performed when the conditions set in the **Filters** tab are met.

Actions for the alarms are classified into the following groups:

- **Notifications** - This group of actions enable you to automatically generate emails and reports for the selected alarms when the conditions specified in the **Filters** tab are met.
- **WIPS Mitigation** - This group of actions enable you to automatically take some specific WIPS mitigation actions and also generate SNMP traps. These actions are performed for the selected alarms when the conditions specified in the **Filters** tab are met.
- **Information Gathering** - This group of actions enable you to automatically do information gathering actions and generate system logs for the selected alarms when the conditions specified in the **Filters** tab are met.

Notification Actions

Notifications actions enables you to create and send automatic emails and also generate reports for the alarms that are raised within your AirDefense system.

The **Email** tab enables you to configure the parameters for creating and sending emails for your alarms.

The **Reports** tab enables you to configure the parameters for creating and sending reports for your alarms.

Email Configuration

The **Email** tab enables you to configure the parameters for sending emails for your alarms.

The screenshot displays the 'Email Notification' configuration window. At the top, there are two tabs: 'EMAIL' (selected) and 'REPORT'. Below the tabs, there is a list of email templates. The first template is highlighted with a yellow box and labeled 'Email'. To its right is a green plus icon. Below the list, the configuration form for the selected email template is shown. It includes fields for 'To:', 'From:', and 'Subject:'. The 'From:' field has a small note: 'Separate multiple addresses with semicolon'. Below these fields are two dropdown menus: 'Format:' (set to 'MailSMSText') and 'Priority:' (set to 'MEDIUM'). At the bottom, there are two radio buttons: 'Send email on alarm active' (which is selected) and 'Send email on alarm active, clear and expire'.

Figure 36: E-Mail Configuration

By default, an empty template is made available for immediate use. Use this empty template to create your first email. To add additional emails, use the green + icon to create a new blank template. When you add a new email, a new block is created for it. You can hover on each of these blocks to get a synopsis of the configuration for that block.

For each email, provide the following information:

Field	Description
To	The email addresses of the recipients for this email. Add multiple email addresses separated with a semi-colon (;) sign.
From	The email address that is used to send this email. This is the address that will receive any reply mails received from the recipients.
Subject	The subject for this email.
Format	Use the drop-down list to select the appropriate format for the email being sent.
Priority	Use the drop-down list to select the priority of this mail.
Send email on alarm active	Select this option to send email for active alarms only. You can use this or the Send email on alarm active, clear, and expire option.
Send email on alarm active, clear, and expire	Select this option to send email every time an alarm is active, cleared, or expires. You can use this or the Send email on alarm active option.

Report Action

The **Reports** tab enables you to configure the parameters for creating and sending reports for your alarms.

The screenshot shows the 'Notifications' configuration window with the 'REPORT' tab selected. A 'Report' button with a green plus icon is highlighted. Below it, the 'Report' configuration area includes:

- Report Type:** Wifi Direct Network Activity
- Scope Increase factor:** 1
- Run immediate for previous:** 1 Day(s) (selected)
- Run on alarm clear / expire:** (unselected)
 - Duration of the alarm: (unselected)
 - *For Previous:** 1 Hour(s) (selected)
- Publish:** SHARED (selected), ***report named:** _____
- E-mail:** HTML (selected), ***report to:** _____

Separate multiple addresses with semicolon

Figure 37: Report Configuration

By default, an empty template is made available for immediate use. Use this empty template to create your first report. To add additional reports, use the green + icon to create a new blank template. When you add a new report, a new block is created for

it. You can hover on each of these blocks to get a synopsis of the configuration for that block.

For each report, provide the following information:

Field	Description
Report Type	Use the drop-down to select from one of the pre-created reports.
Scope Increase Factor	Use the drop-down to select the scope of your report. The value in this field specifies the number of levels to expand the scope of the report. A value of 1 means only use the floor level. A value of 2 indicates that the floor and its parent level is to be included in this report's scope.
Run immediate for previous	Runs the report immediately for the period selected in the two drop-down lists located within this field.
Run on alarm clear / expire	Runs the report when the alarm is either cleared manually or expires automatically. To select a duration of time for this report, use the two drop-down list located within this field.
Publish	Indicates how this report is published. A report can be one of <i>SHARED</i> or <i>PRIVATE</i> . A shared report can be viewed by other users of the AirDefense system. A private report can only be viewed by you. When creating a report, provide a distinct name for it.
E-mail	Indicates if the report is emailed to specific users. Provide a list of recipients for this email, separated by semi-colon (;) in the field provided for the purpose.

WIPS Mitigation

WIPS Mitigation actions are a set of specific actions that you can take at the device level to mitigate issues with wireless intrusion from devices that do not belong to your AirDefense system. You can also configure and send SNMP trap messages to multiple SNMP services within your network.

Use the **General** tab of the **WIPS Mitigation** control to configure the various settings.

Similarly, use the **SNMP Trap** tab of this screen to configure SNMP servers to send SNMP traps to the remote SNMP servers.

General Actions

The **General** tab of the **WIPS Mitigation** field provides you with the following WIPS mitigation tools.

- **ACL** - When devices meet the criteria specified in the **Alarms** and the **Filters** tabs, these devices are automatically added to a switch's access control list.
- **Port Suppression** - This action is used to suppress communication between unauthorized devices and switches on your network.

- Termination - This action is used to terminate devices that generate specific alarms as selected in the **Filters** tab. An option to also terminate the device that a rogue device is paired to is also available.

ACL

The **ACL** action enables the Access Control List on switches that meet the conditions specified in the filters.

Use the **Scope Increase Factor** drop-down to select the scope of this action. The value in this field specifies the number of levels to expand the scope of the addition. A value of one (1) means only use the floor level. A value of two (2) indicates that the devices in the floor and its parent level are to be included. And so on. The maximum value that can be set is six (6).

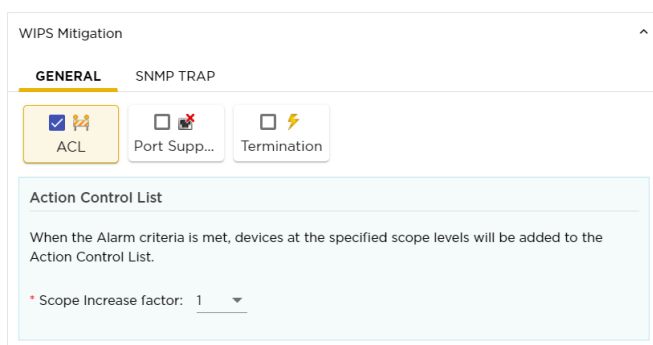


Figure 38: ACL

Hover on the **ACL** box to view a synopsis of its configuration.

Port Suppression

The **Port Suppression** action is used to suppress communication between unauthorized devices and the switches on your network.

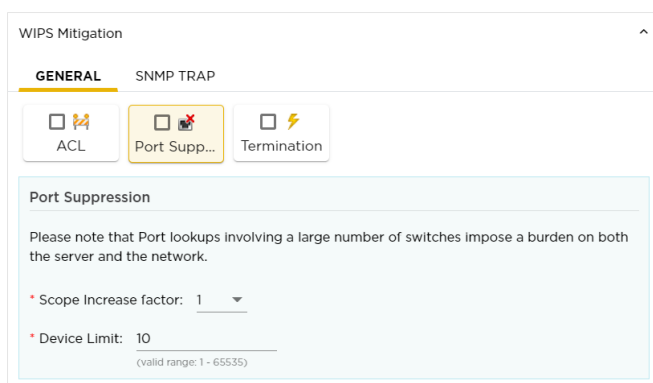


Figure 39: Port Suppression

Use the **Scope Increase Factor** drop-down to select the scope of this action. The value in this field specifies the number of levels to expand the scope of the port suppression action. A value of one (1) means only use the floor level. A value of two (2) indicates that the devices in the floor and its parent level are to be included. And so on. The maximum value that can be set is six (6).

Use the **Device Limit** field to specify a device limit. When a value is specified, for example, ten (10), the port suppression action will not be performed if the number of devices connected to the port exceeds this value.

Hover on the **Port Suppression** box to view a synopsis of its configuration.

Termination

The **Termination** action enables the automatic termination of devices that generate the alarms selected in the **Alarms** tab. When the Alarm criteria are met, devices at the selected scope level are terminated automatically.

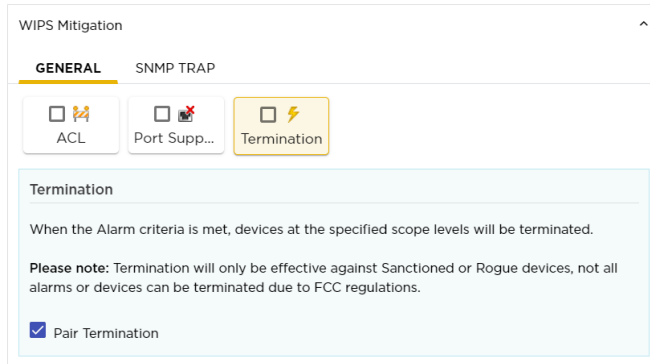


Figure 40: Termination

Select the **Pair Termination** option to enable termination of the offending pair of devices. This feature is only available for the following alarms.

- Ad-Hoc Connection between Sanctioned Stations
- Ad-Hoc Networking Extrusion Detected
- Sanctioned Client Association to Unsanctioned Virtual Wi-Fi
- Unauthorized Roaming
- Unsanctioned Client Associated to Sanctioned Client running Virtual Wi-Fi
- Wireless Client Accidental Association

To use the **Termination** action, you must enable the **Air Termination System** and the **Policy-based Air Termination System** features. These features can be enabled through the web user interface.

Hover on the **Termination** box to view a synopsis of its configuration.

SNMP Trap

The **SNMP Trap** action enables sending SNMP traps to your SNMP servers when the alarms specified in this Alarm Action Manager rule set are generated.

Figure 41: SNMP Trap

By default, an empty template is made available for immediate use. Use this empty template to create your first SNMP Trap. To add additional traps, use the green + icon to create a new blank template. When you add a new SNMP Trap, a new block is created for it. You can hover on each of these blocks to get a synopsis of the configuration for that block.

Multiple SNMP Traps can be generated for a Alarm Action Manager rule set.

For each SNMP Trap, provide the following information:

Field	Description
Server Address	The IP address of your remote SNMP server.
SNMP Port	The port on which your SNMP server is listening for notifications.
Community String	The community string for the receiving SNMP Server. This string is a series of characters manipulated as a group, in this instance for SNMP.
Transport	Specifies the transport protocol to use for sending the SNMP traps. The available protocols are: <ul style="list-style-type: none"> UDP (User Datagram Protocol) TCP (Transmission Control Protocol) In general, UDP is used for transmitting SNMP traps. However, TCP can be used for tunneling the traps over SSL (Secure Sockets Layer).
Max Queue Size	Specifies the maximum queue size for the notifications. Choose a size from the drop-down list.
Send Time	The choices Send SNMP Trap on alarm active , Send SNMP Trap on alarm active, clear, and expire , and Send every <duration> enable configuring when the SNMP traps are sent to the server.

Info Gathering

Info Gathering actions are a set of actions that you can take to gather more information about the state of your AirDefense system when particular alarms are raised in your system. When such alarms are raised, you can configure your system to automatically generate syslog entries.

Use the **General** tab of the **Info Gathering** control to configure the various settings.

Similarly, use the **Sys Log** tab of this screen to configure generating Sys Log entries for these alarms.

General Actions

The **General** tab of the **Info Gathering** field provides you with the following information gathering tools:

- **AP Test** - Runs a pre-configured AP test profile when the specified alarms are generated.
- **Frame Capture** - An action that monitors and analyzes real-time data flow in your network and saves the data for analysis.
- **Vulnerability Assessment** - Runs a pre-configured Vulnerability Assessment test when the specified alarms are generated.
- **Data Collection** - Automatically corrects configuration compliance violations when conditions specified in the filters are met.
- **Spectrum Analysis** - Runs a Spectrum Analysis or Advanced Spectrum Analysis using the profile specified when conditions specified in the filters are met.

AP Test

The *AP Test* action runs an AP test using a specific profile if the conditions specified in the **Filters** tab are met.



Note

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

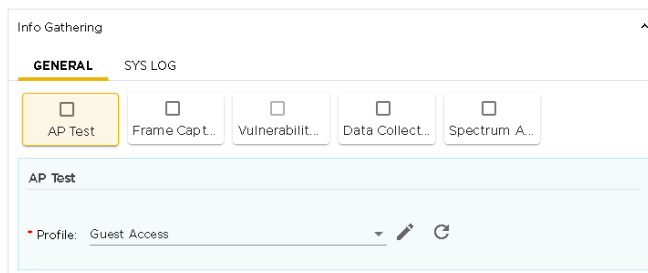



Figure 42: AP Test Configuration

Use the **Profile** drop-down list to select an appropriate AP Test profile. Use the  icon to edit the selected AP Test profile if required.

Hover on the **AP Test** box to view a synopsis of its configuration.

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

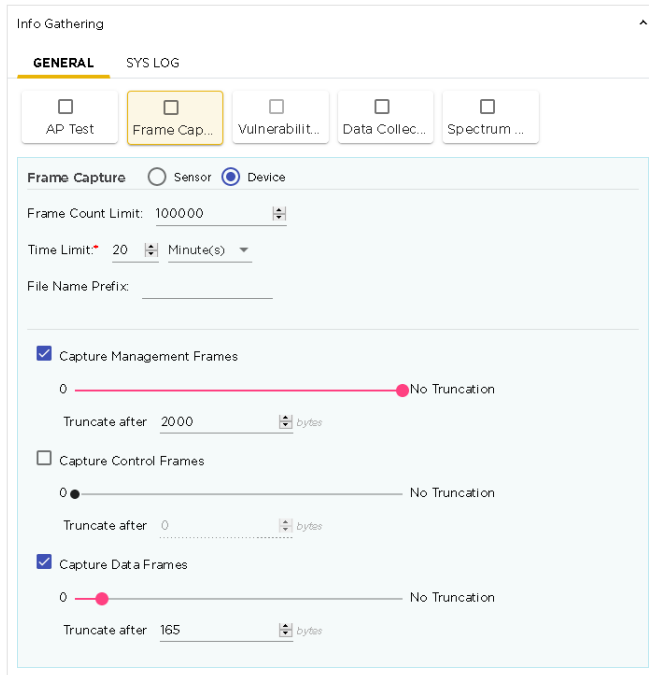


Figure 43: Frame Capture Configuration

Provide the following Frame Capture configuration information:

Field	Description
Frame Capture	Select the scope of the frame capture. Frame capture can be limited to either Sensor or to Device .
Frame Count Limit	Limits the total number of frames to capture for each device category. Use the spinner control to set the value.
Time Limit	Specifies a time duration for the Frame Capture to run. Time can be set in number of minutes or hours. Use the appropriate controls to configure this value.
File Name Prefix	Specifies the prefix for the frame capture file. This prefix along with a number sequence is used to name your frame capture files.
Capture Management Frames	Select to include <i>Management Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Management Frames that will be captured for this instance of frame capture. Capture Management Frames is selected by default.

Field	Description
Capture Control Frames	Select to include <i>Control Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Control Frames that will be captured for this instance of frame capture. Capture Control Frames is not selected by default.
Capture Data Frames	Select to include <i>Data Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Data Frames that will be captured for this instance of frame capture. Capture Data Frames is selected by default.

Hover on the **Frame Capture** box to view a synopsis of its configuration.

Vulnerability Assessment

The *Vulnerability Assessment* action runs a vulnerability assessment test using the specified profile if the conditions defined in the **Filters** tab are met.

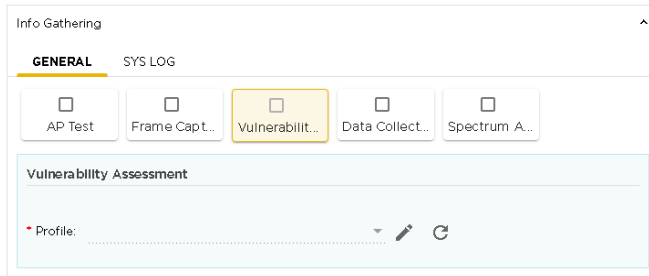



Figure 44: Vulnerability Assessment Configuration

Use the **Profile** drop-down list to select an appropriate Vulnerability Assessment profile. Use the  icon to edit the selected Vulnerability Assessment profile if required.

Hover on the **Vulnerability Assessment** box to view a synopsis of its configuration.

Data Collection

The *Data Collection* action automatically corrects configuration compliance issues and violations when the conditions defined in the **Filters** tab are met.

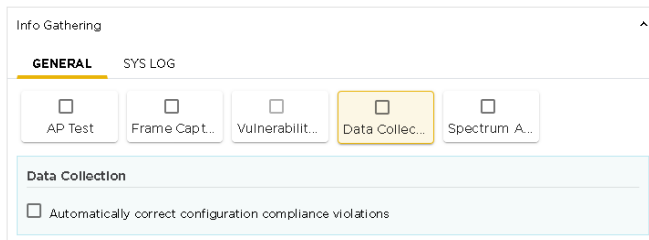


Figure 45: Data Collection Configuration

Select the **Automatically correct configuration compliance violations** option to enable it. When this option is selected, an alarm is generated by a device meeting the

conditions specified in the **Filters** tab and AirDefense automatically uploads the last approved configuration to the device to correct any violations.

Hover on the **Data Collection** box to view a synopsis of its configuration.

Spectrum Analysis

The *Spectrum Analysis* action runs a regular *Spectrum Analysis* or an *Advanced Spectrum Analysis* using the specified profile if the conditions specified in the **Filters** tab are met.

Figure 46: Spectrum Analysis Configuration

Provide the following configuration information.

Field	Description
Time Limit	Specifies a time duration for the Spectrum Analysis to run. Time can be set in number of minutes. Use the spinner control to configure this value.
File Name Prefix	Specifies the prefix for the spectrum analysis file. This prefix is used when creating your spectrum analysis file.
Spectrum Settings	Select this tab for configuring the regular Spectrum Analysis settings.
Advanced Spectrum Settings	Select this tab for configuring the Advanced Spectrum Analysis settings.

Hover on the **Spectrum Analysis** box to view a synopsis of its configuration.

Spectrum Setting

Provide the following configuration information for the normal Spectrum Analysis

Field	Description
Scan Type	Select one of Full Scan or Interference Scan . <ul style="list-style-type: none"> • <i>Full Scan</i> scans the entire 2.4GHz bandwidth (in 5MHz steps) and 5GHz bandwidth (in 20MHz steps) with a short dwell time (around 50 ms). It supports limited classification of interference sources. • <i>Interference Scan</i> scans three frequencies in the 2.4GHz band and three frequencies in the 5GHz band with a longer dwell time (around 500 ms). It supports classification for all interference sources.
Pulse Definition	Defines the values for each pulse when performing Spectrum Analysis. Use the Threshold control to set the pulse threshold value in <i>dBm</i> . Use the Width control to define the gap between two consecutive pulses.

Advanced Spectrum Settings

Provide the following configuration information for the Advanced Spectrum Analysis

Select the scan type. Select one of **Dedicated Scan** or **In-Line Scan**.

- *Dedicated Scan* is a full, detailed spectrum scan.
- *In-Line Scan* is a spectrum scan of all channels except the 802.11 channels and bands.

For each of the above scan types, provide the following configurations:

Field	Description
Scan Time	Defines the scan time in milliseconds. Use the spinner control to set this value. The default value is 1000 milliseconds.
Threshold	For both the 2.4 GHz and 5.0 GHz bands, set the threshold value in <i>dBm</i> .
Duty Cycle Threshold	For both the 2.4 GHz and 5.0 GHz bands, set the duty cycle threshold value in <i>dBm</i> .

Edit Alarm Action Manager Rule Set

The **Alarm Action Manager** screen lists the Alarm Action Manager rules sets configured for your Extreme AirDefense managed system. An Alarm Action Manager Rule Set is a set of configurations that perform certain actions depending on the alarms that are raised in your network.

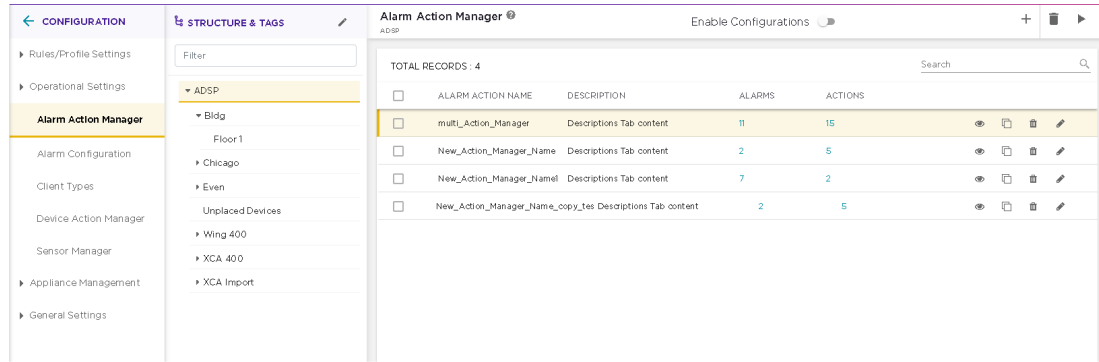



Figure 47: Alarm Action Manager Screen

Use the  icon located to the right of each Alarm Action Manager rule set to edit its configuration.

Alarm Action Manager rule sets are edited the **Alarm Action Manager Screen**.

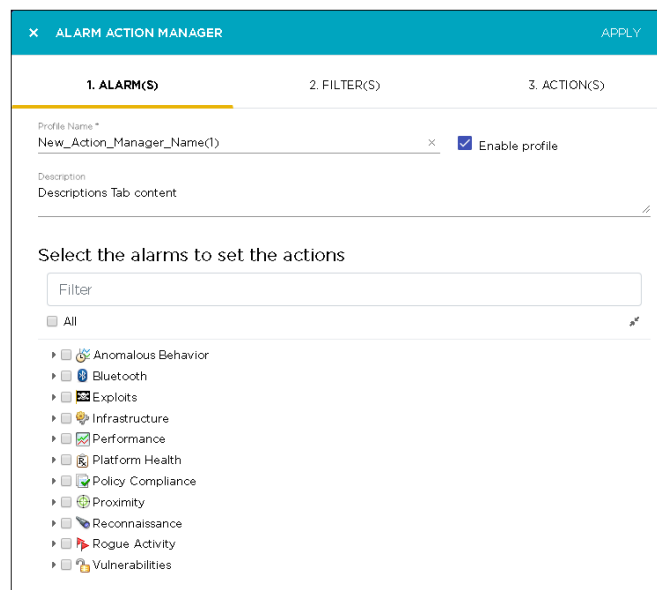


Figure 48: Edit an Alarm Action Manager Rule Set

You can modify all the settings for this Alarm Action Manager rule set except the **Profile Name** assigned to this rule set.

Click the **APPLY** button located to the top right of this screen to save your changes. To exit without saving your changes, select the **X** button to the top left of this screen.

Delete Alarm Action Manager Rule Set

The **Alarm Action Manager** screen lists the Alarm Action Manager rules sets configured for your Extreme AirDefense managed system. An Alarm Action Manager Rule Set is a set of configurations that perform certain actions depending on the alarms that are raised in your network.

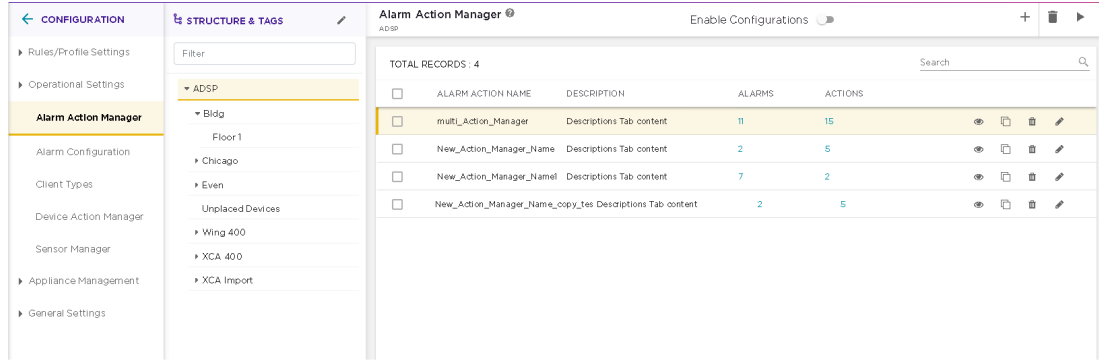



Figure 49: Alarm Action Manager Screen

Use the  icon located to the right of each Alarm Action Manager rule set to delete it. A confirmation dialog displays.

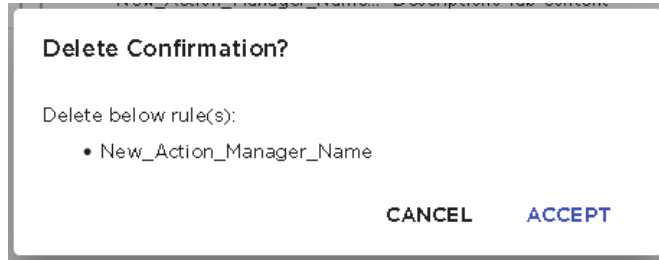


Figure 50: Delete Alarm Action Manager window

To delete the Alarm Action Manager rule set, click the **ACCEPT** button. The Alarm Action Manager rule set is immediately deleted.

To exit without deleting the Alarm Action Manager rule set, click the **CANCEL** button.

Device Action Manager

Device Action Manager enables you to create a set of rules that can be applied to devices in your Extreme AirDefense system. This feature enables you to create filters that define particular conditions, and, create actions that are automatically performed when these conditions are met.

Device Actions are configured using the **Device Action Manager** screen. This screen is launched by selecting the **Configuration > Operational Settings > Device Action Manager** menu path.

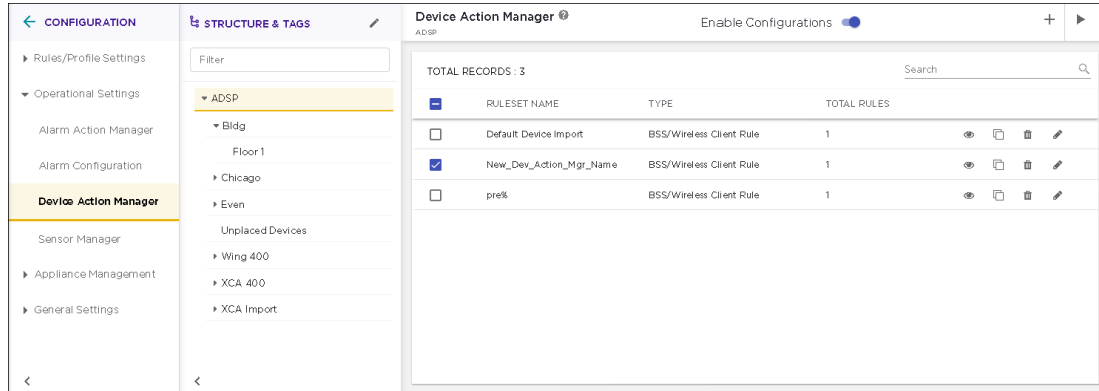


Figure 51: Device Action Manager Rule Set Screen

View Device Action Manager Rule Set

Use the **Device Action Manager** screen to view a list of these rule sets configured for your Extreme AirDefense managed system. A Device Action Manager rule set is a set of configurations that performs certain actions depending on defined conditions that occur in your network.

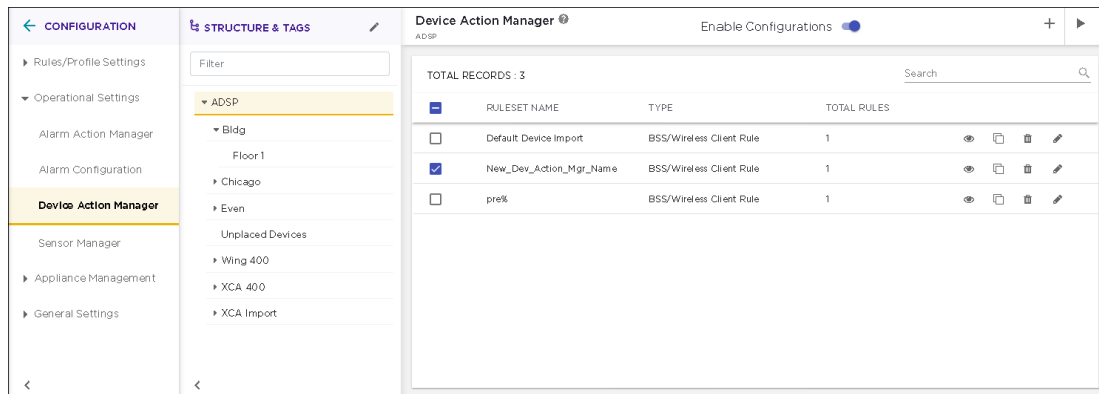







Figure 52: Device Action Manager Screen

The screen displays the following information:

Field	Description
Ruleset Name	The name of the Device Action Manager rule set.
Type	The type of Device Action Manager rule set. Can be one of: <ul style="list-style-type: none"> Infrastructure Device Rule Set - This rule set is for those devices that make up the Extreme AirDefense infrastructure such as switches and access points. Wireless Client /BSS Rule Set - This rule set is for those devices that are managed by the Extreme AirDefense system.

Field	Description
Total Rules	Displays the number of rules that are included in this Device Action Manager rule set.
Action	<p>The actions that can be performed on the Device Action Manager rule set. The icons in this field enable you to manage your Device Action Manager rule set . You can edit the rule set, create a new one by creating a duplicate of an existing rule set, or delete the rule set.</p> <p>The following actions can be performed:</p> <ul style="list-style-type: none"> • View - To view a Device Action Manager rule set, use the  icon for the rule set. The details for this rule set is displayed in a separate dialog. • Duplicate - Use the  icon to create a duplicate of the selected rule set. A duplicate of this rule set is created and the configuration dialog displays the newly created Device Action Manager rule set. Customize the duplicate rule set further to meet your requirements. • Delete - Use the  icon to delete the selected Device Action Manager rule set. • Edit - Use the  to edit the Device Action Manager rule set. A configuration dialog displays where you can make changes to the selected Device Action Manager rule set. For more information, see Add a Device Action Manager Rule Set on page 224.

To apply one or more Device Action Manager rule sets to a particular scope (location), select the context from the **Structure & Tags** area. If permissions for this level are inherited from its parent, change the Override Inherit from: ADSP control to **Override**. Select the check-box next to each selected Device Action Manager rule set to enable it for the selected scope (location). Click the **APPLY** button to apply the override for the selected context.

To add more Device Action Manager rule sets, use the  icon located to the top right of this screen. For more information, see [Add a Device Action Manager Rule Set](#) on page 224.

View Device Action Manager Rule Set

Use the  icon for a Device Action Manager rule set to view its details. A configuration dialog displays all the details about this Device Action Manager rule set.

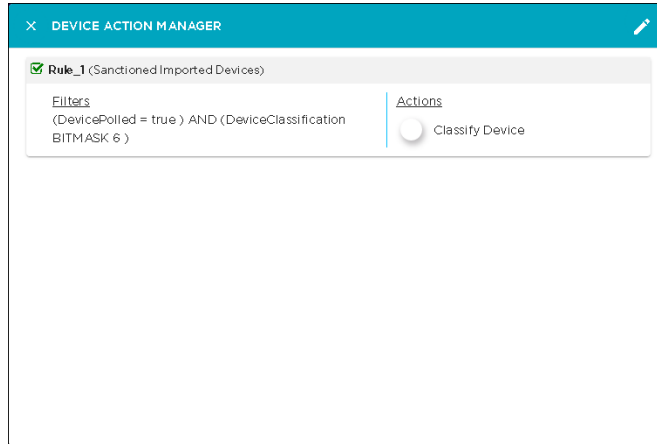



Figure 53: Device Action Manager Rule Set View Dialog

The following information is displayed for each Device Action Manager rule set.

Field	Description
Name	The name of this Device Action Manager rule set.
Rules	<p>A list of rules that are configured for this rule set. For each rule, the following information is displayed.</p> <ul style="list-style-type: none"> Filters - The Filters column displays the rule that is configured. Actions - The Actions column displays the action that will be taken if a device meets the rules specified in the Filters column.

You can directly edit the rule set from within this dialog. Click the  icon located to the top right of the dialog to edit it.

Add a Device Action Manager Rule Set

A Device Action Manager profile is a set of rules that govern actions that can be performed when certain conditions are met. These actions can be performed both on Infrastructure devices and Client devices.

Device Action Manager supports two types of rule sets; one for infrastructure devices and one for wireless clients/BSSs. You have to create separate rules for each device type. Infrastructure devices such as wireless switches, access points, and wired switches can be actioned on separately from Client devices such as wireless clients and devices.

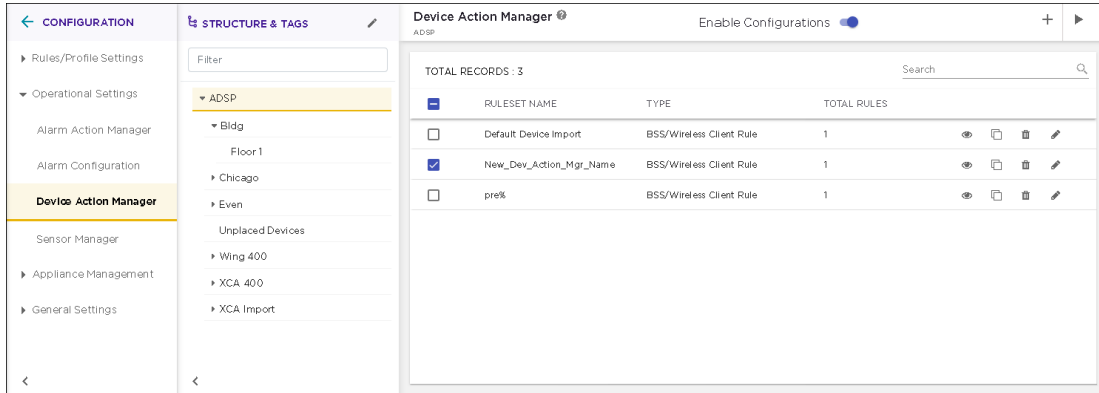


Figure 54: Device Action Manager Profile Screen

Use the **+** icon to add a new Device Action Manager Rule Set.

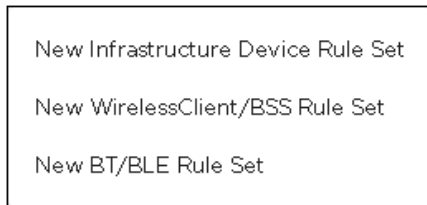


Figure 55: Device Action Manager Rule Set Types

Add a New Wireless Client/BSS Rule Set

Use the **Device Action Manager** screen to add a new wireless client/BSS rule. The same screen is also used to edit an existing rule set of the same type.

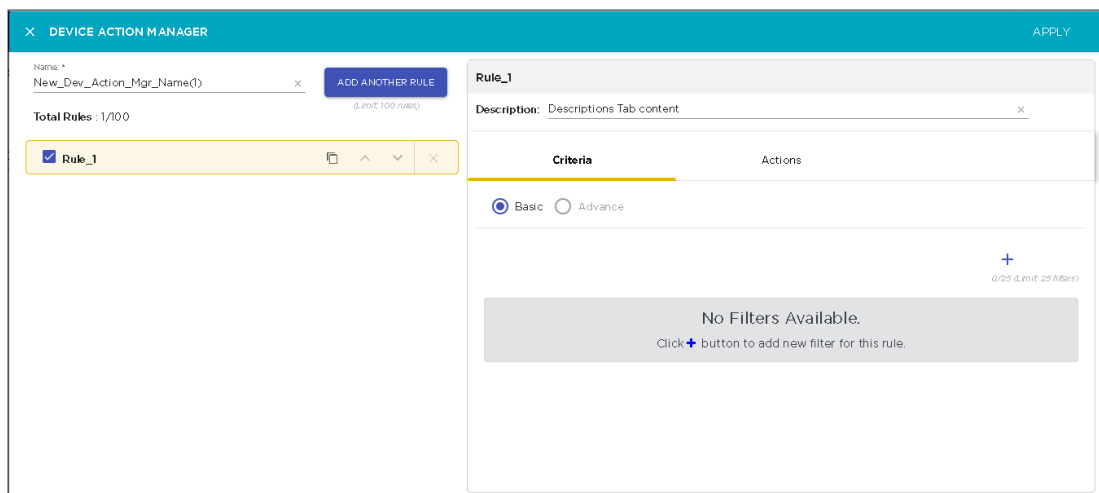


Figure 56: Add a Device Action Manager Rule Set

To create a new wireless client/BSS rule set, you need to do the following:

1. Assign a name to your Device Action Manager rule set. Use the **Name** field that is located to the top left of the screen.
2. Create at least one Rule for this rule set. You can add up to one hundred (100) rules to your rule set. Use the **Add Another Rule** button to add additional rules.

For each rule in your rule set, you must define at least one filter criteria and one action.

3. Create and add at least one filtering criteria for each rule that you create. You can add up to twenty five (25) criteria per rule in your rule set. Use the **+** icon in this tab to add new filters.
4. Create and add at least one action for the rule set. You can add up to five (5) actions for this rule set. Use the **+** icon in this tab to add new actions.

Configuring Filters

Configure your filters by using logical constructs of AND, OR, and NOT that are available for use when creating and adding multiple filter criteria to your rule. These logical constructs are explained below.

- AND - All the conditions defined for this rule must be met for the actions to be triggered.
- OR - One or more of the conditions defined for this rule set must be met for the actions to be triggered.
- NOT (AND) - This is the opposite condition of the AND construct. None of the selected conditions should meet for the action to be triggered.
- NOT (OR) - This is the opposite condition of the OR construct. One or more of the specified filter conditions must not be met for the action to be triggered.

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
- DevicePolledIP
- DevicePolledName
- DevicePolledSSID
- DeviceProtocol
- DeviceSSID
- DeviceSensedIP
- DeviceSensedSSID
- DeviceType
- DeviceVendorPrefix
- SensorIP
- SensorMAC
- SensorName
- SignalStrength
- WatchList
- WiFiDirect.

**Important**

In the Device Action Manager, the order of filters within the rule defines how the filters are applied. For example, if you want create a rule to sanction only BSSs, the first filter should be defined as *DeviceType=Include BSS* before defining other rules such as *DeviceManufacturer* or *DeviceSSID*. Setting the *DeviceType=Include BSS* as the first filter will cause all wireless client devices to be ignored.

Selecting Filters

Select a filter to add to this Wireless Clients/BSS Device Action Manager rule set by clicking the **Criteria** tab. By default the **Basic** option is selected.

Click the  icon within the **Criteria** tab to add a new filter rule to this rule set.

Figure 57: New Filter

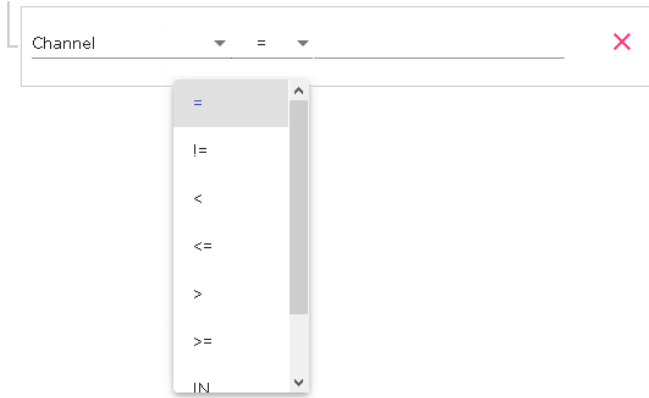
Use the **AND**, **OR**, **NOT (AND)**, and **NOT (OR)** logical constructs to create your rule. You can add up to twenty five (25) filter rules to this Device Action Manager rule set.

The following logical constructs are available for use:

- **AND** - All the conditions defined for this rule must be met for the actions to be triggered.
- **OR** - One or more of the conditions defined for this rule set must be met for the actions to be triggered.
- **NOT (AND)** - This is the opposite condition of the AND construct. None of the selected conditions should meet for the action to be triggered.
- **NOT (OR)** - This is the opposite condition of the OR construct. One or more of the specified filter conditions must not be met for the action to be triggered.

Use the **Filter** drop-down list to select the rule to apply.

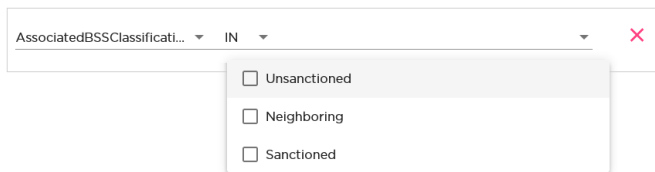
Next, use the **Comparison Criteria** drop-down list to select the comparison operator for this filter rule. The operator indicates the relationship between the filter and a value that you specify.



The selection in this list will vary with the filter selected in the **Filter** field. Some of the most common comparison operators are:

=	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)

For each filter, there will be one or more values that you compare for taking action. The kind and number of value or values will depend on the filter that you have selected. Enter a value that is appropriate for the filter criteria. Any errors that you make will be flagged immediately.



To remove a rule that you have configured, select the red **X** icon located to the right of each rule. When you click this icon, the rule is immediately deleted from this rule set.

Add Actions

Actions are configured from the **Actions** tab. You can specify one or more (up to five (5)) actions that can be performed when the conditions set in the **Criteria** tab are met. The valid actions are:

- Classify Devices - Classifies devices using the filter(s) to determine which devices are to be classified.
- Clear active alarm - 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).
- Email - Sends an email to the administrator if the conditions defined in the filter(s) are met.

Use the **+** icon to add an action to your Device Action Manager Rule Set. You can add up to five (5) rules for each rule set. Configuration settings will be different for each action. For example, the following is the configuration settings when you select *Email* as your action.

The screenshot shows the configuration interface for a rule set named 'Rule_1'. The 'Description' field contains 'Descriptions Tab content'. The 'Criteria' tab is active, and the 'Actions' tab is selected. Two actions are listed: 'Classify Devi...' and 'Email'. The 'Email' action is highlighted, and its configuration form is shown below. The form includes fields for 'To:', 'From:', 'Subject:', and 'Priority: MEDIUM'. The 'To:' field has a note: 'Separate multiple addresses with semicolon'. The 'Priority' is set to 'MEDIUM'.

Figure 58: Action - Send Email

The send email action enables to send an email when the conditions specified in the **Criteria** tab are met. You can send mails to multiple persons with customized subject, priority, and the email from which this mail is supposed to originate.

When you create an action, its name is added to the top of the **Actions** tab.



To delete a specific action, use the small *x* button located to the top right of the action's name in the tab. When you click the button, the action is immediately removed.

Once you have configured your Device Action Manager Rule Set, click the **APPLY** button located to the top right of this window. The rule is saved and is added to the list of Device Action Manager rule sets.

The following image is of a fully configured Device Action Manager Rule Set.

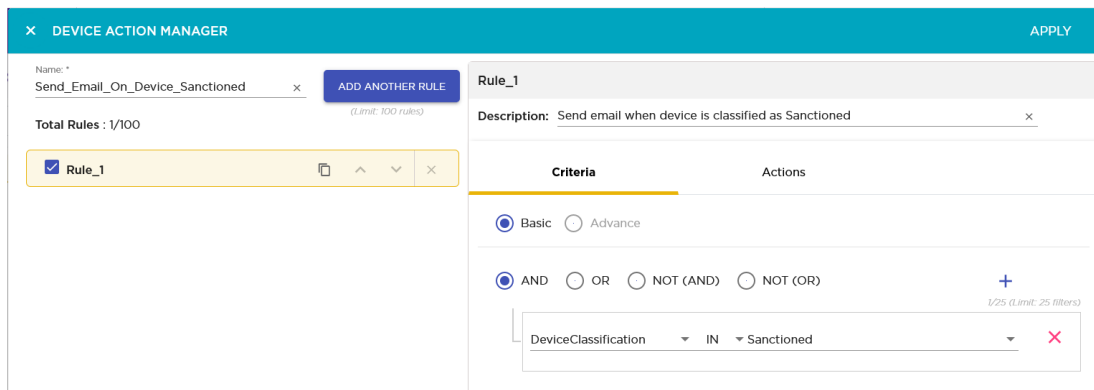


Figure 59: Example Device Action Manager Rule Set

Classify Device Action

The *Classify Device* action enables you to classify a device into various categories if the conditions specified in the **Filters** tab are met.



Figure 60: Classify Device Action

Use the **Classify Devices as** drop-down list to select the device's classification. The devices can be classified as:

- Sanctioned (Inherited Profile) - Devices with Sanctioned (Inherit Profile) classification will inherit all security profiles at device scope level.
- Unsanctioned - Devices will be classified as unsanctioned.

- Neighboring - Devices will be classified as neighboring devices.
- Sanctioned (Assigned Profiles) - Devices will be classified as sanctioned and then assigned the profiles selected from the list of profiles.

Hover on the **Classify Device** box to view a synopsis of its configuration.

Clear Active Alarms

The *Clear Active Alarms* action enables you to clear all active alarms in your AirDefense system. This action is performed when the conditions specified in the **Filters** tab are met.

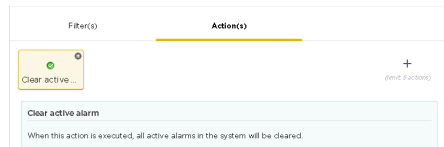


Figure 61: Clear Active Alarms Action

There are no configurable parameters for this action.

Set Client Type Action

The *Set Client Type* action enables you to classify a device as a particular client type. This action is performed when the conditions specified in the **Filters** tab are met.

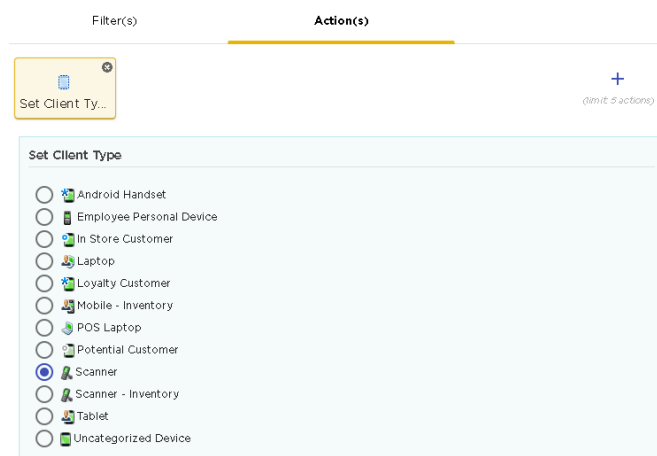


Figure 62: Set Client Type Action

Select the client type to apply to the devices from the list. The items in this list is populated from the **Client Types** screen.

ACL

The **ACL** action enables the Access Control List on devices that meet the conditions specified in the filters.

Use the **Scope Increase Factor** drop-down to select the scope of this action. The value in this field specifies the number of levels to expand the scope of the addition. A value of one (1) means only use the floor level. A value of two (2) indicates that the devices in

the floor and its parent level are to be included. And so on. The maximum value that can be set is six (6).

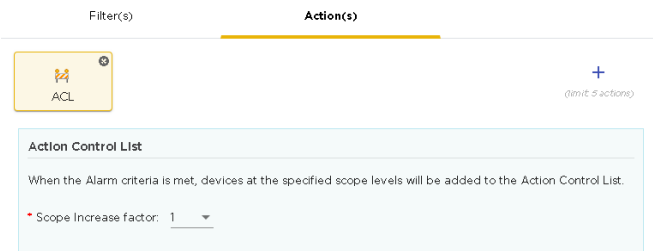


Figure 63: ACL

Hover on the **ACL** box to view a synopsis of its configuration.

Port Suppression

The **Port Suppression** action is used to suppress communication between unauthorized devices and the switches on your network.

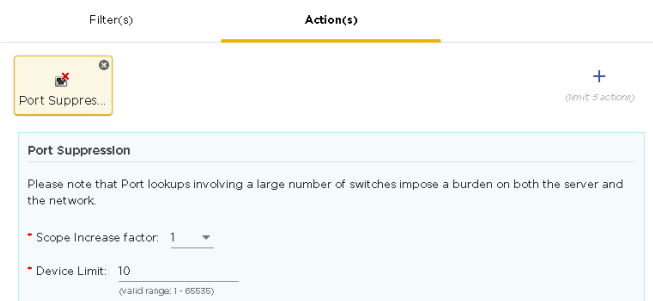


Figure 64: Port Suppression

Use the **Scope Increase Factor** drop-down to select the scope of this action. The value in this field specifies the number of levels to expand the scope of the port suppression action. A value of one (1) means only use the floor level. A value of two (2) indicates that the devices in the floor and its parent level are to be included. And so on. The maximum value that can be set is six (6).

Use the **Device Limit** field to specify a device limit. When a value is specified, for example, ten (10), the port suppression action will not be performed if the number of devices connected to the port exceeds this value.

Hover on the **Port Suppression** box to view a synopsis of its configuration.

Termination

The **Termination** action enables the automatic termination of devices that meet the conditions specified in the **Filters** tab. When the Alarm criteria are met, devices at the selected scope level are terminated automatically.

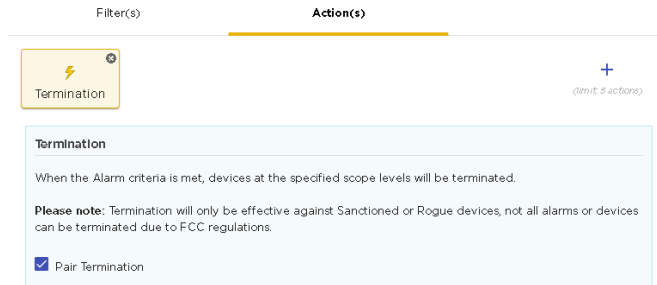


Figure 65: Termination

Select the **Pair Termination** option to enable termination of the offending pair of devices.

To use the **Termination** action, you must enable the **Air Termination System** and the **Policy-based Air Termination System** features. These features can be enabled through the web user interface.

Hover on the **Termination** box to view a synopsis of its configuration.

AP Test

The *AP Test* action runs an AP test using a specific profile if the conditions specified in the **Filters** tab are met.



Note

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

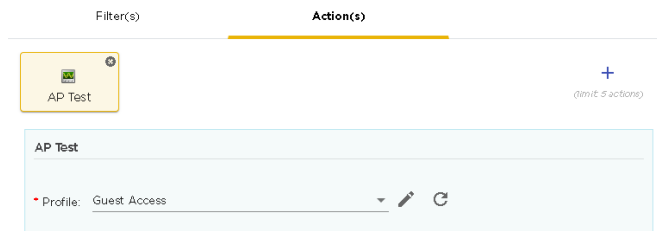



Figure 66: AP Test Configuration

Use the **Profile** drop-down list to select an appropriate AP Test profile. Use the  icon to edit the selected AP Test profile if required.

Hover on the **AP Test** box to view a synopsis of its configuration.

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.

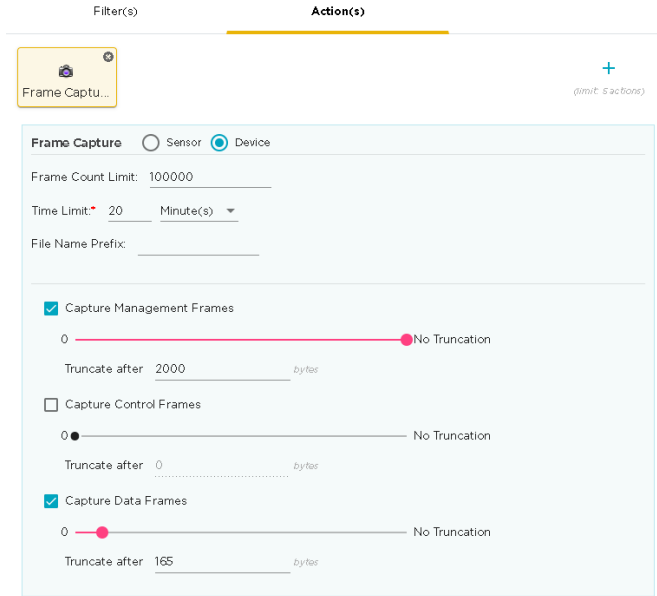


Figure 67: Frame Capture Configuration

Provide the following Frame Capture configuration information:

Field	Description
Frame Capture	Select the scope of the frame capture. Frame capture can be limited to either Sensor or to Device .
Frame Count Limit	Limits the total number of frames to capture for each device category. Use the spinner control to set the value.
Time Limit	Specifies a time duration for the Frame Capture to run. Time can be set in number of minutes or hours. Use the appropriate controls to configure this value.
File Name Prefix	Specifies the prefix for the frame capture file. This prefix along with a number sequence is used to name your frame capture files.
Capture Management Frames	Select to include <i>Management Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Management Frames that will be captured for this instance of frame capture. Capture Management Frames is selected by default.

Field	Description
Capture Control Frames	Select to include <i>Control Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Control Frames that will be captured for this instance of frame capture. Capture Control Frames is not selected by default.
Capture Data Frames	Select to include <i>Data Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Data Frames that will be captured for this instance of frame capture. Capture Data Frames is selected by default.

Hover on the **Frame Capture** box to view a synopsis of its configuration.

Vulnerability Assessment

The *Vulnerability Assessment* action runs a vulnerability assessment test using the specified profile if the conditions defined in the **Filters** tab are met.

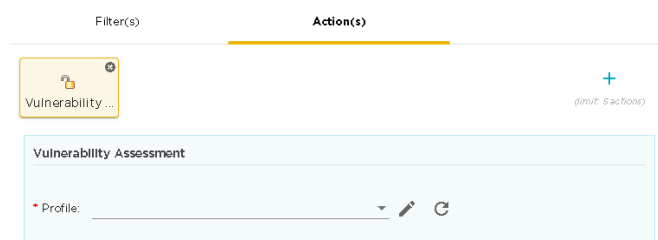



Figure 68: Vulnerability Assessment Configuration

Use the **Profile** drop-down list to select an appropriate Vulnerability Assessment profile. Use the  icon to edit the selected Vulnerability Assessment profile if required.

Hover on the **Vulnerability Assessment** box to view a synopsis of its configuration.

Delete Devices

The *Delete Device* action deletes all devices that meet the conditions specified in the **Filters** tab.

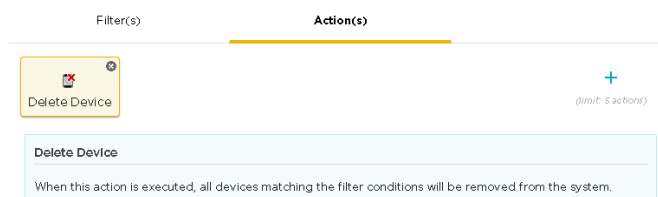


Figure 69: Delete Device Action

There are no configurable parameters for this action.

Email Configuration

The *Email* action enables you to configure the parameters for sending emails when there are some devices that meet the conditions specified in the **Filters** tab.

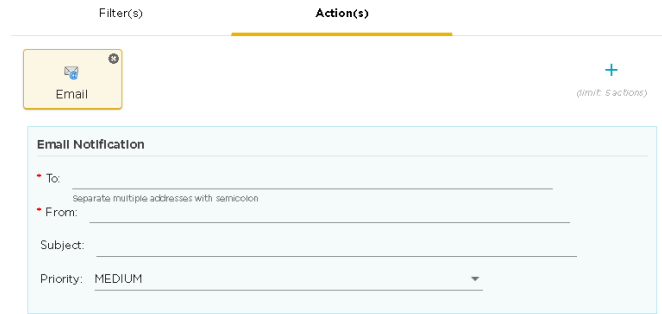


Figure 70: E-Mail Configuration

By default, an empty template is made available for immediate use. Use this empty template to create your first email. To add additional emails, use the green + icon to add a new *Email* action. When you add a new email action, a new block is created for it along with a blank template.

Multiple Emails can be generated for a Device Action Manager rule set.

Hover on the **Email** box to view a synopsis of its configuration.

For each email, provide the following information:

Field	Description
To	The email addresses of the recipients for this email. Add multiple email addresses separated with a semi-colon (;) sign.
From	The email address that is used to send this email. This is the address that will receive any reply mails received from the recipients.
Subject	The subject for this email.
Priority	Use the drop-down list to select the priority of this mail.

Add a New Infrastructure Device Rule Set

Use the **Device Action Manager** screen to add a new infrastructure device rule set. The same screen is used to edit an existing rule set of the same type.

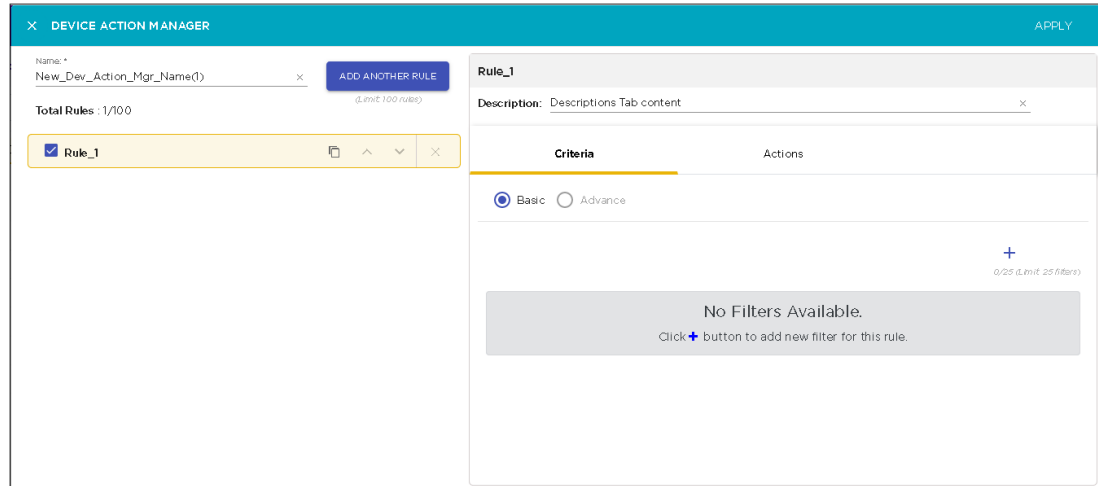


Figure 71: Add a Device Action Manager Rule Set

The actions that you need to perform to add a new Infrastructure Device Action Manager rule set is the same as those that you need to perform to add a new Wireless Clients/BSS rule set. For more information, see [Add a New Wireless Client/BSS Rule Set](#) on page 225.

Configuring Filters

Configure your filters by using logical constructs of AND, OR, and NOT that are available for use when creating and adding multiple filter criteria to your rule. These logical constructs are explained in the topic [Configuring Filters](#) on page 226.

The available filters for Infrastructure devices are:

- DeviceCapabilities
- DeviceDHCP
- DeviceDNS
- DeviceFirmware
- DeviceFirstSeen
- DeviceIP
- DeviceLastDataPoll
- DeviceLastSeen
- DeviceLastStatusPoll
- DeviceMAC
- DeviceManufacturer
- DeviceModel
- DeviceName
- DevicePolledIP
- DeviceSensedIP

- DeviceSerial
- DeviceVendorPrefix.


**Important**

In the Device Action Manager, the order of filters within the rule defines how the filters are applied. For example, if you want create a rule to sanction only BSSs, the first filter should be defined as *DeviceType=Include BSS* before defining other rules such as *DeviceManufacturer* or *DeviceSSID*. Setting the *DeviceType=Include BSS* as the first filter will cause all wireless client devices to be ignored.

Add Actions

Actions are configured from the **Actions** tab. You can specify one or more (up to five (5)) actions that can be performed when the conditions set in the **Filters** tab are met. The valid actions are:

- Clear active alarm - 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 - Automatically corrects configuration compliance violations when conditions specified in the filters are met.
- Live RF / Floor Plan - Automatically updates the heat map predictions in the Live-RF window.
- ACL - Enables the Access Control List on devices that meet the conditions defined in the filter(s).
- Port Suppression - Suppresses communication between unauthorized devices on your network as defined in the filter(s).
- SNMP Trap - Generates SNMP traps when the conditions specified in the filters are met.
- Spectrum Analysis - Runs a Spectrum Analysis or Advanced Spectrum Analysis using the profile specified when the conditions specified in the filters are met.
- Delete Device - Deletes any device from your system that meets the criteria defined in the filter(s).

Use the  icon to add an action to your Device Action Manager Rule Set. You can add up to five (5) rules for each rule set. Configuration settings will be different for each action. For example, the following is the configuration settings when you select *Email* as your action.

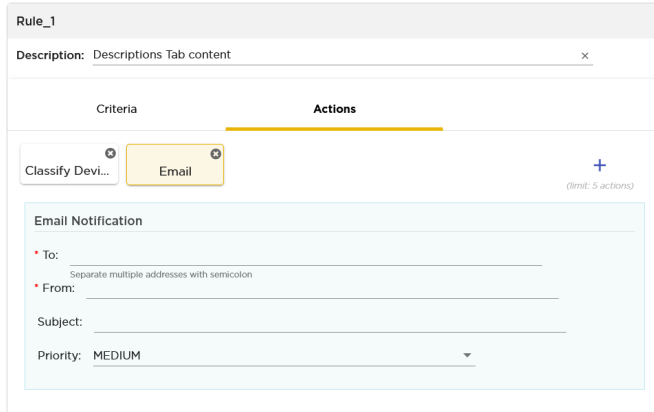


Figure 72: Action - Send Email

The send email action enables to send an email when the conditions specified in the **Filters** tab are met. You can send mails to multiple persons with customized subject, priority, and the email from which this mail is supposed to originate.

When you create an action, its name is added to the top of the **Actions** tab.



To delete a specific action, use the small *x* button located to the top right of the action's name in the tab. When you click the button, the action is immediately removed.

Once you have configured your Device Action Manager Rule Set, click the **APPLY** button located to the top right of this window. The rule is saved and is added to the list of Device Action Manager rule sets.

The following image is of a fully configured Device Action Manager Rule Set.

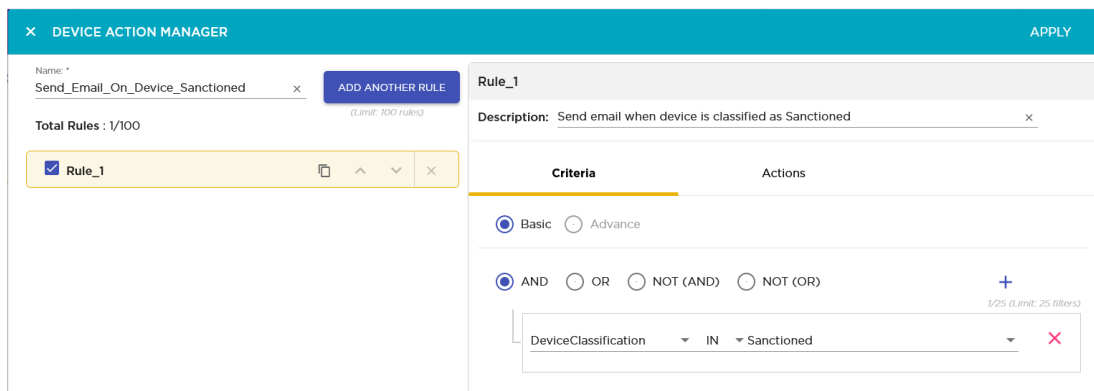


Figure 73: Example Device Action Manager Rule Set

Clear Active Alarms

The *Clear Active Alarms* action enables you to clear all active alarms in your AirDefense system. This action is performed when the conditions specified in the **Filters** tab are met.

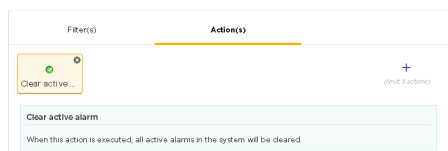


Figure 74: Clear Active Alarms Action

There are no configurable parameters for this action.

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

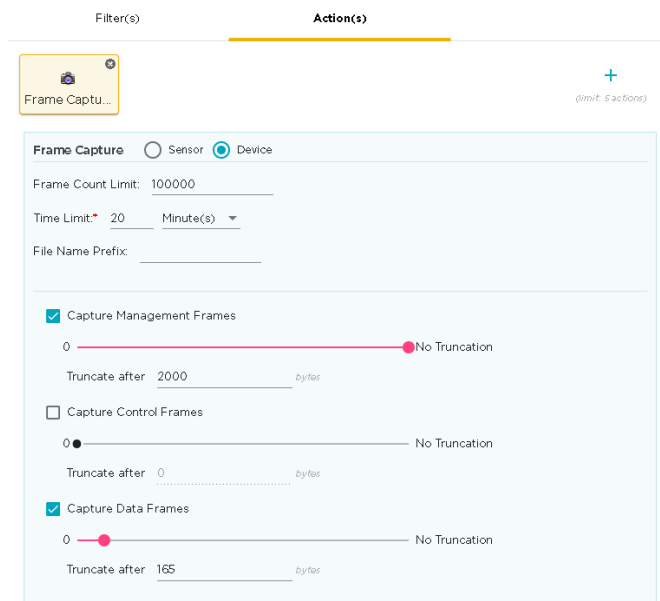


Figure 75: Frame Capture Configuration

Provide the following Frame Capture configuration information:

Field	Description
Frame Capture	Select the scope of the frame capture. Frame capture can be limited to either Sensor or to Device .
Frame Count Limit	Limits the total number of frames to capture for each device category. Use the spinner control to set the value.
Time Limit	Specifies a time duration for the Frame Capture to run. Time can be set in number of minutes or hours. Use the appropriate controls to configure this value.

Field	Description
File Name Prefix	Specifies the prefix for the frame capture file. This prefix along with a number sequence is used to name your frame capture files.
Capture Management Frames	Select to include <i>Management Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Management Frames that will be captured for this instance of frame capture. Capture Management Frames is selected by default.
Capture Control Frames	Select to include <i>Control Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Control Frames that will be captured for this instance of frame capture. Capture Control Frames is not selected by default.
Capture Data Frames	Select to include <i>Data Frames</i> in your frame capture. Use either the slider control or the Truncate After spinner control to set the maximum number of Data Frames that will be captured for this instance of frame capture. Capture Data Frames is selected by default.

Hover on the **Frame Capture** box to view a synopsis of its configuration.

Live RF / Floor Plan

The *Live RF / Floor Plan* action runs an infrastructure device poll to update the heat map predictions in Live RF. This action is performed when the conditions specified in the **Filters** tab are met. The next time the user accesses the Live RF / Floor Plan, they will see the latest updates and will also see whether or not any access points or sensors are offline.

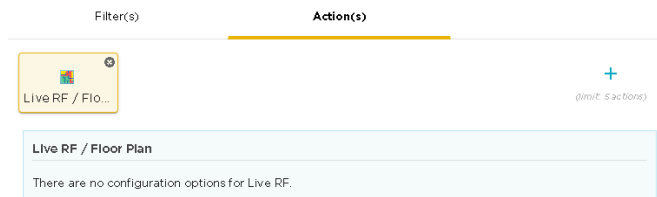


Figure 76: Live RF / Floor Plan Configuration

There are no configurable parameters for this action.

ACL

The **ACL** action enables the Access Control List on devices that meet the conditions specified in the filters.

Use the **Scope Increase Factor** drop-down to select the scope of this action. The value in this field specifies the number of levels to expand the scope of the addition. A value of one (1) means only use the floor level. A value of two (2) indicates that the devices in the floor and its parent level are to be included. And so on. The maximum value that can be set is six (6).

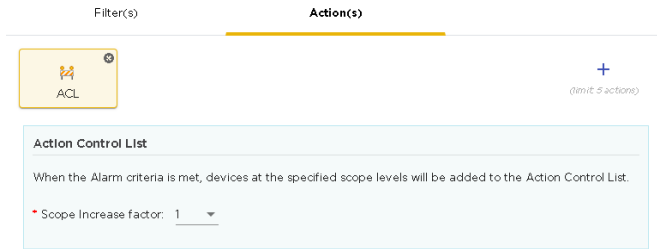


Figure 77: ACL

Hover on the **ACL** box to view a synopsis of its configuration.

Port Suppression

The **Port Suppression** action is used to suppress communication between unauthorized devices and the switches on your network.

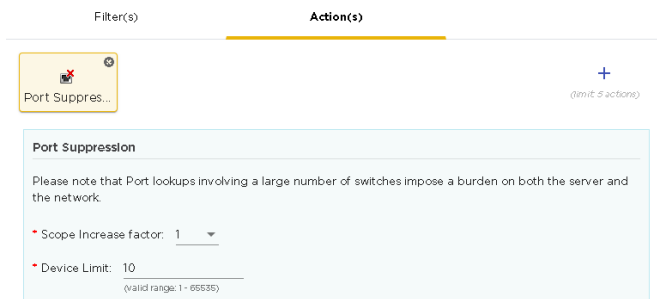


Figure 78: Port Suppression

Use the **Scope Increase Factor** drop-down to select the scope of this action. The value in this field specifies the number of levels to expand the scope of the port suppression action. A value of one (1) means only use the floor level. A value of two (2) indicates that the devices in the floor and its parent level are to be included. And so on. The maximum value that can be set is six (6).

Use the **Device Limit** field to specify a device limit. When a value is specified, for example, ten (10), the port suppression action will not be performed if the number of devices connected to the port exceeds this value.

Hover on the **Port Suppression** box to view a synopsis of its configuration.

SNMP Trap

The *SNMP Trap* action enables sending SNMP traps to your SNMP servers when devices meet conditions specified in the **Filters** tab.

Figure 79: SNMP Trap

By default, an empty template is made available for immediate use. Use this empty template to create your first SNMP Trap. To add additional traps, use the green + icon to create a new SNMP Trap action. When you add a new SNMP Trap action, a new block is created for it along with a new blank template.

Hover on the **SNMP Trap** box to view a synopsis of its configuration.

Multiple SNMP Traps can be generated for a Device Action Manager rule set.

For each SNMP Trap, provide the following information:

Field	Description
Server Address	The IP address of your remote SNMP server.
SNMP Port	The port on which your SNMP server is listening for notifications.
Community String	The community string for the receiving SNMP Server. This string is a series of characters manipulated as a group, in this instance for SNMP.
Transport	Specifies the transport protocol to use for sending the SNMP traps. The available protocols are: <ul style="list-style-type: none"> • UDP (User Datagram Protocol) • TCP (Transmission Control Protocol) In general, UDP is used for transmitting SNMP traps. However, TCP can be used for tunneling the traps over SSL (Secure Sockets Layer).
Max Queue Size	Specifies the maximum queue size for the notifications. Choose a size from the drop-down list.
Send Time	The choices Send SNMP Trap on alarm active , Send SNMP Trap on alarm active, clear, and expire , and Send every <duration> enable configuring when the SNMP traps are sent to the server.

Spectrum Analysis

The *Spectrum Analysis* action runs a regular *Spectrum Analysis* or an *Advanced Spectrum Analysis* using the specified profile if the conditions specified in the **Filters** tab are met.

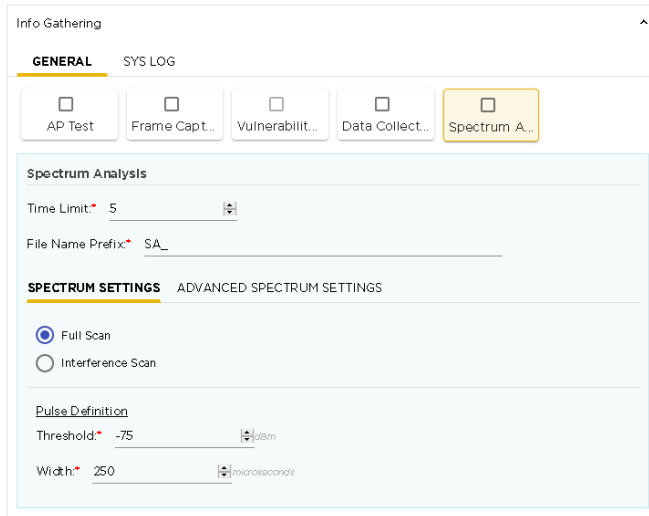


Figure 80: Spectrum Analysis Configuration

Provide the following configuration information.

Field	Description
Time Limit	Specifies a time duration for the Spectrum Analysis to run. Time can be set in number of minutes. Use the spinner control to configure this value.
File Name Prefix	Specifies the prefix for the spectrum analysis file. This prefix is used when creating your spectrum analysis file.
Spectrum Settings	Select this tab for configuring the regular Spectrum Analysis settings.
Advanced Spectrum Settings	Select this tab for configuring the Advanced Spectrum Analysis settings.

Hover on the **Spectrum Analysis** box to view a synopsis of its configuration.

Spectrum Setting

Provide the following configuration information for the normal Spectrum Analysis

Field	Description
Scan Type	Select one of Full Scan or Interference Scan . <ul style="list-style-type: none"> • <i>Full Scan</i> scans the entire 2.4GHz bandwidth (in 5MHz steps) and 5GHz bandwidth (in 20MHz steps) with a short dwell time (around 50 ms). It supports limited classification of interference sources. • <i>Interference Scan</i> scans three frequencies in the 2.4GHz band and three frequencies in the 5GHz band with a longer dwell time (around 500 ms). It supports classification for all interference sources.
Pulse Definition	Defines the values for each pulse when performing Spectrum Analysis. Use the Threshold control to set the pulse threshold value in <i>dBm</i> . Use the Width control to define the gap between two consecutive pulses.

Advanced Spectrum Settings

Provide the following configuration information for the Advanced Spectrum Analysis

Select the scan type. Select one of **Dedicated Scan** or **In-Line Scan**.

- *Dedicated Scan* is a full, detailed spectrum scan.
- *In-Line Scan* is a spectrum scan of all channels except the 802.11 channels and bands.

For each of the above scan types, provide the following configurations:

Field	Description
Scan Time	Defines the scan time in milliseconds. Use the spinner control to set this value. The default value is 1000 milliseconds.
Threshold	For both the 2.4 GHz and 5.0 GHz bands, set the threshold value in <i>dBm</i> .
Duty Cycle Threshold	For both the 2.4 GHz and 5.0 GHz bands, set the duty cycle threshold value in <i>dBm</i> .

Add a New BT/BLE Rule Set

Use the **Device Action Manager** screen to add a new BT/BLE rule. The same screen is also used to edit an existing rule set of the same type.

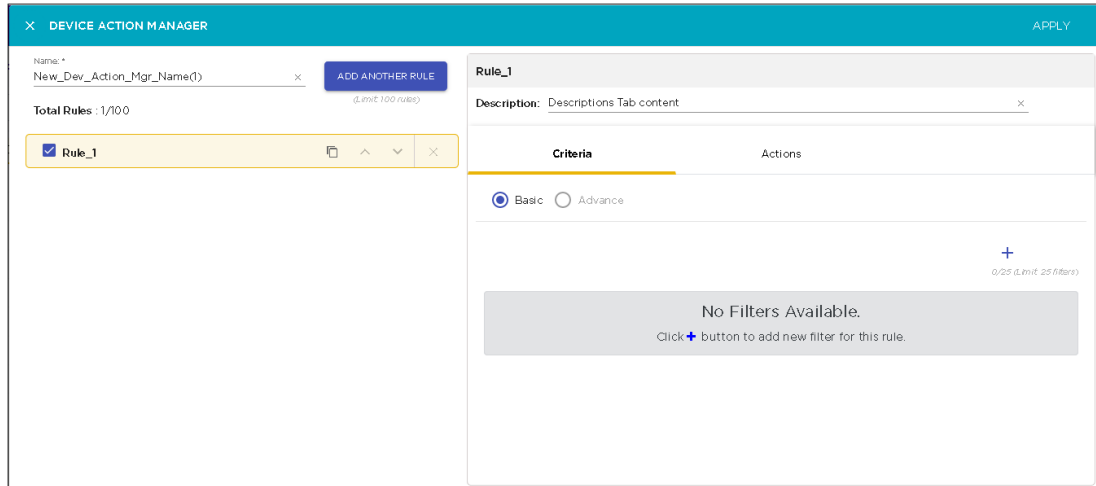


Figure 81: Add a Device Action Manager Rule Set

The actions that you need to perform to add a new BT/BLE Device Action Manager rule set is the same as those that you need to perform to add a new Wireless Clients/BSS rule set. For more information, see [Add a New Wireless Client/BSS Rule Set](#) on page 225.

Configuring Filters

Configure your filters by using logical constructs of AND, OR, and NOT that are available for use when creating and adding multiple filter criteria to your rule. These logical constructs are explained in the topic [Configuring Filters](#) on page 226.

The available filters for BT/BLE devices are:

- BLEType
- DeviceClassification
- DeviceClientType
- DeviceFirstSeen
- DeviceLastSeen
- DeviceMAC
- DeviceManufacturer
- DeviceVendorPrefix
- SignalStrength
- URL
- UUID

Add Actions

Actions are configured from the **Actions** tab. You can specify one or more (up to five (5)) actions that can be performed when the conditions set in the **Filters** tab are met. The valid actions are:

- **Classify Devices** - Classifies devices using the filter(s) to determine which devices are to be classified.
- **Clear active alarm** - Clears any active alarm if the conditions defined in the filter(s) are met.
- **Set Client Type** - Sets the Client Type for BT/BLE devices as defined in the filter(s).
- **Delete Device** - Deletes any device from your system that meets the criteria defined in the filter(s).
- **Email** - Sends an email to the administrator if the conditions defined in the filter(s) are met.

Use the **+** icon to add an action to your Device Action Manager Rule Set. You can add up to five (5) rules for each rule set. Configuration settings will be different for each action. For example, the following is the configuration settings when you select *Email* as your action.

The screenshot shows a configuration window for 'Rule_1'. At the top, there is a 'Description' field with the text 'Descriptions Tab content'. Below this, there are two tabs: 'Criteria' and 'Actions'. The 'Actions' tab is active and highlighted with a yellow underline. In the 'Actions' tab, there are two buttons: 'Classify Devi...' and 'Email'. The 'Email' button is highlighted in yellow. To the right of the 'Email' button is a plus sign icon and the text '(limit: 5 actions)'. Below the buttons, there is a form for 'Email Notification'. The form has four fields: 'To:', 'From:', 'Subject:', and 'Priority:'. The 'Priority' field is set to 'MEDIUM' and has a dropdown arrow. There is a small 'x' icon in the top right corner of the 'Description' field.

Figure 82: Action - Send Email

The send email action enables to send an email when the conditions specified in the **Filters** tab are met. You can send mails to multiple persons with customized subject, priority, and the email from which this mail is supposed to originate.

When you create an action, its name is added to the top of the **Actions** tab.

This is a smaller version of the screenshot above, showing the same configuration window for 'Rule_1' with the 'Actions' tab active and the 'Email' action selected.

To delete a specific action, use the small **x** button located to the top right of the action's name in the tab. When you click the button, the action is immediately removed.

Once you have configured your Device Action Manager Rule Set, click the **APPLY** button located to the top right of this window. The rule is saved and is added to the list of Device Action Manager rule sets.

The following image is of a fully configured Device Action Manager Rule Set.

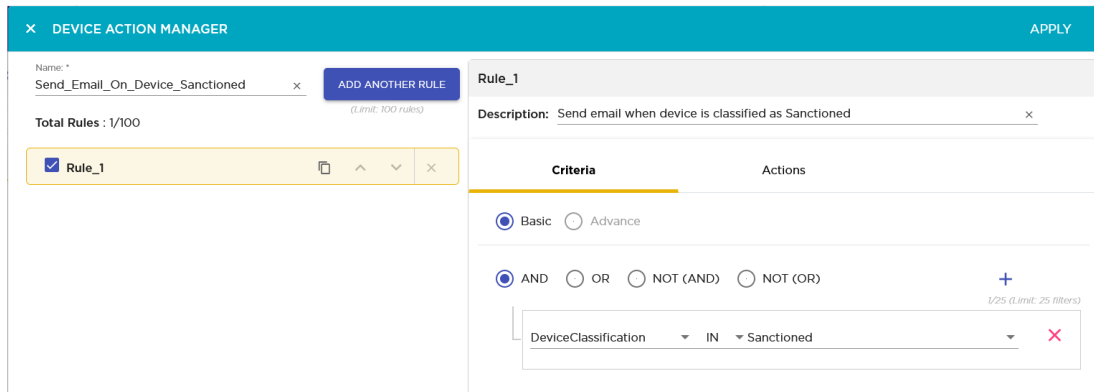


Figure 83: Example Device Action Manager Rule Set

Classify Device Action

The *Classify Device* action enables you to classify a device into various categories if the conditions specified in the **Filters** tab are met.



Figure 84: Classify Device Action

Use the **Classify Devices as** drop-down list to select the device's classification. The devices can be classified as:

- Sanctioned (Inherited Profile) - Devices with Sanctioned (Inherit Profile) classification will inherit all security profiles at device scope level.
- Unsanctioned - Devices will be classified as unsanctioned.
- Neighboring - Devices will be classified as neighboring devices.

Hover on the **Classify Device** box to view a synopsis of its configuration.

Clear Active Alarms

The *Clear Active Alarms* action enables you to clear all active alarms in your AirDefense system. This action is performed when the conditions specified in the **Filters** tab are met.

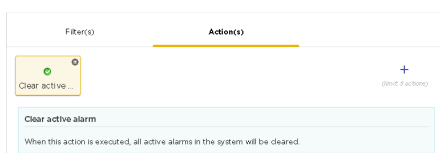


Figure 85: Clear Active Alarms Action

There are no configurable parameters for this action.

Set Client Type Action

The *Set Client Type* action enables you to classify a device as a particular client type. This action is performed when the conditions specified in the **Filters** tab are met.

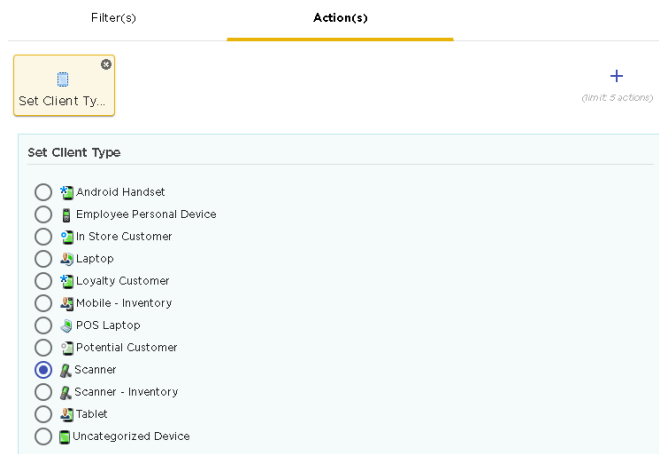


Figure 86: Set Client Type Action

Select the client type to apply to the devices from the list. The items in this list is populated from the **Client Types** screen.

Delete Devices

The *Delete Device* action deletes all devices that meet the conditions specified in the **Filters** tab.

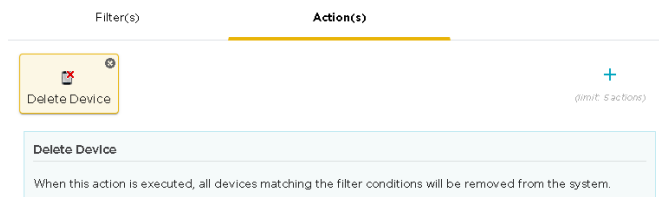


Figure 87: Delete Device Action

There are no configurable parameters for this action.

Email Configuration

The *Email* action enables you to configure the parameters for sending emails when there are some devices that meet the conditions specified in the **Filters** tab.

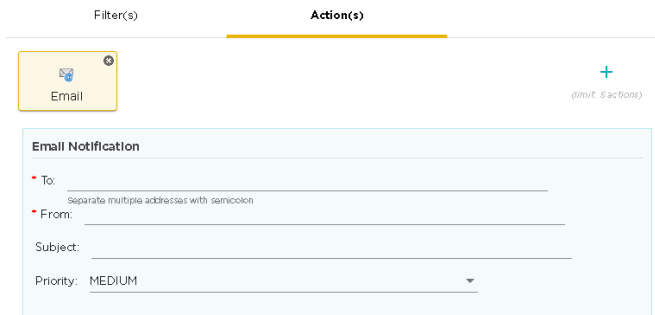


Figure 88: E-Mail Configuration

By default, an empty template is made available for immediate use. Use this empty template to create your first email. To add additional emails, use the green + icon to add a new *Email* action. When you add a new email action, a new block is created for it along with a blank template.

Multiple Emails can be generated for a Device Action Manager rule set.

Hover on the **Email** box to view a synopsis of its configuration.

For each email, provide the following information:

Field	Description
To	The email addresses of the recipients for this email. Add multiple email addresses separated with a semi-colon (;) sign.
From	The email address that is used to send this email. This is the address that will receive any reply mails received from the recipients.
Subject	The subject for this email.
Priority	Use the drop-down list to select the priority of this mail.

Apply or Run the Device Action Manager Rule Sets

Device Action Manager Rule Sets can be run manually or by being applied to your network hierarchy.

When run manually, you can choose the Device Action Manager Rule Sets to run.

When applied to your network using the **Structure & Tags** pane, Device Action Manager Rule Sets are automatically run.

Apply Device Action Manager Rule Sets

Device Action Manager Rule Sets are applied to your network using the **Structure & Tags** pane. The section *Overriding Configuration Settings* in this topic provides a brief description of how permissions and configurations are inherited throughout the AirDefense managed network.

To apply a Device Action Manager Rule Set to any level of the AirDefense network tree, navigate to that level in the hierarchy using the **Structure & Tags** pane.

Select the **Override** option to indicate that you are overriding the inherited configurations starting at this level. The rules that are inherited from this level's parent level are enabled.

Use the option control before each rule to include or exclude it from being applied at this level in the AirDefense hierarchy. These rules will be inherited and applied to all levels that are below this level in the AirDefense hierarchy.

Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to *ON*. The top most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.


By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

Run Device Action Manager Rule Sets Manually

Device Action Manager Rule Sets can be run manually on demand. Use the  icon located to the top right of the Device Action Manager screen.

The **Action Rules on Demand** dialog displays.

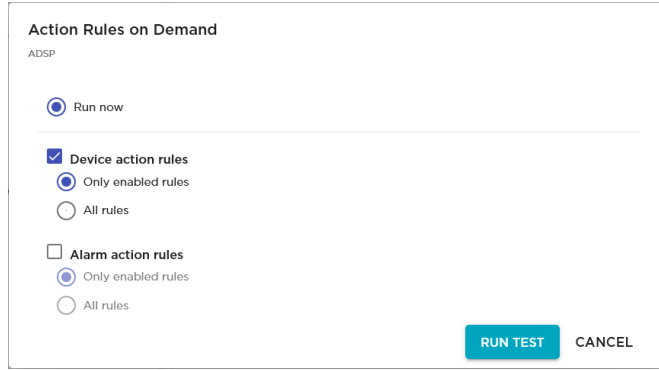


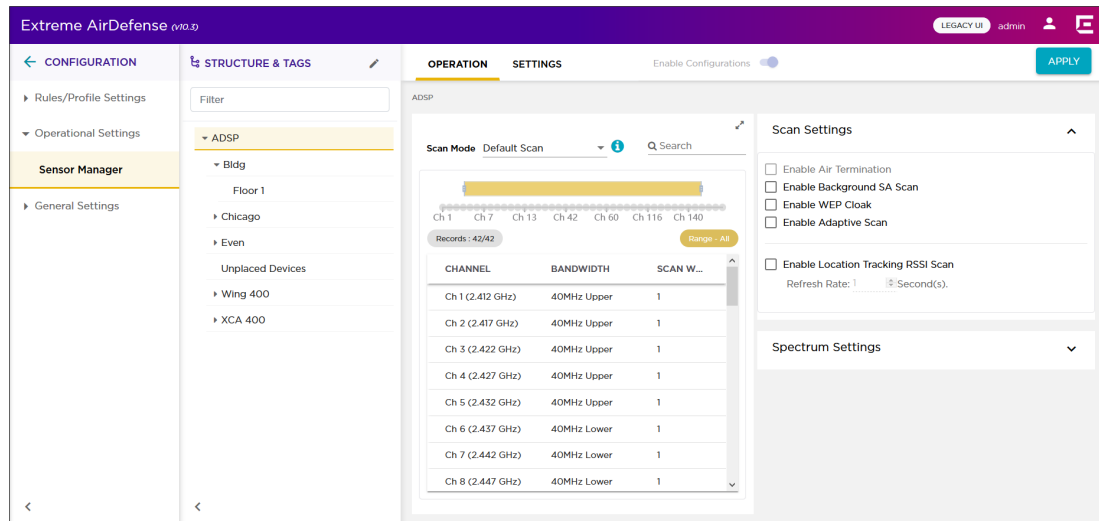
Figure 89: Run Rules On Demand Screen

By default, the **Device action rules** option is selected. Select this option if not selected. You can choose to run only the enabled rules or run all the rules, enabled or disabled. Use the appropriate choice control.

To run the selected rules, click the **RUN TEST** button. On successful completion, a message is displayed. Similarly, if some of your rules fail to execute, an error message is displayed.

Sensor Manager

Use the **Sensor Manager** screen to configure sensor operation mode, channel scan, sensor appliance, and other sensor related settings.



The screen combines the settings that were managed from the **Configuration > Sensor Only Settings** and the **Configuration > Sensor Operation** screens of the legacy user interface.

Operation Tab

The **Sensor Operation** tab of the **Sensor Manager** screen enables you to configure the following parameters.

- Scan Mode - Use the **Scan Mode** control to configure the different scan parameters. For more information, see [Scan Mode Settings](#) on page 255.
- Scan Settings - Use the **Scan Setting** control to configure the various parameters for scanning for devices. For more information, see [Scan Settings](#) on page 260.
- Spectrum Settings - Use the **Spectrum Settings** control to set the threshold values for the two radio bands. For more information, see [Spectrum Settings](#) on page 261.

For more information, see [Operation Tab](#) on page 255.

Settings Tab

The **Settings** tab of the **Sensor Manager** screen enables you to create and manage *Sensor Profiles*. Sensor profiles are a set of sensor configurations that can be applied to any stand-alone sensor (a sensor that is not adopted by any controller) managed by your AirDefense server. For more information, see [Settings Tab](#) on page 262.

Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to *ON*. The top most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

Operation Tab

The following operations can be performed from the **Operation** tab of the **Sensor Manager** screen.

- **Scan Mode** - Use this control to set the channels to scan for unsanctioned devices. AirDefense provides a comprehensive list of scan modes that you can apply to your AirDefense managed network.
- **Scan Settings** - Use this control to set the various parameters associated with scanning and other security related settings.
- **Spectrum Settings** - Use this control to set the threshold values for *Advance Spectrum Analysis* In-Line based scans.

Scan Mode Settings

Use the **Scan Mode** control to choose the channels to monitor for rogue devices. AirDefense provides a set of preconfigured list of channels to scan.

The following pre-configured scan modes are available for use:

- *Default Scan* - This is list of channels that are scanned by default. This list consists of all the standard channels in both the 2.4 GHz and 5.0 GHz bands. This list cannot be edited.
- *Extended Channel Scan* - This list consists of all the standard channels in the 2.4 GHz and 5.0 GHz bands and also includes the extended channels in these bands. This list cannot be edited.
- *Extended and Emergency Channel Scan* - This list consists of all standard, extended, and emergency channels in both the 2.4 GHz and 5.0 GHz bands. This is most comprehensive of all the pre-configured scans. This list cannot be edited.
- *Custom Scan* - This list consists of all standard, extended, and emergency channels in both the 2.4 GHz and 5.0 GHz bands. This list allows you to select those channels that you wish to scan.
- *Channel Lock* - This list enables you to select a particular channel to scan. When selected, the scan is locked to the selected channel.

To set your **Scan Mode** configuration:

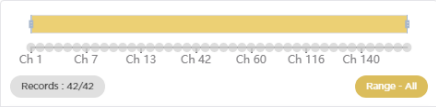
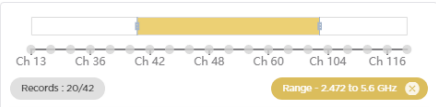
1. Select the appropriate **Scan Mode** from the drop-down list.
Depending on the selection, the list of available channels changes.

Scan Mode: Default Scan 🔍 Search

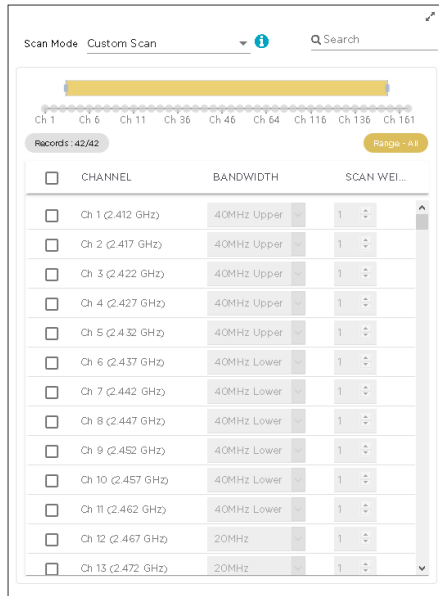
Records: 42/42 Page: 1/1

CHANNEL	BANDWIDTH	SCAN WEIG...
Ch 1 (2.412 GHz)	40MHz Upper	1
Ch 2 (2.417 GHz)	40MHz Upper	1
Ch 3 (2.422 GHz)	40MHz Upper	1
Ch 4 (2.427 GHz)	40MHz Upper	1
Ch 5 (2.432 GHz)	40MHz Upper	1
Ch 6 (2.437 GHz)	40MHz Lower	1
Ch 7 (2.442 GHz)	40MHz Lower	1
Ch 8 (2.447 GHz)	40MHz Lower	1
Ch 9 (2.452 GHz)	40MHz Lower	1
Ch 10 (2.457 GHz)	40MHz Lower	1
Ch 11 (2.462 GHz)	40MHz Lower	1
Ch 12 (2.467 GHz)	20MHz	1
Ch 13 (2.472 GHz)	20MHz	1

This control displays the following additional information for your **Scan Mode** selection.

Field	Description																																				
<p>Channel Range Bar</p>	<p>The channel range bar control enables you to narrow down the range of channels to those channels you are interested in.</p>  <p>Use the small rectangular handles at the vertical edges of the bar to narrow down your selection of channels. The number of records shown in the Records control changes to reflect the number of channels that you have selected. The Range control changes to show the radio frequency range of the channels that you have selected.</p>  <p>You can also click and drag the yellow bar to slide the bar within the control. Sliding the bar selects the appropriate channels within the bar's coverage. To reset your channel selection, click the small x located to the right of the Range control. This resets your channel selection immediately.</p>																																				
<p>Records</p>	<p>This control displays the number of records displayed for your current scan mode selection and the number of channels that have been selected based on your filter.</p>																																				
<p>Channel List</p>	<p>This field displays the channels for your current Scan Mode and the filter (if any) that you have applied to narrow down your channel selection.</p> <table border="1" data-bbox="716 1335 1149 1759"> <thead> <tr> <th>NAME</th> <th>WIDTH</th> <th>WEIGHT</th> </tr> </thead> <tbody> <tr><td>Ch 1 (2.412 GHz)</td><td>40MHz Upper</td><td>1</td></tr> <tr><td>Ch 2 (2.417 GHz)</td><td>40MHz Upper</td><td>1</td></tr> <tr><td>Ch 3 (2.422 GHz)</td><td>40MHz Upper</td><td>1</td></tr> <tr><td>Ch 4 (2.427 GHz)</td><td>40MHz Upper</td><td>1</td></tr> <tr><td>Ch 5 (2.432 GHz)</td><td>40MHz Upper</td><td>1</td></tr> <tr><td>Ch 6 (2.437 GHz)</td><td>40MHz Lower</td><td>1</td></tr> <tr><td>Ch 7 (2.442 GHz)</td><td>40MHz Lower</td><td>1</td></tr> <tr><td>Ch 8 (2.447 GHz)</td><td>40MHz Lower</td><td>1</td></tr> <tr><td>Ch 9 (2.452 GHz)</td><td>40MHz Lower</td><td>1</td></tr> <tr><td>Ch 10 (2.457 GHz)</td><td>40MHz Lower</td><td>1</td></tr> <tr><td>Ch 11 (2.462 GHz)</td><td>40MHz Lower</td><td>1</td></tr> </tbody> </table> <p>The fields in this control are not editable.</p>	NAME	WIDTH	WEIGHT	Ch 1 (2.412 GHz)	40MHz Upper	1	Ch 2 (2.417 GHz)	40MHz Upper	1	Ch 3 (2.422 GHz)	40MHz Upper	1	Ch 4 (2.427 GHz)	40MHz Upper	1	Ch 5 (2.432 GHz)	40MHz Upper	1	Ch 6 (2.437 GHz)	40MHz Lower	1	Ch 7 (2.442 GHz)	40MHz Lower	1	Ch 8 (2.447 GHz)	40MHz Lower	1	Ch 9 (2.452 GHz)	40MHz Lower	1	Ch 10 (2.457 GHz)	40MHz Lower	1	Ch 11 (2.462 GHz)	40MHz Lower	1
NAME	WIDTH	WEIGHT																																			
Ch 1 (2.412 GHz)	40MHz Upper	1																																			
Ch 2 (2.417 GHz)	40MHz Upper	1																																			
Ch 3 (2.422 GHz)	40MHz Upper	1																																			
Ch 4 (2.427 GHz)	40MHz Upper	1																																			
Ch 5 (2.432 GHz)	40MHz Upper	1																																			
Ch 6 (2.437 GHz)	40MHz Lower	1																																			
Ch 7 (2.442 GHz)	40MHz Lower	1																																			
Ch 8 (2.447 GHz)	40MHz Lower	1																																			
Ch 9 (2.452 GHz)	40MHz Lower	1																																			
Ch 10 (2.457 GHz)	40MHz Lower	1																																			
Ch 11 (2.462 GHz)	40MHz Lower	1																																			

- On selecting Custom Scan in the **Scan Mode** control, the **Channel List** control becomes editable.

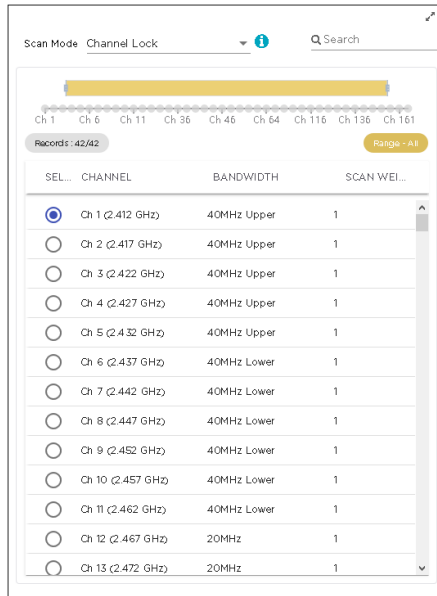


The following fields become available for further configuration.

Field	Description
Channel	This field displays the channel's number and its frequency. This field cannot be changed.
Bandwidth	Use the drop-down list to select the channel's bandwidth. The available bandwidths depend on the channel's frequency.
Scan Weight	<p>This field indicates the number of times the channel is scanned in a scan cycle. A scan cycle is considered complete when each channel in the scan mode is scanned at least once.</p> <p>Note: By default, each channel is scanned for 1 second in each cycle.</p> <p>When this value is set to 1 or more, it indicates the number of times the channel is scanned in a scan cycle. 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, then the channel scan sequence is 1-5-6-11-1-6-11-6-11.</p> <p>When this value is set to a value that is < 1, it indicates that the channel must be scanned for the set fraction of a second.</p>

By default, all channels are selected for scanning. You can use the check box next to the **Channel** control to select or unselect all the channels listed in this control. Use the check box next to each channel in this list to either scan or prevent this channel from being scanned in each scan cycle.

- On selecting Channel Lock in the **Scan Mode** control, the **Channel List** control becomes editable.



Note

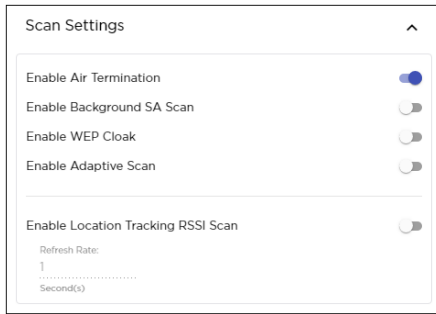
You can only select one channel at a time for this scan mode.

Use the option control next to the channel's name to lock the channel scan to that particular channel. You cannot select multiple channels for this scan mode. The **Width** and **Weight** parameters cannot be modified.

Scan Settings

The settings in the **Scan Settings** control additional scan parameters.

Set the following parameters



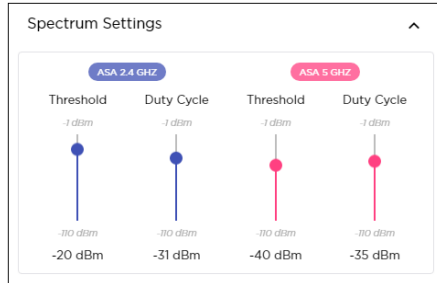
Field	Description
Enable Air Termination	Air Termination lets you terminate the connection between your wireless LAN and any access point or station associated with it. By default, Air Termination is disabled. It can only be enabled in the Appliance Manager.
Enable Background SA Scan	Spectrum Analysis (SA) can be run as a background process. Use this switch to run SA as a background process. By default, background scans are 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.
Enable Location Tracking RSSI Scan	Devices can report RSSI scan data to AirDefense. This option allows you to use that data in location tracking these devices. Once this option is selected, you can adjust the location tracking refresh rate from 1 to 60 seconds in the Refresh Rate control. The optimal rate is 1 second. (You must have a Proximity and Analytics license before this option is visible.)

Spectrum Settings

The **Spectrum Settings** control in the **Sensor Manager** screen controls the *Advanced Spectrum Analysis (ASA)* configuration parameters.

Set the following parameters:

The settings in this control are for the *Advanced Spectrum Analysis In-Line* based scan. They are not for the *Dedicated* scan. Four settings are available for configuration, two (2) each for the 2.4 GHz and 5.0 GHz bands. The values in these fields are the default settings for these bands. These settings will work for normal use and they should not have to be changed.



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

Settings Tab

The **Settings** tab of the **Sensor Manager** screen lets you create and manage *Sensor Profiles*. Sensor profiles are a set of sensor configurations that can be applied to any sensor or a group of sensors managed by your AirDefense server.

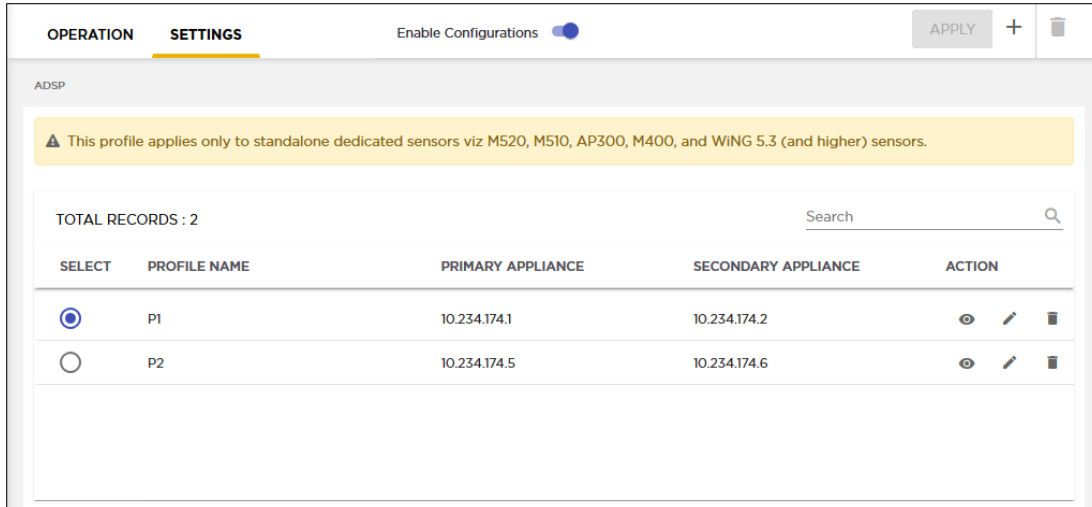
Sensor profiles can be created, modified, and deleted using this screen.



Important

These policies are applicable to stand alone, dedicated sensors such as *M520*, *M510*, *AP300*, *M400* and those sensors that support Extreme Networks WiNG 5.3 version and higher firmware.

Select the **Settings** tab to load the **Settings** screen.



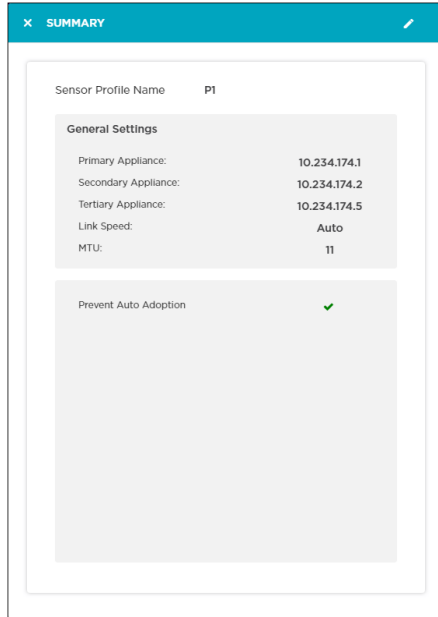
The following information is displayed for each sensor profile.

Field	Description
Select	Use this option control to select the current sensor profile and apply it to the scope selected in the Structure & Tags control.
Profile Name	Displays the name of the sensor profile.
Primary Appliance	Displays the IP address of the primary AirDefense appliance.
Secondary Appliance	Displays the IP address of the secondary AirDefense appliance.
Created On	Displays the timestamp when this sensor profile was created.
Actions	<p>The icons in this field enable to manage your sensor profile. You can edit your profile, create a new profile, and delete the profile.</p> <p>The following actions can be performed:</p> <ul style="list-style-type: none"> View Profile - Use the icon to view this sensor profile. For more information, see View Sensor Profile on page 263 Edit Profile - Use the icon to edit the sensor profile. A configuration dialog displays where you can edit and update the sensor profile. For more information, see Add a Sensor Profile on page 264. Delete Profile - Use the icon to delete the selected sensor profile. For more information, see Delete a Sensor Profile on page 267

View Sensor Profile

To view a sensor profile:

- Select the icon next to the profile that you wish to view.
- The profile opens in a dialog.

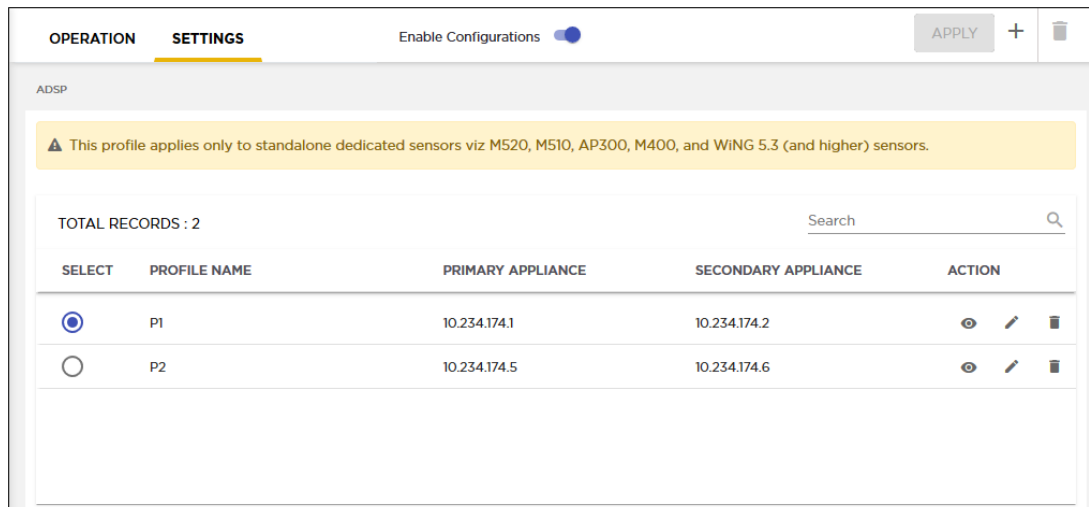


For each profile, the following information is displayed.


Field	Description
Sensor Profile Name	The sensor profile's name.
Primary Appliance	The IP address for the primary AirDefense appliance. This is the IP address of the AirDefense server which sensors will attempt connecting to first.
Secondary Appliance	The IP address for the secondary AirDefense appliance. This is the IP address of the AirDefense server, which sensors will try connecting to, if the attempt to connect to the <i>Primary Appliance</i> fails.
Tertiary Appliance	The IP address for the tertiary AirDefense appliance. This is the IP address of the AirDefense server, which sensors will try connecting to, when attempts to connect to the <i>Primary Appliance</i> and the <i>Secondary Appliance</i> fail.
Link Speed	The link speed for the Ethernet interface. This value can be one of auto negotiate (default), 10Mbps (Full Duplex or Half Duplex), or 100Mbps (Full Duplex or Half Duplex).
MTU	The <i>Maximum Transmission Unit</i> value for your interface.
Prevent Auto Adoption	Displays a green check mark when enabled. Displays a red 'x' mark when disabled. When enabled, auto adoption of sensors is prevented.

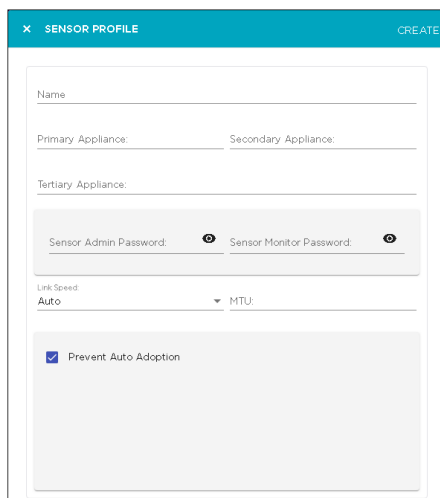
Add a Sensor Profile

Sensor profiles are a set of sensor configurations that can be applied to a sensor or a group of sensors.



To add a new sensor profile:

1. From the **Settings** screen, select the  icon located to the top right. The **Sensor Profile** dialog displays.



2. Provide the following information to create a new sensor profile:

Field	Description
Name	Provide a meaningful name for the sensor profile. You should name your profile such that it is easy to identify the profile from among similar profiles.
Primary Appliance	Provide the IP address for the primary AirDefense appliance. This is the IP address of the AirDefense server which the sensors will attempt connecting to first.
Secondary Appliance	Provide the IP address for the secondary AirDefense appliance. This is the IP address of the AirDefense server, which sensors will attempt to connect to, if the attempt to connect to the <i>Primary Appliance</i> fails.

Field	Description
Tertiary Appliance	Provide the IP address for the tertiary AirDefense appliance. This is the IP address of the AirDefense server, which sensors try connecting to, when attempts to connect to the <i>Primary Appliance</i> and the <i>Secondary Appliance</i> fail.
Sensor Admin Password	Enter the password to the account that has <i>Sensor Administration</i> privilege on your sensors. This is a mandatory field.
Sensor Monitor Password	Enter the password to the account that has <i>Sensor Monitoring</i> privilege on your sensors.
Link Speed	Select the link speed. <i>Link Speed</i> control enables you to set the Ethernet interface to one of auto negotiate (default), fix interface speeds to 10Mbps (Full Duplex or Half Duplex), or to fix interface speeds to 100Mbps (Full Duplex or Half Duplex). Use the drop-down list to select the link speed.
MTU	Sets the <i>Maximum Transmission Unit</i> value for your interface. Use the spinner control to set the MTU value.
Prevent Auto Adoption	Select this option to prevent a sensor from being adopted by a switch.

3. Select the **CREATE** button located to the top right of this dialog to save your sensor profile.
4. Select the small 'x' icon to the top left of the dialog to close it.

Edit a Sensor Profile


Sensor profiles are a set of sensor configurations that can be applied to a sensor or a group of sensors.

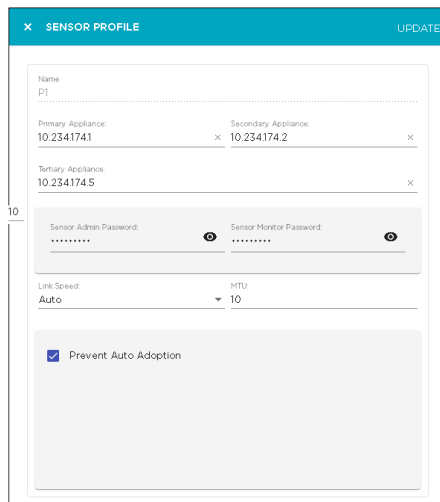
The screenshot shows the 'SETTINGS' tab in the ADSP interface. At the top, there are tabs for 'OPERATION' and 'SETTINGS', and a toggle for 'Enable Configurations'. An 'APPLY' button and a trash icon are also visible. A yellow warning banner states: 'This profile applies only to standalone dedicated sensors viz M520, M510, AP300, M400, and WING 5.3 (and higher) sensors.' Below this, a table displays sensor profiles. The table has columns for 'SELECT', 'PROFILE NAME', 'PRIMARY APPLIANCE', 'SECONDARY APPLIANCE', and 'ACTION'. Two profiles are listed: P1 and P2.

SELECT	PROFILE NAME	PRIMARY APPLIANCE	SECONDARY APPLIANCE	ACTION
<input checked="" type="radio"/>	P1	10.234.174.1	10.234.174.2	
<input type="radio"/>	P2	10.234.174.5	10.234.174.6	

To edit an existing sensor profile:

1. From the **Settings** screen, select the sensor profile to edit.

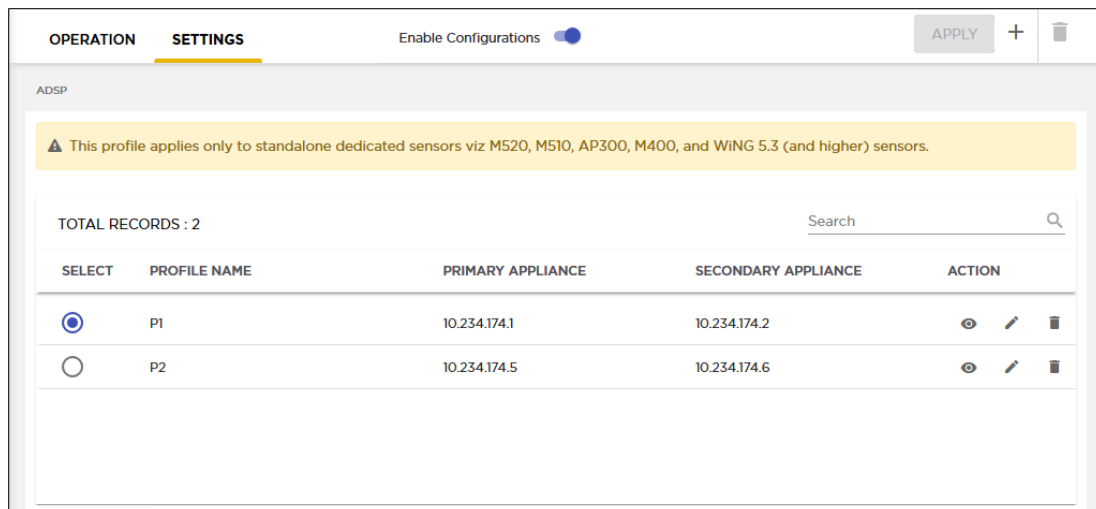
2. Select the  icon to edit the selected sensor profile.
The **Sensor Profile** dialog displays.









3. Modify the required fields.
For more information on the fields of this screen, see [Add a Sensor Profile](#) on page 264
4. Select the **UPDATE** button located to the top right of this dialog to save your modified sensor profile.
5. Select the small 'x' icon to the top left of the dialog to close it.

Delete a Sensor Profile


Sensor profiles are a set of sensor configurations that can be applied to a sensor or a group of sensors.

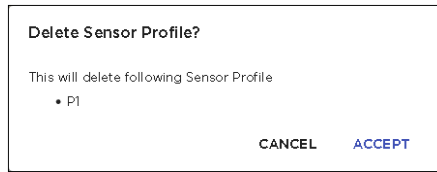


SELECT	PROFILE NAME	PRIMARY APPLIANCE	SECONDARY APPLIANCE	ACTION
<input checked="" type="radio"/>	P1	10.234.174.1	10.234.174.2	  
<input type="radio"/>	P2	10.234.174.5	10.234.174.6	  

To delete a sensor profile:

1. From the **Settings** screen, select the sensor profile to edit.

2. Select the  icon to delete the selected sensor profile.
The **Delete Sensor Profile** dialog displays.



3. Review the information displayed in this dialog.
4. Select **ACCEPT** button to delete the selected sensor profile.

Alarm Configuration

The **Alarm Configuration** screen lists all the alarms that are generated within the Extreme AirDefense system. Alarms are broadly classified into the following categories. Some of these categories are further sub divided.

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

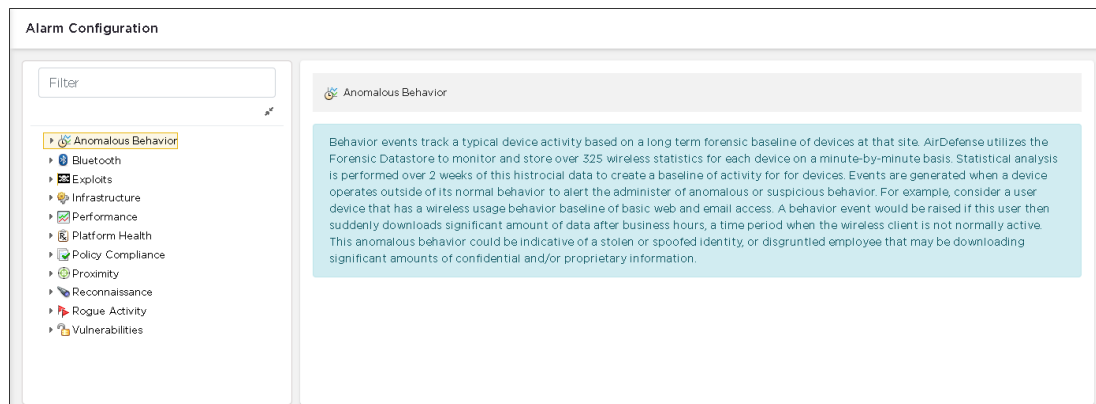



Figure 90: Alarm Configuration Screen

A detailed description of the alarm category is displayed for each category or sub-category of alarms in the right pane.

Use the  icon located before each category to expand that category and to view the alarms under that category.

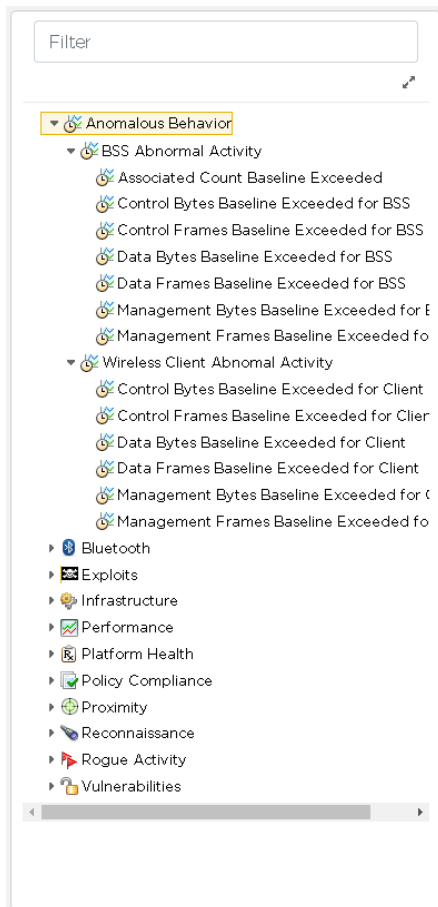


Figure 91: Expanded Alarm Category

Select an alarm to view its configuration fields in the **Alarm Configuration Screen**. Each alarm has its own set of parameters that can be modified to meet your requirements. The following is the set of configuration for the **Anomalous Behaviour > BSS Abnormal Activity > Associated Count Baseline Exceeded** alarm.

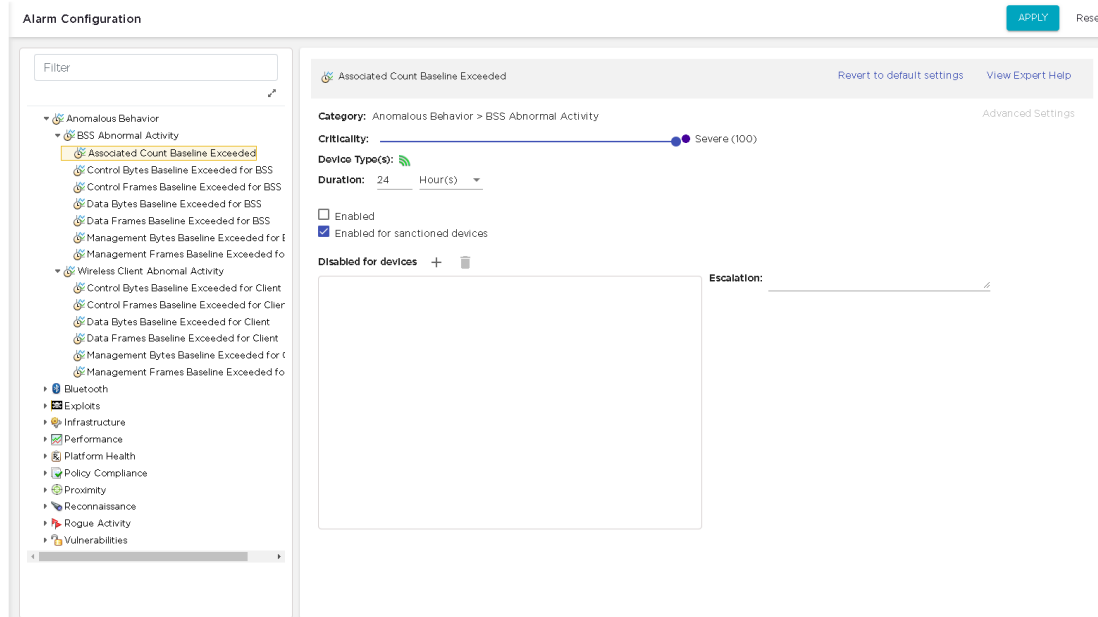


Figure 92: Alarm Configuration Settings

Use the **Revert to default settings** link to revert the configuration of the alarm to its defaults. Use this link in case you are not satisfied with the current settings for this particular alarm.

Use the **View Expert Help** link to view in-depth information for this alarm. When selected, the alarm's details are displayed in a separate browser tab or window. The following is the **Expert Help** screen for the **Anomalous Behaviour > BSS Abnormal Activity > Associated Count Baseline Exceeded** alarm.

AirDefense Services Platform

Associated Count Baseline Exceeded

- [Description](#)
- [Investigation](#)
- [Mitigation](#)

While AirDefense Enterprise is monitoring all wireless devices operating in the airspace, it is collecting 300 wireless data statistics per device every minute and storing them in the intelcenter's datastore. This collected information is then used to create a behavioral baseline for each of these devices that is always based upon the device's wireless activity from the last four weeks. The baseline will then be used as a reference to detect any abnormal activity that falls outside the realm of the device's expected wireless behavior. Deviations from the baseline will result in the generation of a behavior.

Reason for abnormal behavior include:

Wireless activity outside of typical working hours

Excessive data transmissions -- Significant transfer of information from or to the wired network.

Client Software/Hardware issues. Unusual management frame transmissions from a device may be the result of malfunctioning hardware or software.

Figure 93: Expert Help

To save the changes made to an alarm's configuration, use the **APPLY** button located to the top right of the screen. The alarm's configuration is immediately updated.

The **Reset** button located next to the **APPLY** button is used to revert any changes that you have made to the alarm's configuration. The previous settings are restored. This

action is different from the **Revert to default settings** action, where the alarm's default configuration is restored.

Wired Network Monitoring

Wired Network Monitoring is used to monitor the wired network devices in your Extreme AirDefense monitored system. Use this screen to generate generate alarms for your wired network by selecting any of the following conditions:

- New device detected on the wired network - This option is enabled by default. When selected, an alarm is generated when a new device is detected on the wired side of your Extreme AirDefense managed network.

Using the **Known Vendors** button, you can select the wired equipment vendors of devices that are commonly used in your network. When a device of a vendor found in the list is added to the wired network, the system will generate an alarm of lower severity than that is normally generated.

- Sanctioned wired device detected at different location in tree hierarchy than when originally discovered - Select this option to generate an alarm when a device has moved to a different location in your Extreme AirDefense tree hierarchy from where it was originally discovered when it was first added to the system.
- Sanction device no longer observed. - Select this option to generate an alarm when a sanctioned device is not observed in your wired network. You must specify a minimum time for the device to have not been seen on your network for this alarm to be generated. Use the **Minimum not seen time** control and its associated spinner control to set the time duration.

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

Figure 94: Wired Network Monitoring Screen

It is recommended to enable **Wired Network Monitoring** at the appliance level by selecting the **Enable Configurations** switch. When you do, all the other network levels are also monitored.

If you need to monitor a specific level in your Extreme AirDefense hierarchy, navigate to the level in the **Structure & Tags** pane and select it. Use the

Override Inherit from: ADSP

control's **Override** option to monitor this level and all the levels below it. Customize the monitoring options to meet your requirements.

For more information on overriding, see the section *Overriding Configuration Settings* in this document.

Network PCI Compliance Monitoring

Use the **Set Network PCI Scope** button to add VLANs to be monitored for PCI compliance. When this button is selected, the **Network PCI Scope** screen displays.

Figure 95: Network PCI Compliance Screen

Use the **Add VLANs to PCI scope** field to enter the VLAN that has to be monitored. Select the **+** icon next to this field to add this VLAN to the list below. You can add multiple VLANs to monitor for PCI compliance. Once you have added all the VLANs, click the **OK** button to save your changes.

Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to *ON*. The top most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

Performance Profile

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.

Performance Profiles are managed from the **Performance Profile** screen.

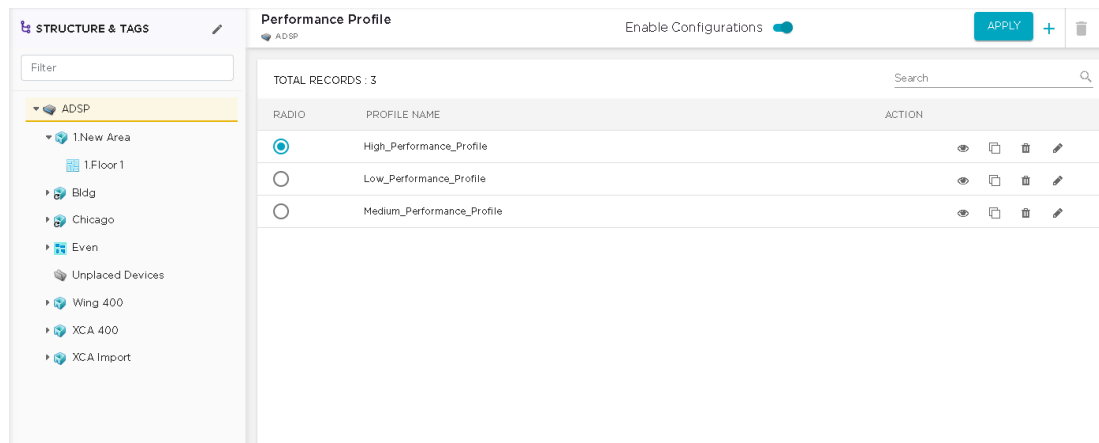


Figure 96: Performance Profile Screen

View Performance Profile

Use the **Performance Profile** screen to view a list of all performance profiles configured for this Extreme AirDefense system.

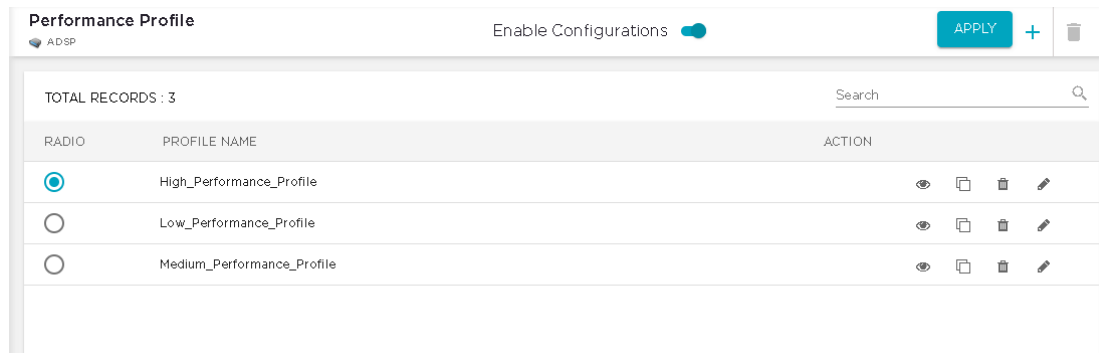







Figure 97: Performance Profiles Screen

The screen displays the following information:

Field	Description
Profile Name	The name of the Performance Profile.
Action	<p>The actions that can be performed on the Performance Profile. The icons in this field enable you to manage your profile. You can edit the profile, create a new one by creating a duplicate of an existing rule set, or delete it. The following actions can be performed:</p> <ul style="list-style-type: none"> • View - To view a Performance Profile, use the  icon for the profile. The details for this profile is displayed in a separate dialog. • Duplicate - Use the  icon to create a duplicate of the selected Performance Profile. A duplicate of this profile is created and the configuration dialog displays the newly created Performance Profile. Customize the duplicate profile further to meet your requirements. • Delete - Use the  icon to delete the selected Performance Profile. • Edit - Use the  to edit the Performance Profile. A configuration dialog displays where you can make changes to the selected profile.

Add Performance Profile

A Performance Profile is a set of parameters the define the threshold of performance of the BSS and wireless devices in your Extreme AirDefense system. A performance alarm is generated if the performance threshold for the selected profile are exceeded. No alarms are generated if no Performance Profiles are applied to your system.

New Performance Profiles are created from the **Performance Profiles** screen. Use the  icon to add a new Performance Profile. The same screen is also used to edit an existing profile.

The screenshot shows a configuration window titled "PERFORMANCE PROFILE" with an "APPLY" button in the top right and a close "X" button in the top left. The window contains four tabs: "General", "Cumulative", "Wireless Clients", and "BSS". The "General" tab is active. Below the tabs is a form with the following fields:

- Profile Name: (with a close "x" button)
- Short Slot Time Enabled:
- Allow Streaming Traffic:
- Protection Mode Enabled:

Figure 98: Performance Profile Screen

Define your Performance Profile using the **General**, **Cumulative**, **Wireless Clients**, and **BSS** tabs. Once you have defined your Performance Profile, click the **APPLY** button to save your profile. Use the small **X** button to the top left of this screen 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 APs 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 APs 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

Use the **General Tab** of the **Performance Profile** screen to configure some basic settings for this Performance Profile.

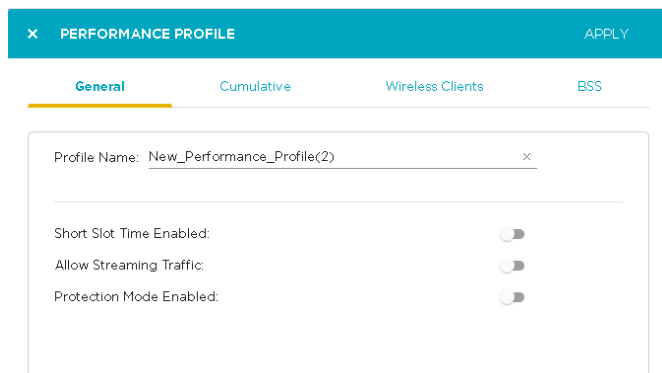


Figure 99: General Tab

Configure the following parameters:

Field	Description
Short Time Slot Enabled	Use the switch to allow or disable the Short Time Slot capability as advertised in the Beacon, which when used on a pure 802.11g deployment, improves WLAN throughput by reducing wait time for transmitter to assure clear channel assessment.
Allow Streaming Traffic	Use the switch to allow or block Streaming traffic in the wireless environment, such as video or audio traffic in wireless environment. It applies only to un-encrypted wireless traffic. Warning: Streaming traffic applications consume large bandwidth and can adversely impact all other Wireless Clients connected on the Wireless LAN.
Protection Mode Enabled	Use the switch to allow or prevent 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. 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

Use the **Cumulative** tab to configure threshold to network characteristics for all wireless clients and traffic in the access point BSS (Basic Service Set).



Note

Entering 0 (zero) as a threshold value disables alarm-generation for that particular threshold.

✕ PERFORMANCE PROFILEAPPLY

GeneralCumulativeWireless ClientsBSS

New Associations: 0

Total Associations: 0

Data Frames Seen: 0

Management Frames Seen: 0

Control Frames Seen: 0

Association Frames Seen: 0

Disassociation Frames Seen: 0

80211 Authentication Frames Seen: 0

8021x Authentication Frames Seen: 0

Deauthentication Frames Seen: 0

Probe Requests Seen: 0

Wired to Wireless Traffic %: Percent: 0 Min Frame: 0

Wireless to Wired Traffic %: Percent: 0 Min Frame: 0

Wireless station to station Traffic %: Percent: 0 Min Frame: 0

Wired station to station Traffic %: Percent: 0 Min Frame: 0

Low Speed Frames %: Percent: 0 Min Frame: 0

Layer 3 Multicast Frames %: Percent: 0 Min Frame: 0

Layer 3 Broadcast Frames %: Percent: 0 Min Frame: 0

Retransmission Frames %: Percent: 0 Min Frame: 0

PS Poll Frames Seen: 0

Figure 100: Cumulative Tab

Configure the following thresholds:

Threshold	Description
New Associations	<p>Enter the maximum number of new associations per minute Extreme AirDefense will allow between a BSS and all Wireless Clients combined.</p> <p>Default = 20.</p> <p>Generally, this number should be low. Your Wireless Clients should associate with a BSS once in the morning when users log on, and rarely after that. In some cases, if the threshold value represents the actual number of Wireless Clients in a BSS, an alarm will be generated if the BSS goes off-line, forcing the Wireless Clients to re-associate with it. In no case should this value be greater than the actual number of Wireless Clients in a BSS.</p> <p>If the signal strength between a Wireless Client and a BSS is very low, the Wireless Client may repeatedly lose connectivity and then reconnect, increasing the number of associations per minute.</p>
Total Associations	<p>Enter the total number of Wireless Clients allowed to associate at any one time with a BSS. This number should reflect your actual number of Wireless Clients. Extreme AirDefense generates an alarm if it detects a greater number, assuming that the extra associations are made by hackers.</p> <p>Default = 15.</p>
Data Frames Seen	<p>Enter the maximum number of data frames per minute allowed to be transmitted from all Wireless Clients combined. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Management Frames Seen	<p>Enter the maximum number of management frames per minute allowed to be transmitted from all Wireless Clients combined. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Control Frames Seen	<p>Enter the maximum number of control frames per minute allowed to be transmitted from all Wireless Clients combined. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Association Frames Seen	<p>Enter the maximum number of association frames allowed to be transmitted or received from all Wireless Clients. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>
Disassociation Frames Seen	<p>Enter the maximum number of disassociation frames allowed to be transmitted or received from all Wireless Clients. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>

Threshold	Description
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 Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.
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 Extreme AirDefense 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 Extreme AirDefense 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 Extreme AirDefense 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 Extreme AirDefense detects a greater number, it generates an alarm. Default = 60. Use the Min Frame control set the minimum number of frames for this threshold.
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 Extreme AirDefense detects a greater number, it generates an alarm. Default = 60. Use the Min Frame control set the minimum number of frames for this threshold.
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 Extreme AirDefense detects a greater number, it generates an alarm. Default = 50. Use the Min Frame control set the minimum number of frames for this threshold.
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 Extreme AirDefense detects a greater number, it generates an alarm. Default = 1. Use the Min Frame control set the minimum number of frames for this threshold.

Threshold	Description
Low Speed Frames %	<p>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.</p> <p>Enter the maximum percentage of data per minute allowed for low speed frames to be transmitted or received from all stations. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Use the Min Frame control set the minimum number of frames for this threshold.</p> <p>Default = 0.</p>
Layer 3 Multicast Frames %	<p>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.</p> <p>Enter the maximum percentage of data per minute allowed for multicast frames to be transmitted or received within a BSS from all stations. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Use the Min Frame control set the minimum number of frames for this threshold.</p> <p>Default = 0.</p>
Layer 3 Broadcast Frames %	<p>An alarm that is generated when the system has detected a high percentage of broadcast traffic violating the policy thresholds. This may be a result of potential Layer 3 broadcast storm attacks on the network.</p> <p>Enter the maximum percentage of data per minute allowed for broadcast frames to be transmitted or received within a BSS from all stations. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Use the Min Frame control set the minimum number of frames for this threshold.</p> <p>Default = 0.</p>
Retransmission Frames %	<p>Enter the maximum percentage of retransmitted data frames allowed during a transmission of data within a BSS from all stations. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Use the Min Frame control set the minimum number of frames for this threshold.</p> <p>Default = 0.</p>
PS Poll Frames Seen	<p>An alarm is generated by a DOS attack using an excessive number of PS-POLL frames have been detected.</p> <p>Enter the maximum number of PS Poll frames to be seen within a BSS. If Extreme AirDefense detects a greater number, it generates an alarm.</p> <p>Default = 0.</p>

Wireless Clients

Use the **Wireless Clients** tab to configure thresholds for any wireless client. These thresholds will typically be lower than the aggregate Wireless Client thresholds. Extreme AirDefense 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 0 (zero) as a threshold value disables alarm generation for that particular threshold.

The screenshot shows the 'PERFORMANCE PROFILE' configuration window with the 'Wireless Clients' tab selected. The 'Wireless Clients' tab is highlighted with a yellow underline. Below the tab, there are four sub-tabs: 'General', 'Cumulative', 'Wireless Clients', and 'BSS'. The 'Wireless Clients' sub-tab contains a list of thresholds, each with a text input field set to '0':

- Data Frames Sent: 0
- Data Frames Received: 0
- Management Frames Sent: 0
- Management Frames Received: 0
- Control Frames Sent: 0
- Control Frames Received: 0
- Fragment Frames Sent: 0
- Association Frames Sent: 0
- Disassociation Frames Sent: 0
- 802.11 Authentication Frames Sent: 0
- 802.1x Authentication Frames Sent: 0
- Deauthentication Frames Sent: 0
- Probe Request Sent: 0
- Retransmission Frames Sent %: Percent: 0 Min Frame: 0

Figure 101: Wireless Client Tab

Configure the following thresholds:

Threshold	Description
Data Frames Sent	Enter the maximum number of data frames per minute any Wireless Client is allowed to transmit. If Extreme AirDefense 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 Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.

Threshold	Description
Management Frames Sent	<p>Enter the maximum number of management frames per minute any Wireless Client is allowed to transmit. If Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.</p> <p>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.</p>
Management Frames Received	<p>Enter the maximum number of management frames per minute any Wireless Client is allowed to receive. If Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.</p>
Control Frames Sent	<p>Enter the maximum number of control frames per minute any Wireless Client is allowed to transmit. If Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.</p>
Control Frames Received	<p>Enter the maximum number of control frames per minute any Wireless Client is allowed to receive. If Extreme AirDefense detects a greater number, an alarm is generated. Default = 0.</p> <p>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.</p>
Fragment Frames Sent	<p>Enter the maximum number of fragment frames per minute that are allowed from any Wireless Client. If Extreme AirDefense detects a greater number, it generates an alarm. Default = 1.</p>
Association Frames Sent	<p>Enter the maximum number of association frames allowed to be transmitted from all Wireless Clients. If Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.</p>
Disassociation Frames Sent	<p>Enter the maximum number of disassociation frames allowed to be transmitted from all Wireless Clients. If Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.</p>
802.11 Authentication Frames Sent	<p>Enter the maximum number of 802.11 authentication frames allowed to be transmitted from all Wireless Clients. If Extreme AirDefense detects a greater number, it generates an alarm. Default = 0.</p>

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 Extreme AirDefense 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 Extreme AirDefense 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 Extreme AirDefense 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 Extreme AirDefense detects a greater number, it generates an alarm. Use the Min Frame control set the minimum number of frames for this threshold. Default = 0.

BSS Tab

Use the **BSS** tab to configure thresholds for data transmission to/fro from BSSs.

PERFORMANCE PROFILE
APPLY

General
Cumulative
Wireless Clients
BSS

Data Frames Sent: 0

Data Frames Received: 0

Management Frames Sent: 0

Management Frames Received: 0

Control Frames Sent: 0

Control Frames Received: 0

Fragment Frames Sent: 0

Association Frames Sent: 0

Disassociation Frames Sent: 0

802.11 Authentication Frames Sent: 0

802.1x Authentication Frames Sent: 0

Deauthentication Frames Sent: 0

Probe Request Sent: 0

Minimum Beacon Frames to be Sent: 0

Retransmission Frames Sent %: Percent: 0 Min Frame: 0

Figure 102: BSS Tab



Note

Entering 0 (zero) as a threshold value disables alarm generation for that particular threshold.

Configure the following thresholds:

Threshold	Description
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 AirDefense 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 AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 0.

Threshold	Description
Control Frames Sent	Enter the maximum number of control frames per minute BSSs are allowed to transmit. If AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 0.

Apply Performance Profile

It is recommended to apply the Performance Profile at the appliance level by selecting the **Enable Configuration** switch.

If you need to apply a different Performance Profile at a specific level in your Extreme AirDefense hierarchy, navigate to the level in the **Structure & Tags** pane and select

it. Use the Override Inherit from: ADSP control's **Override** option to apply the alternate Performance Profile.

For more information see the section *Overriding Configuration Settings* in this document.

Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to *ON*. The top most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

Environment Monitoring

Use the **Environment Monitoring** screen to monitor the local RF environment. If one of the configured threshold exceeds, an alarm is generated. You can also choose to monitor your Extreme AirDefense system for unobserved devices and also generate alarms for missing devices.

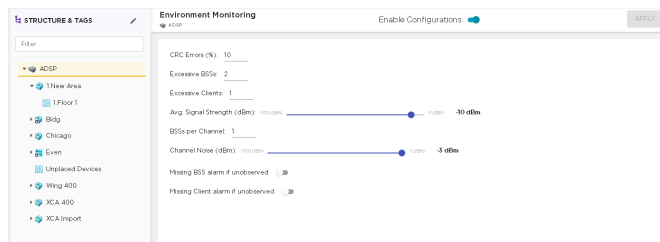


Figure 103: Environment Monitoring

It is recommended to apply Environment Monitoring at the Extreme AirDefense appliance level by selecting the **Enable Configuration** switch.

Configure the following parameters:

Field	Description
CRC Errors	Cyclic redundancy check (CRC) errors should not exceed the specified percentage value. Use the spinner control to set this threshold value.
Excessive BSSs	BSSs on your network are considered excessive if the specified value is exceeded. Use the spinner control to set this threshold value.
Excessive Clients	Wireless clients on your network are considered excessive if the specified value is exceeded. Use the spinner control to set this threshold value.
Avg. Signal Strength (dBm)	The average signal strength (in dBm) of APs on your network should not exceed the specified value. Use the slider to set this threshold value in the range of -100 dBm and -1 dBm.
BSSs per Channel	The number of BSSs on any particular channel should not exceed the specified value. Use the spinner control to set this threshold value.
Channel Noise (dBm)	Channel noise is monitored to ensure that the noise does not exceed the specified value. Use the slider to set this threshold value in the range of -100 dBm and -1 dBm.
Missing BSS Alarm if unobserved	When this switch is selected, it generates a missing BSS alarm when any of the threshold values are exceeded.
Missing Client Alarm if unobserved	When this switch is selected, it generates a missing Client alarm when any of the threshold values are exceeded.

Use the **APPLY** button located to the top right of this window to save your changes.

Apply Environment Monitoring Configuration

If you need to apply a different set of Environment Monitoring configurations at a specific level in your Extreme AirDefense hierarchy, navigate to the level in **Structure**

& **Tags** pane and select it. Use the **Override** **Inherit from: ADSP** control's **Override** option to apply the alternate configuration at that level.

For more information see the section *Overriding Configuration Settings* in this document.

Overriding Configuration Settings

The **Enable Configuration** switch is only available at the top most node of the **Structure & Tags** pane. Configurations can only be applied when this switch is set to *ON*. The top most node is always named *ADSP* and you must use this switch to apply the selected configuration through out the Extreme AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits configuration from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the configurations set at that node. However, you can override the inherited configuration at any level in the hierarchy.

To override the inherited settings, in the **Structure & Tags** pane, select the node where you want to override the inherited configuration. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the configuration settings are inherited from. Use this information to orient your self on how the configurations are inherited.

Change the configuration for the selected level as required and then use the **APPLY** button to implement the modified configuration settings. These settings will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

Client Types

Client Types are classification of devices that are found within your Extreme AirDefense system. Use the **Client Type** screen to create and manage custom client types within your system.

The **Client Types** screen enables you to:

- Add new client types to your system.
- Edit existing client types to change its icon or name.
- Remove existing client types from your system.

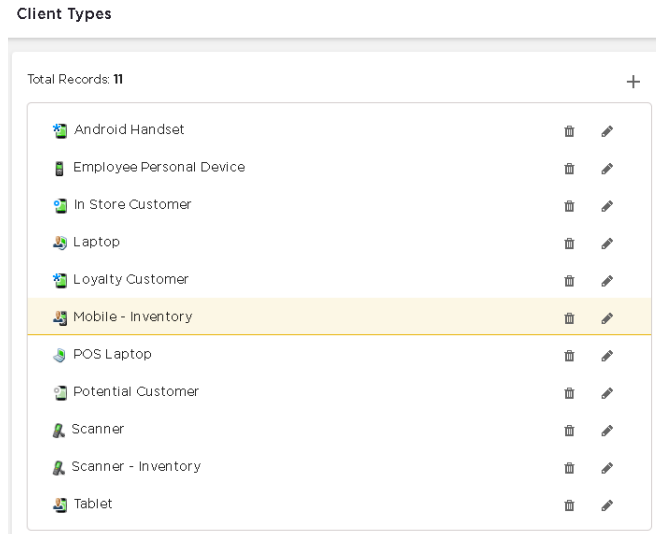


Figure 104: Client Types Screen

Manage Client Types

Add a New Client Type

Use the **Client Types** screen to manage your client types. To add a new client type, use the icon located to the top of this list. The following window displays.

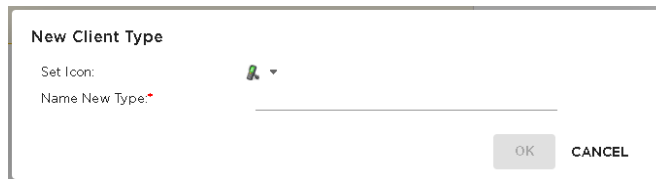


Figure 105: New Client Window

Use the **Set Icon** drop-down list to select an icon to apply to this client type. In the **Name New Type** field, provide a name for this new client type.

Click the **OK** button to save this client type. If you do not want to create this client type, use the **CANCEL** button.

Edit a Client Type

Each Client Type in this window has two icons. Use the icon to edit the selected client type. The following window displays.



Figure 106: Edit Client Type Window

Use the **Set Icon** drop-down list to select an icon to apply to this client type. In the **Name New Type** field, edit the name for this client type.

Click the **OK** button to save this client type. If you do not want to edit this client type, use the **CANCEL** button.

Delete a Client Type

Use the  icon to delete the selected client type. The following window displays.



Figure 107: Remove Client Type

When this client type is deleted, all devices of this type must be assigned an another type. Use the **Reset To** drop-down list to select the client type to assign to the devices.

Click the **OK** button to remove this client type. If you do not want to remove this client type, use the **CANCEL** button.

Appliance Settings

Use the **Appliance Settings** screen to configure settings specific to this instance of the Extreme AirDefense appliance. An appliance is the physical device on which the Extreme AirDefense software runs. These settings are global in nature and apply to all networks managed by this Extreme AirDefense instance.

Appliance Settings
APPLY

Port:
8543

Mail Relay Server: _____ (IP address or fully qualified host name)

Max Connections:
201 (Total simultaneous application server connections)

User Session Limit of 1 _____ simultaneous sessions per user

Air-Termination system

Policy based Air-Termination system

Port Suppression system

Auto-Logout 1 _____ minute(s)

Spectrum Scan Timeout after 20 _____ minute(s)

Sensors Cloaking Limit 3 _____ simultaneous cloaked sensors

The following Extreme AirDefense appliance settings can be configured from this screen.

Field	Description
Port	<p>Set the port on which the Extreme AirDefense user interface is available. This setting configures the system port to access the Extreme AirDefense graphical user interface. Enter a port number that is available for use. Choose a port number in the range 1024-65000. The default port is 8543.</p> <p>Note: Extreme AirDefense will not allow you to choose a port that is already in use.</p>
Mail Relay Server	<p>Define the mail relay host. Enter an IP address or a fully-qualified host name. The mail relay host is a mail server that forwards all mails received from Extreme AirDefense to their intended recipients.</p>
Max Connections	<p>Specify the maximum number of simultaneous application server connections that can occur with this Extreme AirDefense instance. A maximum of two thousand (2000) simultaneous application server connections can be set.</p>

Field	Description
User Session Limit	<p>Configures the number of simultaneous sessions that the same user can have with the Extreme AirDefense appliance. By default, this option is not enabled. It is suggested to enable this option and set the simultaneous session value to one (1) to increase security when permitting access to the physical Extreme AirDefense device.</p> <p>An upper limit of one hundred (100) simultaneous connections can be set for a single user.</p>
Air Termination System	<p>Air Termination enables you to terminate the connection between your wireless LAN and any associated Wireless Client, authorized or unauthorized.</p> <p>Select the Air-Termination system option to enable this feature.</p> <p>The Policy based Air-Termination system option is only available for use when the Air-Termination system option is selected.</p> <p>Note: This setting will not be visible if you are not a user with administrative permissions.</p>
Policy-based Air Termination System Enabled	<p>Policy-based Air Termination is an automated version of Air-Termination. This feature enables you to create and apply rules to automatically terminate the connection between your monitored Wireless LANs and any associated device or wireless client, either authorized or unauthorized, based on alarms that are generated by the Extreme AirDefense system.</p> <p>Select this option to enable Policy-based Air Termination. This is enabled by default when you enable Air-Termination system.</p> <p>Note: This setting will not be visible if you are not a user with administrative permissions.</p>
Port Suppression System	<p>Port Suppression enables you to turn off the port on the network switch through which a device is communicating. You can suppress the communications port for any network device, effectively shutting down the communication port for the device.</p> <p>This is useful for devices that are connected to your network through the physical network.</p> <p>Select this option to enable Port Suppression system.</p> <p>Note: You must have added SNMP Managed Switches and have full read and write privileges to enable Port Suppression system</p>

Field	Description
Auto-Logout	Use this option to enable/disable the automatic logout of any logged in user after a specified amount of time. Select the Auto-Logout option to enable it and then use the spinner control to set the logout time in minutes. Note: You must log off Extreme AirDefense and then log back in before the Auto-Logout change takes effect.
Spectrum Scan Timeout	Use this option to enable timeout when performing dedicated spectrum scan for spectrum analysis. Then, use the spinner control set the timeout duration in minutes. Timeout duration can be in the range of 1-120 minutes.

Device Age Out

The **Device Age Out** screen displays a synopsis of the devices seen within your Extreme AirDefense managed networks. Devices are classified into BSSs, wireless clients, and BT/BLE devices. Data is displayed for the previous 24 hours, last 7 days, and for days beyond a week.

Device Age Out (APPLY Reset)

Sensed devices last seen observations

All Devices	19	4	1	14
BSS	SUB TOTALS	LAST 24 HRS	LAST 1-7 DAYS	OVER 7 DAYS
Sanctioned	16	2	0	14
Unsanctioned	0	0	0	0
Neighbor	0	0	0	0
Sub Totals	16	2	0	14

WIRELESS CLIENT	SUB TOTALS	LAST 24 HRS	LAST 1-7 DAYS	OVER 7 DAYS
Sanctioned	3	2	1	0
Unsanctioned	0	0	0	0
Neighbor	0	0	0	0
Sub Totals	3	2	1	0

BLUETOOTH	SUB TOTALS	LAST 24 HRS	LAST 1-7 DAYS	OVER 7 DAYS
Sanctioned	0	0	0	0
Unsanctioned	0	0	0	0
Neighbor	0	0	0	0
Sub Totals	0	0	0	0

Age out settings

You may enter a value between 1 hour and 7 days.

Unsanctioned BSSs: 6 Hours

Ad-Hoc BSS: 4 Hours

Unsanctioned Wireless Clients: 6 Hours

Unsanctioned Bluetooth: 6 Hours

Unsanctioned Unknown: 6 Hours

Figure 108: Device Age Out

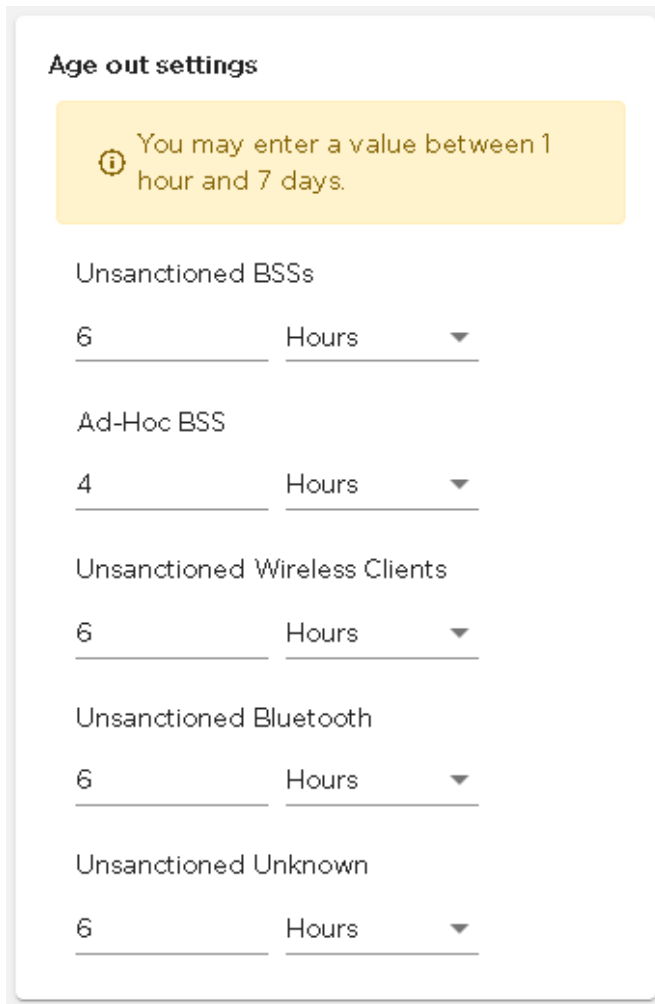
Configurations in the *Device Age Out* screen allow you to specify various timeout values that are used when displaying devices in the left pane. You can set an age out value for any of the following device types:

- Unsanctioned BSSs
- Ad-Hoc BSSs

- Unsanctioned Wireless Clients
- Unsanctioned Bluetooth devices
- Unknown, unsanctioned devices

Values are specified in hours or days with a minimum of 1 hour and a maximum of 7 days.

When a device exceeds the age out value specified in this screen, it is no longer seen in any of the screens in the **Networks** tab. However, these devices will still be visible for forensics analysis. All alarms associated with these removed devices are removed as well and will not be displayed in any of the screens of the **Alarms** tab.



Age out settings

i You may enter a value between 1 hour and 7 days.

Unsanctioned BSSs
6 Hours ▼

Ad-Hoc BSS
4 Hours ▼

Unsanctioned Wireless Clients
6 Hours ▼

Unsanctioned Bluetooth
6 Hours ▼

Unsanctioned Unknown
6 Hours ▼

Figure 109: Age out setting

After configuring the age out values, click the **APPLY** button to save your changes. Click **Reset** button to discard any changes and revert the age out values to the previous settings.

Configuration Backup

The **Configuration Backup** screen enables you to manage your manual and scheduled configuration backup settings.

Configurations can be backed up to your local PC or to another directory within the Extreme AirDefense appliance. Backups can either be done manually or automatically on a preset schedule.

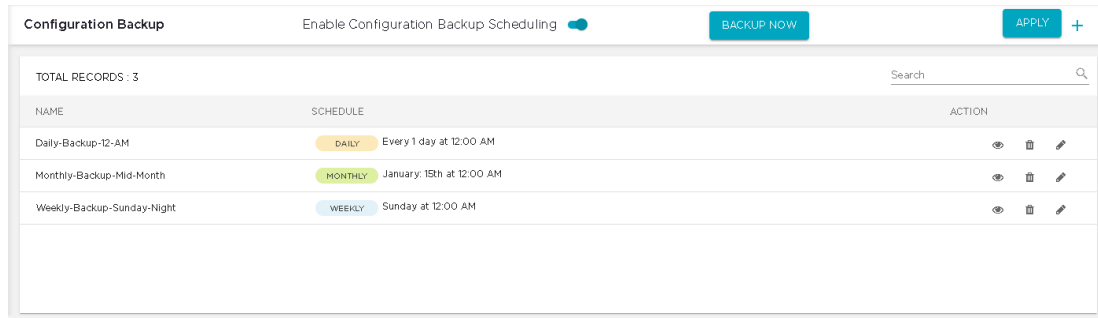


Figure 110: Configuration Backup Screen

By default, scheduling of backup is not turned on. You must use the **Enable Configuration backup Scheduling** switch to turn it on. When this switch is turned on, the **+** icon located to the right of the **APPLY** button is enabled. Use this icon to create a new scheduled backup configuration.

Use the **BACKUP NOW** button to start a configuration backup manually. The following window displays.

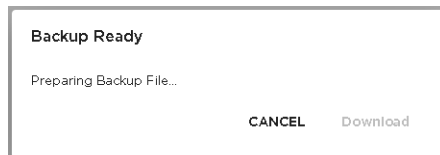


Figure 111: Backup Ready Window

When the configuration has been backed up locally on the Extreme AirDefense appliance, the **Download** button is enabled. Click this button to download and save the configuration backup to your PC.

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 the `/usr/local/smx/backups` folder.
- 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.

View Backup Schedules

The **Configuration Backup** screen displays a list of schedules that have been configured for this Extreme AirDefense system.

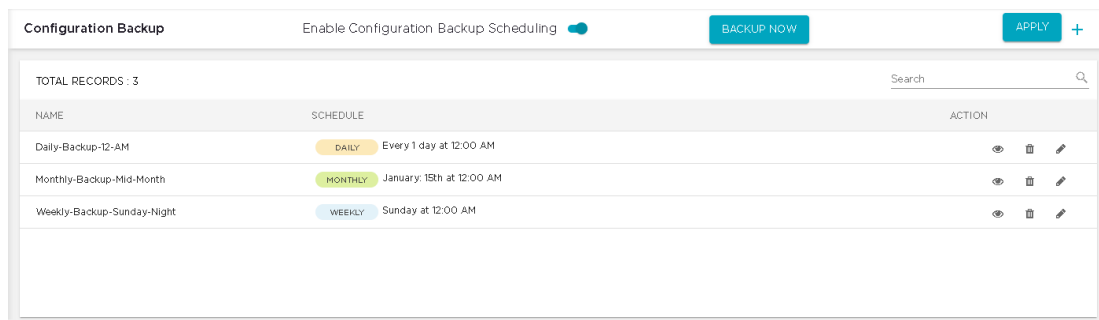


Figure 112: Configuration Backup Screen

The following information is displayed for each configuration backup schedule:

Field	Description
Name	Displays the name assigned to this schedule
Schedule	Displays the type of this schedule and the time or frequency for this schedule.
Action	The icons in this field enable to view, edit or delete your schedule. Use the icon to view the configuration schedule. Use the icon to delete the selected schedule. Similarly, use the icon to edit the schedule.

If you are managing a large number of configuration backup schedules, use the **Search** field located to the top of this list to narrow down the number of items in this list.

Scheduling Configuration Backup

To ensure that you have the latest backups for recovering from disasters, use the scheduling features of the **Configuration Backup** screen to create backups on a pre set schedule.

Use the **+** icon located to the right of the **APPLY** button. This icon is only enabled when the **Enable Configuration Backup Scheduling** switch is set to on.

The screenshot shows a window titled "SCHEDULE BACKUP" with a "SAVE" button. Below the title bar, there is a "Job Name" field containing "New Scheduled Configuration Backup". Underneath, there are two sections: "Settings" and "Schedule". The "Settings" section is expanded, showing "Destination" with radio buttons for "Local" (selected) and "Remote". The "Schedule" section shows a dropdown menu with "INTRA-DAY" selected and "Every 3 hrs at 6:25 AM" displayed below it.

Figure 113: Add New Schedule Window

This window is also used to edit existing backup schedules.


In the **Job Name** field, add a name for this backup schedule.

If the **Settings** field is not expanded, use the **∨** icon to expand the field. By default, the destination for the backed up configuration is always on the Extreme AirDefense appliance. For more information on how configuration backup works and to know where the backup files are stored locally on the Extreme AirDefense system, see the topic [How Backups Work](#) on page 296 in this document.

If you require that your configuration backup is stored on a remote sever, click the **Remote** option. The **Settings** field expands to show more fields. Configure the following:

Field	Description
Host	The IP address of the remote server on which to store the backup configuration.
Port	The port number on which the remote server is listening to incoming connections.
Select Protocol	The protocol to use to connect to the remote server. Can be one of: <ul style="list-style-type: none"> • HTTP • HTTPS • FTP • SCP • SFTP • TFTP
Path	The destination directory on the remote sever where the backup configuration files will be stored.

Field	Description
User	The username used to connect to the remote server.
Password	The valid password for the account in the User field.
Retries	The number of attempts that will be made to connect to the remote server in the case the remote server is not accessible. Set a value in the range of 1-5 attempts. Extreme AirDefense will stop trying to connect to the remote server once it has tried this many number of times.
Verify Server Certificate/Key	Forces Extreme AirDefense to verify that the server certificate (for HTTPS connections) or server key (for SCP or SFTP connections) is valid for the remote server.

Expand the **Schedule** tab using the  icon.

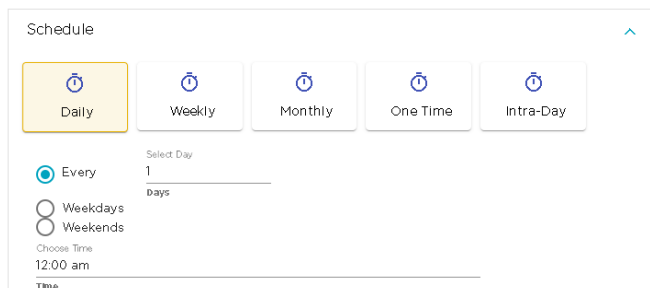


Figure 114: Schedule Field

Select from one of the available schedules. The available schedules are:

- Daily
- Weekly
- Monthly
- One Time
- Intra-Day

Each of these schedules have different configurations. The following table lists the various configurations and their individual settings.

Field	Description
Daily	<p>The following configurations are available for the <i>Daily</i> schedule.</p> <ul style="list-style-type: none"> • Every - Use this field to take a daily backup every set number of days. Use the spinner control to set the number of days between two consecutive backups. The value can be set between 1-31 days. • Weekdays - Use this field to enable backups to be taken only on week days. Backups are not taken on weekends, i.e., Saturdays and Sundays. • Weekends - Use this field to enable backups to be taken only on weekends. Backups are only taken on Saturdays and Sundays. • Choose Time - Use this field to set the time when the backup is taken every day.
Weekly	<p>The following configurations are available for the <i>Weekly</i> schedule.</p> <ul style="list-style-type: none"> • Select Weekday - Use this drop-down list to select the specific weekday or weekdays on which this schedule will run. Use the check-box before each day to select it. You can select multiple weekdays. • Choose Time - Use this field to set the time when the backup is taken every selected weekday.
Monthly	<p>The following configurations are available for the <i>Monthly</i> schedule.</p> <ul style="list-style-type: none"> • Select Month - Use this drop-down list to select the specific month or months during which this schedule will run. Use the check-box before each month to select it. You can select multiple months. • Day - Use the Day control to indicate the numerical date on which this schedule will run. For example, if this value is fifteen (15), then this schedule is run on the 15th of the selected month or months. • Last day of the month - Use this control to indicate the schedule is to be run on the last day of the month of the selected month or months. • Use the last option to indicate a specific schedule that is repeated at a particular combination. For example, if the values are <i>Second</i> and <i>Saturday</i>, then this schedule will run only on the second Saturday of the selected month or months. • Choose Time - Use this field to set the time when the backup is taken every selected month or months.

Field	Description
One Time	<p>The following configurations are available for the <i>One Time</i> schedule.</p> <ul style="list-style-type: none"> • Choose a date - Use this field to select the particular date on which you want to run this schedule. Use the calendar icon next to this field to select the date. • Choose Time - Use this field to set the time when the backup is taken on the specified day.
Intra-Day	<p>The following configurations are available for the <i>Intra-Day</i> schedule. This schedule is used to take multiple backups on the same day.</p> <ul style="list-style-type: none"> • Set Frequency - Use this field to define the frequency of this intra-day backup schedule. When this value is specified, a backup is taken with this frequency. For example, when this value is set to three (3), a configuration backup is taken every three hours. • Choose Time - Use this field to set the time when the intra-day backup is started. For example, if the value is set at 10:30 am, then the first backup of the day will be done at the above time. Subsequent backup will be taken after ever Set Frequency interval.

Once you have configured your backup schedule, use the **SAVE** button to save the backup. To exit without saving your changes, use the small **X** button located to the top left of this window.

Forensic and Log Backup

The **Forensic And Log Backup** window enables you to set the various parameters for automatic backup of your forensic logs and system logs to different remote servers. To configure the same server, you must configure the same details for both forensic and system logs fields.

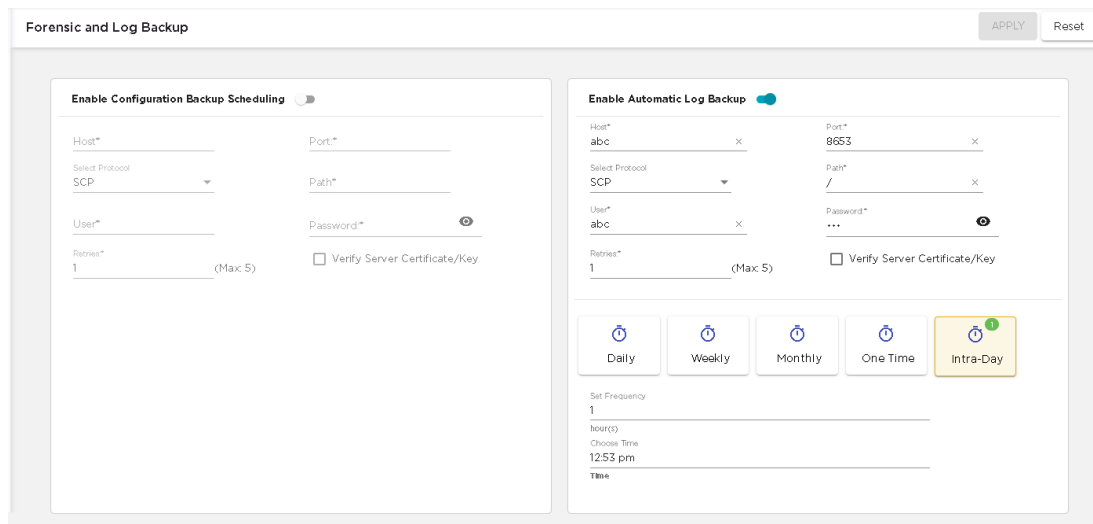


Figure 115: Forensic And Log Backup Screen

Forensic Backup Configuration

Use the fields in the left of the screen to set the remote server for saving the forensic backups.

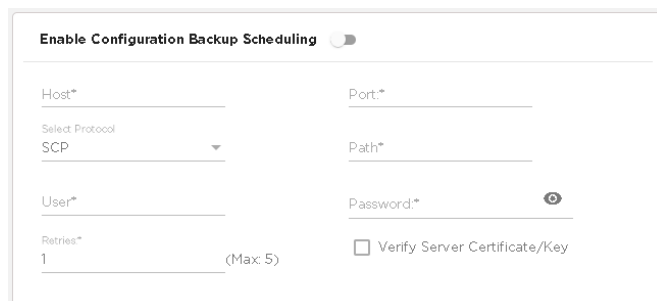


Figure 116: Forensic Logs - Remote Server Configuration

To save your forensic logs on a remote server, you should enable the feature. Use the switch in this field and set it to the *ON* position.

Configure the following:

Field	Description
Host	The IP address of the remote server on which to store the forensic logs.
Port	The port number on which the remote server is listening to incoming connections.

Field	Description
Select Protocol	The protocol to use to connect to the remote server. Can be one of: <ul style="list-style-type: none"> • HTTP • HTTPS • FTP • SCP • SFTP • TFTP
Path	The destination directory on the remote sever where the forensic log files will be stored.
User	The username used to connect to the remote server.
Password	The valid password for the account in the User field.
Retries	The number of attempts that will be made to connect to the remote server in the case the remote server is not accessible. Set a value in the range of 1-5 attempts. Extreme AirDefense will stop trying to connect to the remote server once it has tried this many number of times.
Verify Server Certificate/Key	Forces Extreme AirDefense to verify that the server certificate (for HTTPS connections) or server key (for SCP or SFTP connections) is valid for the remote server.

Use the **APPLY** button to save the changes made to the configurations in this screen. Use the **Reset** button to revert the changes made to the fields in this screen to their previous settings.

Log Backup Configuration

Use the fields to the right of the screen to set the remote server for saving log backups.

Enable Automatic Log Backup

Host* _____ Port* _____

Select Protocol
SCP _____ Path* _____

User* _____ Password* _____

Retries* 1 (Max: 5) Verify Server Certificate/Key

Choose a date
5/10/2020

Choose Time
12:00 am

Time _____

Figure 117: Logs - Remote Server Configuration

To save your logs automatically to a remote server, you should enable the feature. Use the switch in this field and set it to the *ON* position.

Configure the following:

Field	Description
Host	The IP address of the remote server on which to store the logs.
Port	The port number on which the remote server is listening to incoming connections.
Select Protocol	The protocol to use to connect to the remote server. Can be one of: <ul style="list-style-type: none"> • HTTP • HTTPS • FTP • SCP • SFTP • TFTP
Path	The destination directory on the remote sever where the backup configuration files will be stored.
User	The username used to connect to the remote server.
Password	The valid password for the account in the User field.

Field	Description
Retries	The number of attempts that will be made to connect to the remote server in the case the remote server is not accessible. Set a value in the range of 1-5 attempts. Extreme AirDefense will stop trying to connect to the remote server once it has tried this many number of times.
Verify Server Certificate/Key	Forces Extreme AirDefense to verify that the server certificate (for HTTPS connections) or server key (for SCP or SFTP connections) is valid for the remote server.

If you want to automatically backup the logs on a particular schedule, configure the following fields.

Field	Description
Daily	<p>The following configurations are available for the <i>Daily</i> schedule.</p> <ul style="list-style-type: none"> • Every - Use this field to take a daily backup every set number of days. Use the spinner control to set the number of days between two consecutive backups. The value can be set between 1-31 days. • Weekdays - Use this field to enable backups to be taken only on week days. Backups are not taken on weekends, i.e., Saturdays and Sundays. • Weekends - Use this field to enable backups to be taken only on weekends. Backups are only taken on Saturdays and Sundays. • Choose Time - Use this field to set the time when the backup is taken every day.
Weekly	<p>The following configurations are available for the <i>Weekly</i> schedule.</p> <ul style="list-style-type: none"> • Select Weekday - Use this drop-down list to select the specific weekday or weekdays on which this schedule will run. Use the check-box before each day to select it. You can select multiple weekdays. • Choose Time - Use this field to set the time when the backup is taken every selected weekday.

Field	Description
Monthly	<p>The following configurations are available for the <i>Monthly</i> schedule.</p> <ul style="list-style-type: none"> • Select Month - Use this drop-down list to select the specific month or months during which this schedule will run. Use the check-box before each month to select it. You can select multiple months. • Day - Use the Day control to indicate the numerical date on which this schedule will run. For example, if this value is fifteen (15), then this schedule is run on the 15th of the selected month or months. • Last day of the month - Use this control to indicate the schedule is to be run on the last day of the month of the selected month or months. • Use the last option to indicate a specific schedule that is repeated at a particular combination. For example, if the values are <i>Second</i> and <i>Saturday</i>, then this schedule will run only on the second Saturday of the selected month or months. • Choose Time - Use this field to set the time when the backup is taken every selected month or months.
One Time	<p>The following configurations are available for the <i>One Time</i> schedule.</p> <ul style="list-style-type: none"> • Choose a date - Use this field to select the particular date on which you want to run this schedule. Use the calendar icon next to this field to select the date. • Choose Time - Use this field to set the time when the backup is taken on the specified day.
Intra-Day	<p>The following configurations are available for the <i>Intra-Day</i> schedule. This schedule is used to take multiple backups on the same day.</p> <ul style="list-style-type: none"> • Set Frequency - Use this field to define the frequency of this intra-day backup schedule. When this value is specified, a backup is taken with this frequency. For example, when this value is set to three (3), a configuration backup is taken every three hours. • Choose Time - Use this field to set the time when the intra-day backup is started. For example, if the value is set at 10:30 am, then the first backup of the day will be done at the above time. Subsequent backup will be taken after ever Set Frequency interval.

Once you have configured your backup schedule, use the **SAVE** button to save the backup. To exit without saving your changes, use the small **X** button located to the top left of this window.

Configuration Restore

Use the **Configuration Restore** window to restore your Extreme AirDefense system's configuration from backups.

Configuration Restore APPLY Reset

Select backup configuration file BROWSE

Selected configuration will be cleared and restored

- Restore All Configuration
All current appliance configuration settings will be replaced. All devices and sensors will be replaced.
- Restore Appliance Network Configuration
The appliance's IP Address, Hostname, DNS settings, and Time settings will be replaced.
- Restore System Configuration
All current configuration profiles, including user settings will be replaced. All devices and sensors will be replaced.
- Restore Alarm Configuration
All current alarm configuration will be replaced.
- Restore Custom Reports
All current custom report settings will be replaced.

Figure 118: Configuration Restore Screen

By default, all the fields in this screen are disabled. These fields are only enabled when you select a backup from using the **BROWSE** button. When you click the **BROWSE** button, it opens the operating system's *File Browser* window. Use this window to locate the correct backup file.

Once the backup file is uploaded to the Extreme AirDefense system, the other controls in this screen are enabled. The following options are available when restoring a system from a backup file.

Field	Description
Restore All Configurations	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	Restore any configuration that pertains to Alarms.
Restore Custom Reports	Restores any custom reports that were backed up.

Once you have selected the appropriate restore options, click the **APPLY** button located to the top right of the screen.

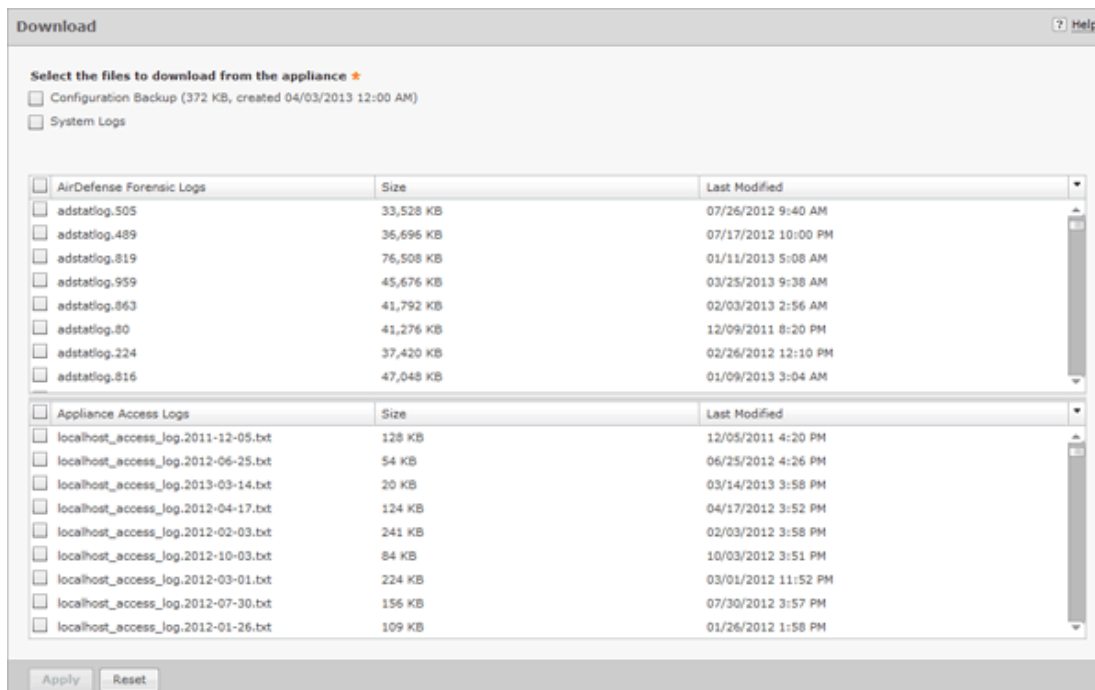
The **Reset** button clears all your restore selections in this screen.

Download Logs

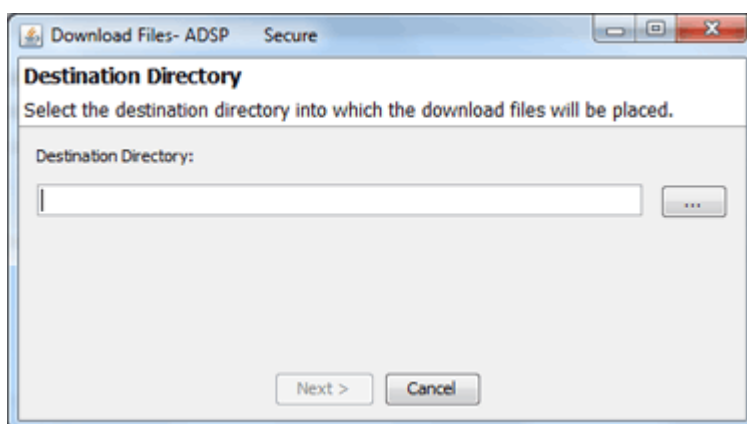
You can download configuration files that were automatically backed up to your ADSP server to your workstation. Once the backed up configuration is on your workstation, you can restore it. (See [Configuration Restore](#).)

To download a configuration, follow these steps:

1. Navigate to **Configuration > Appliance Management > Download Logs**.

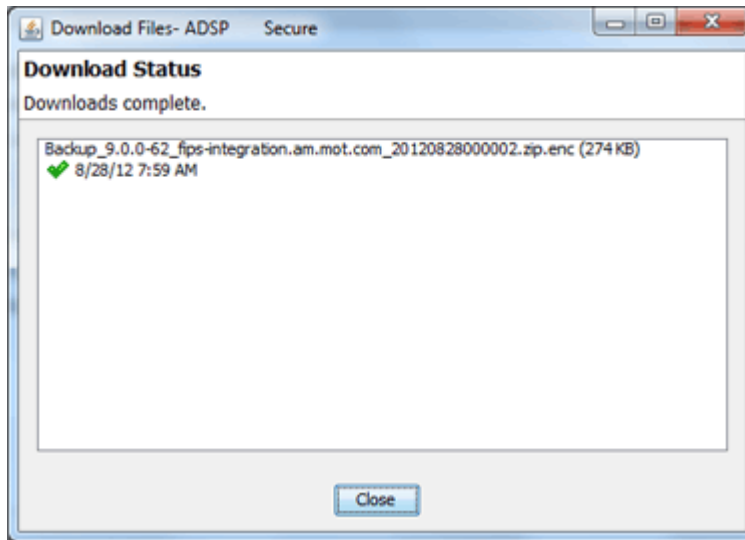


2. Select if you want to download a backup that exists on your appliance and/or the system logs.
3. You can download all forensic logs or all appliance access logs. Alternatively, you can pick and choose the forensic logs or appliance access logs that you want to download.
4. Click **Apply**. A destination directory window is displayed.



5. Click the **Browse** button to open a window where you can select your destination directory (folder).
6. Navigate to the directory where you want to download your server configuration.
7. Click **Select** to select the destination. The destination path displays in the **Destination Directory** field.

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



- Click **Close**.

Forensic and Log Backup

To enable 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.

You can automatically back up forensics data and log files by navigating to **Configuration > Appliance Management > Forensic and Log Backup**.

Field	Description
Host	The name of the server where you want to back up forensics or log files. This can be an IP address or a DNS name defined by your DNS server.
Port	The port number to use during the backup.
Protocol	The file transfer protocol to use for backing up forensics or log files.
Path	The directory (folder) where to place the backup on the destination server.
User	The username used to log in on the destination server.
Password	The password used to log in on the destination server.
Verify Server Certificate/Key	Verifies that the server certificate (HTTPS connections) or server key (SCP and SFTP connections) is valid.
Retries	The number of times to retry the forensic backup if a failure occurs. The maximum number is 5.

You can schedule the backups for system and access logs. Select an interval and then fill in the related fields using the following table:

Interval	Action
One Time Schedule	Choose a time for the backup by selecting a time from the 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.

Redundant Appliance Synchronization

Extreme AirDefense provides a feature that allows you to configure a second server as a redundant server. This server will automatically take over if the primary server fails for any reason. To enable smooth transition between the two servers, the configurations of the primary server must be synchronized with the secondary server, either manually, or automatically as per a preset schedule.

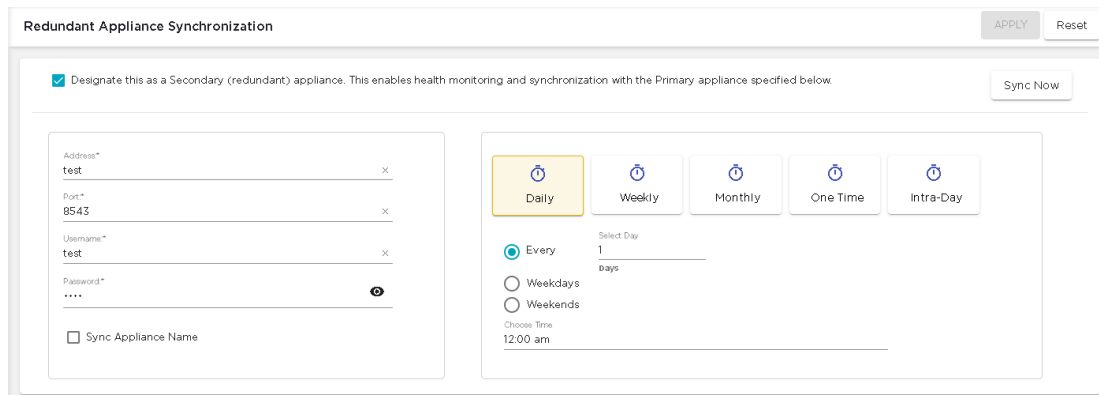


Figure 119: Redundant Appliance Synchronization Screen

The correct way to synchronize your servers is to configure your primary server first and then synchronized your secondary server with your primary server. All configuration settings are copied from your primary server to your secondary server. After synchronization, both the servers will have the same configuration. When synchronizing these servers, the configurations from the primary server will override any configurations set 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`.
- 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.

Automatic Synchronization

As with manual synchronization, use the **Redundant Appliance Synchronization** screen to synchronize the configurations from your primary server to the secondary server.

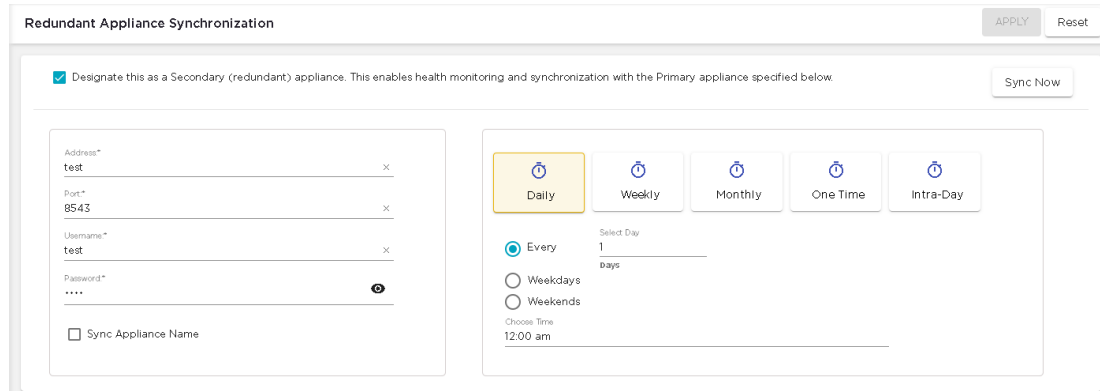


Figure 120: Redundant Appliance Synchronization Screen

Use the left pane of this screen to provide the details for the primary Extreme AirDefense appliance.

The right pane of this screen enables you to automatically synchronize configurations from the primary server on a pre defined schedule.

Before you can synchronize between two devices, you must designate the current device as a redundant device. Select the **Designate this as a Secondary (redundant) device...** option to indicate that this device is a redundant server. When this option is not selected, this device becomes the primary server and all the fields in this screen are disabled.

To automatically synchronize this Extreme AirDefense appliance with a primary server, provide the following information:

Field	Description
Address	The IP address or host name of the primary Extreme AirDefense appliance.
Port	The port number on which the Extreme AirDefense primary server is running. 8543 is the default port.
Username	The username for an account that has login permissions on the primary Extreme AirDefense server.
Password	Password for the above username.
Sync Appliance Name	Select this option if you want to synchronize the appliance names between the primary and secondary servers.
Sync Mail Relay	Select this option if you want to synchronize the mail relay server information between the two servers.

The right pane of this screen enables you to configure the schedule for automatic synchronization. Set the following parameters:

Field	Description
Daily	<p>The following configurations are available for the <i>Daily</i> schedule.</p> <ul style="list-style-type: none"> • Every - Use this field to synchronize the servers every set number of days. Use the spinner control to set the number of days between two consecutive backups. The value can be set between 1-31 days. • Weekdays - Use this field to enable synchronization to take place only on week days. Synchronization does not happen on weekends, i.e., Saturdays and Sundays. • Weekends - Use this field to enable synchronization to take place only on weekends. Synchronization is only performed on Saturdays and Sundays. • Choose Time - Use this field to set the time when the synchronization happens every day.
Weekly	<p>The following configurations are available for the <i>Weekly</i> schedule.</p> <ul style="list-style-type: none"> • Select Weekday - Use this drop-down list to select the specific weekday or weekdays on which this schedule will run. Use the check-box before each day to select it. You can select multiple weekdays. • Choose Time - Use this field to set the time when the synchronization happens every day.
Monthly	<p>The following configurations are available for the <i>Monthly</i> schedule.</p> <ul style="list-style-type: none"> • Select Month - Use this drop-down list to select the specific month or months during which this schedule will run. Use the check-box before each month to select it. You can select multiple months. • Day - Use the Day control to indicate the numerical date on which this schedule will run. For example, if this value is fifteen (15), then this schedule is run on the 15th of the selected month or months. • Last day of the month - Use this control to indicate the schedule is to be run on the last day of the month of the selected month or months. • Use the last option to indicate a specific schedule that is repeated at a particular combination. For example, if the values are <i>Second</i> and <i>Saturday</i>, then this schedule will run only on the second Saturday of the selected month or months. • Choose Time - Use this field to set the time when the synchronization happens every day.

Field	Description
One Time	<p>The following configurations are available for the <i>One Time</i> schedule.</p> <ul style="list-style-type: none"> • Choose a date - Use this field to select the particular date on which you want to run this schedule. Use the calendar icon next to this field to select the date. • Choose Time - Use this field to set the time when the synchronization happens every day.
Intra-Day	<p>The following configurations are available for the <i>Intra-Day</i> schedule. This schedule is used to take multiple backups on the same day.</p> <ul style="list-style-type: none"> • Set Frequency - Use this field to define the frequency of this intra-day backup schedule. When this value is specified, a backup is taken with this frequency. For example, when this value is set to three (3), a configuration backup is taken every three hours. • Choose Time - Use this field to set the time when the intra-day synchronization is started. For example, if the value is set at 10:30 am, then the first synchronization of the day will be done at the above time. Subsequent synchronizations will be taken after ever Set Frequency interval.

Once you have configured your synchronization schedule, use the **APPLY** button to save the schedule. To exit without saving your changes, use the **RESET**.

Appliance Replacement Considerations

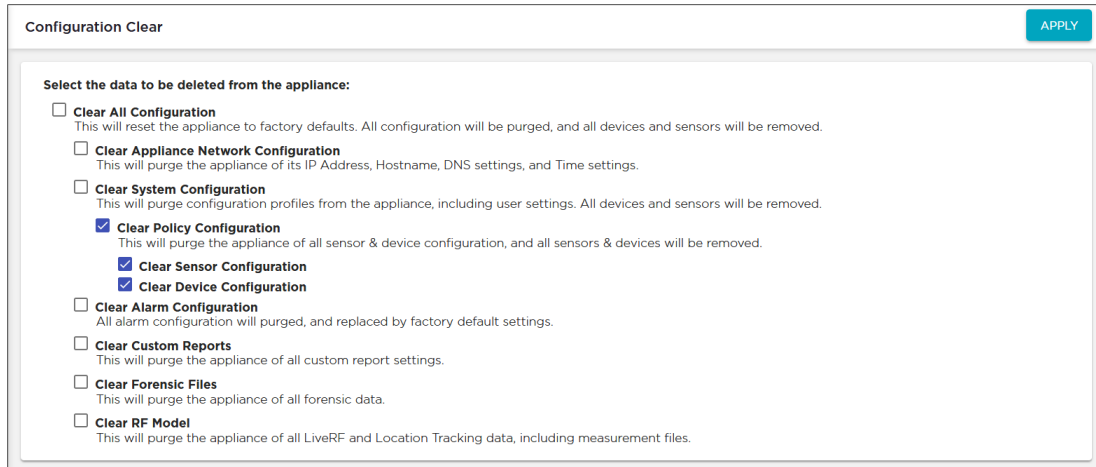
Replacing an appliance should be done in such a way that no data is lost during the transition. Following these recommendations will help prevent data loss:

- 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.

Configuration Clear

Use the **Configuration Clear** screen to clear configurations for the various features of the Extreme AirDefense system.



The screenshot shows the 'Configuration Clear' interface. At the top right is an 'APPLY' button. Below the title, there is a section titled 'Select the data to be deleted from the appliance:' followed by a list of checkboxes and their descriptions:

- Clear All Configuration**
This will reset the appliance to factory defaults. All configuration will be purged, and all devices and sensors will be removed.
- Clear Appliance Network Configuration**
This will purge the appliance of its IP Address, Hostname, DNS settings, and Time settings.
- Clear System Configuration**
This will purge configuration profiles from the appliance, including user settings. All devices and sensors will be removed.
- Clear Policy Configuration**
This will purge the appliance of all sensor & device configuration, and all sensors & devices will be removed.
 - Clear Sensor Configuration**
 - Clear Device Configuration**
- Clear Alarm Configuration**
All alarm configuration will be purged, and replaced by factory default settings.
- Clear Custom Reports**
This will purge the appliance of all custom report settings.
- Clear Forensic Files**
This will purge the appliance of all forensic data.
- Clear RF Model**
This will purge the appliance of all LiveRF and Location Tracking data, including measurement files.

Extreme AirDefense provides a comprehensive set of options that are used to have granular control on the data that can be retained or cleared. Extreme AirDefense configuration settings and the data that is stored on the physical Extreme AirDefense instance can be broadly classified into the following broad categories:

- Appliance's Network Configuration
- Extreme AirDefense System Configuration
- Sensor and Device Configuration, including device details
- Alarm Configuration
- Custom Report Configuration, including stored reports
- Forensic Files
- Life RF and Location Tracking data, including measurement files

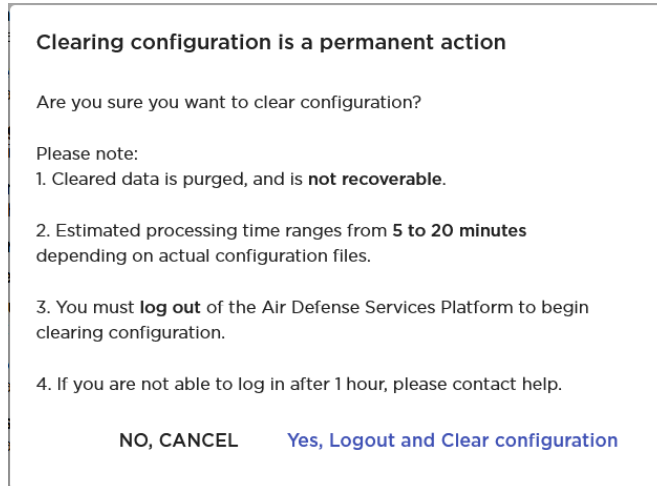
The **Configuration Clear** screen also provides a switch to reset the Extreme AirDefense appliance to its factory defaults. This will purge all configurations and remove all devices and sensors.

Configurations

The following parameters can be managed through this screen:

Field	Description
Clear All Configuration	Clears all configuration data, setting the Extreme AirDefense server back to its original default state. This option is used to set the device to its factory defaults.
Clear Appliance Network Configuration	Clears the Extreme AirDefense appliance's network configuration. The appliance is cleared of its IP Address, host name, DNS configurations, and Time settings. Device and sensor information is not cleared.
Clear System Configuration	<p>Clears all system configuration data. This includes the data that is covered by the other sub options. The configurations cleared include user settings and configuration profiles. All sensors and devices will also be removed.</p> <p>There are three sub-options associated with this option.</p> <ul style="list-style-type: none"> • Clear Policy Configuration - Clears all policy configurations that you have changed. Selecting this option also clears the devices and sensor. If you select this option, the Sensor and Device configurations will be automatically selected. • Clear Sensor Configuration - Clears all Sensor configurations that you customized. Sensors will not be removed. • Clear Device Configuration - Clears all device configurations that you customized. Devices will not be removed. <p>You can choose to select the Clear Sensor Configuration or Clear Device Configuration without select the Clear Policy Configuration option. When selected in this manner, the sensors and devices will not be removed, however, their configurations are removed.</p>
Clear Alarm Configuration	Clears any configuration dealing with alarms and sets alarm configuration data back to its default.
Clear Custom Reports	Clears any custom reports that you have created. This also removes any reports that are stored on the Extreme AirDefense instance.
Clear Forensic Files	Clears (removes) any forensic data files that exist on the Extreme AirDefense server.
Clear RF Model	Clears the RF data used by Live RF and Location Tracking in the Floor Plan. This information includes the measurement files.

Once you have made your choices, select the **APPLY** button located to the top right of the screen to apply your changes. A warning dialog displays.



Read and understand the information displayed within this screen. To confirm your changes, select the **Yes, Logout and Clear configuration** button.

Select the **NO, CANCEL** button to exit without applying the changes you made to the parameters in this screen.

Language Settings

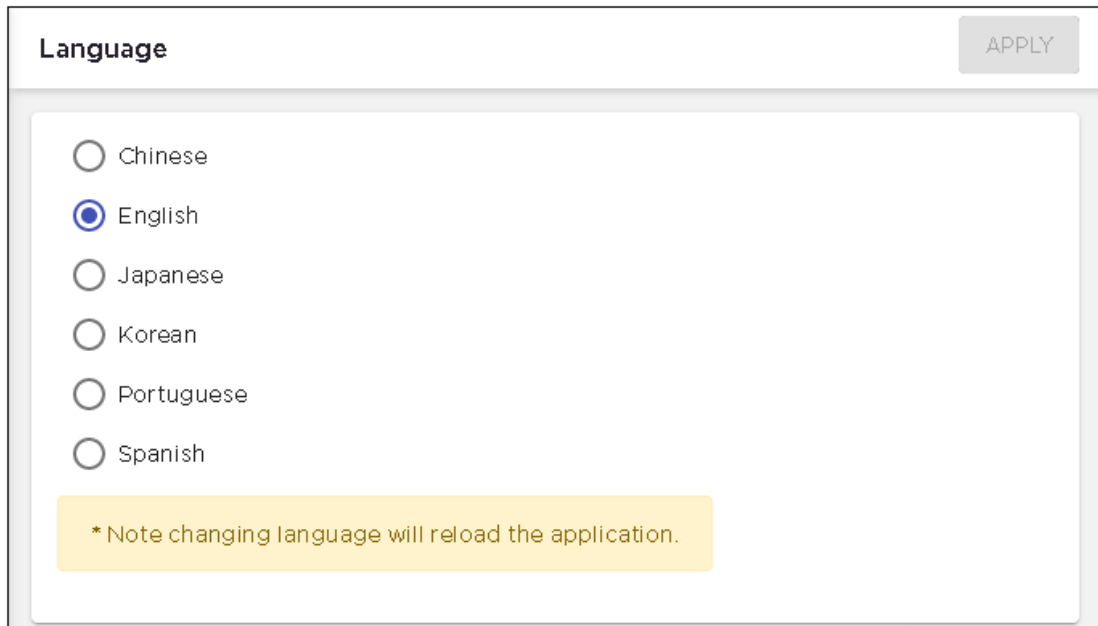
Extreme AirDefense user interface can be localized in a few selected language. Use the **Language** screen to select the language for the user interface elements.

The following user interface elements can display their content in your selected language.

Change the Language

To set the language for your user interface:

1. Select the appropriate language from the list of available languages.



The screenshot shows a configuration window titled "Language". In the top right corner, there is a button labeled "APPLY". Below the title, there is a list of radio buttons for selecting a language: Chinese, English (selected), Japanese, Korean, Portuguese, and Spanish. At the bottom of the window, there is a yellow note that reads: "* Note changing language will reload the application."

The **APPLY** button located to the top right of the screen enables if your language has changed from the current selection.

2. Select the **APPLY** button to confirm your change of language.

The user interface refreshes immediately. The interface now displays in the language that you selected.

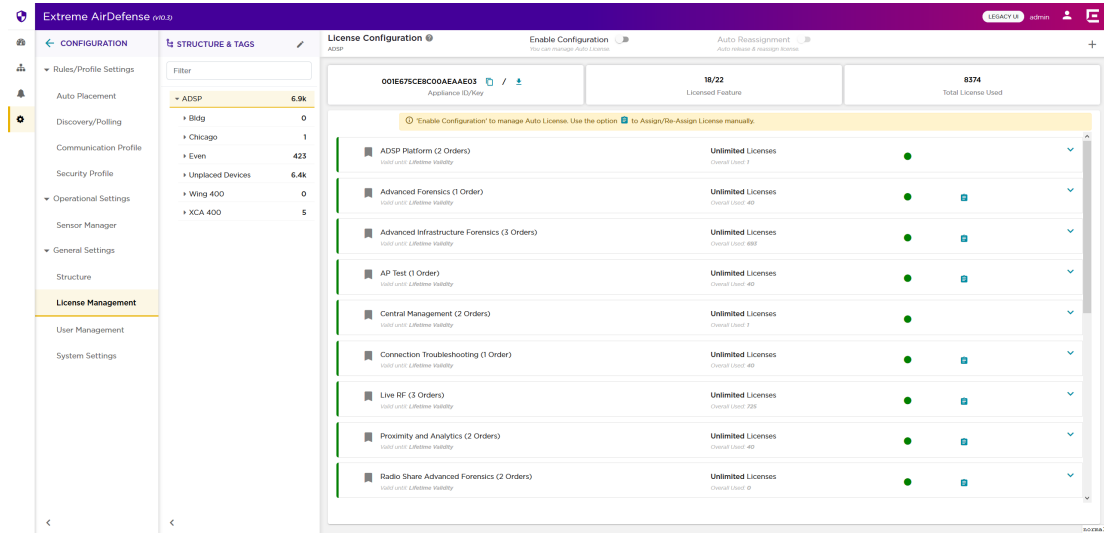
License Management

Use the **License Configuration** screen to manage your AirDefense licenses.

The **License Configuration** screen, in the new user interface, combines the activities performed from the **Configuration > Appliance Platform > Appliance Licensing** and **Configuration > Appliance Platform > Auto-Licensing** screens (from the legacy interface) into it.



The **Auto-Licensing** screen in the legacy user interface enables you to assign licenses automatically when a device is discovered. Similarly, the **Appliance Licensing** screen enables you to assign licenses to individual devices within your network tree.

The **License Configuration** screen is accessed from the **Configuration > License Management** menu path. The following screen displays.

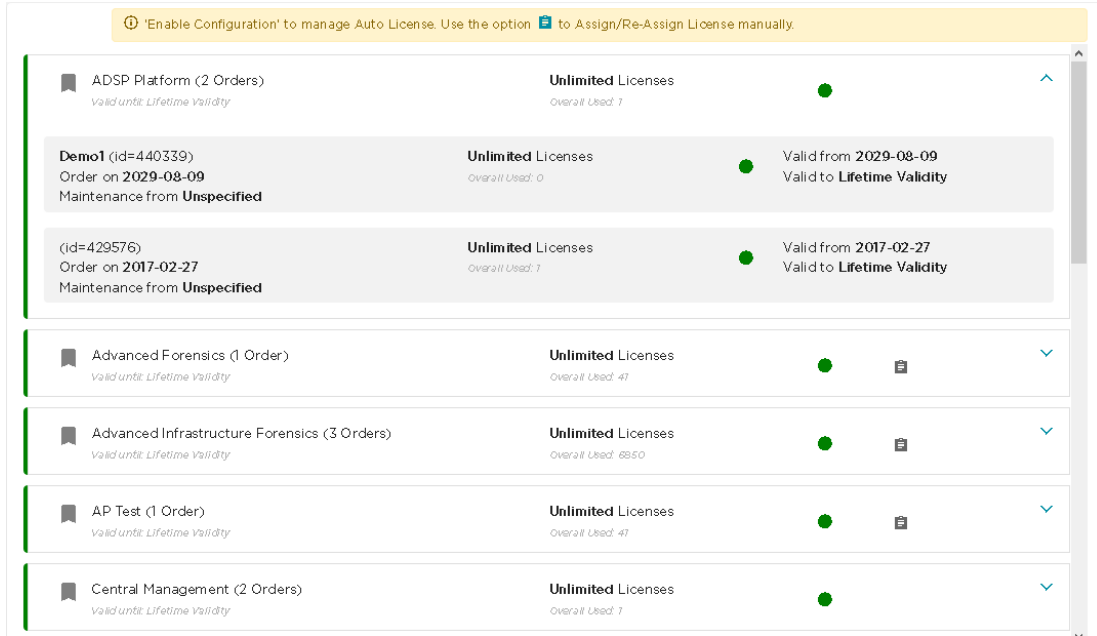


The screen displays two panes. The **Structure & Tags** pane displays the tree of your AirDefense managed network. Use this pane to drill down to the particular device of interest when applying licenses. For more information about this pane, see [View And Manage Your Network Tree](#) on page 151

The **License Configuration** pane displays the list of all licenses available for this AirDefense instance. The **License Configuration** pane displays the following information.

Field	Description
Appliance ID/Key	The unique key or ID assigned to this AirDefense appliance. This ID cannot be modified or removed. This key is required to generate any license that you purchase for use with this AirDefense appliance. Select the  icon to copy this <i>Appliance ID/Key</i> to your PC's clipboard. Select the  icon to download the <i>Appliance ID/Key</i> to a text file.
Licensed Feature	The number of licensed features installed in this AirDefense instance. This field also shows the total number of available AirDefense features.
Total Licenses Used	The count of licenses used by this AirDefense instance.

The list of licenses that are available for this AirDefense instance is also displayed.



For each license, a colored dot indicates the state of the license.



Indicates that all the licenses for this feature are active.



Indicates that some of the multiple licenses applied for this feature have expired. Remaining licenses are still active

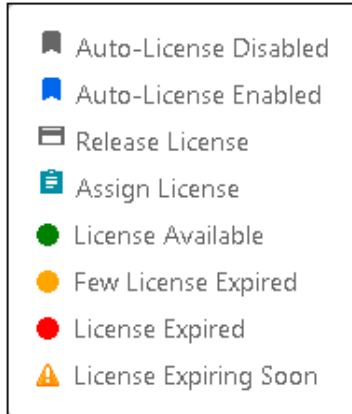


Indicates that all licenses applied for this feature have expired and this feature will not be available for use.



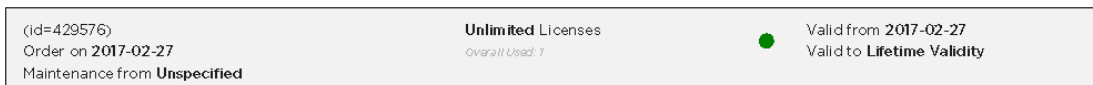
Indicates that some licenses will expire in the near future.

The small icon located to the right of the **License Configuration** label displays a brief explanation of all the icons displayed on this screen. When you hover over this icon, the following popup displays.



You can order a feature's license multiple times to meet your deployment's requirements. Each time you purchase a license for a particular feature, it is recorded separately under that feature's license.

To view a feature's license orders, click on its label. The label expands and displays all the orders for the selected feature. When expanded, this area displays the details of each license ordered. This area also displays a color dot indicating the current state of validity of each license order.



The following information is shown for each order.

Order Date

The date the license was ordered and the license ID number generated by the license management system.

License Count

The number of licenses units in this order. Device count may be 0 (zero), a specific number, or *unlimited*.

Valid From

The date from which this license order become valid and is applied to your AirDefense instance.

Valid Date

The date till which this license is valid. A warning is also displayed if the license is about to expire.

Maintenance Date

Displays the date the license expires and the start date of the maintenance agreement with the customer.

A colored dot indicates the validity state of the order. The following is a list of the various states of the order.



Indicates that the order is valid.



Indicates that the order has expired.



Indicates that the order will expire in the near future.

Overriding License Assignments

The **Enable Configuration** switch is only available when the top most node of the **Structure & Tags** pane is selected. Auto Licenses can only be applied when this switch is set to *ON* and remains *ON*. The top most node is always named *ADSP* and you must use this switch to enable Auto Licensing through out the AirDefense system.

By default, any level in the **Structure & Tags** pane always inherits the licenses from the level above it unless explicitly overridden.

Since Extreme AirDefense manages its devices using a hierarchy that is configured using the **Structure & Tags** pane, all the nodes under the top *ADSP* node inherit the licenses from the top node. However, you can override the inherited licenses at any level in the hierarchy.

To override the inherited licenses, in the **Structure & Tags** pane, select the node where you want to override the inherited licenses. Then from the Override Inherit from: ADSP control, select the **Override** option. Note that the **Inherited from :** control always displays the name of the level from which the licenses are inherited from. Use this information to orient your self on how the licenses are inherited.

Change the licenses for the selected level as required and then use the **APPLY** button to implement the modified license settings. These licenses will now be inherited by all levels below the selected level unless a sub-level has been explicitly overridden.

Auto Reassignment

License Auto Reassignment enables you to manage your license reassignments without manual intervention. Generally, licenses are manually reassigned from any online, offline, or orphan device within your network to those devices that are added to your network. When reassigning a license manually, you would remove the license from an existing device and move it to the new device. This feature does this action automatically if you have enabled it and have adequate number of reassignment licenses that you can use.



Important

License Auto Reassignment works for those licenses that have enabled *Auto License*. For more information, see [Auto License Management](#) on page 324.

When you purchase a feature license, you are also provided with a few reassignment licenses which you can use as required. Reassignments of license is generally done

when a device is being replaced with a newer model or when you are reallocating assets between various sites that you manage.



Important

Please note that, at present, we support license reassignment for the following tri-radio access points: AP 410i, AP 410e, AP 460i, and AP 460e.

For automatic reassignment of licenses, the following rules apply:

1. **Auto License** must be enabled for each feature license that you want to reassign automatically. Feature licenses that do not have **Auto License** enabled, cannot be reassigned automatically.
2. If licenses for a feature are available for use, a license from these free licenses is assigned to the new tri-radio sensor added to your Extreme AirDefense managed network.
3. If no licenses are available for assignment, then the following logic is used to select a license for reassignment.
 - a. Extreme AirDefense searches for orphaned devices within your network. If an orphan device is found, its license is released and added as a re-assignable license. This license is then used for the newly added tri-radio access point.

Orphans are those devices that are no longer managed/monitored by Extreme AirDefense. However, licenses on these devices are not immediately remove but retained for future use. At a later date, when these devices are brought back online, these retained licenses are considered valid by Extreme AirDefense and the devices are joined to the network without consuming additional licenses. For more information on how to manually remove licenses from such orphaned devices, see [Manage License Manually](#) on page 327.

- b. When there are no orphaned devices within the network, Extreme AirDefense scans for and collects a list of all sensors that are considered offline. For Extreme AirDefense, an offline sensor is one that has not reported back to it for a duration of at least six (6) hours.

From this list of offline sensors, Extreme AirDefense releases the license of the sensor that has been offline for the maximum duration. This license is then reassigned to the newly added tri-radio access point.


The **Auto Reassignment** switch is only enabled when you set the **Enable Configuration** to the *ON* position. By default, the **Auto Reassignment** switch is *OFF*. You must manually set this switch to the *ON* position to use Auto License Reassignment.

Auto License Management

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

You may define Auto-Licensing at the appliance network level all the way down to the floor network level, but the best practice is to 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 for the selected level.

The **Override** settings option is available when you select (highlight) a network level below the Appliance level. Use the Expand  icon in the **Structure & Tags** pane to reveal the other levels. By default, the licenses settings are inherited from the level above the current level.

When applying *Auto Licensing* the following rules apply:

- Only selected licenses, those explicitly selected by using the option control next to that license, are assigned automatically
- You can narrow the scope of the license by selecting the network level from the **Structure & Tags** pane.
- A license will not be assigned if there are no licenses available to apply.
- After a license is applied, the number of available licenses is reduced accordingly.

To enable or disable *Auto Licensing* for the selected licenses:

1. Select the **Enable Configuration** switch to enable applying *Auto Licensing* for your various licenses. At a level that is lower than the Appliance level, select the **Override** button.

When you select the **Enable Configuration** switch or the **Override** radio control, option controls appear next to all the licenses.

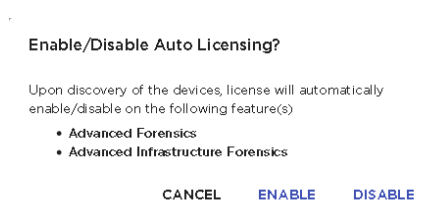


Note



Option controls next to the **ADSP Platform** and **Central Management** are disabled by default as these are the base licenses available with all AirDefense instances.

2. Select the option control for each license that you want to auto apply. The **AUTO LICENSE** button is enabled. This button is located to the top right of the pane.
3. Select those licenses that you want modified and then select the **AUTO LICENSE** button.

The **Enable/Disable Auto Licensing** dialog displays.



4. Review the list of licenses that you have enabled or disabled.
5. Select the **ENABLE** button to enable the selected licenses.

All feature licenses that are auto-licensed are indicated with the  icon. Normal licenses are indicated with the  icon.

The process to change the selected licences from *Auto Licenses* to normal licenses is the same. Select the **DISABLE** button instead.

At anytime, select the **CANCEL** button to cancel this activity.




Important

Please note that *Auto License* is only available till the **Enable Configurations** switch is set to **On**. It is not enabled if the **Enable Configuration** switch is set to **Off**.

Add Licenses

Use the **License Configuration** screen to add new feature license to this AirDefense instance.

License Name	Status	Total License Used
ADSP Platform (2 Orders)	Unlimited Licenses	Overall Used: 0
Advanced Forensics (1 Order)	Unlimited Licenses	Overall Used: 40
Advanced Infrastructure Forensics (3 Orders)	Unlimited Licenses	Overall Used: 888
AP Test (1 Order)	Unlimited Licenses	Overall Used: 40
Central Management (2 Orders)	Unlimited Licenses	Overall Used: 9
Connection Troubleshooting (1 Order)	Unlimited Licenses	Overall Used: 40
Live RF (3 Orders)	Unlimited Licenses	Overall Used: 728
Proximity and Analytics (2 Orders)	Unlimited Licenses	Overall Used: 40
Radio Share Advanced Forensics (2 Orders)	Unlimited Licenses	Overall Used: 0

1. Select the  icon located to the top right of this screen. The **License Verify** screen displays.



License Verify

Please provide License file to verify

*License file only allowed

Browse

Ok, Verify License

Cancel


2. Select the **Browse** button to load the feature license using the operating system's *File Upload* dialog. Navigate to the location where your license file is stored and upload it to the AirDefense system. The **OK, Verify License** button enables.

3. Select the **OK, Verify License** button to verify the license's validity for use with this AirDefense system.
If the license is found to be valid, then the feature is added to the AirDefense system and the licensed feature becomes available through the AirDefense user interface.
4. Use the **Cancel** button to exit without adding the license to your AirDefense system.

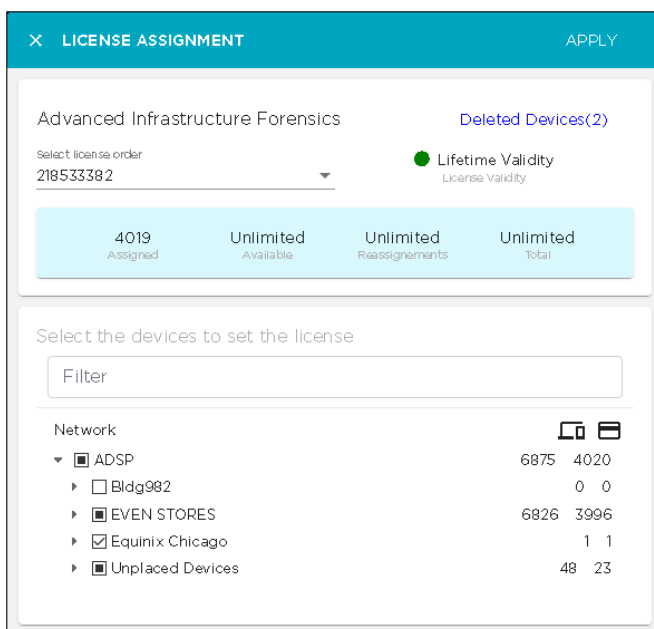
Manage License Manually

Assign licenses manually to have the best control on how your licenses are utilized within your AirDefense monitored network. Use the **License Configuration** screen to manually assign licenses to your devices.

To manually assign licenses:

1. Select the  icon that is available for all licenses except the ADSP Platform and Central Management licenses.

The **License Assignment** dialog displays.




The following information is displayed.

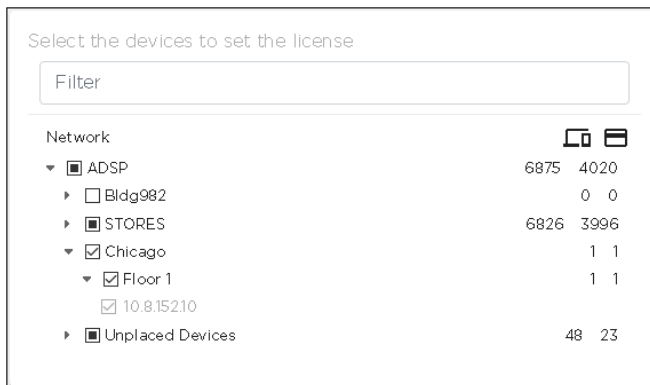
Field	Description
Feature Name	Displays the feature name for which this license detail is displayed.
Select License Order	Use this drop-down list to select a specific license order from which to apply licenses.
Validity	This area displays details about the validity of this license.

The following area displays additional details about the license order selected in the **Select License Order** field.

0 Assigned	50 Available	5 Reassignments	50 Total
---------------	-----------------	--------------------	-------------

Field	Description
Assigned	The number of licenses assigned to devices out of the total licenses in this order.
Available	The number of licenses that are remaining after being assigned, and are thus available for use. For <i>Unlimited</i> licenses, the field will display <i>Unlimited</i> .
Reassignments	Displays the number of reassignments that are left for this license order. AirDefense allows you to reassign your licenses between devices a fixed number of times. Every time a license is reassigned, this value is reduced. Once this value reaches zero (0), you cannot reassign any more licenses. A license is considered reassigned when it is removed from a device and applied to another device. When such a activity is performed, AirDefense reduces the count of reassignments that are available for the selected license order.
Total	Displays the total number of licenses purchased in this license order. Displays <i>Unlimited</i> for <i>Unlimited</i> licenses.

- Use the **Select the devices to set the license** pane within this dialog to drill down to the individual devices that you wish to apply the license. Use the  icon next to each level to expand it.



- Select the option control next to the level or the device name to apply the license. When you select a level, this license is applied to all devices that are found within the selected level.

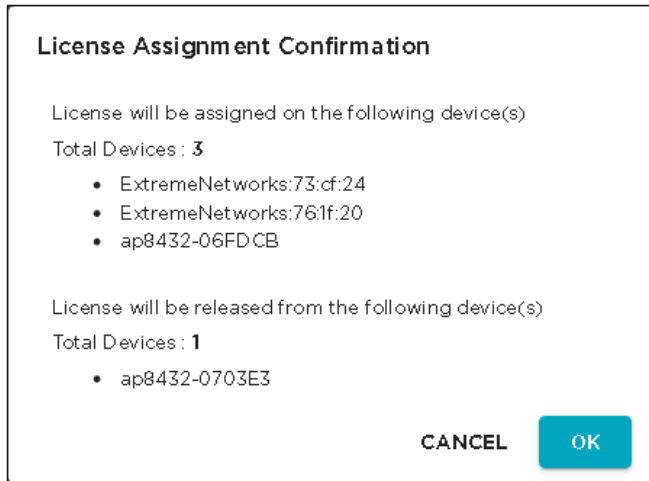
You can also select multiple devices to apply this license to.



Note

Unselect a device's option control to revoke this license from it. You can add and remove licenses to multiple devices simultaneously in one single action. If you revoke permission from a level in the tree, then the selected license is removed from all devices under the selected level.

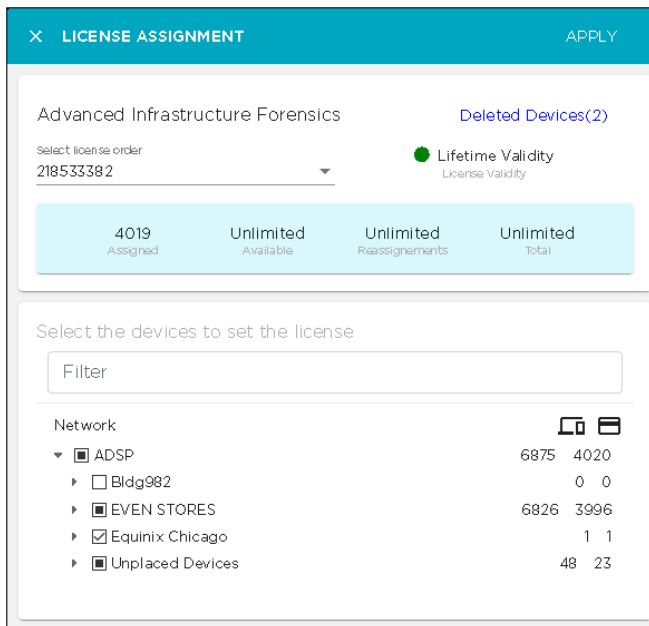
- Select the **APPLY** button to apply the changes made to the selected device or devices' license configuration. This license is added to or removed from the selected device depending on your choice.



- Review the actions that will be performed.
- Select the **OK** button to apply the changes listed in the dialog.
At any time, select the **CANCEL** button to exit without applying the licensing changes made to the devices.

The screen refreshes to display the **License Configuration** screen.

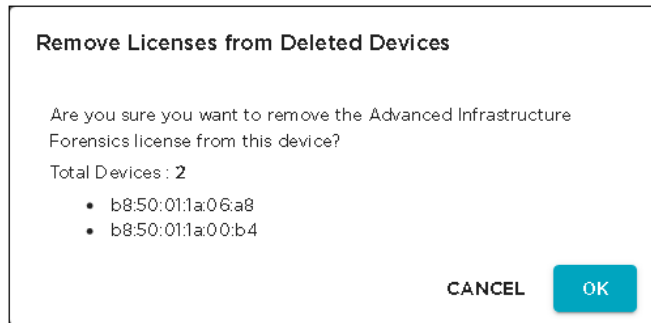
- (Optional) Select the **Deleted Device** link if displayed.



If the **License Assignment** dialog displays **Deleted Devices** in the top right of the screen, it indicates that there are some licenses that are applied to devices that have been deleted from this AirDefense monitored network.

The numerical value next to this control indicates the number of licenses that can be released from these deleted devices.

The following dialog displays.



8. (Optional) Select the **OK** button to apply the changes listed in the dialog.
At any time, select the **CANCEL** button to exit without applying the licensing changes made to the devices.

The screen refreshes to display the **License Configuration** screen.

User Management

Use the **User Management & Configuration** screen to manage the users that are authorized to access your AirDefense instance. User access to various screens in your AirDefense user interface are controlled by the roles assigned to the user account. Depending on the roles assigned, a user may or may not be allowed to view a screen or to modify any details that are displayed on the screen.

AirDefense provides a set of predefined user roles called *User Profile* that encapsulates all the permissions that are applicable to a user assigned this category. By default, the following user profiles are predefined.

- Super Admin
- Admin
- Guest
- Help Desk
- Operation Center

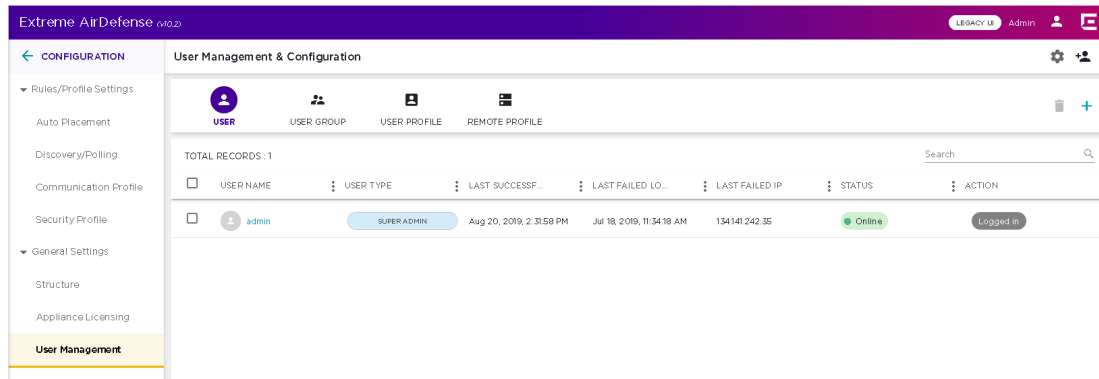
Users can be grouped together as groups for ease of management and permission settings. Use the **User Management & Configuration** screen to create and manage these user groups.

You can also use the **User Management & Configuration** screen to configure user authentication when user credentials are stored in remote RADIUS or LDAP servers.

The following actions can be performed from the **User Management & Configuration** screen.

- Create, modify, and delete AirDefense users.
- Configure the settings for user accounts local to a AirDefense appliance.
- Create, modify, and delete AirDefense user groups.

- Create, modify, and delete AirDefense user profiles.
- Create, modify, and delete remote authentication profiles.



By default, this screen display a list of all the users configured for this AirDefense system.

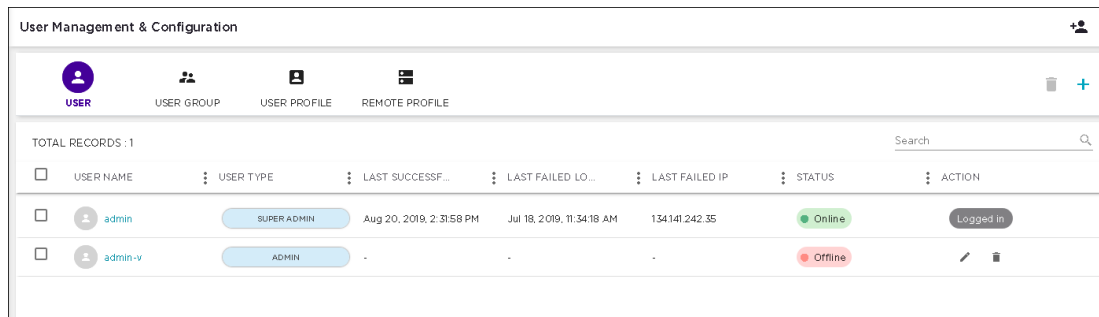
Use the icon located to the top right of this screen to quickly add a user, a user group, a user profile or a remote authentication profile. When selected, this icon expands to display a menu for these options.

Use the icon located to the top right of this screen to configure the permissions for any local user account created on this AirDefense appliance. When selected, a new dialog opens to display the various configurations that can be applied to any local user account. For more information, see [Local User Settings](#) on page 340.



Manage User Accounts

Users are managed from the **User Management & Configuration** screen. This screen is displayed when you select **Settings > User Management** menu path from the AirDefense user interface.

A list of users is displayed by default when you select the **User Management** menu item.



For each user, the following information is displayed:


Field	Description
User Name	The user name.
Profile Name	The user account type. Select this field to view permissions assigned to this user account. The permissions are displayed in a separate popup dialog.
Last Successful Login	The timestamp for the last successful login by this user account.
Last Failed Login	The timestamp for the last failed login attempt by this user.
Last Failed IP	The IP address recorded by AirDefense when this user account failed to login to AirDefense. This information is only recorded for the last failed login attempt by this user.
Status	The current login status of the account.
Action	The actions that can be performed on the user account. For the user account that is logged in, this field displays the term <i>Logged In</i> . For other accounts, you can use the  icon to edit the account or use the  icon to delete the account.

The following activities can be performed from this screen.

- [Add User](#) - Add a new user to the list of valid users for this AirDefense instance .
- [Edit User](#) - Edit the details for an existing user.
- [Delete User](#) - Delete an existing user.

Add User

To add a new user to the list of approved users for this AirDefense instance:

1. Select the  icon located to the top right of this screen.
The **User Creation** dialog displays.

The screenshot shows a 'USER CREATION' dialog box with a teal header containing a close button (X) and a 'CREATE' button. The form contains the following elements:

- A user icon placeholder.
- 'Select User Type' dropdown menu with 'Operation Center' selected.
- 'Full Name' text input field.
- 'Description' text input field.
- 'Select Authentication Type' section with radio buttons for 'Local' (selected) and 'Remote'.
- 'User Name' text input field.
- 'New Password' text input field with an eye icon for visibility toggle.
- 'Confirm Password' text input field with an eye icon for visibility toggle.
- Small text below 'Confirm Password': 'Password Requirements: Minimum 6 character. Maximum 32 characters. Include upper case and lower case. One numeric digit. One Special Character.'
- A blue link: 'VIEW ACCOUNT PREFERENCE'.
- Text: 'Default Settings Enabled'.

2. Use the **Select User Type** drop-down list to select user type to create.
Access to various features of AirDefense depends on the permissions assigned to the selected user type. The default user type is *Operation Center*.
3. In the **Full Name** field, provide a user name for this account.
The name of the user account. This is different from the name entered in the **User Name** field. The name entered in the **User Name** field is used to login into AirDefense. This is a mandatory field.
4. In the **Description** field, provide a brief description about this account.
This information should enable you to uniquely identify this account from similar accounts.
5. From the options available under the **Select Authentication Type** field, select the appropriate authentication type for this new account.
Select from one of **Local** or **Remote**.



Local

Indicates that the new user account will be local to this AirDefense instance.


Remote

Indicates that the new user account will be remote and must be verified with the remote authentication server when used.

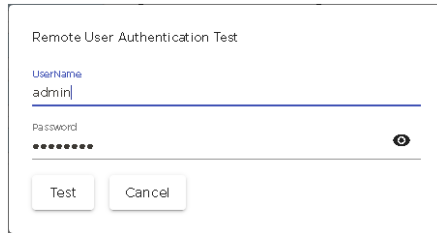
6. When you select `Local` in the **Select Authentication Type** field, the following additional inputs are required.

Field	Description
User Name	The user name for this account. This is a mandatory field. The maximum allowed user name length is 32 characters. Spaces and special characters are not allowed in user names.
New Password	Enter the password for this user account. Follow the password requirement guidelines specified below the Confirm Password field. Use the  icon to view the password entered in this field.
Confirm Password	Enter the same password as entered in the New Password field. This color of this field changes to black only when the passwords that you enter are the same and meet the password guidelines. Use the  icon to view the password entered in this field.

7. When you select `Remote` in the **Select Authentication Type** field, the following additional inputs are required.

Field	Description
User Name	The user name for this account. This is a mandatory field. The maximum allowed user name length is 32 characters. Spaces and special characters are not allowed in user names.
Select Remote Profile Name	The remote authentication profile to use. Use the Select Remote Profile Name drop-down list to select the authentication profile to use. This configuration is defined in the Remote Profile screen. To create a new <i>Authentication Profile</i> , expand the drop-down list and then select the <i>Add New Profile</i> entry in the list. The <code>All</code> menu item is the only selectable option available within this drop-down list. Support for other items will be enabled in future.
Enable Fall back local authentication	Set this switch to <code>ON</code> to enable local authentication of this user account if remote authentication fails. AirDefense will use the supplied password to enable this user to login successfully. Fallback Local Password The password for this user account as stored locally. Use the  icon to view the entered password. Confirm Password Re-enter the password to verify that the correct password is been entered.

- Use the **TEST CONNECTION** field to test if the connection to the remote server is successful. The following dialog opens.

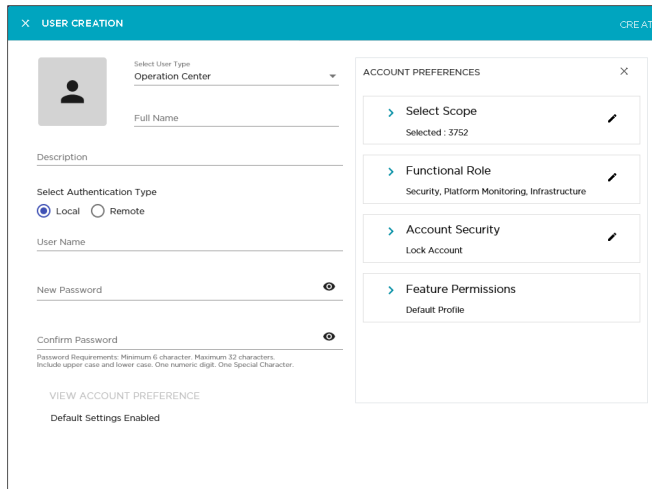


Provide the correct username and password for testing the remote connection and then select the **Test** button to test the connection.

The status of this test is indicated within this dialog.

- Select the **VIEW ACCOUNT PREFERENCE** button to configure additional settings for this new user account.

The **USER CREATION** window expands to display additional fields.

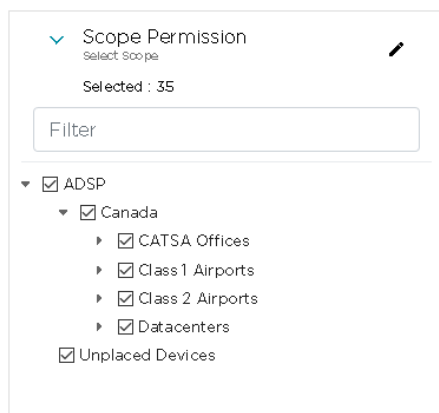


The following fields are displayed.

Field	Description
Scope Permission	This field sets the scope in the AirDefense network tree where this user account is considered valid. Expand this field and select the scope for this setting.
Functional Role	This field sets the functional roles that can be performed. Expand this field to view and edit the various parameters for this setting.
Account Security	This field sets the user account's security settings. Expand this field to view and edit the various parameters for this setting.
Feature Permissions	This field sets the permissions that can be assigned. Expand this field to view and edit the various parameters for this setting.

10. Select the **Scope Permission** label to expand it.

The **Scope Permission** field displays a selectable network tree for this AirDefense instance.



When you select or unselect any level in this network tree, all sub-levels under the level are selected or unselected respectively. A selected level is indicated by icon. A unselected level is blank.

Use the option control next to each level to include or exclude that level when the user account is considered valid in this AirDefense instance. When a level is selected, the configuration is applied to all its sub-levels. Use the option controls for each level to apply or revoke the user's permission on that level.

11. Select the **Functional Role** label to expand it.

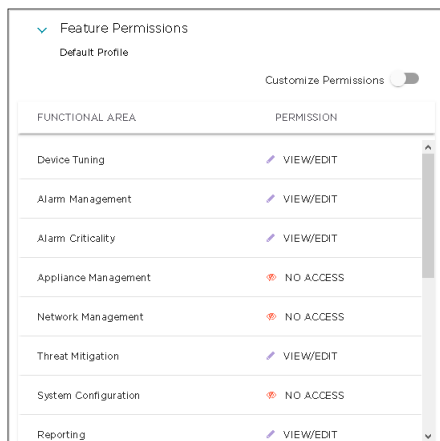
The following additional fields are displayed. Select each option to enable or disable that functional role.

Field	Description
Security	When selected, this option grants permission to manage Security alarms. Is enabled by default.
Performance Monitoring Troubleshooting	When selected, this option grants permission to manage alarms that monitor the AirDefense system performance and alarms generated by the troubleshooting features such as AP Test. Is enabled by default.
Platform Monitoring	When selected, this option grants permission to manage alarms that monitor the AirDefense system (platform). Is enabled by default.
Infrastructure Management	When selected, this option grants permission to manage alarms that are generated by the infrastructure management features. Is enabled by default.
Locationing	When selected, this option grants permission to manage alarms triggered by the Location Based Services system. Is enabled by default.


- Select the **Account Security** label to expand it.
The following additional fields are displayed. Select each option to enable or disable that security feature. These fields control the security of this new user account.

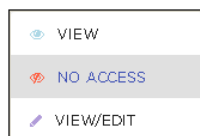
Field	Description
Lock Account	When selected, the account is locked and cannot be used for logging into this AirDefense instance. Is not enabled by default. Use this option to prepare a user account for later deployment or to temporarily suspend a user account.
Lock after ...	When selected, enter the number of days of inactivity to consider before the account is automatically deactivated. Is not enabled by default. Use this option to create accounts that automatically expire after a set number of days.
Change password at next logon	When selected, the user is forced to change password at next logon. This option is not available for <i>Remote</i> accounts.

- Select the **Feature Permissions** label to expand it.
Review the **FUNCTIONAL AREA** and the **PERMISSION** fields. This area lists all the functional areas of AirDefense and the permission that can be set to view or edit that area. If no permission is granted for that particular functional area, the value *NO ACCESS* is displayed for it.



Permissions to view and edit particular areas of AirDefense is set based on the permissions configured in the *User Profile* selected when creating any user or user group.

Select the **Customize Permissions** control to enable editing these permissions individually. After enabling the **Customize Permissions** field, select the  icon located next to the current permission for the functional area that you wish to modify permissions for. The drop-down expands and lists the available permissions that can be applied to the functional area.



The following permissions can be applied to each functional area.

View

Grants permission to view all screens of the functional area. Editing is not permitted in these screens.

No Access

When selected, access is not granted to this functional area. The menus used to access these functional areas are also not displayed.


View/Edit

Grants permission to view and edit all the screens of the functional area and modify the fields in that area. The permission grants full control over this functional area.

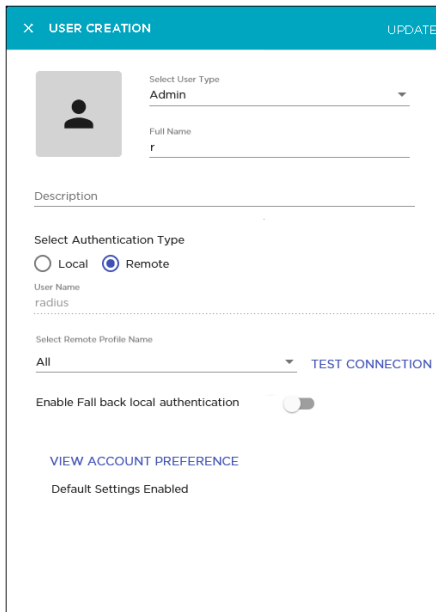
14. Select the **CREATE** button located to the top of this dialog to save the newly created user account.

At any point of time, if you wish to exit without creating the user account, select the small **X** button located to the top left of this dialog.

Edit User Information

You can edit any user in the **User Management & Configuration** screen by selecting the  icon next to its entry in this list.

AirDefense uses the **User Creation** screen to edit the user account details.



USER CREATION UPDATE

Select User Type
Admin

Full Name
r

Description

Select Authentication Type
 Local Remote

User Name
radius

Select Remote Profile Name
All TEST CONNECTION

Enable Fall back local authentication

[VIEW ACCOUNT PREFERENCE](#)
Default Settings Enabled

All details for this user account are pre-filled in the fields of this screen and can be modified. However, you cannot modify the **User Name** for the selected account.

**Note**

If you do not want to modify your account's password, do not modify the password entered in the **New Password** field. When saving your other modifications, AirDefense will retain the existing password for this account. However, if you only want to modify the password for this account, enter the same password in the **New Password** and the **Confirm Password** fields and then save your changes.


1. Review the fields in this screen. Make the modifications as required.
For more information on the fields of this screen, see [Add User](#) on page 332.
2. Select the **UPDATE** button to save the changes made to this user account information.
Use the small **X** button located to the top left of the dialog to close it. AirDefense does not prompt you to save your changes when exiting this dialog. You will lose any unsaved changes when exiting this dialog.

Delete User Account

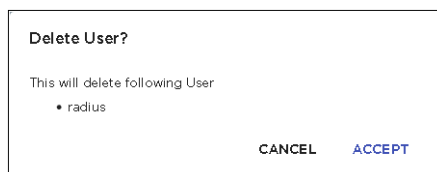
Use the **User Management & Configuration** screen to delete any user account added to this AirDefense instance.

**Note**

You cannot delete the account that you have used to login into the AirDefense instance.

1. If not selected, select the **User** icon from the toolbar.
2. From the list of user accounts that are saved for this AirDefense instance, select the account that you want to delete. Then select the  icon located to the right of this user account's entry.


The **Delete User** dialog displays.



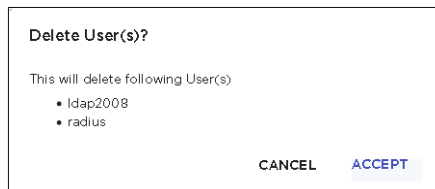
3. Review the account name listed in this dialog.
4. Select the **ACCEPT** button to delete the selected user account.
At anytime, select the **CANCEL** button to exit without deleting this user account.

The selected user account is deleted and removed from the list of valid accounts for this AirDefense instance.

- The option control in the first column of each user account entry enables you to select multiple accounts simultaneously. To delete many accounts in the same action, select this option control for each of those accounts that you wish to delete.

The  icon located on top right of this list enables. Select this icon to delete the selected user accounts.

The **Delete User(s)** dialog opens.



- Review the list of accounts that you wish to delete.
- Select the **ACCEPT** button to delete the selected user accounts.

At anytime, select the **CANCEL** button to exit without deleting these user accounts.

The selected user accounts are deleted and removed from the list of valid accounts for this AirDefense instance.

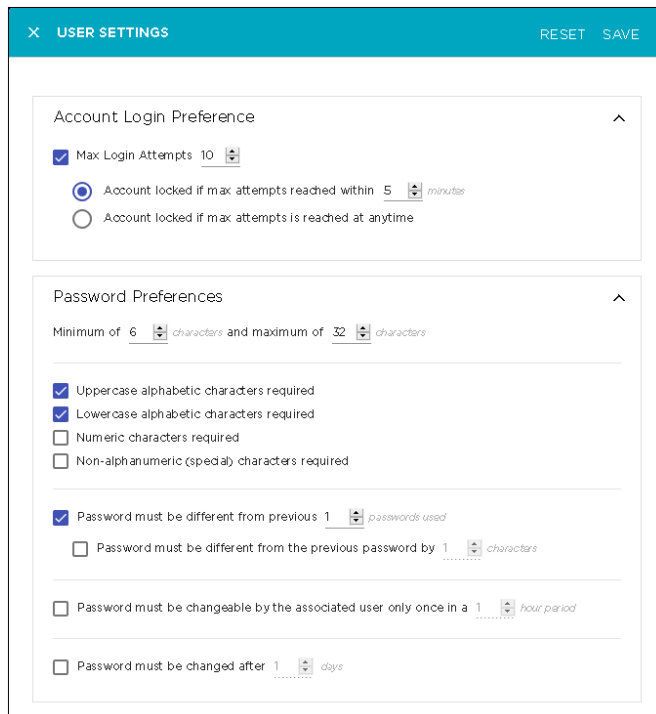
Local User Settings

The **User Settings** dialog of the **User Management** screen configures the settings for all local user accounts configured on this AirDefense appliance.

In the legacy user interface, the settings in this dialog are managed from the **Configuration > Account Management > Local Authentication** screen.

- Select the  icon located to the top right of the **User Management & Configuration** screen

The **User Settings** dialog displays.



2. Configure the following **Account Login Preference** parameters.

Field	Description
Max Login Attempts	Use the spinner control to set the maximum number of failed login attempts allowed before the user account is locked.
Account locked if max attempts reached within ...	Use the spinner control to set this value. When set, the user account is locked if the number of attempts specified in the Max Login Attempts control is exceeded in the time specified, in minutes, by this control. For example, if this value is set to five (5) and the Max Login Attempts value is set to ten (10), then the account is locked if an user tries and fails to login for ten (10) times within a span of five (5) minutes. This failure count is reset every time a user successfully logs in.
Account locked if max attempts is reached anytime	When selected, an account is locked immediately when the number of failed attempts exceeds the value set in the Max Login Attempts control. This failure count is reset every time a user successfully logs in.

3. Configure the following **Password Preference** parameters.

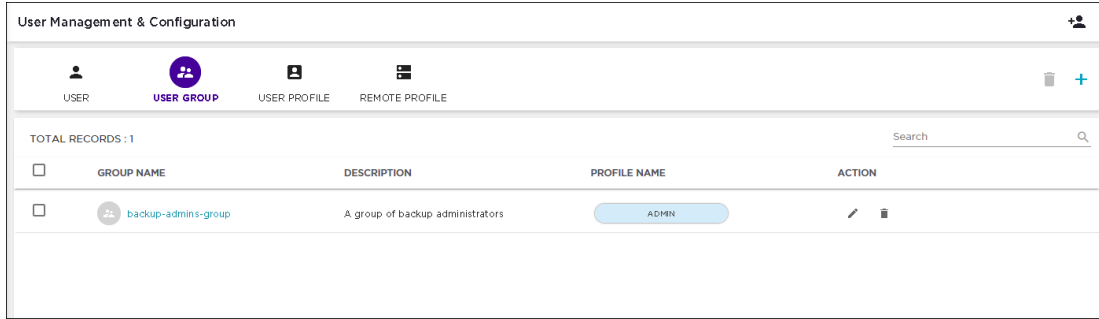
Field	Description
Minimum of ... Characters	Use the first spinner control to set the minimum length for the local user account passwords. The default value is <i>6</i> . The maximum value that can be selected is <i>100</i> .
Maximum of ... Characters	Use the second spinner control to set the maximum length for the local user account passwords. The default value is <i>32</i> . The maximum value that can be selected is <i>100</i> .
Uppercase alphabetic characters required	Select this option to ensure that Uppercase alphabets are included in the user account password.
Lowercase alphabetic characters required	Select this option to ensure that Lowercase alphabets are included in the user account password.
Numeric characters required	Select this option to ensure that numbers are included in the user account password.
Non-alphanumeric (special) characters required	Select this option to ensure that non-alphanumeric characters such as #, \$, %, ^, are included in the user account password.
Password must be different from previous ... passwords used	Select this option to ensure that passwords are not reused. Use the spinner control set the number of previous passwords that the current password must not match for it to be considered valid.
Password must be different from the previous password by ... characters	Select this option to ensure that the current password does not match any previous password. Use the spinner control to enforce the number of characters that the passwords must differ by.
Password must be changeable by the associated user only once in a ... hour period	Select this option to prevent a user from frequently changing the password. Use the spinner control to set the time limit in hours within which the user cannot reset the password.
Password must be changed after ... days	Select this option to enforce password expiry. Use the spinner control to set the number of days after which the user is forced to change the password.

4. Select the **SAVE** button to save the changes made to the **User Settings** screen.



Select the **RESET** button to reset the changes made to this screen. All your changes will be lost on reset.

User Group Management

User Groups are managed from the **User Management & Configuration** screen. In the **User Management & Configuration** screen, select the **User Group** button. The **User Management & Configuration** screen displays a list of all user groups created for this AirDefense instance.



For each user group, the following information is displayed.


Field	Description
Group Name	The name of this group. Click the group name to edit its information.
Description	The description assigned to this user group.
Profile Name	The user profile applied to this user group. Click this field to view permissions assigned to this user group. This information is fetched from the user profile used to create this user group and any customizations that you have made to it. The permissions are displayed in a separate popup dialog.
Action	The actions that can be performed on this user group. You can use the  icon to edit the user group or use the  icon to delete the user group.

The following activities can be performed from this screen.

- [Add User Group](#) - Add a new user group for this AirDefense instance.
- [Edit User Group](#) - Edit the details for an existing user group.
- [Delete User Group](#) - Delete an existing user group.

Add User Group

To add a new user group to the list of user groups used with this AirDefense instance:

1. Select the  icon located to the top right of this screen. The **User Group Creation** dialog displays.

2. Use the **Select User Type** drop-down list to select user type to create.
Access to various features of AirDefense depends on the permissions assigned to the selected user type. The default user type is *Operation Center*.
3. In the **Group Name** field, provide a name for this user group.
This is a mandatory field.
4. In the **Description** field, provide a brief description about this user group and its purpose.
This information should enable you to uniquely identify this user group from similar groups.
5. Use the **Select Remote Profile Name** drop-down list to select the authentication profile to use. This configuration is defined in the [Remote Profile](#) screen. To create a new *Authentication Profile*, expand the drop-down list and then select the *Add New Profile* entry in the list.
The **All** menu item is the only selectable option available within this drop-down list. Support for other items will be enabled in future.
6. Use the **TEST CONNECTION** field to test if the connection to the remote server is successful. The following dialog opens.

Provide the correct username and password for testing the remote connection and then select the **Test** button to test the connection.

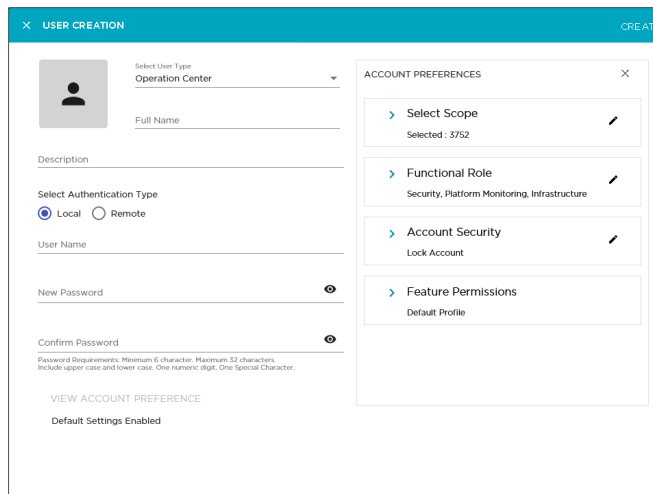
The status of this test is indicated within this dialog.

7. Select the **Disable group login** control to prevent users belonging to this group from logging into this AirDefense instance.

When a user is authenticated from a RADIUS or LDAP server, and when *Group Authentication* is enabled, the authentication servers return the group name to which the user belongs. This group name is verified with the local AirDefense groups and if the group is found, the user is allowed access. Use this option to temporarily suspend users belonging to this group from accessing this AirDefense instance.

8. Select the **VIEW ACCOUNT PREFERENCE** button to configure additional settings for this new user account.

The **USER CREATION** window expands to display additional fields.

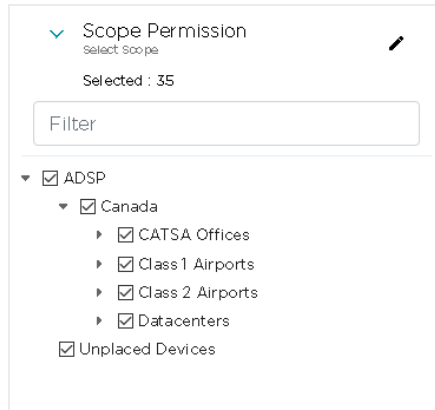


The following fields are displayed.

Field	Description
Scope Permission	This field sets the scope in the AirDefense network tree where this user account is considered valid. Expand this field and select the scope for this setting.
Functional Role	This field sets the functional roles that can be performed. Expand this field to view and edit the various parameters for this setting.
Account Security	This field sets the user account's security settings. Expand this field to view and edit the various parameters for this setting.
Feature Permissions	This field sets the permissions that can be assigned. Expand this field to view and edit the various parameters for this setting.

9. Select the **Scope Permission** label to expand it.

The **Scope Permission** field displays a selectable network tree for this AirDefense instance.



When you select or unselect any level in this network tree, all sub-levels under the level are selected or unselected respectively. A selected level is indicated by icon. A unselected level is blank.

Use the option control next to each level to include or exclude that level when the user account is considered valid in this AirDefense instance. When a level is selected, the configuration is applied to all its sub-levels. Use the option controls for each level to apply or revoke the user's permission on that level.

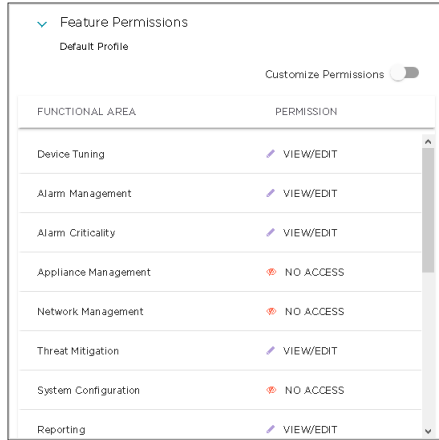
10. Select the **Functional Role** label to expand it.

The following additional fields are displayed. Select each option to enable or disable that functional role.


Field	Description
Security	When selected, this option grants permission to manage Security alarms. Is enabled by default.
Performance Monitoring Troubleshooting	When selected, this option grants permission to manage alarms that monitor the AirDefense system performance and alarms generated by the troubleshooting features such as AP Test. Is enabled by default.
Platform Monitoring	When selected, this option grants permission to manage alarms that monitor the AirDefense system (platform). Is enabled by default.
Infrastructure Management	When selected, this option grants permission to manage alarms that are generated by the infrastructure management features. Is enabled by default.
Locationing	When selected, this option grants permission to manage alarms triggered by the Location Based Services system. Is enabled by default.

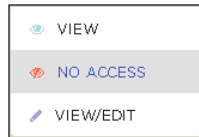
11. Select the **Feature Permissions** label to expand it.

Review the **FUNCTIONAL AREA** and the **PERMISSION** fields. This area lists all the functional areas of AirDefense and the permission that can be set to view or edit that area. If no permission is granted for that particular functional area, the value *NO ACCESS* is displayed for it.



Permissions to view and edit particular areas of AirDefense is set based on the permissions configured in the *User Profile* selected when creating any user or user group.

Select the **Customize Permissions** control to enable editing these permissions individually. After enabling the **Customize Permissions** field, select the  icon located next to the current permission for the functional area that you wish to modify permissions for. The drop-down expands and lists the available permissions that can be applied to the functional area.



The following permissions can be applied to each functional area.

View

Grants permission to view all screens of the functional area. Editing is not permitted in these screens.

No Access

When selected, access is not granted to this functional area. The menus used to access these functional areas are also not displayed.


View/Edit

Grants permission to view and edit all the screens of the functional area and modify the fields in that area. The permission grants full control over this functional area.

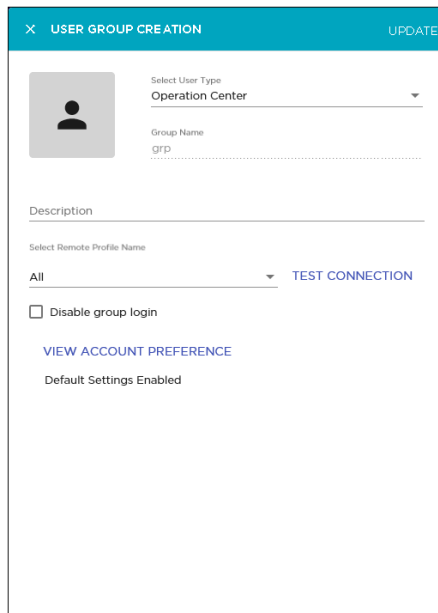
12. Select the **CREATE** button located to the top of this dialog to save the newly created user group.

At any point of time, if you wish to exit without creating the user group, select the small **X** button located to the top left of this dialog.

Edit User Group Information

You can edit any user group in the **User Management & Configuration** screen by selecting the  icon next to its entry in this list.

AirDefense uses the **User Group Creation** screen to edit user group details.




All details for this user group are pre-filled in the fields of this screen and can be modified. However, you cannot modify the **Group Name** for the selected group.

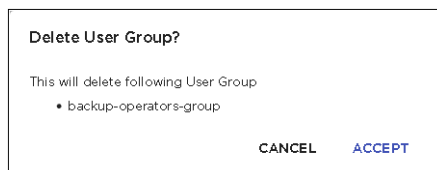
1. Review the fields in this screen. Make the modifications as required.
For more information on the fields of this screen, see [Add User Group](#) on page 343
2. Select the **UPDATE** button to save the changes made to this user group information.
Use the small **X** button located to the top left of this dialog to close it. AirDefense does not prompt you to save your changes when exiting this dialog. Unsaved changes are not saved when exiting this dialog.

Delete User Group

Use the **User Management & Configuration** screen to delete any user group added to this AirDefense instance.

1. If not selected, select the **User Group** icon from the toolbar.
2. From the list of user groups that are created for this AirDefense instance, select the user group that you want to delete. Then select the  icon located to the right of this user group's entry.

The **Delete User Group** dialog displays.




3. Review the user group name listed in this dialog.

4. Select the **ACCEPT** button to delete the selected user group.

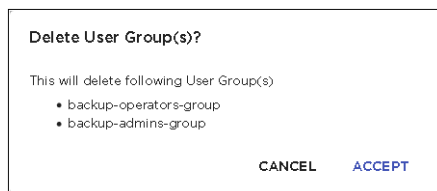
At anytime, select the **CANCEL** button to exit without deleting this user group.

The selected user group is deleted and removed from the list of valid user groups for this AirDefense instance.

5. The option control in the first column of each user group entry enables you to select multiple groups simultaneously. To delete many groups in the same action, select this option control for each of those groups that you wish to delete.

The  icon located to the top right of this list enables. Select this icon to delete the selected user groups.

The **Delete User Group(s)** dialog opens.



6. Review the list of user groups that you wish to delete.
7. Select the **ACCEPT** button to delete the selected user groups.

At anytime, select the **CANCEL** button to exit without deleting these user groups.

The selected user groups are deleted and removed from the list of valid user groups for this AirDefense instance.

User Profile Management

User Profiles are used to configure a set of permissions and other settings that can be applied to new and existing user accounts. AirDefense provides a few pre-created user profiles with commonly used permissions already defined within these profiles. These pre-created profiles are:

- *Super Admin* - This user profile is used only for the account that is created as the default account for this AirDefense instance. There is only one account with this user profile in any instance of AirDefense.
- *Admin* - This user profile is used to provide full administrative control to this instance of AirDefense. You can have multiple users with this user profile.
- *Guest* - This user profile is used to grant some minimum set of permissions to users to view some of the functional areas within this AirDefense instance.

- *Help Desk* - This user profile is used to grant certain permissions to users that act as help desk for resolving issues with this instance of AirDefense.
- *Operation Center* - This user profile provides higher access than *Help Desk* users and is generally granted to a networks operation center user to manage this AirDefense instance from a remote location.



Important

Please note that the user profiles that are marked as *Default* in the **Profile Type** field are created by the AirDefense system and cannot be edited or deleted. You can use these default profiles as a template to create your customized user profiles.

User Profiles are managed from the **User Management & Configuration** screen. In the **User Management & Configuration** screen, select the **User Profile** button. The **User Management & Configuration** screen displays a list of all the user profiles configured for this AirDefense instance.


User Management & Configuration					
USER USER GROUP USER PROFILE REMOTE PROFILE					
TOTAL RECORDS : 6 Search <input type="text"/>					
<input type="checkbox"/>	PROFILE NAME	PROFILE TYPE	USAGES	PROFILE SINCE	ACTION
<input type="checkbox"/>	Super Admin	Default	1	-	
<input type="checkbox"/>	Admin	Default	2	-	
<input type="checkbox"/>	Guest	Default	0	-	
<input type="checkbox"/>	Help Desk	Default	0	-	
<input type="checkbox"/>	Operation Center	Default	0	-	
<input type="checkbox"/>	Restricted Operation Center	Custom	0	Oct 08, 2019, 10:43:37 AM	

For each user profile, the following information is displayed.

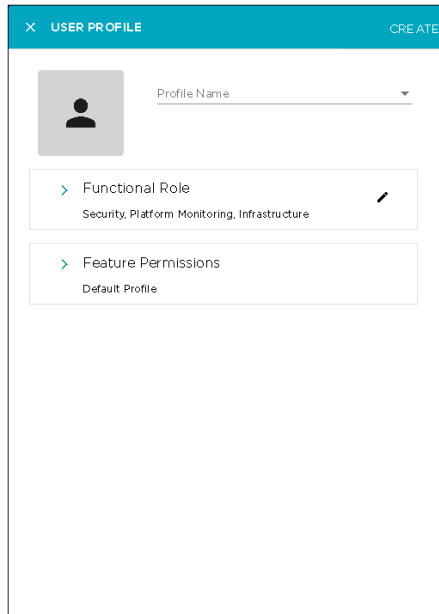
Field	Description
Profile Name	The name of this user profile.
Profile Type	The profile type. For a profile created by the AirDefense system, this field displays <i>Default</i> . For all user created profiles, this field displays <i>Custom</i> .
Usages	The number of times this profiles was assigned to user accounts valid for this AirDefense instance.
Profile Since	The time stamp when this user profile was created. This is only shown for profiles that are created by users and are marked as <i>Custom</i> in the Profile Type field.
Action	The actions that can be performed on this user profile. You can use the icon to edit this user profile or use the icon to delete this user profile. These actions are not enabled for profiles that are marked as <i>Default</i> in the Profile Type field.

Add User Profile

To add a new custom user profile to the list of valid profiles used with this AirDefense instance:

1. Select the  icon to the top right of this screen.

The **User Profile Creation** dialog displays.



2. In the **Profile Name** field, provide a name for this user profile.

This is a mandatory field.

3. Select the **Functional Role** label to expand it.

The following additional fields are displayed. Select each option to enable or disable that functional role.


Field	Description
Security	When selected, this option grants permission to manage Security alarms. Is enabled by default.
Performance Monitoring Troubleshooting	When selected, this option grants permission to manage alarms that monitor the AirDefense system performance and alarms generated by the troubleshooting features such as AP Test. Is enabled by default.
Platform Monitoring	When selected, this option grants permission to manage alarms that monitor the AirDefense system (platform). Is enabled by default.
Infrastructure Management	When selected, this option grants permission to manage alarms that are generated by the infrastructure management features. Is enabled by default.
Locationing	When selected, this option grants permission to manage alarms triggered by the Location Based Services system. Is enabled by default.

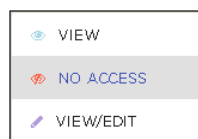
4. Select the **Feature Permissions** label to expand it.

Review the **FUNCTIONAL AREA** and the **PERMISSION** fields. This area lists all the functional areas of AirDefense and the permissions that can be set to view or edit that area. If no permissions are granted for that particular functional area, the value *NO ACCESS* is displayed for it.

FUNCTIONAL AREA	PERMISSION
Device Tuning	VIEW/EDIT
Alarm Management	VIEW/EDIT
Alarm Criticality	VIEW/EDIT
Appliance Management	NO ACCESS
Network Management	NO ACCESS
Threat Mitigation	VIEW/EDIT
System Configuration	NO ACCESS
Reporting	VIEW/EDIT
Analysis Tools	VIEW/EDIT

Permissions to view and edit particular areas of AirDefense is set based on the permissions configured in the *User Type* selected when creating any user or user group.

Select the **Edit** button to enable editing these permissions individually. Select the  icon located next to the current permission for the functional area that you wish to modify permissions for. The drop-down expands and lists the available permissions that can be applied to the functional area.



The following permissions can be applied to each functional area.

View

Grants permission to view all screens of the functional area. Editing is not permitted in these screens.

No Access

When selected, access is not granted to this functional area. The menus used to access these functional areas are also not displayed.

View/Edit

Grants permission to view and edit all the screens of the functional area and modify the fields in that area. The permission grants full control over this functional area.

5. Select the **CREATE** button located to the top of this dialog to save the newly created user profile.

At any point of time, if you wish to exit without creating the user profile, select the small **X** button located to the top left of this dialog.




Note

Please note that this user profile will be created as a *Custom* profile inside the AirDefense instance.

Edit User Profile

You can edit any user profile marked as *CUSTOM* in the **Profile Type** field in the **User**

Management & Configuration screen. Use the  icon next to the user profile's entry in this list.



Important

Profiles marked as *DEFAULT* in the **Profile Type** field are created by the AirDefense system and cannot be modified.

AirDefense uses the **User Profile** screen to edit user profile details.

All details for this user profile are pre-filled or set for all the fields of this screen and can be modified. However, you cannot modify the **Profile Name** for the selected profile.

1. Review the fields in this screen. Make the modifications as required.
For more information on the fields of this screen, see [Add User Profile](#) on page 351.
2. Select the **UPDATE** button to save the changes made to this user profile information.
Use the small **X** button located to the top left of this dialog to close it. AirDefense does not prompt you to save your changes when exiting this dialog. If there are any unsaved changes when exiting this dialog, they are lost.


Delete User Profile

Use the **User Management & Configuration** screen to delete any user profile added to this AirDefense instance.

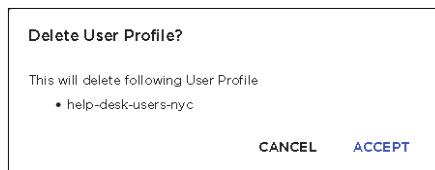


Important

You cannot delete any profile marked as *DEFAULT* in this screen. These are created by the ExtremeLocation system and cannot be edited or deleted.

1. If not selected, select the **User Profile** icon from the toolbar.
2. From the list of user profiles created for this AirDefense instance, select the profile that you want to delete. Then select the  icon to the right of this user profile's entry.

The **Delete User Profile** dialog displays.




3. Review the user profile listed in this dialog.
4. Select the **ACCEPT** button to delete the selected profile.

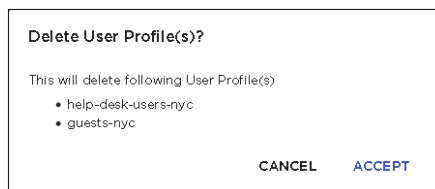
At anytime, select the **CANCEL** button to exit without deleting this user profile.

The selected user profile is deleted and removed from the list of valid profiles for this AirDefense instance.

5. The option control in the first column of each user profile entry enables you to select multiple profiles simultaneously. To delete many profiles in the same action, select this option control for each of those profiles that you wish to delete.

The  icon located to the top right of this list enables. Select this icon to delete the selected user profiles.

The **Delete User Profile(s)** dialog opens.



6. Review the list of user profiles that you wish to delete.
7. Select the **ACCEPT** button to delete the selected user profiles.

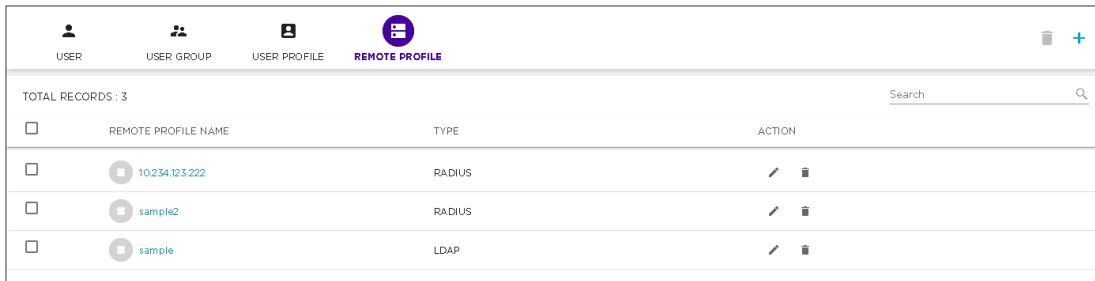
At anytime, select the **CANCEL** button to exit without deleting these user profiles.

The selected user profiles are deleted and removed from the list of valid user profiles for this AirDefense instance.

Remote Profile Management

Remote Profiles are used to configure the user authentication parameters required to authenticate users on remote RADIUS or LDAP servers. Storing user credentials on a centralized data store reduces the cost of managing user credentials across different systems and avoids replication of the same data across multiple databases.

Remote Profiles are managed from the **User Management & Configuration** screen. In the **User Management & Configuration** screen, select the **Remote Profile** button. The **User Management & Configuration** screen displays a list of all remote profiles configured for this AirDefense instance.



For each remote profile, the following information is displayed.

Field	Description
Remote Profile Name	The name of this remote profile.
Type	The type of this profile. Displays <i>RADIUS</i> if the remote server is a RADIUS server. Displays <i>LDAP</i> if the remote server is a LDAP server.
Action	The actions that can be performed on this remote profile. You can use the icon to edit this remote profile or use the icon to delete this remote profile.

The following activities can be performed from this screen.

- [Add Remote Profile](#) - Add a new remote profile for this AirDefense instance.
- [Edit Remote Profile](#) - Edit the details for an existing remote profile.
- [Delete Remote Profile](#) - Delete an existing remote profile.

Add Remote Profile

To add a new remote profile to the list of valid profiles used with this AirDefense instance.

1. Select the icon to the top right of this screen. The **Remote Authentication** dialog displays.

The screenshot shows a configuration window titled 'REMOTE AUTHENTICATION' with a 'CREATE' button in the top right. The form contains the following fields and options:

- Remote Server Name:** A text input field.
- Type:** A dropdown menu currently showing 'LDAP'.
- LDAP/LDAPS Selection:** Two radio buttons, with 'LDAP' selected.
- LDAP Server:** A text input field containing '192.168.0.1'.
- LDAP Port:** A text input field containing '389'.
- User Prefix:** A text input field with the example 'CN='.
- User Suffix:** A text input field with the example 'DN=MyCompany,DC=room'.
- Use LDAP for external group based authentication:** An unchecked checkbox.

- In the **Remote Server Name** field, provide a name for this profile.
This is a mandatory field.
- From the **Type** drop-down list, select the type of remote authentication server used to authenticate your users.

Select from one of *LDAP* or *RADIUS*.

LDAP

Indicates that the remote authentication server is a LDAP server.

RADIUS

Indicates that the remote authentication server is a RADIUS server.

- When you select *LDAP* in the **Type** field, the following additional inputs are required.
Select one of **LDAP** or **LDAPS** as your server type.

Field	Description
LDAP Server	The IP address of the remote LDAP server.
LDAP Port	The port on which the LDAP authentication server is listening. The default LDAP port is 389.
User Prefix	The name of the windows domain for the server. This field 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 find out the correct option that works with your LDAP deployment.

Field	Description
User Suffix	Enter the domain name for this server. This field is optional. You can leave this field blank or supply a valid suffix.
Use LDAP for external group based authentication	Select this option to enable authentication of a user with a LDAP server based on the group that the user account is a member of.

5. When you select `Use LDAP for external group based authentication` option, the following additional fields are displayed.

Field	Description
Server Type	The server type of the remote LDAP server. This value is always <code>Active Directory</code> . The other fields are used in group identification for the Active Directory server type.
Search base	The name of your domain in the Active Directory. Use the format <code>DC=<your-domain-name>DC=<your-domain-name></code> . The Search base field should be the same as the User Prefix field but without any backslashes (<code>/</code>).
User field name	Enter a string to find your user name in the Active Directory. Normally, this string is <code>sAMAccountName</code> .
Group attribute	Enter a string to find your group name in the Active Directory. Normally this string is <code>memberOf</code> .
Group Reg Ex	Enter a string that is used to strip out the unnecessary information and send only that information that is relevant for AirDefense for use in group identification. Normally, this string is <code>CN= ([^,]*)</code> .



Note


If your LDAP administrator changes any of the above strings, your authentication will fail. Please ask your LDAP administrator to inform you of any changes in the above strings.

6. When you select `RADIUS` in the **Type** field, the following additional inputs are required.

Select from one of the following RADIUS protocols.

- PAP
- CHAP
- MSCHAP
- MSCHAPv2

Provide the following additional information for the RADIUS server.

Field	Description
RADIUS Server	The IP address of the remote RADIUS authentication server.
RADIUS Port	The port on which the RADIUS authentication server is listening. The default RADIUS port is 1812.
Shared Secret	The shared secret for accessing this RADIUS server. Use the  icon to view this secret.
Time Out	Timeout value for authentication. Once this time exceeds, the authentication fails.
Retries	The number of retries allowed when authentication fails for any reason.
User Prefix	The name of the windows domain for the server. This field 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 find out the correct option that works with your RADIUS deployment.
User Suffix	Enter the domain name for this server. This field is optional. You can leave this field blank or supply a valid suffix.
Use RADIUS for external group based authentication	Select this option to enable authentication of a user with a RADIUS server based on the group that the user account is a member of.

7. When you select Use RADIUS for external group based authentication control the following additional input is required.

Field	Description
Group attribute	Displays a list of attributes used to identify the group the user belongs to in the remote RADIUS server. When an attribute is selected, values are inserted into the Vendor Code , Attribute Code , and Group RegEx fields for AirDefense to use with group authentication.




Note

Do not change any values that are inserted in the **Vendor Code**, **Attribute Code**, and **Group RegEx** fields when you select any value the **Group Attribute** field.

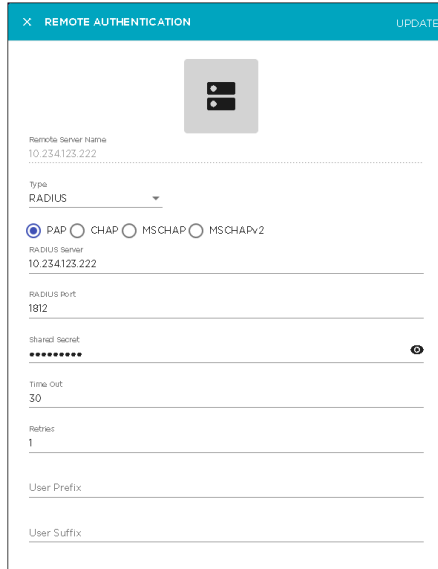
8. Select the **CREATE** button located to the top of this dialog to save the newly created remote profile.

At any point of time, if you wish to exit without creating the remote profile, select the small **X** button located to the top left of this dialog.

Edit Remote Profile

You can edit a remote profile's settings in the **User Management & Configuration** screen by selecting the  icon next to its entry in this list.

AirDefense uses the **Remote Authentication** screen to edit the remote profile details.




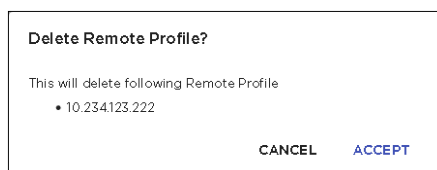
All details for this remote profile is pre-filled in the fields of this screen and can be modified. However, you cannot modify the **Remote Server Name** field for the selected remote profile.

1. Review the fields in this screen. Make the modifications as required.
For more information on the fields of this screen, see [Add Remote Profile](#) on page 355.
2. Select the **UPDATE** button to save the changes made to this remote profile's information.
Use the small **X** button located to the top left of the dialog to close it. AirDefense does not prompt you to save changes when exiting this dialog. If you have not saved your data, you will lose any unsaved changes when exiting this dialog.

Delete Remote Profile

Use the **User Management & Configuration** screen to delete any remote profile added to this AirDefense instance.

1. If not selected, select the **Remote Profile** icon from the toolbar.
2. From the list of remote profiles, select the profile that you want to delete. Then select the  icon located to the right of this profile's entry.
The **Delete Remote Profile** dialog displays.




3. Review the remote profile listed in this dialog.
4. Select the **ACCEPT** button to delete the selected profile.

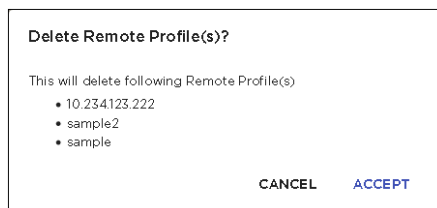
At anytime, select the **CANCEL** button to exit without deleting this remote profile.

The selected remote profile is deleted and removed from the list of valid profiles for this AirDefense instance.

5. The option control in the first column of each remote profile entry enables you to select multiple profiles simultaneously. To delete many profiles in the same action, select this option control for each of those profiles that you wish to delete.

The  icon located to the top right of this list enables. Select this icon to delete the selected remote profiles.

The **Delete Remote Profile(s)** dialog opens.



6. Review the remote profile listed in this dialog.
7. Select the **ACCEPT** button to delete the selected remote profiles.

At anytime, select the **CANCEL** button to exit without deleting these remote profiles.

The selected remote profiles are deleted and removed from the list of valid profiles for this AirDefense instance.

System Settings

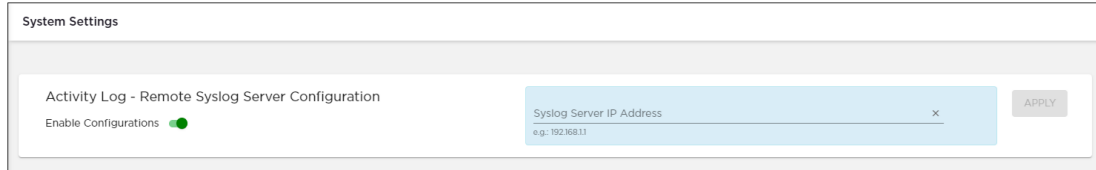
Use the **System Settings** screen to configure a remote System Log server to store the log of activities performed directly on your AirDefense instance. This log can then be used for various purposes like performing security audits, audits for fulfilling statutory requirements, and other similar audits of your AirDefense installation.

When enabled, any activity performed directly on the AirDefense system, using its web interface, is logged automatically and then sent to the remote system log server.

An activity is an action that is performed directly on the AirDefense physical device. Logins, logouts, configuration changes, user management actions, and reboots are some of the activities that are recorded and forwarded to the remote system log server.

System log settings are managed from the **System Settings** screen. This screen displays when you select **Settings > System Settings** menu path from the AirDefense user interface.

The following screen displays.



System Settings

Activity Log - Remote Syslog Server Configuration

Enable Configurations

Syslog Server IP Address

APPLY

If a remote system log server is already configured, this screen displays the IP address of the currently configured server.

Data Format

Activity data from AirDefense is sent in the standard *syslog* format. Your system log server should listen for data on the standard port number 514.



Note

We do not support system log servers listening on non-standard ports.

Severity Levels

All activity log entries for your AirDefense server are sent with the following levels:

Facility Code

1 - User

Severity Value

6 - Information

Add System Log Server IP Address

To add an external *system log* server to record activities performed directly on your AirDefense instance:

1. Select the **Enable Configurations** switch to enable it.

The IP address of the remote system log server can only be entered if the **Enable Configurations** switch is set to the *ON* position.

The **Syslog Server IP Address** field gets enabled. If a System Log server is already configured for receiving activity logs, then this field displays its IP address.

2. Provide the IP address of the remote *system log* server in the **Syslog Server IP Address** field.

The IP address is only verified for proper formatting. AirDefense does not verify that the IP address is of a valid system log server.

If already configured, you can also choose to provide the IP address of your current *system log* server in this field. This is the server where your Alarm logs are currently being sent.

**Note**

This field will not accept host names.

**Note**

You cannot enter multiple IP addresses in this field.

3. Select the **APPLY** button to save the information.

On successful registration, activity logs from your AirDefense system is sent to the remote *system log* server.



System Overview

- [AirDefense in Standalone Mode](#) on page 364
- [System Components](#) on page 364
- [System Requirements](#) on page 365
- [Version Compatibility for Upgrade](#) on page 366
- [Connecting to Hardware Appliance](#) on page 367
- [Configuring the Appliance](#) on page 368
- [System Configuration](#) on page 369
- [Selecting and Deploying APs and Sensors](#) on page 370
- [Connecting to the Network](#) on page 371
- [Assigning User Interfaces](#) on page 371
- [Basic Navigation](#) on page 373
- [Alarm Time Reporting](#) on page 375

Extreme AirDefense (AirDefense) 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. AirDefense 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.

AirDefense 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 Extreme AirDefense. The comprehensive configuration features give you full control over your network from a central location.

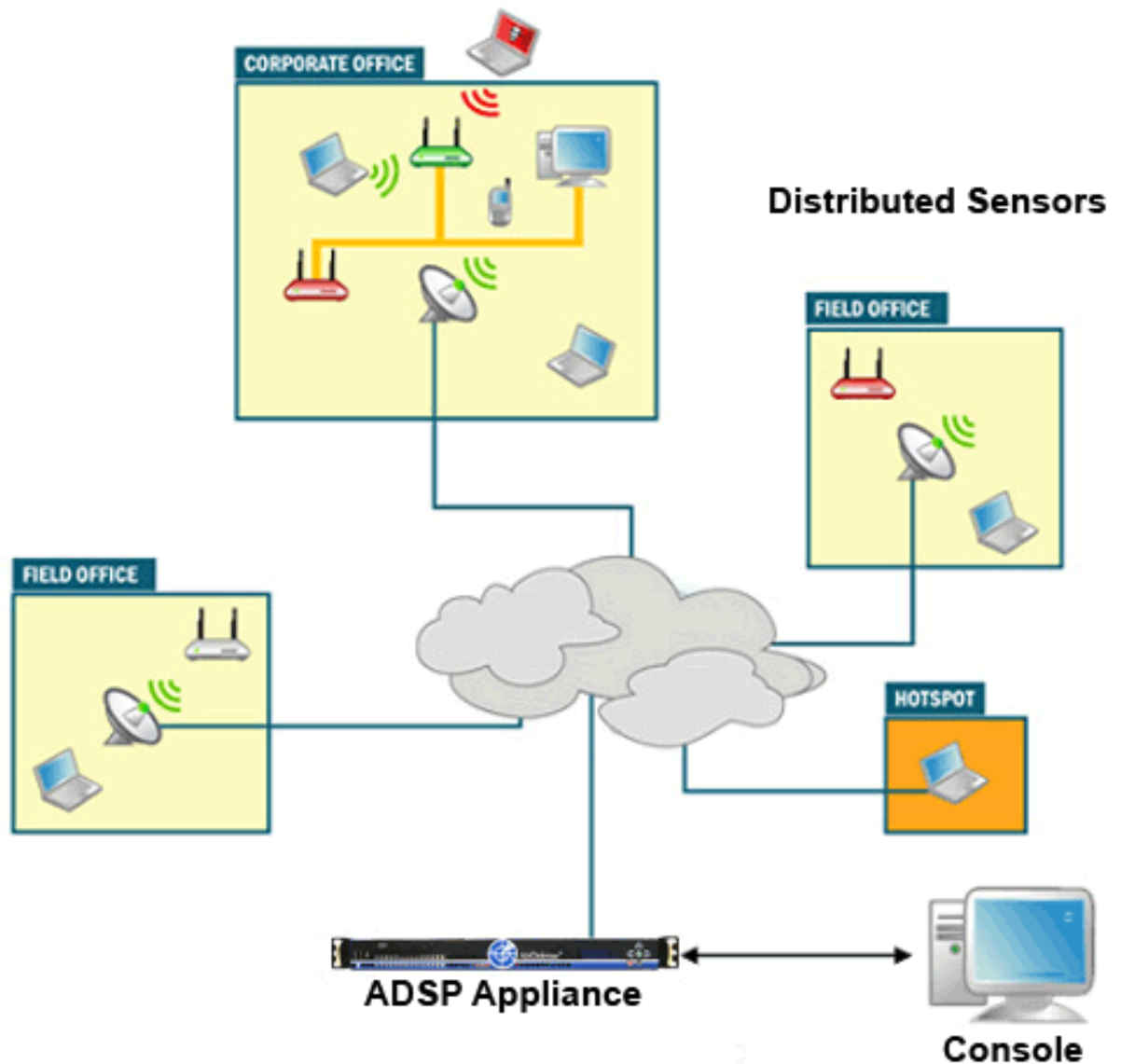
AirDefense in Standalone Mode

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

The AirDefense appliance provides a scalable, secure, and manageable solution for enterprises to deploy in a single office or corporate campus. As an appliance, AirDefense 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.

System Components

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



The AirDefense remote sensors collect frames being transmitted from any 802.11 devices and sends that data to a central AirDefense appliance for analysis and correlation.

System Requirements

The following are the different requirements for AirDefense:

- [Supported Hardware Appliances](#)
- [Supported Browsers](#)
- [Supported Operating Systems](#)

Supported Hardware Appliances

Model NX95x0

Supported Browsers

- Firefox 36 and higher
- Internet Explorer 11 and higher
- Google Chrome 40, 41 and 53.

Supported Operating Systems

The following operating systems can be used to install the AirDefense toolkit. The AirDefense toolkit is a set of utilities for managing an AirDefense instance.

- Windows 7
- Windows 10 Enterprise
- Linux
- Mac (Thin Client Applications only)

Version Compatibility for Upgrade

The following versions can be updated to the latest version of AirDefense.



Important

Upgrading from versions other than those listed in this section are not supported. If you have a version not listed in this section, and would like to upgrade to , you must have an AirDefense support contract. Please contact your Extreme Networks sales person if you currently do not have a support contract and would like to receive access to software updates for this product.

Version 9.5

Version 10.0 can be upgraded directly from version 9.5.0-11 only. Direct upgrade from any other version is not supported.



Note

For existing customers who would like to upgrade to 10.0, you must have an AirDefense support contract. Please contact your Extreme Networks 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

AirDefense is compatible with sensors operating on WiNG APs running WiNG-5 and WiNG-7. Individual AirDefense functionality will vary depending upon AP hardware model. Refer to AirDefense release notes for a detailed matrix indicating AP hardware and AirDefense feature support.

Extreme Wireless Version Compatibility

AirDefense is compatible with the following Extreme Wireless versions:

- Extreme Wireless 10.41.07 (dedicated sensor support for 39xx series APs only)
- Extreme Wireless 10.41.09

Extreme Cloud Appliance Compatibility

AirDefense is compatible with the following Extreme Cloud Appliance versions:

- Extreme Cloud Appliance 4.76.08

Connecting to Hardware Appliance

AirDefense Hardware Appliance is accessible through:

- By directly connecting a keyboard and mouse to the hardware appliance
- Using a laptop by connecting directly to the hardware appliance's LAN port
- Remote access through SSH

Connect a Laptop

You can physically connect a laptop to the AirDefense hardware appliance's Ethernet port to communicate through an IP address.

By default, a fresh installation of AirDefense does not have a default IP address. It has to be assigned by the AirDefense operator. Ensure that your laptop has an IP address in the same subnet as the AirDefense Appliance.

Connect a Monitor and Keyboard

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

Access Appliance Remotely

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



Note

You must have a client that supports SSH v 2 installed on the remote workstation used to connect to the AirDefense 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 AirDefense 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 AirDefense appliance after the initial installation.



Note

For details on installing the AirDefense appliance, see the Extreme AirDefense Appliance Installation Guide at the following URL:

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

Table 12: AirDefense Basic Commissioning

Planning and Assessment	Review your security policies, network infrastructure and WLAN sensor coverage requirements, and then establish your AirDefense policy configuration.
Analysis and Design	Develop a system implementation design tailored to your specific wireless security requirements.
Appliance Implementation	Configure the AirDefense 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)

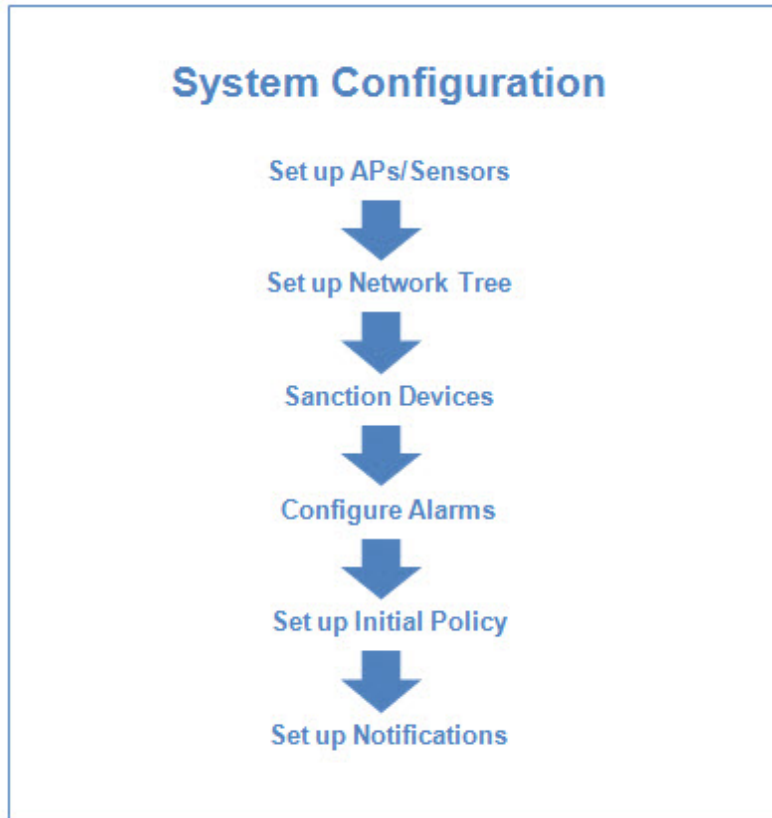
Module	Actions	Category
WIPS (Wireless Intrusion Prevention System) (Dedicated sensor WIPS, Radio-Share sensor WIPS)	<ul style="list-style-type: none"> • License and configure. License is per AP operating with a sensor. • Set up the automated configuration for policies and associated devices. • Configure optimal rogue detection and mitigation. • Define and tune threat monitoring policy. 	Security and Compliance
Wireless Vulnerability Assessment (Dedicated sensor only)	<ul style="list-style-type: none"> • License and configure. License is per AP operating with a sensor. 	Security and Compliance
Advanced Forensics (Dedicated sensor, Radio-Share sensor)	<ul style="list-style-type: none"> • License and configure. License is per AP operating with a sensor. 	Security and Compliance

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 by referencing the feature support matrix in the AirDefense release notes.

System Configuration

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



Selecting and Deploying APs and Sensors

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

- 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

Refer to the Extreme AirDefense Release Notes for the full list of AP models, management platforms, and minimum supported firmware.

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 simultaneously act as a sensor, providing multi-band sensing. OCS essentially allows the AP to tune its radio to a different channel for a finite amount of time for threat scanning.

Example:

An AP that provides 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 of communication with associated clients. 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 transmissions of other APs and to monitor any off-channel RF transmissions.

**Note**

When utilizing OCS, the APs/sensors take more time to detect threats than when utilizing a dedicated sensor. The amount of time required to detect threats depend on several factors, such as, data load, timing, and the channel where the threat is active. OCS is a part of Part-time WIPS and requires that license for this feature.

Setting Up APs and Sensors

In order to implement WLAN monitoring, APs must be properly selected to operate as sensors in order to ensure full coverage of the desired RF airspace. The AirDefense Sensors passively observe all wireless LAN traffic within 40,000 to 60,000 square feet of typical office space. These 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.

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](https://)) 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](https://)).
- Console-to-Server: you must use encrypted (port 8543) communication.

Assigning User Interfaces

User interfaces allow system users to access certain AirDefense 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
AirDefense Command Line Interface	AirDefense admin (utilities)	Manage Dbase Software Config	Command Line User
AirDefense Graphical User Interface (GUI)	Extreme AirDefense	Dashboard Network Alarms Configuration Rogue Performance Compliance Forensic Intrusion Device Management Report Builder Reports Troubleshooting Downloads	User
AirDefense New User Experience (GUI)	Extreme AirDefense	Dashboard Network Alarms	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 AirDefense is **admin/admin123**.

User Accounts

AirDefense has one default `Admin User` account. Admin Users may create other users with role-based permissions that control which functionality each user can access. The Admin User creates individual accounts and assigns these 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 AirDefense server and sensor administration, including creation of other admin users.
- Guest—Gives users read permission to Alarm Management, Reporting, and Analysis Tools. 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.

Use the Admin User account to bypass templates and to customize the user accounts to fit your unique needs.

System Access Limitations

Your particular AirDefense 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.

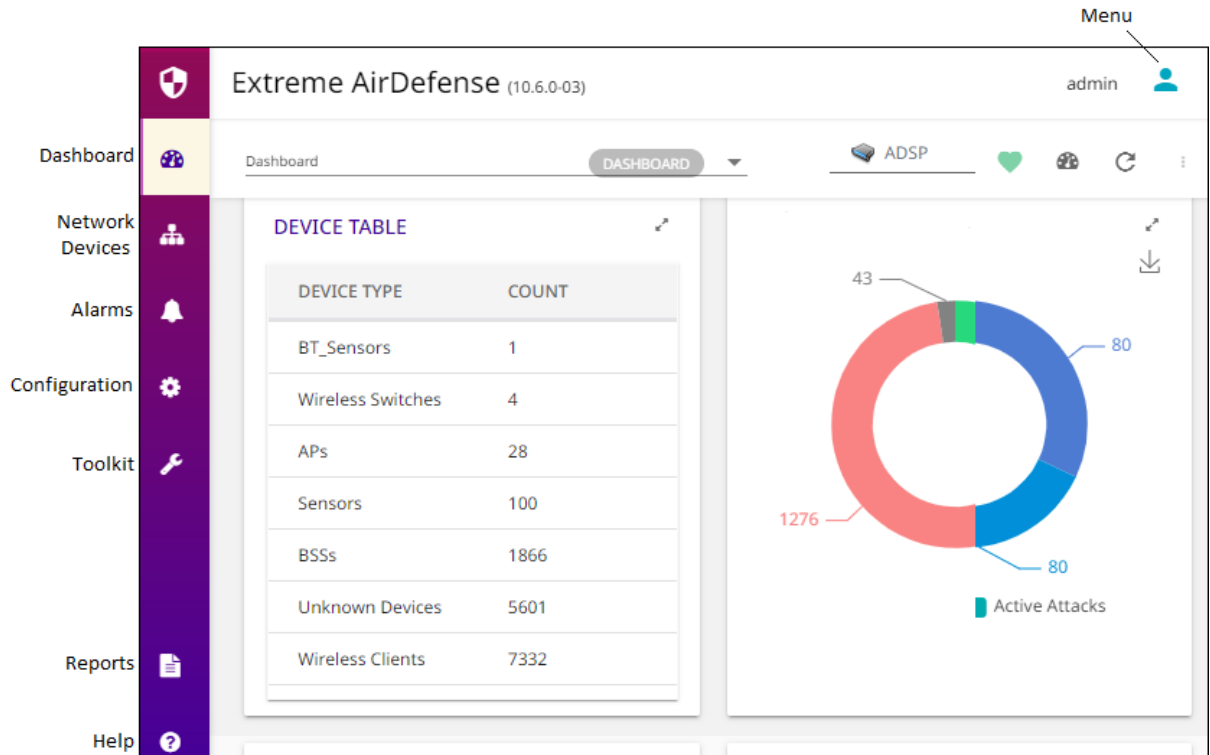
Example:

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



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

Tree Structure

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

Device Search

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

Filters

Filtering options make it easy to focus on the devices and alarms that are important to you. You can use filters to narrow down what you see. For example, you can use the filter to view only devices that are displaying rogue activity.

Dashboard Drill Down

The dashboard lets you quickly assess your overall security and performance status.

Alarm Time Reporting

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

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

However, when reporting the alarm to the GUI, AirDefense 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.



Extreme AirDefense on Virtual Platform

[Prerequisites](#) on page 376

[Installing Extreme AirDefense 10.0 on VMware](#) on page 377

[Install Extreme AirDefense on Xen Hypervisor](#) on page 386

Extreme AirDefense (AirDefense) 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 AirDefense has the host hardware's processor, memory and resources.

The following sections provide step-by-step instructions on how to install Extreme AirDefense (AirDefense) on a virtual platform.

Prerequisites

AirDefense can be installed on an appliance or as a Virtual Machine.

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

- VMware® vSphere 5.5, 6.0, 6.5 (ESXi)
- Xen Hypervisor 4.1.2 and higher

Required Files

The following files are required for installation:

To Install On VMware

To install AirDefense using VMware/ESXi, refer to this [Extreme article](#).

To Install On Xen Hypervisor

To install AirDefense as a VM on Xen Hypervisor, download the files `AD-VM-adsp-9-2-0-09-dvd.gz` and `AD-VM-adsp-9-2-0-09-dvd.xm`.



Note

Xen Cloud Platform (XCP) is no longer supported.

You can download the latest version from the [Extreme Portal](#).

Required License

No license is required to install AirDefense on the Virtual Machine of your choice. However, you will require an AirDefense Platform license in order to use AirDefense on the 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	Physical CPU cores - 2 hyper-threads per core (vCPUs)*	Memory for ADSP VM	Hard Disk for ADSP VM	Scanning Sensors	RadioShare non scanning	Active WLAN Devices	Total WLAN Devices
Large**	12 (24 vCPUs)	36GB	1TB	2500	3000	250,000	1,000,000
Mid**	8 (16 vCPUs)	25GB	500GB	1000	1500	100,000	400,000
Small	4 (8 vCPUs)	8GB	250GB	500	750	40,000	160,000
Micro	2 (4 vCPUs)	4GB	250GB	100	100	10,000	40,000

* The number of vCPUs will be twice the number of physical cores since there are 2 hyper-threads per core.

** With multi-core operation mode enabled in software.

Device age-out is assumed to be 1 hour for the above table.



Note

In a multi-VM environment, over-allocation of CPUs to other VMs could potentially impact performance of the AirDefense VM.



Note

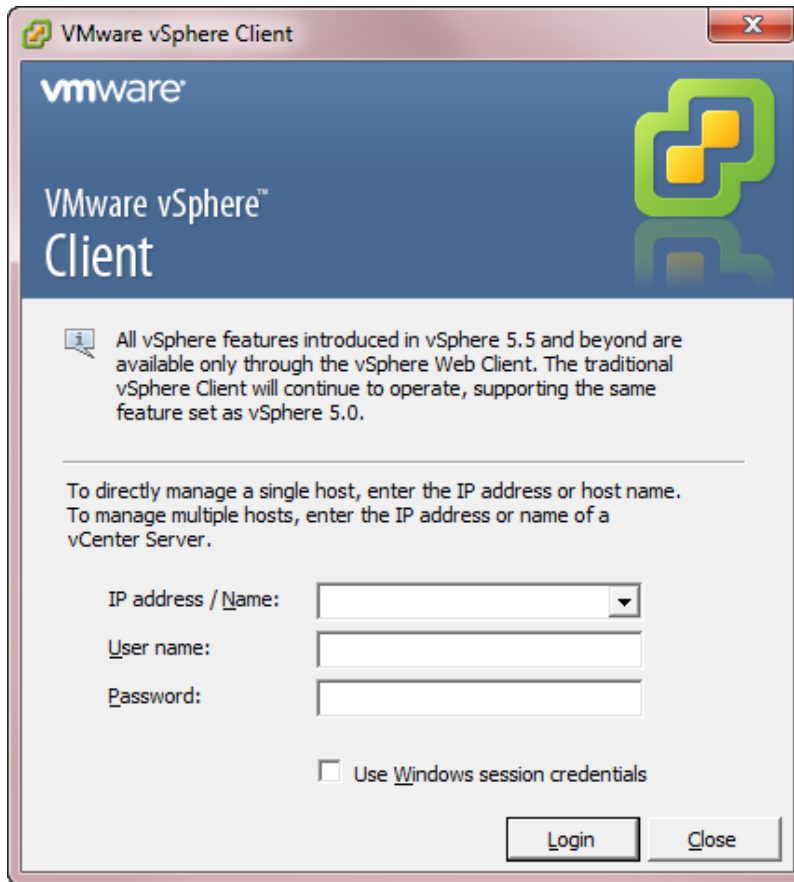
Higher sensor count will cause forensic analysis to take longer to run.

Installing Extreme AirDefense 10.0 on VMware

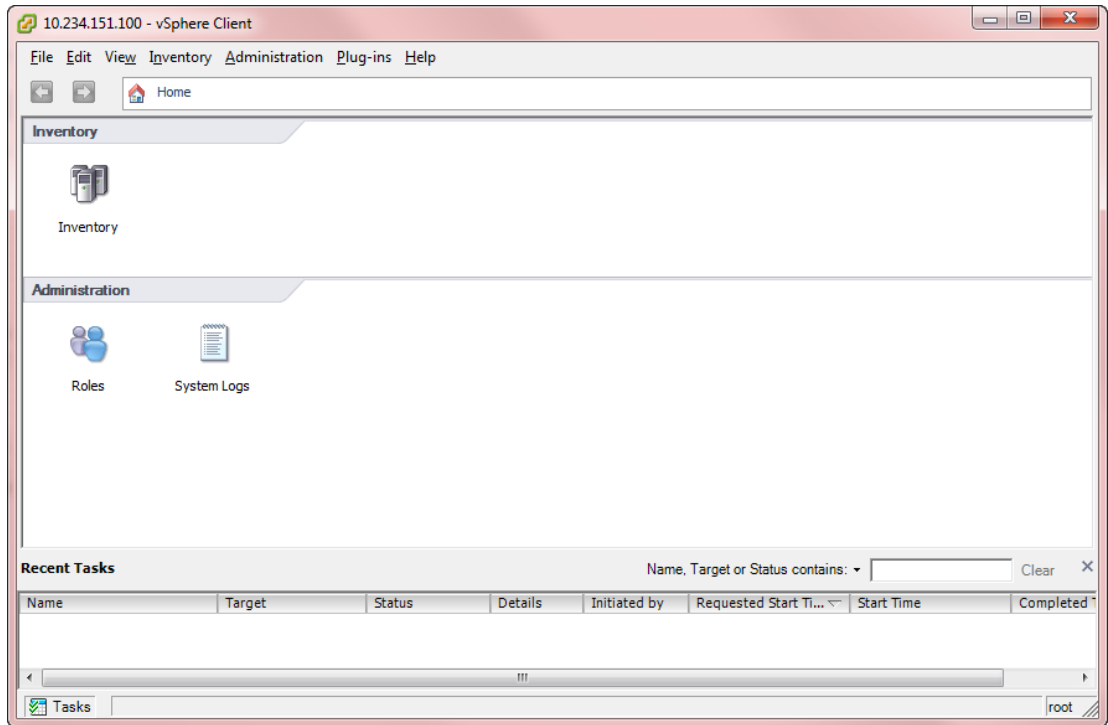
Follow these steps to install AirDefense on VMware:

1. Install VMware ESXi according to the instructions located at <https://docs.vmware.com/en/VMware-vSphere/5.5/com.vmware.vsphere.install.doc/GUID-7C9A1E23-7FCD-4295-9CB1-C932F2423C63.html>
2. Install the vSphere Client to install and manage the AirDefense VM running on a VMware ESXi host. Follow the vSphere Client instructions. For vSphere documentation, see <https://docs.vmware.com/en/VMware-vSphere/index.html>.

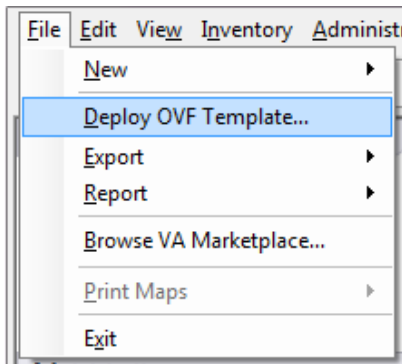
3. Once VMware is installed, double-click the **VMware vSphere Client** icon on your desktop to access the VMware vSphere server.



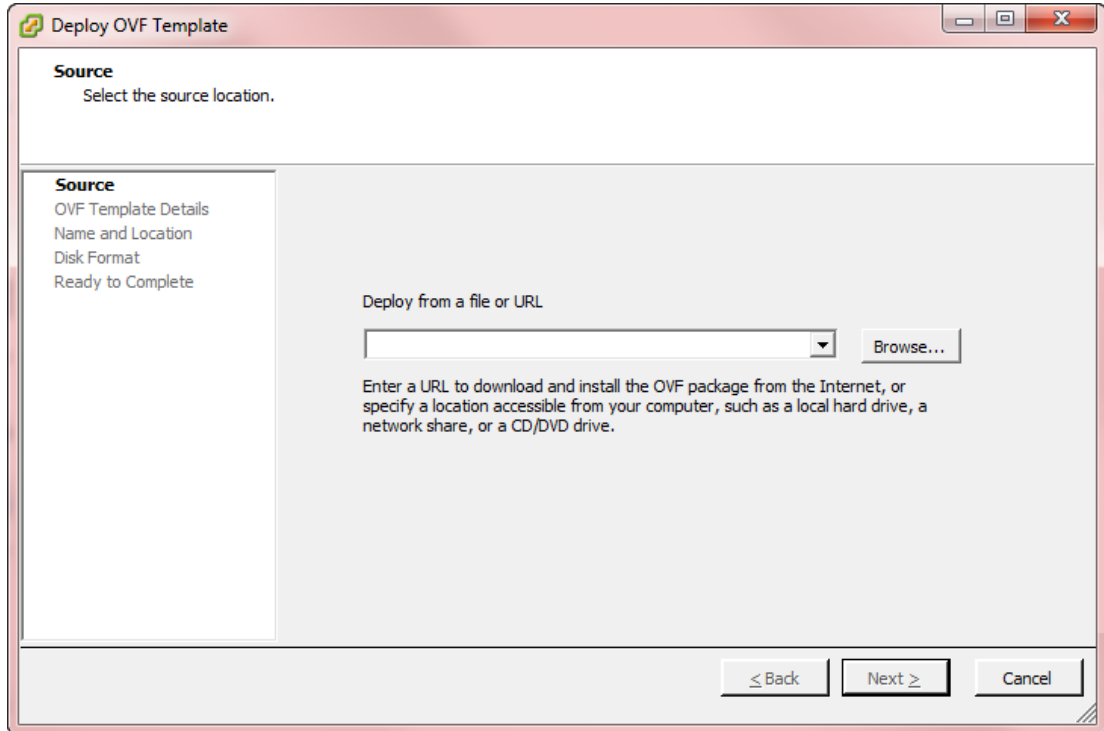
4. Enter the IP address of your server, your user name and password; then, click **Login**.



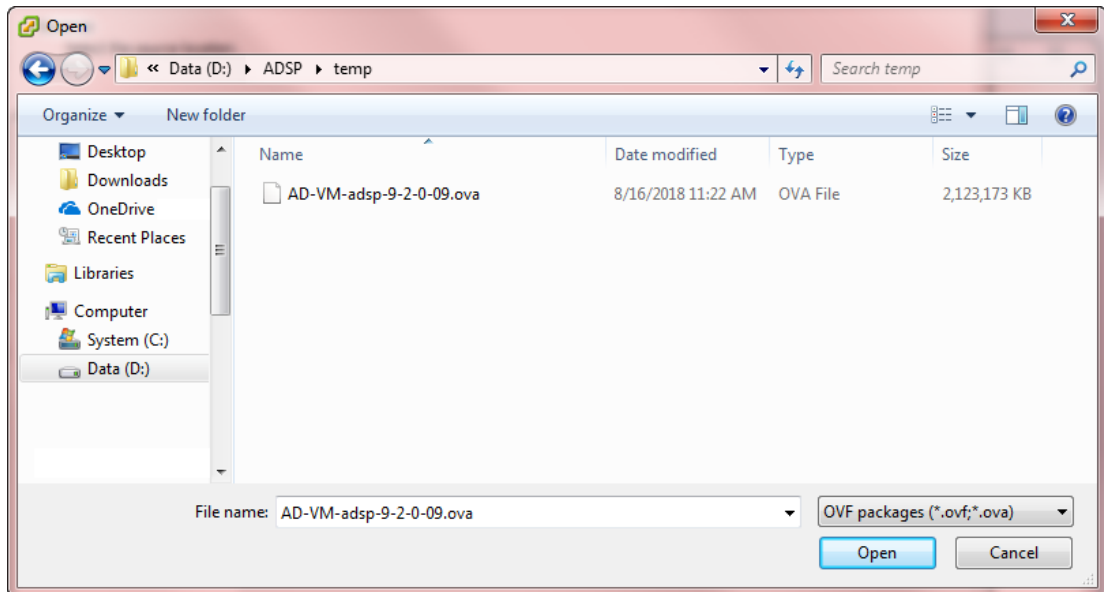
5. Select **File > Deploy OVF Template**.



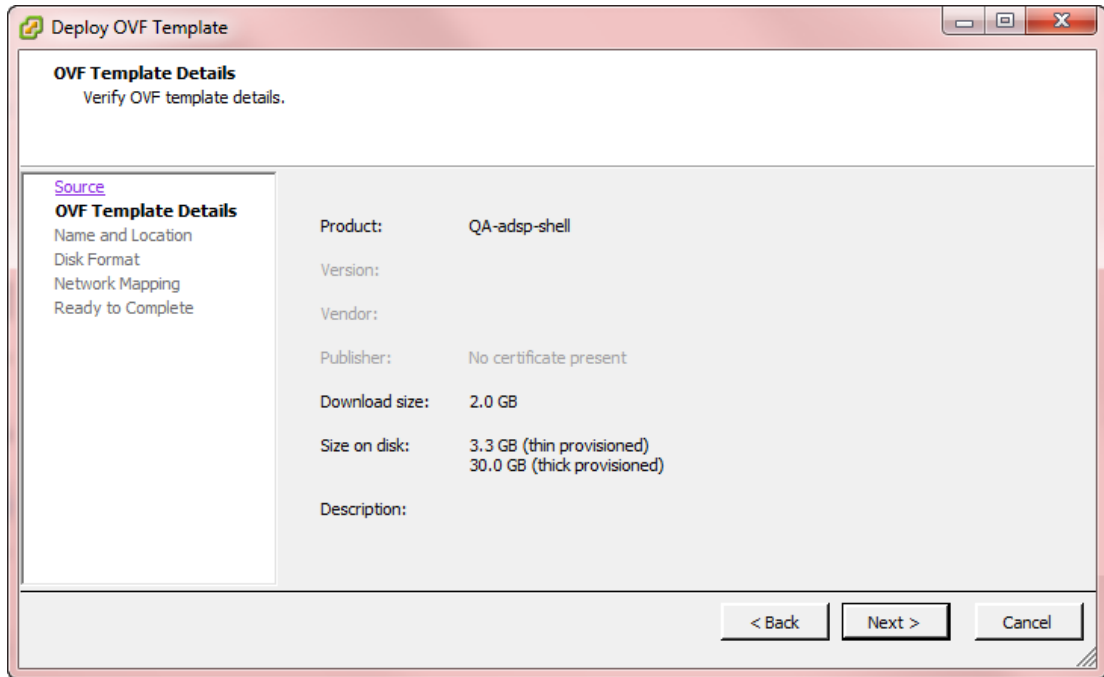
The **Deploy OVF Template** window is displayed.



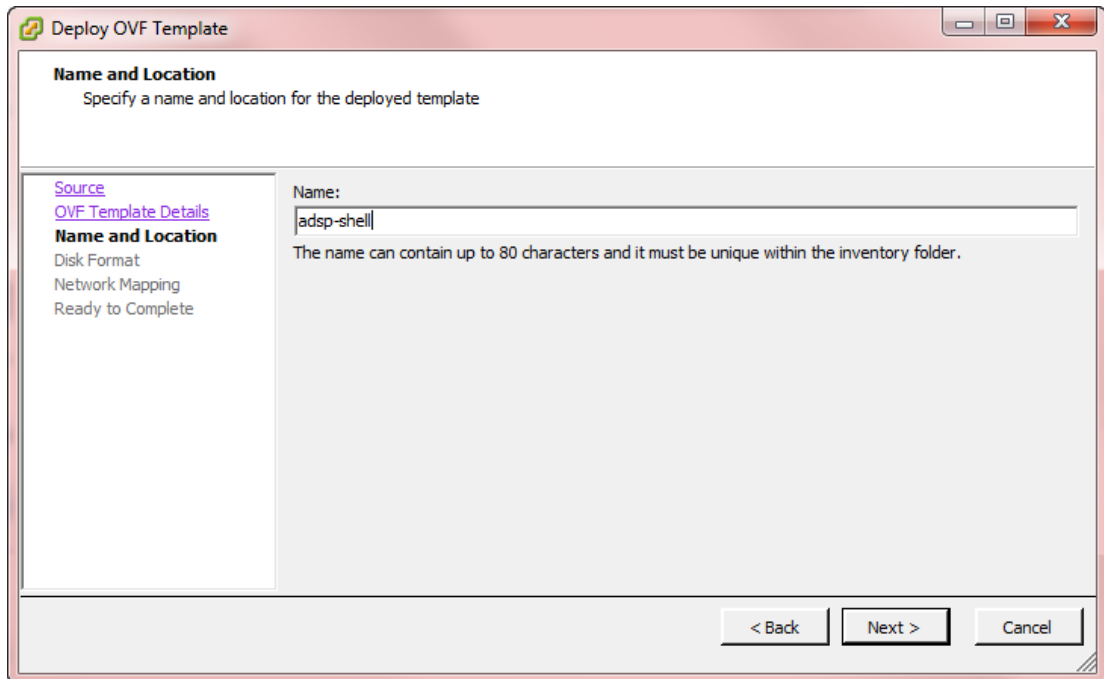
6. Click **Browse** and select the VMware image for the latest version of AirDefense. In the following example, you would select the `AD-VM-adsp-9-2-0-09.ova` file from your local PC.



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



- Verify the OVF template details and then click **Next**. The **Name and Location** screen displays.



- Enter a name (for example, adsp-shell) and then click **Next**.
- When multiple installation destinations are available, you must select a destination for storage of the VM files and then click **Next**.

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

The screenshot shows the 'Deploy OVF Template' wizard at the 'Disk Format' step. The window title is 'Deploy OVF Template'. The main heading is 'Disk Format' with the sub-heading 'In which format do you want to store the virtual disks?'. On the left, there is a navigation pane with links for 'Source', 'OVF Template Details', 'Name and Location', 'Disk Format' (which is selected), 'Network Mapping', and 'Ready to Complete'. The main area contains the following fields and options:

- Datastore:** A text box containing 'datastore1'.
- Available space (GB):** A text box containing '428.4'.
- Provisioning Options:** Three radio buttons:
 - Thick Provision Lazy Zeroed
 - Thick Provision Eager Zeroed
 - Thin Provision

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

12. Map the networks used in this OVF template to the networks available in your inventory. Use the drop-down list under the **DestinationNetworks** column to select the correct network.

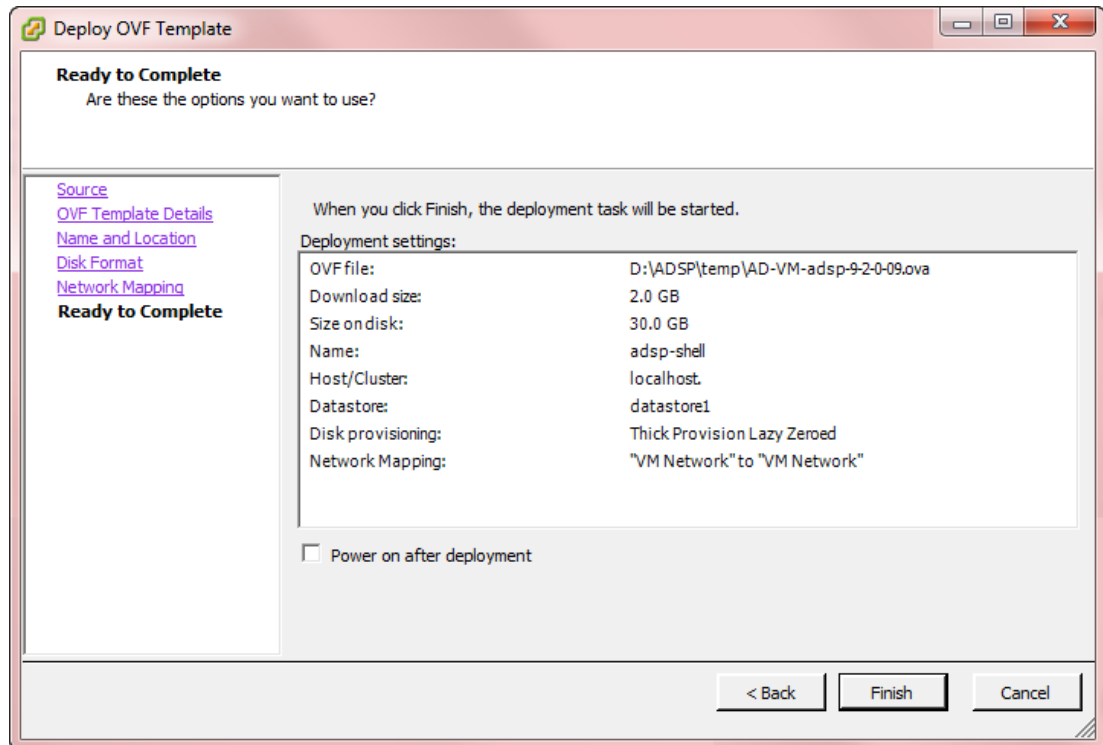
The screenshot shows the 'Deploy OVF Template' wizard at the 'Network Mapping' step. The window title is 'Deploy OVF Template'. The main heading is 'Network Mapping' with the sub-heading 'What networks should the deployed template use?'. On the left, there is a navigation pane with links for 'Source', 'OVF Template Details', 'Name and Location', 'Disk Format', 'Network Mapping' (which is selected), and 'Ready to Complete'. The main area contains the following elements:

- Instruction:** 'Map the networks used in this OVF template to networks in your inventory'.
- Table:** A table with two columns: 'Source Networks' and 'DestinationNetworks'.

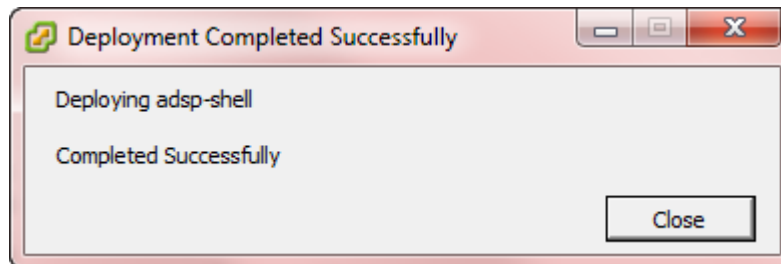
Source Networks	DestinationNetworks
VM Network	VM Network

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

13. Verify the information. **Power on after deployment** should not be enabled by default. If enabled, select the control to disable this option. Click **Finish** to deploy.



14. 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 AirDefense image being deployed.



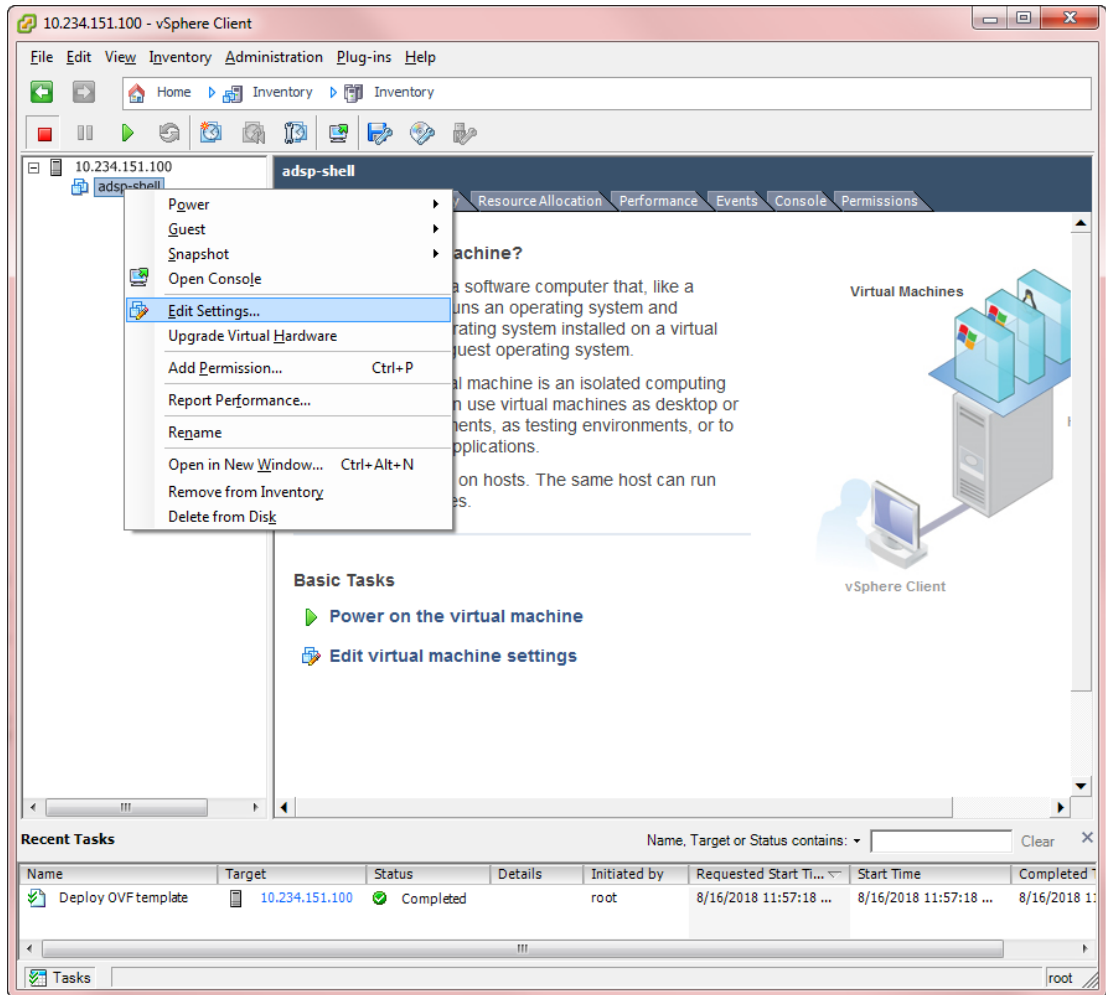
15. Click **Close**.



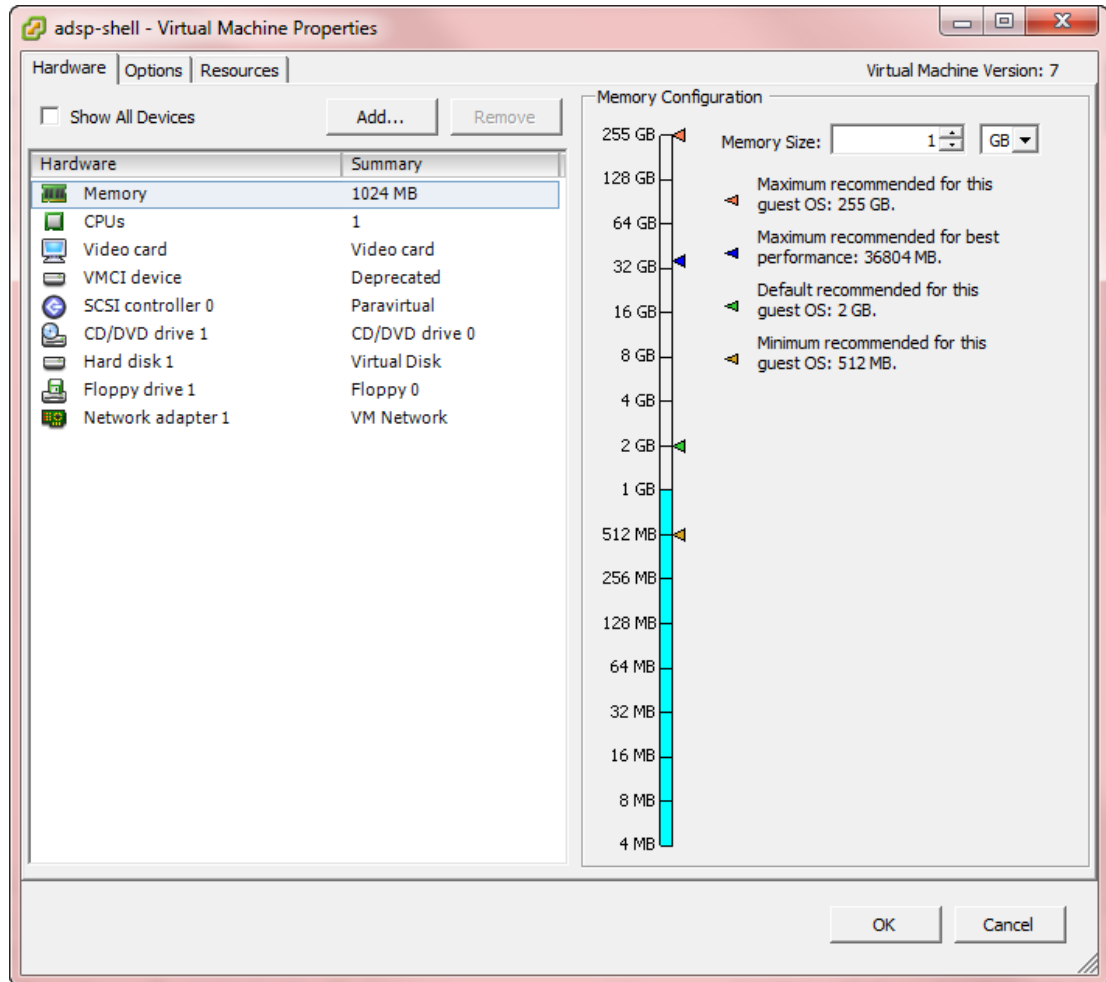
Note

If you receive a deployment error, download the `zlib1.dll` file from the Extreme Networks Support Center at [and](#) copy the file to your local hard drive.

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



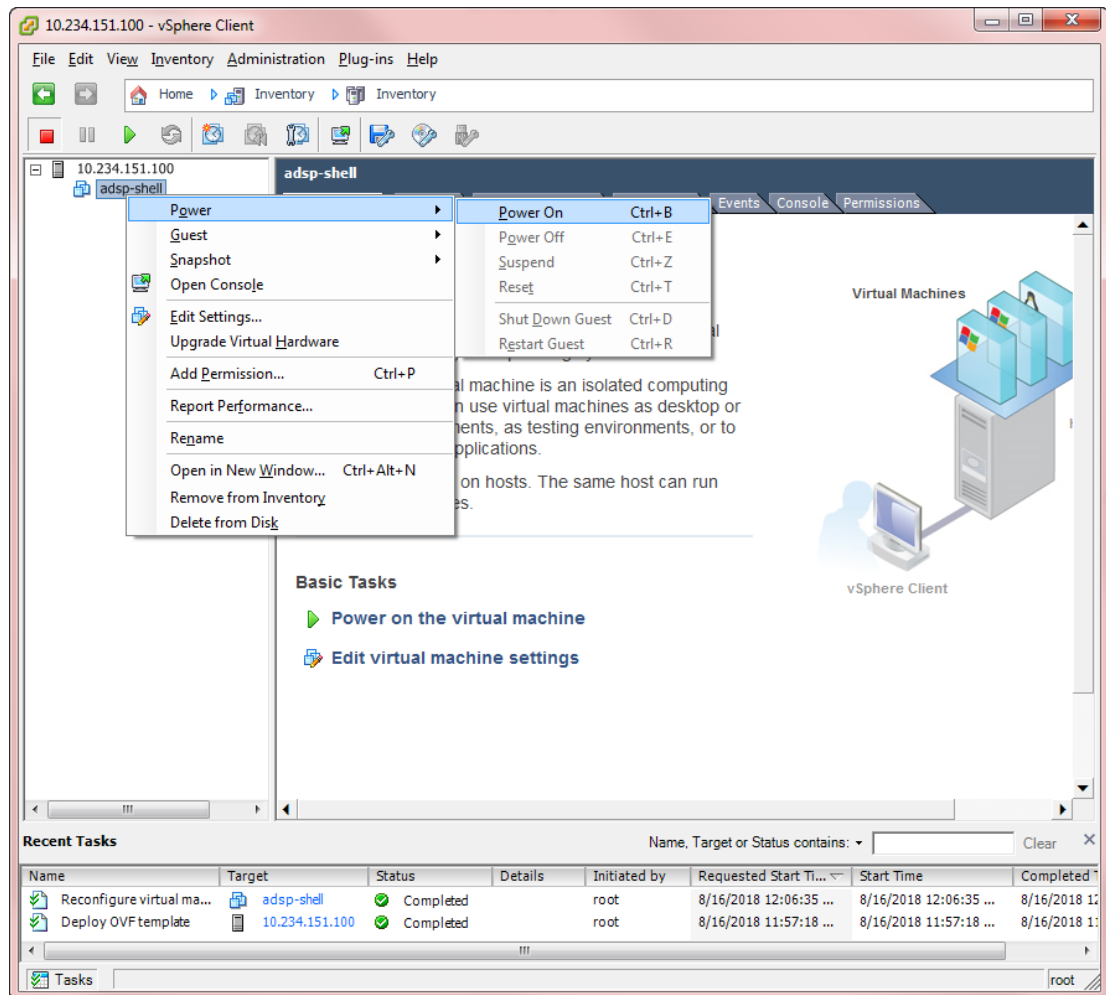
The following window is displayed.



17. Set Memory, CPUs and hard disk size as specified in [Required System Configuration](#) on page 377 section and also based on the network devices and clients to be supported by AirDefense.

18. Click **OK**.

19. Right-click on the AirDefense VM and then select **Power > Power On**.



20. Double-click the VM, then select the **Console** tab, and wait for login prompt. While waiting, AirDefense VM configures automatically.
21. When login prompt displays, log into AirDefense and configure just like you would any AirDefense appliance.



Note

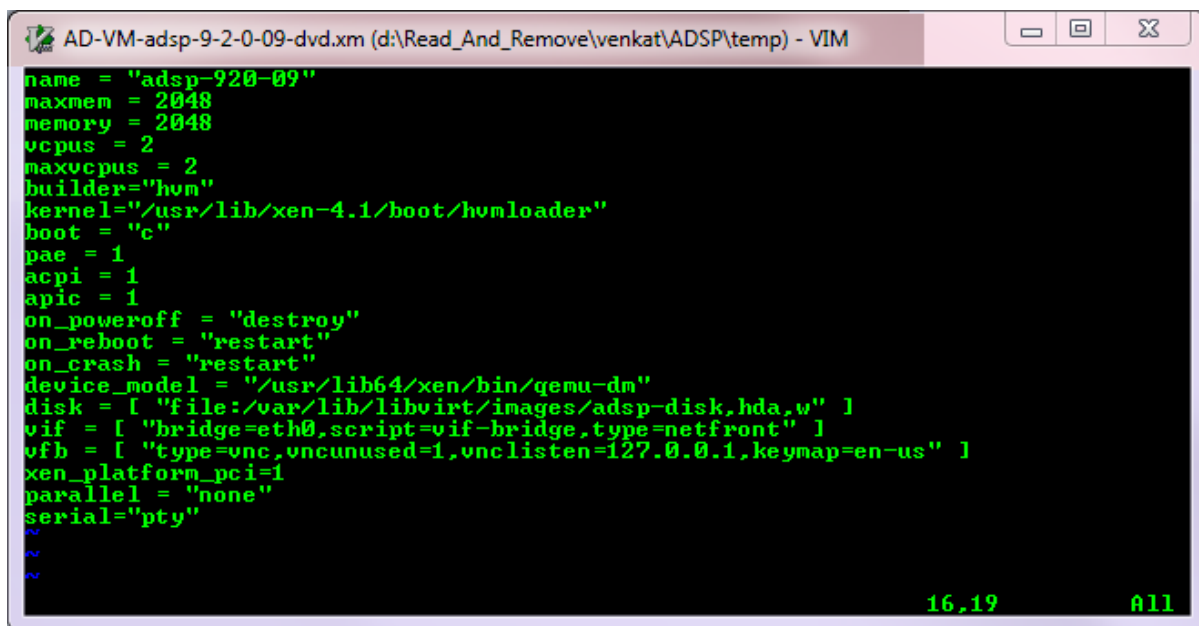
If you lose control of the cursor while using the VM, press **Ctrl+Alt** key combination to regain control.

Install Extreme AirDefense on Xen Hypervisor

Follow these steps to install AirDefense on the Xen Hypervisor:

1. Install Xen Hypervisor 4.x. Follow the Xen instructions located at https://wiki.xen.org/wiki/Main_Page
2. SCP the disk image (AD-VM-adsp-9-2-0-09-dvd.gz) and the configuration file (AD-VM-adsp-9-2-0-09-dvd.xm) to a location on your Xen server. Let us assume that the location is: /var/lib/libvirt/images.

3. Unzip the disk image using the following command: `gunzip AD-VM-adsp-9-2-0-09-dvd.gz`.
4. Go to `/var/lib/libvirt/images` and edit the configuration file: `vi AD-VM-adsp-9-2-0-09-dvd.xml`.



```
AD-VM-adsp-9-2-0-09-dvd.xml (d:\Read_And_Remove\venkat\ADSP\temp) - VIM
name = "adsp-920-09"
maxmem = 2048
memory = 2048
vcpus = 2
maxvcpus = 2
builder="hvm"
kernel="/usr/lib/xen-4.1/boot/hvmloader"
boot = "c"
pae = 1
acpi = 1
apic = 1
on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"
device_model = "/usr/lib64/xen/bin/qemu-dm"
disk = [ "file:/var/lib/libvirt/images/adsp-disk,hda,w" ]
vif = [ "bridge=eth0,script=vif-bridge,type=netfront" ]
vfb = [ "type=vnc,vncunused=1,vnclisten=127.0.0.1,keymap=en-us" ]
xen_platform_pci=1
parallel = "none"
serial="pty"
16,19 All
```

Figure 121: Edit the Configuration File

5. Change the line beginning with `disk` to point to your the location of your AirDefense image: `disk = [file:/var/lib/libvirt/images/adsp-disk,hda,w]`
6. Change the values for `name`, `maxmem`, `memory`, and `maxvcpus` to match your criteria. Refer to [Required System Configuration](#) on page 377 for the recommended resource configuration for AirDefense.
7. Increase the disk size of your AirDefense installation using the following command:


```
# fallocate -l <new size in bytes> /var/lib/libvirt/images/adsp-disk
```

By default, the size of the AirDefense image is set as the size your AirDefense VM disk. It is recommended that you increase the disk size to match the system requirements as specified in [Required System Configuration](#).

8. Create an AirDefense VM from the new configuration file: `xm new AD-VM-adsp-9-0-2-09-dvd.xml`
9. Start the AirDefense VM: `xm start adsp-920-09`



Note

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


10. The AirDefense Console can be started with the following command: `xm console <ADSP VM name>`
11. Log in to Virtual AirDefense and configure it as you would any AirDefense appliance.



Legacy Content

- [Menu](#) on page 388
- [AirDefense Dashboard](#) on page 434
- [Network Tab](#) on page 442
- [Alarms](#) on page 480
- [Configuration Tab](#) on page 495
- [Security](#) on page 801
- [ADSPAdmin](#) on page 814
- [Troubleshooting](#) on page 823
- [AirDefense Icons](#) on page 829

The menus in this section can be accessed from the legacy interface. To launch the legacy interface:

1. From within the new user interface, select the  icon in the top right corner of the Dashboard.
2. From the list of options, select **Legacy UI**.



Note

The legacy interface requires Flash support, which can be obtained by downloading WINGMAN from the support site under Wireless.

Menu

The Menu gives you access to AirDefense features.



Features such as **Add Devices** and **Import/Discover Devices** are features that are an integral part of AirDefense. **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 AirDefense Toolkit on your local workstation. (If you have no need to run the applets, there is no need to install these AirDefense Toolkit.)

Installing the Toolkit

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



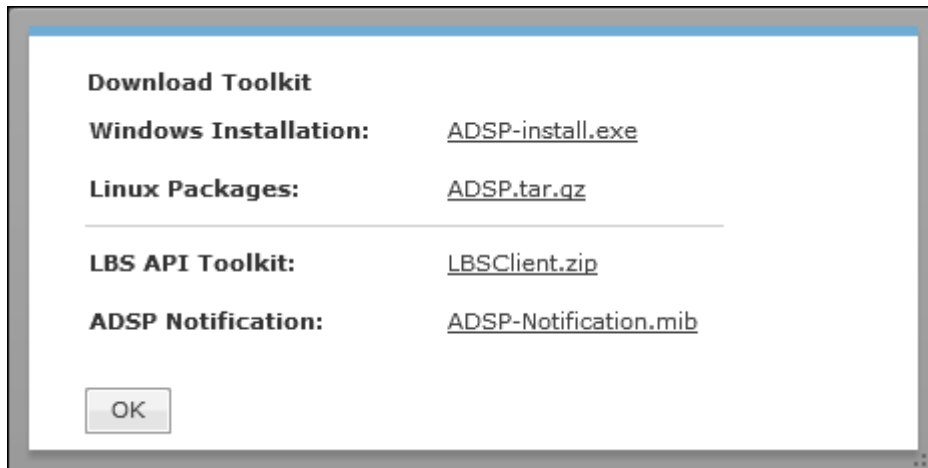
Note

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

To install the AirDefense 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

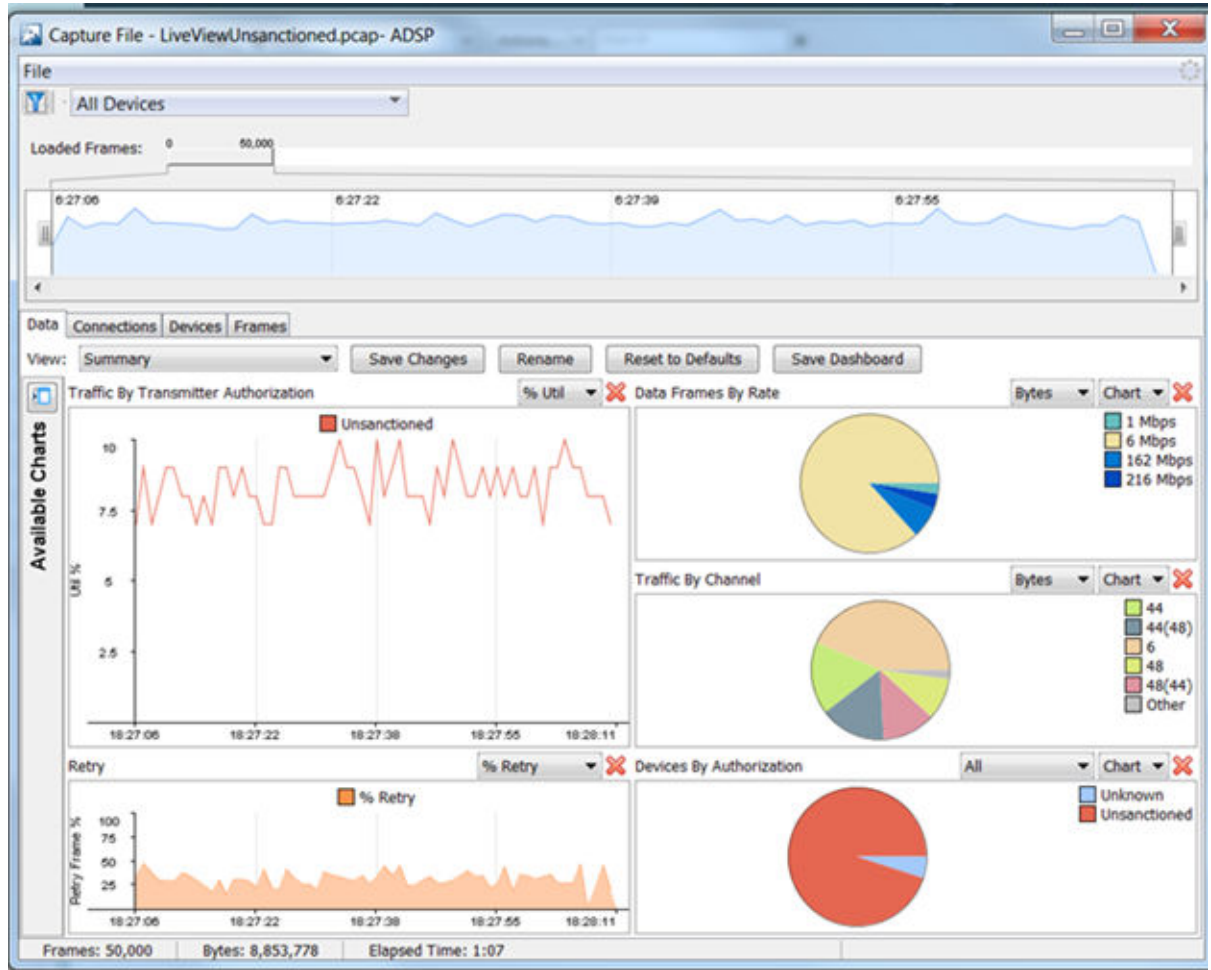
Click **Open** to access a saved Frame Capture or Spectrum Analysis file.

- [Frame Capture Analysis](#) on page 390
- [Spectrum Analysis](#) on page 391

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 then 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** pop-up 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 AirDefense, 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

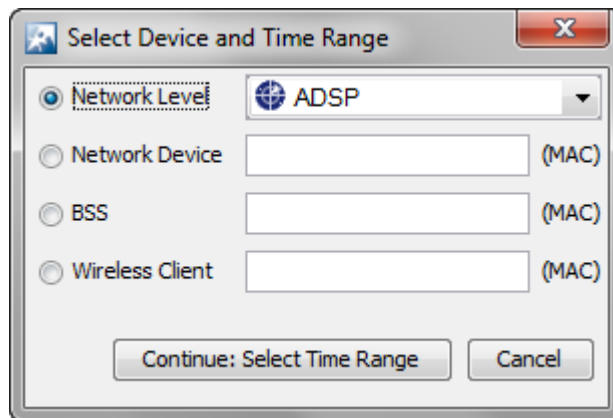
Forensic Analysis data is accessed in two ways:

- Using the menu
- Using left click the drop-down menu  next to a device within the AirDefense user interface and then selecting **Forensic Analysis**.

Method 1

To access forensic data for a device:

1. Select **Menu > Forensic Analysis**

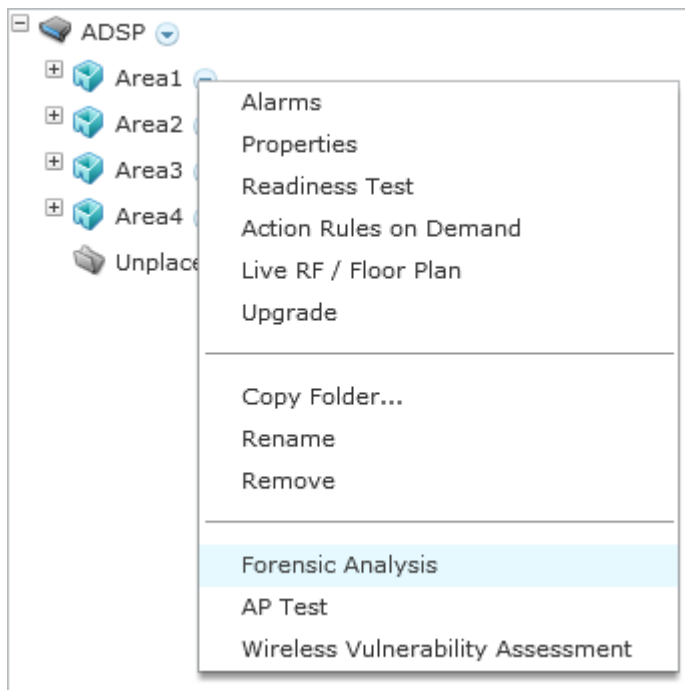


2. Enter the MAC address of the device in the appropriate field.

Method 2

Use the context sensitive menu for the device to view Forensic Analysis:

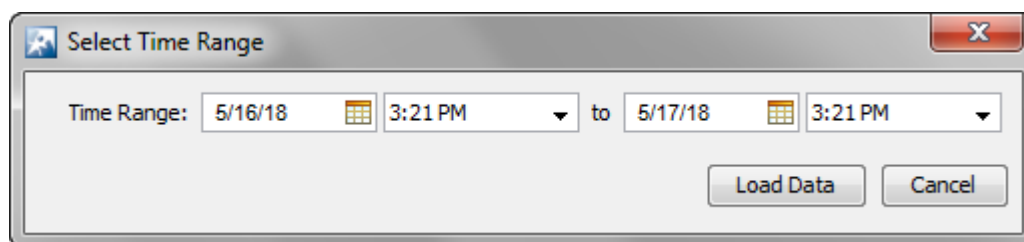
1. Left-click the drop-down menu button  of a device anywhere within AirDefense.



2. 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](#) on page 395.

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.

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 Extreme AirDefense.

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 13: 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.



Note

BSSs, Wireless Clients, APs, or switches are not 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.

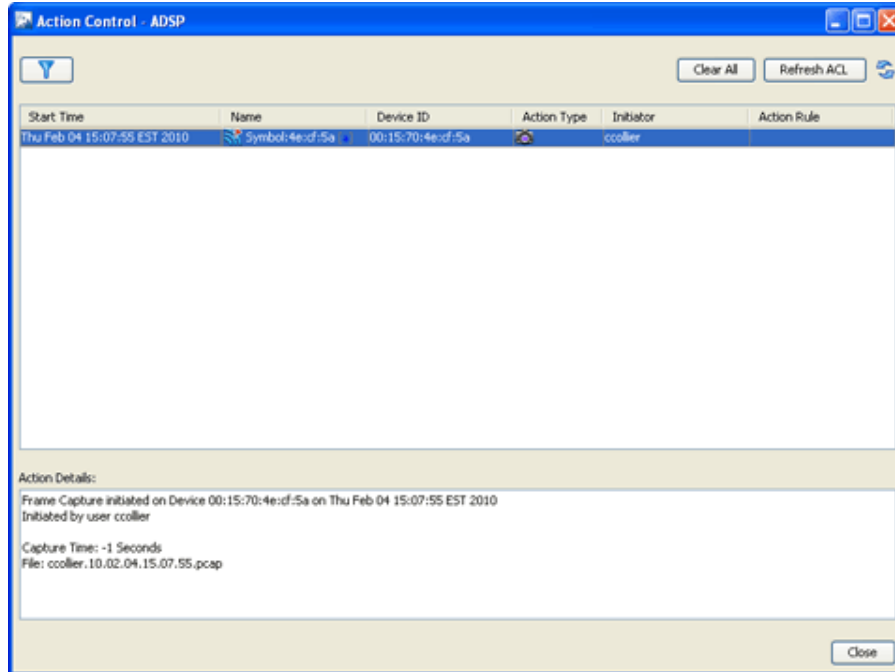
Device Based Forensic Analysis provides AirDefense administrators with the same forensic data that Basic Forensic Analysis, but also includes the extra features. The Basic Forensic Analysis tabs are included plus an extra **Location Analysis** tab for BSSs and Wireless Clients is added.

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

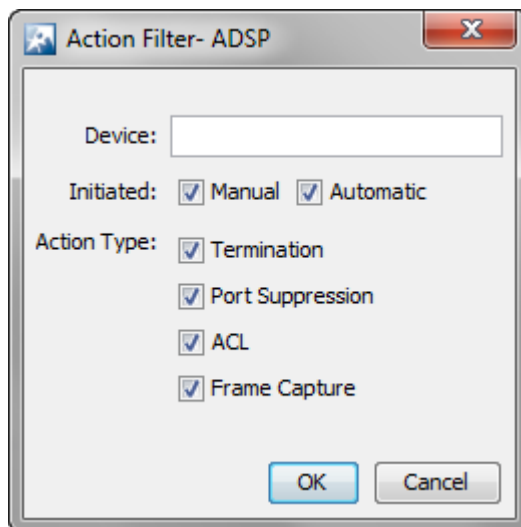
Action Control displays a table listing specific actions that are occurring to devices seen on your WLAN. The type of actions displayed are:

- Air Termination
- Port Suppression
- ACL
- Frame Capture



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

Use the  button to launch a window that enables you to filter to the actions of interest on a specific device.



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

AirDefense provides dual approaches to reporting. You can access a web reporting interface and populate report templates with data or you can 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 AirDefense or designing them from scratch. Reports you create with the report builder become available as templates in the Web Reporting interface. For more information on the Report Builder interface, see [Report Builder](#) on page 399.

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, saved as a published report or have scheduled to run periodically. 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 check-box and clicking **Delete**.
 - Share a published report by checking its check-box and clicking **Share**.
 - Make a published report private by checking its check-box 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 check-box 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

The Report Builder application allows advanced users to create completely original reports from blank templates. Alternatively, you can choose a report template you like and edit it to meet your requirements. 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 interface lets you create reports using any data point the appliance collects. The graphic below shows an example tree in the Report Builder application and some elements from the resultant report, along with tips on how to add different types of components.

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

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

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

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

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

System Name: maha-wds-mgr-013
Scope: system
Generated: 2010-02-02 14:01:33
Version: 8.0.0-24
Time Zone: EST - Eastern Standard Time

Performance Summary

Performance Alarms By Sub-Category

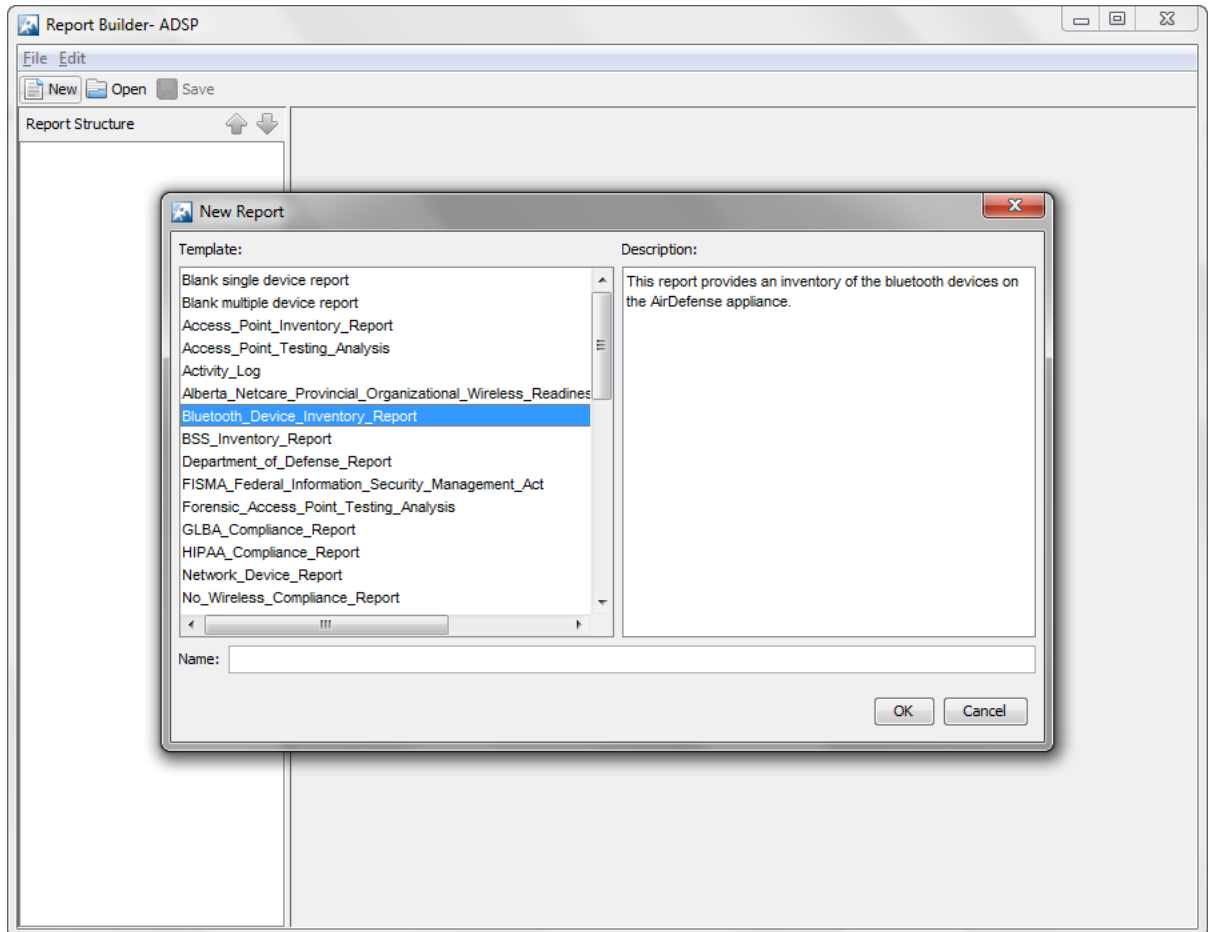
Sub-Category	Count
Operational Alarms	1
Performance Alarms	1

Alarm Details

Alarm Name	Severity	Category	Count
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1
Auth-Auth-Auth-Auth	Warning	Auth-Auth-Auth-Auth	1

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 creating a report. To change then number of devices on your report, you must create a new report.

3. In the **Name** field, type the name you want to use for this report.



Note

Report 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 enhancing it:



Note

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

- To 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.
- To 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.
- To 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.
- To add data fields, tables, charts, and floor plans - 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.



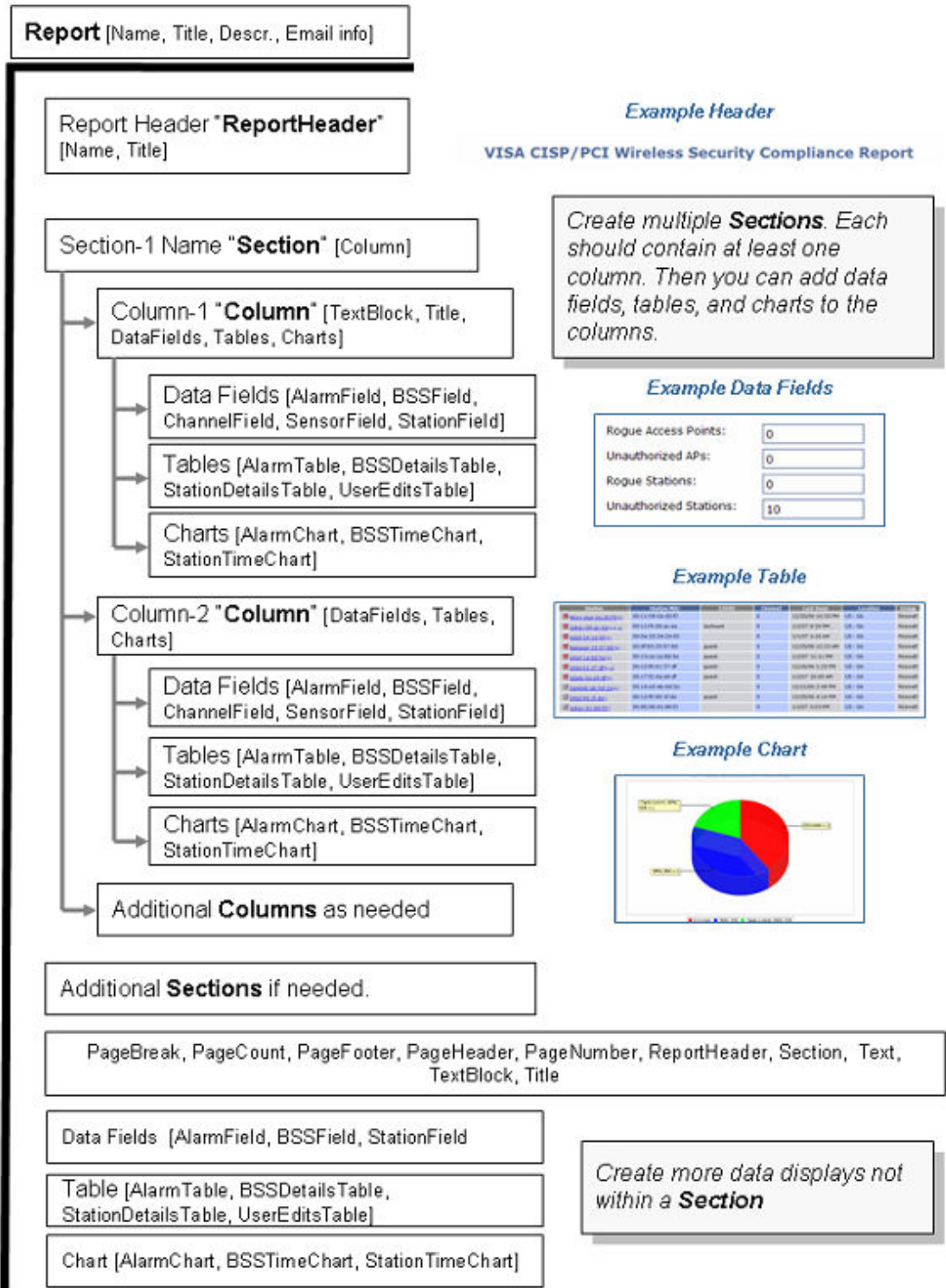
Note

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.

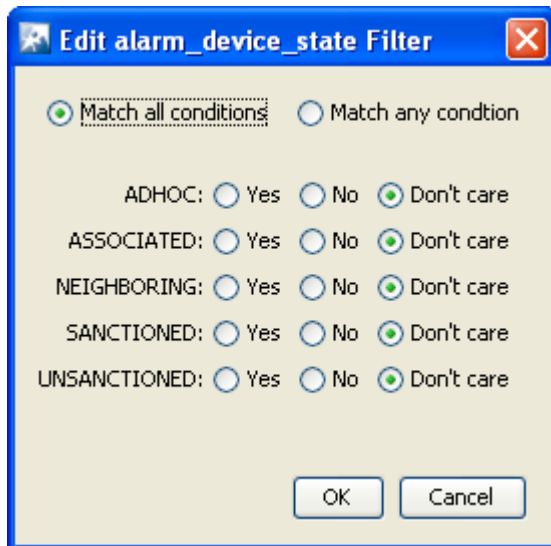
**Note**

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

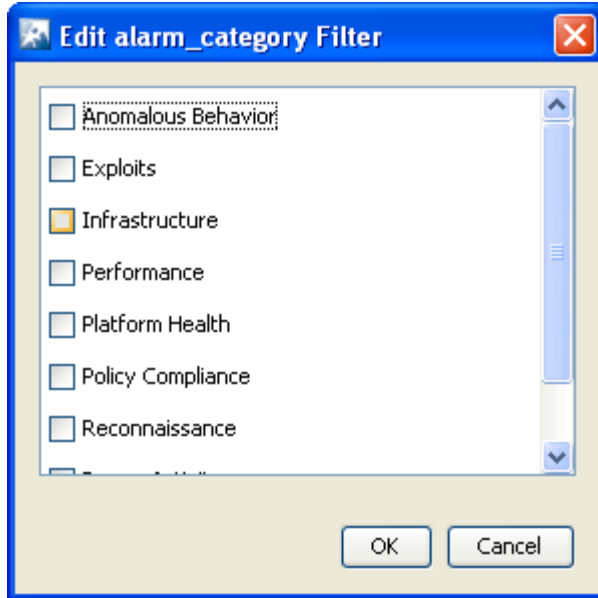
Configuring Report Filters

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:

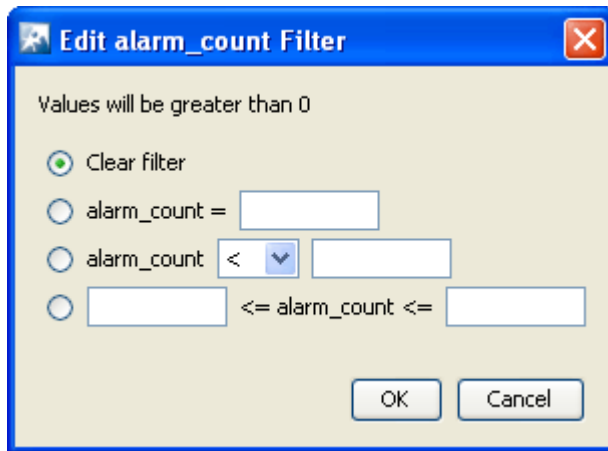
- Radio buttons (example):



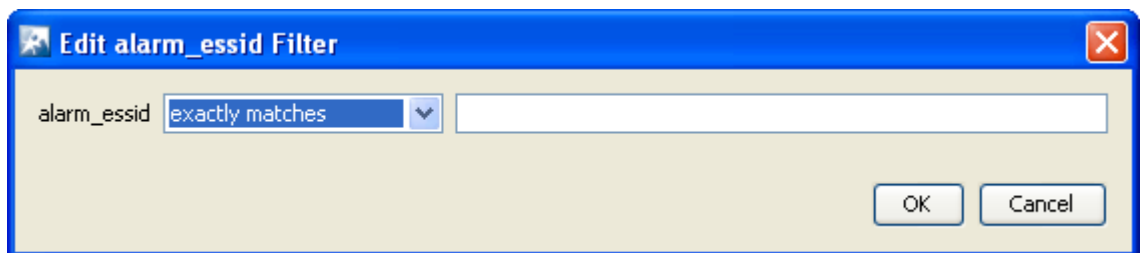
- Checkboxes (example):



- Boolean (example):



- Text box (example):

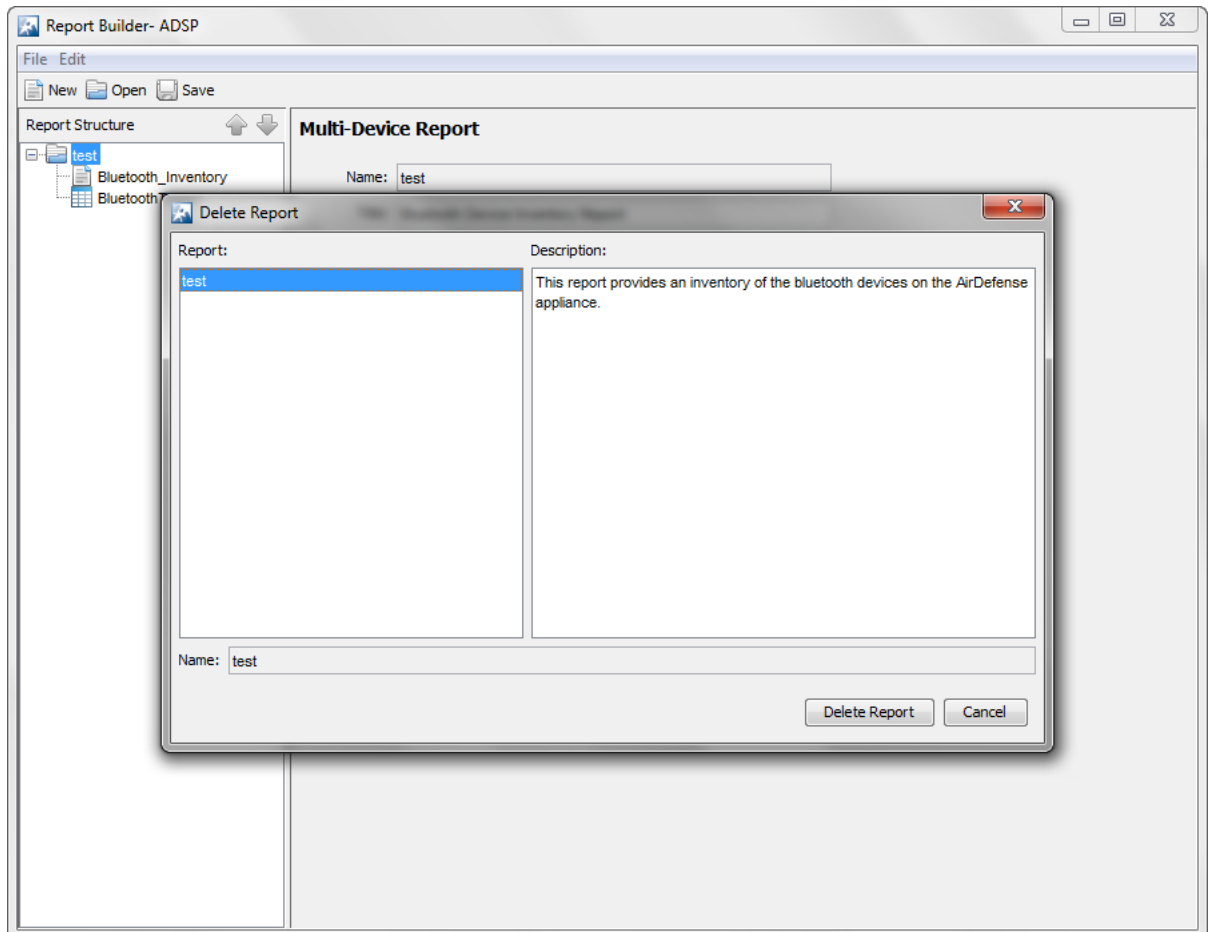


Deleting a Report

To delete an existing report:

1. Select **File > Delete Report** in the tool bar.

A Confirmation Window appears.



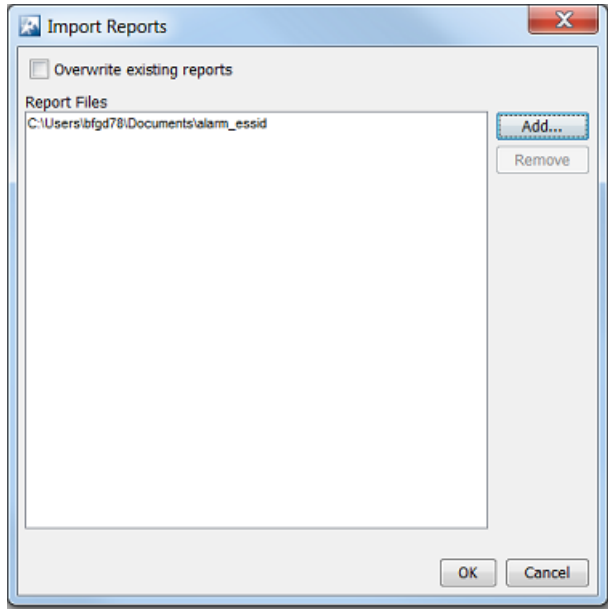
2. Select (highlight) the report that you want to delete.
3. Click **Delete Report** to delete.
4. Click **Yes** to confirm.

Importing a Report

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

1. Select **File > Import**.

The Import Reports window is displayed.



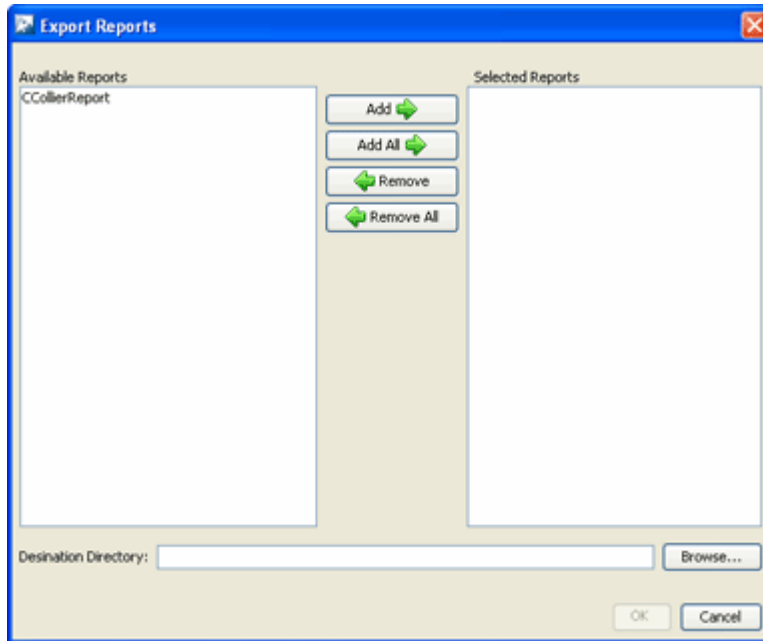
2. Click **Add**.
3. Navigate to the selected report, select (highlight) it, and click **Open**.
The report is added to the **Report Files** list. You may add as many reports as you like.
4. If a report name already exists, click the **Overwrite existing reports** checkbox.
5. Click **OK** to import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

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 then click **OK**.

The reported is exported to the selected directory on your PC.

Scheduled AP Tests

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 applications data path. Connectivity test can be configured two ways:

- scheduled
- on-demand

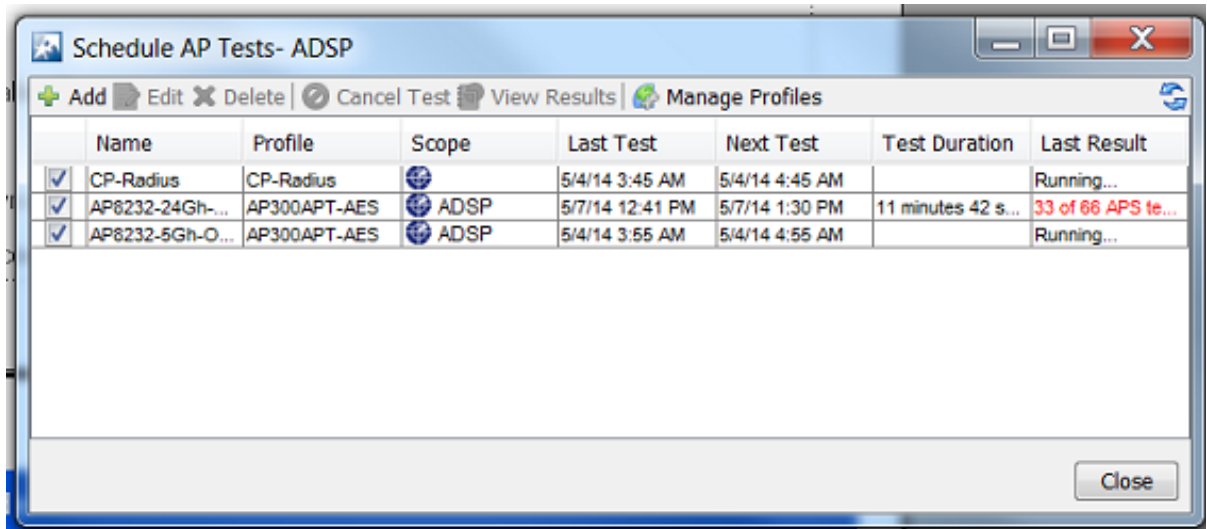
Scheduled AP Test



Note

Scheduled AP Test requires the 'AirDefense Toolkit' to work. Please download and install the AirDefense Toolkit from **Menu > Download Toolkit**.

You can schedule AP tests and view a list of AP Test scheduled for execution from the **Scheduled AP Test - ADSP** dialog.



You can do the following tasks from the **Scheduled AP Test - ADSP** window:

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

Scheduled AP Test can be launched from **Menu > Scheduled AP Test**

On-demand AP Tests

On-demand AP tests can be performed on sanctioned APs only. Select the AP to test from the **Networks** tab and then run the required AP tests on it.

To run an on-demand AP test:

1. Click the **Network** tab.
The **Network** tab loads and displays a list of all discovered APs.

2. Select BSS from the **Show** drop-down menu.
A list of APs is displayed.

Device	Severity	Last Seen	Scope	Floor	Channel	Signal S...	SSID	Rogue	AP
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	11(2.462 ...	-77 dBm	Aspen1.2	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-79 dBm	Aspen1.2	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	7(2.442 ...	-84 dBm	ASPENLBS	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm	Alpha-Corp	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm	Alpha-Net	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm		--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-72 dBm	Alpha-Corp	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-72 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-72 dBm	Alpha-Net	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-71 dBm		--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	7(2.442 ...	-86 dBm	ASPENLBS	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	11(2.462 ...	-87 dBm	tb1_auto...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-88 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-84 dBm	Paris	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-73 dBm	devextre...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-87 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-86 dBm	Aloha-Cord	--	

3. Select the AP you wish to test.



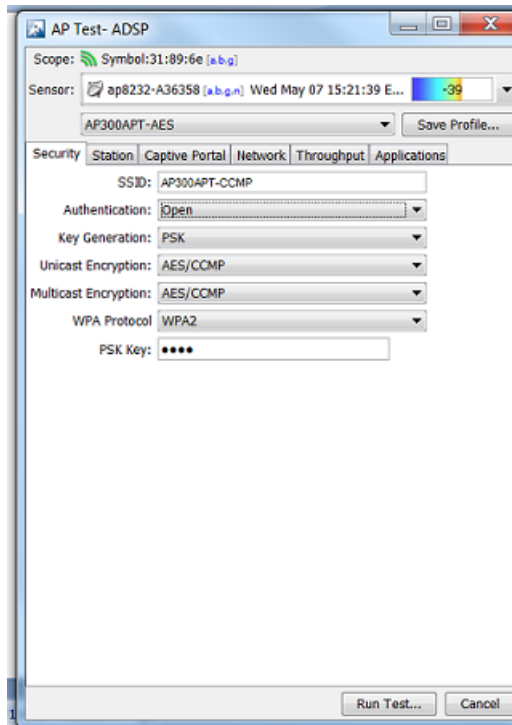
Note

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

4. Click on the down arrow on the device and in the drop-down menu, select **AP Test**.

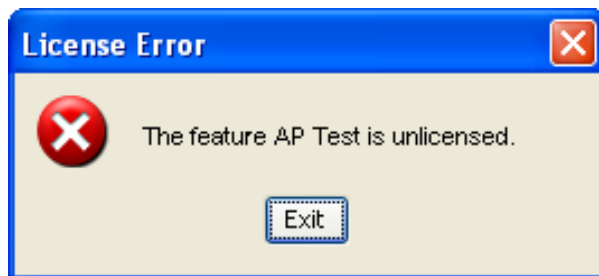
Device	Severity	Last Seen	Scope	Floor	Channel	Signal S...	SSID	Rogue	AP
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	11(2.462 ...	-77 dBm	Aspen1.2	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-79 dBm	Aspen1.2	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	7(2.442 ...	-84 dBm	ASPENLBS	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm	Alpha-Corp	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm	Alpha-Net	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-82 dBm		--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-72 dBm	Alpha-Corp	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-72 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-72 dBm	Alpha-Net	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-71 dBm		--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	7(2.442 ...	-86 dBm	ASPENLBS	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	11(2.462 ...	-87 dBm	tb1_auto...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-88 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-84 dBm	Paris	--	
ExtremeNetworks:...	Sever...	Wed Jan ...	ADSP	Unp...	1(2.412 ...	-73 dBm	devextre...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-87 dBm	Alpha-Ph...	--	
ExtremeNetworks:...	Safe(0)	Wed Jan ...	ADSP	Unp...	6(2.437 ...	-86 dBm	Aloha-Cord	--	

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



AP Test License

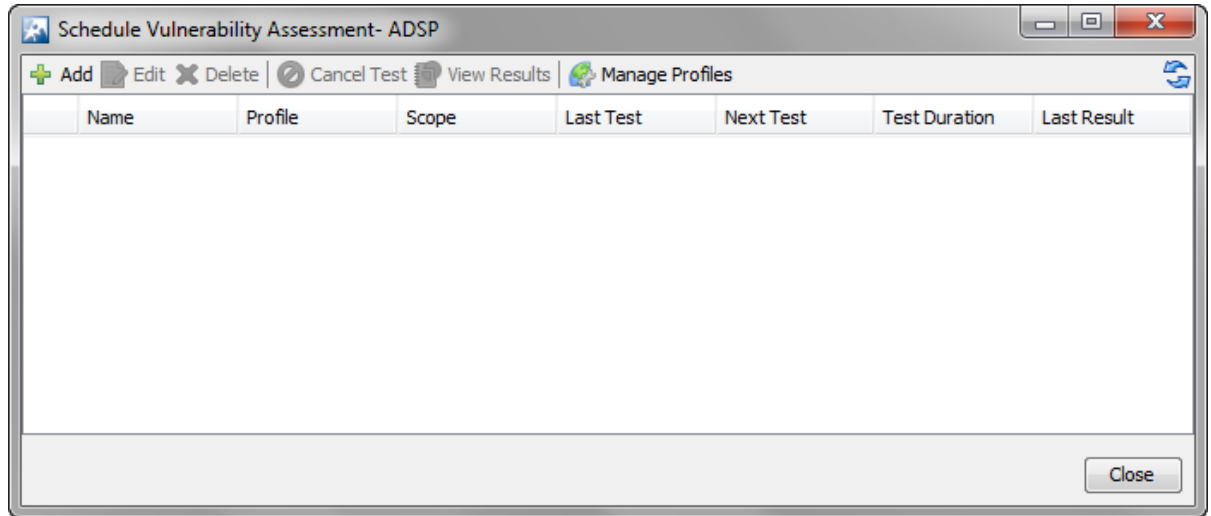
An AP Test license is required to access the **Scheduled AP Test** feature. AP Test is not part of the default AirDefense system. If the AP Test license is not installed, you will receive the following error when attempting to access the **Scheduled AP Test** feature:



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

Scheduled Vulnerability Assessment

Wireless vulnerability assessment provides remote wireless security testing. By simulating attacks from a wireless hackers 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.

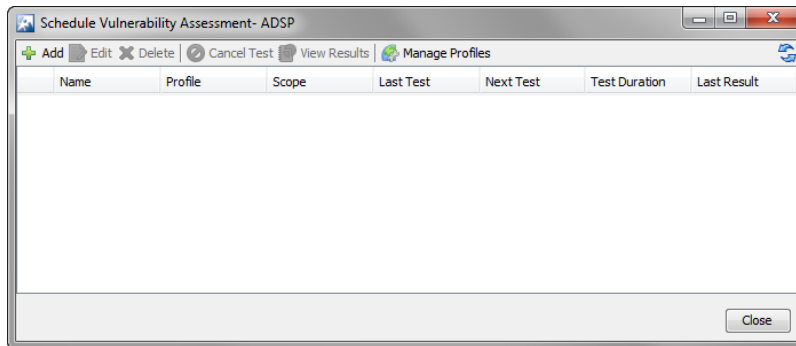


Scheduled Vulnerability Assessment

To manage and schedule Vulnerability Assessment:

1. Click **Menu > Scheduled Vulnerability Assessment**.

The **Vulnerability Assessment** window displays a list of existing Vulnerability Assessment tests.



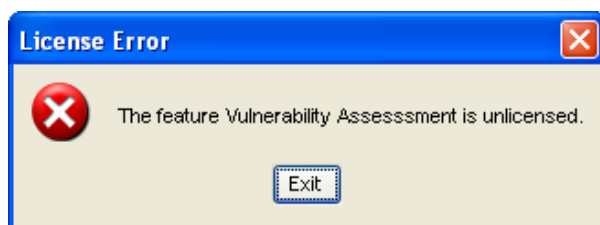
2. Select **Add** to create and add a new Scheduled Vulnerability Assessment test.

3. Select the **Ok** button after setting the parameters for this Vulnerability Assessment test.

At any time, select **Cancel** to exit without saving the configuration.

Vulnerability Assessment License

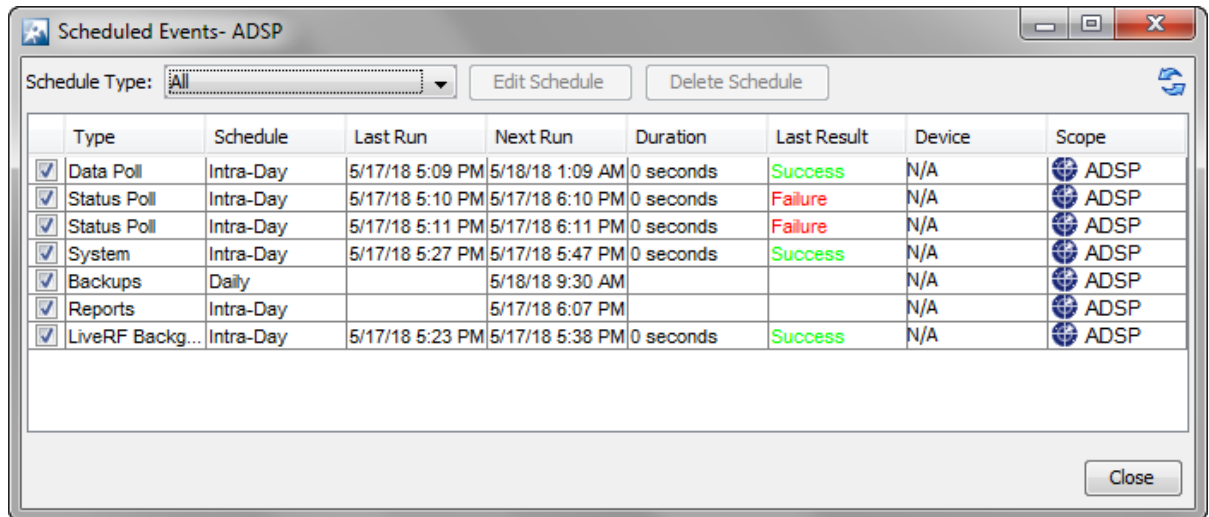
A Vulnerability Assessment license is required to access the Scheduled Vulnerability Assessment feature. Vulnerability Assessment is not part of the AirDefense basic system; therefore, you will receive the following license error when attempting to access the Scheduled Vulnerability Assessment feature:



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 AirDefense, and monitor the scheduled events from the Scheduled Events window.

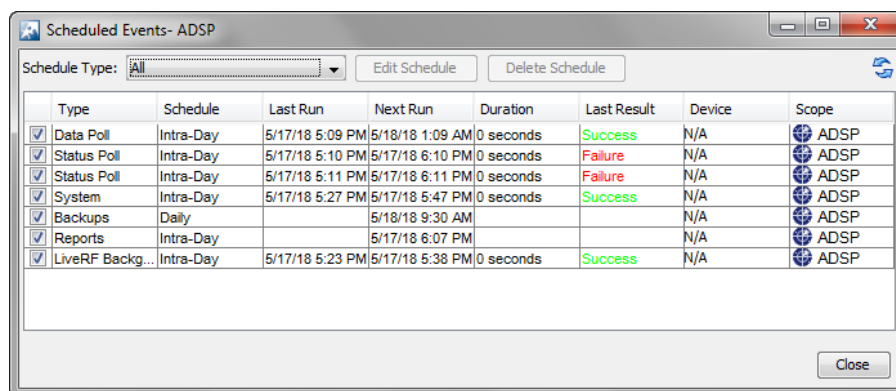


Monitoring Scheduled Events

Scheduled events can be monitored by:

1. Select **Menu > Scheduled Events**.

The **Scheduled Events** window displays with a list of events.



2. Use the **Schedule Type** drop-down to filter to the events of a particular type. Select **All** to view all scheduled events (default).

The different types of events that can be selected are:

<ul style="list-style-type: none"> • AP Test • Auto Classification • Backups • Firmware Upgrade • Frame Capture • Server Sync • System • Forensic Backup • Device Import • Vulnerability Assessment 	<ul style="list-style-type: none"> • Device Management Poll • Device Configuration • Deferred Device Configuration • LiveRF Background Analysis. • Primary Appliance Poll • Spectrum Analysis • WiNG Integration: Keep Alive • Logs Backup • Reports
---	---



Note

You cannot schedule new events using the **Scheduled Events** feature. You can only view, edit, or delete events.

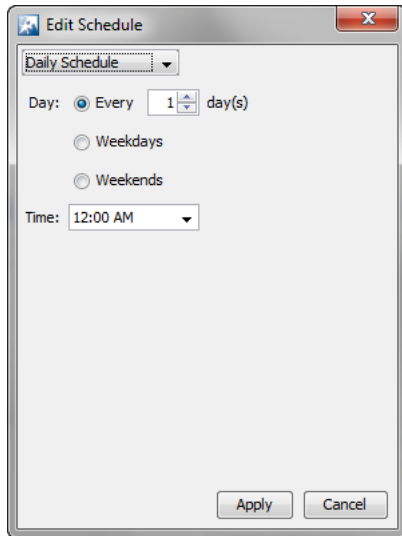
The following information is displayed for each event:

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.
Device	MAC address of the device if the event is reported for the device.
Scope	Scope of the report.

Altering Event Schedules

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

1. Select the event by highlighting it and then select the **Edit Schedule** button. The **Edit Schedule** window displays.



2. From the drop-down, select the appropriate schedule. 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 <i>day</i> , <i>weekdays only</i> , or <i>weekends only</i> . Then, select a time of day.
Weekly Schedule	Select the days of the week on which you want to schedule this event. Select the checkbox next to each day of the week to run the event on that particular day.
Monthly Schedule	Choose the months that you want to run the event 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.

Add Devices

Device Type: **BSS**

MAC Address:

Name:

Description:

Add to appliance: Primary appliance only All appliances

Annotations: Flagged Bridge

Classification: Neighboring
 Unsanctioned
 Sanctioned (Inherit Profiles)
 Sanctioned (Assign Profiles)

SecurityProfile1
 SecurityProfile10
 SecurityProfile11
 SecurityProfile12
 SecurityProfile13
 SecurityProfile14
 SecurityProfile15

Invalid MAC Address

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 screen is displayed when BSS is selected.

The screenshot shows the 'Add Devices' interface with the following elements:

- Device Type:** BSS (selected in a dropdown menu)
- MAC Address:** Text input field
- Name:** Text input field
- Description:** Large text area
- Add to appliance:** Radio buttons for 'Primary appliance only' and 'All appliances' (selected)
- Annotations:** Checkboxes for 'Flagged' and 'Bridge'
- Classification:** Radio buttons for 'Neighboring', 'Unsanctioned', 'Sanctioned (inherit)' (selected), and 'Sanctioned (override)'
- AD_ralfenator_Security_Profil:** A dropdown menu with a selected option.

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
Add to appliance	You may add the device to your primary appliance or all appliances that Extreme AirDefense is monitoring. Select the appropriate radio button.

Field	Description
Annotations	Specify if the device should be flagged or if it will be bridged. Select the appropriate checkbox.
Classification	Specify if the device should be classified as: <ul style="list-style-type: none"> • Neighboring • Unsanctioned • Sanctioned (Inherit Profiles) • Sanctioned (Assign Profiles) - 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 screen is displayed when `wireless client` is selected.

Add Devices

Device Type: Wireless Client

MAC Address:

Name:

Description:

Add to appliance: Primary appliance only All appliances

Annotations: Flagged Watch List

Client Type: Employee Personal Device

Classification: Neighboring
 Unsanctioned
 Sanctioned (Inherit Profiles)
 Sanctioned (Assign Profiles)

SecurityProfile1
 SecurityProfile10
 SecurityProfile11
 SecurityProfile12
 SecurityProfile13
 SecurityProfile14
 SecurityProfile15

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 Extreme AirDefense is monitoring. Select the appropriate radio button.
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Neighboring • Unsanctioned • Sanctioned (Inherit Profiles) • Sanctioned (Assign Profiles) - 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 screen is displayed when one of the following device types, Access Points, Wired Switches, Wireless Switches, WLSE, AirWave, or MSP, is selected.

The screenshot shows the 'Add Devices' interface. At the top right, 'Device Type' is set to 'Access Point'. The form contains the following fields:

- MAC Address:
- Name:
- Scope:
- Host:
- Description:

The following fields are available when adding the above device types.

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 screen is displayed when Appliance is selected.

The screenshot shows the 'Add Devices' interface with 'Device Type' set to 'Appliance'. The form contains the following fields:

- Name:
- Host:
- Port:

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 device 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.

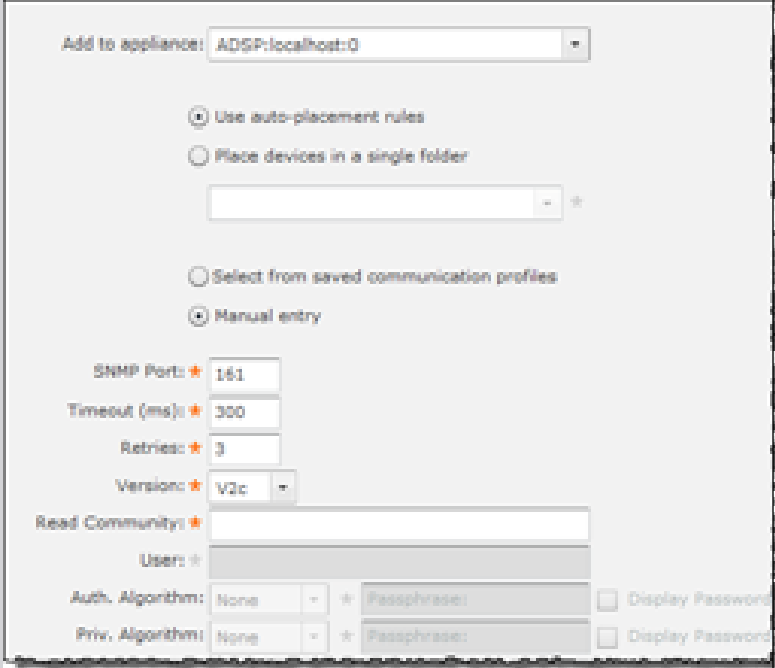
Importing profile settings requires a separate import file. You should not combine importing profiles with importing devices.

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.

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

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)
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)

Import from Wireless Manager or 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
- 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 the appropriate topic in the AirDefense Help.



Note

You can only access this information in the AirDefense 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 AirDefense 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](#) on page 431 topic.

To view the information, click on a link below in the AirDefense Help.

**Note**

You can only access this information in the AirDefense 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=
- 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/UnplacedDevices,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.

Bluetooth devices are imported into AirDefense using a *csv* file. These devices are initially classified as *Unplaced* devices. When an imported Bluetooth device is seen, it is classified into its proper category and placed appropriately.

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.

Bluetooth is natively supported in AP7602, AP7622, AP8532, AP8533 and AP8432 devices and these devices do not require the IO Gear GBU321 BT sensor.

Importing Bluetooth Devices

To import Bluetooth devices, go to Menu in the AirDefense 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 AirDefense, 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 WIPS license on the sensor device in order to access the Bluetooth feature.

AirDefense Dashboard

The Extreme AirDefense Dashboard provides a quick visual representation of your network. Network state and other information is displayed using widgets. You can select from a large array of useful widgets to customize the AirDefense Dashboard to display the network state information that you are interested in.

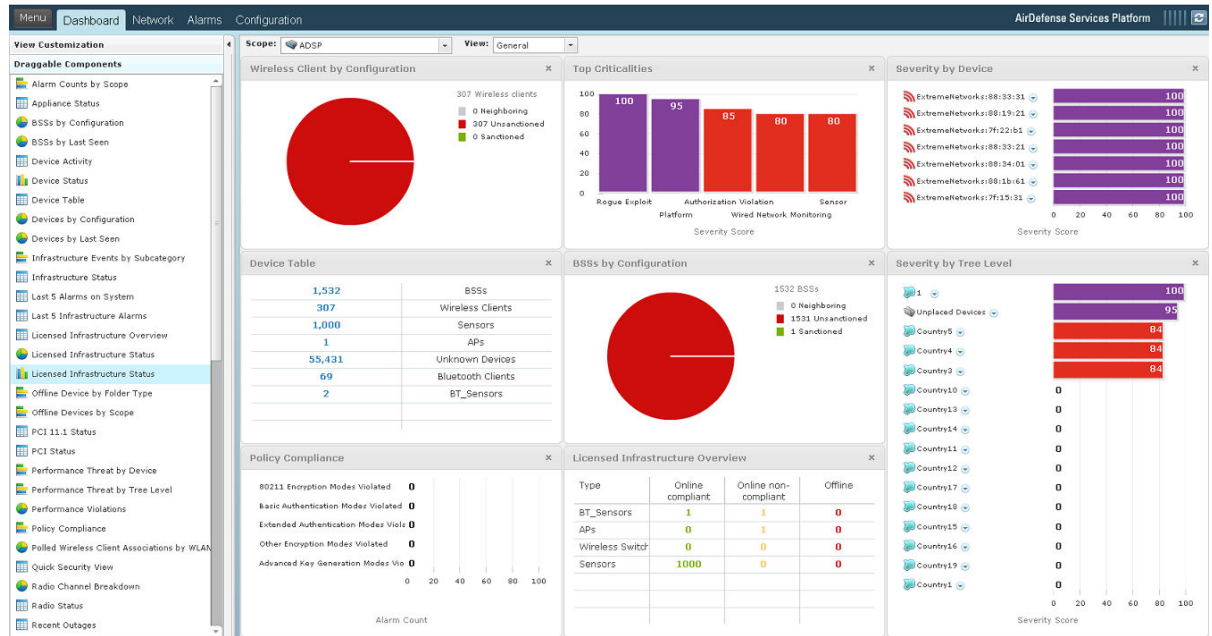
The Dashboard

The AirDefense 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.

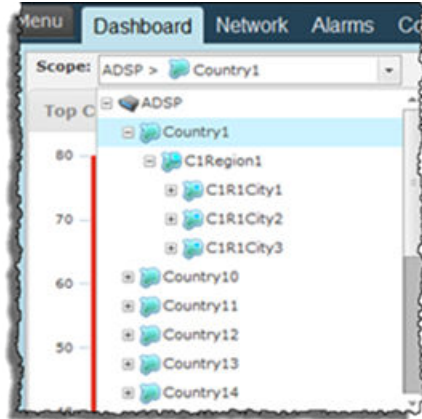
See the [Dashboard Components](#) on page 439 topic for a description of all the available components.

You can hide dashboard components by clicking **Hide Dashboard Components** bar .

You can show (un-hide) dashboard components by clicking the **i** 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:

- SystemDisplays 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.
- ADSPDisplays 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.
- CountryDisplays information about a specific country including regions, cities, campuses, buildings, and floors.
- RegionDisplays information about a specific region including cities, campuses, buildings, and floors.
- CityDisplays information about a specific city including campuses, buildings, and floors.
- CampusDisplays information about a specific campus including buildings and floors.
- BuildingDisplays information about a specific campus including floors.
- FloorDisplays information about a specific floor.

Capabilities with a Central Management License

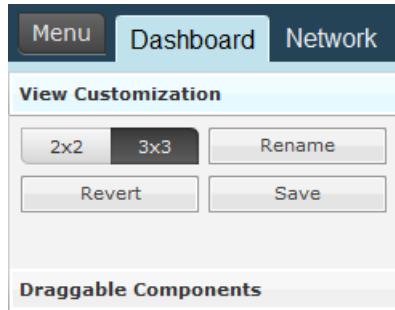
With a Central Management license, the Dashboard becomes a monitor of all appliances along with their associated devices. You can monitor your entire system at once or each individual appliance. Additionally, you may include information about other servers in your network. When you include other servers in your Dashboard, all scope information is included.

Customizing Dashboard Views

This topic discusses the options available to customize your AirDefense Dashboard.

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 seen 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.
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.

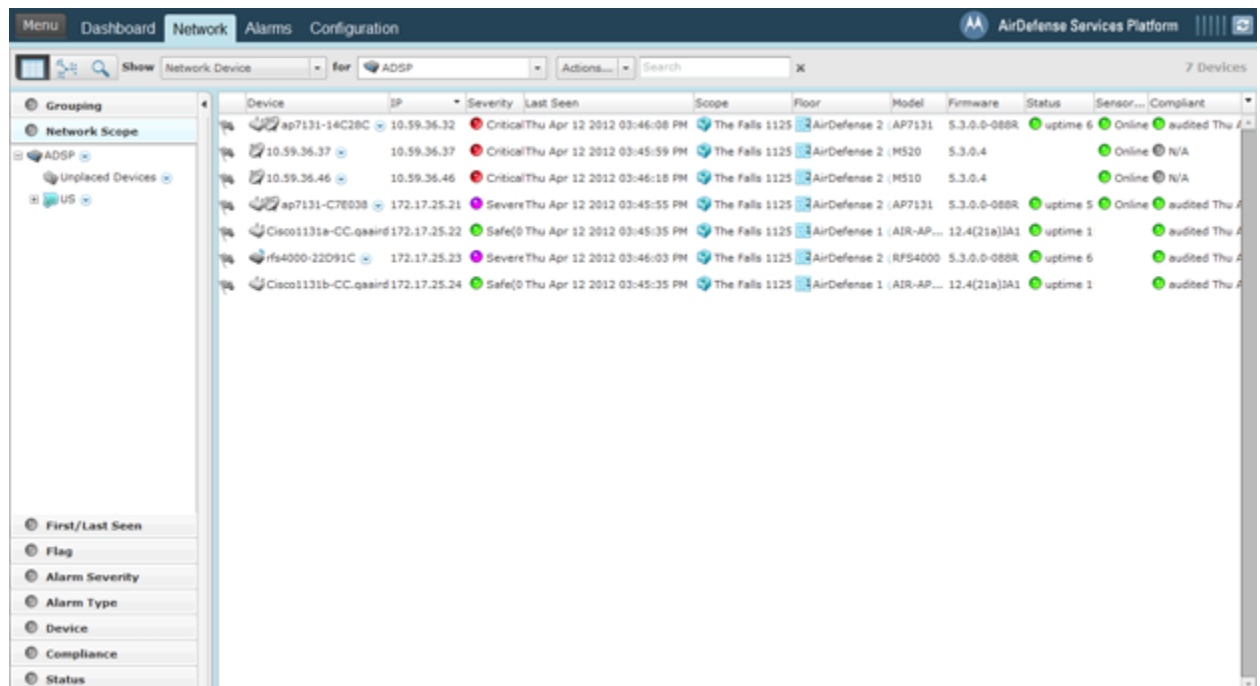
Component	Description
Licensed Device Breakdown by Model	Displays a pie chart showing licensed devices on your network grouped by model.
Licensed Infrastructure Overview	Displays a list of infrastructure devices in three columns (Online compliant, Online non-compliant, and Offline).
Licensed Infrastructure 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.
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.

Component	Description
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: <ul style="list-style-type: none"> • Sensor count • Managed network devices • Total device load • Active device load.
Termination Count by Scope	Displays a bar chart showing a total termination count by scope.
Termination Status	Displays a pie chart showing the number devices not on the termination list and number of devices on the termination list.
Top Criticalities	Displays a column chart showing top alarms observed by ADSP.
Top Infrastructure Alarms by Count	Displays a bar chart showing the top infrastructure alarms by count.
Top Infrastructure Criticalities	Displays a column chart showing the top infrastructure alarms observed by ADSP.
Top Performance Alarms by Count	Displays a bar chart showing the alarm count of the top performance policy violations.

Component	Description
Top Security Alarms by Count	Displays a bar chart showing the alarm count of the top security policy violations.
Top Talkers	Displays a bar chart showing the top 5 BSS and Wireless Client talkers on the network based on the combined value of sensed total TX and total RX bytes.
Top Wireless Exploits by Count	Displays a bar chart showing the alarm count for wireless exploits on your network.
Top Wireless Extrusions by Count	Displays a bar chart showing the alarm count for wireless extrusions on your network.
Top Wireless Vulnerability by Count	Displays a bar chart showing the alarm count for wireless vulnerability on your network.
Wireless Client by Configuration	Displays a pie chart of Wireless Clients by configuration (authorized, ignored, and unauthorized). Also lists the total number of Wireless Clients seen on your network.
Wireless Client by Last Seen	Displays a pie chart of the Wireless Clients seen on your network over the last five days. Also lists the total number of Wireless Clients as well as the totals for each day.
Wireless IPS Availability	Lists a count of online and offline Sensors on your network.

Network 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.

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 AirDefense system or a specific city, building, floor, etc.

Actions Menu

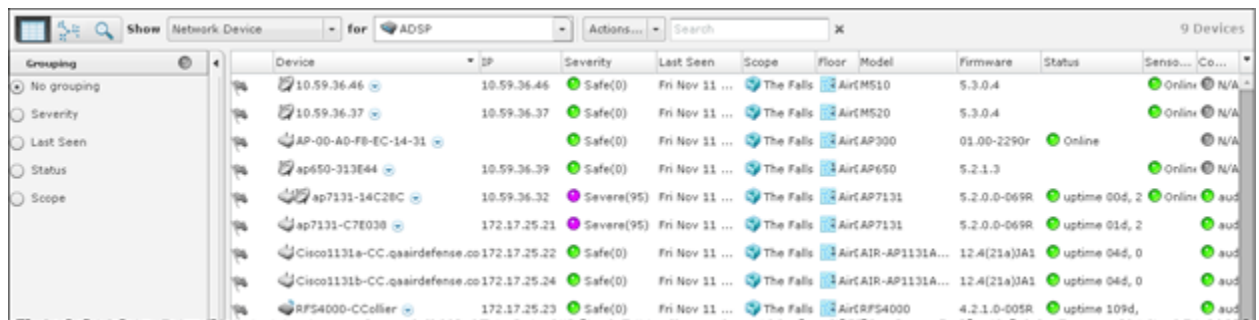
From the drop-down menu under Actions on the top menu bar, you can select an action to apply to the selected device. The actions available vary by device, as explained in the following section, Network Devices.

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 .

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)






Column	Description
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)
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**. AirDefense displays a list of all BSSs seen in your wireless network.

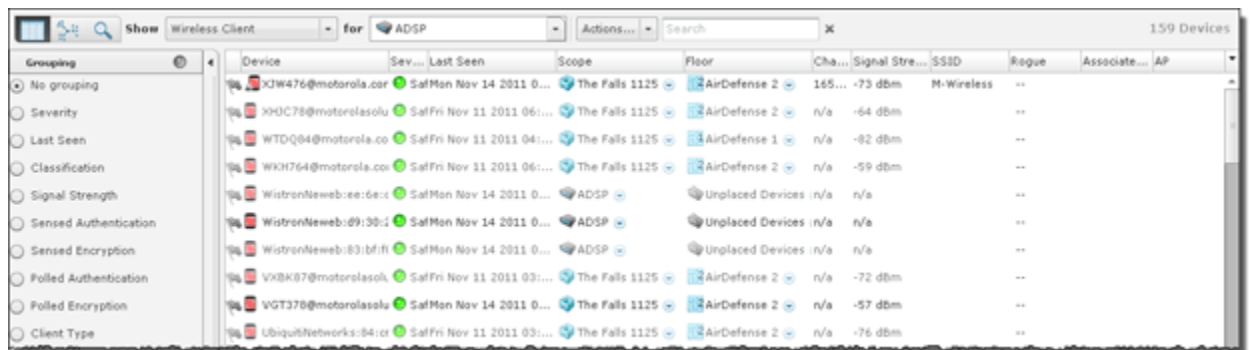
The list of BSSs are displayed in a tabular format using a combination of the following columns:

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)
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.


Column	Description
Rogue	Indicates if a BSS is a rogue (true or false). (default header)
Device Actions	Indicates a current live state. <ul style="list-style-type: none"> 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**. AirDefense displays a list of all Wireless Clients seen in your wireless network.



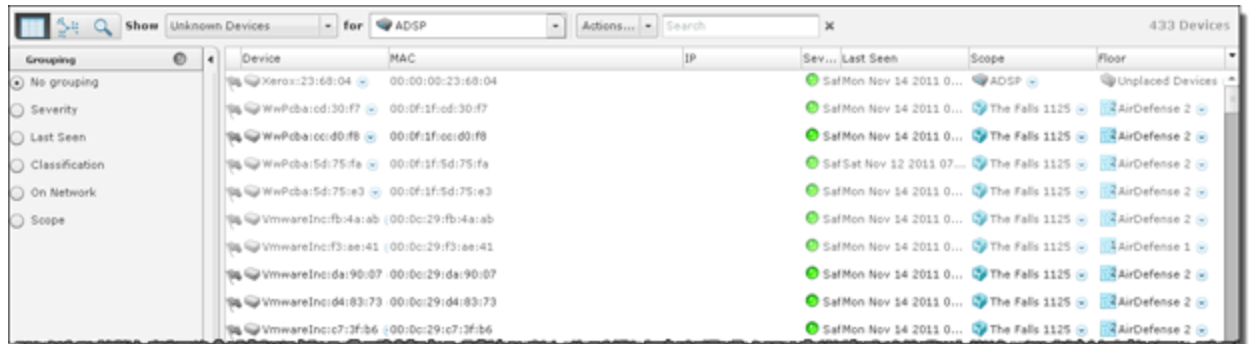
A list of wireless clients is displayed in a tabular format using a combination of the following columns:

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 Clients MAC address.
IP	Displays the Wireless Clients IP address.
Severity	Displays the Wireless Client threat level to your network. (default header)

Column	Description
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)
Device Actions	Indicates if any of the following actions have occurred: <ul style="list-style-type: none"> • 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**. AirDefense 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. AirDefense 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 AirDefense, it is considered 'unknown'. These are almost always infrastructure devices on the wired network.



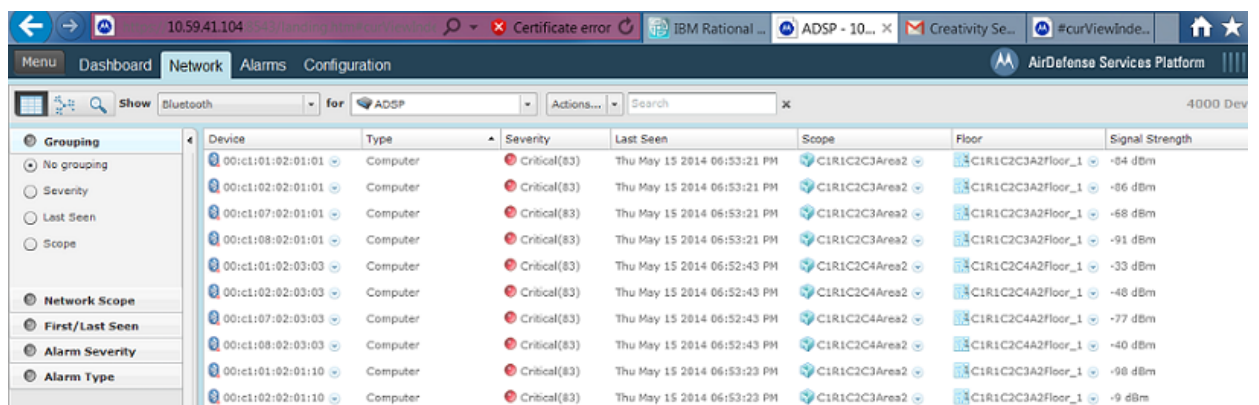
The list of Unknown Devices are displayed in a tabular format using a combination of the following columns:

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 Devices MAC address. (default header)
IP	Displays the Unknown Devices 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.

Column	Description
On Network	<p>Identifies how AirDefense obtained the MAC address of a non-wireless device. The different entries are:</p> <ul style="list-style-type: none"> • Sensor SegmentThe 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. • SwitchThis 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. • BlankThis MAC address was detected by a sensor radio and the wireless device communicating with this MAC is not sanctioned in AirDefense. This is most likely a device on a neighboring network and not part of the AirDefense protected infrastructure. • Sanctioned BSSThis MAC address has been seen by a sensor in communication with a Sanctioned BSS and is likely to be a device on the AirDefense protected infrastructure, but has not been reported to AirDefense 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**. AirDefense 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

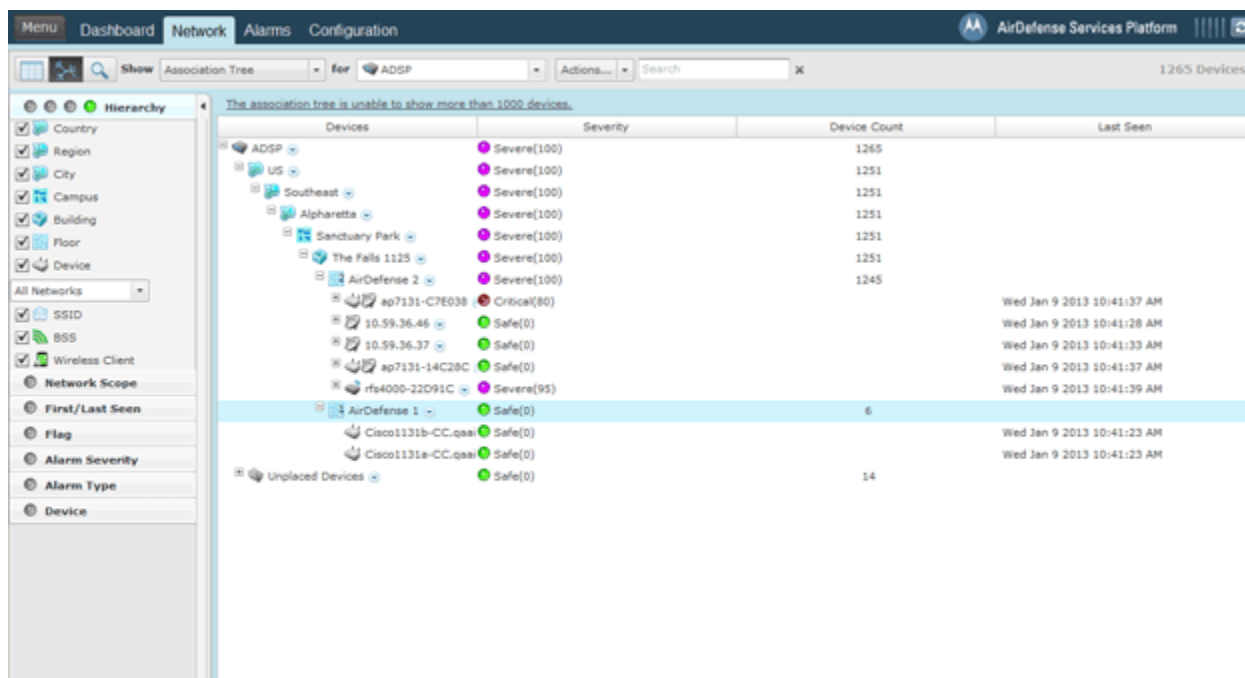
Live View is not supported on Menu Networks.

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.



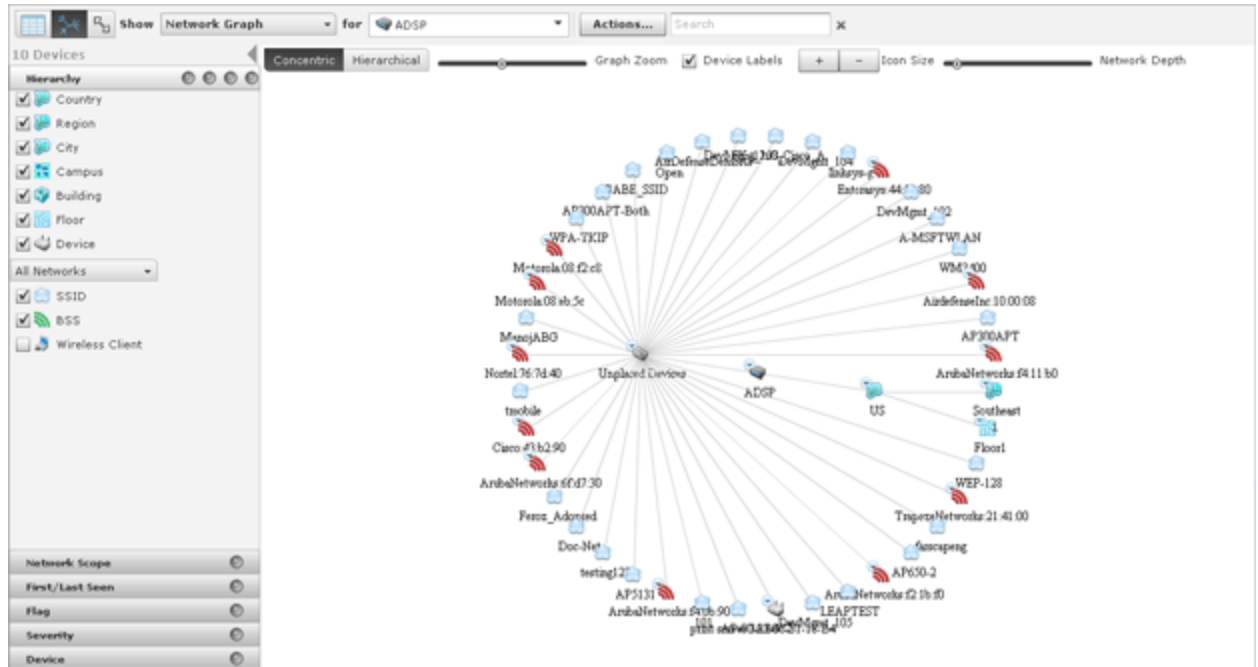
Click the **Expand** button to open a branch of the tree. Click the **collapse** button to close a branch of the tree. The table columns for the Association Tree are:

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.

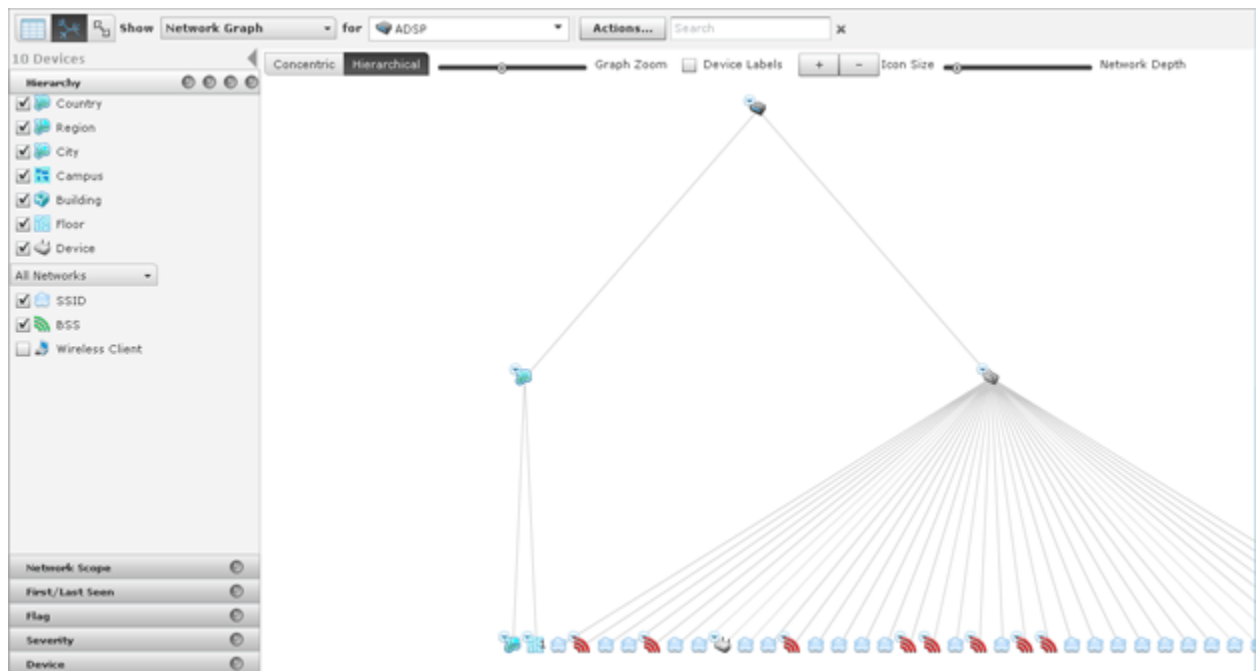
Network Graph

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.

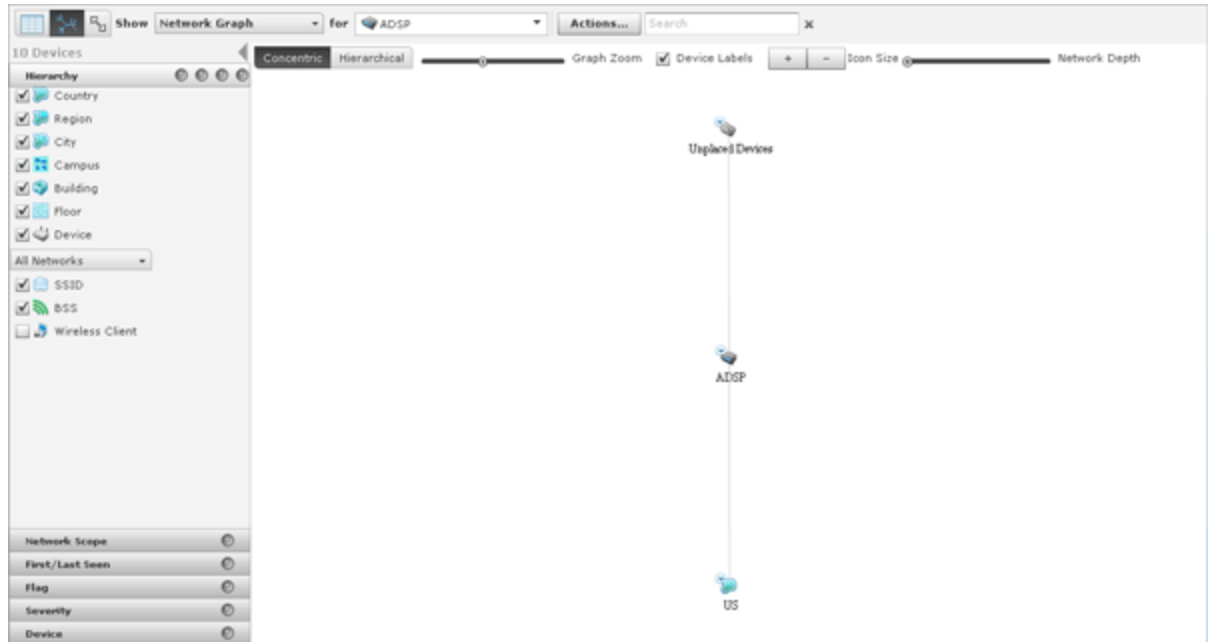


To switch to the Hierarchical view, click the **Hierarchical** button.



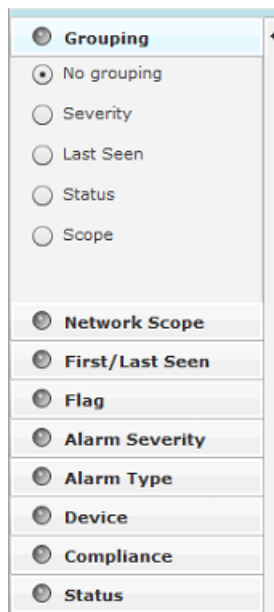
Click **Concentric** to return to the **Concentric** view. You can manipulate the graph by using:

- **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 were first seen and/or last seen on your network.

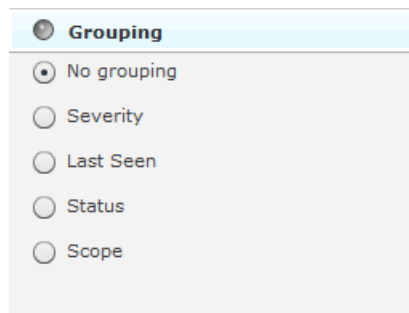
- **Flag** - you can optionally view all flagged devices.
- **Alarm Severity** - you can view devices by alarm criticality.
- **Alarm Type** - filters devices by alarm type.
- **Device** - filters devices by model, manufacturer, and/or capabilities.
- **Compliance** - displays devices according to state 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.

Severe	13 Devices
Critical	5 Devices
Major	213 Devices

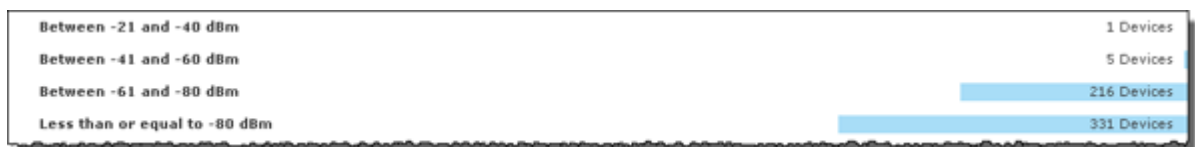
- **Last Seen** - Groups devices by a time frame when the devices were last seen on your network. This view is accessible when displaying any type of device.



- **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.



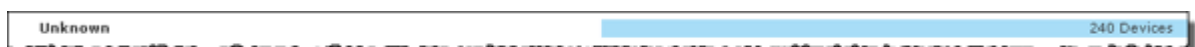
- **Sensed Encryption** - Groups devices based on their sensed method of encryption. This view is accessible when displaying BSSs or Wireless Clients.



- **Polled Authentication** - Groups devices based on their polled method of authentication. This view is accessible only when displaying Wireless Clients.



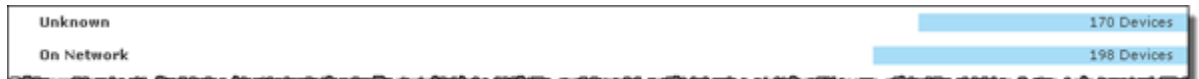
- **Polled Encryption** - Groups devices based on their polled method of encryption. This view is accessible only when displaying Wireless Clients.



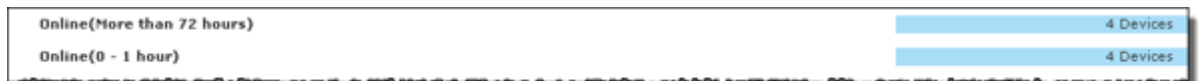
- **Client Type** - Groups devices based on their client type. This view is accessible only when displaying Wireless Clients.



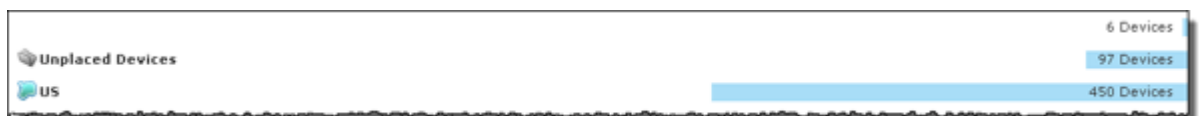
- **On Network** - Groups devices based whether they are on the network or not. This view is accessible only when displaying Unknown Devices.



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



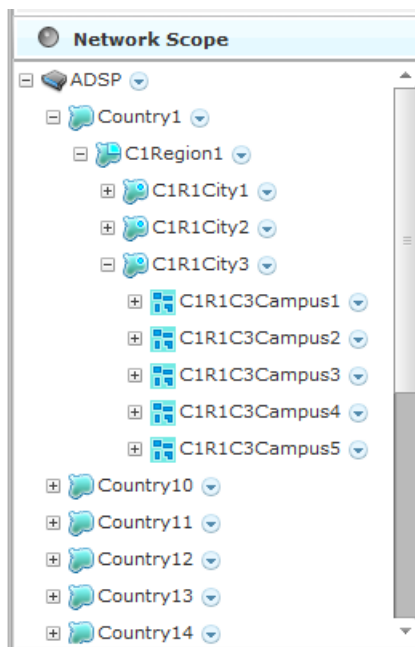
- **Scope** - Groups devices based on where they are in the network. The highest network level under the appliance level is displayed as the group. This view is accessible when displaying any type of device.



Clicking on a group will display the devices in that group.

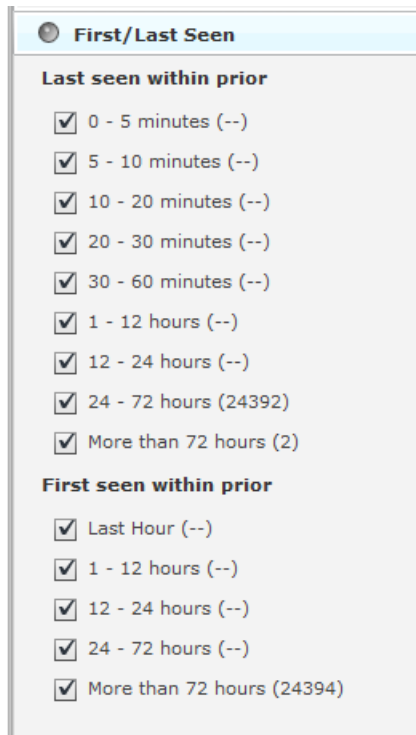
Network Scope Filter

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



The screenshot shows a configuration window titled "First/Last Seen". It contains two sections: "Last seen within prior" and "First seen within prior". Each section has a list of time intervals with checkboxes. In the "Last seen within prior" section, all checkboxes are checked. In the "First seen within prior" section, all checkboxes are also checked. The counts for the "More than 72 hours" options are 24392 for the last seen filter and 24394 for the first seen filter.

Section	Filter Option	Count
Last seen within prior	<input checked="" type="checkbox"/> 0 - 5 minutes (--)	
	<input checked="" type="checkbox"/> 5 - 10 minutes (--)	
	<input checked="" type="checkbox"/> 10 - 20 minutes (--)	
	<input checked="" type="checkbox"/> 20 - 30 minutes (--)	
	<input checked="" type="checkbox"/> 30 - 60 minutes (--)	
	<input checked="" type="checkbox"/> 1 - 12 hours (--)	
	<input checked="" type="checkbox"/> 12 - 24 hours (--)	
	<input checked="" type="checkbox"/> 24 - 72 hours (24392)	24392
	<input checked="" type="checkbox"/> More than 72 hours (2)	2
First seen within prior	<input checked="" type="checkbox"/> Last Hour (--)	
	<input checked="" type="checkbox"/> 1 - 12 hours (--)	
	<input checked="" type="checkbox"/> 12 - 24 hours (--)	
	<input checked="" type="checkbox"/> 24 - 72 hours (--)	
	<input checked="" type="checkbox"/> More than 72 hours (24394)	24394

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.

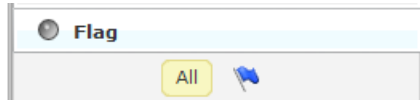
The first seen times may be:

- 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

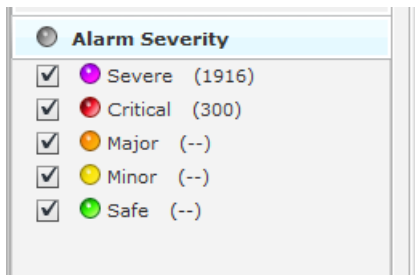
The Flag filter gives you the option of viewing all devices or only flagged devices.








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.



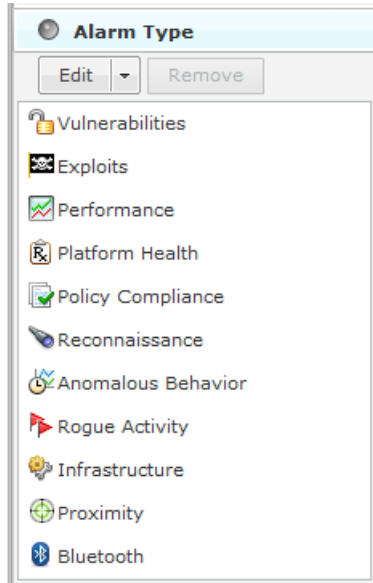
The severities are:

- 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

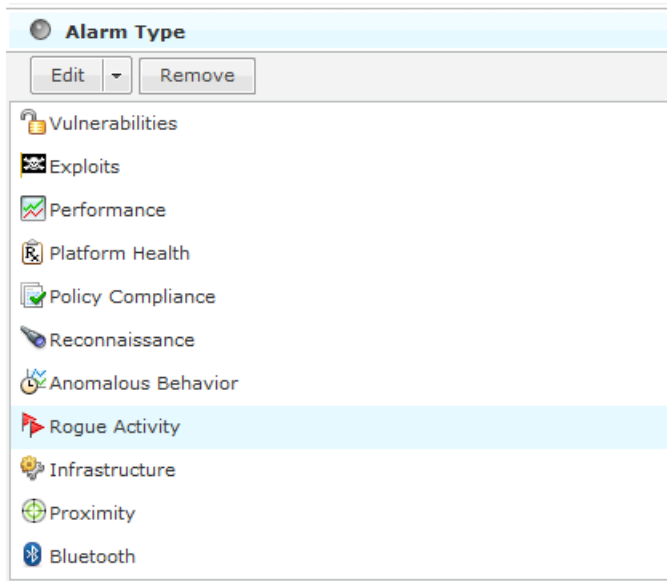
The Alarm Type filter allows you to view devices by alarm type. Devices are grouped together according to their alarm threat to your network.



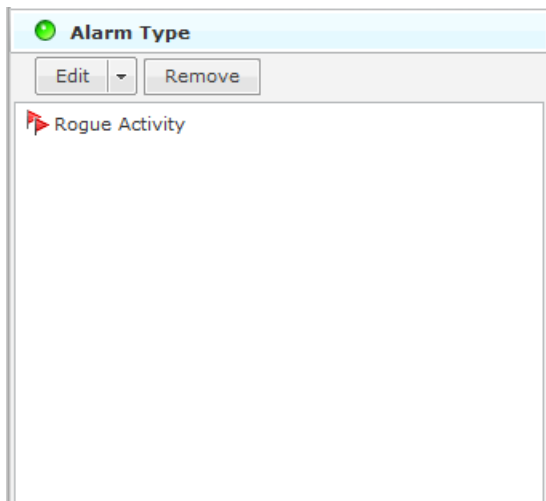
You have the option of displaying all alarm types or filtering alarms by a specific type. The different alarm types are:

- 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.



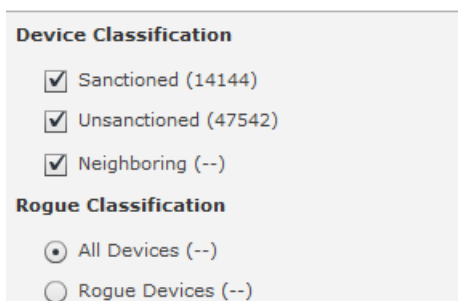
Click Edit, select the alarm type(s), and then click OK. The following graphic shows that you only want to display rogue alarms.



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:

- SanctionedDisplay sanctioned devices.
- UnsanctionedDisplay unsanctioned devices.
- NeighboringDisplay 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 check-box 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

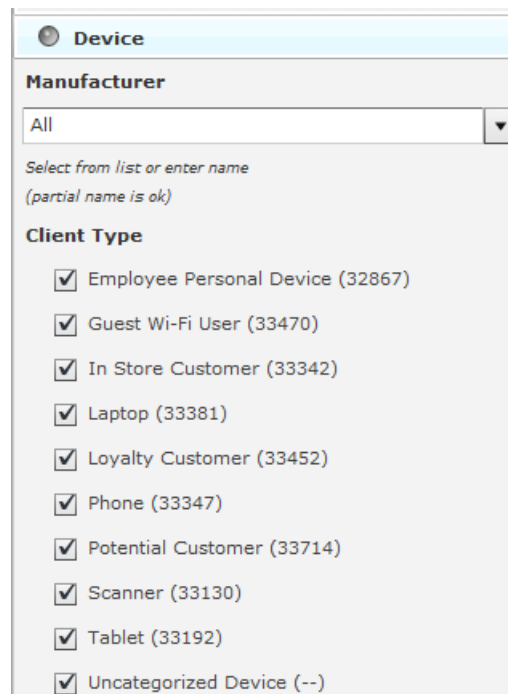
For network devices, you can filter devices based on the model type. Select a model from the Model drop-down menu

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:

- Access Point
- 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.



The screenshot shows a web interface for filtering devices. At the top, there is a tab labeled "Device". Below it, the "Manufacturer" section features a dropdown menu currently set to "All". Underneath the dropdown, there is a prompt: "Select from list or enter name (partial name is ok)". The "Client Type" section below contains a list of ten categories, each with a checked checkbox and a count in parentheses: Employee Personal Device (32867), Guest Wi-Fi User (33470), In Store Customer (33342), Laptop (33381), Loyalty Customer (33452), Phone (33347), Potential Customer (33714), Scanner (33130), Tablet (33192), and Uncategorized Device (--).

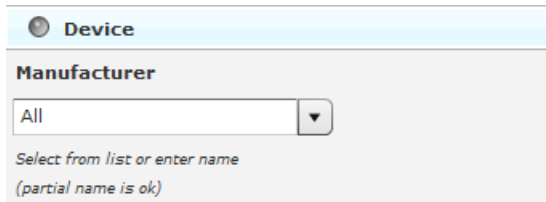
You can also filter Wireless Clients based on the client type. When you select a client type, only devices of that type are displayed. You may select from the following client types:

- 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.



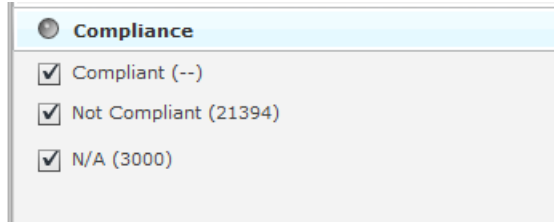
The screenshot shows a filter panel titled "Device". Under the "Manufacturer" section, there is a dropdown menu currently set to "All". Below the dropdown, there is a text prompt: "Select from list or enter name (partial name is ok)".

Bluetooth Devices

There are no device filter for Bluetooth devices.

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



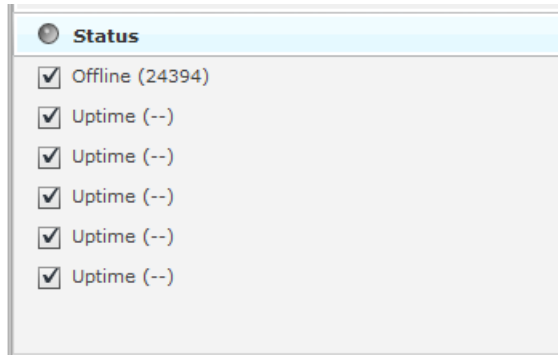
The screenshot shows a filter panel titled "Compliance". It contains three checked options: "Compliant (--)", "Not Compliant (21394)", and "N/A (3000)".

.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.



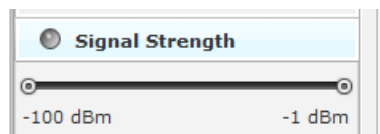
Note

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.

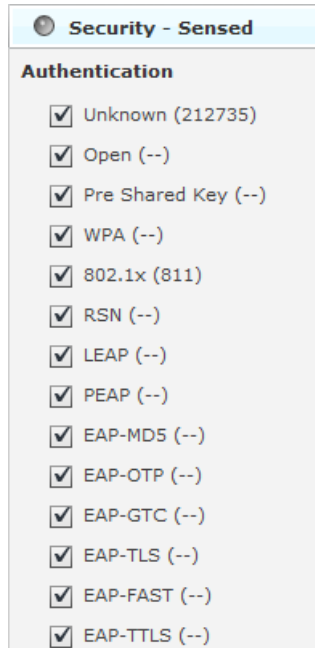


Figure 122: Authentication

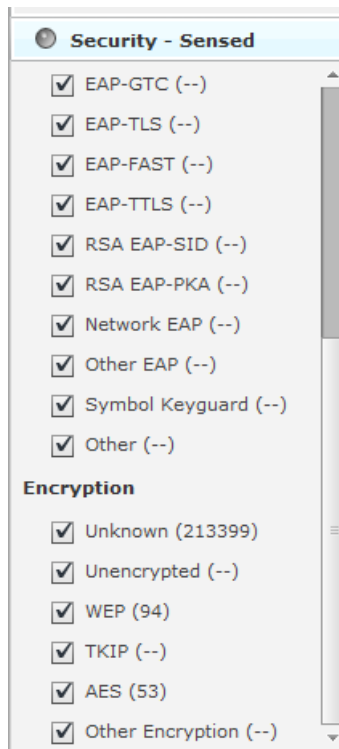


Figure 123: Encryption

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.



The screenshot shows a configuration window titled "Security - Polled". It is divided into two sections: "Authentication" and "Encryption". Each section contains a list of options, each with a checked checkbox and a label. The "Authentication" section includes: Open (--), Pre Shared Key (--), EAP (--), WPA (--), WPA PSK (--), WPA2 (--), WPA2 PSK (--), and Unknown (213546). The "Encryption" section includes: Unencrypted (--), WEP64 (--), WEP128 (--), AES (--), TKIP (--), Symbol Keyguard (--), and Unknown (213546).

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.

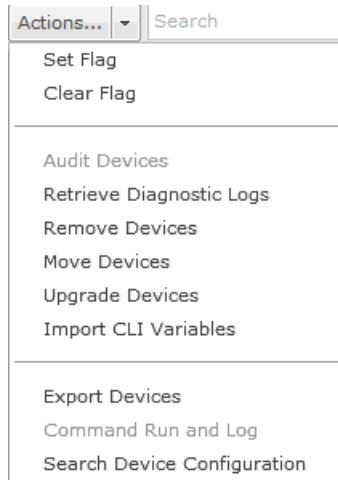
The available encryption methods are:

- Unencrypted
- WEP64
- WEP128
- AES(CCMP)
- TKIP
- Symbol Keyguard
- WPA2 PSK.

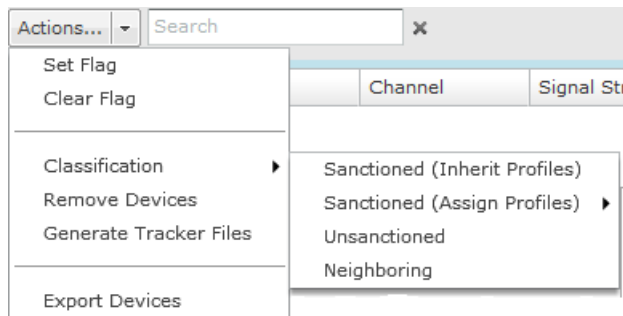
Actions Menu

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:

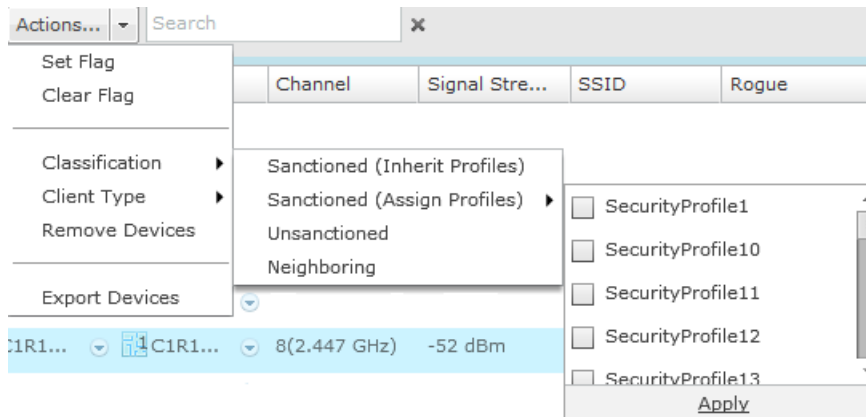
Network Device Actions

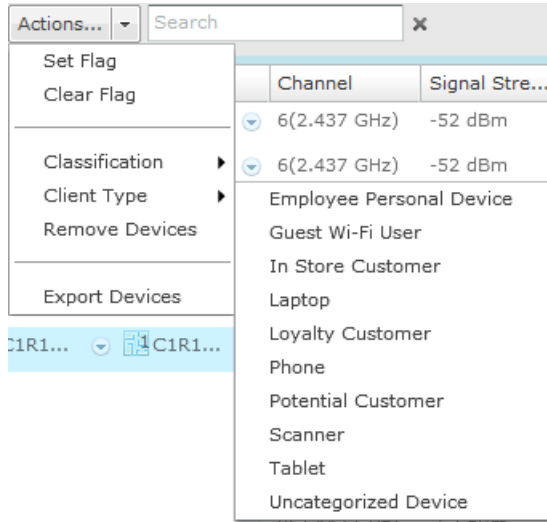


BSS Actions

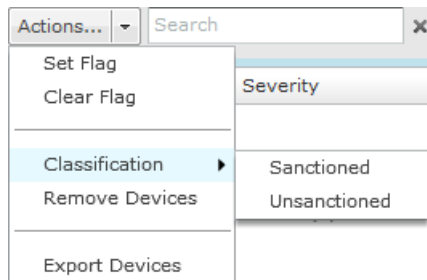


Wireless Client Actions

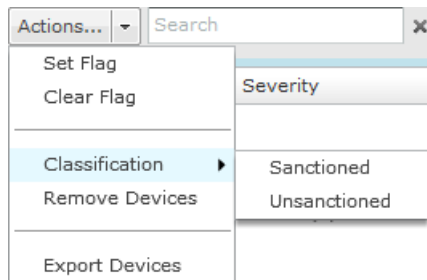




Unknown Devices Actions



Bluetooth Devices Actions



Actions Descriptions

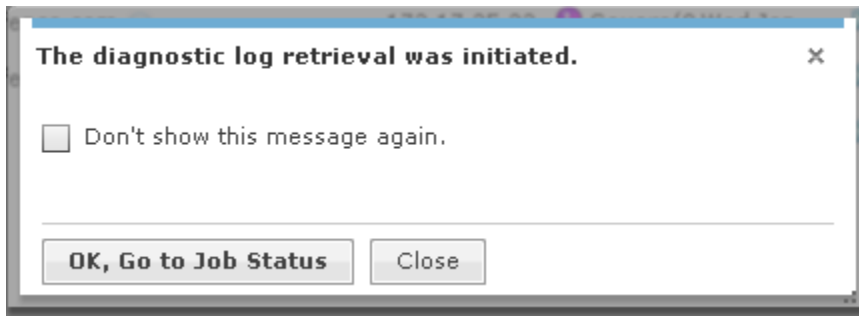
Actions are active (selectable) or inactive (un-selectable) depending on the device type selected in the Show menu. Some actions are executed when you select a device and then select an action. In this case, no other input is required. Other actions will display a dialog that require more input. Descriptions 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).

Action	Description
Classification	<p>Sanctioned (inherit) Classify the selected device(s) as a sanctioned device that inherits its traits from wherever its location in the network tree.</p> <p>Sanctioned (override) Classify the selected device(s) as a sanctioned device using traits that override the inherited traits. For example, a security profile can be applied to a BSS that overrides the inherited traits.</p> <p>Sanctioned Classify the selected device(s) as sanctioned (Unknown Devices only)</p> <p>Unsanctioned Classify the selected device(s) as unsanctioned.</p> <p>Neighboring Classify the selected device(s) as a neighboring device.</p>
Client Type	<p>Classifies a Wireless Client as one of the following types:</p> <ul style="list-style-type: none"> • 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 < LINK HERE >.)
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 < LINK HERE >.)
Remove Devices	Allows you to remove selected device(s) from monitoring (see < LINK HERE >.)
Move Devices	Allows you to place selected device(s) on a floor (see < LINK HERE >.)
Upgrade Devices	Allows you to upgrade the firmware for the selected device(s) (see < LINK HERE >.)
Import CLI Variables	Allows you to import CLI variables at the device level (see < LINK HERE >.)
Export Devices	Allows you to export information about selected device(s) to a CSV file (see < LINK HERE >.)
Command Run and Log	Allows you to execute CLI commands for selected device(s) and save results in a log file (see < LINK HERE >.)
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

Retrieve Diagnostic Logs

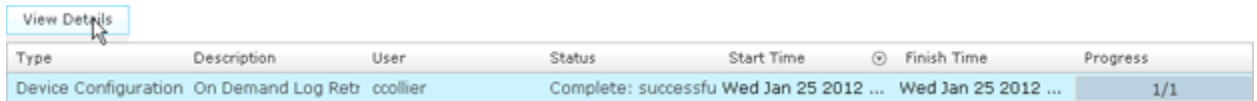
To retrieve the diagnostic logs for the selected device in one consolidated file, elect (highlight) a device and then click **Actions > Retrieve Diagnostic Logs**.



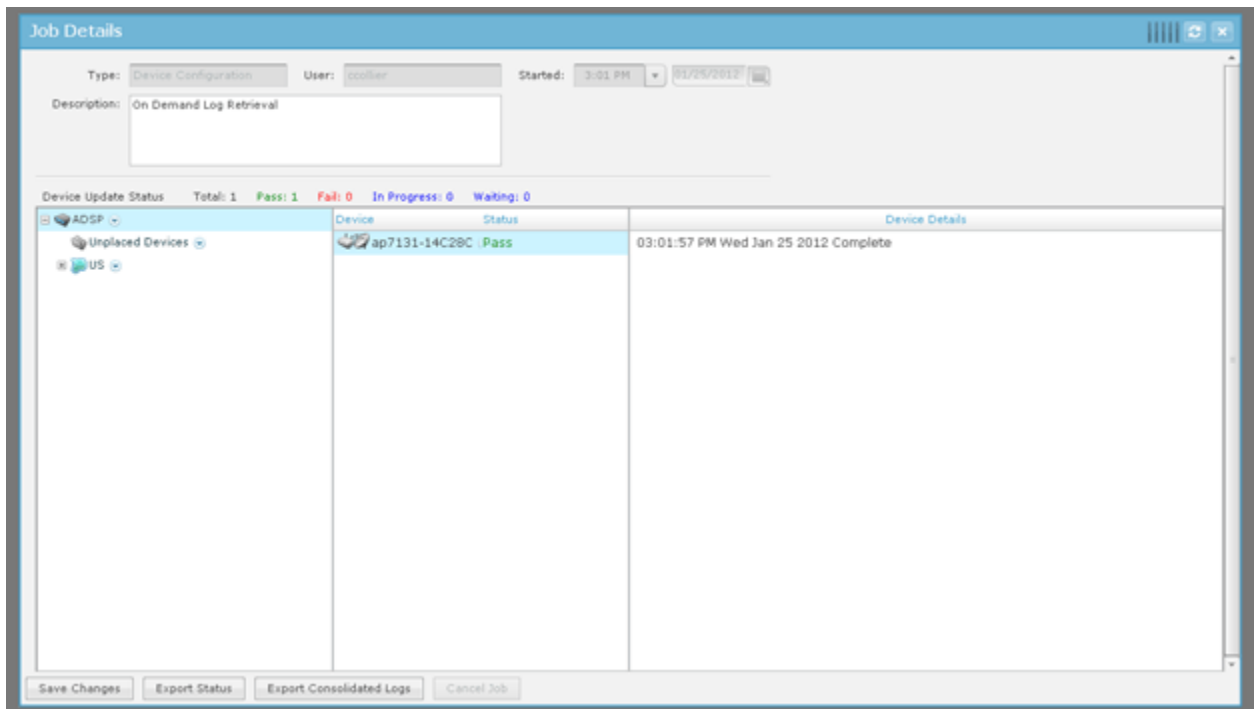
Note

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.



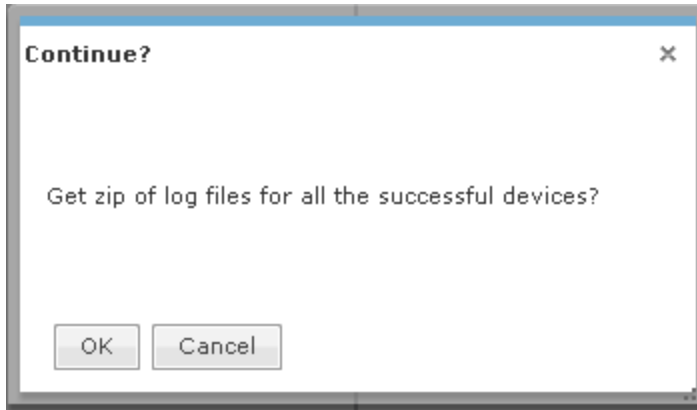
Select your job and then click **View Details** to display the job details.



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.

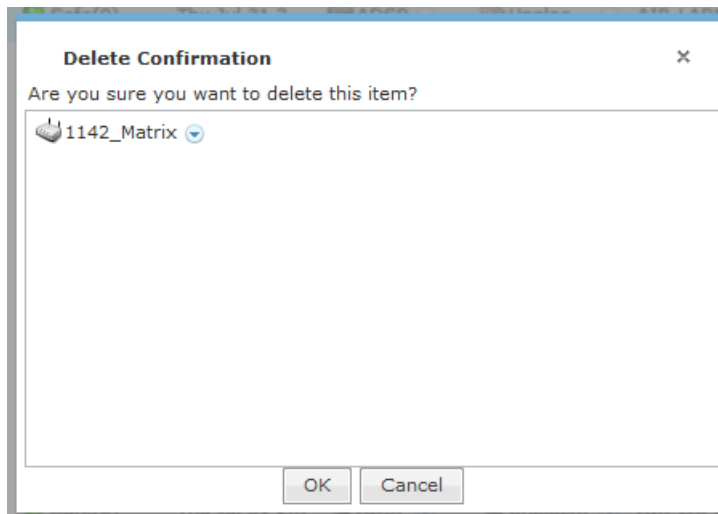


Click **OK** to continue. Navigate to a location and click **Save**. The consolidated logs are saved in a ZIP file using the specified file name. You can now view the logs.

Remove Devices

To remove devices:

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



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

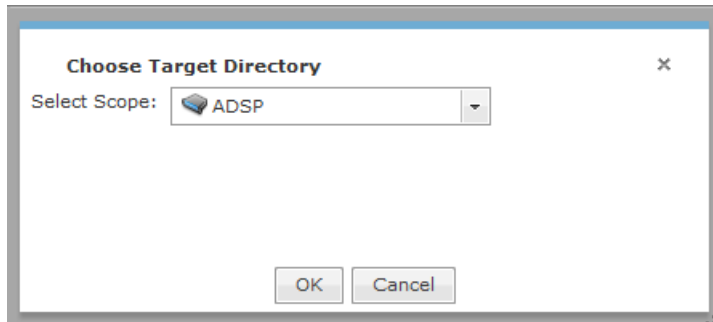
Move Devices

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

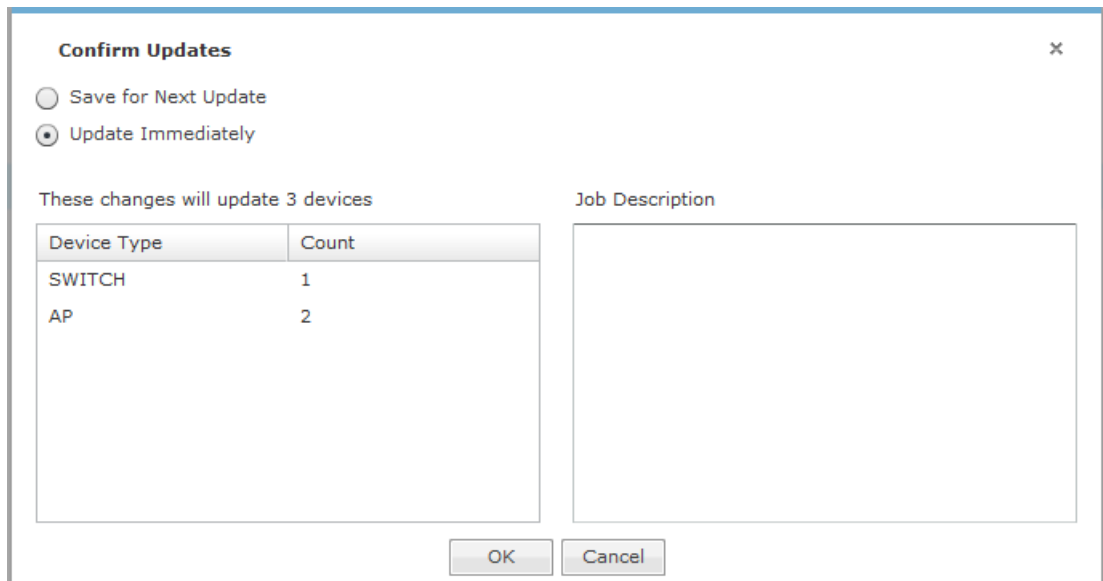
To move a device:

1. Select **Move Devices** action.

The **Choose Target Directory** dialog displays.



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



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

Import CLI Variables



Note

A WLAN Management license is required to import CLI variables.

The Import CLI Variables action is used to import CLI variables at the device level. Naturally, the CLI variable should already exist in the device's profile or it will not be applied.

Comma delimited files are used to import CLI variables. The format of the file is:

```
cli_variables, server, deviceMAC or
folderPath, deviceType, var1, var1_value, var2, var2_value, var3, var3_value,
[etc.]
```

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

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

Examples:

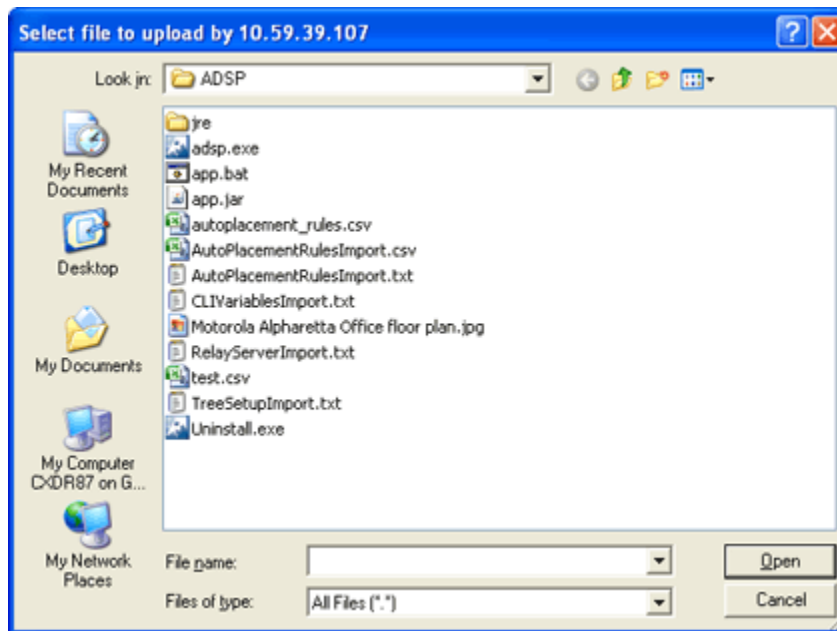
```
cli_variables,localhost,00:00:00:a0:e7:33,ap,MASK,255.255.0.0
cli_variables,localhost,00:00:00:c7:00:39,ap,HOSTNAME,AP7131_Cube44,MASK
,255.255.0.0,GATEWAY,192.10.1.1 cli_variables,localhost,US/Southeast/
Alpharetta/Floor1,,HOSTNAME,AP7131_Cube44
```



Note

deviceType can be blank if designating a folderPath.


When 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.

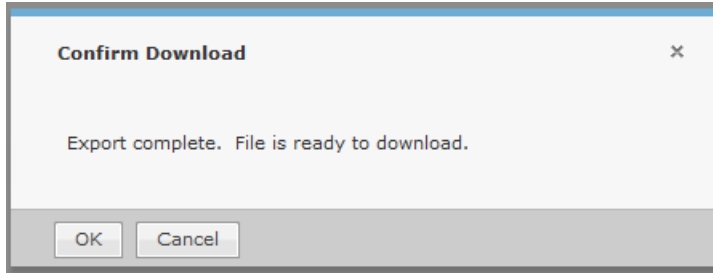
Verify Import of CLI Variables

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 asks you to confirm the download.



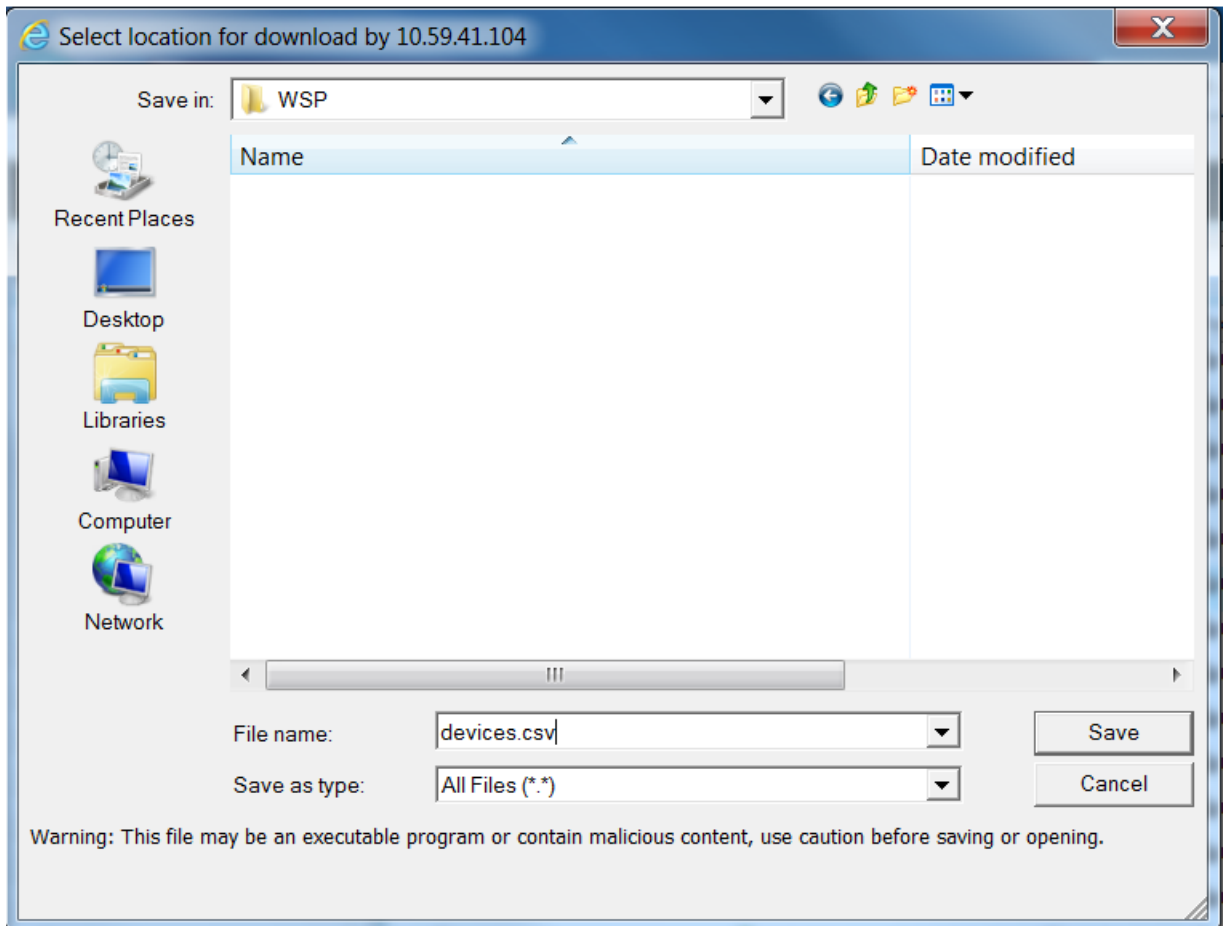
Click **OK** to confirm or click **Cancel** to exit without exporting the device(s).

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 AirDefense.



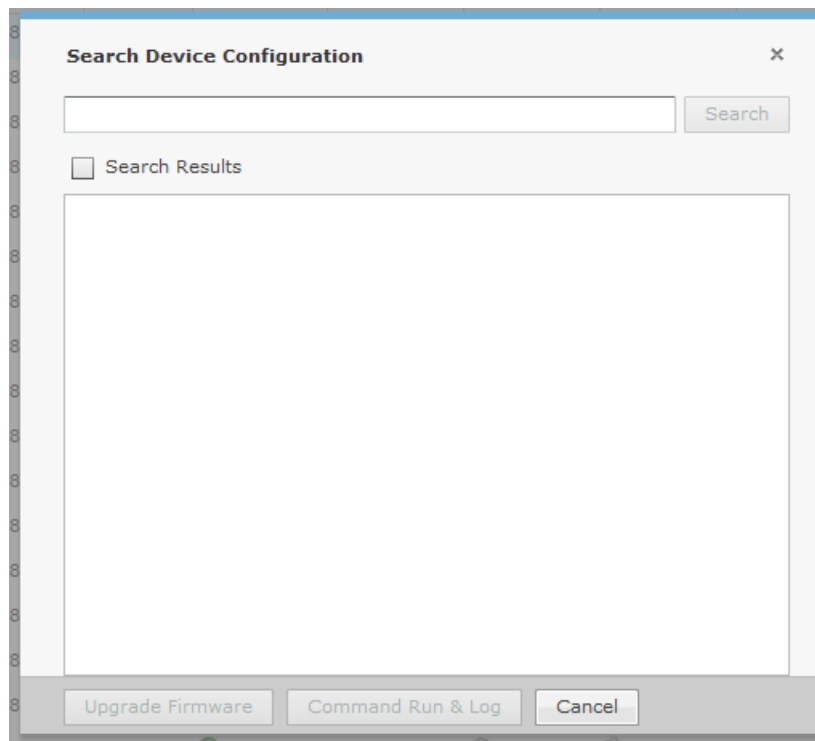
AirDefense names the CSV file devices.csv by default. You can keep that name or change it.

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.

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:

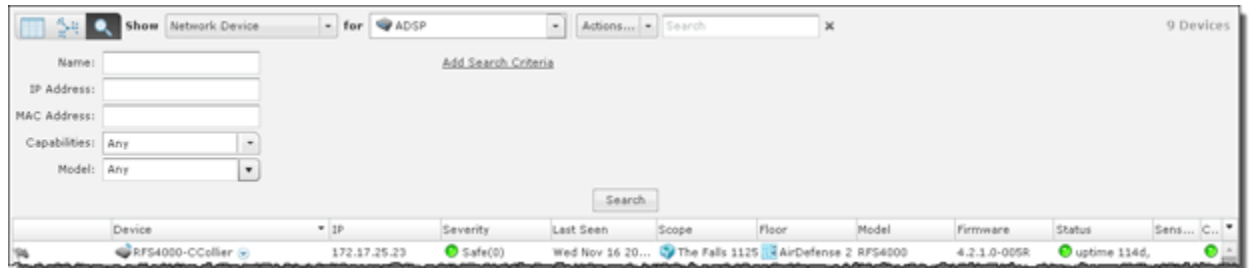
1. Select **Network Device** from the Show menu.
2. Highlight the desired device(s).
3. From the **Actions** menu, select **Search Device Configuration**.



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

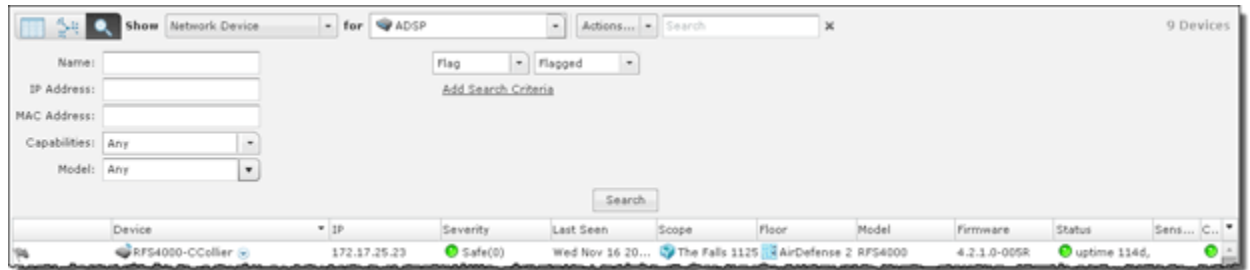
The **Network** tab has an advanced search feature that allows you to supply additional criteria to the basic search. Click the **Advance Search** icon  to access the advanced search feature.



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.

Criteria	Description
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.

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 screenshot shows the 'Alarms' tab in the AirDefense Services Platform. The interface includes a navigation menu (Menu, Dashboard, Network, Alarms, Configuration) and a search bar. The main area displays a table of 1057 alarms. The table has columns for Alarm ID, Alarm Type, Device, Start Time, Status, and SSID. The alarms are sorted by start time, showing a mix of active and inactive states. The left sidebar shows various grouping and filtering options like 'No Grouping', 'Severity', 'Alarm Category', etc.

Alarm ID	Alarm Type	Device	Start Time	Status	SSID
S 2433254...	Rogue AP on Wired Ne...	Motorola:ca:f9:d1	Fri Apr ...	Inactive (expires in 22:08)	Test_100
S 5553530...	Rogue AP on Wired Ne...	Motorola:ca:f9:d0	Fri Apr ...	Inactive (expires in 22:08)	MayerS131
S 5122746...	Rogue AP on Wired Ne...	Motorola:cb:f9:f0	Fri Apr ...	Inactive (expires in 22:08)	MayerS131
S 2828001...	Rogue AP on Wired Ne...	Motorola:cb:f9:f1	Fri Apr ...	Inactive (expires in 22:08)	Test_100
S 3294987...	Rogue AP on Wired Ne...	Motorola:2f:72:e0	Fri Apr ...	Active	MayerS131
S 3984849...	Rogue AP on Wired Ne...	Motorola:2f:72:e1	Fri Apr ...	Active	Test_100
S 9319765...	Rogue AP on Wired Ne...	Motorola:2f:74:20	Fri Apr ...	Active	MayerS131
S 1468755...	Rogue AP on Wired Ne...	Motorola:2f:74:21	Fri Apr ...	Active	Test_100
S 4159659...	Rogue AP on Wired Ne...	Cisco:bfe7:20	Fri Apr ...	Inactive (expires in 19:48)	1140-N
S 3862793...	Rogue AP on Wired Ne...	Symbol:ce:06:51	Fri Apr ...	Inactive (expires in 18:32)	AP300APT-OPEN
S 2349844...	Rogue AP on Wired Ne...	Symbol:27:36:19	Fri Apr ...	Inactive (expires in 13:41)	AP300APT-OPEN
S 2486069...	Rogue AP on Wired Ne...	Symbol:76:0f:50	Thu Apr ...	Active	AP5131-SH
S 2410922...	Rogue AP on Wired Ne...	Motorola:08:05:b2	Thu Apr ...	Inactive (expires in 2:51)	DevHgmt_104
S 1530972...	Rogue AP on Wired Ne...	Motorola:08:05:b3	Thu Apr ...	Inactive (expires in 2:50)	DevHgmt_105
S 2059755...	Rogue AP on Wired Ne...	Motorola:86:44:c2	Thu Apr ...	Inactive (expires in 2:44)	DevHgmt_104
S 1263574...	Rogue AP on Wired Ne...	Motorola:2ca:2:27	Thu Apr ...	Inactive (expires in 2:17)	DevHgmt_108
S 1668760...	Rogue AP on Wired Ne...	Motorola:2ca:2:23	Thu Apr ...	Inactive (expires in 2:12)	DevHgmt_105
S 2926010...	Rogue AP on Wired Ne...	Motorola:2ca:2:22	Thu Apr ...	Inactive (expires in 2:10)	DevHgmt_104
S 1314810...	Rogue AP on Wired Ne...	Motorola:2ca:2:25	Thu Apr ...	Inactive (expires in 2:20)	DevHgmt_106
S 2211873...	Rogue AP on Wired Ne...	Motorola:2ca:2:24	Thu Apr ...	Inactive (expires in 2:19)	DevHgmt_105
S 2676730...	Rogue AP on Wired Ne...	Motorola:2ca:2:26	Thu Apr ...	Inactive (expires in 2:16)	DevHgmt_107

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](#) on page 482 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 .



Alarm Table

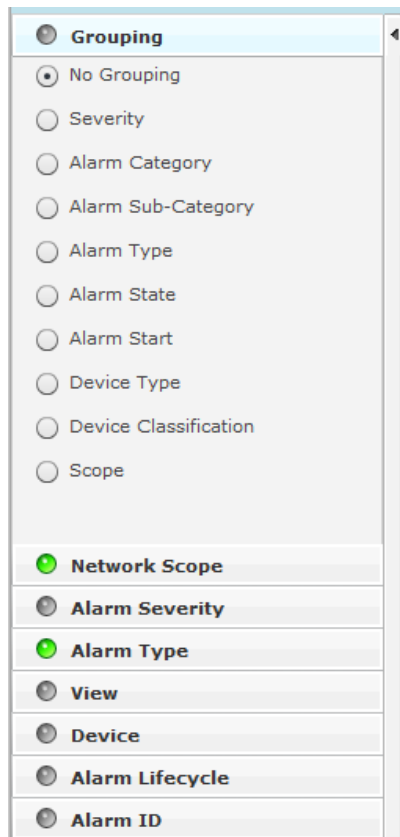
The alarm table is customizable and includes the following information (columns):


Column	Description
Flag	Indicates whether or not a alarm has been flagged.
Criticality	Displays the criticality of the alarm. (See Alarm Criticality on page 490 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.

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

Alarm Filters

The alarm filters are used to filter the displayed alarm information. The filters are displayed on the left side of the window.



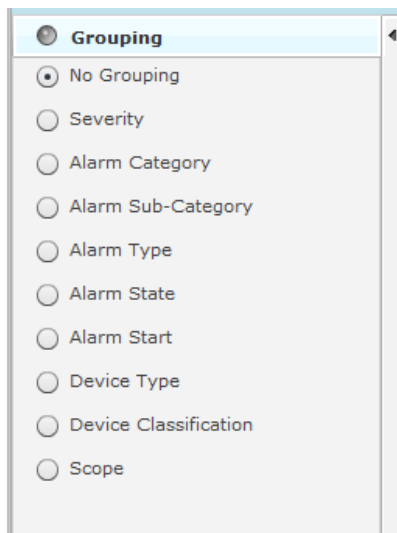
The indicator on the right of each filter turns green  when you change a filter from its original state. Click the green indicator to return a filter to its default state.

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.

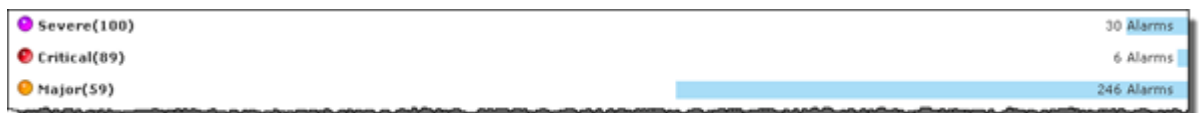
Grouping Filter

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.



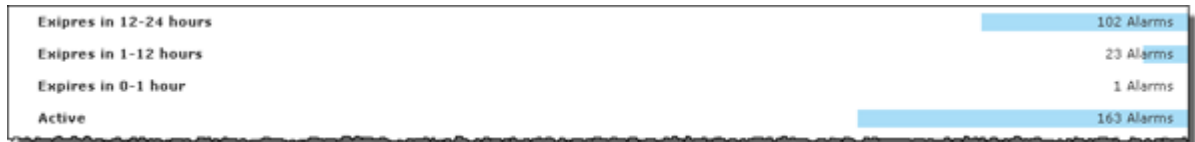
- Alarms Sub-Category Groups alarms into alarm sub-categories.



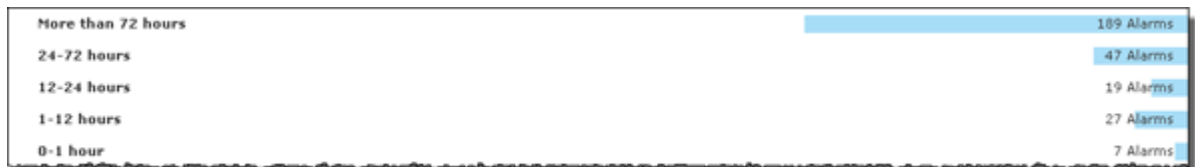
- Alarm TypeGroups alarms by alarm type.



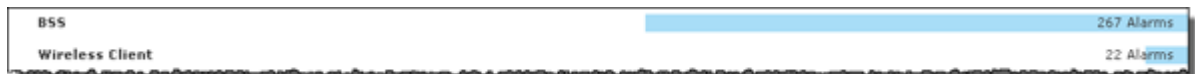
- Alarm StateGroups alarms by the state of the alarms.



- Alarm StartGroups alarms by when they started.



- Device TypeGroups alarms by the device type.



- Device ClassificationGroups alarms based on the device classification.



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

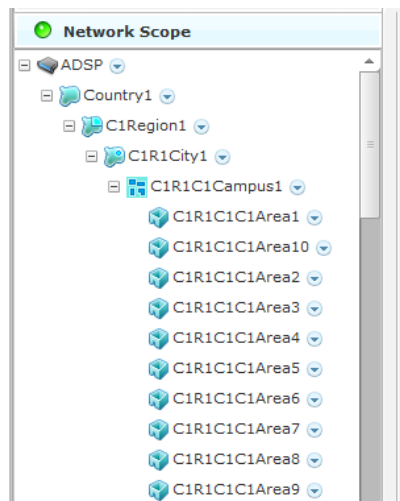


Clicking on a group will display the individual alarms in that group.

Severe(100)		34 Alarms	
Critical(89)		6 Alarms	
Critical Wireless Client Accide...	SolomonExtreme:1a:13:37	10:33:00 AM ...	Inquire (expires at 0:13)
Cr Level: Critical Score: 89	hed #55 Using ...	Cisco:d4:2b:50	09:40:00 AM ... Active Doc-Net
Critical Sanctioned #55 Using ...	Cisco:d0:2b:80	09:40:00 AM ... Active	Doc-Net
Critical Sanctioned #55 Using ...	Motorola:2e:92:90	10:00:00 AM ... Active	Doc-Net
Critical Sanctioned #55 Using ...	Motorola:2e:9a:e0	10:00:00 AM ... Active	Doc-Net
Critical Sanctioned #55 Using ...	Symbolic:519f:43	10:04:00 AM ... Active	Doc Not
Major(59)		249 Alarms	

Network Scope Filter

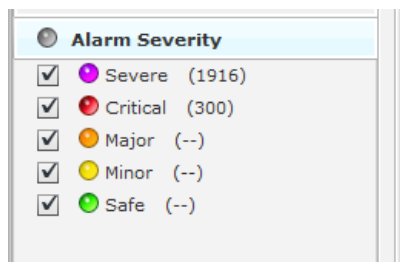
The **Network Scope** filter is used to view alarms according to where they are in the network tree. By selecting a network level, you limit the displayed alarms to only the ones under that particular network level.



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:

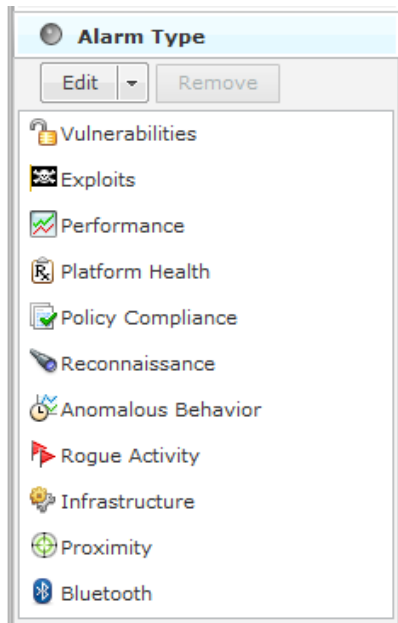
- Severe - - Displays only Severe alarms.
- Critical - - Displays Critical and Severe alarms.
- Major - - Displays Major, Critical, and Severe alarms.

- 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

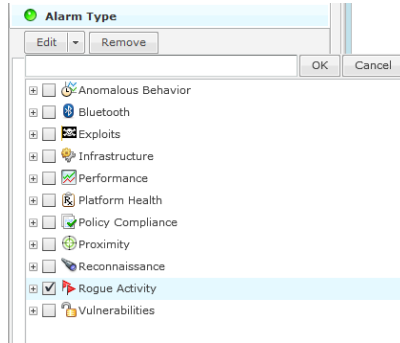
The **Alarm Type** filter allows you to view devices by alarm type.



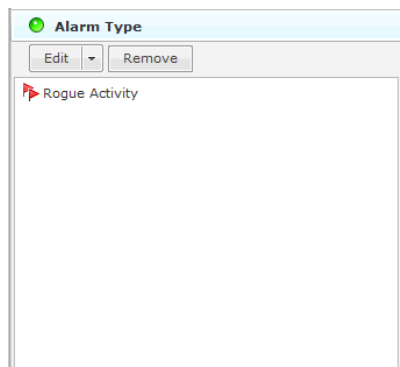
You also have the option of displaying all alarm types or you may filter alarms by a specific type. The different alarm types are:

- 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.



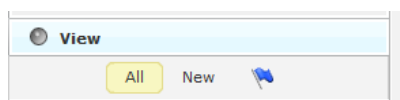
Click the **Edit** button, select the alarm type(s), and then click **OK**. The following screen shots shows that you only want to display rogue alarms.




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

View Filter

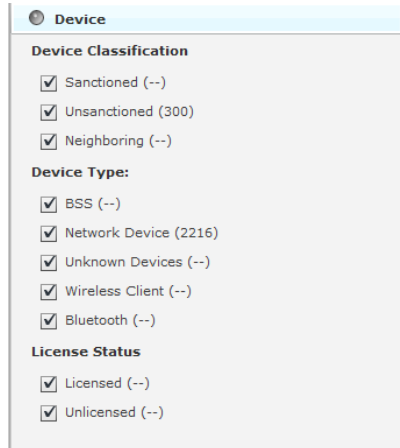
The **View** filter gives you the option of viewing all alarms, new alarms, or flagged alarms.



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.



Device

Device Classification

- Sanctioned (--)
- Unsanctioned (300)
- Neighboring (--)

Device Type:

- BSS (--)
- Network Device (2216)
- Unknown Devices (--)
- Wireless Client (--)
- Bluetooth (--)

License Status

- Licensed (--)
- Unlicensed (--)

Alarms can be displayed by the following device classifications:

- SanctionedDisplay alarms for sanctioned devices. You may also choose to display any sanctioned device, inherited sanctioned devices, or overridden sanctioned devices.
- UnsanctionedDisplay alarms for unsanctioned devices.
- NeighboringDisplay 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 **Alarm Lifecycle** filter to filter alarms over a specified range of time.

Alarm Lifecycle

Alarm State

- Active (85)
- Expires in 0-1 hour (232)
- Expires in 1-12 hours (339)
- Expires in 12-24 hours (1189)
- Expires in 24-72 hours (--)
- Expires in more than 72 hours (--)

Alarm started within prior

- 0-1 hour (5)
- 1-12 hours (850)
- 12-24 hours (377)
- 24-72 hours (612)
- More than 72 hours (1)

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

Use the **Alarm ID** to filter alarms using the alarm ID.

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, AirDefense groups alarms into nine categories, and assigns a criticality to each alarm. Alarm notifications can also be delivered to the administrator via Email, SNMP, or Syslog.

Alarm Categories






The nine alarm categories are as follows:

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

Alarm Criticality

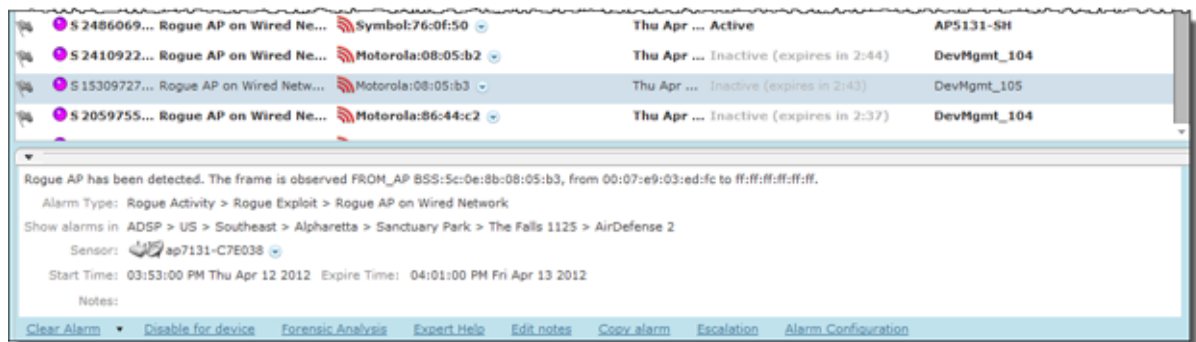
Alarms are assigned a default criticality by ADSP. You can optionally change the default criticality of each alarm to match your environment when configuring alarms under **Configuration > Operational Management > Alarm Configuration**. You must be a user

with read/write permission for the Alarm Management functional area to change the criticality of an alarm.

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

Alarm Details

Additional alarm information can be displayed by selecting an alarm. Information about the alarm is displayed at the bottom of the **Alarms** tab.



If you do not see the alarm details, click the **Open** bar to display them.



The following alarm information is displayed:

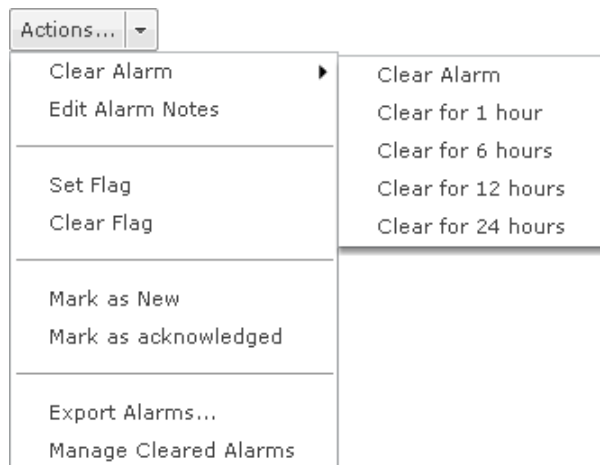
- A description of the alarm
- The alarm type
- The network level of the device
- The Sensor that observed the device
- The time when the alarm started
- The time when the alarm will expire
- Any notes added by a user.

At the bottom of the detailed information are links that allow you to execute a function or provide more information.

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

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

AirDefense 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 AirDefense 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, AirDefense 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.

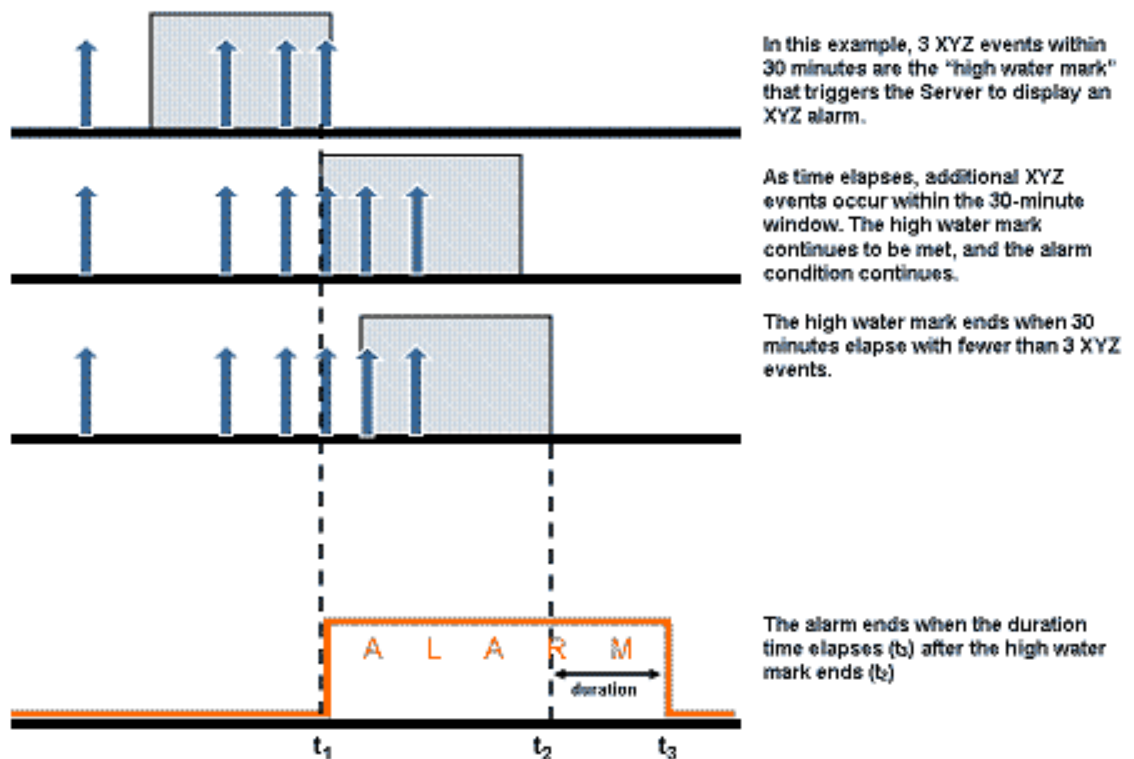
How an Alarm is Generated

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

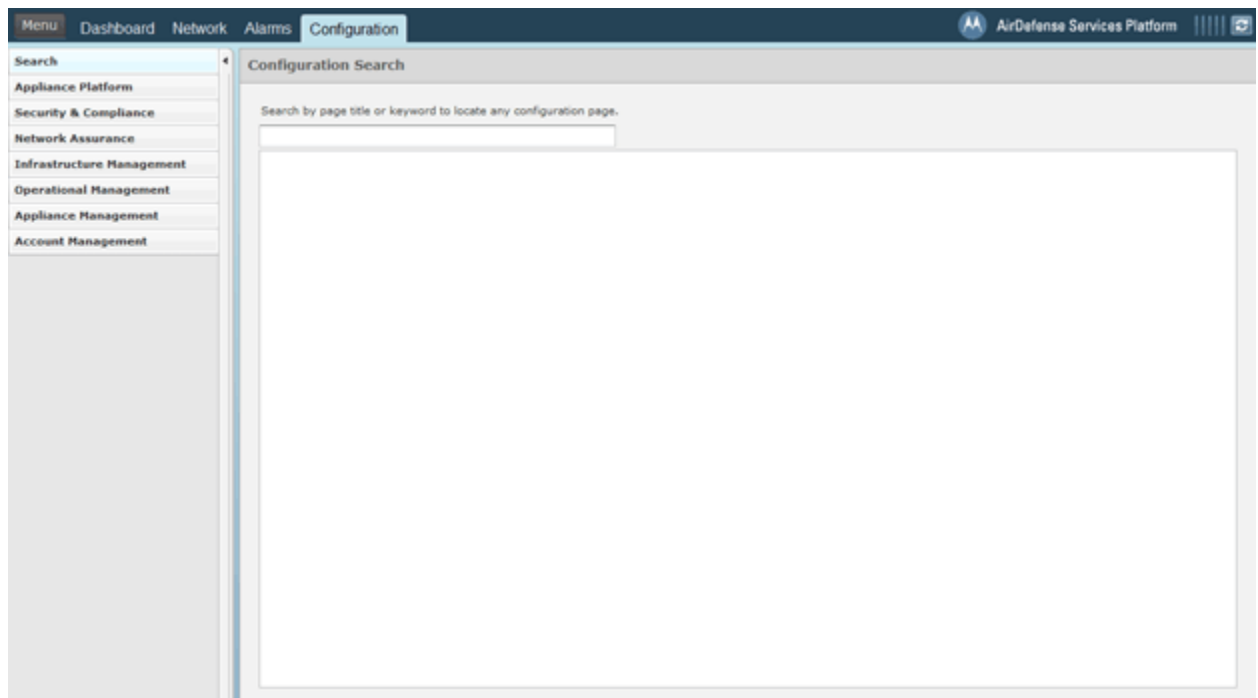
event. When the duration time ends, the alarm becomes inactive. You can use the forensic analysis to view historical alarms.

Configuration Tab

The **Configuration** tab allows you to initially set up AirDefense, configure devices for management, and perform other administrative tasks such as user and sensor administration. Once you configure your network with AirDefense, you can administer and monitor your network from one central location.

The following configuration categories allow you fully set up and manage AirDefense:

- Appliance Platform is used to initially set up AirDefense.
- 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 AirDefense.
- Operational Management is used to configure features that apply to the normal operations of AirDefense.
- Appliance Management is used to configure the AirDefense appliance.
- Account Management is used to set up user account parameters, including access, authentication and passwords.

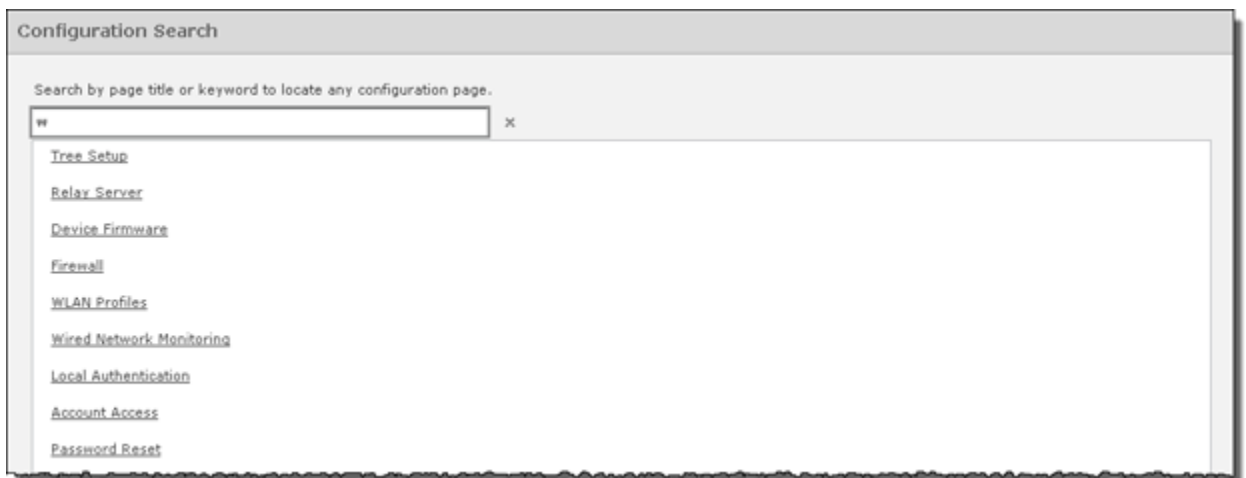


Search

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



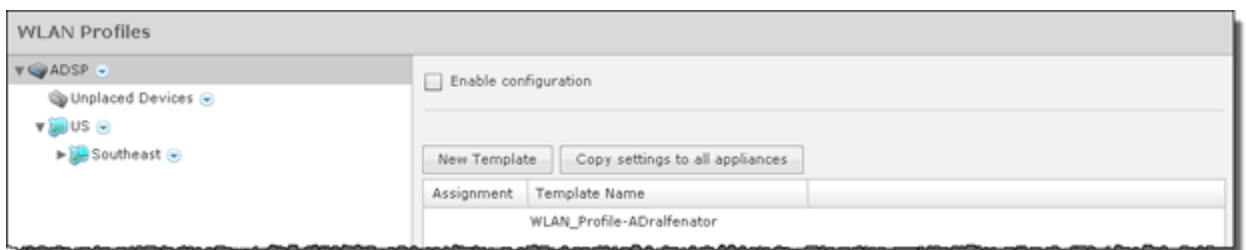
To conduct a search, just start typing.



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 AirDefense.

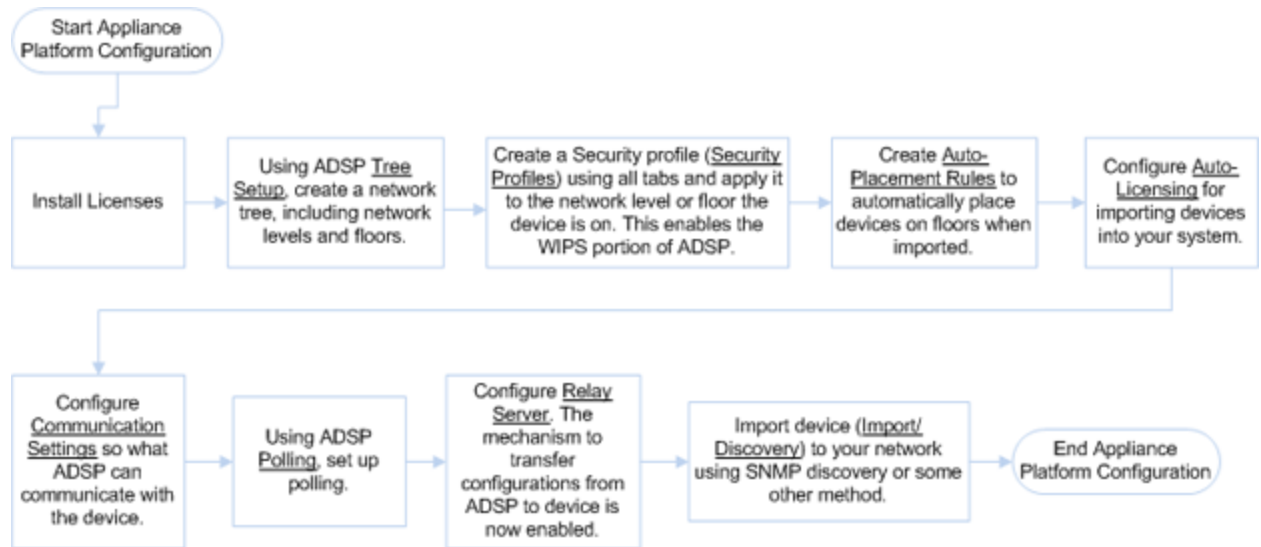
Search
Appliance Platform
01. Appliance Licensing
02. Tree Setup
03. Security Profiles
04. Auto-Placement Rules
05. Auto-Licensing
06. Communication Settings
07. Polling
08. Relay Server
09. Import / Discover Devices
Security & Compliance
Network Assurance
Infrastructure Management
Operational Management
Appliance Management
Account Management

The Appliance Platform category allows you to:

- Appliance Licensing - License your appliance and devices.
- Tree Setup - Establish a network tree.
- Security Profiles - Create security profiles that will initiate WIPS.
- Auto-Placement Rules - Define Auto-Placement rules that will automatically place devices in your network tree.
- Auto-Licensing - Establish an import policy that controls how device licenses are applied during the import process.
- Communication Settings - Set up communication profiles that allow AirDefense to communicate with devices in your network.
- Polling - Determine how often AirDefense polls your devices for status information and sets the frequency.
- Relay Server - Set up a relay server that facilitates downloading/uploading configuration profiles to/from your devices. (Optional.)
- 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 AirDefense, follow the numbered steps sequentially. Once you have completed the last step, AirDefense is set up for use.

The following flowchart shows the fundamental steps to initially configure AirDefense.



Appliance Licensing

The AirDefense GUI handles license management for AirDefense 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

The screenshot shows the 'Appliance Licensing' window. At the top, there's a 'Licenses for' dropdown menu currently set to 'ADSP'. To its right are three buttons: 'Add Licenses', 'Appliance ID', and 'Appliance Keys'. Below this is a list of licenses, each with a green checkmark icon. The licenses are grouped into categories: 'Advanced Forensics', 'Advanced Troubleshooting', and 'WIPs'. Each license entry shows the license name, the number of licenses remaining, and the number of licenses in use. For example, 'Advanced Forensics' shows 'Unlimited licenses remaining / 5 in use'. To the right of each license entry is a link labeled 'License Assignments'. The 'Radio Share AP Test' license is highlighted in blue.

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

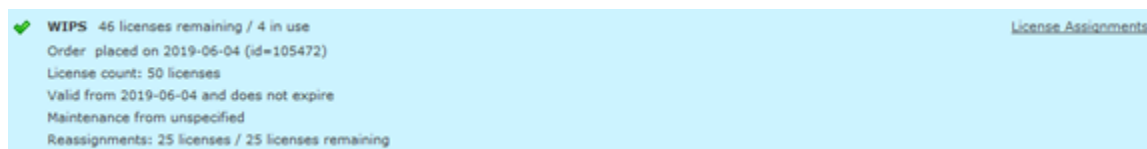
- Radio Share Network Assurance License, which includes:
 - Radio Share AP Test (available as a separate license)
 - Radio Share Advanced Forensics (available as a separate license)
 - Radio Share Connection Troubleshooting (available as a separate license)
 - Radio Share Spectrum Analysis (available 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.



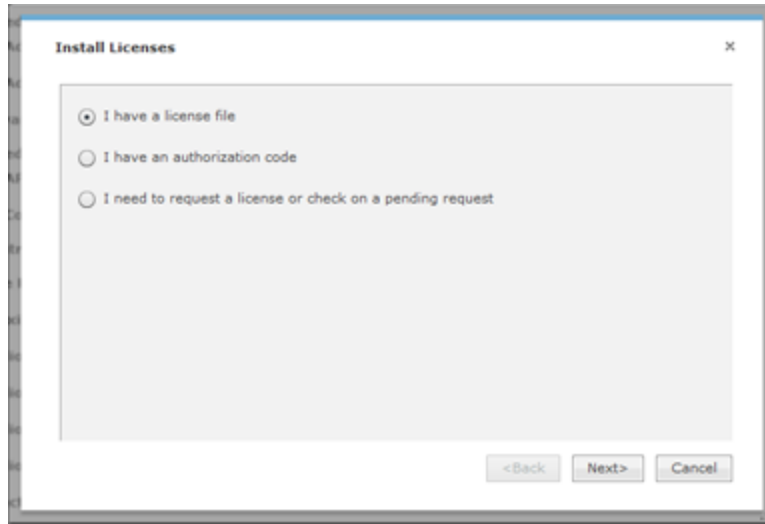
 **WIPS** 46 licenses remaining / 4 in use [License Assignments](#)
 Order placed on 2019-06-04 (id=105472)
 License count: 50 licenses
 Valid from 2019-06-04 and does not expire
 Maintenance from unspecified
 Reassignments: 25 licenses / 25 licenses remaining

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

Field	Description
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

To install a license, click the **Add Licenses** button to begin.

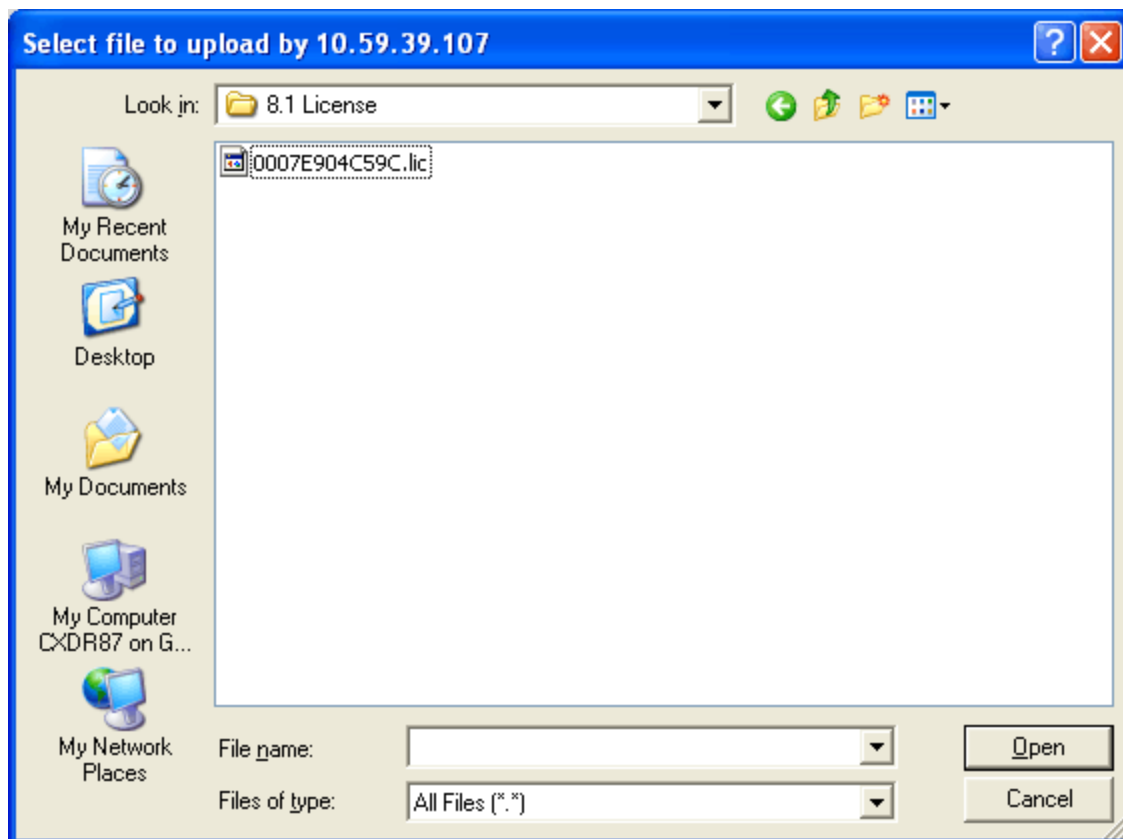


There are three ways to install a license:

- [Using a License File](#) on page 501
- [Using an Authorization Code](#) on page 502
- [Requesting a License](#) on page 504

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**.

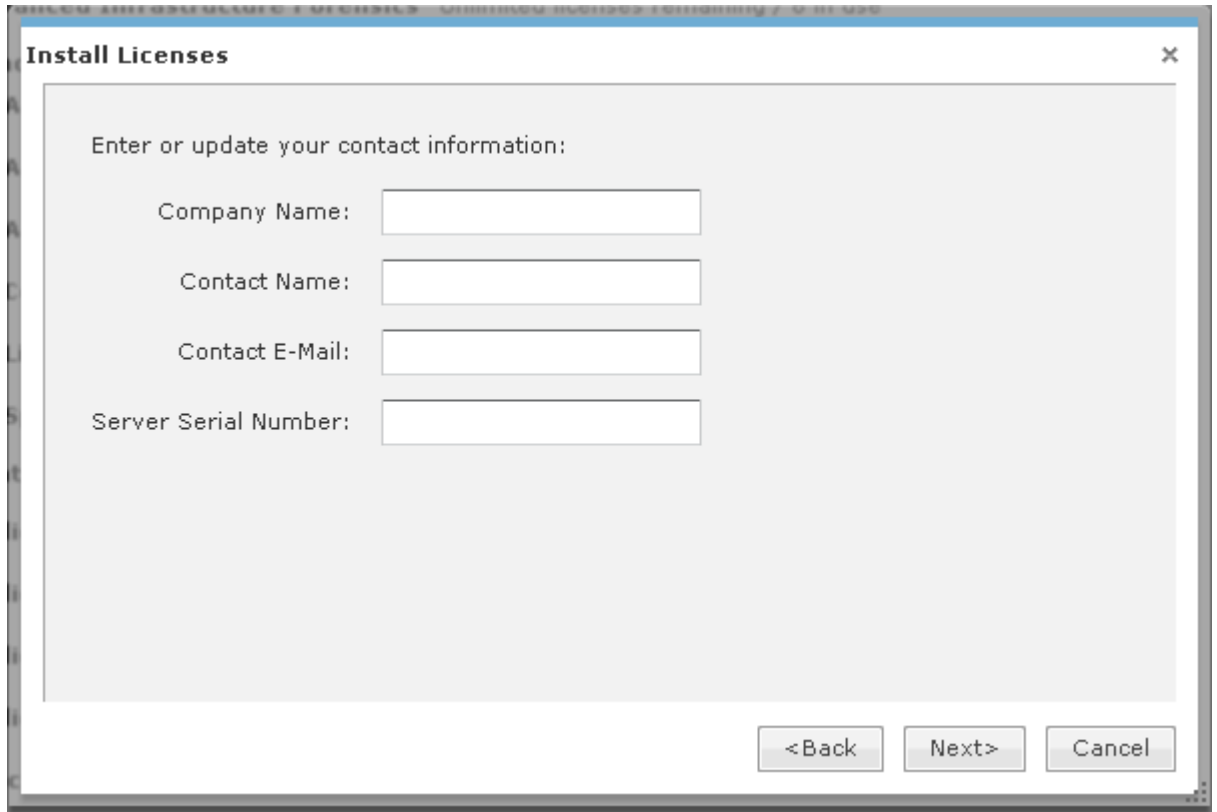


Navigate to the file and select it. Once you have selected the licensing file, click **Open**. The license information is updated.

Using an Authorization Code

To add licenses using authorization codes:

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



Install Licenses [X]

Enter or update your contact information:

Company Name:

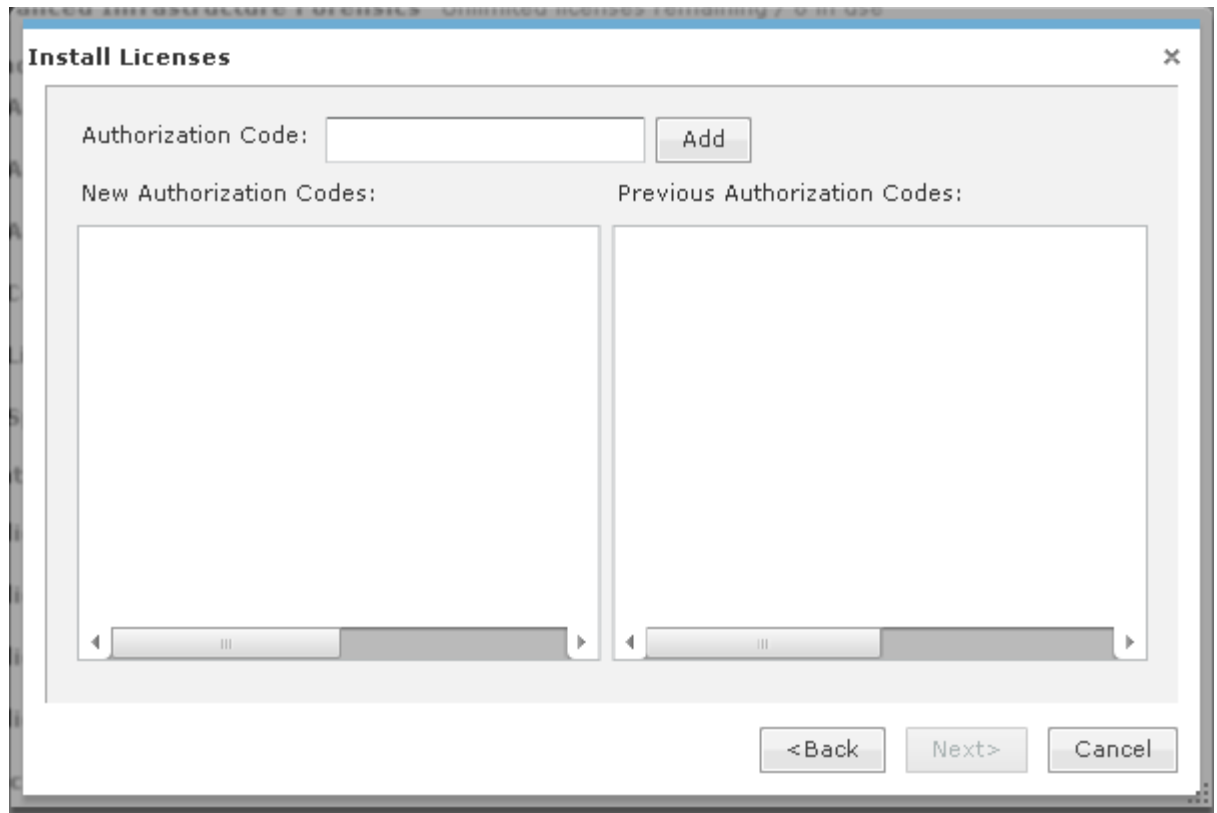
Contact Name:

Contact E-Mail:

Server Serial Number:

<Back Next> Cancel

2. Enter your company name, contact name, email address, and server serial number. Click **Next**.



3. 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.

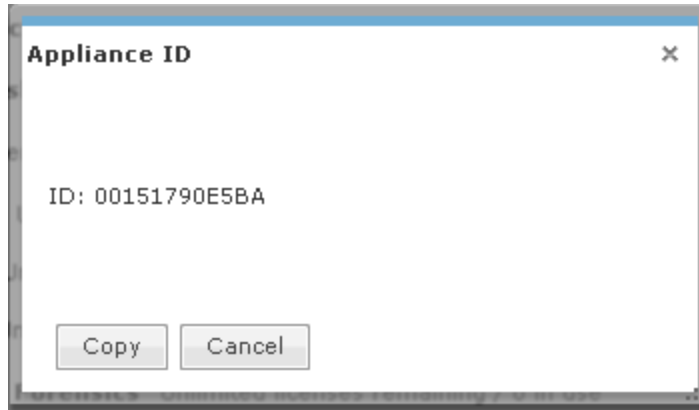
After installation, the following message is displayed:

Licenses installed successfully.

4. If there are no pending request, follow the prompts to request a license.

Copy Appliance ID

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

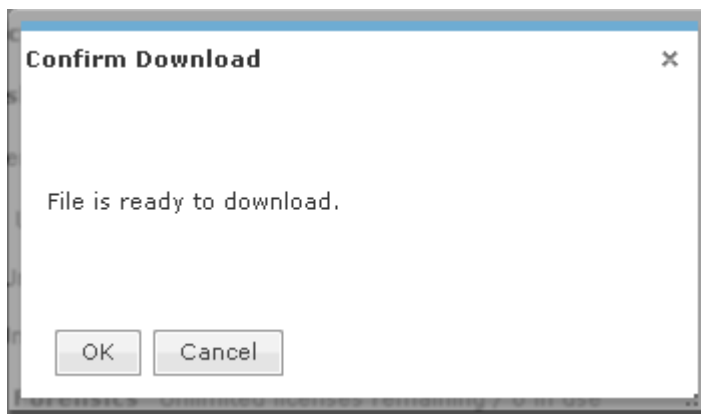


Once the ID is displayed, click the Copy button to copy the ID.

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.

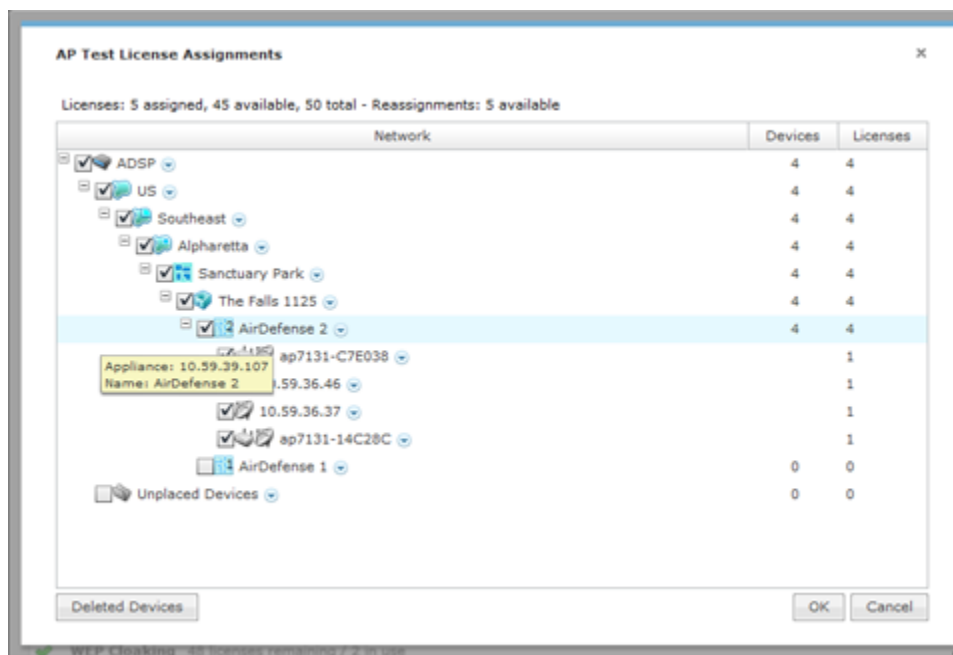


Note

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 displayed:

- 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 select it.
5. Click the **OK** button. The fixed license is assigned to the device.

Open tree levels until all the devices that you want to assign a license to are displayed. Then, select the checkbox for each device to assign a license to each of these devices.

Tree Setup

Use the Tree Setup feature to configure your network tree.



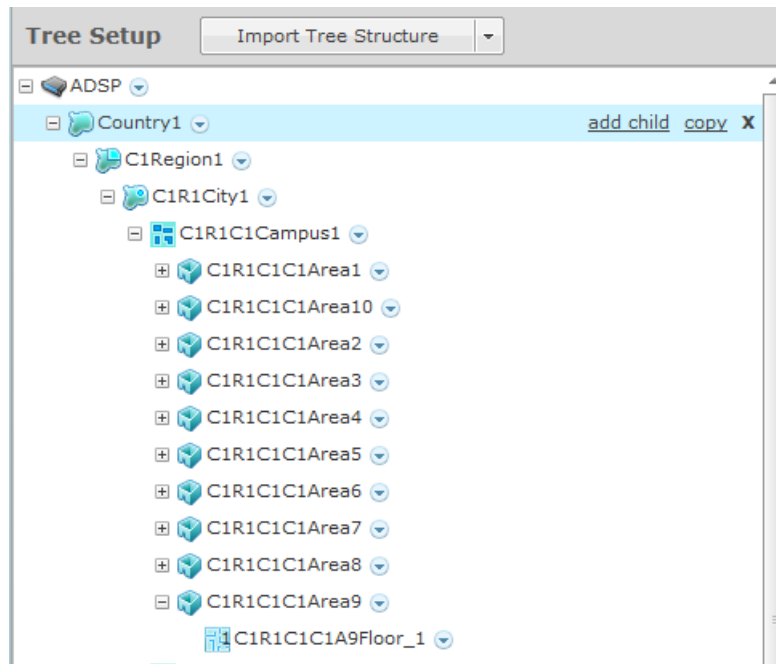
Note

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

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 AirDefense 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 (AirDefense) 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 AirDefense 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

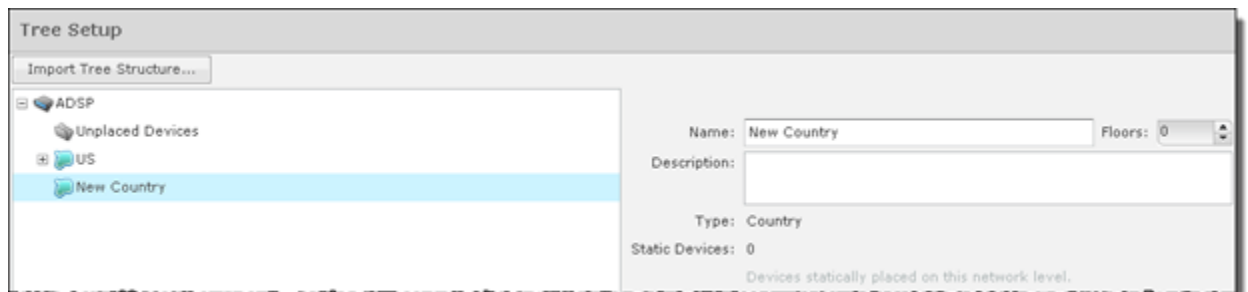
If the parent of the new level already contain sensors, you cannot add a new level to it.

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.

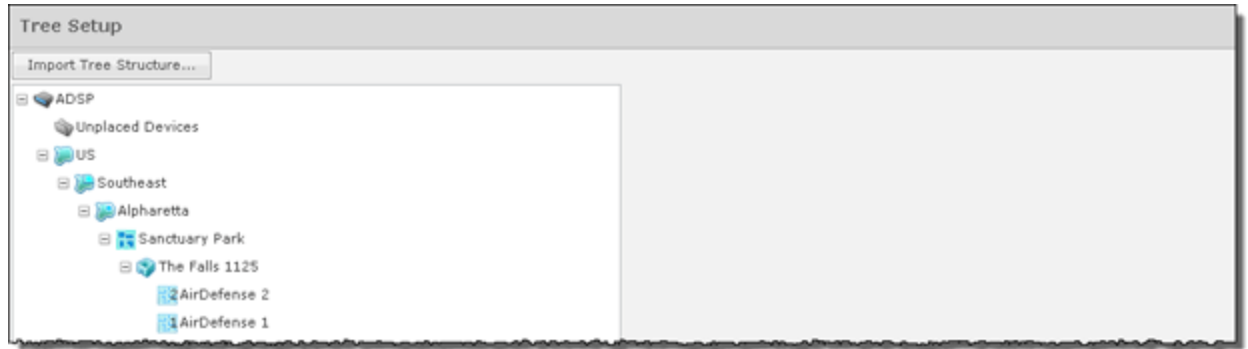


Note

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 it contains static devices. Also, if the network level is the last level for an appliance, it may not be deleted.

Add Floors

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

Name: Floors:

Description:

Type: Building

Static Devices: 7

Devices statically placed on this network level.



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 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/Floor3,delete
```



Note

The add command is assumed when neither add or delete is used in a comma delimited file, and add is included in the default exportable CSV file.

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

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

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

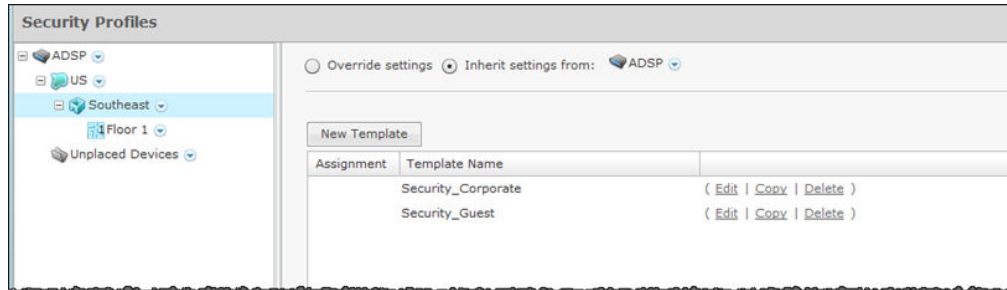
Security Profiles

Security profiles 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.

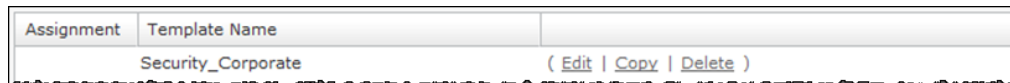
View Security Profiles

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.

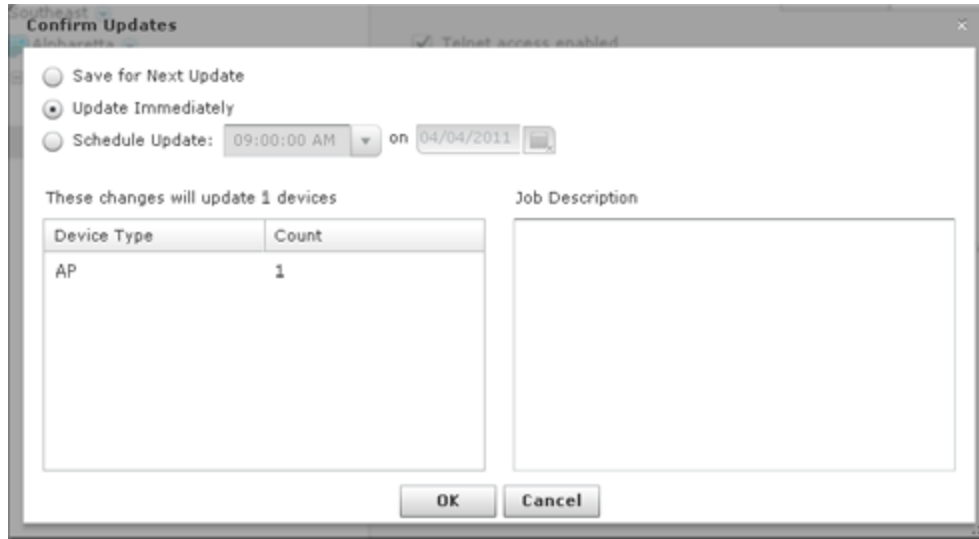
Click the **Copy settings to all appliances** button to copy the defined Security Profiles and all profile assignments to all appliances in your system.



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.

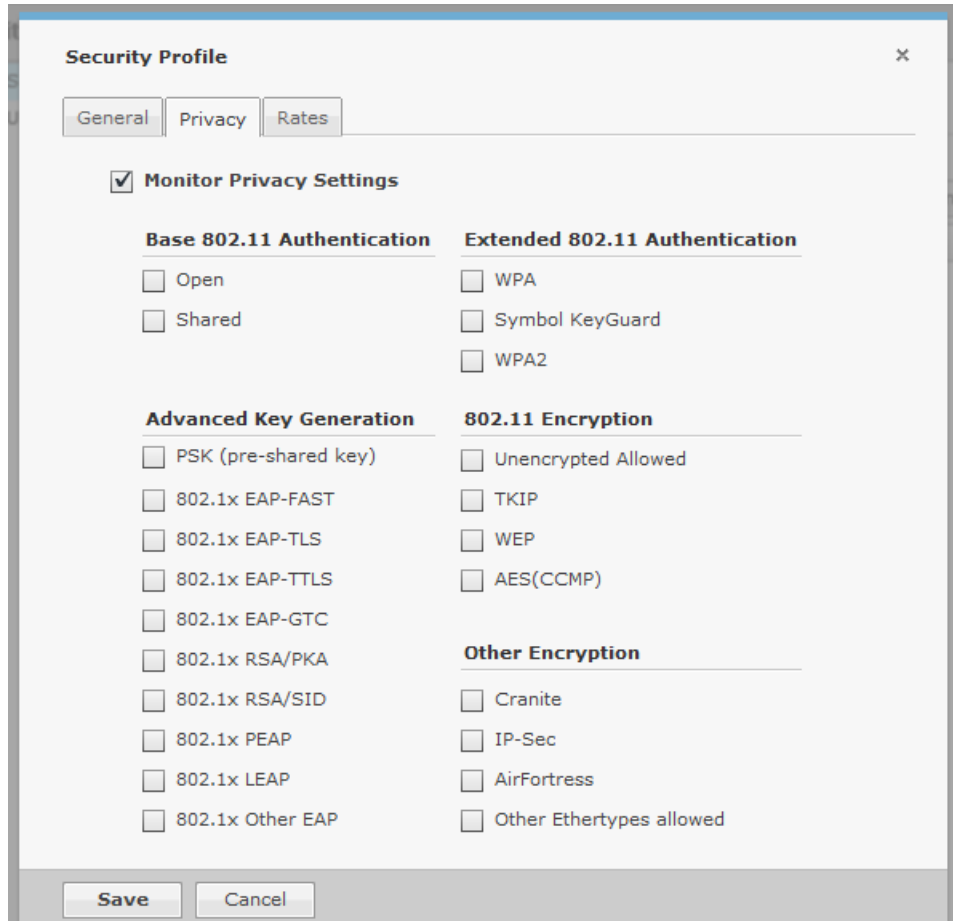
The **Name** field specifies the profile name. If you are adding or copying a Security Profile, ADSP gives the profile a default name beginning with `New_Security_Profile` and ending with a system generated number. You should change the default name to one that is more appropriate to its function. Once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



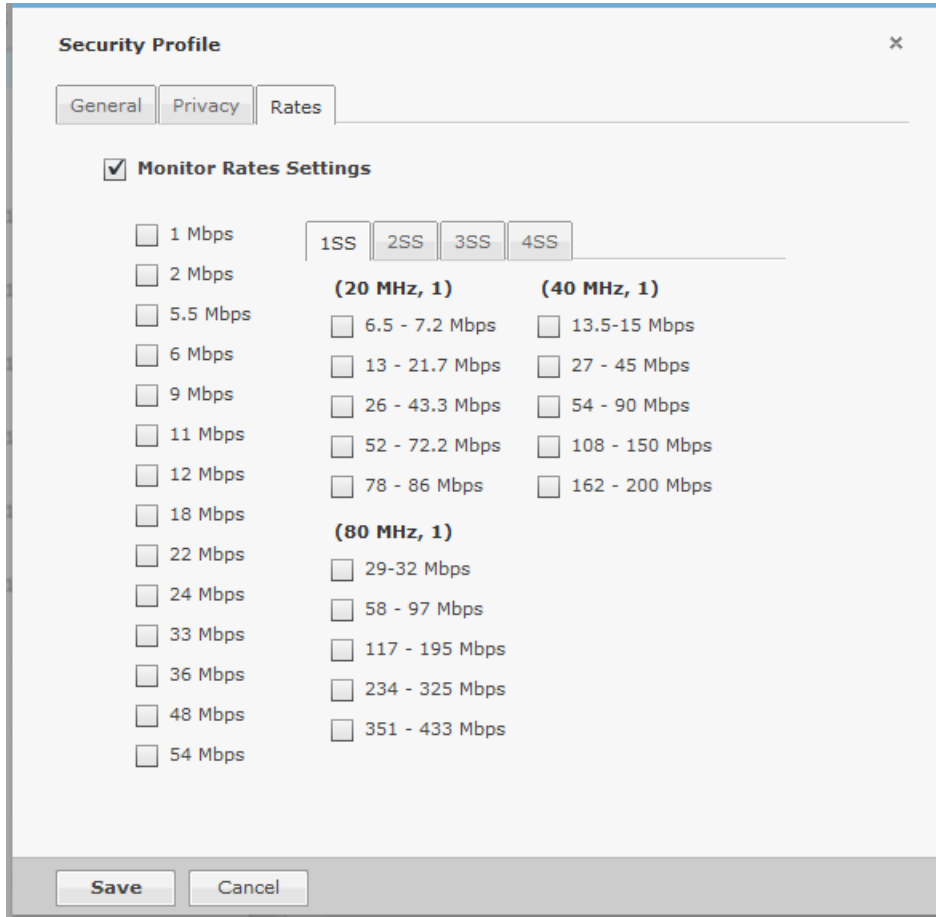
You must check the **Monitor Privacy Settings** checkbox to activate the functions. The functions are:

Function	Description
Base 802.11 Authentication	<p>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).</p> <p>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.</p>
Extended 802.11 Authentication	<p>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.</p> <p>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.</p> <p>Symbol KeyGuard - When this checkbox is selected, it activates Symbol KeyGuard authentication protocols, which is provided by Symbol.</p>

Function	Description
Advanced Key Generation	<p>PSK (preshared key) - When selected, it activates the Pre-shared Key authentication.</p> <p>802.1x EAP-FAST - When selected, it keys 802.1X EAP Flexible Authentication via Secure Tunneling.</p> <p>802.1x EAP-TLS - When selected, it keys EAP Transport Level Security.</p> <p>802.1x EAP-TTLS - When selected, it keys EAP Tunneled Transport Layer Security.</p> <p>802.1x EAP-GTC - When selected, it keys EAP Generic Token Card.</p> <p>802.1x RSA/PKA - When selected, it keys EAP RSA Public Key Authentication Protocol.</p> <p>802.1x RSA/SID - When selected, it keys EAP RSA SecurID.</p> <p>802.1x PEAP - When selected, it keys any 802.1X Protected Extensible Authentication Protocol (PEAP).</p> <p>802.1x LEAP - When selected, it keys EAP Lightweight Extensible Authentication Protocol.</p> <p>802.1x Other EAP - Keys any 802.1x EAP authentication/key distribution mechanism other than the types previously mentioned.</p>
802.11 Encryption	<p>Unencrypted Allowed - Select this checkbox to allow no 802.11 encryption for wireless traffic.</p> <p>TKIP - When selected, this enables the BSS to advertise support for Temporal Key Integrity Protocol (TKIP).</p> <p>WEP - When selected, causes the BSS and Wireless Client to use WEP as their encryption policy.</p> <p>AES (CCMP) - When selected, causes the BSS to advertise support for Advanced Encryption Standard (AES-CCMP).</p>
Other Encryption	<p>Cranite - When selected, enables AP usage of Layer 3 Cranite encryption.</p> <p>AirFortress - When selected enables AP usage of Layer 3 Airfortress encryption.</p> <p>IP-Sec - When selected, enables AP usage of Layer 3 IP security protocol as encryption.</p> <p>Other Ethertypes allowed - When selected, enables AP usage of other Layer 3 encryption mechanism which is not specified here.</p>

Rates Tab

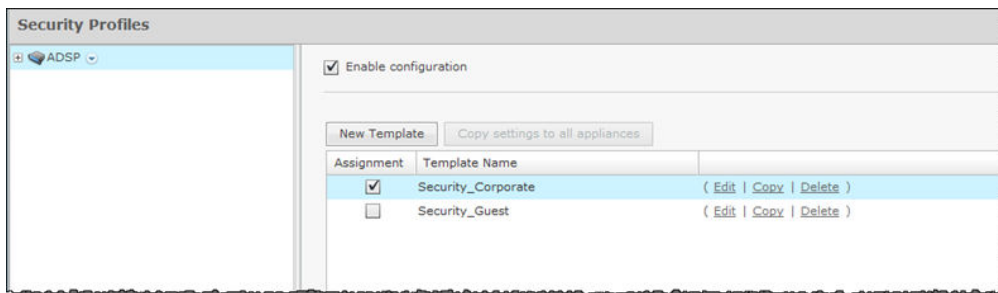
The **Rates** tab is where you can select transmit and receive data rates for BSSs to use.



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

Apply a Security Profile

Once you have defined and added a Security Profile, you must apply it to your system

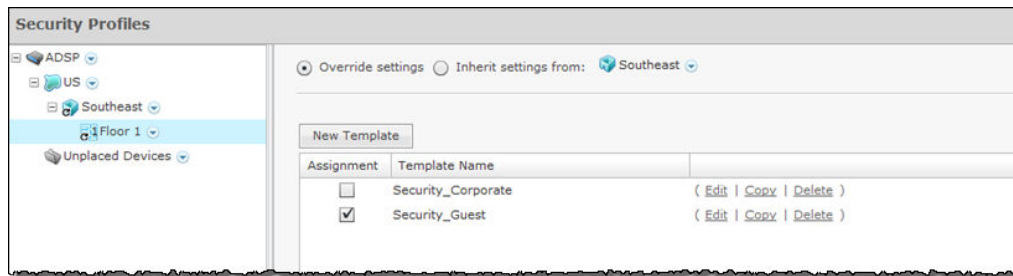


Note


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 AirDefense is the `Security_Corporate` profile. Then, for a special case, you can override the Security Profile at the AirDefense 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](#) on page 519
- [APs and Switches](#) on page 519

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 AirDefense.
 - The first IP address on the list is the Devices Management IP Address. This is the IP address that AirDefense 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 AirDefense 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 AirDefense for this purpose and is not saved by AirDefense. It is not used as a configured or managed IP address for the device, and it will not be displayed by AirDefense.
 - 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 AirDefense to communicate with the switch. It may NOT be the switch's configured IP address.

Auto-Placement Rules

Auto-placement rules determine where devices will be placed in the network tree when they are imported.

Rules for localhost

Sequence	Destination Folder
1	The Falls 1125 > AirDefense 2
2	The Falls 1125 > AirDefense 2
3	The Falls 1125 > AirDefense 1
4	The Falls 1125 > AirDefense 2
5	The Falls 1125 > AirDefense 2
6	The Falls 1125 > AirDefense 1
7	The Falls 1125 > AirDefense 2
8	The Falls 1125 > AirDefense 1

Place in Folder: localhost

Device Selection Rules:

Parameter	Value



Note

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

Add Auto-Placement Rules

Follow these steps to add a new auto-placement rule:

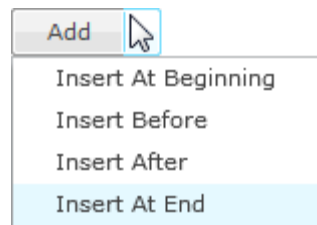
1. Click the **Add** button.

The new rule is added to the list of rules and is automatically selected (highlighted) in the **ADD** drop-down menu.



Note

You may optionally choose where you want the new rule to be placed by selecting a placement item from the drop-down menu. (Inset At End is the default.)



2. Using the **Place devices in scope** drop-down menu, select a scope to place devices when rule is applied.
3. Select one or more of the **Device Selection Rules**, and specify a value for each rule using the following criteria:

Field	Description
Network Address	The device's network address.
IP Range	A range of IP addresses that the device(s) must fall within.
MAC Address	A range of MAC addresses that the device(s) must fall within.
DNS Server	The DNS server that the device(s) are using. This parameter only works with sensors not 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.

- 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 (For Example `1.1.1.1-1.1.1.1`).

Example:

```
autoplacement_rule,localhost,/USA/AutoPlacementTest/
Floor1,,172.17.17.0-172.17.17.19,,,,,,6.0.196.0
autoplacement_rule,localhost,/USA/AutoPlacementTest/
Floor6,,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

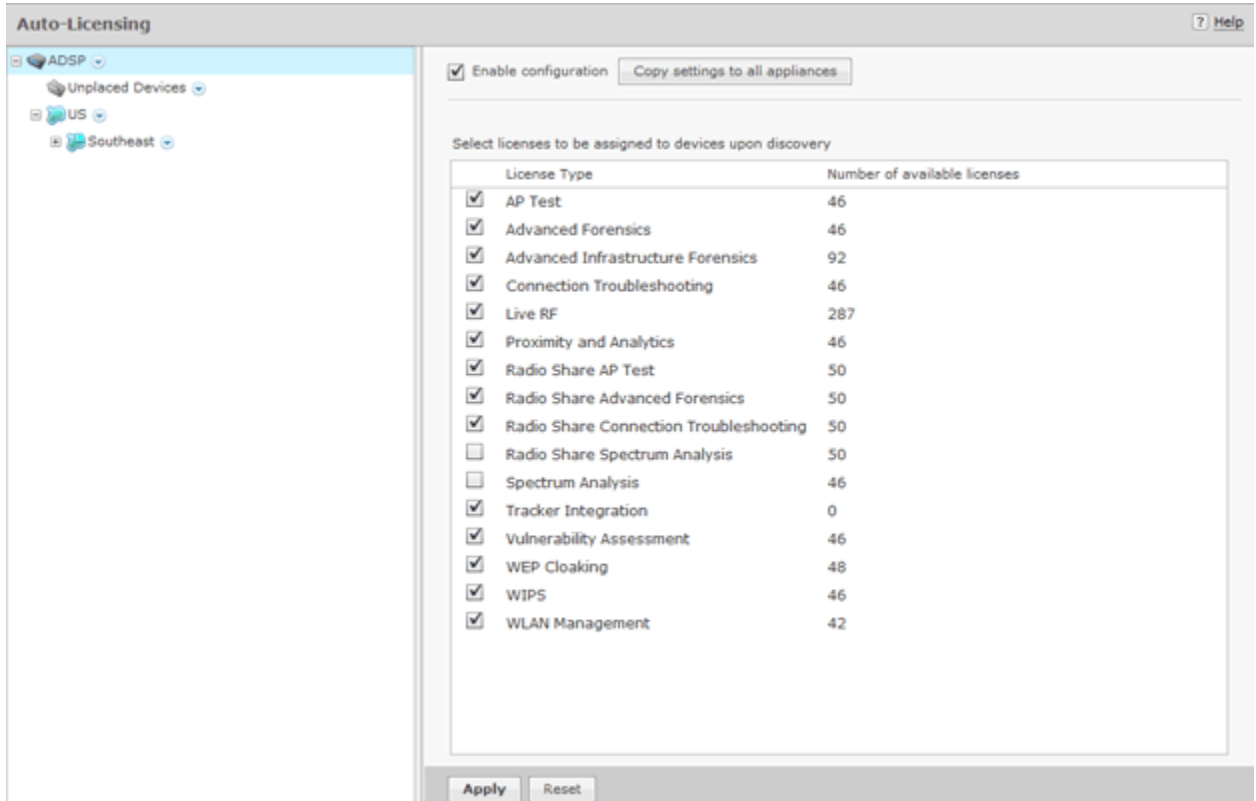
Auto-Licensing allows you to select licenses to be assigned to devices upon discovery. You can define licensing rules for importing BSSs and Wireless Clients into your network system.

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.



License Type	Number of available licenses
<input checked="" type="checkbox"/> AP Test	46
<input checked="" type="checkbox"/> Advanced Forensics	46
<input checked="" type="checkbox"/> Advanced Infrastructure Forensics	92
<input checked="" type="checkbox"/> Connection Troubleshooting	46
<input checked="" type="checkbox"/> Live RF	287
<input checked="" type="checkbox"/> Proximity and Analytics	46
<input checked="" type="checkbox"/> Radio Share AP Test	50
<input checked="" type="checkbox"/> Radio Share Advanced Forensics	50
<input checked="" type="checkbox"/> Radio Share Connection Troubleshooting	50
<input type="checkbox"/> Radio Share Spectrum Analysis	50
<input type="checkbox"/> Spectrum Analysis	46
<input checked="" type="checkbox"/> Tracker Integration	0
<input checked="" type="checkbox"/> Vulnerability Assessment	46
<input checked="" type="checkbox"/> WEP Cloaking	48
<input checked="" type="checkbox"/> WIPS	46
<input checked="" type="checkbox"/> WLAN Management	42

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** button.



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.

Assignment	Template Name	
<input checked="" type="checkbox"/>	comm_settings_AirDefense1	(Edit Copy Delete)
<input checked="" type="checkbox"/>	comm_settings_AirDefense2	(Edit Copy Delete)
<input checked="" type="checkbox"/>	comm_settings_AirDefense3	(Edit Copy Delete)

Modify Communication Settings Profile

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

Assignment	Template Name	
<input checked="" type="checkbox"/>	comm_settings_AirDefense1	(Edit Copy Delete)

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](#) on page 525
- [Console Tab](#) on page 526
- [HTTP Tab](#) on page 527

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.
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.

Field	Description
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 screenshot shows a dialog box titled "Communication Settings Profile" with a close button (X) in the top right corner. The "Profile Name" field contains "New_comm_settings_pro". Below this are three tabs: "SNMP", "Console" (which is selected), and "HTTP". Under the "Console" tab, there is a checkbox for "Enable Console settings" which is currently unchecked. Below this are four input fields: "User:", "Password:", "Enable Password:", and "Protocol:". The "Protocol:" dropdown menu is set to "SSH". Below the "Protocol:" field is a "Port:" field with the value "22". To the right of the "Password:" field is a checkbox for "Display Passwords" which is also unchecked. At the bottom of the dialog box are two buttons: "Save" and "Cancel".

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 screenshot shows a dialog box titled "Communication Settings Profile" with a close button (X) in the top right corner. Below the title, there is a "Profile Name" field containing the text "New_comm_settings_pro". There are three tabs: "SNMP", "Console", and "HTTP", with "HTTP" being the active tab. Under the "HTTP" tab, there is a checkbox labeled "Enable HTTP settings" which is currently unchecked. Below this, there are three input fields: "User:" (empty), "Password:" (empty), and "Port:" (containing the number "80"). To the right of the "Password:" field is another checkbox labeled "Display Password" which is also unchecked. Below the "Protocol:" label, there is a dropdown menu currently showing "HTTP". At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

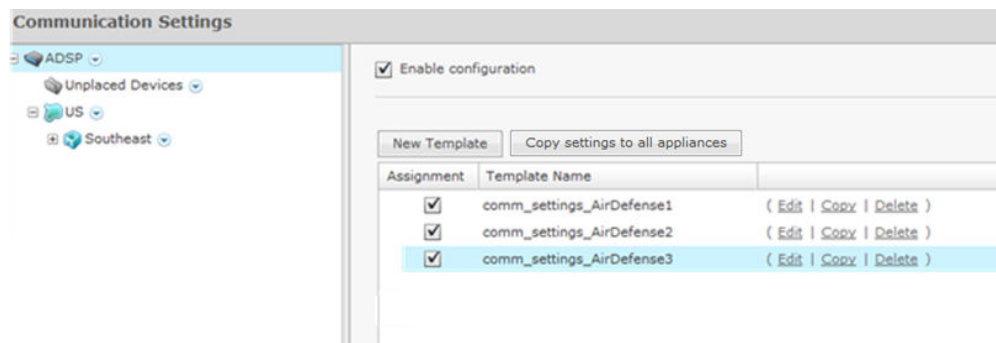
The following fields must be set when using a web UI to interface with a device:

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.




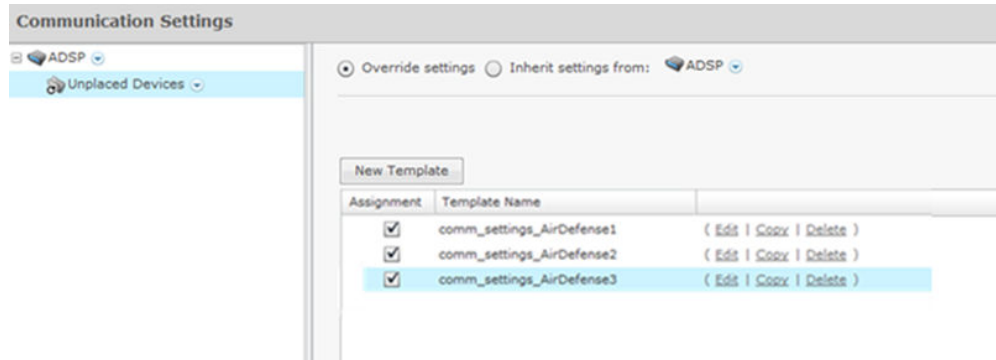
You should always configure Communication Settings at the appliance level. When you do, the configuration is inherited for all the other levels. Then, if you have a level that needs a different configuration, you can apply that profile to that level using the override feature.

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,snmpV3privpassphr,
MD5,
3DES,161,300,4,Cisco,Cisco,Cisco,SSH,22,admin,adminpassword,https,443
```



Note

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

The fields for the `comm_settings_loc` record are:

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

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

Examples:

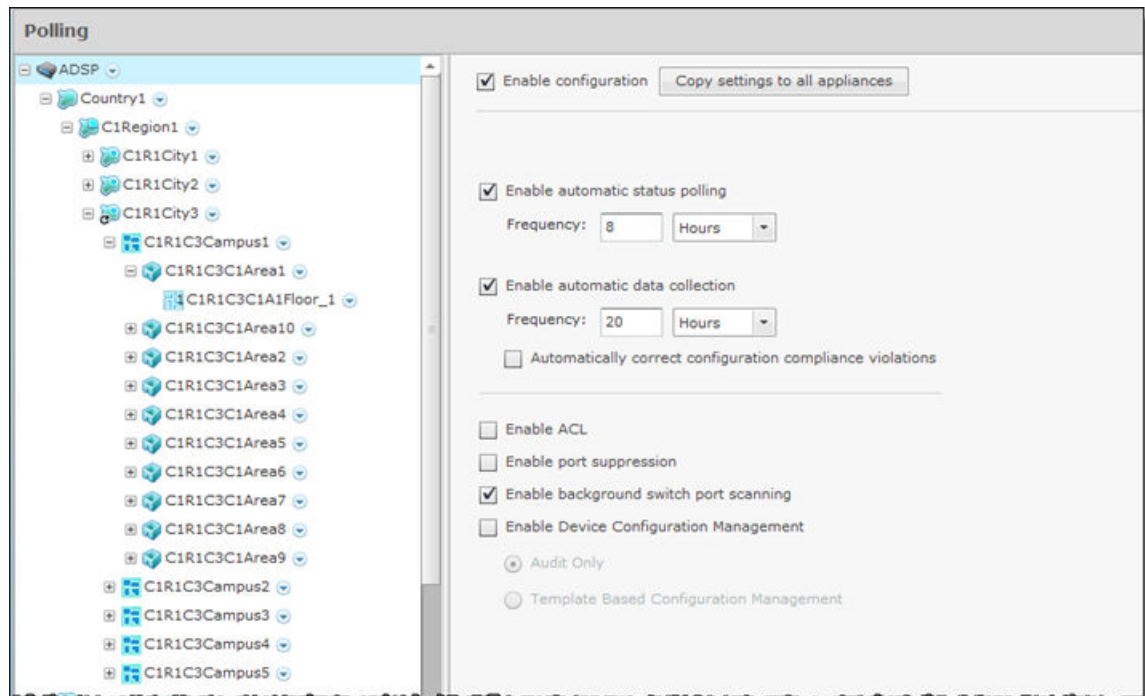
```
comm_settings_loc,ProfileName,00:23:04:5e:d3:00,ap
comm_settings_loc,ProfileName,/US/Southeast/AirDefense, folder3
```

**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.

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.

The screenshot displays the 'Import / Discover Devices' configuration interface. At the top, there are three buttons: 'Add', 'Delete', and 'Run Now'. Below these is a table with two columns: 'Name' and 'Schedule'. The table contains one row with the text 'New Scheduled Import' and 'Daily: Every 1 day at 12:00 AM'. To the right of the table is a 'Settings' panel with a 'Schedule' tab. The 'Settings' panel includes the following fields and options:

- Job Name: New Scheduled Import
- Import Source: Import Remote File (dropdown)
- Host: (text input)
- Protocol: SCP (dropdown)
- Path: (text input)
- User: (text input)
- Password: (text input) with a 'Display Password' checkbox
- Verify Server Certificate/Key: (checked checkbox)
- Add to appliance: ADSP (dropdown)

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](#) rules.

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

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 Formats](#) 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

Refer to the following table for more information:

Field	Description
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:

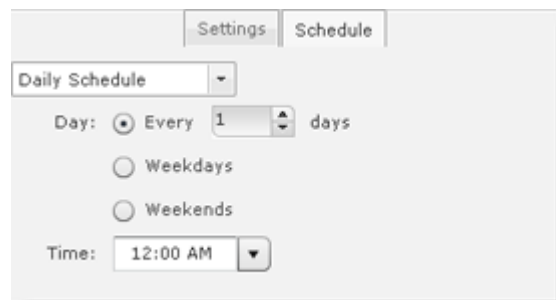
```
snmpwalk -v2c -c public xxx.xxx.xxx.xxx (this is the IP address).
```

Refer to the following table for more information:

Field	Description
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.

Field	Description
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

This section lists the various formats for importing devices.

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

The value `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

The value `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

The value `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,NX9600
switch,switchname,switchdesc,05:05:05:05:05:05,11.11.11.11,wired,switch.dns.name,
```

**Note**

The value `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**

The value `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

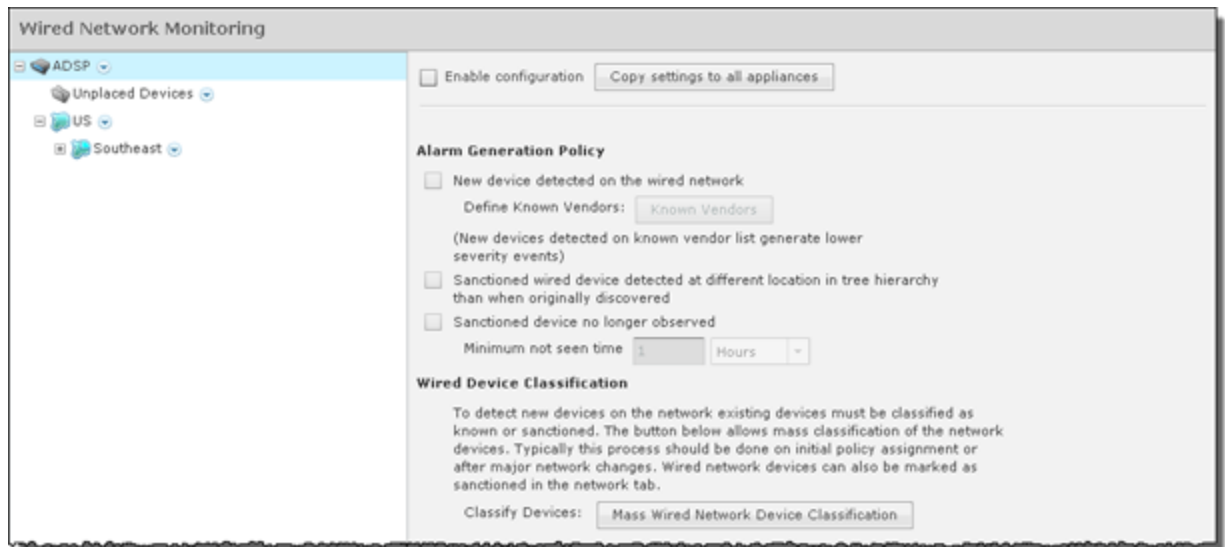
Security Profiles (also part of Appliance Platform) define the security configurations of sanctioned wireless clients on your wireless LAN. Refer to [Security Profiles](#) under the Appliance Platform topic.

Wired Network Monitoring

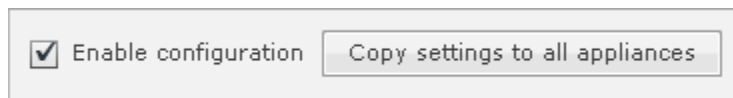
Wired Network Monitoring is used to monitor the wired network devices in your system. You can generate an alarm policy for your wired network by selecting any of the following conditions:

- 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.

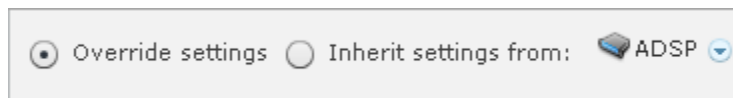
To detect new devices on your network, existing devices must be classified as sanctioned. The **Mass Wired Network Device Classification** button opens a dialog where you can sanction all or a selection of devices at one time. Typically, this process should be done when you initially configure policies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

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

Enable configuration Copy settings to all appliances

Alarm Generation Policy

New device detected on the wired network
 Define Known Vendors: Known Vendors

(New devices detected on known vendor list generate lower severity events)

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

Classify Devices: Mass Wired Network Device Classification

The Sanction Devices dialog opens.

Sanction Devices

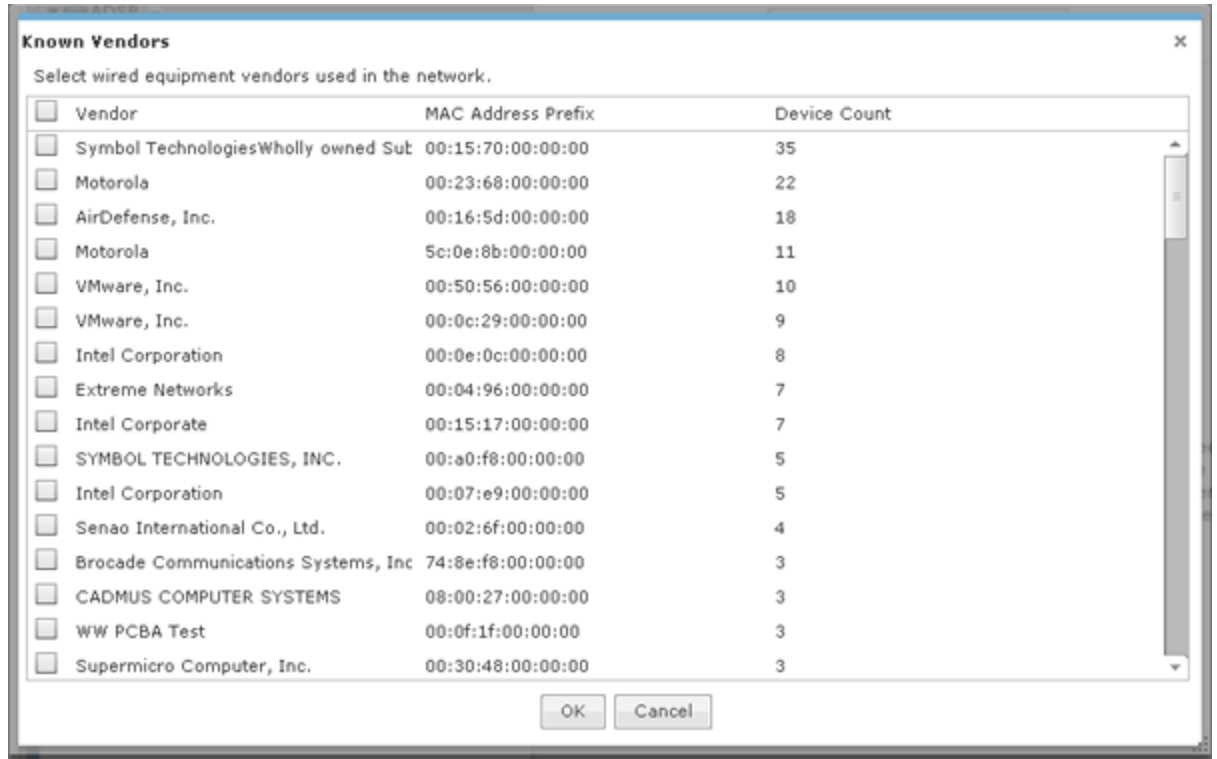
The selected devices will be sanctioned.

<input type="checkbox"/> Vendor	MAC Address Prefix	Device Count
<input type="checkbox"/> Symbol Technologies/Wholly owned Sut	00:15:70:00:00:00	35
<input type="checkbox"/> Motorola	00:23:68:00:00:00	23
<input type="checkbox"/> AirDefense, Inc.	00:16:5d:00:00:00	18
<input type="checkbox"/> Motorola	5c:0e:8b:00:00:00	11
<input type="checkbox"/> VMware, Inc.	00:50:56:00:00:00	10
<input type="checkbox"/> VMware, Inc.	00:0c:29:00:00:00	9
<input type="checkbox"/> Intel Corporation	00:0e:0c:00:00:00	8
<input type="checkbox"/> Extreme Networks	00:04:96:00:00:00	7
<input type="checkbox"/> Intel Corporate	00:15:17:00:00:00	7
<input type="checkbox"/> SYMBOL TECHNOLOGIES, INC.	00:a0:f8:00:00:00	5
<input type="checkbox"/> Intel Corporation	00:07:e9:00:00:00	5
<input type="checkbox"/> Senao International Co., Ltd.	00:02:6f:00:00:00	4
<input type="checkbox"/> APPLE COMPUTER INC.	08:00:07:00:00:00	3
<input type="checkbox"/> Brocade Communications Systems, Inc	74:8e:f8:00:00:00	3
<input type="checkbox"/> CADMUS COMPUTER SYSTEMS	08:00:27:00:00:00	3
<input type="checkbox"/> WW PCBA Test	00:0f:1f:00:00:00	3

OK Cancel

Select all the vendors you recognize as authorized and permanent for that site. (Help text is provided just above the **Mass Wired Network Device Classification** button.) Then, sanction devices detected at your site by clicking **OK**.

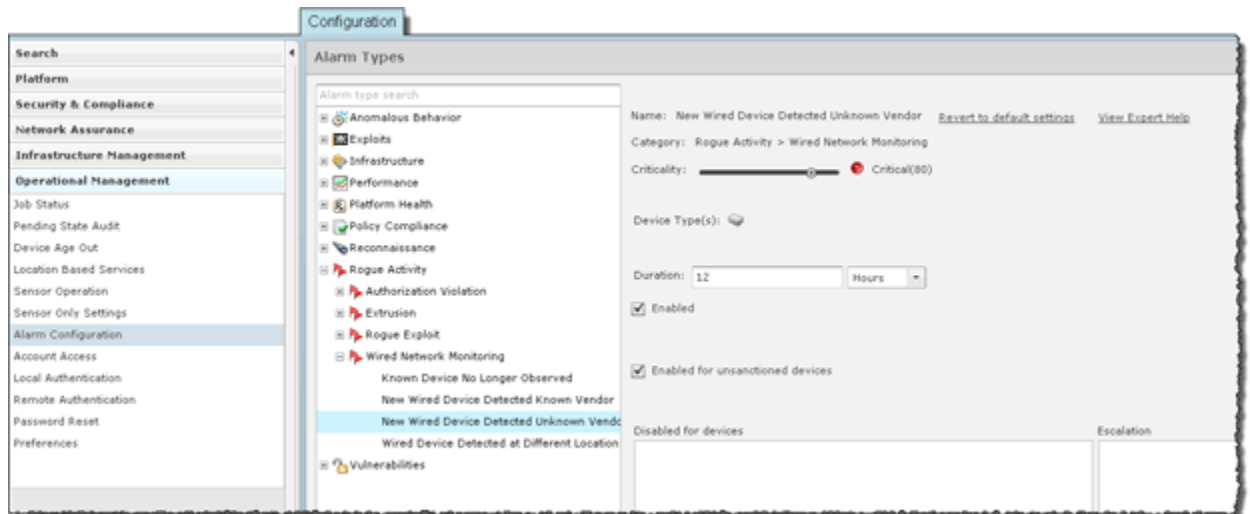
To have a finer control over alarms about new known vendor devices and new unknown vendor devices, you can utilize the Known Vendors classification tool. Click on the **Known Vendors** button to display a list of known vendors.



Select the approved vendors and click **OK**.

After configuring the **Wired Network Monitoring** options, click the **Apply** button to save your changes. Click the **Reset** button to discard your changes.

Once new devices are detected at your site, you will receive one of two alarms: *New Wired Device Detected Known Vendor* or *New Wired Device Detected Unknown Vendor*. Below is a screen shot of **Alarm Configuration**, where you can customize the criticality, duration, state and exception for each of the alarms.



Network Assurance

The Network Assurance category allows you to:

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

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.

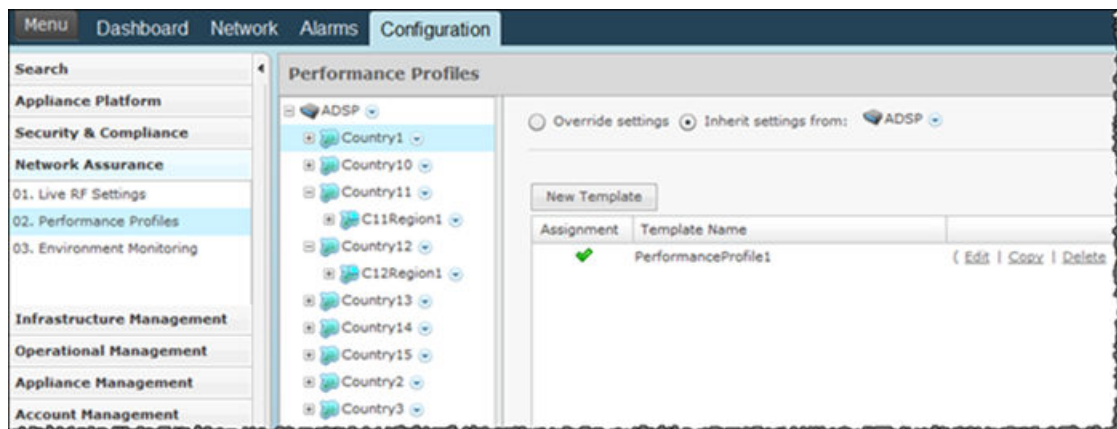


Note

You should monitor new ADSP deployments for several weeks to determine normal network activity before configuring Performance Profiles.

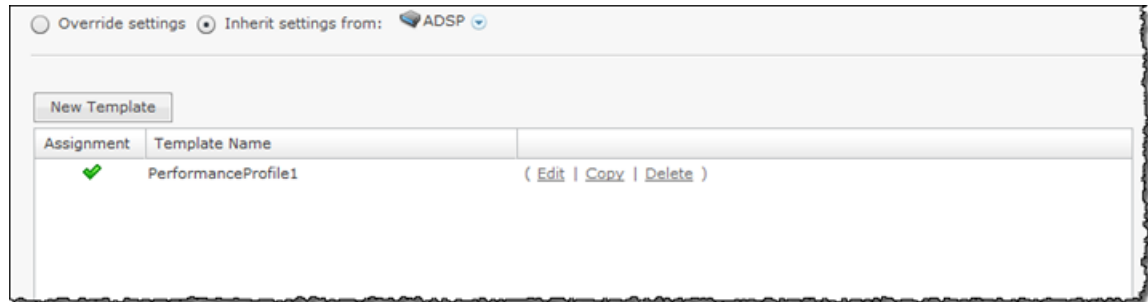
View Performance Profiles

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 included in **Job Status** under **Configuration > Operational Management**. The description supplied in the confirmation helps identify jobs.

Add a New Performance Profile

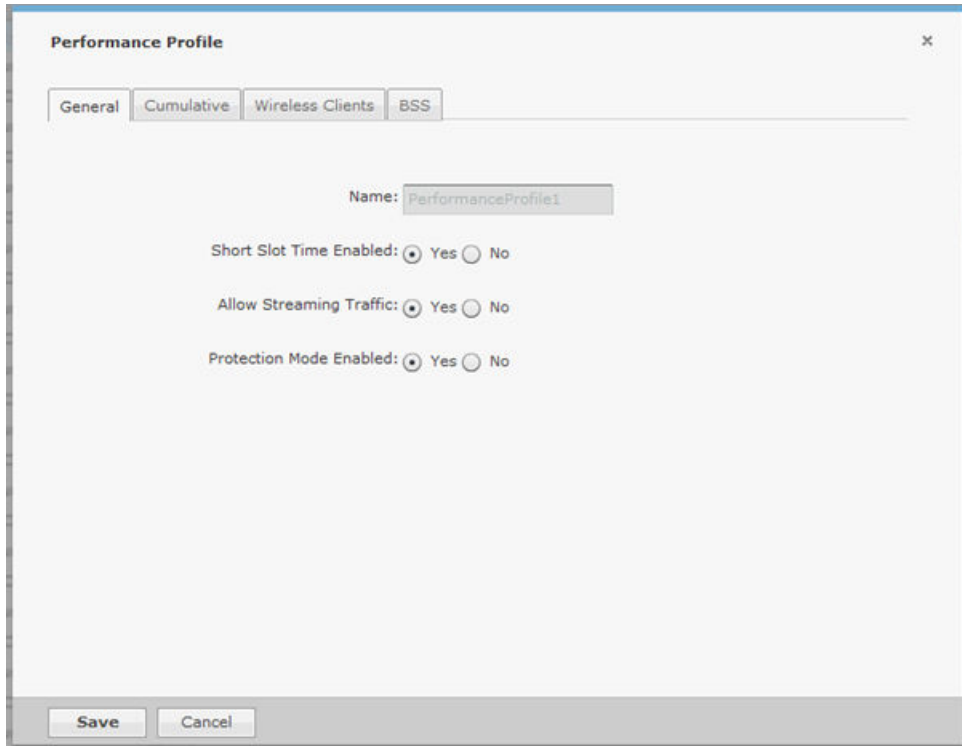
Click the New Profile button to add a new profile. Define your Performance Profile using the **General**, **Cumulative**, **Wireless Clients**, and **BSS** tabs. Once you have defined your Performance Profile, click OK to save your profile or Cancel to exit without saving the profile.

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 APs 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 APs 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 screenshot shows a dialog box titled "Performance Profile" with a close button (X) in the top right corner. Below the title bar are four tabs: "General", "Cumulative", "Wireless Clients", and "BSS". The "General" tab is selected. In the center, there is a "Name:" label followed by a text input field containing "PerformanceProfile1". Below this are three radio button options, each with "Yes" and "No" choices: "Short Slot Time Enabled:" (Yes selected), "Allow Streaming Traffic:" (Yes selected), and "Protection Mode Enabled:" (Yes selected). At the bottom of the dialog are "Save" and "Cancel" buttons.

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.

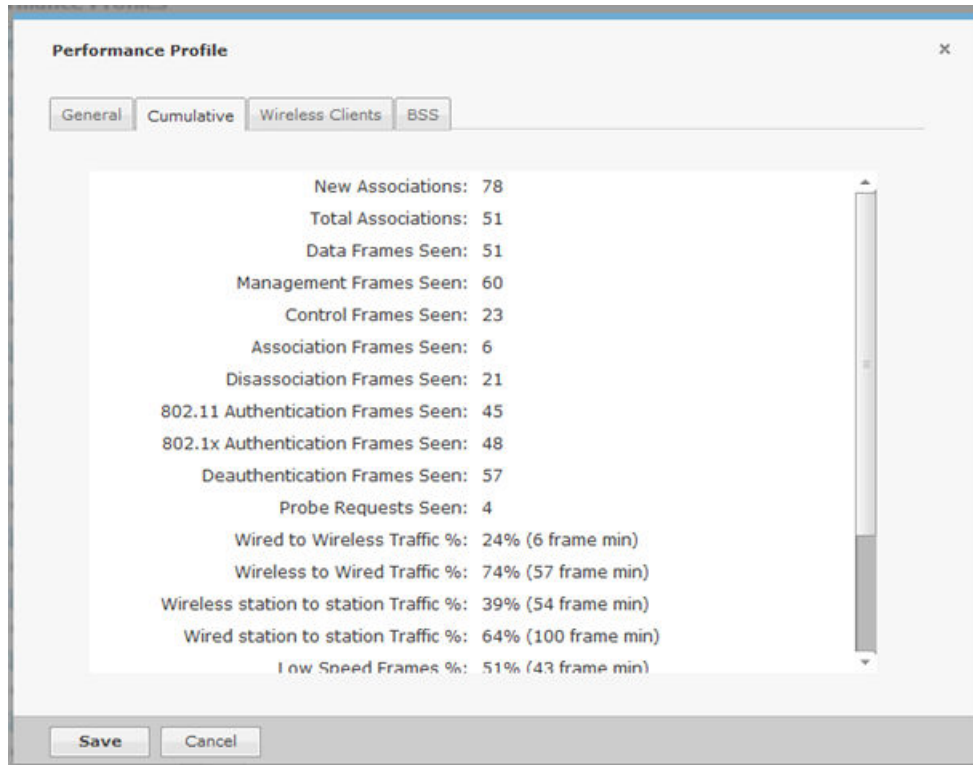
Cumulative Tab

The Cumulative tab is where you assign thresholds to network characteristics for all Wireless Clients and traffic in the APs 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 AirDefense 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. AirDefense generates an alarm if it detects a greater number, assuming that the extra associations are made by hackers. Default = 15.

Threshold	Description
Data Frames Seen	Enter the maximum number of data frames per minute allowed to be transmitted from all Wireless Clients combined. If AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 0.
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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 60.

Threshold	Description
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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 0.
Layer 3 Multicast Frames %	An alarm that is generated when the system has detected a high percentage of multicast traffic violating the policy thresholds. This may be a result of potential Layer 3 broadcast storm attacks on the network. Enter the maximum percentage of data per minute allowed for multicast frames to be transmitted or received within a BSS from all stations. If AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 0.

Threshold	Description
Retransmission Frames %	Enter the maximum percentage of retransmitted data frames allowed during a transmission of data within a BSS from all stations. If AirDefense 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 AirDefense detects a greater number, it generates an alarm.Default = 0.

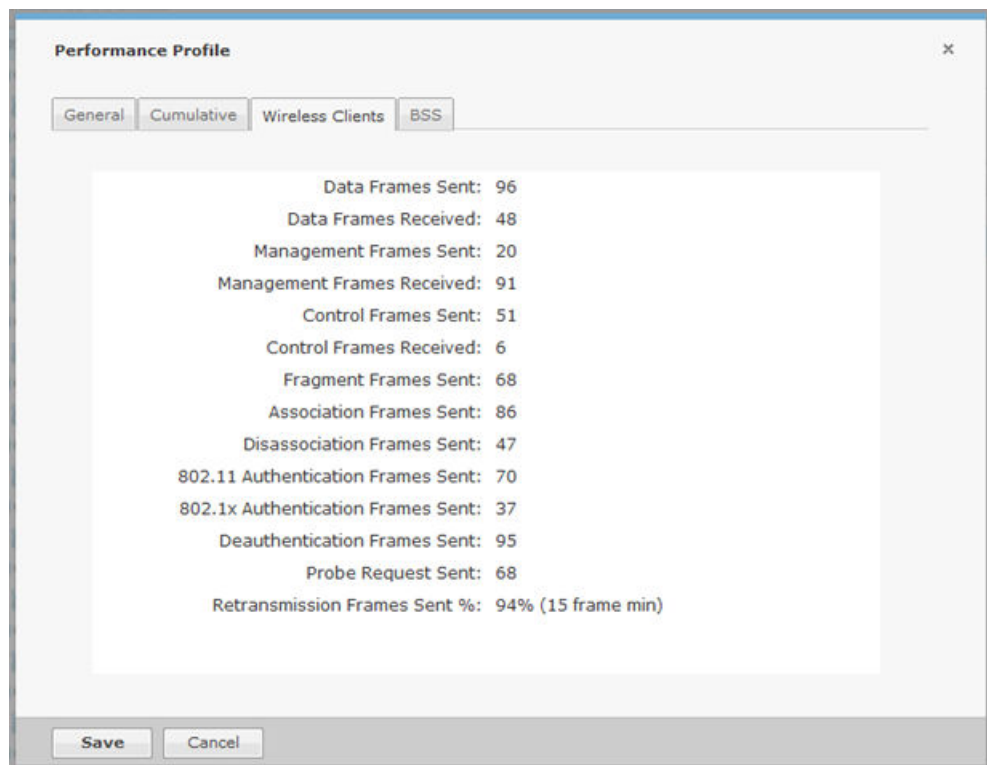
Wireless Clients Tab

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. AirDefense 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.



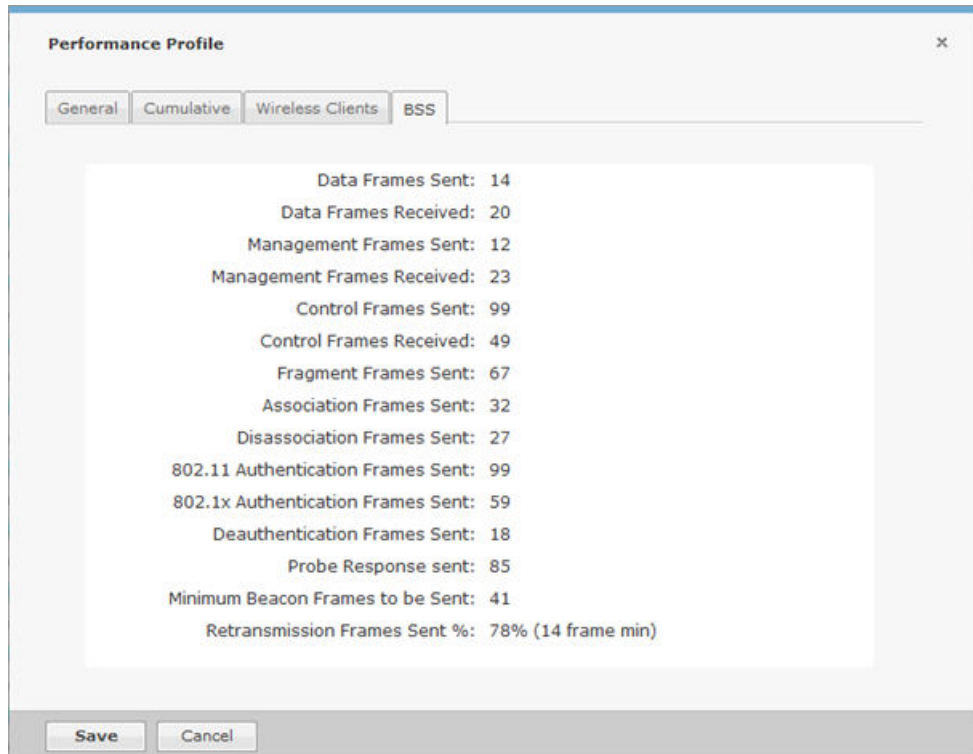
The thresholds are:

Threshold	Description
Traffic Sent %	Enter the maximum percentage of data per minute any Wireless Client is allowed transmit. If AirDefense 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 AirDefense 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 AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 0.
Management Frames Sent	Enter the maximum number of management frames per minute any Wireless Client is allowed to transmit. If AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 Mbps. Unusually high numbers of Control frames may indicate bandwidth and network problems.

Threshold	Description
Fragment Frames Sent	Enter the maximum number of fragment frames per minute that are allowed from any Wireless Client. If AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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.



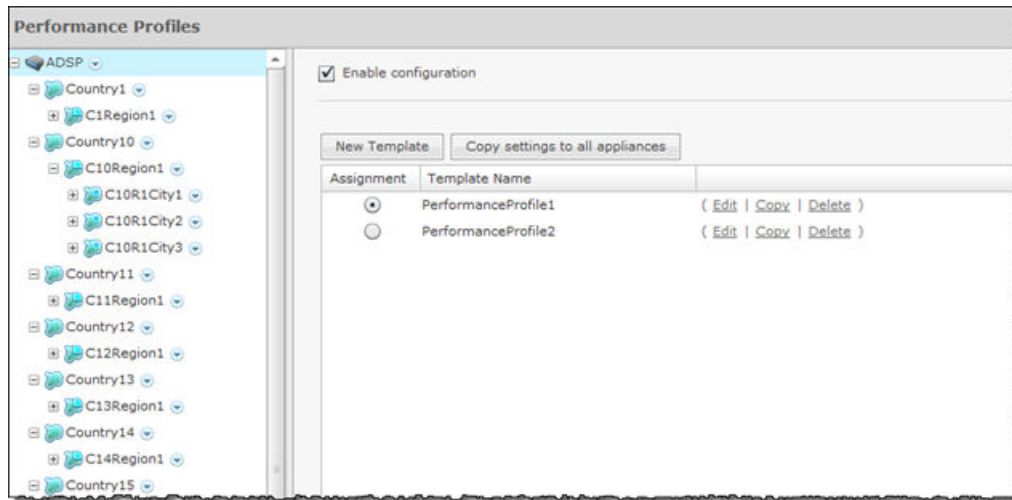
The thresholds are:

Threshold	Description
Traffic Sent %	Enter the maximum percentage of data per minute BSSs are allowed to transmit. If AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense detects a greater number, it generates an alarm. Default = 0.

Threshold	Description
Control Frames Sent	Enter the maximum number of control frames per minute BSSs are allowed to transmit. If AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense 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.

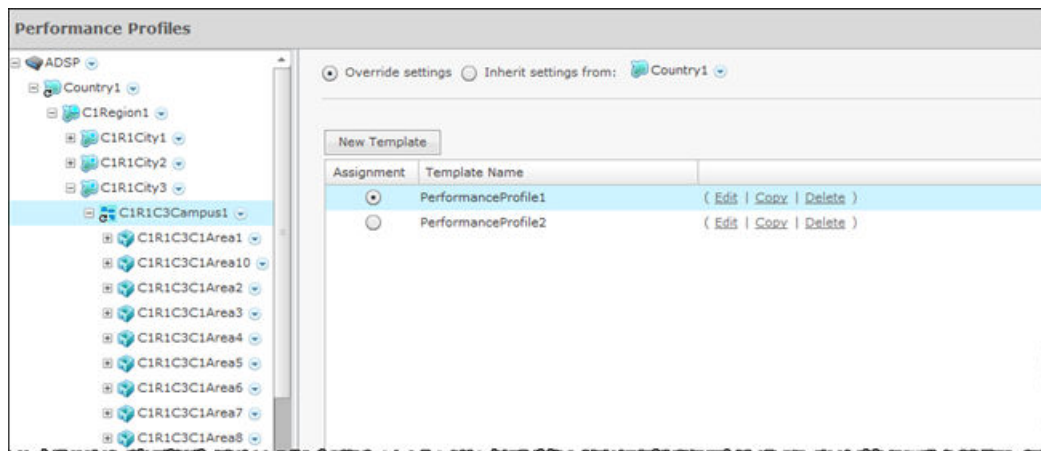


You should always apply a Performance Profile at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Performance Profile, you can apply that profile to that level.



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.

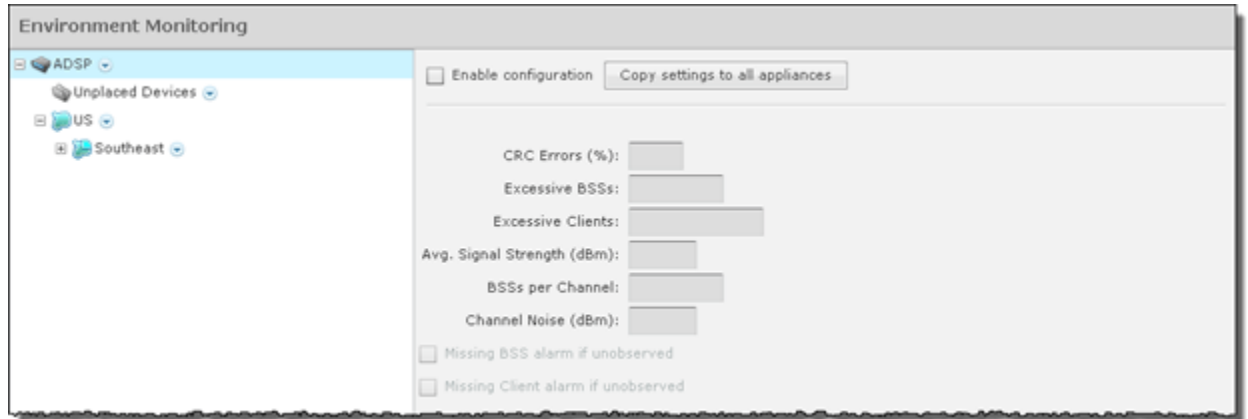


In this example, the *PerformanceProfile2* profile will be accessible to corporate-wide employees and guests while the *PerformanceProfile1* profile will be available employees and guests on *Campus1* of the facilities.

Click the **Apply** button at the bottom of the screen to save your changes. Click the **Reset** button to discard your changes.

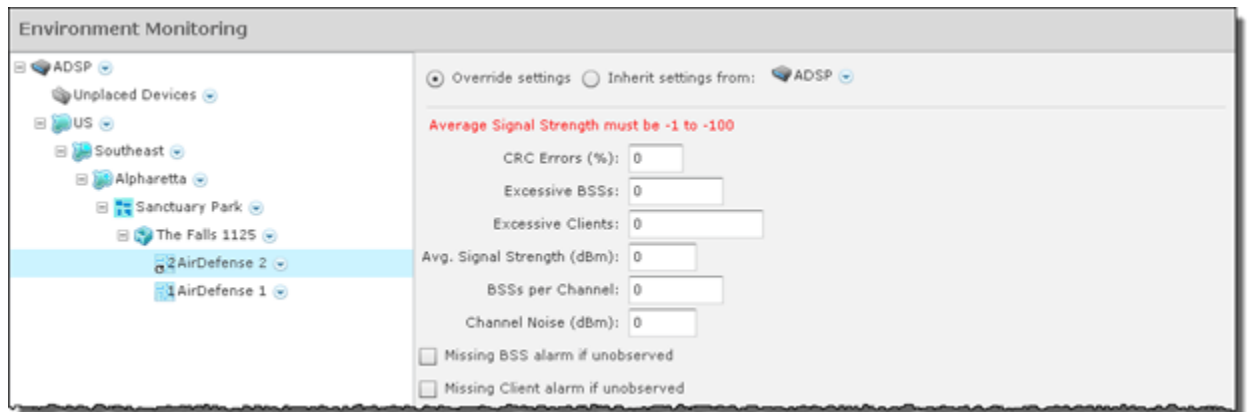
Environment Monitoring

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.

Threshold	Description
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.

Anomaly Baseline View

This screens displays the computed baseline thresholds for the triggering Anomalous Behavior alarms.

Anomaly Baseline Types	Threshold
BSS Baselines	
Management Frames	1658
Control Frames	5867
Data Frames	3897
Associated Count	234
Management Bytes	477920
Control Bytes	82220
Data Bytes	3470536
Client Baselines	
Management Frames	3921
Control Frames	16494
Data Frames	4394
Management Bytes	1038206
Control Bytes	218587
Data Bytes	4455962

Anomalous Behavior Alarms (ABA) feature is only available for AirDefense Enterprise servers and does not require any specific license. This feature is enabled when you enable **Performance Profile**. ABA is calculated for sanctioned clients and BSS only. All other data is ignored.

The AirDefense server flags traffic behavior that deviates significantly from observed normal behavior. The server learns specific attributes of traffic monitored over a configurable period of time. It uses this information to flag any traffic that deviates significantly from its learned traffic behavior.

AirDefense ABA works in two phases.

- Background Learning Phase
- Live Data Threshold Comparison Phase

These phases are common to all alarms based on the anomaly detection paradigm. Each alarm type could have different learning parameters and custom threshold computation methods.

In the *Background Learning Phase*, the AirDefense server monitors the forensic data in the data store for a configured duration of time. It then computes a baseline behavior against which an event will be tested. The learning phase training window is sliding to enable including the live data being added to the forensic store. ABA learning happens at regular intervals during the day to compute thresholds for all anomalous alarms. The default learning interval for each alarm is 14 days. Thresholds are computed and stored in 5 minute windows. These learning interval configuration values cannot be modified. These thresholds are computed on the scope where performance profile is enabled. The scopes can be at *Site Level*, *Floor Level*, or *System Level*.

In the *Live Data Threshold Comparison Phase*, live data from the sensors is compared with the computed thresholds for the enabled scope. If the live data is above the computed threshold, its corresponding alarm is triggered. For example, if, in the live data, the total *AP Management Frames* in a location in a 5 minute interval exceeds the computed threshold value of the total *AP Management Frames* in the same 5 minute interval over the last 14 days, then the *AP Management Frame Anomalous Behavior Frames* alarm is raised.

ABA computation starts at 00:00 hour. The computed threshold values are not persistent across server reboots and restarts. In case a server is restarted or rebooted, threshold computation will commence at 00:00 hours. You will not have computed threshold value from the time the server was rebooted or restarted till the nearest 00:00 hour.

The following Anomalous Behavior Alarms are supported

- MU Management Frame Anomalous Behavior Frames
- MU Data Frame Anomalous Behavior Frames
- MU Control Frame Anomalous Behavior Frames
- AP Management Frame Anomalous Behavior Frames
- AP Data Frame Anomalous Behavior Frames
- AP Control Frame Anomalous Behavior Frames
- MU Management Frame Anomalous Behavior Bytes
- MU Data Frame Anomalous Behavior Bytes
- MU Control Frame Anomalous Behavior Bytes
- AP Management Frame Anomalous Behavior Bytes
- AP Data Frame Anomalous Behavior Bytes
- AP Control Frame Anomalous Behavior Bytes
- AP Anomalous Number of Connected MUs

Operational Management

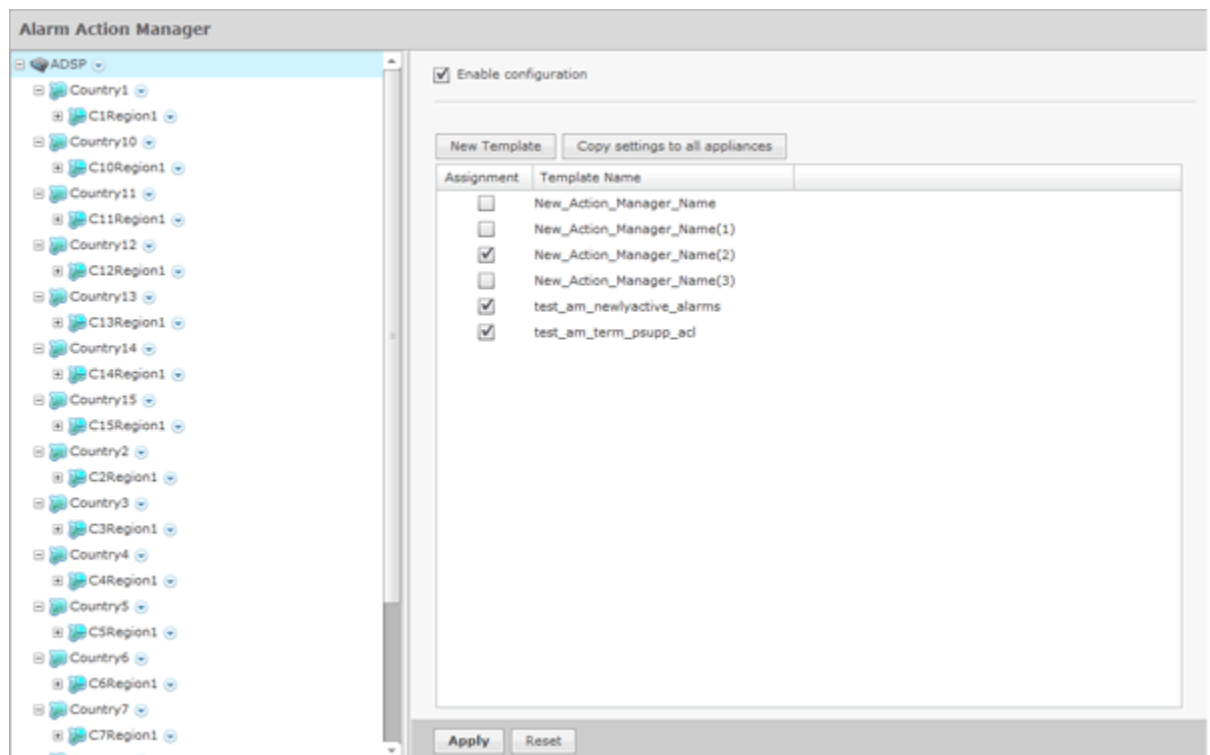
The Operational Management category includes features that apply to the normal operations of AirDefense. The Operational Management category allows you to:

- Automatically respond to alarms in your system with a predetermined action.
- Configure alarms for your network environment.
- Specify an age out value that AirDefense uses to display devices in the Network tab.
- View and check on jobs initiated by users using AirDefense.
- 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.

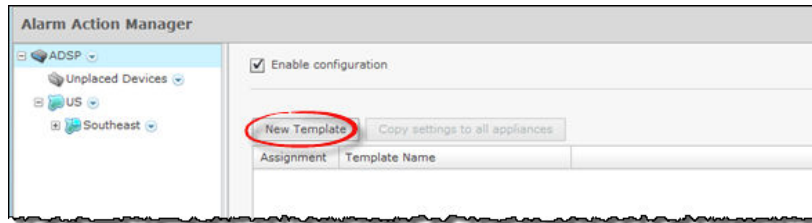
The Alarm Action Manager table displays one rule per row using the following columns:

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.

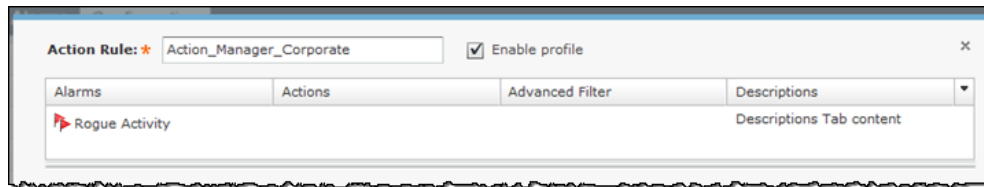
Once a template is added to the **Alarm Action Manager**, you can edit, copy, or delete it by selecting (highlighting) a template and then clicking on the appropriate link that appears to the right of the template.

Add an Action Rule

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



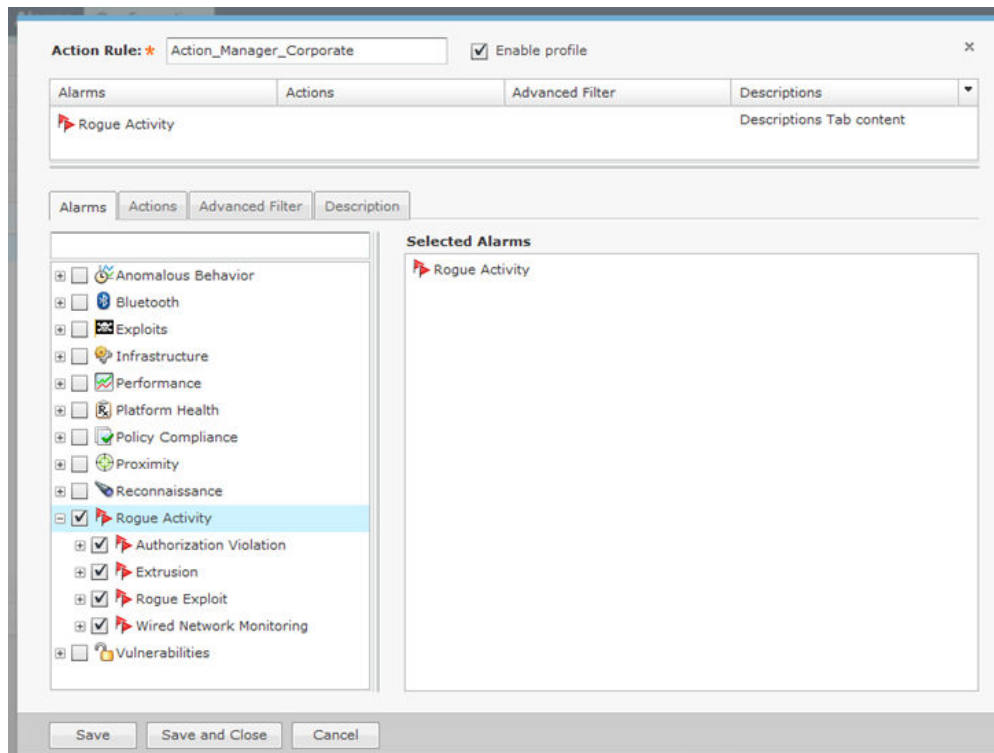
In the **Action Rule** field, give your action rule a name and select the **Enable profile** checkbox to enable the action rule.



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

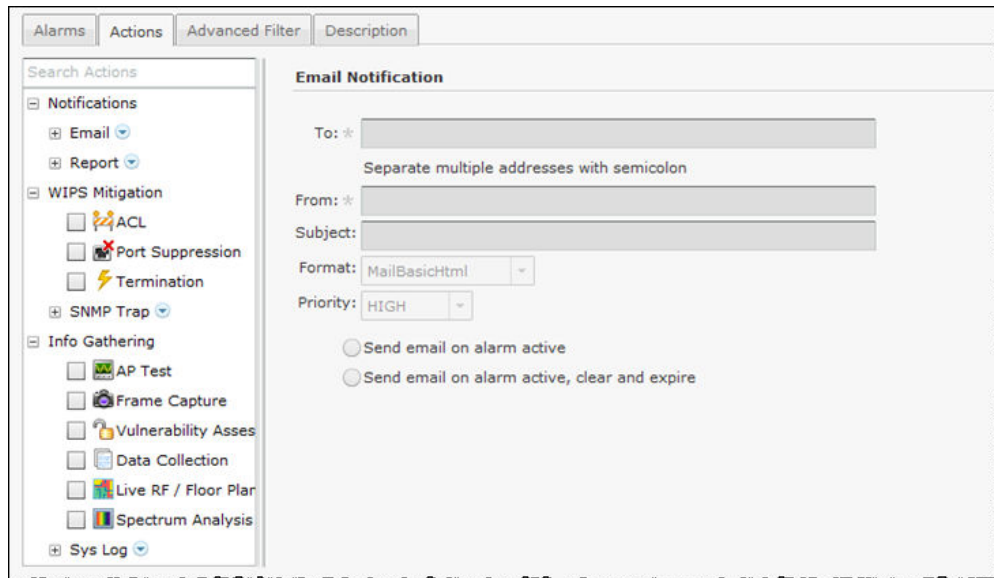
The **Alarms** tab is where you identify the alarms that you want to generate for your Action Rule. You may select one or more alarms to generate when the conditions in the filter are met. In the following example, the **Rogue Activity** alarm is selected.



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:

- The following fields should be filled:[Report.Email](#)
- The following fields should be filled:[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**.

Action Rule: * Enable profile

Alarms | Actions | Advanced Filter | Descriptions

Alarms | Actions | Advanced Filter | Description

Search Actions

- Notifications
 - Email
 - Email
 - Report
 - WIPS Mitigation
 - Info Gathering

Email Notification

To: *

Separate multiple addresses with semicolon

From: *

Subject:

Format: MailSmartPhone

Priority: MEDIUM

Send email on alarm active

Send email on alarm active, clear and expire

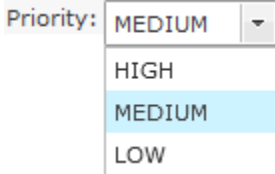
Save | Save and Close | Cancel

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.
Format	Specifies a format in which to send the email. Choose a format from the drop-down menu.

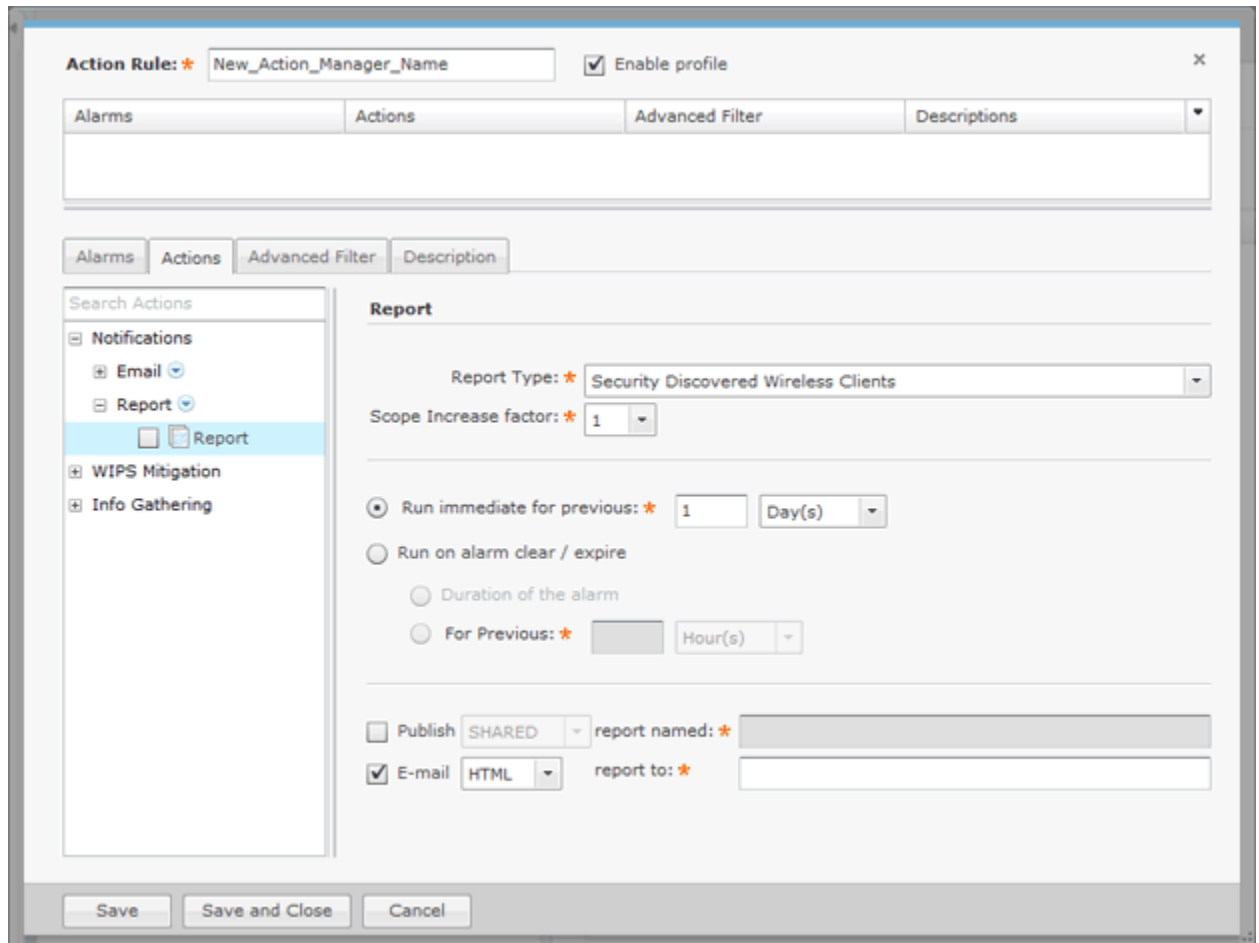
Format:

- MailSmartPhone
- MailBasicText
- MailBasicHtml
- MailDetailedHtml
- MailSMSText

Field	Description
Priority	<p>Specifies a priority for the email. Choose a priority from the drop-down menu.</p> 
Send email options	<p>There are two options to send email:</p> <ul style="list-style-type: none"> • 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.
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.

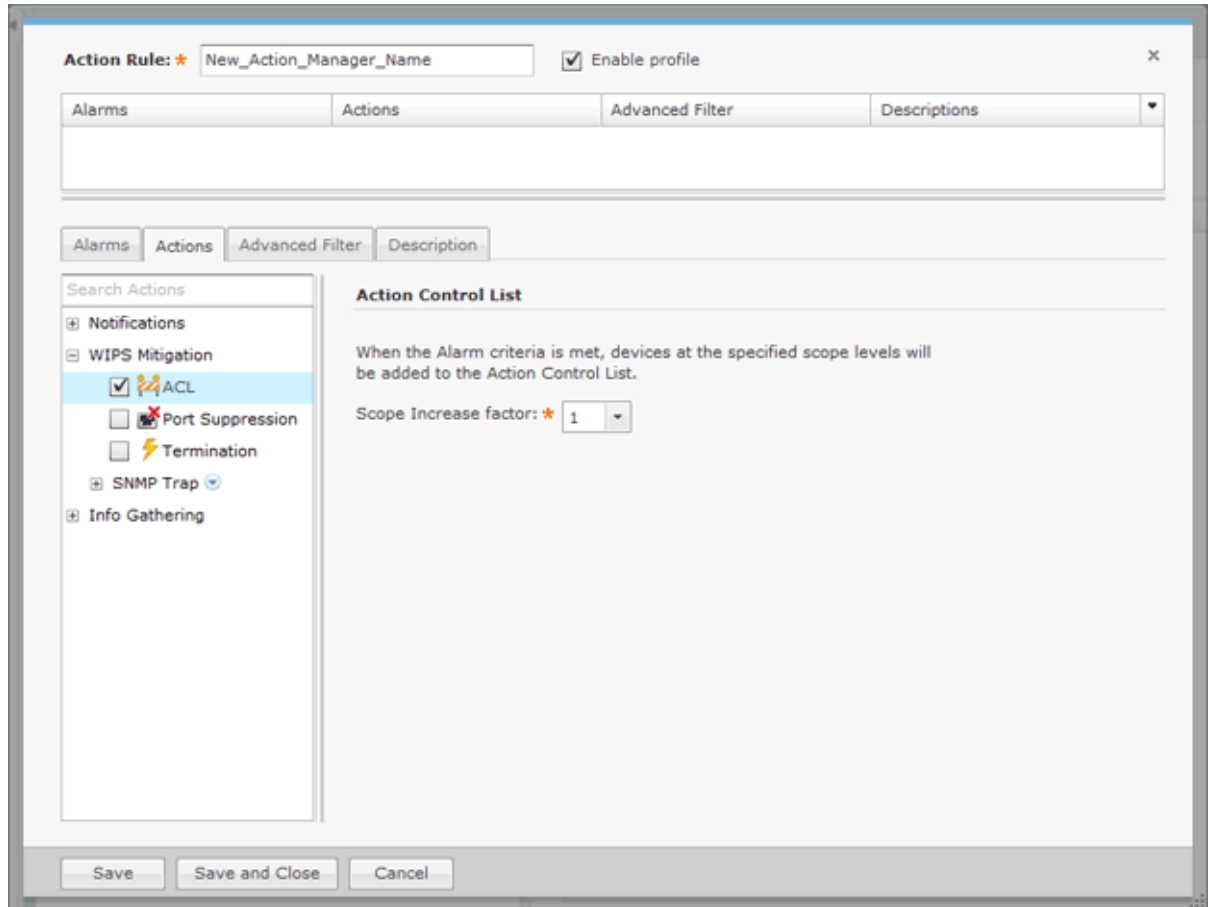
WIPS Mitigation

The following actions are part of WIPS Mitigation:

- [ACL](#)
- [Port Suppression](#)
- [Termination](#)
- [SNMP 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 **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.

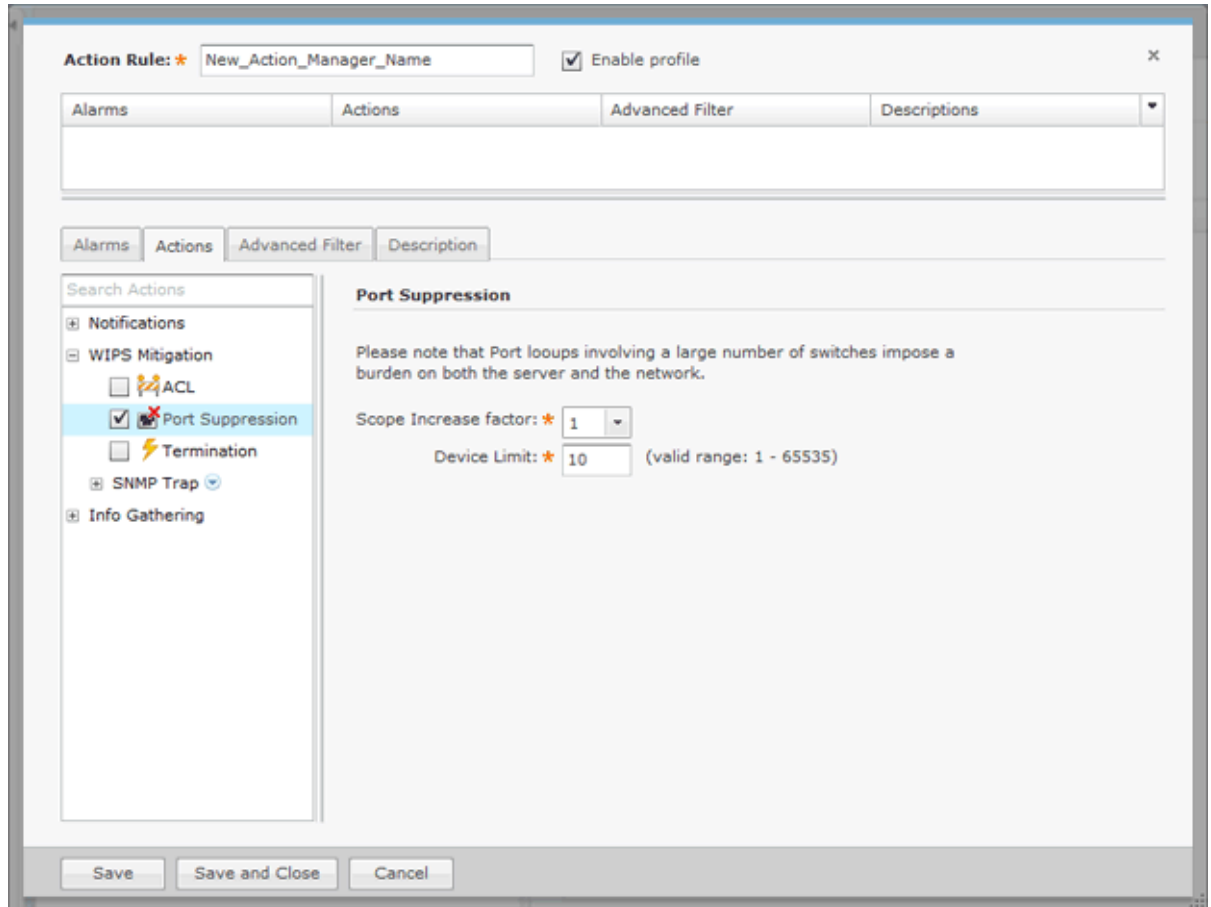
Port Suppression

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** menu tree.



Note

Before you can use Port Suppression, it must be enabled in **Configuration > Appliance Management > Appliance Settings**.



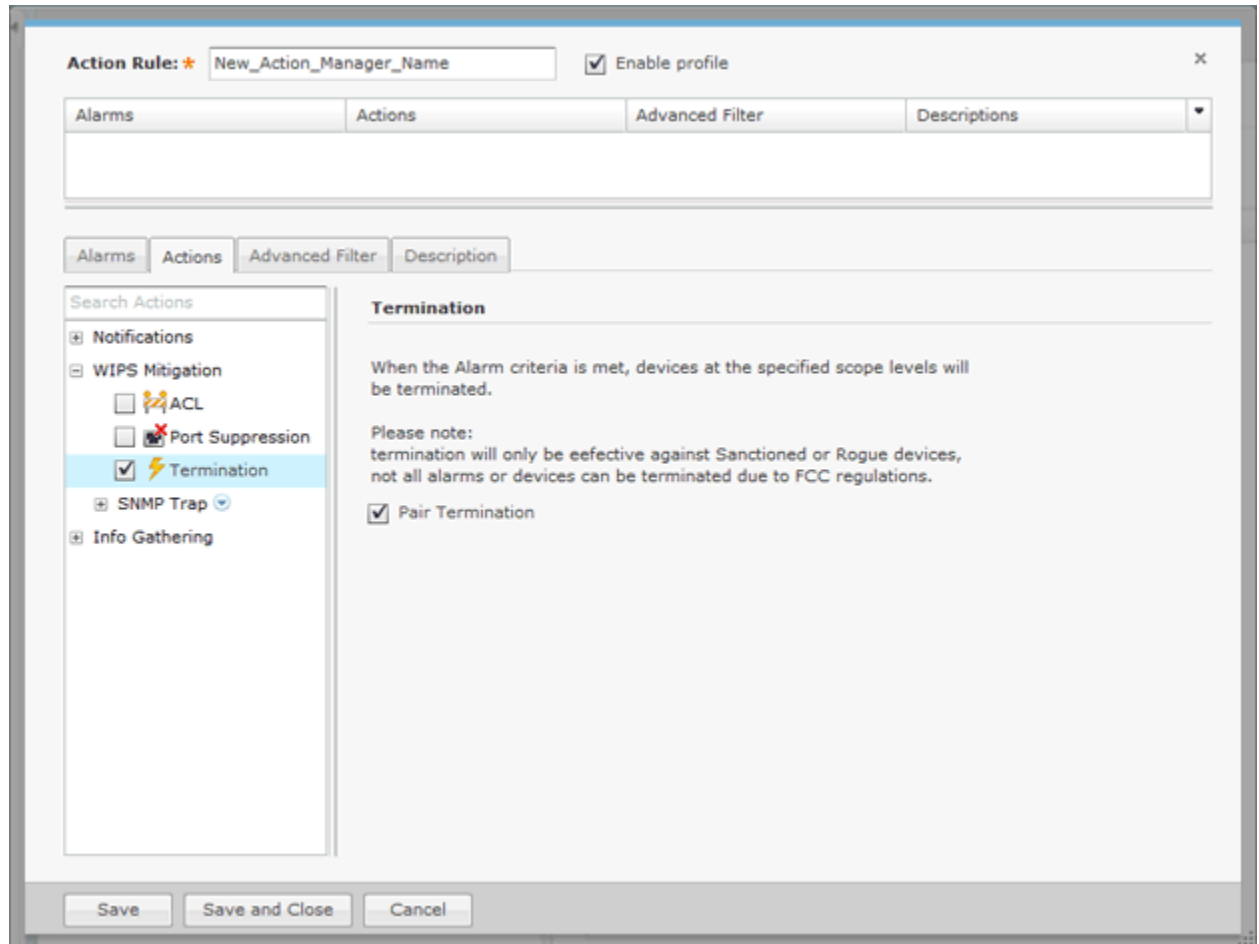
There are two options to configure: **Scope Increase Factor** and **Device Limit**.

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

SNMP Trap

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

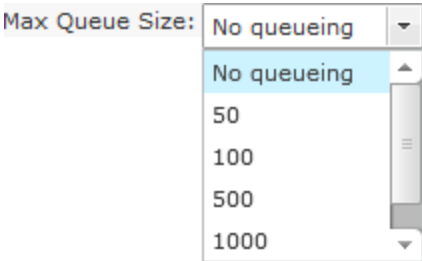


Note

Before you can use the SNMP Trap action, you must enable SNMP trap. 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	<p>Specifies the desired transport protocol. Choices are:</p> <ul style="list-style-type: none"> • UDP: User Datagram Protocol • TCP: Transmission Control Protocol. <p>Hint: Typically, UDP is the transport for SNMP traps. However, TCP can be useful for tunneling the traps over Secure Socket Layer (SSL).</p>
Max Queue Size	<p>Specifies the maximum queue size for the notification. Choose a size from the drop-down menu.</p> 
Send Time	<p>Specifies when to send the email by selecting one of the following conditions:</p> <ul style="list-style-type: none"> • 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](#) on page 567
- [Frame Capture](#) on page 568
- [Vulnerability Assessment](#) on page 570
- [Data Collection](#) on page 571
- [Live RF / Floor Plan](#) on page 571
- [Spectrum Analysis](#) on page 572
- [Sys Log](#) on page 573

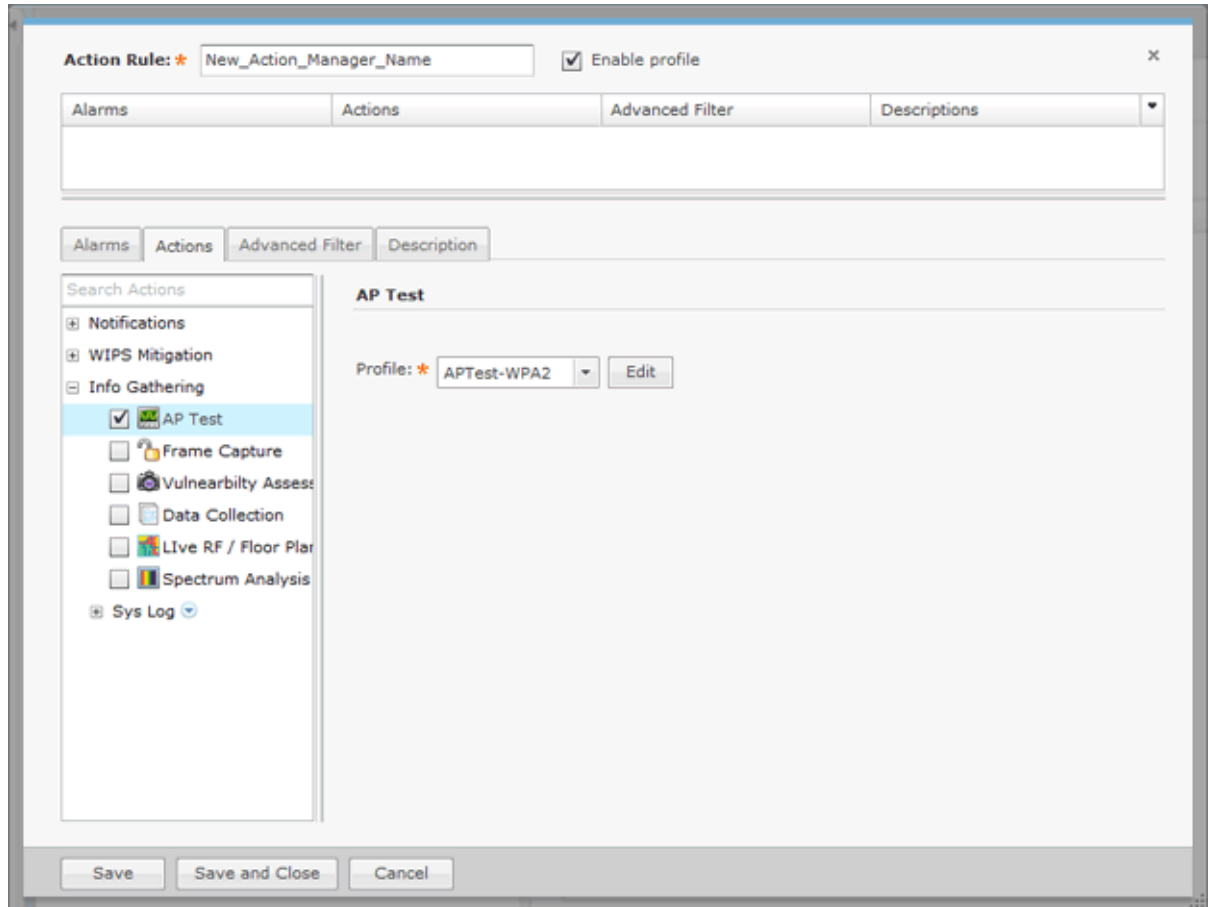
AP Test



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**.

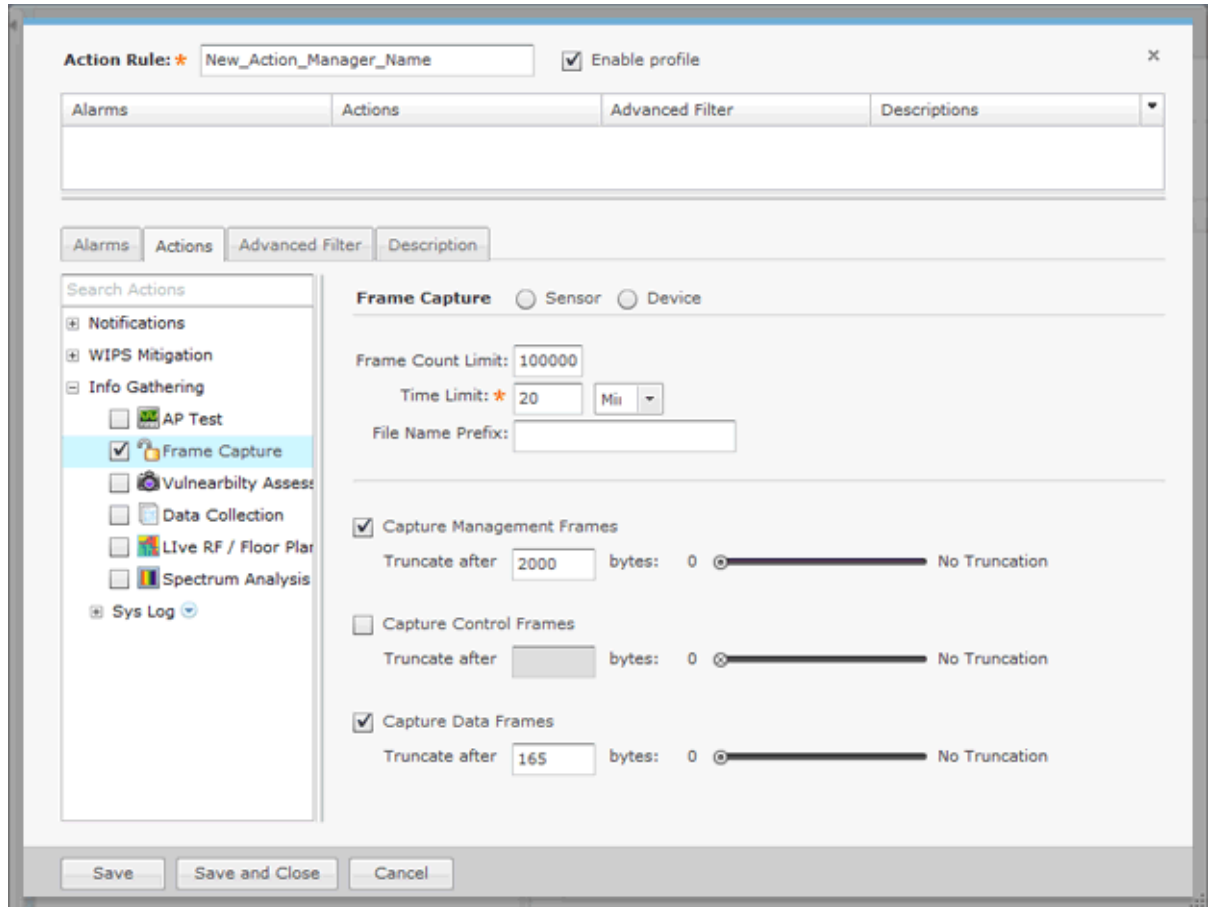


The following field is available:

Field	Description
Profile	Select a test profile from the drop-down menu. The Edit button can be used to modify the test profile. See Scheduled AP Tests on page 409 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 a Device.
Frame Count Limit	Limits the total amount of frames to capture.
Time Limit	Specifies a time duration for the Frame Capture to run. You must enter x amount of minutes or hours.
File Name Prefix	Specifies a prefix for the file name. The prefix is added to a number sequence to make up the file name.
Capture Management Frames	Turns on capturing Management frames. Check the checkbox and slide the slider to specify when to stop capturing Management frames.
Capture Control Frames	Turns on capturing Control frames. Check the checkbox and slide the slider to specify when to stop capturing Control frames.
Capture Data Frames	Turns on capturing Data frames. Check the checkbox and slide the slider to specify when to stop capturing Data frames.

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

/usr/local/smx/pcaptures OR /usr/local/smx/pcaptures/saved.

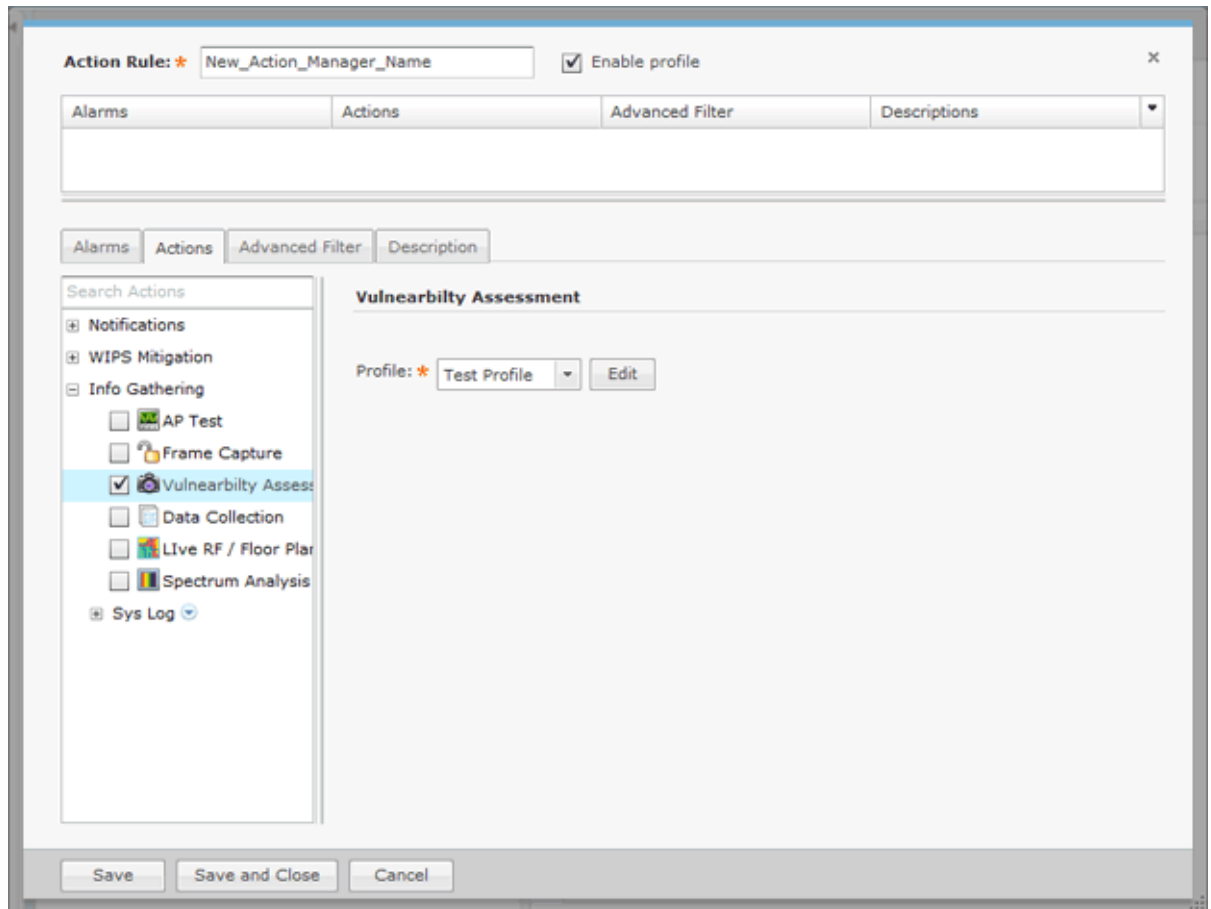
Vulnerability Assessment



Note

Vulnerability Assessment requires a Vulnerability Assessment license for access.

The Vulnerability Assessment action runs a 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:

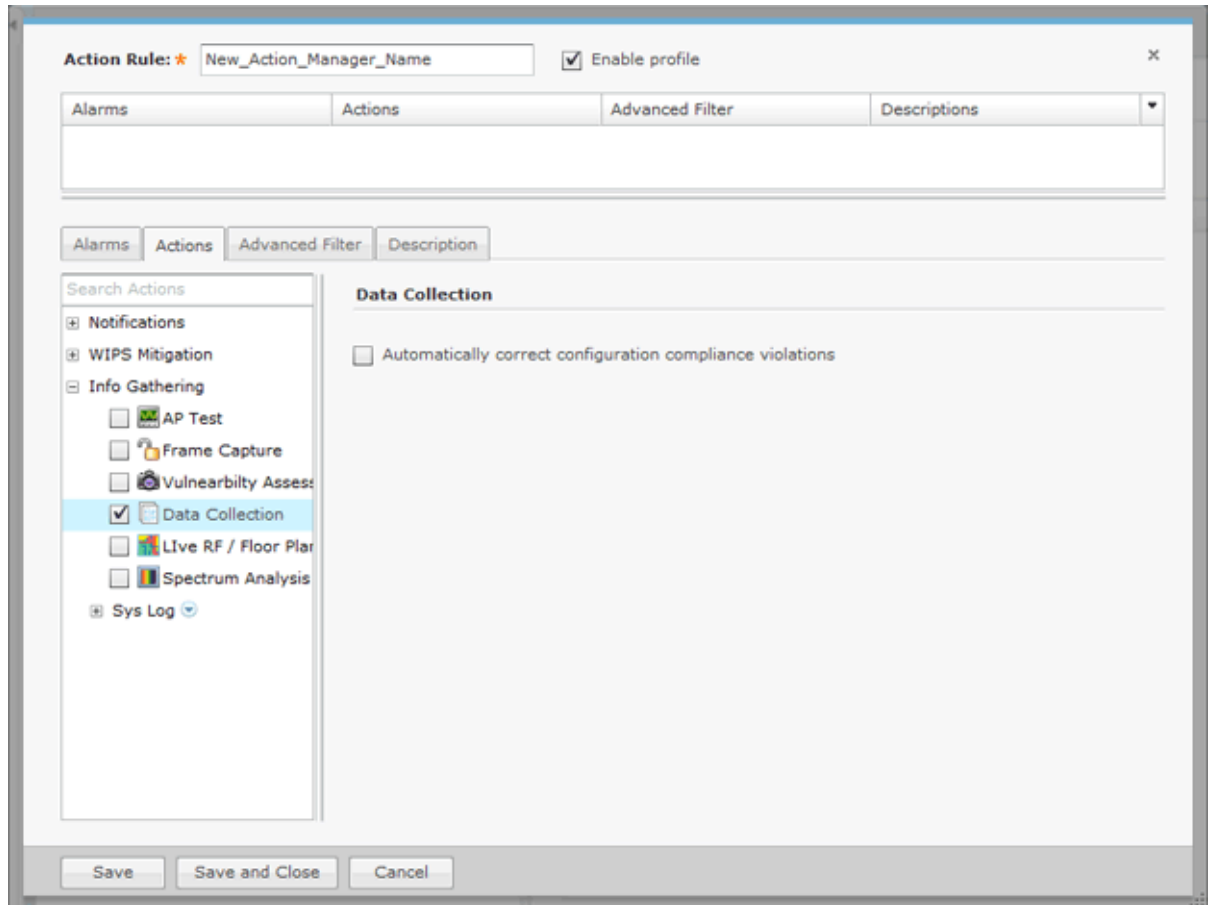
Field	Description
Profile	Select an assessment profile from the drop-down menu. The Edit button can be used to modify the assessment profile. For more information on assessment profiles, refer to the for Vulnerability Assessment section in the Security chapter.

Once you enable a Vulnerability Assessment action rule for BSSs, a vulnerability assessment will only start when AirDefense 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

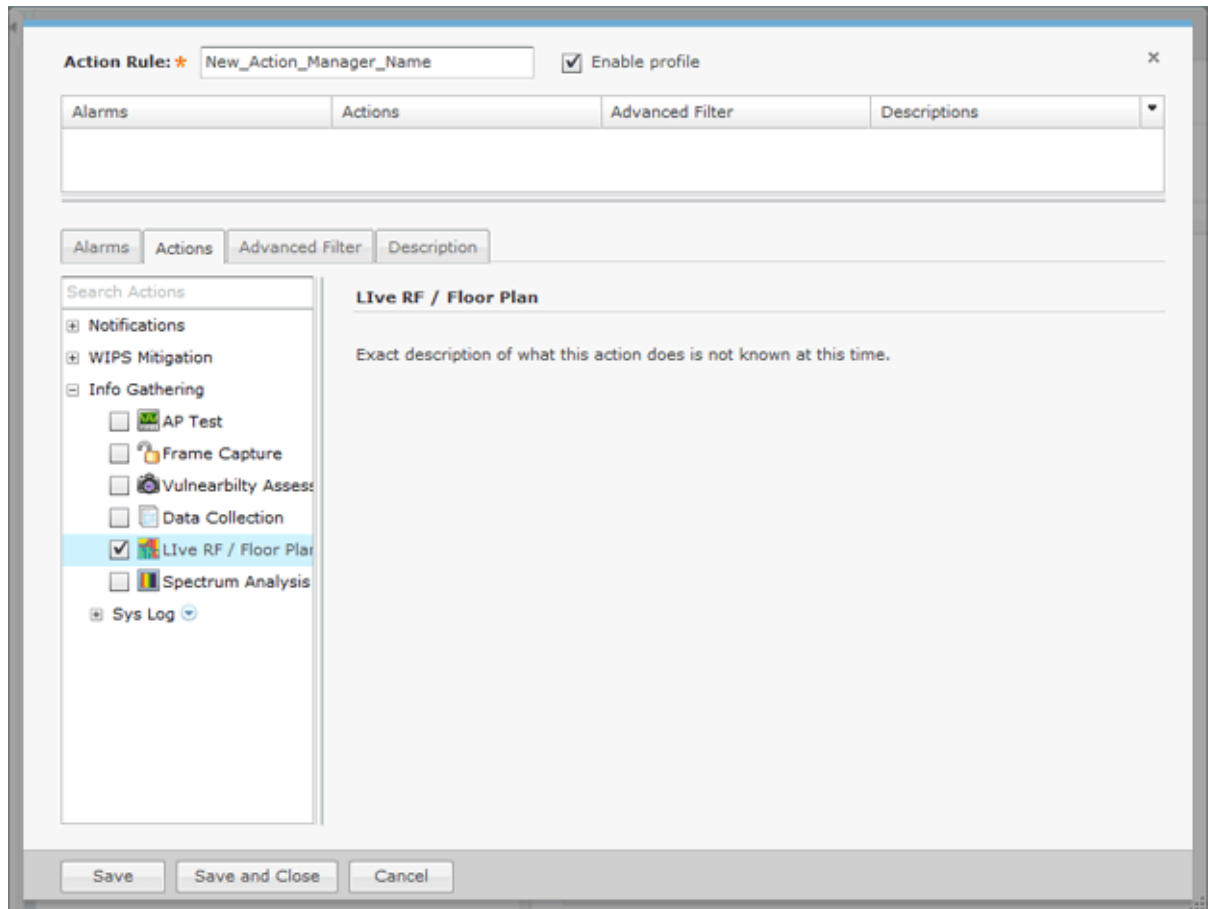


Note

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.

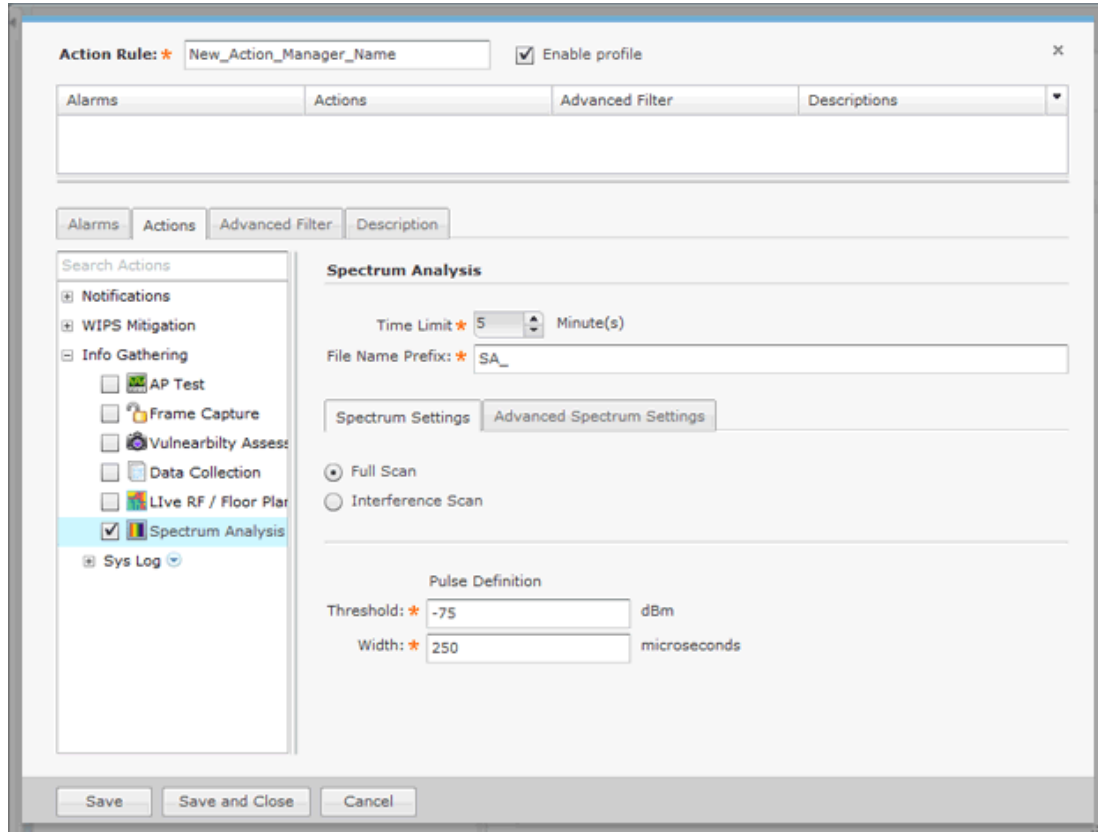
Spectrum Analysis



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 Spectrum Settings .
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

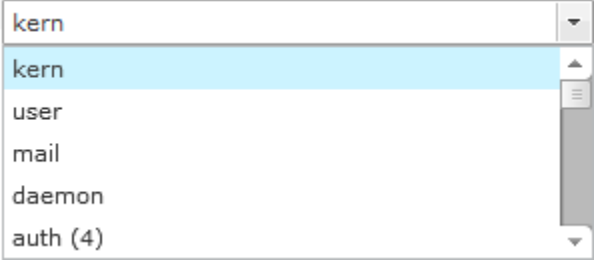
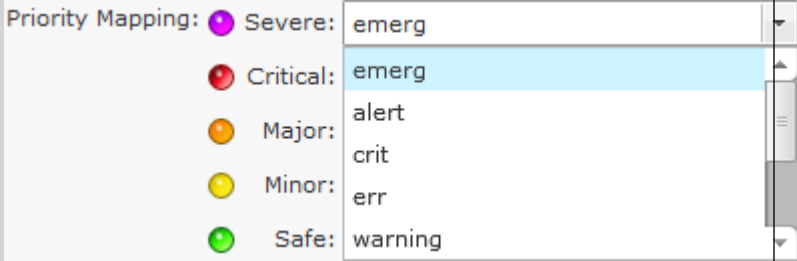
The Sys Log action sends an alarm notification to your Sys Log server if the conditions defined in the filter are met. To select the Sys Log action, select **Info Gathering > Sys Log > Sys Log** from the **Search Options**.

The screenshot shows a configuration window for an 'Action Rule' named 'New_Action_Manager_Name'. The 'Sys Log' action is selected in the left sidebar. The main configuration area includes the following fields:

- Server Address: *
- Syslog Port: * 514
- Facility: kern
- Format: Syslog
- Email Send Time: On Alarm Activation
- Priority Mapping:
 - Severe: emerg
 - Critical: alert
 - Major: crit
 - Minor: warning
 - Safe: notice

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.

Field	Description
Facility	<p>Specifies a Syslog Facility which is an information field associated with a Syslog message. It is defined by the Syslog protocol. The intent of the facility is to provide an indication as to what part of the system the Syslog message originated.</p> <p>This facility can be very helpful to define rules that split messages, for example, to different log files based on the facility level.</p> <p>Choose a Syslog Facility from the drop-down menu.</p> 
Format	<p>Specifies the format of the notification. At this time, the only option is Syslog.</p>
Email Send Time	<p>Specifies when to send the email by selecting one of the following conditions:</p> <ul style="list-style-type: none"> • On Alarm Activation • On Activation, clear or expire • Every x amount of minutes or hours.
Priority Map	<p>The Priority Map enables you to change the name of the default priorities to an alternate selection. Click on the drop-down menu for the priority you would like to change and choose from the list. For example, if you want to change the priority for Severe, select an option from the Severe drop-down menu.</p> 

Advanced Filter Tab

The Advanced Filter tab allows you to build a custom alarm filter or an expression to use as a alarm filter.



The following options are available:

- [Filter List](#) on page 576
- [Expression Editor](#) on page 579

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 `Channel1` 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 screen shot shows an example of a Filter List.

You can have up to 25 filters. 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:

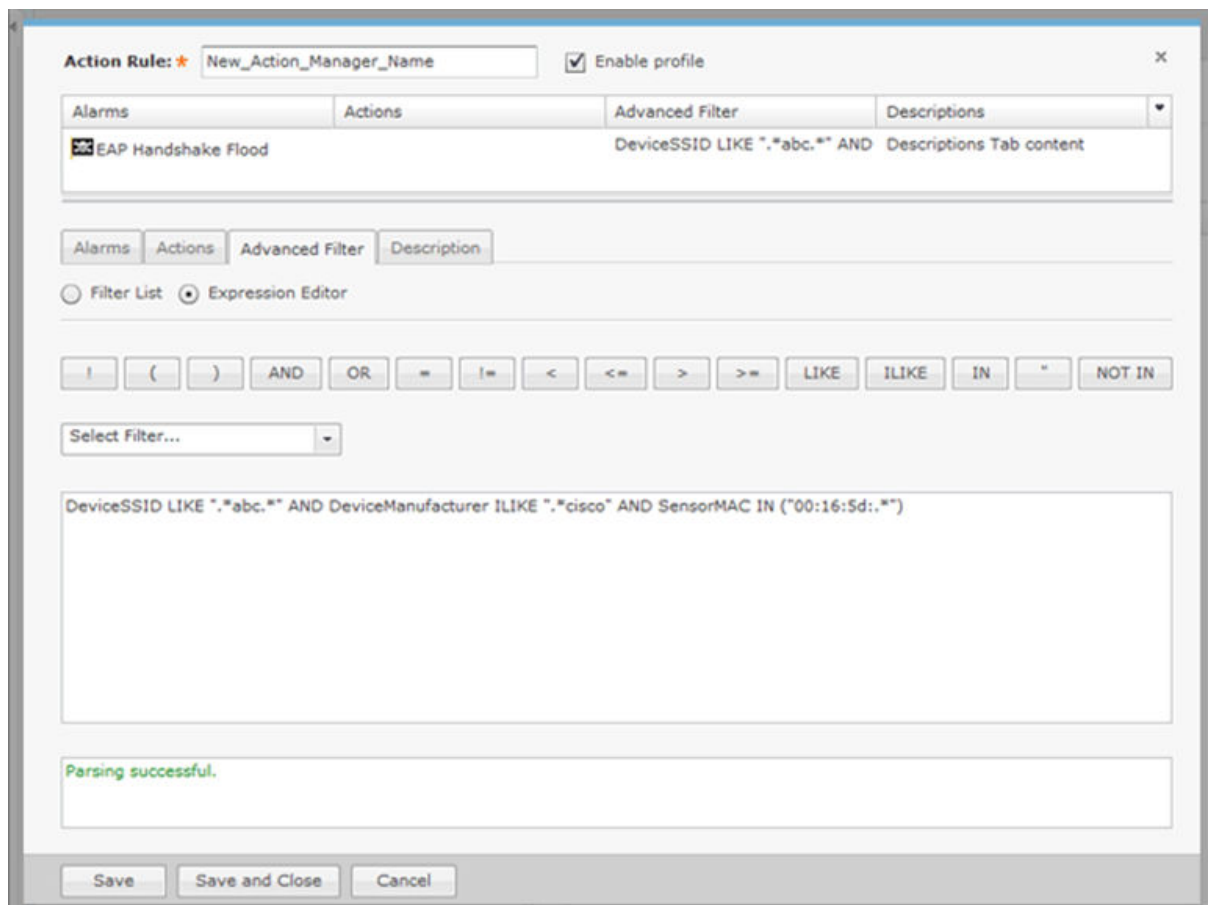
!	Logical NOT operator.
(
)	
AND	Logical operator. Used to combine two expressions
OR	Logical operator. Use to choose one of two expressions
=	Is equal to
!=	Is not equal to
<	Is less than
<=	Is less than or equal to
>	Is greater than
>=	Is greater than or equal to
LIKE	Is similar to, matches some portion (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.



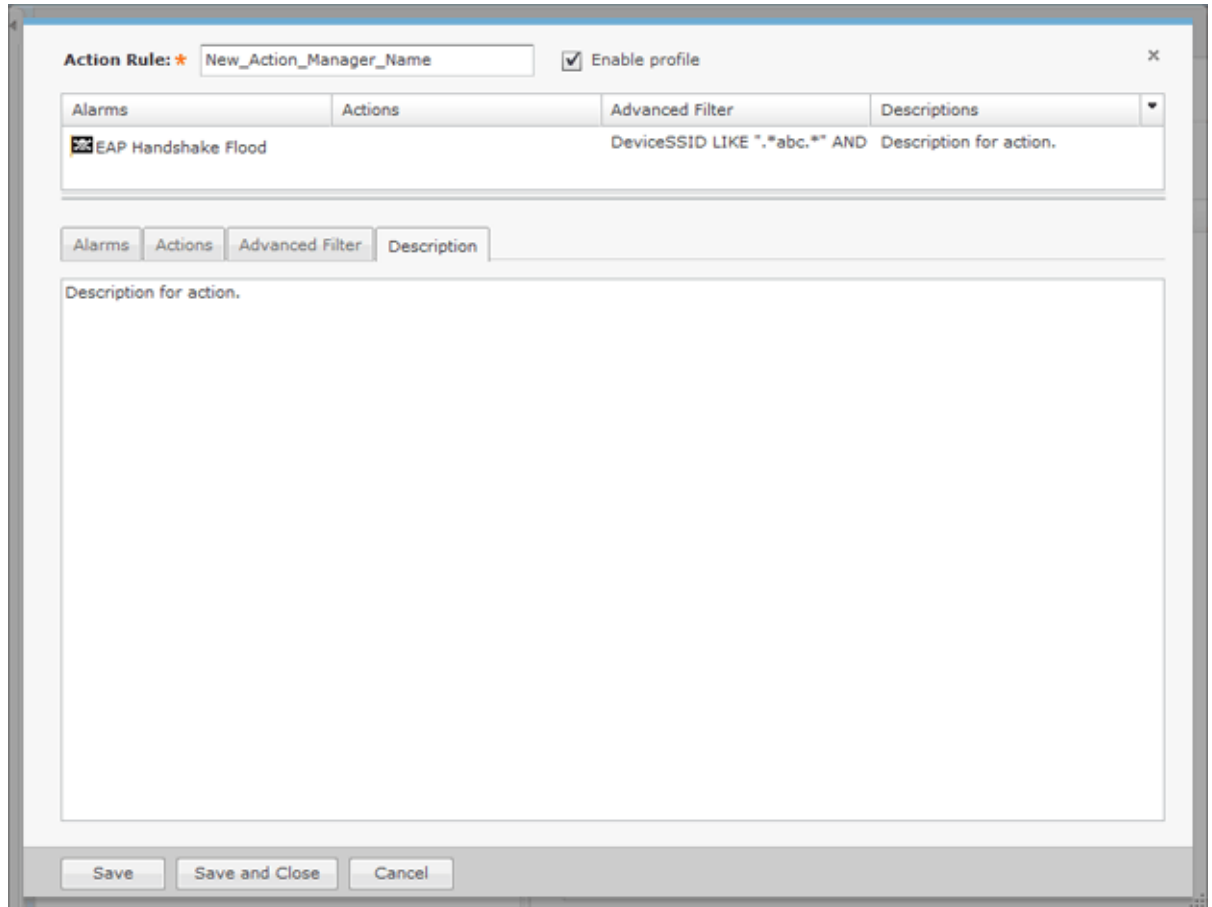
Note the use of wild cards in the screen shot expression:

```
DeviceSSID LIKE *.abc.* AND DeviceManufacturer ILIKE *.cisco* AND SensorMAC IN (\"00:16:5d:.*\")
```

When using wild cards with the operators LIKE, ILIKE, or IN, you must use "*" notation instead of "" notation. If you use the "" notation, the **Action Rule** will fail.

Description Tab

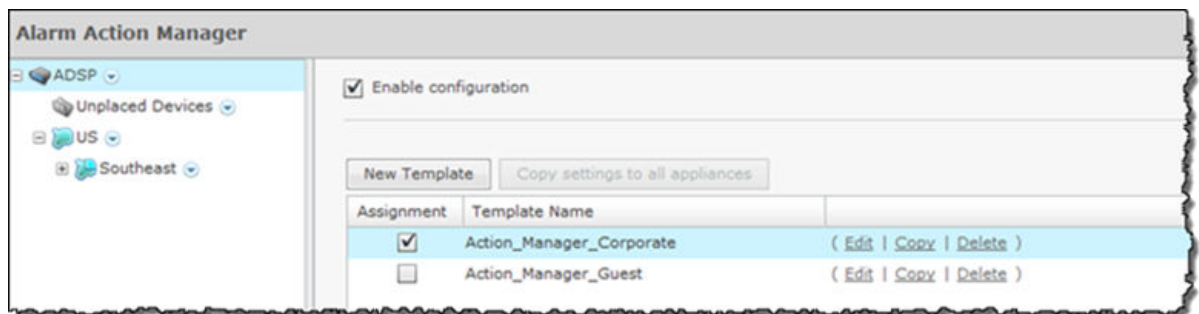
Enter a description of the action on the **Description** tab.



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** check box.



Note


You may select multiple **Alarm Action Manager** templates by checking more than one check box.

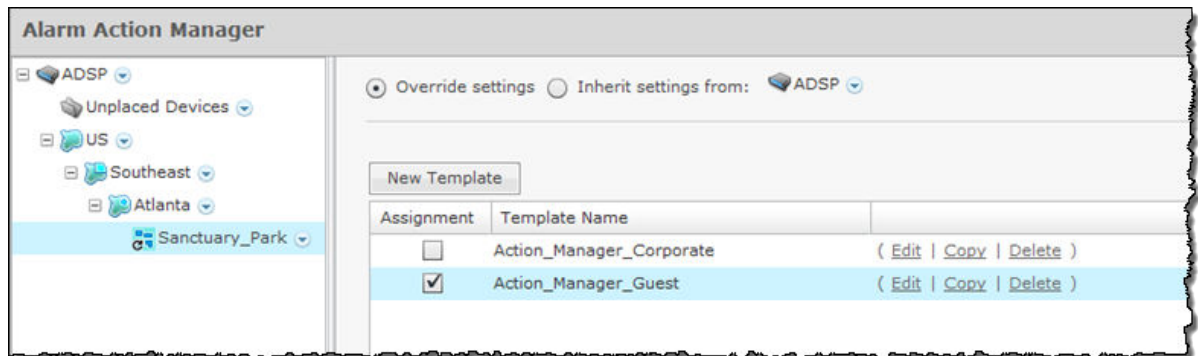
You should always apply an Alarm Action Manager template at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that

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.



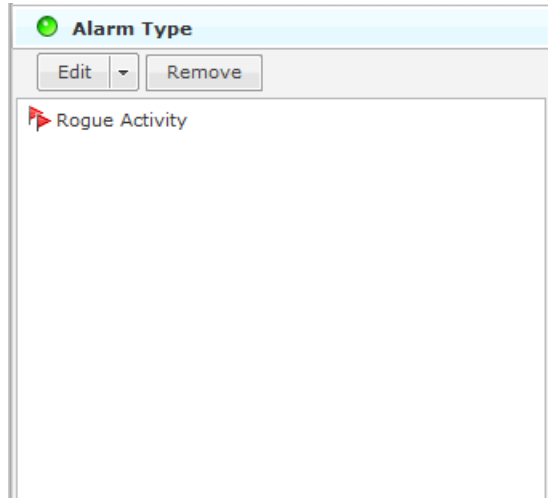
Note

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 a 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.

Alarm Configuration

Alarm type search

- [-] Anomalous Behavior
- [-] Bluetooth
- [-] Exploits
- [-] Infrastructure
- [-] Performance
- [-] Platform Health
- [-] Policy Compliance
- [-] Proximity
- [-] Reconnaissance
- [-] Rogue Activity
 - [-] Authorization Violation
 - [-] Extrusion
 - [-] Rogue Exploit
 - [-] Wired Network Monitoring
 - [-] Known Device No Longer Observed
 - [-] **New Wired Device Detected Known Vendor**
 - [-] New Wired Device Detected Unknown Vendor
 - [-] Wired Device Detected at Different Location
- [-] Vulnerabilities

Name: New Wired Device Detected Known Vendor [Revert to default settings](#) [View Expert Help](#)

Category: Rogue Activity > Wired Network Monitoring

Criticality: Critical(80)

Device Type(s):

Duration:

Enabled

Enabled for unsanctioned devices

Disabled for devices

Escalation

[Add Device](#) [Remove selected](#)

[Advanced Settings](#)

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 <i>Safe, Minor, Major, Critical, and Severe</i> . The new numerical value will be used to calculate the Threat Score .

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

Click **Apply** to save your changes. You can revert back to the original settings by clicking the **Reset** link.

The **Check Synchronization** button is used to check all appliances in the network to ensure they are using the same alarm configuration. (The synchronization feature 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. AirDefense 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 exist due to network configuration, corporate policy, or an inherent flaw in the 802.11 protocol. A malicious user with basic computer skills, a laptop, and a CD drive can obtain various sets of open source tool kits which will transform the laptop into a fully configured wireless attack platform.

As time has progressed these tools kits have become increasingly easier to use while offering an increasingly sophisticated toolset. The bottom line is the wireless attack tools have become accessible to a broader range of users. Because exploits involve active interaction with the wireless network, AirDefense recommends timely action to understand and mitigate the threat to minimize security exposure. Exploits Alarms 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 resource. 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 SSID, whereas a more directed attack will only impact a single station leaving other stations connected to the SSID. 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:

- PresenceA Wireless Client has been detected in the environment or has left the environment.
- Region PresenceA 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.

Alarm Library

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 that uses live data from sensors and WLAN infrastructure to provide real-time visualizations of the environment. The use of live data feeds ensures the visualizations accurately represent environmental changes and transient issues which may not have been captured in the plan or site survey. Visualizations provided allow administrators to troubleshoot wireless connectivity, throughput issues, capacity problems and identify RF interference sources for a floor or entire building. All of this is performed from a central console, so troubleshooting can be performed without having to send administrators out to remote locations. LiveRF also allows runs in the background to automatically detect network problems based on thresholds defined by the administrator. The alarms in this category are a result of these proactive network problem detection capabilities.
- Potential Interference Sources - 802.11 devices operate in unlicensed frequency ranges, 2.4GHz for b/g and 5GHz for a-channels and are subject to interference from other devices utilizing the same frequency. Common examples of these devices are: microwave ovens, Bluetooth devices, baby monitors, cordless telephones, Zigbee devices, non 802.11 wireless security cameras and wireless USB devices (wireless keyboard and mouse).
- RF Spectrum Analysis - 802.11 Wireless networks operate in unlicensed frequencies. This includes any non 802.11 transmitters such as cordless phones, and Bluetooth share frequency spectrum with 802.11 wireless networks. A non 802.11 transmitter can impact the network by causing interference. Identifying the source is difficult with standard 802.11 hardware as these simply appear as noise. Spectrum Analysis can be used to identify the source of the interference and judge the impact the interferer will have on the wireless network.
- Utilization - 802.11 Wireless networks operate in a medium where all devices share the available bandwidth. Any single device is capable of impacting performance by using all available wireless resources. AirDefense Enterprise monitors over 50 performance related utilization statistics for the authorized wireless devices, to ensure that utilization related performance problems are discovered before causing significant wireless network performance degradation.

Alarm Library

To view a list of Performance Alarms for each alarm sub-type, go to **Configuration > Operational Management > Alarm Configuration**, open **Performance**, and then open the alarm sub-type to see all the alarms associated with the sub-type.

Platform Health Alarms

Platform Health Alarms alert you to events that provide information about the state of the AirDefense Services Platform and the Sensors which report back to the appliance. Platform Health Alarms are broken down into the following three sub-types:

- License Manager - License events provide information about the features and functionality in the AirDefense that require a license to operate.
- Platform - Platform events provide operational and health information about the AirDefense appliance.
- Sensor - Sensor events provide operation and health information about the Sensors that are reporting back to the AirDefense 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 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.

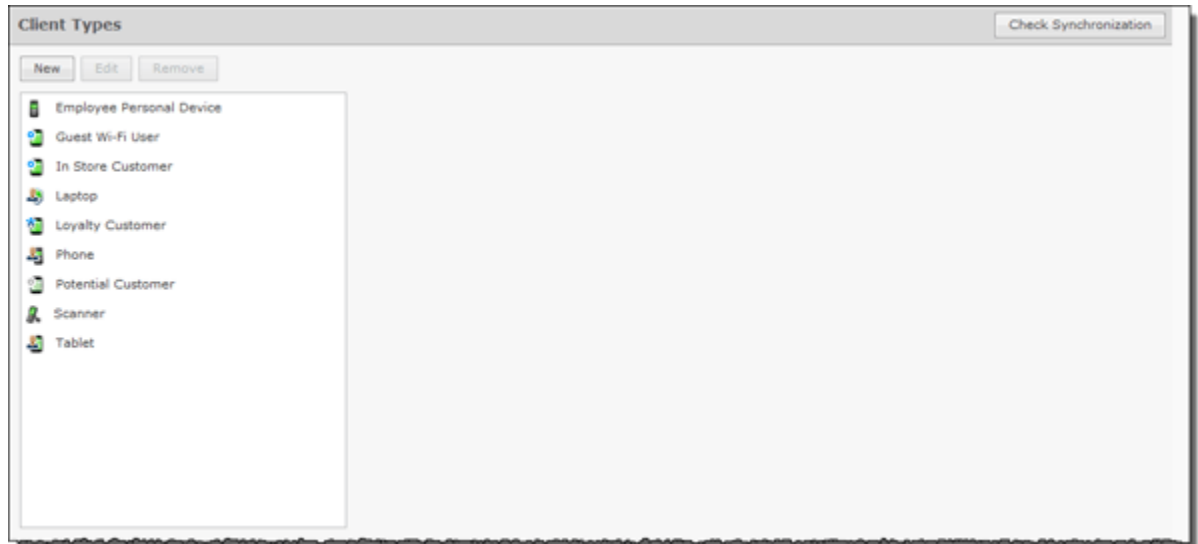
Alarm Library

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:

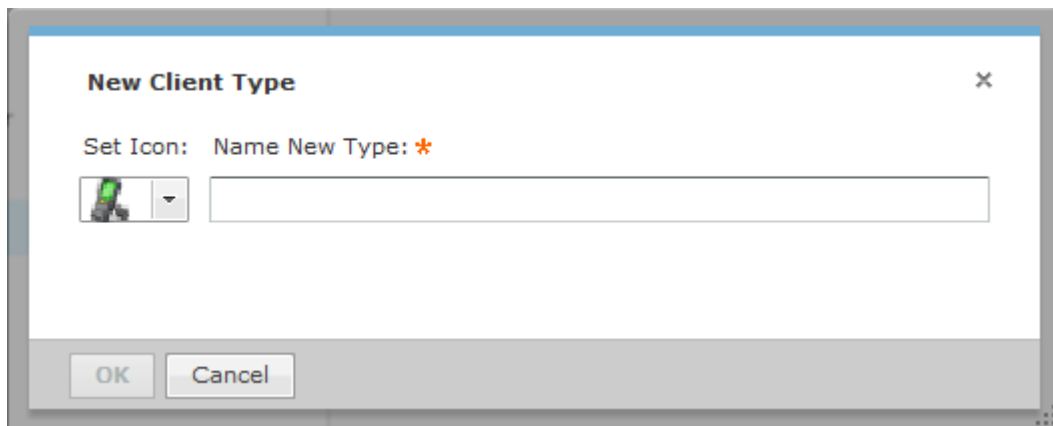
- Add new client types to your system.
- Edit existing client types to change the icon or name.
- Remove existing client types from your system.



Manage Client Types

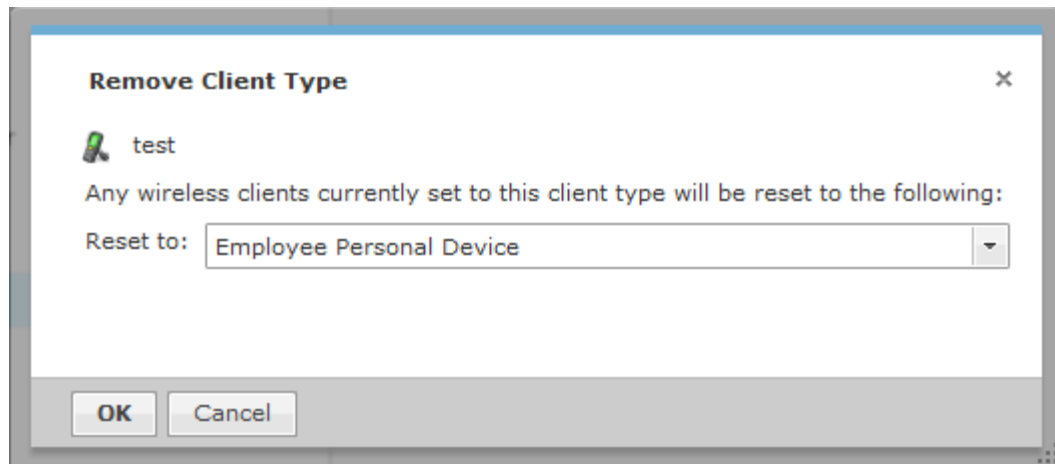
To manage Client Types:

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



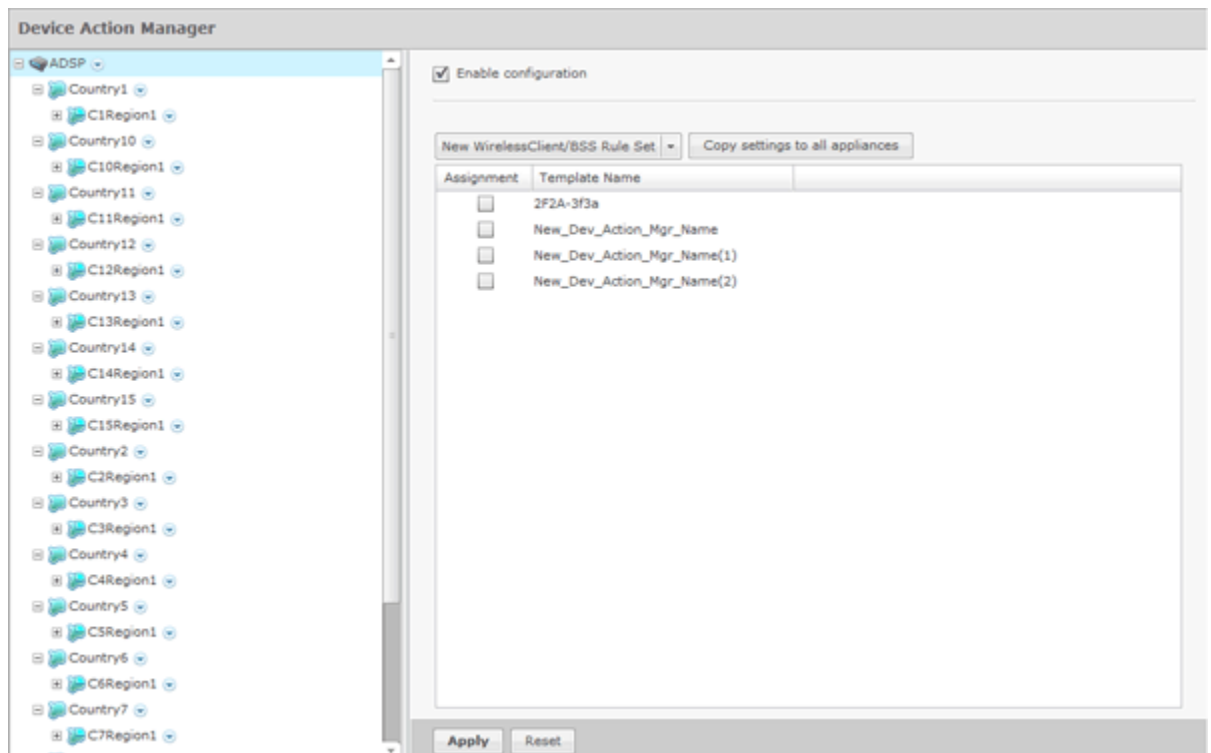
2. Select an icon by choosing an icon from the **Set Icon** drop-down menu, type in a new name in the **Name New Type** field, and then click **OK**.
A new Client Type is created.
3. To edit a client type select (highlight) the client type and then click the **Edit** button. You can change the client type icon or the client type name.

4. 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. AirDefense 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_IXName
- DeviceAuthentication
- DeviceClassification
- DeviceClassificationInherit
- DeviceClientType
- DeviceEncryption
- DeviceFirstPolled
- DeviceFirstSeen
- DeviceIP
- DeviceLastPolled
- DeviceLastSeen
- DeviceMAC
- DeviceManufacturer
- DeviceName
- DevicePolledID
- DevicePolledName
- 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.

WirelessClient / BSS / Unknown Devices Rule Set

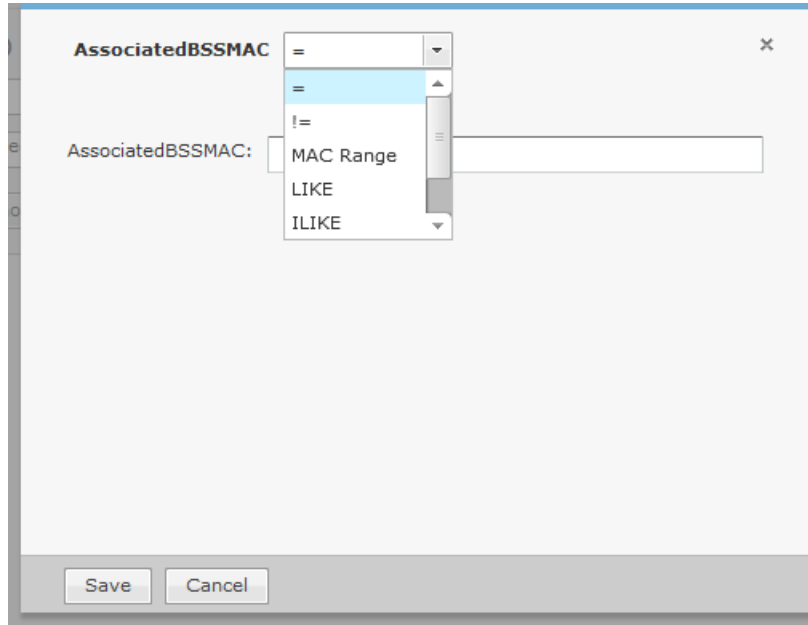
Name: * (Limit: 100 rules)

Rule_01 Enable

Filter(s)	Action(s)
When <input type="text" value="All"/> of these filters are met... If <input type="text" value="AssociatedBSSMAC"/> <input type="button" value="Edit"/> ×	Perform the following action(s): <input type="text" value="Select action..."/> <input type="button" value="Add Another"/> (limit: 5 actions)

AssociatedBSSIP
AssociatedBSSMAC
 AssociatedBSSName
 AssociatedBSSVendorPrefix
 Channel
 ConnectedToWired
 Device802_1XName
 DeviceAuthentication
 DeviceClassification
 DeviceClassificationInherit
 DeviceClientType

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.

WirelessClient / BSS / Unknown Devices Rule Set

Name: * (Limit: 100 rules)

Rule_01 Enable

Filter(s)

When of these filters are met...

If

And

(limit: 25 filters)

Action(s)

Perform the following action(s):

(limit: 5 actions)

You can remove a statement by clicking the **X** next to the statement.

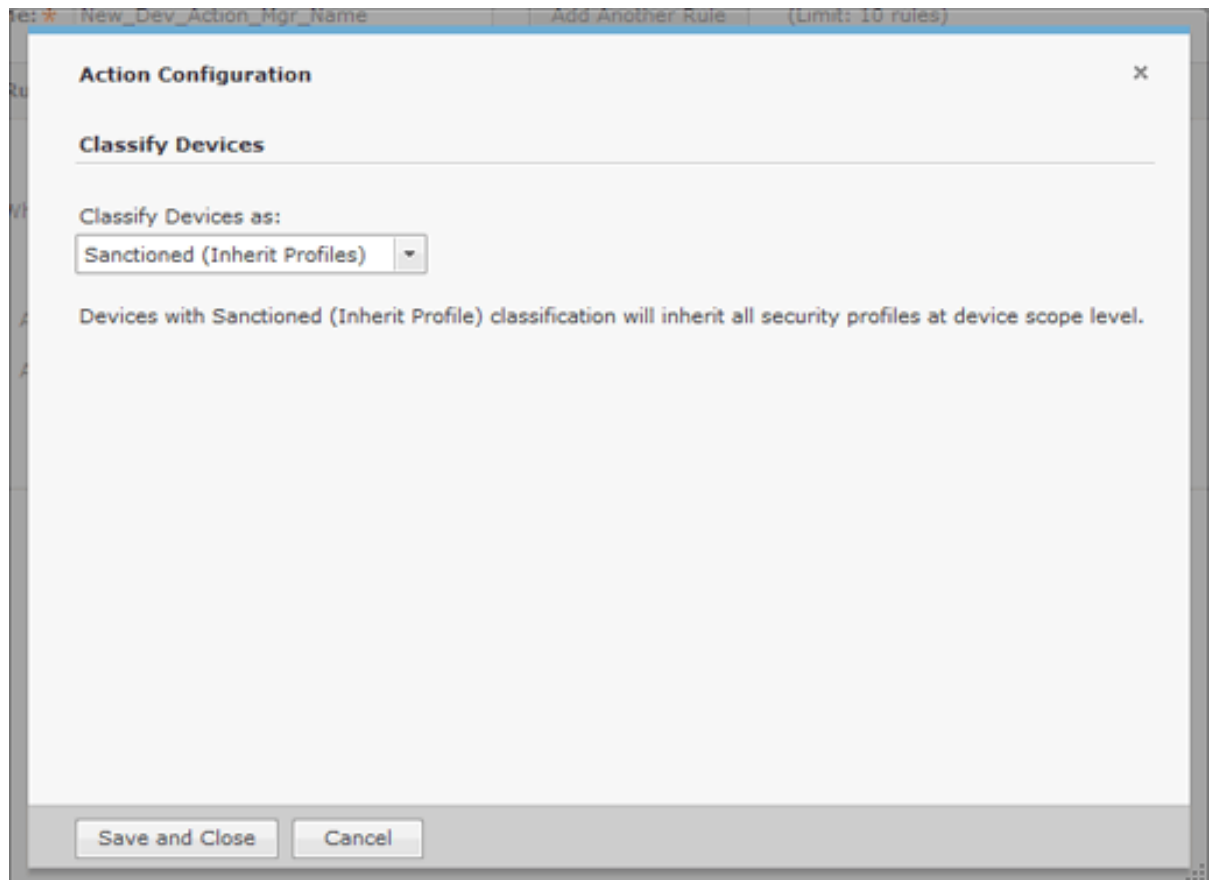
Actions

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.

WirelessClient / BSS / Unknown Devices Rule Set

Name: * New_Dev_Action_Mgr_Name Add Another Rule (Limit: 100 rules)

Rule_01 Enable Click to add/edit description.

Filter(s)

When All of these filters are met...

If DeviceClientType Edit x

And Associated Edit x

And DeviceSSID Edit x

Add Another (limit: 25 filters)

Action(s)

Perform the following action(s):

Port Suppression Edit x

Add Another (limit: 5 actions)

Save Save and Close Cancel

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.

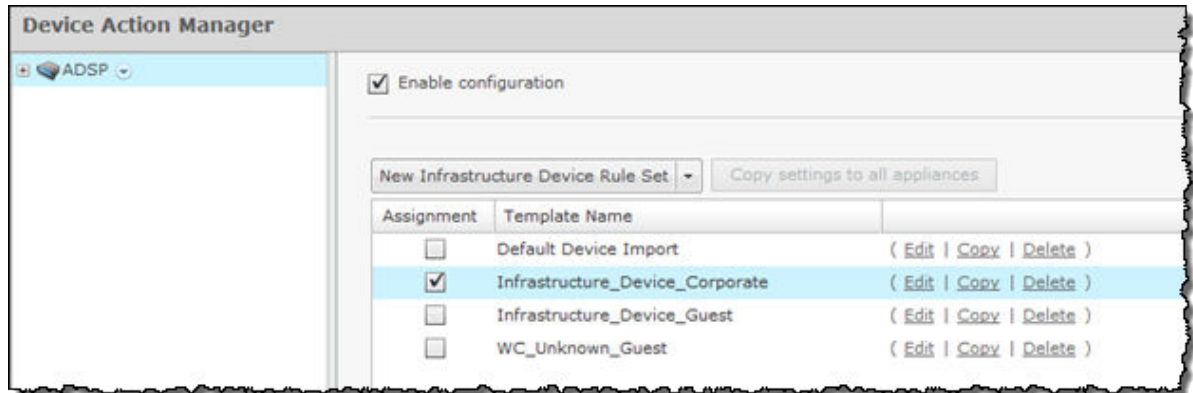
Actions

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).
- EMail - Sends information about an alarm via email to a recipient if the conditions defined by the filter(s) are met.

Applying a Device Action Manager Template

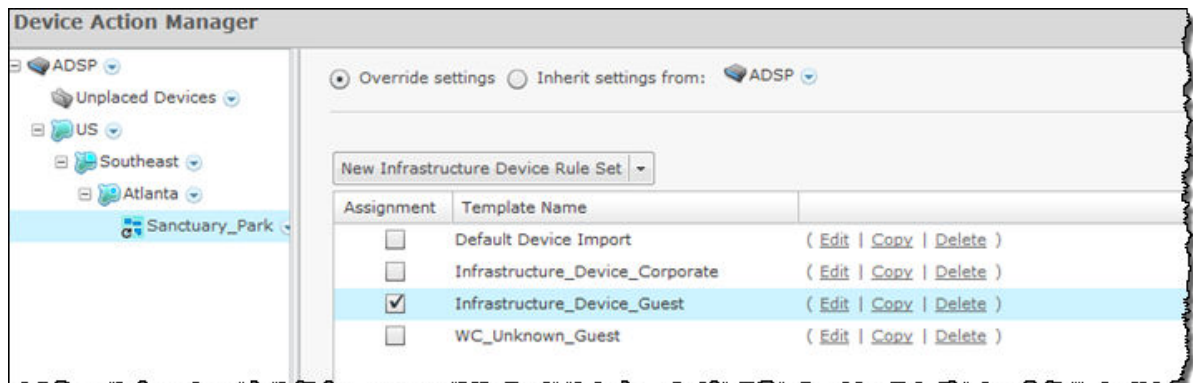
Once you have defined **Device Action Manager** templates, to use them, you must apply them to your system.




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 AirDefense 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 AirDefense 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 AirDefense 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 AirDefense uses to display devices in the Network tab. For your convenience, a table is displayed listing the devices seen on your network.

Sensed devices last seen observations					Age out settings	
BSSs					You may enter a value between 1 hour and 7 days.	
	Sub Totals	Last 24 Hrs	Last 1-7 Days	Over 7 Days	Unsanctioned BSSs	<input type="text" value="3"/> Day(s) ▾
Sanctioned	9	9	0	0	Ad-Hoc BSS	<input type="text" value="4"/> Hours ▾
Unsanctioned	954	829	125	0	Unsanctioned Wireless Clients	<input type="text" value="3"/> Day(s) ▾
Neighbor	0	0	0	0	Unsanctioned Unknown	<input type="text" value="2"/> Day(s) ▾
Sub Totals	963	838	125	0		
Wireless Clients						
	Sub Totals	Last 24 Hrs	Last 1-7 Days	Over 7 Days		
Sanctioned	0	0	0	0		
Unsanctioned	251	190	61	0		
Neighbor	0	0	0	0		
Sub Totals	251	190	61	0		
Unknown						
	Sub Totals	Last 24 Hrs	Last 1-7 Days	Over 7 Days		
Sanctioned	0	0	0	0		
Unsanctioned	775	648	127	0		
Sub Totals	775	648	127	0		
All Devices	1,989	1,676	313	0		

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

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

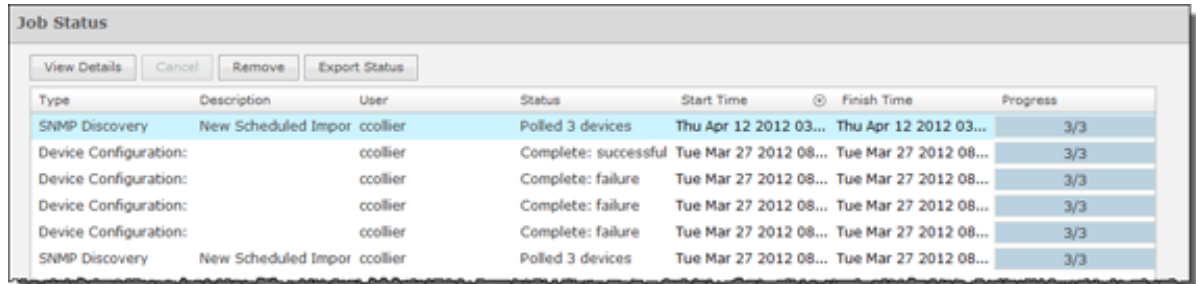
Values are specified in hours or days with a minimum of 1 hour and a maximum of 7 days. If you enter an illegal value, the field is highlighted by a red box.

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.



The screenshot shows a window titled "Job Status" with buttons for "View Details", "Cancel", "Remove", and "Export Status". Below the buttons is a table with the following data:

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

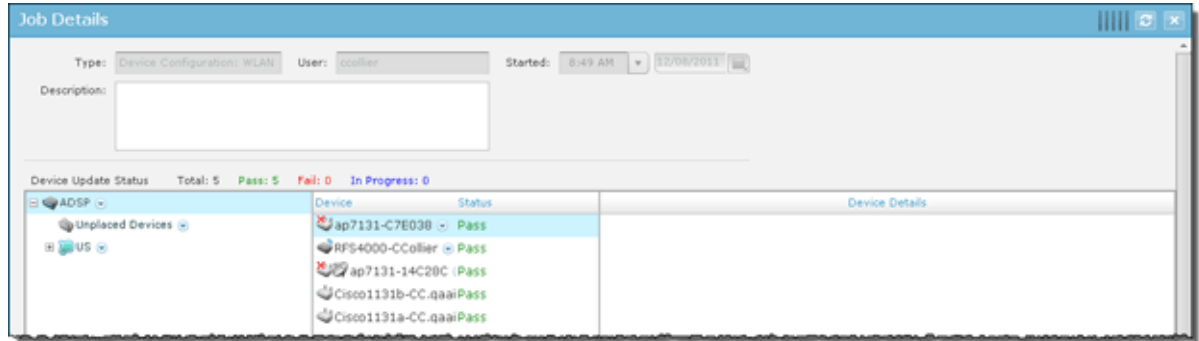
Job statuses are displayed in table format with seven columns.

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

Jobs more than 7 days old will age out of the system and will not be displayed. Jobs may be canceled by selecting (highlighting) the job and clicking the **Cancel** button. Jobs may be removed from the **Job Status** list by selecting (highlighting) the job and clicking the **Remove** button.

You can export a job's status by selecting (highlighting) the job and clicking the **Export Status** button. A window displays where you can name the file and specify where to save it.

You can view job details by clicking the **View Details** button.



The **Job Details** overlay displays all the information displayed in Job Status plus some additional details such as:

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

While viewing job details, you can:

- Export the job's status to a file on your workstation using the **Export Status** button.
- Cancel the job using the **Cancel Job** button.
- Save any changes such as changing the job description using the **Save Changes** button.

Close the Job Details overlay by clicking the **Close (X)** button.

Location Based Services

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 AirDefense to track devices by location. To manage your LBS profiles, go to **Configuration > Operational Management > Location Based Services** to display the LBS screen.

Location Based Services

Override settings Inherit settings from: **ADSP**

New Template

Assignment	Template Name	
✓	Default LBS Profile	(Edit Copy Delete)

Apply Reset

Add a New LBS Profile

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

A LBS Profile consists of **Client Based Settings** and **Global LBS Settings** configuration.

- [Client Based Settings](#) on page 615
- [Global LBS Settings](#) on page 618

Client Based Settings

Select the **Client Based Settings** tab to define your LBS profile.

Use the **Copy Settings** button to copy the configuration of the selected **Client type configuration** to other client types. For more information see [Copy Settings](#) on page 615.

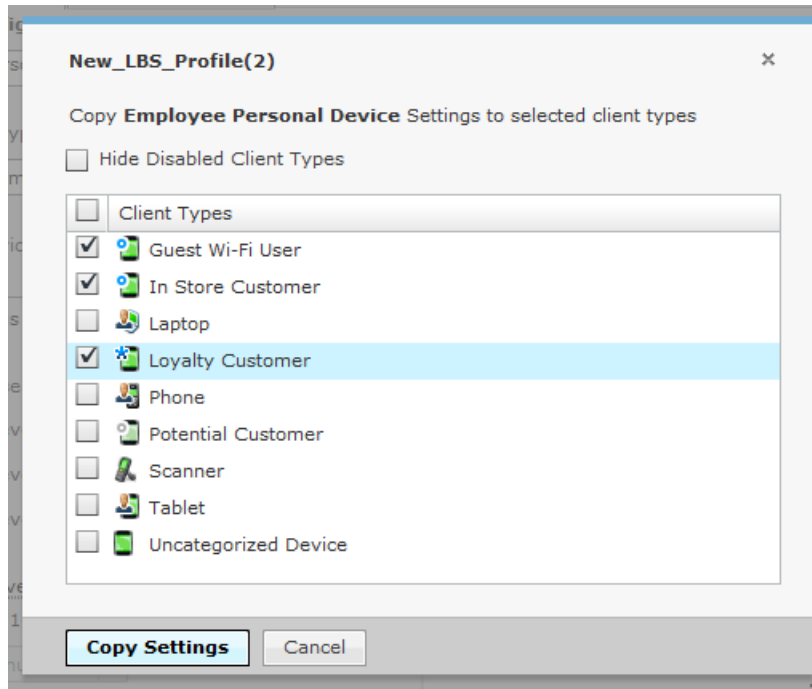
Use the **Set all client type priorities** button to set the tracking and prioritizing the devices in the order of their importance. For more information see [Set Client Type Priorities](#) on page 616.

Select the **Enable Client Type** check box to enable the selected client type configuration. Use the **Priority** drop down list to set the client type priority.

Select the **Only track devices connected to authorized BSSs** check box to ignore devices that are connected to unauthorized BSSs.

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 their check boxes.

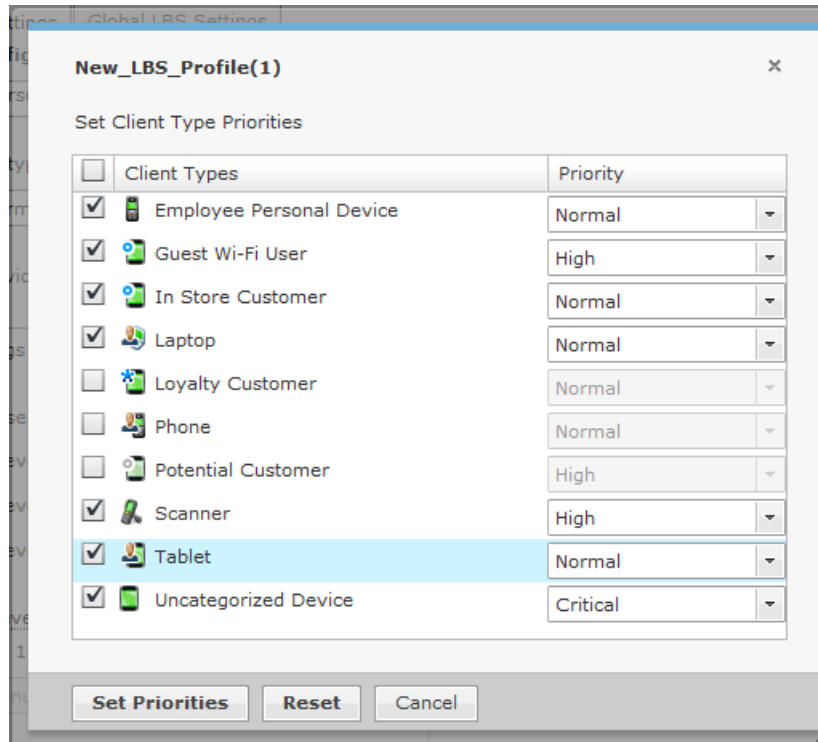


When finished selecting, click **Copy Settings** to copy the settings and return to the previous dialog box.

Set Client Type Priorities

Use the **Set all client type priorities** button to set the default priorities for the different client types.

Click the **Set all client type priorities** button 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 check box of the client type you want to prioritize or select the check box at the top of the list for all clients types. If you do not wish to track a certain client type, leave the check box unchecked 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. Use the **Reset** button to reset your priorities to their previous 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 LBS Profile

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 AirDefense appliance level. You can also apply the LBS settings to all appliances in your system at the same time.

Edit LBS Profiles

You 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 AirDefense 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.

Enable configuration

Assignment	Template Name	
<input checked="" type="radio"/>	Default LBS Profile	(Edit Copy Delete)
<input type="radio"/>	New_LBS_Profile	(Edit Copy Delete)
<input type="radio"/>	New_LBS_Profile(1)	(Edit Copy Delete)
<input type="radio"/>	New_LBS_Profile(2)	(Edit Copy Delete)

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

Successfully saved configuration

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 AirDefense appliance icon to reveal the other levels.

Location Based Services

ADSP

- Country1
 - C1Region1
 - C1R1City1
 - C1R1City2
 - C1R1City3
- Country10
- Country11
- Country12
 - C12Region1
- Country13
 - C13Region1
- Country14
 - C14Region1
- Country15
 - C15Region1
- Country2
 - C2Region1
- Country3
 - C3Region1
- Country4
 - C4Region1
- Country5
 - C5Region1

Override settings Inherit settings from: Country1

New Template

Assignment	Template Name	
<input type="radio"/>	Default LBS Profile	(Edit Copy Delete)
<input checked="" type="radio"/>	New_LBS_Profile	(Edit Copy Delete)
<input type="radio"/>	New_LBS_Profile(1)	(Edit Copy Delete)
<input type="radio"/>	New_LBS_Profile(2)	(Edit Copy Delete)

Apply Reset

For example, in the above screen shot, the LBS profile for AirDefense 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 Subscriptions

Enable configuration

New Template Copy settings to all appliances

Assignment	Template Name
<input checked="" type="checkbox"/>	New_LSP

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.

Location Subscriptions

Enable configuration

Assignment	Template Name
<input checked="" type="checkbox"/>	New_LSP

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.

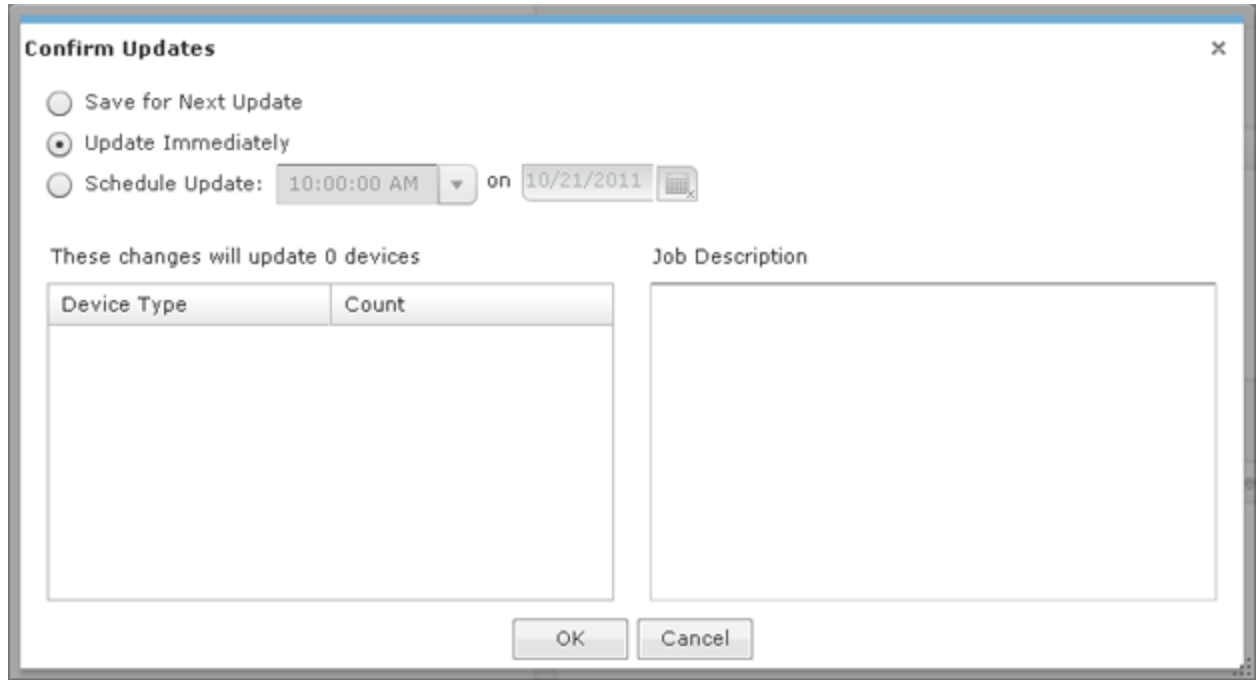
The **Copy settings to all appliances** button will copy the defined Location Subscriber Profiles and all profile assignments to all appliances in your system.



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.



The image shows a 'Confirm Updates' dialog box with the following elements:

- Three radio buttons: 'Save for Next Update', 'Update Immediately' (which is selected), and 'Schedule Update:'. The 'Schedule Update' option is followed by a time dropdown set to '10:00:00 AM' and a date field set to '10/21/2011'.
- A status message: 'These changes will update 0 devices'.
- A table with two columns: 'Device Type' and 'Count'. The table is currently empty.
- A text area labeled 'Job Description'.
- 'OK' and 'Cancel' buttons at the bottom.

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

Updates to 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

To add a new Location Subscription Profile:

1. Click **New Template** to add a new profile.

2. 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.

3. Click **Save and Close** to save the profile and exit.
 You can also click **Save** to save the profile and leave it open for further modifications.
 Click **Cancel** to cancel any changes that are not saved and exit the profile.

Connection Settings

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 and Region Events

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.

Field	Description
Select all Sources	<p>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.</p> <p>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.</p>
Select all Events	<p>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.</p>
Select all Client Types	<p>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.</p>
Filter by Wireless Clients	<p>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.</p>
Filter by Region	<p>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.</p>

Presence Events

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.
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

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.

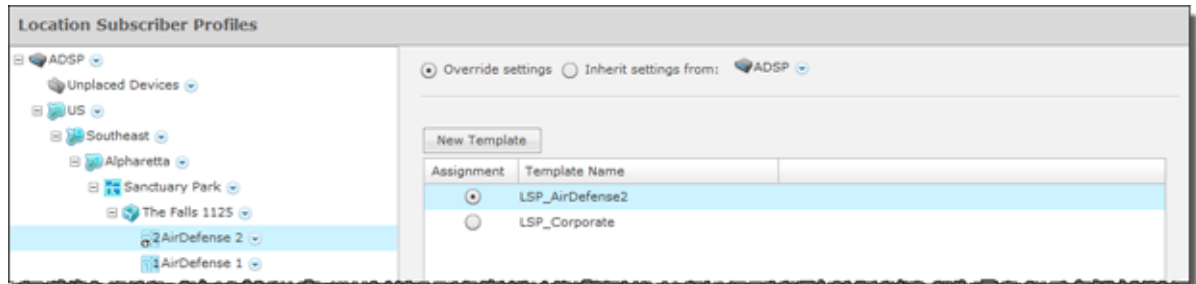
You should always apply a Location Subscriber Profile at the appliance level. When you do, the profile is inherited for all the other levels. Then, if you have a level that needs a different Location Subscriber Profile, you can apply that profile to that level. For example, in the above screen shot, the Location Subscriber Profile for AirDefense 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 AirDefense 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.

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:

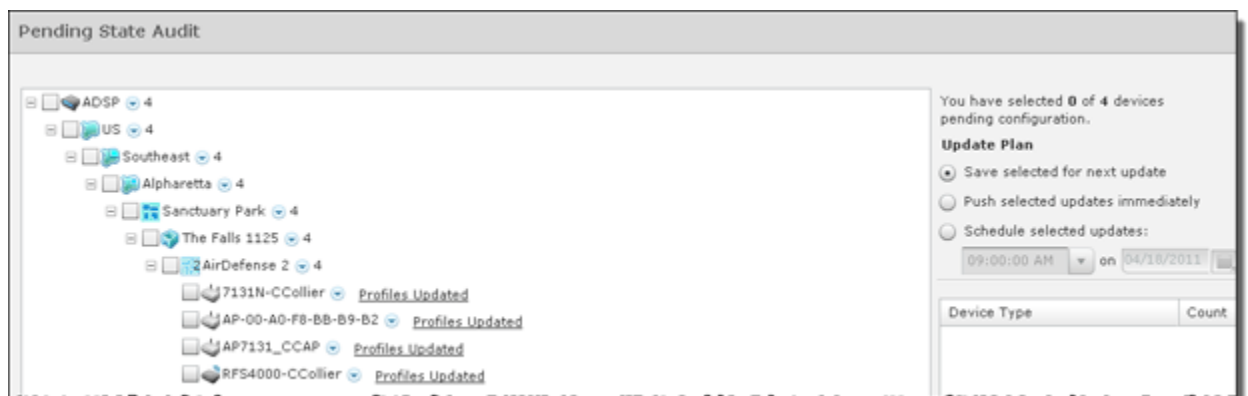
Pending State - Audit



Note

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

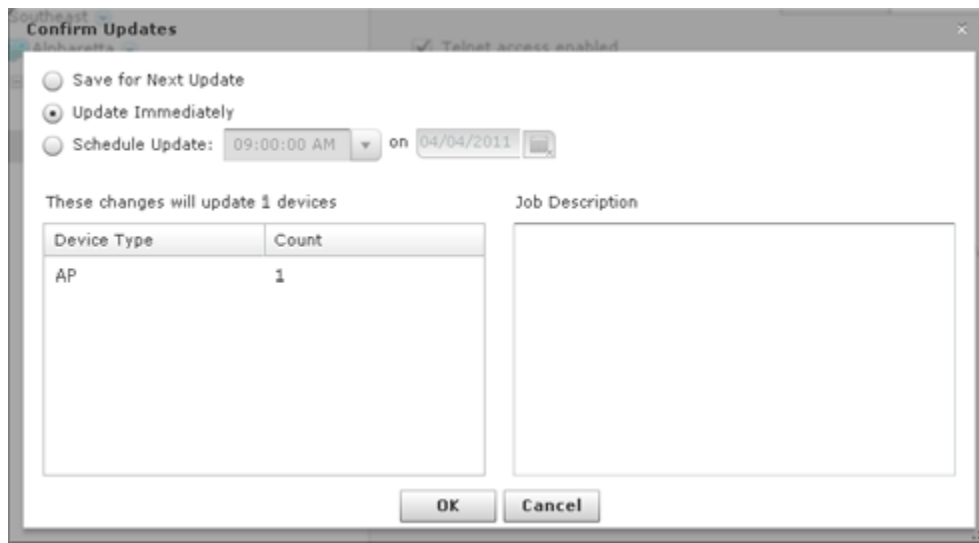
Pending State Audit is used to identify any devices that are in a pending state. Devices in a pending state have been scheduled or need to be scheduled for configuration.



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

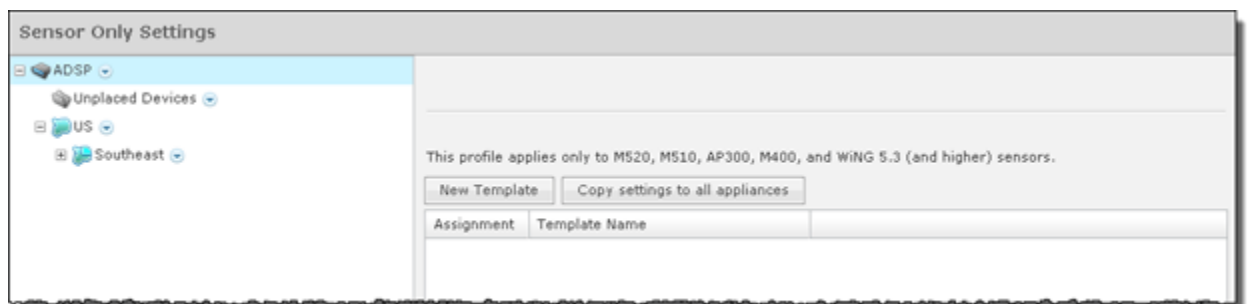
You have the option to save for the next update, update immediately or update later. If you choose to update later, you must supply a date and time. You can supply a description that will help identify the update later using **Job Status** under **Operation Management**. A list of device types along 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 (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.

Assignment	Template Name	
<input type="checkbox"/>	New_sensor_settings_pro	(Edit Copy Delete)

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.

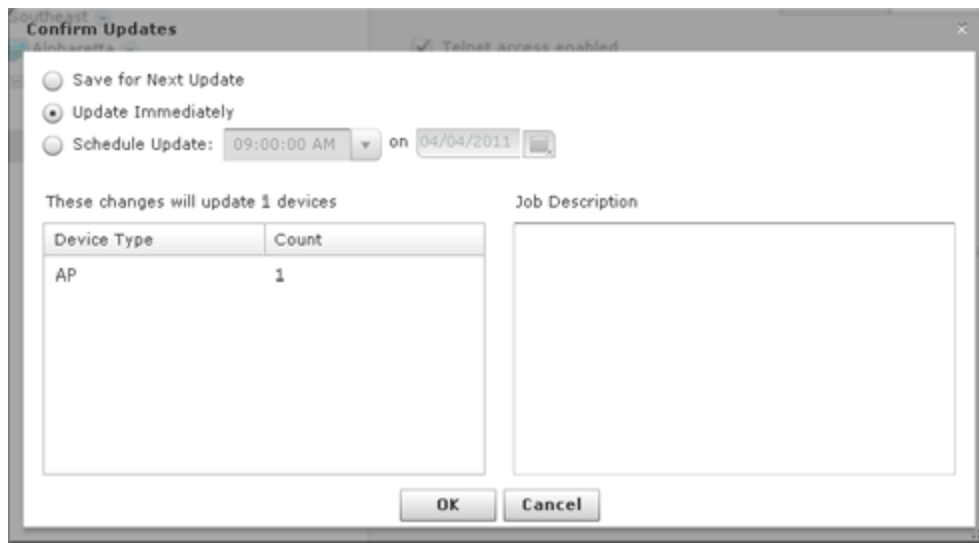
The **Copy settings to all appliances** button will copy the defined Sensor Only Settings profiles and all profile assignments to all appliances in your system.



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:

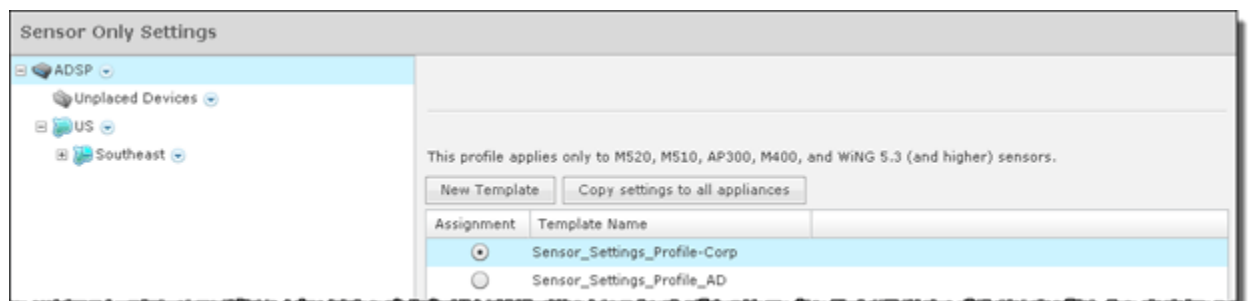
Field	Description
Primary Appliance	Specifies the IP address of the primary appliance.
Secondary Appliance	Specifies the IP address of the secondary appliance.
Sensor Admin Password	Specifies the admin password for your Sensors. Supplying this password is mandatory.
Sensor Monitor Password	Specifies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




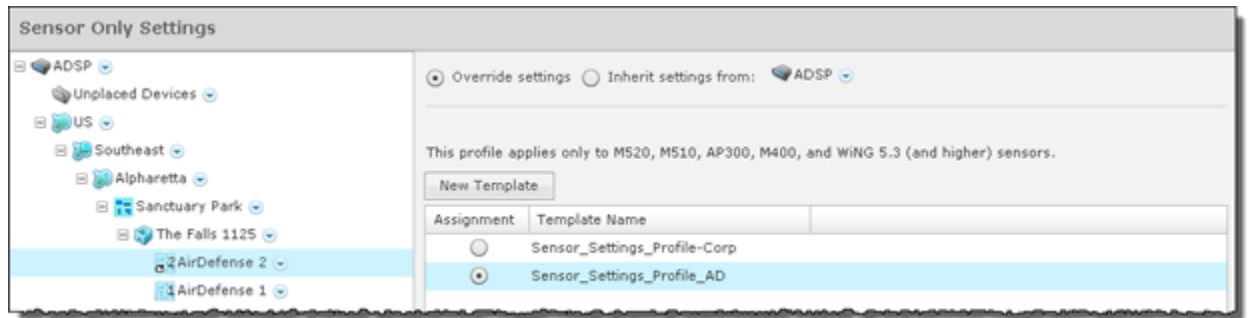
You should always apply a Sensor Only Settings Profile at the appliance level. When you do, the profile is inherited for all the other network levels. Then, if you have a level that needs a different Sensor Only Settings Profile, you can apply that profile to that level. For example, in the above screen 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**.

Channel	802.11N Extension	Scan Weight
Ch 1(2.412 GHz)	Upper	1
Ch 2(2.417 GHz)	Upper	1
Ch 3(2.422 GHz)	Upper	1
Ch 4(2.427 GHz)	Upper	1
Ch 5(2.432 GHz)	Upper	1
Ch 6(2.437 GHz)	Lower	1

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 screenshot shows the 'Scan Settings' tab in the Appliance Manager. It includes the following options:

- Enable Air Termination
 - Enable Fast Termination
 - Rate: 30 Second(s).
- Enable Background SA Scan
- Enable WEP Cloak
- Enable Adaptive Scan

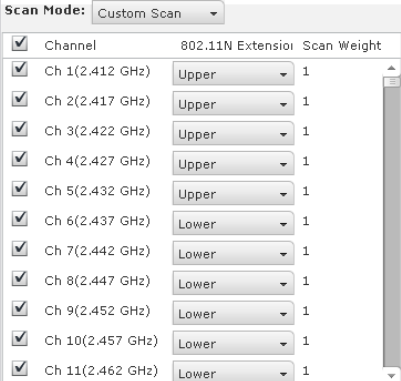
- Enable Location Tracking RSSI Scan
 - Refresh Rate: 1 Second(s).

Scan Mode: Default Scan

Channel	802.11N Extension	Scan Weight
Ch 1(2.412 GHz)	Upper	1
Ch 2(2.417 GHz)	Upper	1
Ch 3(2.422 GHz)	Upper	1
Ch 4(2.427 GHz)	Upper	1
Ch 5(2.432 GHz)	Upper	1
Ch 6(2.437 GHz)	Lower	1

The appliance level can be expanded to show the lower levels. If a lower level is selected from the tree, its scan settings are displayed on the right. If the scan settings are inherited from a parent level, the options are read only and grayed-out. If the scan settings are overridden, the options have read/write permission and can be edited. All tree levels that do not inherit the same settings as the selected node are displayed with gray text. The following options are available:

Feature/Function	Description
Enable Air Termination	Air Termination lets you terminate the connection between your wireless LAN and any 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
<p>Enable Location Tracking RSSI Scan</p>	<p>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.)</p>
<p>Scan Mode</p>	<p>You can choose channels to monitor by selecting one of the following scan modes:</p> <ul style="list-style-type: none"> • <code>Default Scan</code> - the table displays the channels that will be scanned and is not editable. • <code>Extended Channel Scan</code> - the table displays all standard channels plus the extended channels that will be scanned. • <code>Extended and Emergency Channel Scan</code> - the table displays all channels including emergency channels that will be scanned. • <code>Custom Scan</code> - 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.  <p>A scan weight of 1 specifies that the selected channel will be scanned once during each scan rotation. A scan weight of 2 specifies that the selected channel will be scanned twice and so forth. The scan sequence is determined by the specified scan weights. All selected channels are initially scanned once during the scan rotation. Any selected channels that have weights of 2 or more are then scanned again at the end of each rotation period for the number of times specified by the weight value. For example, if channels 1, 6 and 11 are assigned scan weights of 1, 2 and 2, the channel scan sequence is 1-6-11-6-11. Another example is if channels 1, 5, 6 and 11 are assigned scan weights of 2, 1, 3 and 3, the channel scan sequence is 1-5-6-11-1-6-11-6-11.</p> <ul style="list-style-type: none"> • <code>Channel Lock</code> - used to lock a Sensor on a specific channel for scanning. A drop-down menu is displayed where you can select a channel.

Feature/Function	Description
	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> Scan Mode: Channel Lock Ch 1 (2.412 GHz) </div> <p>Note: Note that all channels in the 2.4 and 5 GHz bands are grouped together.</p>

ASA In-Line Settings

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

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**.

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. Note: AirDefense 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.

Function	Description
Air Termination System	<p>Air Termination enables you to terminate the connection between your wireless LAN and any associated authorized or unauthorized or Wireless Client.</p> <p>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.)</p> <p>No: (Default). Click this radio button to disable AirTermination.</p> <p>Note: If you are not an Admin User, this setting will not be visible.</p>
Policy-based Air Termination System Enabled	<p>Policy-based Air Termination is an automated version of Air Termination. This feature enables you to formulate an Action Plan to automatically terminate the connection between your wireless LAN and any associated authorized or unauthorized or Wireless Client, based on alarms.</p> <p>Yes: Click this radio button to enable Policy-based Termination at the system level.</p> <p>No: (Default). Click this radio button to disable Policy-based Termination.</p> <p>Note: If you are not an Admin User, this setting will not be visible.</p>
Port Suppression System	<p>Port Suppression enables you to turn off the port on the network switch through which a device is communicating. You can suppress the communications port for any network device, effectively shutting down the communication port for the device.</p> <p>Yes: Click this radio button to enable Port Suppression at the system level. See the Note, below.</p> <p>No: (Default). Click this radio button to disable Port Suppression.</p> <p>Note: You must have added SNMP Managed Switches and have full read and write privileges (see Adding/Importing Switches).</p>
Auto-Logout Enabled	<p>Use this feature to enable/disable the automatic logout feature, which logs a user out of AirDefense after a specified amount of time.</p> <p>Yes: Click this radio button to use Auto-Logout and activate the Auto-Logout Timeout scroll list.</p> <p>No: Click this radio button to disable the Auto Logout and deactivate the Auto-Logout Timeout drop down list.</p> <p>Note: You must log off AirDefense and then log back in before changes take effect.</p>



Function	Description
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 AirDefense 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.

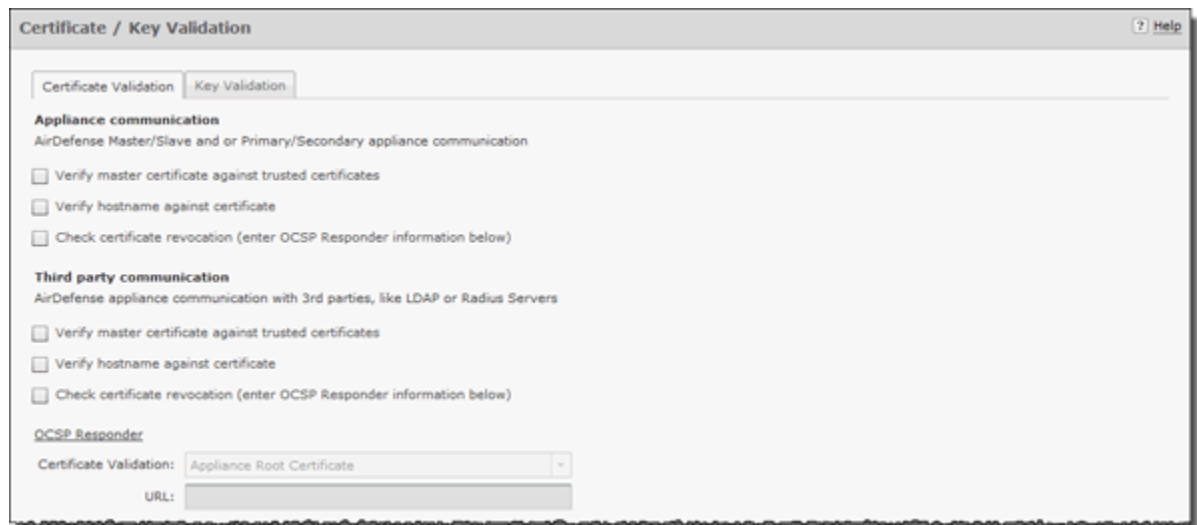
- A start and end time is displayed to show you when the backup/restore started and when it ended.
- Any errors are displayed in the error window for each section.

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.



The screenshot shows a web interface titled "Certificate / Key Validation" with a "Help" icon in the top right. There are two tabs: "Certificate Validation" (selected) and "Key Validation". The interface is divided into two main sections: "Appliance communication" and "Third party communication".

Appliance communication
AirDefense Master/Slave and or Primary/Secondary appliance communication

- Verify master certificate against trusted certificates
- Verify hostname against certificate
- Check certificate revocation (enter OCSP Responder information below)

Third party communication
AirDefense appliance communication with 3rd parties, like LDAP or Radius Servers

- Verify master certificate against trusted certificates
- Verify hostname against certificate
- Check certificate revocation (enter OCSP Responder information below)

OCSP Responder

Certificate Validation:

URL:

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

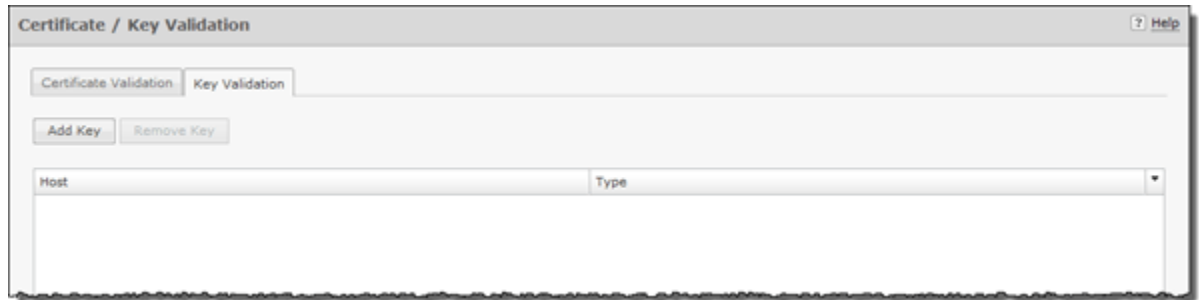
- Verify master certificate against trusted certificates
- Verify hostname against certificate
- Check certificate revocation.

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.

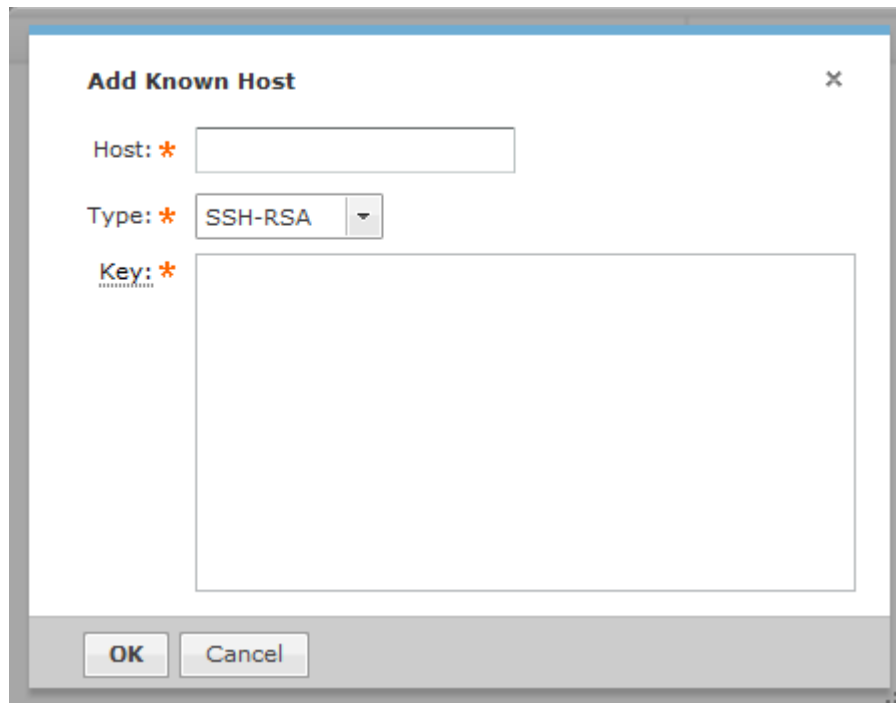
Key Validation

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 ----
AAAAB3NzaC1yc2EAAAABJQAAAIBrxx+YqQARTVMHfyyjisoQvBZoxvBMxf9CbXoo
VpWHBezQbm3anaav+4rEPIylcfFrIR/9o3/IdXT+arnXlrZ+7v3kBVx9SRWr5GY1
BtPFE1VQi1PJz/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
BtPFE1VQi1PJz/tXTp3erWyoZ4mwsb0kmoFAPc9LBrwrLtSlkrXezZrKZMa4VzB9
yK6dAQ==
```

5. Click **OK**.

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

Certificate Manager

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



Important

AirDefense recommends using a security certificate for every AirDefense appliance in your network. Furthermore, we recommend that you replace the pre-installed security certificate from AirDefense with either a self-signed certificate or a root-signed certificate.

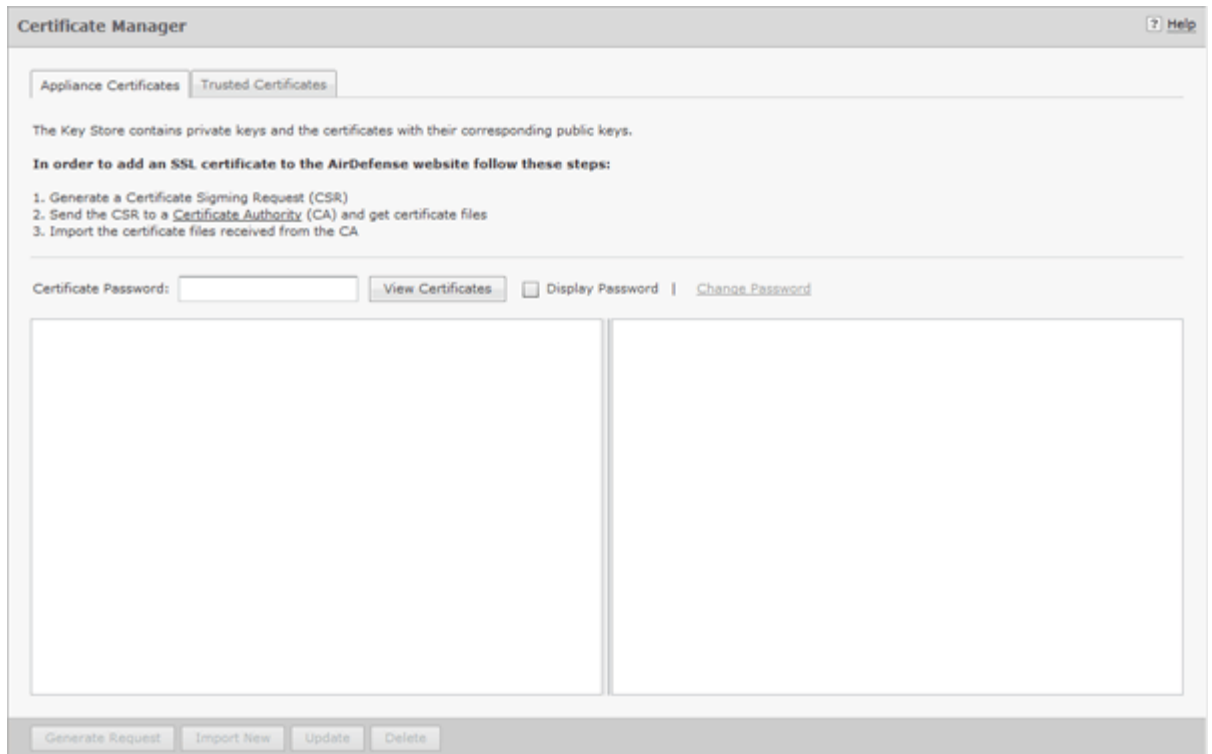
AirDefense supports the X.509 ITU-T (ITU Telecommunication Standardization Sector) standard for certificates. The supported encryption key lengths are 2048, 4096, and 8192. More information about the X.509 ITU-T standard can be found by searching the Internet.

Use the Certificate feature to view and create security certificates for the AirDefense 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 iCertificates feature by following these steps:

View Certificate Details

To view certificate details:

1. Navigate to **Configuration > Appliance Management > Certificate Manager**.



The screenshot shows the 'Certificate Manager' web interface. At the top, there are two tabs: 'Appliance Certificates' (selected) and 'Trusted Certificates'. Below the tabs, a message states: 'The Key Store contains private keys and the certificates with their corresponding public keys.' This is followed by instructions: 'In order to add an SSL certificate to the AirDefense website follow these steps: 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'. Below the instructions, there is a 'Certificate Password:' label, a text input field, a 'View Certificates' button, a 'Display Password' checkbox, and a 'Change Password' link. The main content area is currently empty. At the bottom, there are four buttons: 'Generate Request', 'Import New', 'Update', and 'Delete'.

2. Enter your certificate password.



Note

The first time you access Certificates use the default password (security). Immediately change the default password to one that is more secure. Do not continue to use the default password.

3. Click the **View Certificates** button.

Certificate Types

Every AirDefense appliance comes with an AirDefense certificate. However, there are three other certificates available; each represents a different level of security.

- Self-signed certificate
- Root-signed certificate
- SSL certificate.

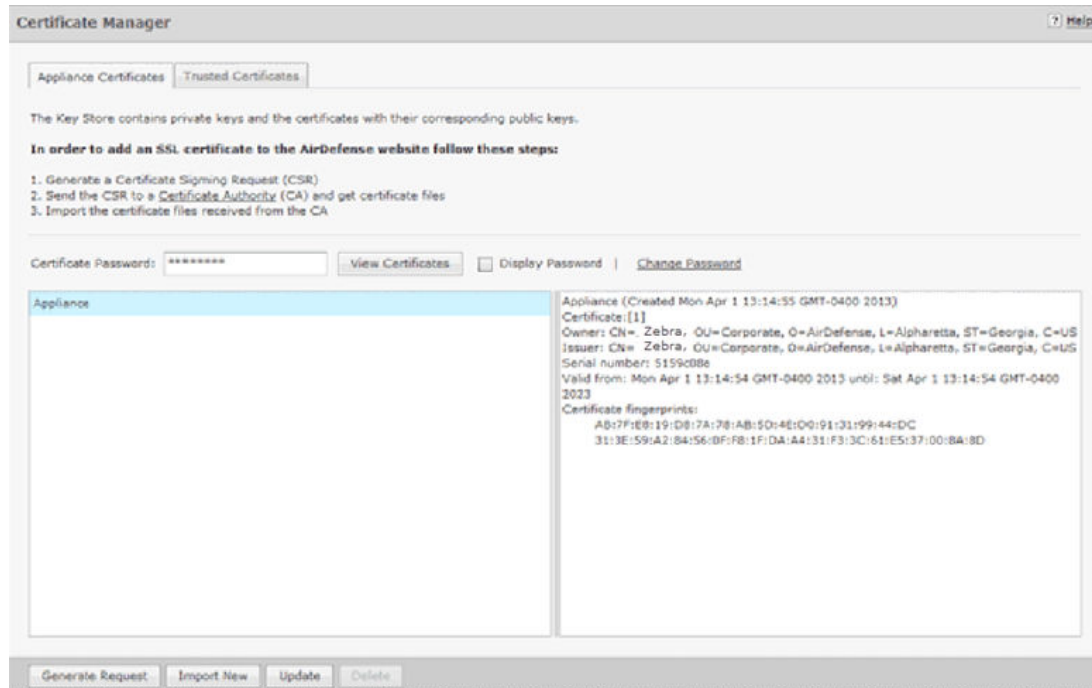
The following table describes each of the certificate types:

Certificate	Description
AirDefense Certificate	<p>The AirDefense certificate represents a minimal level of security.</p> <p>AirDefense ships the AirDefense 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 AirDefense appliance. Unless the certificate meets all required criteria, you will receive one or more alert screens when you open a session with AirDefense.</p>
Self-Signed Certificate	<p>A self-signed certificate represents an intermediate level of security.</p> <p>A self-signed certificate (also called Tomcat Certificate) is a certificate that you must generate. In this certificate, you specify the host name of the AirDefense Server, but do not have the certificate verified and digitally signed by a root Certificate Authority. Unless the certificate meets all required criteria, you will receive one or more alert screens when you open a session with AirDefense.</p>
Root-Signed Certificate	<p>A root-signed certificate represents a high level of security.</p> <p>A root-signed certificate is a public certificate that is verified by a root Certificate Authority (CA). This is a digitally-signed certificate that ensures the authenticity of the AirDefense Server.</p>
SSL Certificate	<p>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://.</p>

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

AirDefense 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 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:

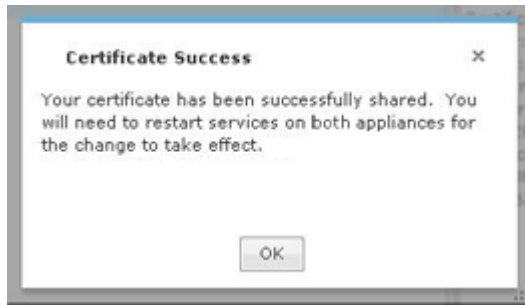
For the slave appliance:

- The user name and password used to access the GUI
- The appliance certificate password
- The trusted certificate password.

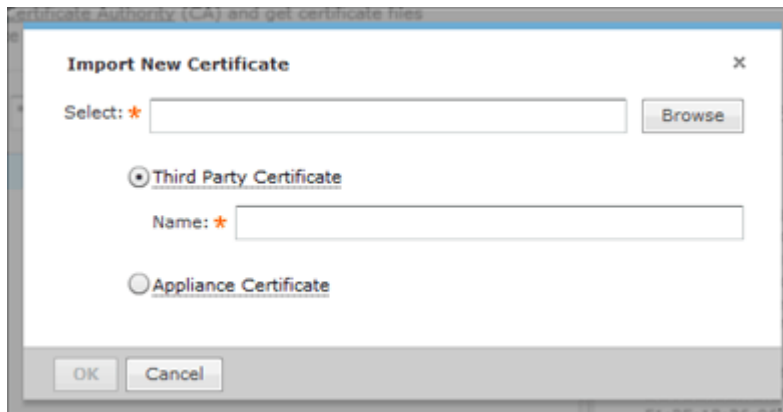
For the master appliance:

- 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.

- Click the **Share** button.



- Click **OK**.
- On the master appliance, access the **Trusted Certificate** tab.
- In the **Appliance** field, select the master appliance.
- Type in the certificate password and then click **View Certificates**.
- Click the **Import New** button.



- Browse to CA certificate and select it.
- Click **OK**.
- Restart the master appliance.
- On the slave appliance, access the **Trusted Certificate** tab and then repeat steps 9 through 13.
- Restart the slave appliance.
- 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

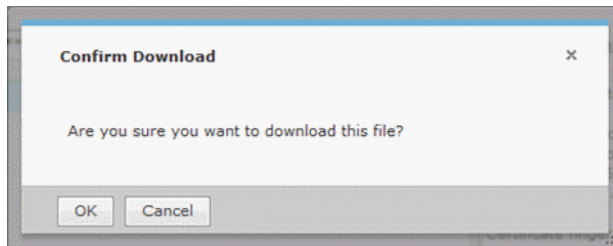
The Appliance Certificates store private keys and the certificates with their corresponding public keys. There are three main steps to adding an appliance certificate. They are:

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.

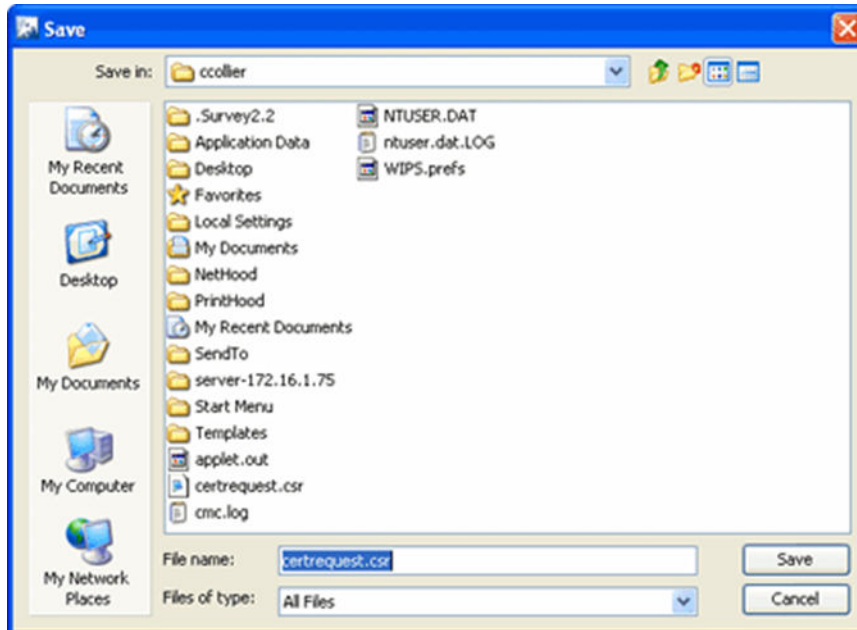
Generate Certificate Signing Request

To generate a Certificate Signing Request (CSR), do the following:

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.

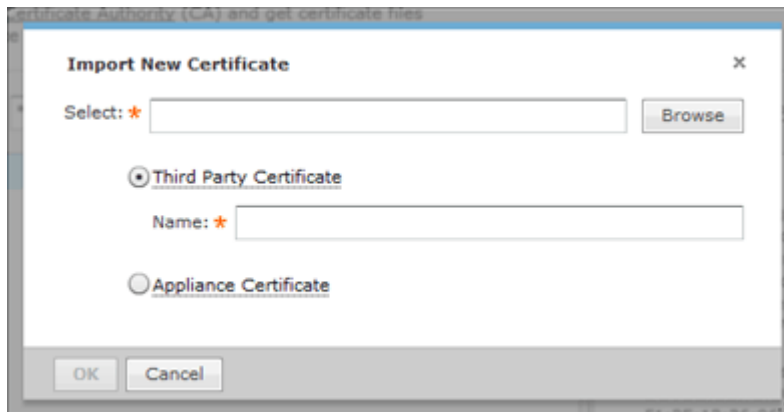
The file save in Generate a CSR has the information that a CA needs to issue certificate files. You will have to present this information to the CA in some way.

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.

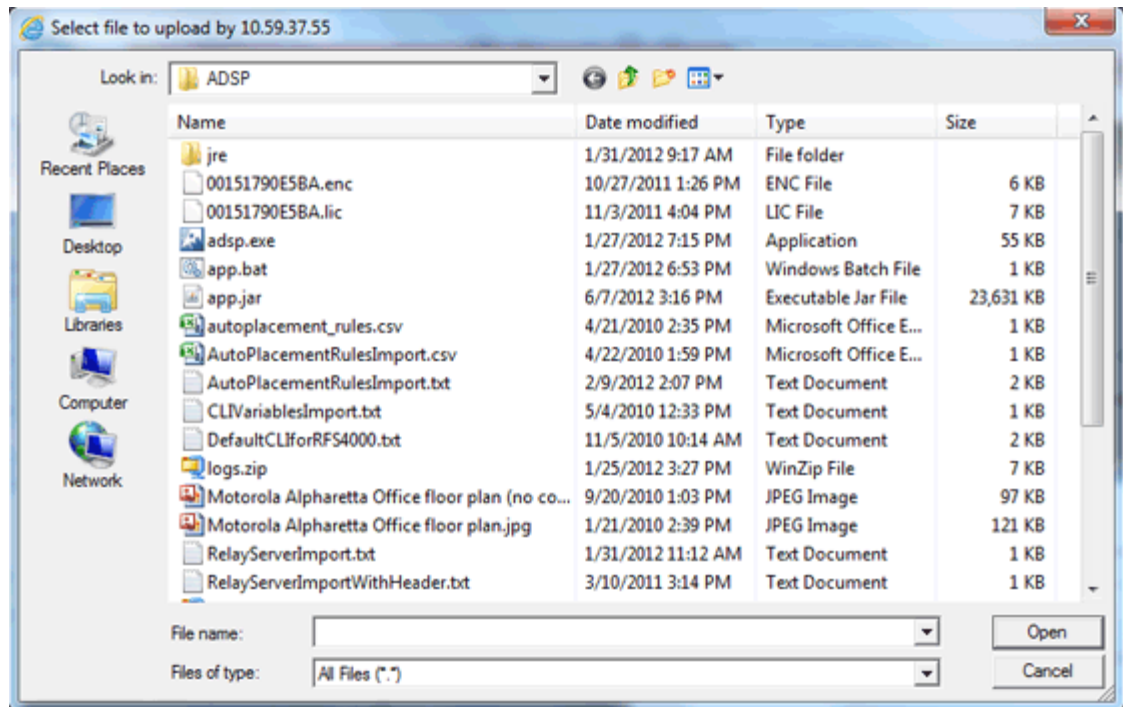


- Click the **Browse** button to open the **Select file to upload** window.



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.



- Navigate to the Intermediate certificate, select (highlight) it, and then click the **Open** button. The file name should now display in the **Select** field.
- Type in a name for the certificate.
- Click **OK**.
- Repeat Steps 1 to 5 to import the Root certificate.
- 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.

- Click **OK**.



Note

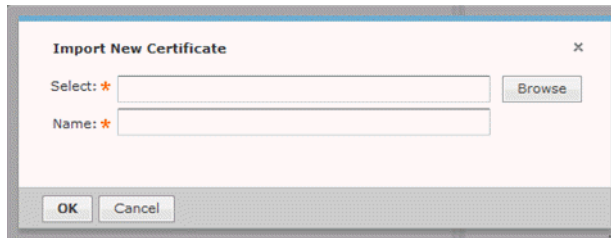
You will have to restart tomcat services before the certificates are activated. The tomcat services are located on your ADSP appliance.

Import New Certificate

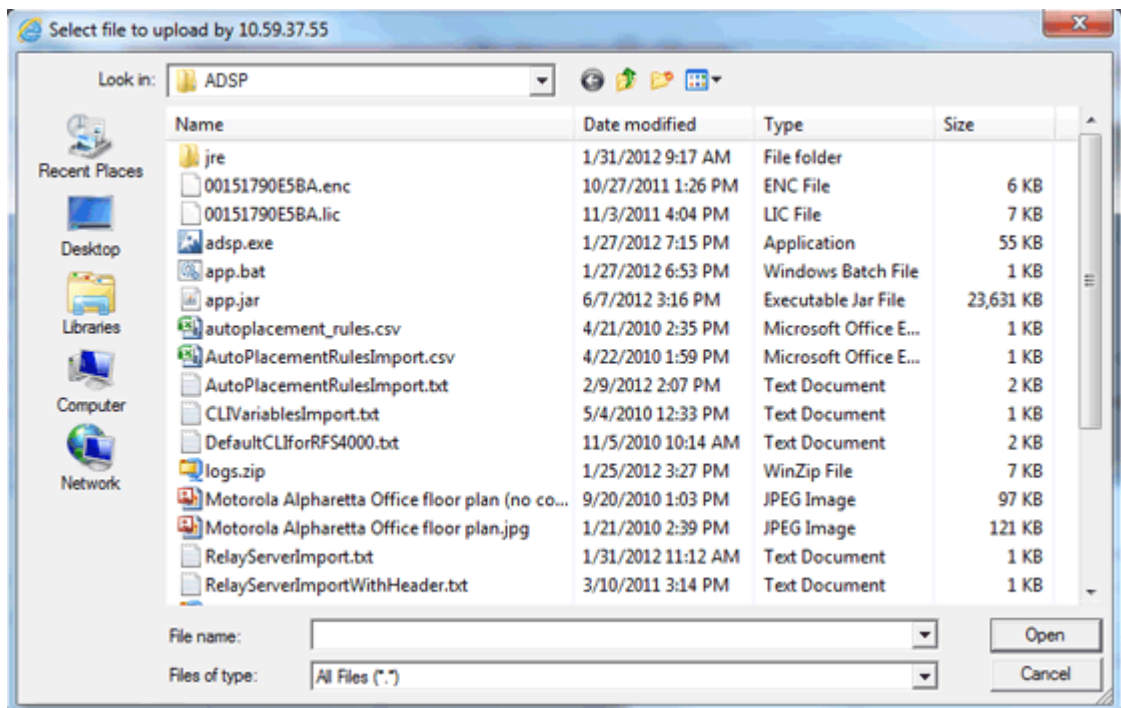
The Trusted Certificates store contains certificates from other parties (like AirDefense kAppliances, LDAP or Radius Servers) that you expect to communicate with, or from

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

This topic discusses the process to update certificate information for certificates already stored in your appliance.

Changing Default Information

A certificate's default information is included with each certificate that you add.

To change the certificate's default information:

1. Click the **Update** button to display the **Update Appliance Certificate** window.

The screenshot shows a dialog box titled "Update Appliance Certificate" with a close button (X) in the top right corner. The dialog contains the following fields:

- Name * (text input): Appliance-01
- Department Name * (text input): Corporate
- Company Name * (text input): AirDefense
- City * (text input): Alpharetta
- State * (text input): Georgia
- Country * (text input): US
- Valid Days * (text input): 3652
- Key Size (dropdown menu): 2048

At the bottom of the dialog are two buttons: "Ok" and "Cancel".

The following table describes the certificate information fields that can be modified:

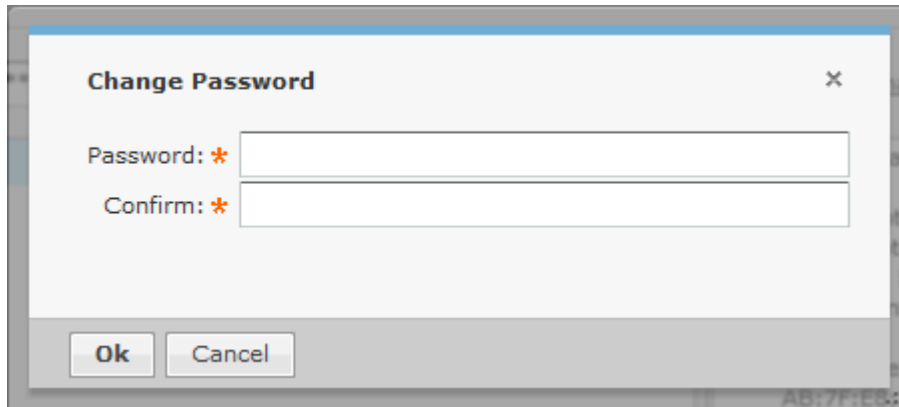
Field	Description
Name	The hostname you assigned the AirDefense appliance.
Department Name	The department in which the AirDefense administrator is a member.
Company Name	The name of your company.
City	The city in which your company is located.
State	The State (full name - not abbreviated) in which the company is located.
Country	The two-character country code for the country in which the company is located.
Valid Days	The number of days a certificate is valid once you add it.
Key Size	The certificate encryption key length. Supported encryption key lengths are 2048, 4096, and 8192.

2. Once done, 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 local computer.



Note

This information is required for Managed Services Provider (MSP) integration.

Depending on your browser, follow one of these procedures:



Note

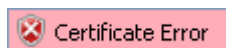
Procedures for Internet Explorer and Firefox are included here. Other browsers will have similar buttons/links that allow you to export a certificate.

- [For Internet Explorer](#) on page 131
- [For Firefox](#) on page 132

For Internet Explorer

To export certificates using Microsoft™ Internet explorer:

1. Click **Certificate Error** near the top of Internet Explorer window.



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. Select a location on the local PC 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

To export certificate using Mozilla™ Firefox:

1. Click the area with the appliance ID located near the top the Firefox window.

10.59.39.107

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](#)

Configuration Backup

Enable Configuration Backup Scheduling

Name	Schedule
Default Backup	Default Backup - Daily: Every 1 day at 12:00 AM

Settings

Job Name: *

Destination: Local
 Remote

Host: *

Port: *

Protocol:

Path: *

User: *

Password: * Display Password

Retries: (Max: 5)

Schedule

Frequency:

Time:

Date:

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 the `/usr/local/smx/backups` folder.
- 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.

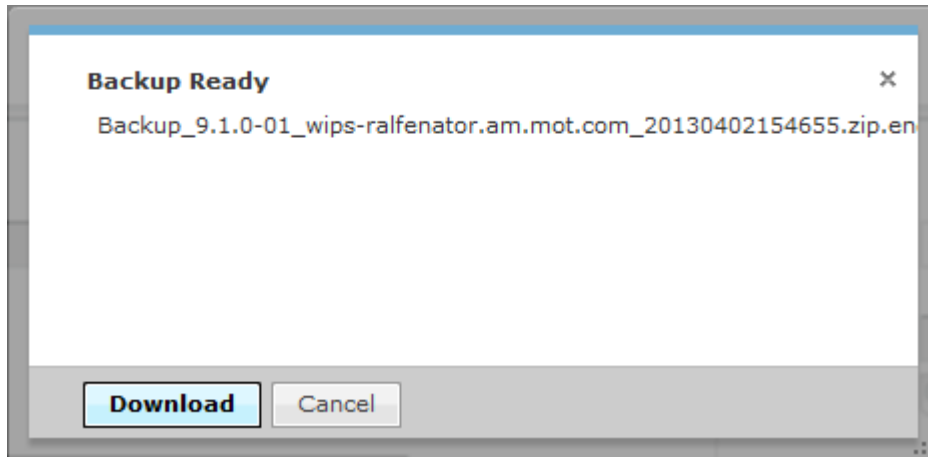
Backup Recommendations

- 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.

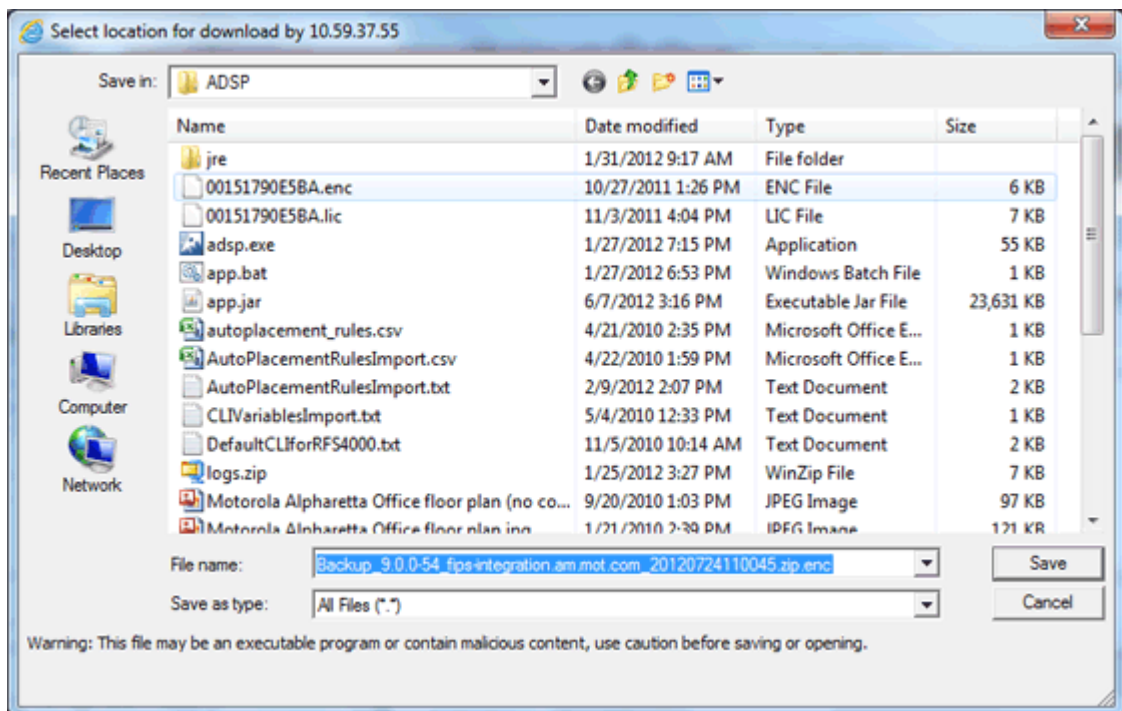
Manual Backups

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.



Note

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 in the **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.

5. Click the **Apply** button to set the automatic backup schedule.
6. During an automatic backup, you can 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).

Field	Description
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.

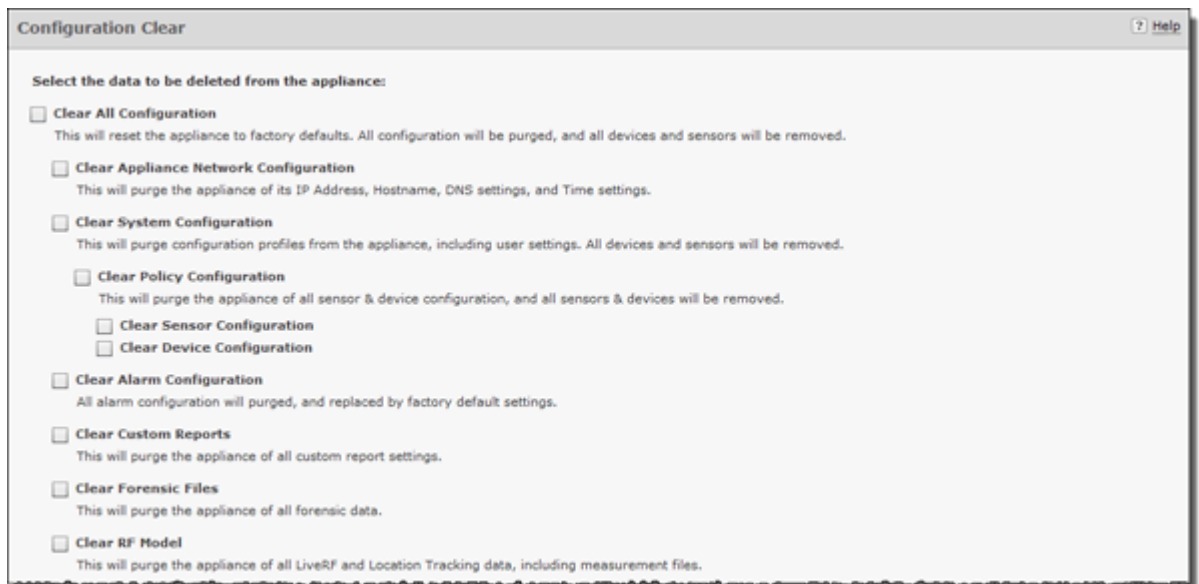
Configuration Clear

Use the Configuration Clear option to clear configuration data and set your appliance back to its default state when your system was first delivered.

You can either clear the complete configuration data and reset the system as it was first delivered or can clear specific configuration data.

The available options are:

1. Navigate to **Configuration > Appliance Management > Configuration Clear**.

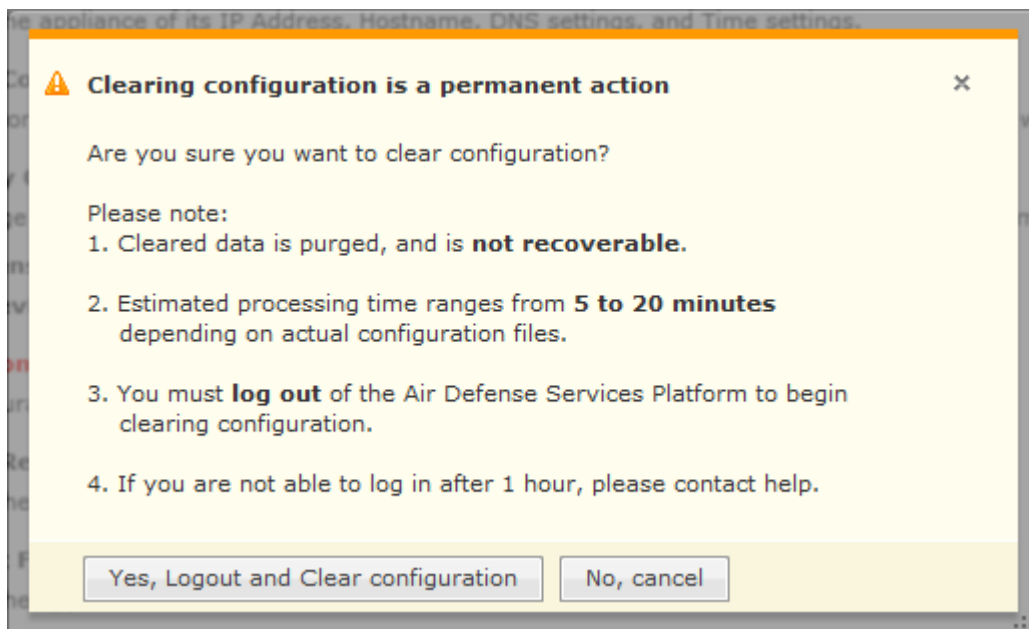


2. You can select from the following configuration options:

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.

Option	Description
Clear System Configuration	Clears all system configuration data. This encompasses everything except what is covered by the other options. There are three other options associated with this option. <ul style="list-style-type: none"> 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.
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.

3. Select one or more options by placing a checkmark in the checkbox.
4. After selecting your options, click the **Next** button. A confirmation window is displayed.



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



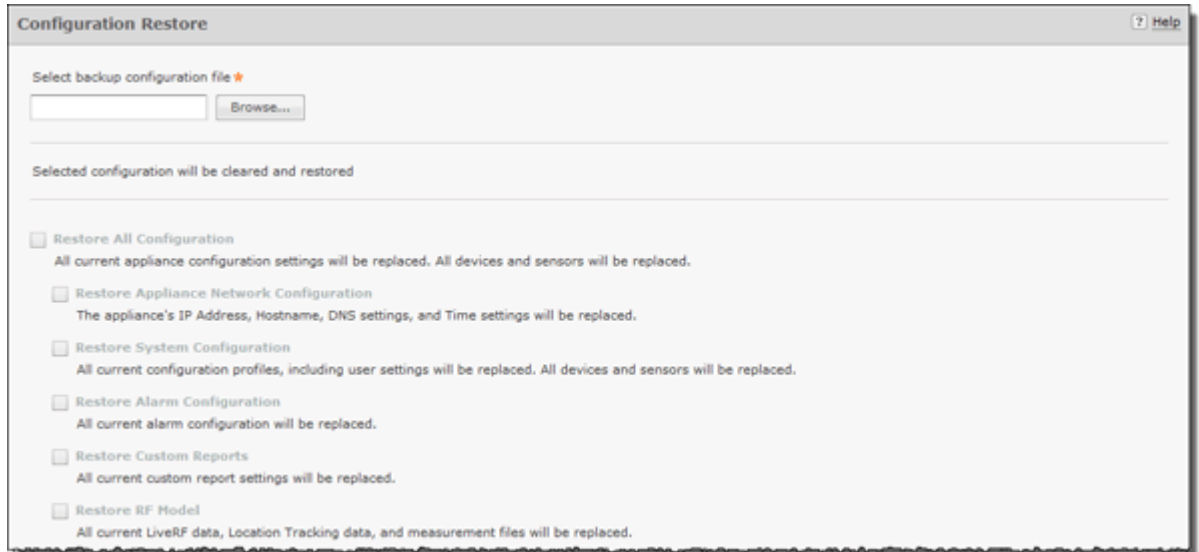
Note

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 AirDefense server.

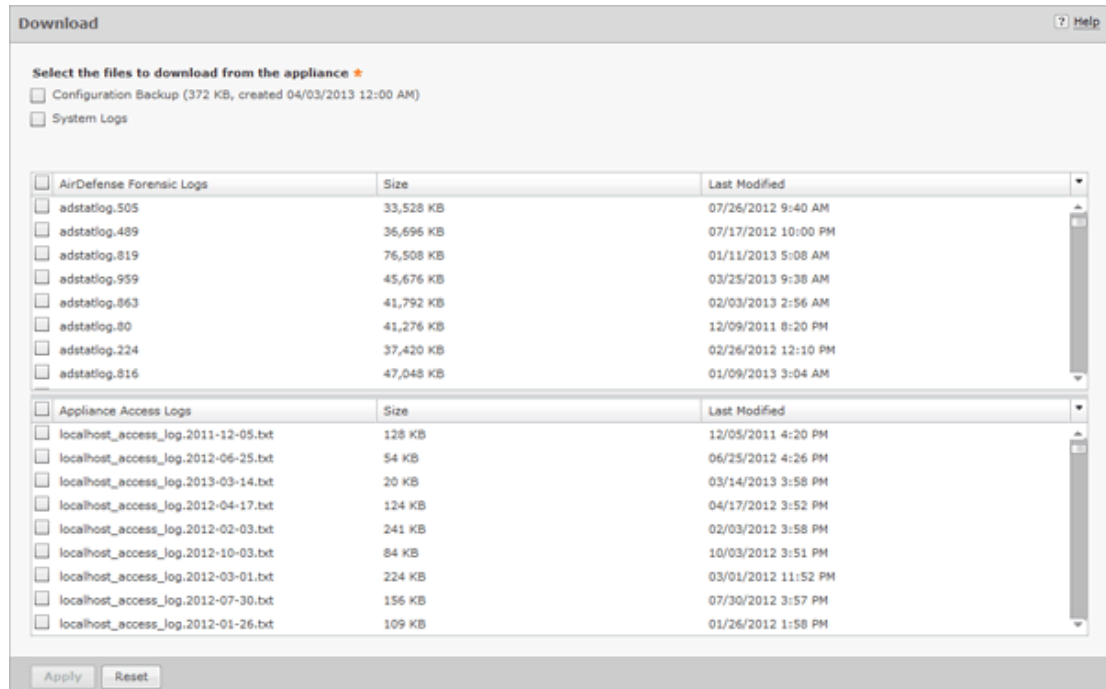
If you want to restore a configuration that was automatically backed up to your AirDefense server, you can download it to your workstation. (See [Download Logs](#).)

Download Logs

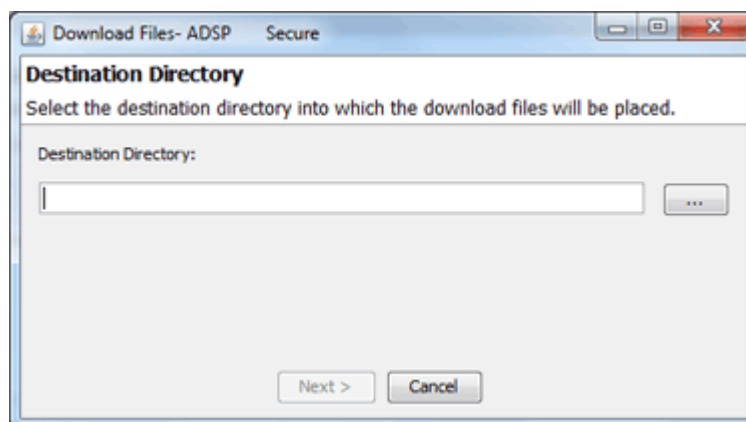
You can download configuration files that were automatically backed up to your ADSP server to your workstation. Once the backed up configuration is on your workstation, you can restore it. (See [Configuration Restore](#).)

To download a configuration, follow these steps:

1. Navigate to **Configuration > Appliance Management > Download Logs**.

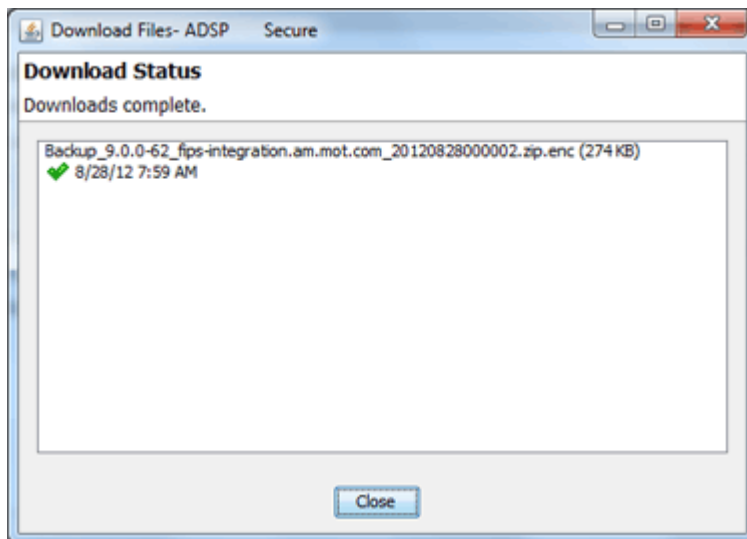


2. Select if you want to download a backup that exists on your appliance and/or the system logs.
3. You can download all forensic logs or all appliance access logs. Alternatively, you can pick and choose the forensic logs or appliance access logs that you want to download.
4. Click **Apply**. A destination 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

To enable 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.

You can automatically back up forensics data and log files by navigating to **Configuration > Appliance Management > Forensic and Log Backup**.

Forensic and Log Backup

Enable Automatic Forensics Backup

Host:

Port:

Protocol:

Path:

User:

Password: Display Password

Retries: (Max: 5)

Verify Server Certificate/Key

Enable Automatic Log Backup

Host:

Port:

Protocol:

Path:

User:

Password: Display Password

Retries: (Max: 5)

Verify Server Certificate/Key

Frequency:

Time:

Date:

Field	Description
Host	The name of the server where you want to back up forensics or log files. This can be an IP address or a DNS name defined by your DNS server.
Port	The port number to use during the backup.
Protocol	The file transfer protocol to use for backing up forensics or log files.
Path	The directory (folder) where to place the backup on the destination server.
User	The username used to log in on the destination server.
Password	The password used to log in on the destination server.
Verify Server Certificate/Key	Verifies that the server certificate (HTTPS connections) or server key (SCP and SFTP connections) is valid.
Retries	The number of times to retry the forensic backup if a failure occurs. The maximum number is 5.

You can schedule the backups for system and access logs. Select an interval and then fill in the related fields using the following table:

Interval	Action
One Time Schedule	Choose a time for the backup by selecting a time from the 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

AirDefense 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](#)
- [Login Banner](#)
- [SSH Banner](#)

Pre-Login Banner

The **Pre-Login Banner** tab is provided for AirDefense deployments who wish to display their own customized banner before allowing users to log into AirDefense. You could use this banner to force user to accept "Terms and Conditions".



The screenshot shows the 'Banners' configuration page with three tabs: 'Pre-Login Banner', 'Login Banner', and 'SSH Banner'. The 'Pre-Login Banner' tab is selected. Below the tabs, there is a checkbox labeled 'Enable Pre-Login Banner'. Underneath, there is a text area with a placeholder text: '* (Please enter text)' and a note: 'This is the default agreement. Replace this text with the actual agreement text.'

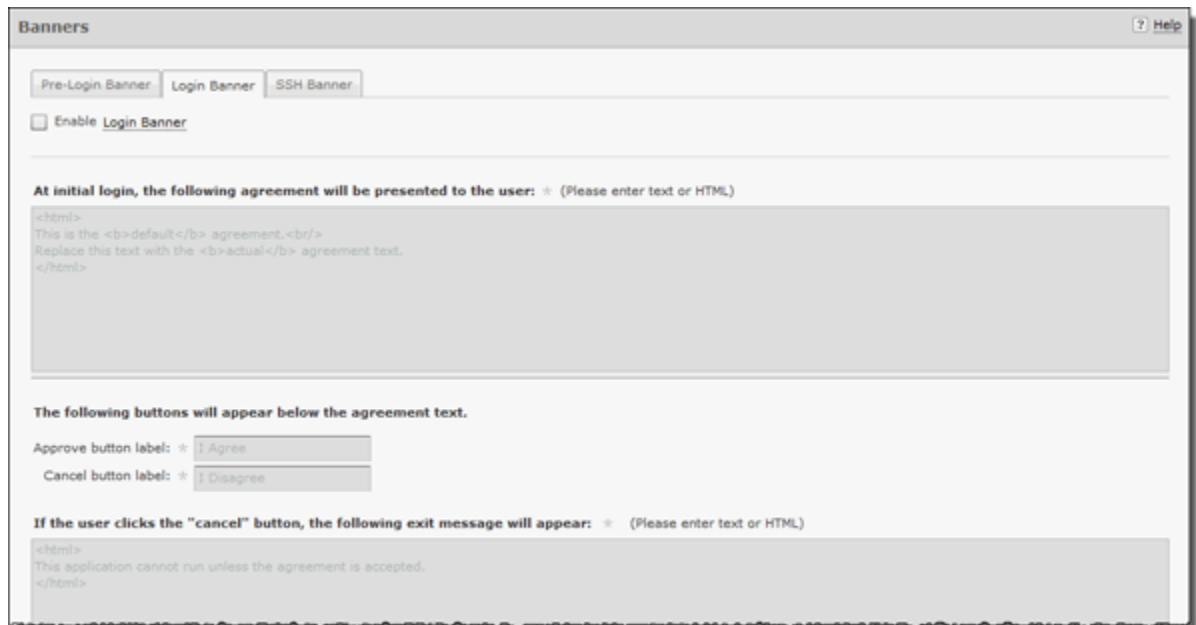
To activate, select **Enable Pre-Login Banner** checkbox.

The * **(Please enter text)** field is available to enter text that users will see before logging into AirDefense. Text can be entered in HTML or text format.

Click **Apply** to save the pre-login banner.

Login Banner

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



The screenshot shows the 'Banners' configuration page with three tabs: 'Pre-Login Banner', 'Login Banner', and 'SSH Banner'. The 'Login Banner' tab is selected. Below the tabs, there is a checkbox labeled 'Enable Login Banner'. Underneath, there is a text area with a placeholder text: '* (Please enter text or HTML)' and a note: 'At initial login, the following agreement will be presented to the user:'. Below this, there is a text area with a placeholder text: '<html> This is the default agreement.
 Replace this text with the actual agreement text. </html>'. Below this, there is a text area with a placeholder text: 'The following buttons will appear below the agreement text.' and two input fields: 'Approve button label: * I Agree' and 'Cancel button label: * I Disagree'. Below this, there is a text area with a placeholder text: '* (Please enter text or HTML)' and a note: 'If the user clicks the "cancel" button, the following exit message will appear:'. Below this, there is a text area with a placeholder text: '<html> This application cannot run unless the agreement is accepted. </html>'. Below this, there is a text area with a placeholder text: '* (Please enter text or HTML)'.

To activate, select **Enable Login Banner** field.

The following configuration options are available for customizing the Login Banner.

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 AirDefense users who wish to add their own customized text for users accessing the AirDefense appliance through SSH.



To activate, select **Enable SSH Banner** field.

The following configuration option is available for customizing the SSH Banner.

The **At initial login...** field is available to enter text that users will see when accessing the AirDefense appliance through SSH. Text can be entered in HTML or text format.

Click **Apply** to save the SSH banner.

Redundant Appliance Sync

AirDefense 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`.
- 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:



Note

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.

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.
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.

5. 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).



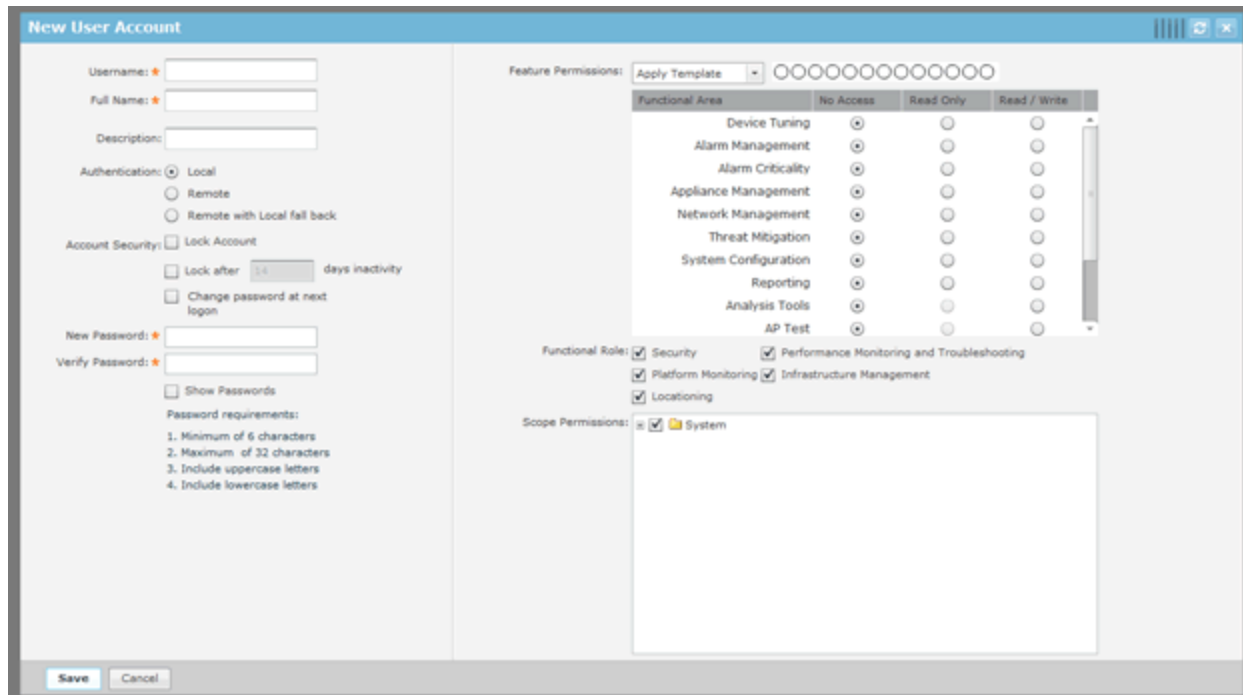
Note

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

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


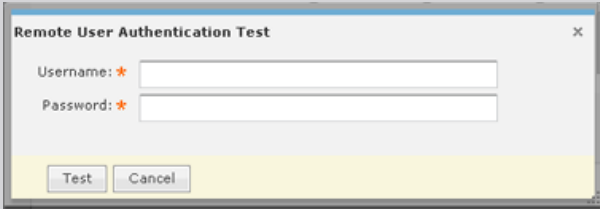
New User Account

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



Use the following table to configure the user account:

Field	Description
Username	The account name of the user.
Full Name	Enter a formal name of the user, if desired.
Description	Enter a description of the user account, if desired.

Field	Description
Authentication	<p>Select 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.</p> <p>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.</p> <p>When adding a remote user, Remote Authentication must be set up first. Once Remote Authentication is set up, select the Remote radio button.</p>  <p>You can test remote user authentication using the Test Authentication button.</p>  <p>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.</p>
New Password	<p>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.</p>
Verify Password	<p>Enter the new password again to verify the password.</p>
Lock Account	<p>Check this checkbox if you want to lock the account.</p>

Field	Description
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.
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	<p>Limits users to specific functions within ADSP. Functional areas include:</p> <ul style="list-style-type: none"> • Device Tuning • Alarm Management • Appliance Management • Alarm Criticality • Network Management • Threat Mitigation • System Configuration • Reporting • Analysis Tools • AP Test • Vulnerability Assessment • Connection Troubleshooting. <p>You can apply a template or you can select individual functions for users to access. The following templates are available:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. AirDefense 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.

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, AirDefense 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

AirDefense has four default role types with different levels of access to its 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.

Feature Permissions: ○○○○○○○○○○○○○○○○○○○

Functional Area	No Access	Read Only	Read / Write
Device Tuning	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Alarm Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Alarm Criticality	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Appliance Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Mitigation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reporting	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Analysis Tools	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
AP Test	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability Assessment	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Connection Troubleshooting	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Capabilities for the individual functional areas are:

Functional Area	Capabilities (use of)
Device Tuning	<ul style="list-style-type: none"> Setting annotations Device profile configuration (existing)
Alarm Management	<ul style="list-style-type: none"> 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 scale of an alarm's criticalness.
Network Management	<ul style="list-style-type: none"> Configure performance policy Configure configuration policy Configure monitoring policy Configure infrastructure profiles Configure sub-profiles Action Manager use Auto classification of devices Network setup Map configuration Auto-Placement Discovery policies Manual modification to network tree hierarchy Device placement Inherited policy/profile assignment (network and device levels)
Threat Mitigation	<ul style="list-style-type: none"> Manual termination ACL Port suppression
System Configuration	The configuration categories that affect the whole system
Reporting	<ul style="list-style-type: none"> Reporting UI Report builder
Analysis Tools	<ul style="list-style-type: none"> Live View LiveRF Location Tracking Spectrum Analysis Advanced Forensics Scope Forensics

Functional Area	Capabilities (use of)
AP Test	<ul style="list-style-type: none"> On-demand or scheduled AP Test AP Test profiles
Vulnerability Assessment	<ul style="list-style-type: none"> On-demand or scheduled Vulnerability Assessment Vulnerability Assessment profiles
Connection Troubleshooting	Troubleshooting tools

AirDefense 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

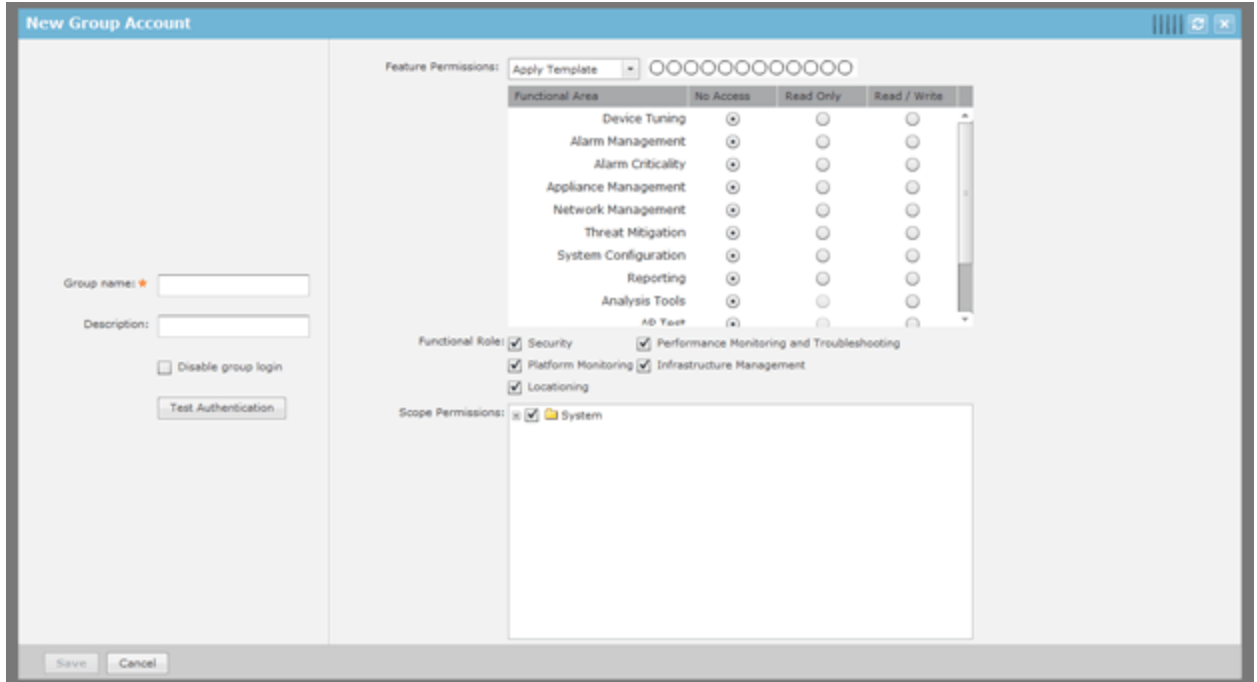
Group accounts involve a group of users set up through remote authentication (either LDAP or RADIUS). When a user attempts to log into AirDefense that is a member of a group, AirDefense first uses local authentication to log in the user. If the user is not part of local authentication, remote authentication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

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

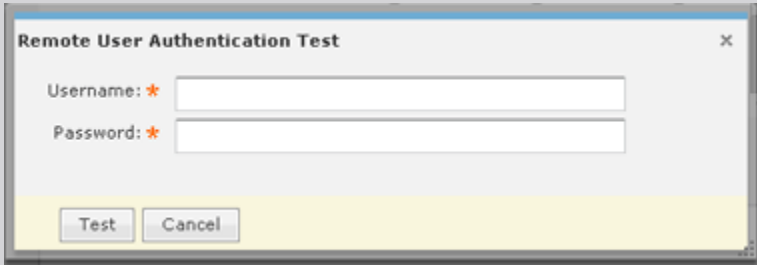


Note

The **New Group Account** button is part of a multi-purpose button. Clicking the drop-down menu button displays a menu where you can select **New User Account** or **New Group Account**. The last option that you select becomes the button.



Use the following table to configure the user account:

Field	Description
Group Name	Enter the name of the group account.
Description	Enter a description of the group account, if desired.
Disable group login	Disable the current login group.
Test Authentication	<p>Test remote user authentication using LDAP or RADIUS.</p>  <p>Enter a user's username and password. Then, click the Test button. If the credentials are valid, you will receive a pass message. If the credentials are invalid, you will receive a failed message.</p>
Feature Permissions	Functions the same as in user accounts.
Functional Roles	Functions the same as in user accounts.
Scope Permissions	Functions the same as in user accounts.

Once you have configured the group options, click **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. AirDefense 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 User 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.

guest (Guest) Guest User Account Admin ([Edit](#) | [Copy](#) | [Delete](#))

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.

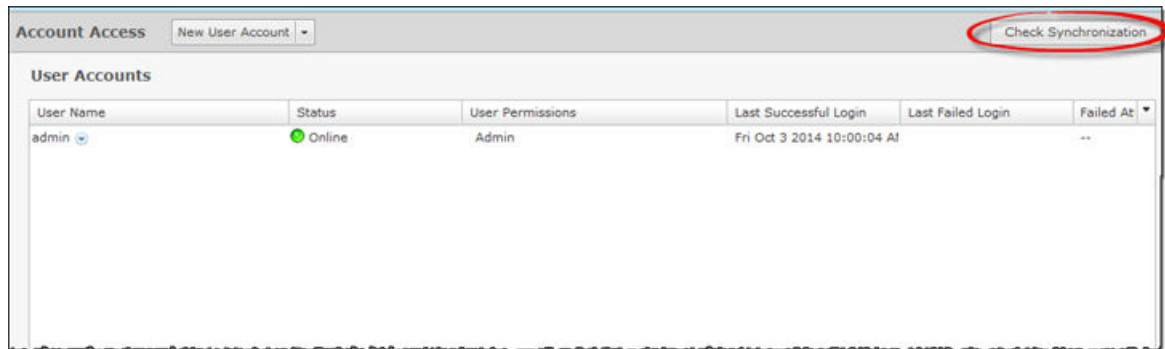
Functional Area	No Access	Read Only	Read / Write
Device Tuning	○	○	○
Alarm Management	○	○	○
Alarm Criticality	○	○	○
Appliance Management	○	○	○
Network Management	○	○	○
Threat Mitigation	○	○	○
System Configuration	○	○	○
Reporting	○	○	○
Analysis Tools	○	○	○
AD Test	○	○	○

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.

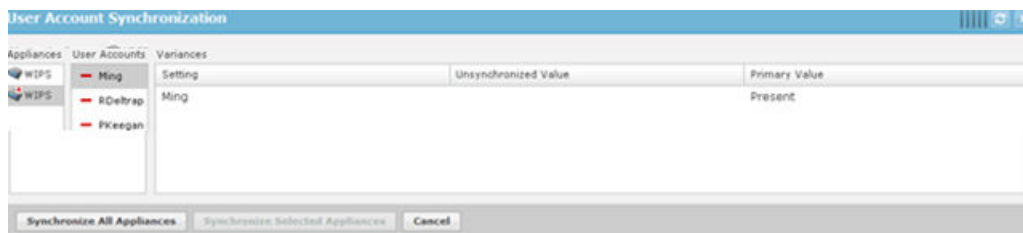


Note

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, a red asterisk (*) is displayed on the out of sync appliance. If you select (highlight) the out of sync appliance, a list of accounts are displayed that are out of sync on the selected appliance.



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

Click the **X** in the top, right corner to exit the **User Account Synchronization** overlay.

Local Authentication

Local Authentication is used to authenticate users on the local appliance. It also allows you to manage password aging, password complexity, and account lockout criteria. To access this window, go to **Configuration > Account Management > Local Authentication**.

Local Authentication

Max Login Attempts

Account locked if max attempts reached within minutes

Account locked if max attempts is reached at anytime

Password must be changed after days

High complexity password is required

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 feature 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**.

Password Reset

Old Password:

New Password:

Verify Password:

Field	Description
Old Password	Enter your current password here.
New Password	Enter your new user password here.
Verify Password	Enter your new password here again.

After entering your password information, click the **Apply** button to save your changes. Click the **Reset** button to discard any changes.

Remote Authentication

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

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

Remote Authentication [New] [Move Up] [Move Down] [Delete]

New_Auth_Source

Name:

Type:

LDAP LDAPS

LDAP Server:

LDAP Port:

User Prefix: (Example: "CN=")

User Suffix: (Example: "DN=mycompany, DC=com")

Use LDAP for external group based authentication

LDAP basics

Contact your LDAP administrator - be sure to follow your organization's protocol.

Prefix is added to the username to form the user distinguished name (DN).

Suffix is a DN that identifies the top entry in a locally held directory hierarchy. There is no requirement that you use a suffix.



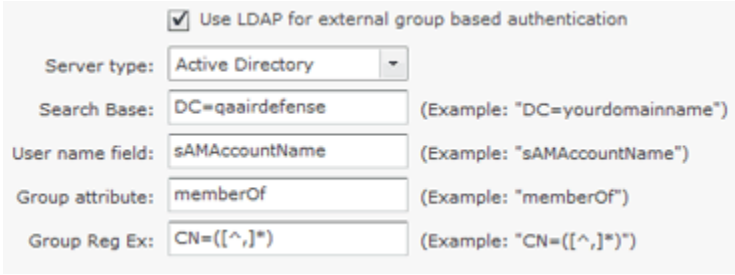
Note

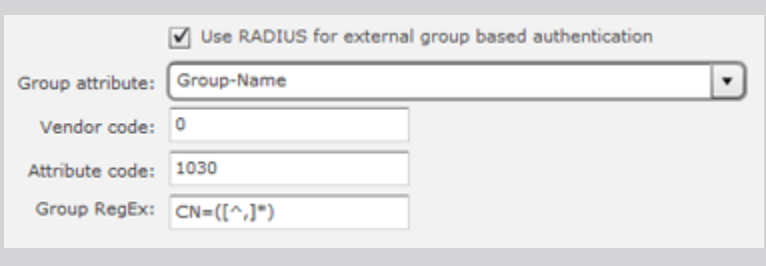
If you encounter problems, contact your LDAP administrator. He/she can advise you on how to fill in the fields. If you can, use an LDAP browser (<https://www.ldapadministrator.com/download.htm>) to login and browse. This will allow you to test your settings to see if they are right. There should also 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.

Field	Description
Use LDAP for ...	<p>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.</p> <ul style="list-style-type: none"> • 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 is left to AirDefense for use in group identification. Normally, the string is CN=([^,]*). <p>If the LDAP administrator changes any of the strings from what is normally used, he/she must inform you of the string to use. Example:</p>  <p>The screenshot shows a configuration form with the following fields and values:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Use LDAP for external group based authentication Server type: Active Directory (dropdown) Search Base: DC=qaairdefense (Example: "DC=yourdomainname") User name field: sAMAccountName (Example: "sAMAccountName") Group attribute: memberOf (Example: "memberOf") Group Reg Ex: CN=([^,]*) (Example: "CN=([^,]*)")
Use RADIUS for ...	<p>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.</p> <ul style="list-style-type: none"> • 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 AirDefense to use in group identification. You should not change any of the inserted values. <p>Example :</p>

Field	Description
	 <p>The screenshot shows a configuration panel with the following fields:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Use RADIUS for external group based authentication Group attribute: Group-Name (dropdown menu) Vendor code: 0 (text input) Attribute code: 1030 (text input) Group RegEx: CN=([^\,]*) (text input)

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 AirDefense 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 AirDefense. The following views are available:

- Dashboard tab
- Network tab
- Alarms tab
- Configuration tab.

Auto Refresh

AirDefense 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 AirDefense data every 10 minutes.
- `5 minute refresh` - Automatically refresh AirDefense data every 5 minutes.
- `1 minute refresh` - Automatically refresh AirDefense data every minute (default).

Log Level

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

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

Device Inactivity

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

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

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

- The 0 - 5 minutes option is selected
- The 5 - 10 minutes option is selected
- All other options are deselected.

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

Copy MAC Formats

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

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

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

00:a0:f8:bb:c5:69
00-a0-f8-bb-c5-69
00a0.f8bb.c569
00a0f8bbc569

Use Proxy to Access Appliance

You can specify that users must use a proxy to access your AirDefense 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 AirDefense 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



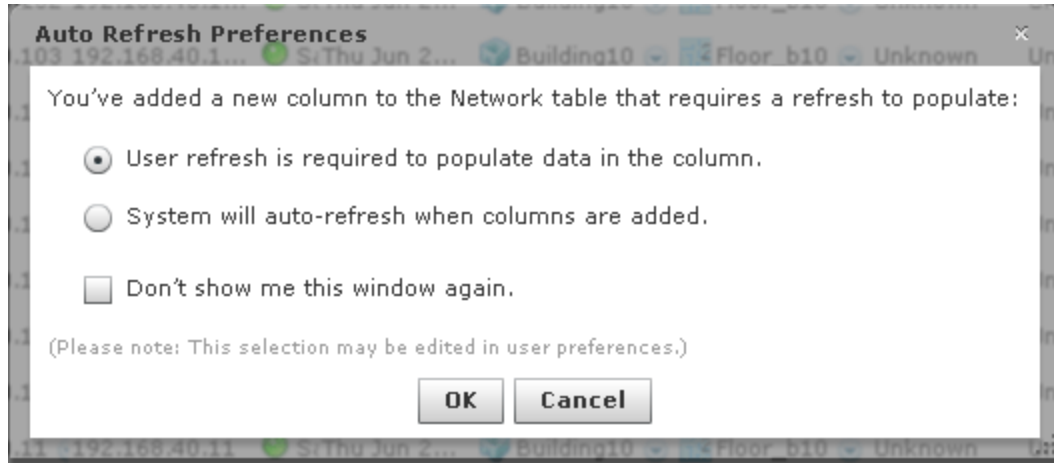
Note

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.

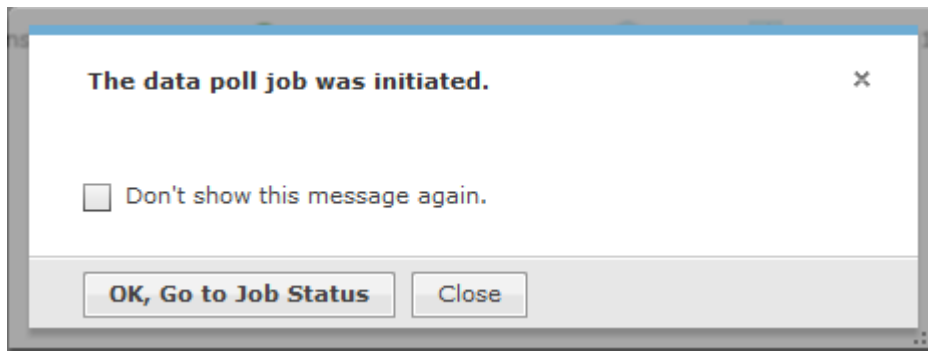


Click OK to save your changes.

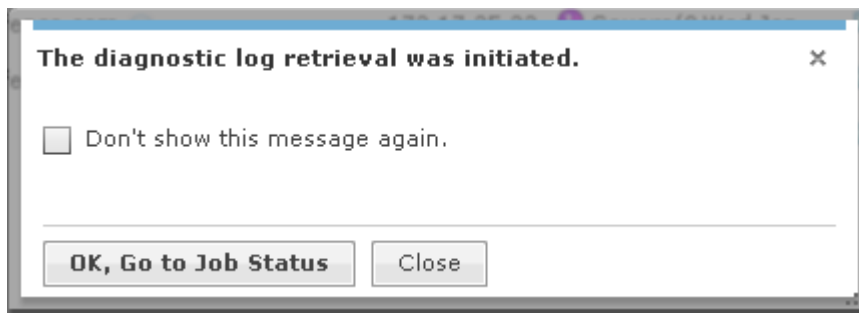
Show Job Initiation Message Dialogs

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

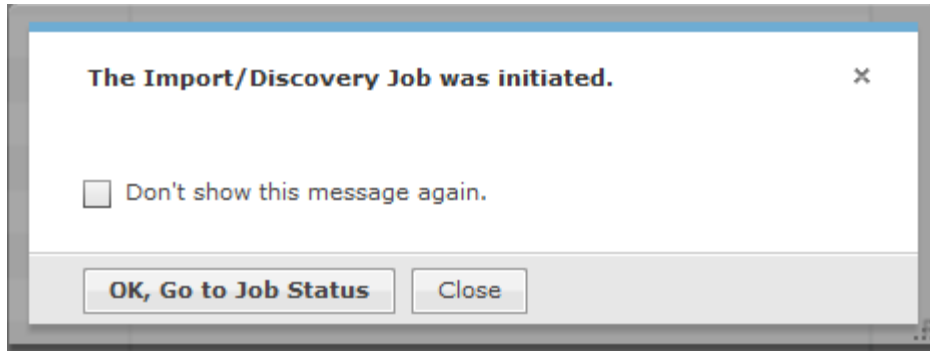
- Show Data Poll Job Initiation Message Dialog - Displays the following dialog window when a data poll is manually initiated:



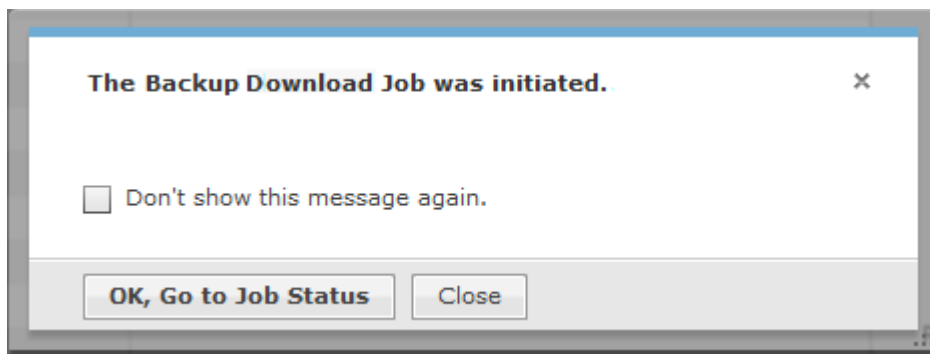
- Show Diagnostic Logs Job Initiation Message Dialog - Displays the following dialog window when manually retrieving the diagnostic log:



- 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.

Job Status						
Type	Description	User	Status	Start Time	Finish Time	Progress
Data Poll	On Demand Data Poll	ccollier	Polled 1 devices	Tue May 15 2012 02...	Tue May 15 2012 02...	1/1
Device Configuration	On Demand Log Retri	ccollier	Complete: successful	Tue May 15 2012 10...	Tue May 15 2012 10...	1/1
Data Poll	On Demand Data Poll	ccollier	Polled 1 devices	Tue May 15 2012 10...	Tue May 15 2012 10...	1/1
SNMP Discovery	New Scheduled Impor	ccollier	Polled 3 devices	Mon May 14 2012 0...	Mon May 14 2012 0...	3/3


Drop-down Menu Access

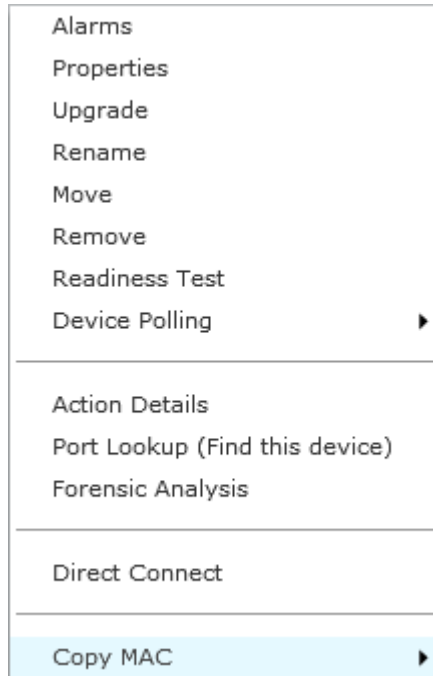
Drop-down menus are located throughout AirDefense. Whenever a device or network level is displayed, it has an associated drop-down menu. You can access the drop-down menu to get details on functions and properties. Click the drop-down menu button to display information on functions that operate on a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

Devices Drop-down Menu

This section describes the available drop down menus for the different contexts in AirDefense.

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.




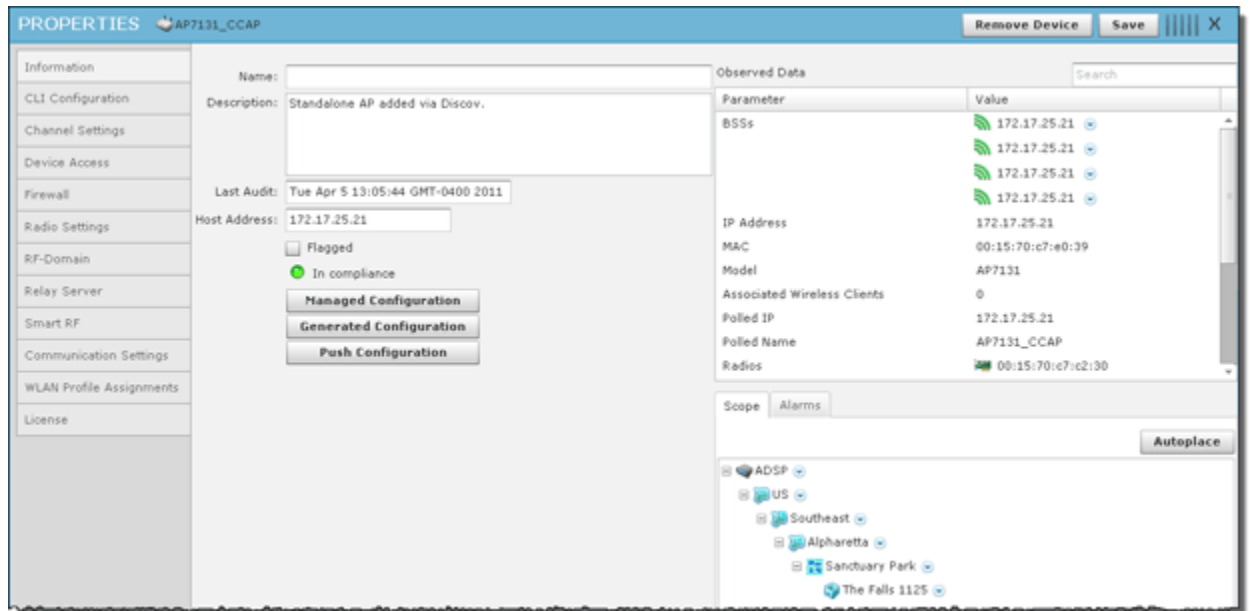
The drop-down menu for APs contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected AP. See Alarms
Properties	Opens the Properties overlay for the selected AP.
Upgrade	Upgrades the firmware for the selected AP.
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 on page 743 for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected AP.
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.

Function	Description
Forensic Analysis	Opens the Forensic Analysis - Basic window for the specified .
Direct Connect	Accesses the user interface (UI) for the selected device.
Copy MAC	Copies the MAC address of the selected for later use.

APs - 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.
Flagged	Flag an AP that you want to bring attention to.

Field	Description
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.

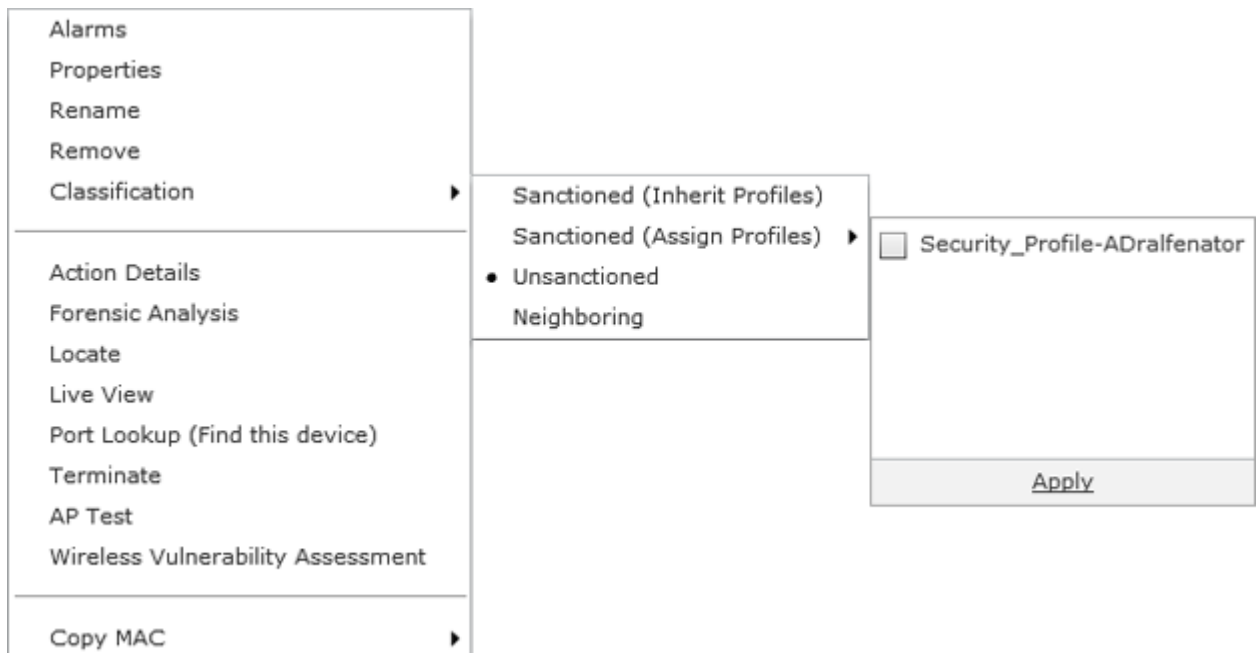
Alarms related to the AP are shown in the **Alarms** tab. The **Actions** button can be used to perform one of the listed functions on a selected (highlighted) alarm.

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

Click the Close buttonX 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.

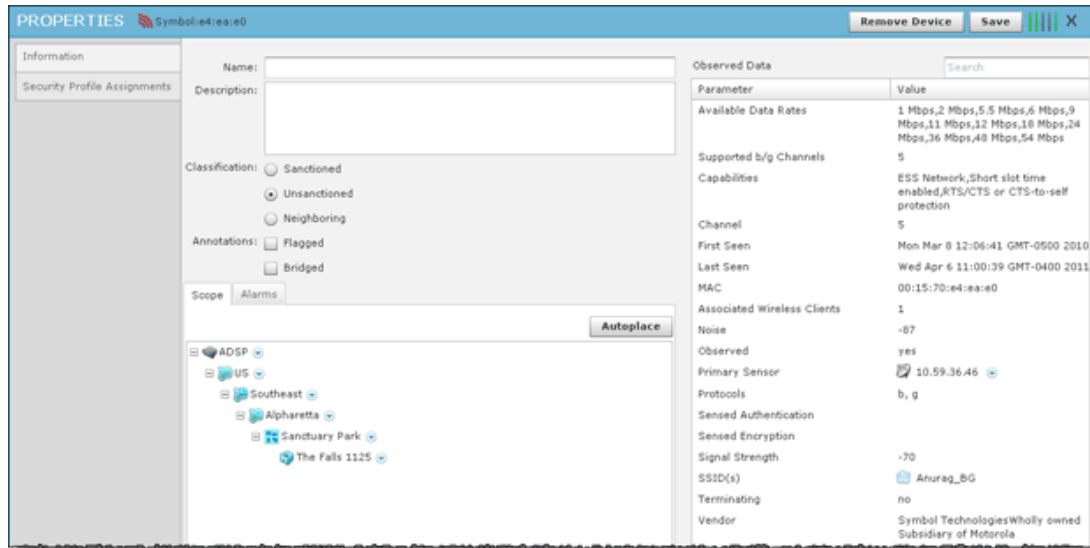


The drop-down menu for BSSs contains the following functions:

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.
Classification	Classifies the BSS using one of the following classifications: <ul style="list-style-type: none"> • <i>Sanctioned (inherit)</i>—Classify the selected BSS as a sanctioned device that inherits its traits from wherever its location in the network tree. • <i>Sanctioned (override)</i>—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. • <i>Unsanctioned</i>—Classify the selected BSS as unsanctioned. • <i>Neighboring</i>—Classify the selected BSS as a neighboring device.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Forensic Analysis	Opens the Forensic Analysis-Basic on page 391 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 on page 719 window for the selected BSS; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the Port Lookup on page 741 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 on page 409 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 on page 810 for more information.)
Copy MAC	Copies the MAC address of the selected BSS for later use.

BSS 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 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](#) on page 511


This configuration profile is located in the [Configuration Tab](#) on page 495.

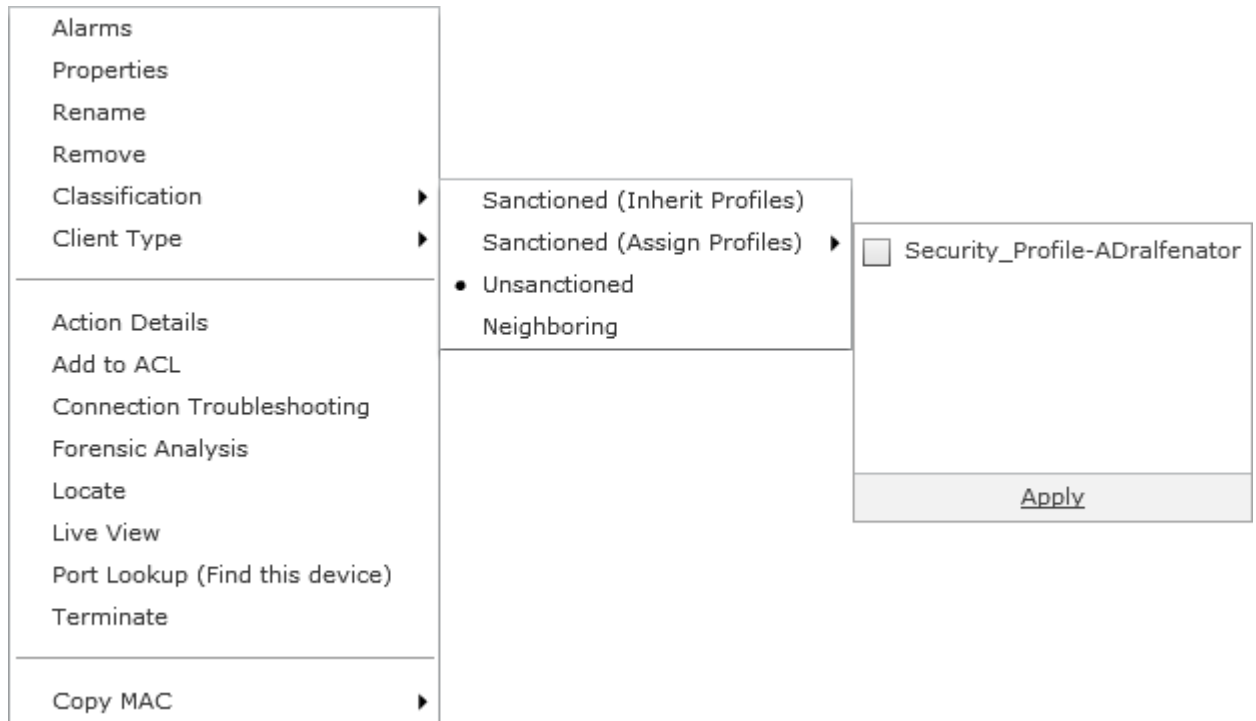
If you make changes, click **Save** to save them.

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

Click the **i** button to close the Properties overlay.











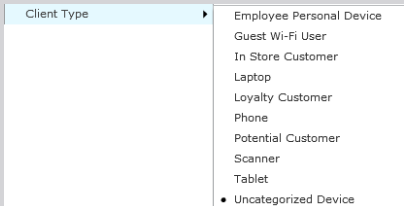
Wireless Clients Drop-down Menu

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:

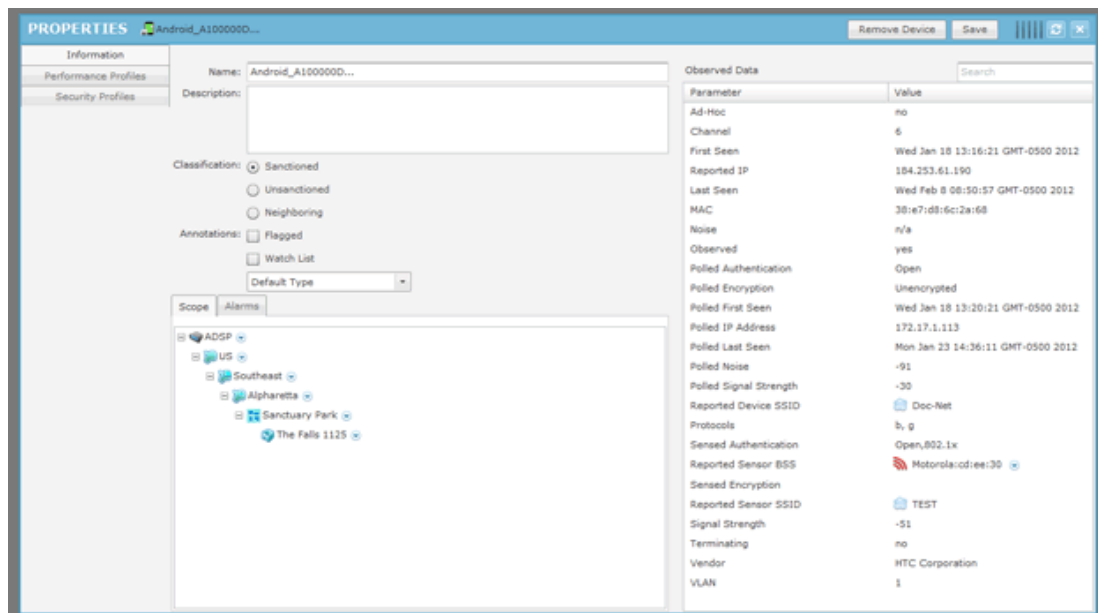
Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Wireless Client. See Alarms on page 480 for more information.
Properties	Opens the Properties overlay for the selected Wireless Client.
Rename	Opens a dialog window to rename the selected Wireless Client.
Remove	Removes the selected Wireless Client from your network. See Remove Devices on page 473 for more information.

Function	Description
Classification	<p>Classifies the Wireless Client using one of the following classifications:</p> <ul style="list-style-type: none"> • <i>Sanctioned (inherit)</i>— Classify the selected Wireless Client as a sanctioned device that inherits its traits from wherever its location in the network tree. • <i>Sanctioned (override)</i>— 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. • <i>Unsanctioned</i>— Classify the selected Wireless Client as unsanctioned. • <i>Neighboring</i>— Classify the selected Wireless Client as a neighboring device.
Client Type	<p>Client Type appears in the menu only when a Wireless Client is sanctioned. As default, Wireless Clients are assumed to be laptops, displaying a laptop icon. This menu item allows you to differentiate phones and hand-held devices from laptops in ADSP.</p> <ul style="list-style-type: none"> • Employee Personal Device  • Guest Wi-Fi User  • In Store Customer  • Laptop  • Loyalty Customer  • Phone  • Potential Customer  • Scanner  • Tablet  • Uncategorized Device   <ul style="list-style-type: none"> • Select the appropriate device to represent a Wireless Client and use its icon for the selected Wireless Client throughout the GUI.
Action Details	<p>Displays a table listing specific actions that are occurring to devices seen on your WLAN.</p>
Add to ACL	<p>Adds the selected Wireless Client to the Access Control List (ACL).</p>

Function	Description
Connection Troubleshooting	Opens Connection Troubleshooting so that you can troubleshoot a Wireless Client's ability to connect to your wireless network.
Forensic Analysis	Opens the Forensic Analysis-Basic on page 391 window for the specified Wireless Client.
Locate	Opens the Floor Plan and adds the Wireless Client to the Location Tracking list so that you can quickly locate the selected Wireless Client.
Live View	Opens the Live View on page 719 window for the selected Wireless Client; allows you to analyze current WLAN activity on the device.
Port Lookup	Opens the Port Lookup on page 741 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 on page 757 for more information.)
Copy MAC	Copies the MAC address of the selected Wireless Client for later use.

Wireless Clients - Properties

You can view the properties of a Wireless Client by clicking the drop-down menu button  and clicking **Properties**.



The screenshot displays the 'PROPERTIES' window for a wireless client named 'Android_A100000D...'. The window is divided into several sections:

- Information:**
 - Name: Android_A100000D...
 - Description: (Empty)
 - Classification: Sanctioned, Unsanctioned, Neighboring
 - Annotations: Flagged, Watch List
 - Scope: Alarms (Expanded to show a tree view: ADSP > US > Southeast > Alpharetta > Sanctuary Park > The Falls 1125)
- Observed Data:** A table with columns for Parameter and Value.

Parameter	Value
Ad-Hoc	no
Channel	6
First Seen	Wed Jan 18 13:16:21 GMT-0500 2012
Reported IP	194.253.61.190
Last Seen	Wed Feb 8 08:50:57 GMT-0500 2012
MAC	38:e7:d8:6c:2a:68
Noise	n/a
Observed	yes
Polled Authentication	Open
Polled Encryption	Unencrypted
Polled First Seen	Wed Jan 18 13:20:21 GMT-0500 2012
Polled IP Address	172.17.1.113
Polled Last Seen	Mon Jan 23 14:36:11 GMT-0500 2012
Polled Noise	-91
Polled Signal Strength	-30
Reported Device SSID	Doc-Net
Protocols	b, g
Sensed Authentication	Open,802.1x
Reported Sensor BSS	Motorola:cd:ee:30
Sensed Encryption	
Reported Sensor SSID	TEST
Signal Strength	-51
Terminating	no
Vendor	HTC Corporation
WLAN	1

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](#) on page 540
- [Security Profiles](#) on page 511.


These configuration settings (or profiles) are all located in the [Configuration Tab](#) on page 495.

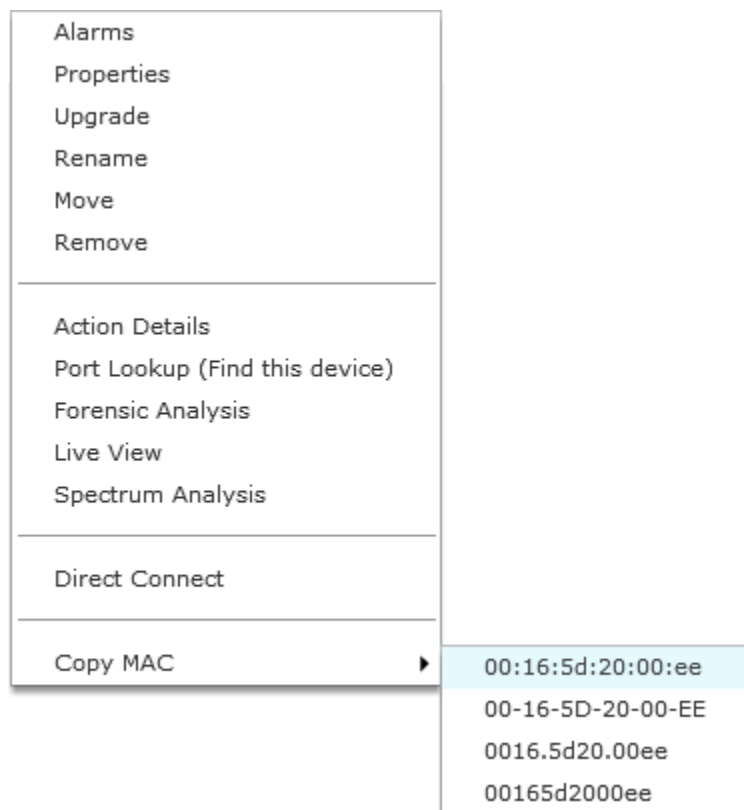
If you make changes, click **Save** to save them.

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

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

Sensors 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.




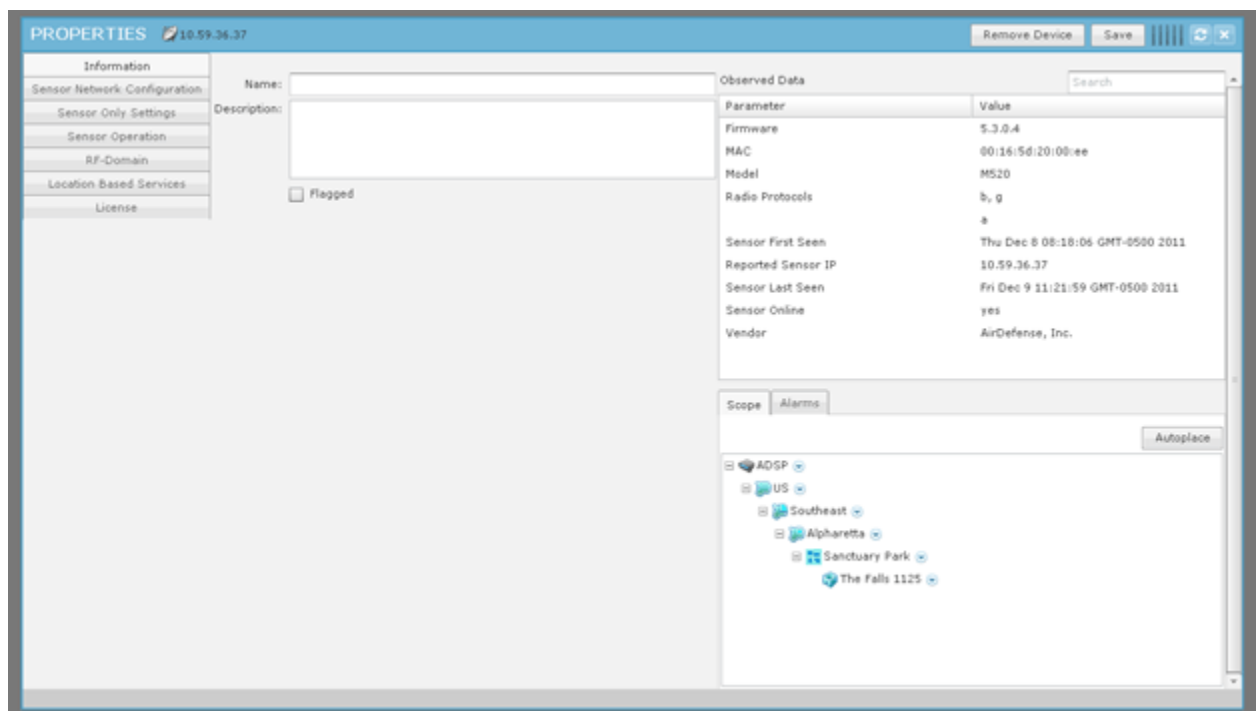
The drop-down menu for Sensors contains the following functions:

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.
Rename	Opens a dialog window to rename the selected Sensor.
Move	Moves the selected Sensor to another network level (floor). (See Move Devices on page 473 for more information.)
Remove	Removes the selected Sensor from your network. See Remove Devices on page 473 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 on page 391 window for the specified Sensor.
Live View	Opens the Live View on page 719 window for the selected Sensor; allows you to analyze current WLAN activity on the device.

Function	Description
Spectrum Analysis	Accesses Spectrum View to identify and locate interference sources on your wireless network. (See Spectrum Analysis on page 746 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.

Sensor - 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](#) on page 706
- [Sensor Only Settings](#) on page 630
- [Sensor Operation](#) on page 634
- [Location Based Services](#) on page 613

These configuration settings (or profiles), except Sensor Network Configuration, are all located in the [Configuration Tab](#) on page 495.

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](#) on page 706
- [IPv6](#) on page 707
- [DNS](#) on page 707

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.

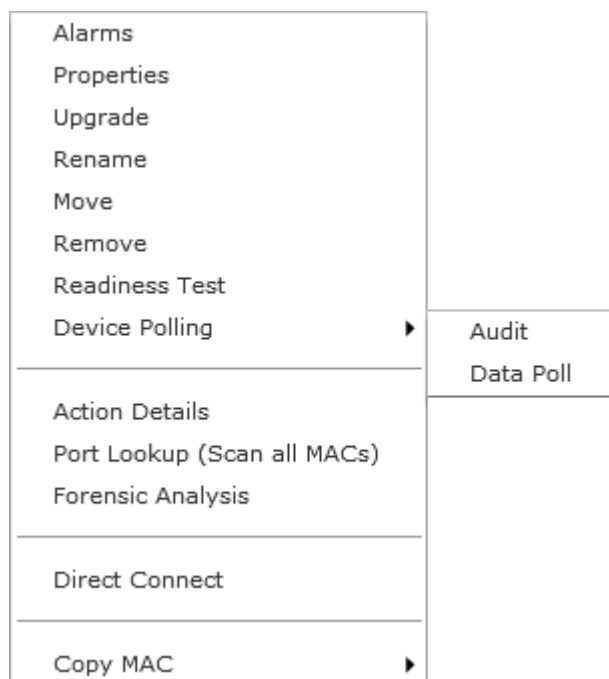
Field	Description
Use DHCP	Select the checkbox to enable DHCP.
IP Address	Manually enter a static IP address for the Sensor.
Prefix Length	Specify the static prefix length as a decimal value.
Gateway	Manually assign a valid static Gateway IP address to the Sensor.

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.

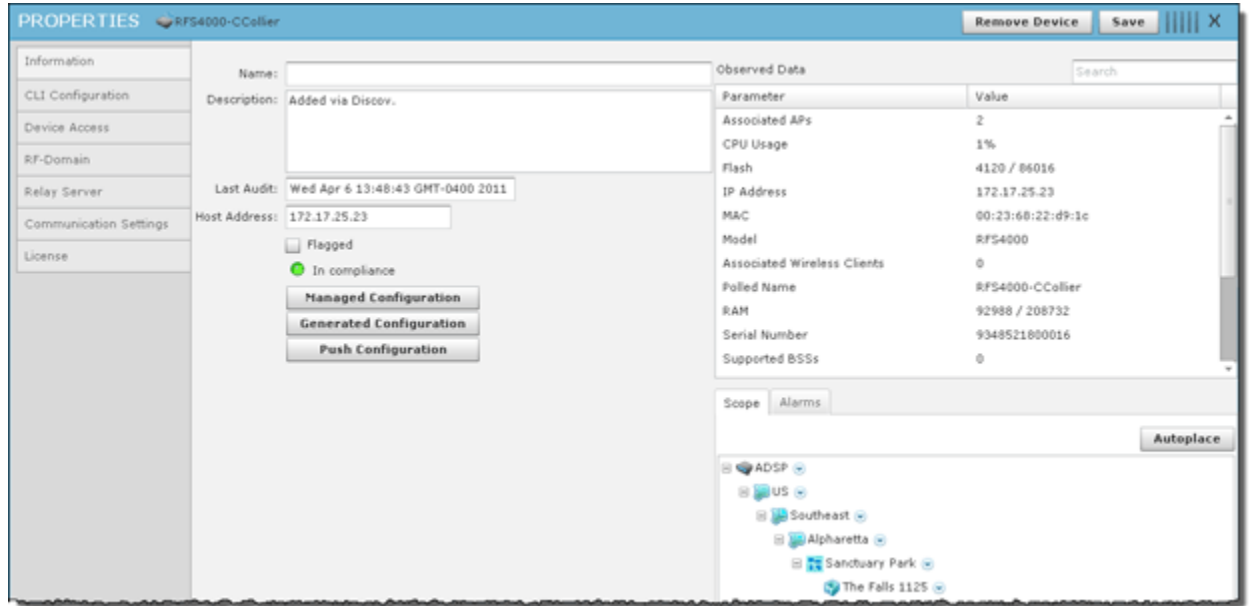


The drop-down menu for Wireless Switches contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Wireless Switch. See Alarms on page 480 for more information.
Properties	Opens the Properties overlay for the selected Wireless Switch.
Upgrade	Upgrades the firmware for the selected Wireless Switch.
Rename	Opens a dialog window to rename the selected Wireless Switch.
Move	Moves the selected Wireless Switch to another network level (floor). See Move Devices on page 473 for more information.
Remove	Removes the selected Wireless Switch from your network. See Remove Devices on page 473 for more information.
Readiness Test	Validates that the Wireless Switch is management ready (that is, it can be managed through ASDP). You are alerted of problem areas. (See Readiness Test on page 743 for more information.)
Device Polling	Conducts a compliance audit or a data poll on the selected Wireless Switch.
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. See Port Lookup on page 741 for more information.
Forensic Analysis	Opens the Forensic Analysis Basic window for the specified Wireless Switch. See Forensic Analysis-Basic on page 391 for more information.
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.

Wireless Switch - 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 Data 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.

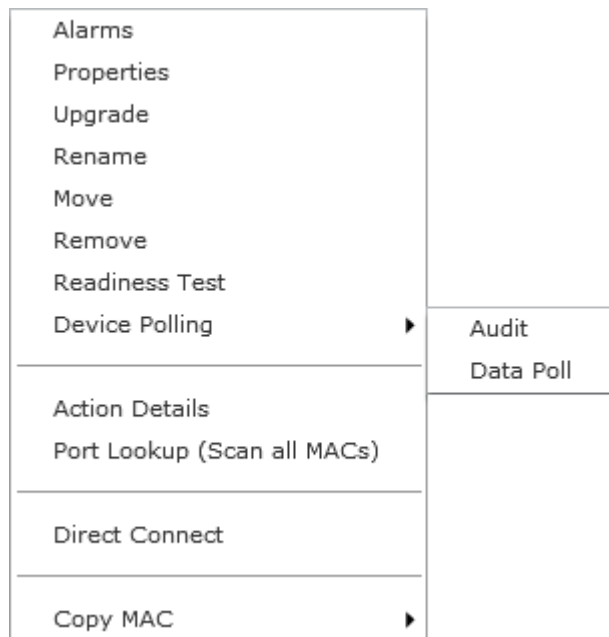
If you make changes, click **Save** to save them.

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. See Alarms on page 480 for more information.
Properties	Opens the Properties overlay for the selected Wired Switch.
Upgrade	Upgrades the firmware for the selected Wired Switch.
Rename	Opens a dialog window to rename the selected Wired Switch.
Move	Moves the selected Wired Switch to another network level (floor). See Move Devices on page 473 for more information.
Remove	Removes the selected Wired Switch from your network. See Remove Devices on page 473 for more information.
Readiness Test	Validates that the Wired Switch is management ready (that is, it can be managed through ASDP). You are alerted of problem areas. (See Readiness Test on page 743 for more information.)

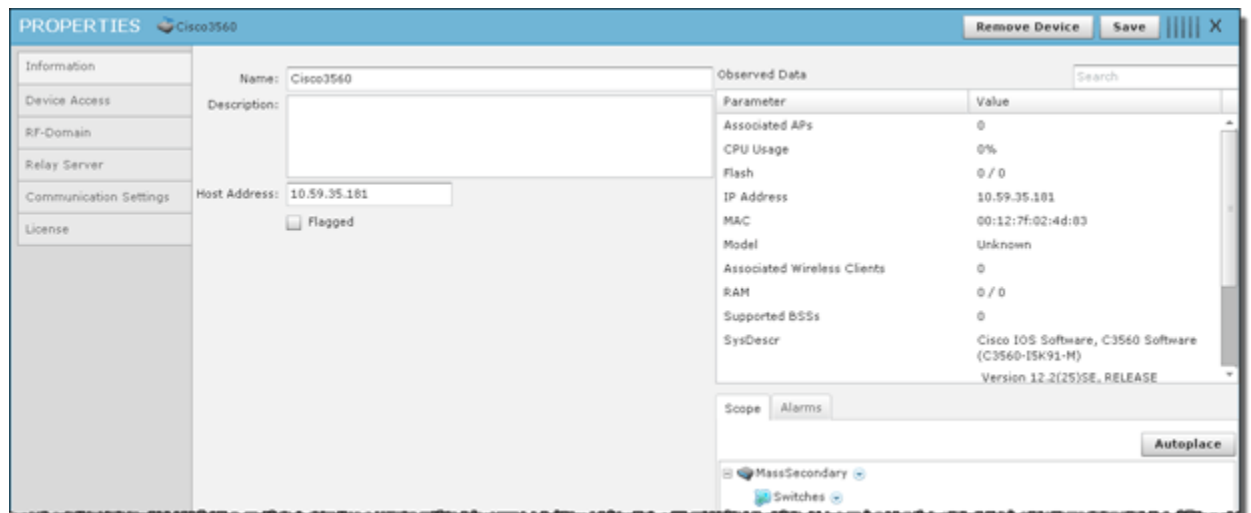
Function	Description
Device Polling	Conducts a compliance audit or a data poll on the selected Wired Switch.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup (Scan all MACs)	Scans MAC Addresses to view a list of switch ports. See Port Lookup on page 741 for more information.
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.

Wired Switch - 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.

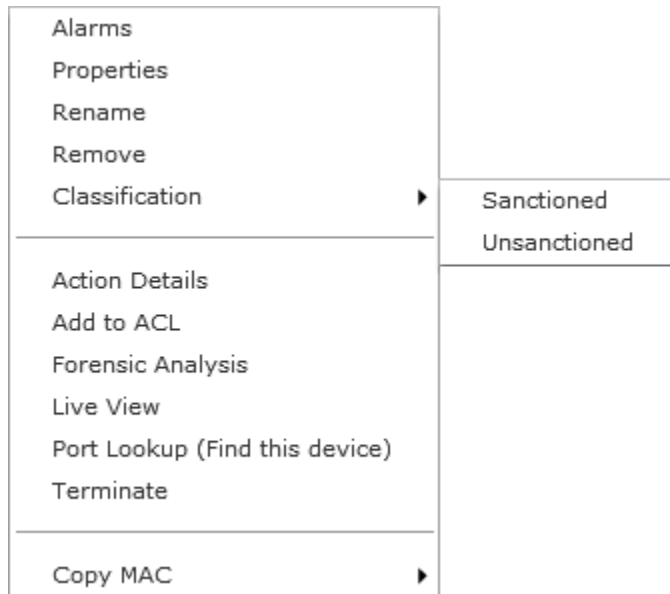
If you make changes, click **Save** to save them.

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.



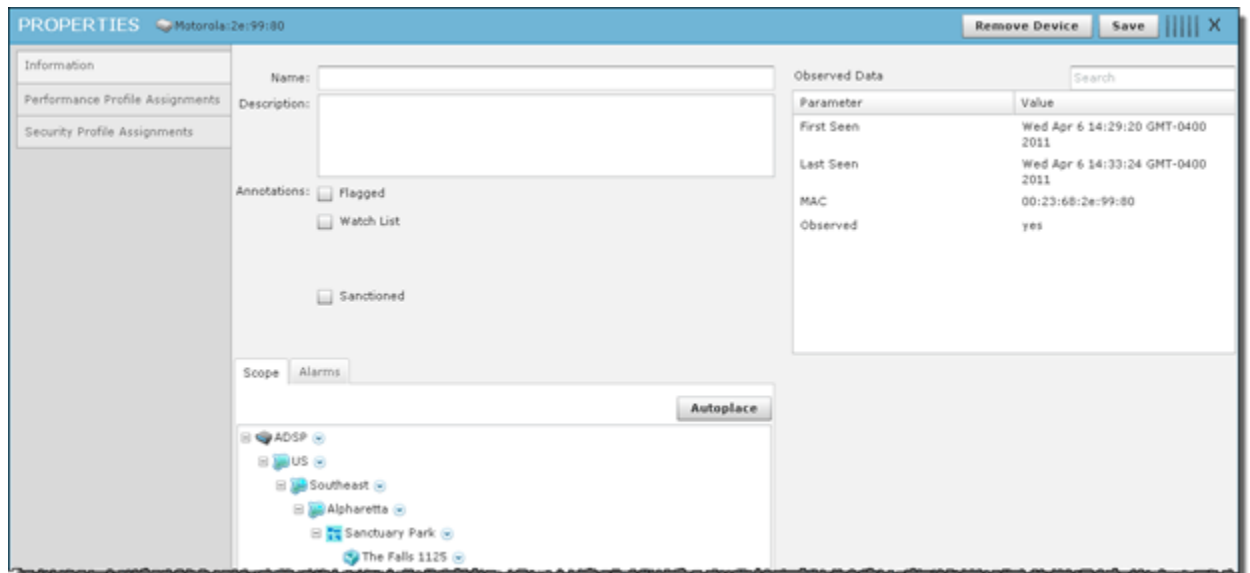
The drop-down menu for unknown devices contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected unknown device. See Alarms on page 480 for more information.
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 on page 473 for more information.

Function	Description
Classification	Classifies the unknown device as Sanctioned or Unsanctioned.
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Add to ACL	Adds the selected Unknown Device to the Access Control List (ACL).
Forensic Analysis	Opens the Forensic Analysis - 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.

Unknown Devices - 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](#) on page 495.

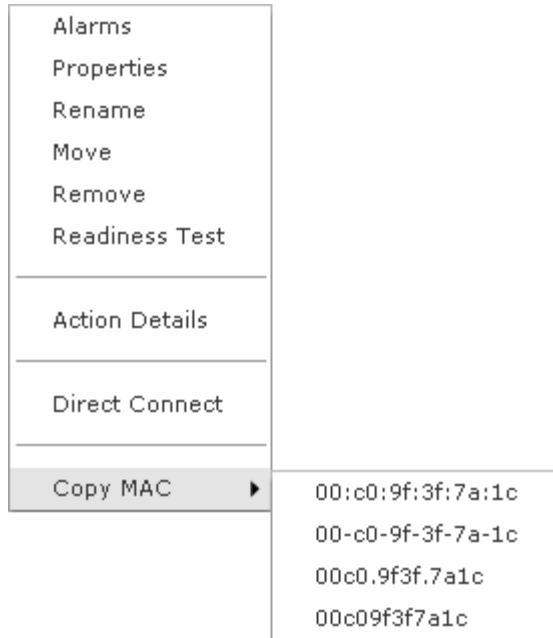
If you make changes, **Save** to save them.

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.

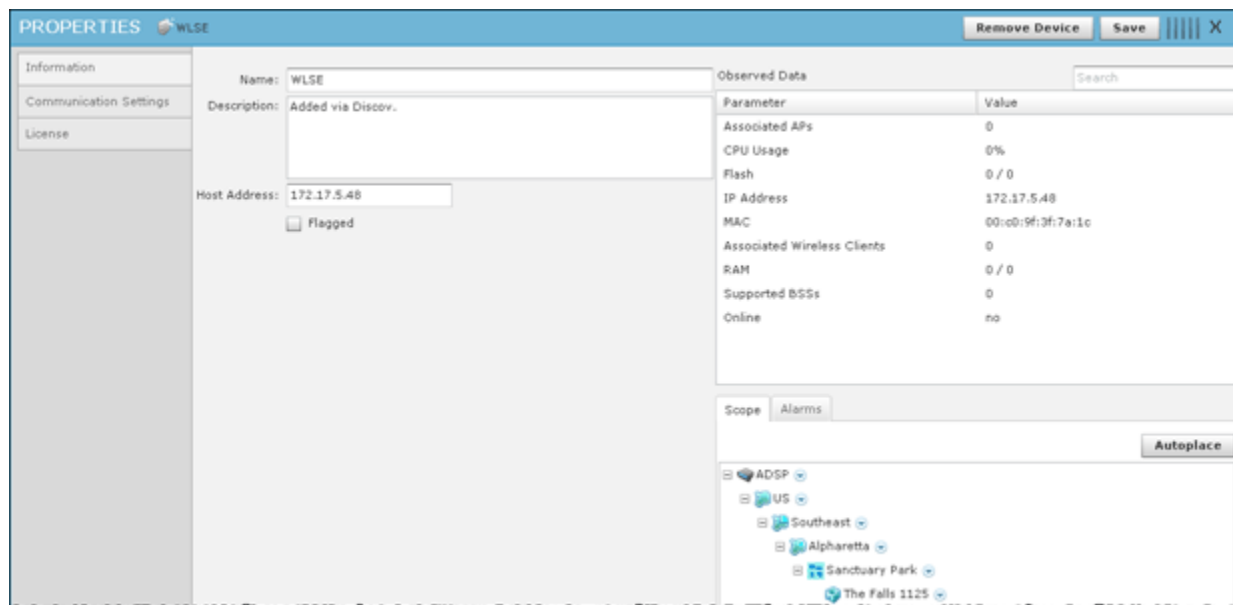


The drop-down menu for WLSE devices contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected WLSE device. See Alarms on page 480 for more information.
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 on page 473 for more information.
Remove	Removes the selected WLSE device from your network. See Remove Devices on page 473 for more information. i
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 on page 743 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.

WLSE - 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. These configuration settings are all located in the [Configuration Tab](#) on page 495.


You can display valid licenses for a WLSE by selecting **License**.

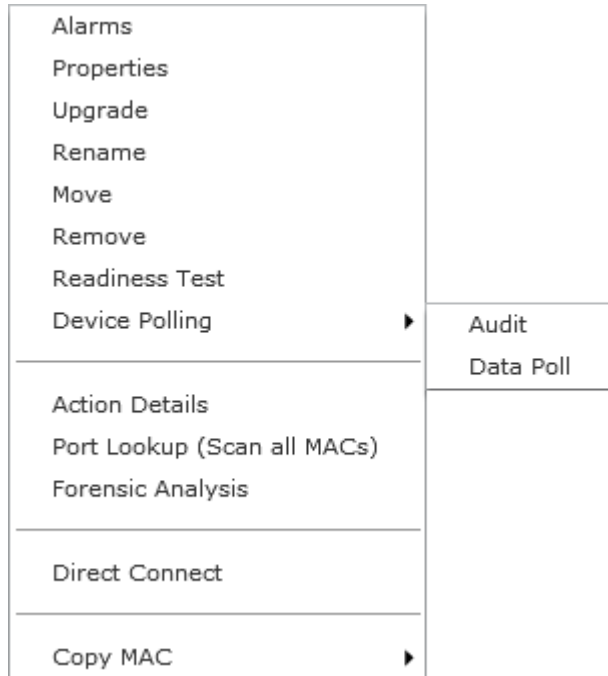
If you make changes, click **Save** to save them.

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

Click the **i** 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.




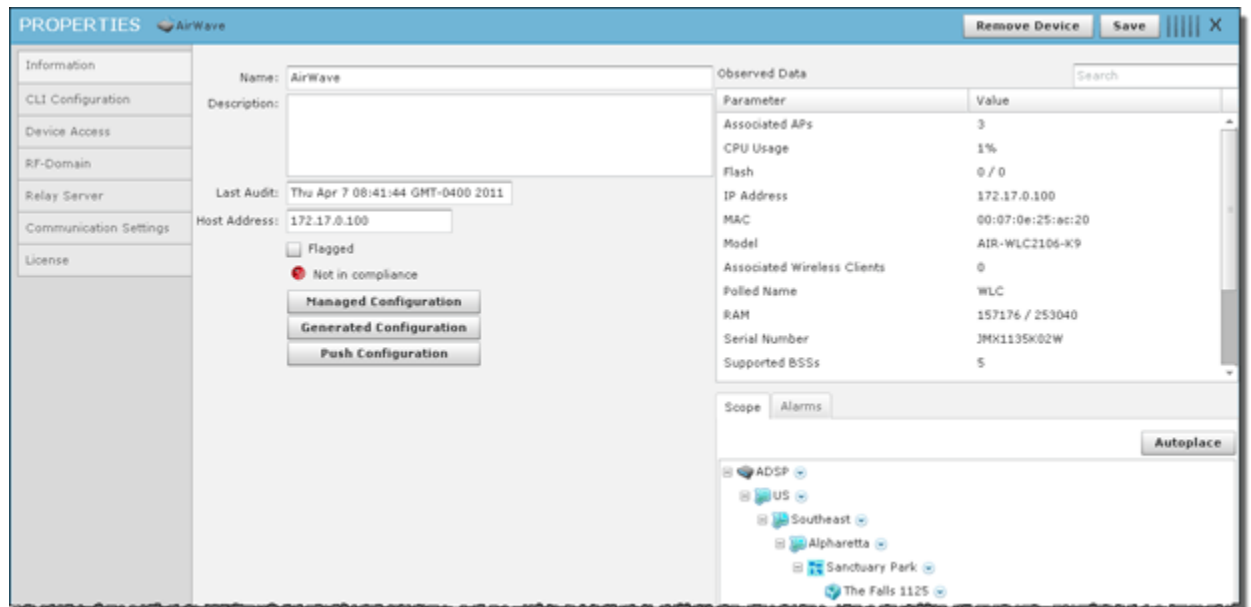
The drop-down menu for AirWave devices contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected AirWave device. See Alarms on page 480 for more information.
Properties	Opens the Properties overlay for the selected AirWave device.
Upgrade	Upgrade the firmware for the selected AirWave switch.
Rename	Opens a dialog window to rename the selected AirWave device.
Move	Moves the selected AirWave device to another network level (floor). See Move Devices on page 473 for more information.
Remove	Removes the selected AirWave device from your network. See Remove Devices on page 473 for more information.
Readiness Test	Validates that the AirWave device is management ready (that is, it can be managed through ASDP). You are alerted of problem areas. See Readiness Test on page 743 for more information.
Device Polling	Conduct a compliance audit on the selected AirWave switch.

Function	Description
Action Details	Displays a table listing specific actions that are occurring to devices seen on your WLAN.
Port Lookup (Scan all MACs)	Scan MAC addresses to view a list of switch ports. See Port Lookup for more information.
Forensic Analysis	Opens the Forensic Analysis—Basic window for the specified AirWave switch. See Forensic Analysis-Basic on page 391 for more information.
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.

AirWave Switch - Properties

You can view the properties of a AirWave switch by clicking the drop-down menu button  and clicking Properties.



The following information is displayed:

Field	Description
Name	The name of the AirWave Switch.
Description	A description of the AirWave Switch.
Last Audit	The date and time of the last audit.
Host Address	The IP address of the AirWave Switch.
Flagged	Flag a AirWave Switch that you want to bring attention to.

Field	Description
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.

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.

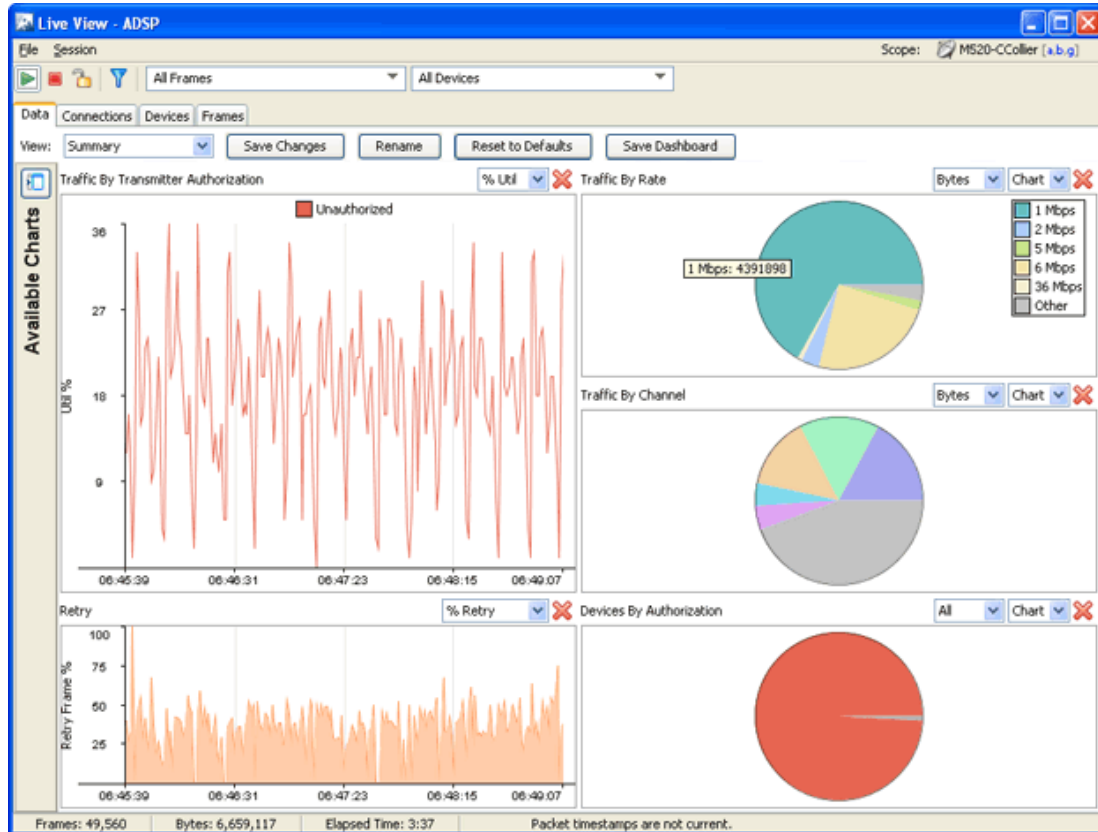
Device Functions Requiring More Explanation

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.

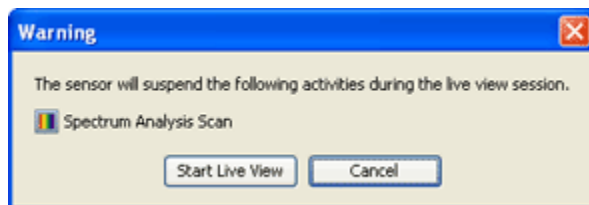
Live View

AirDefense 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.



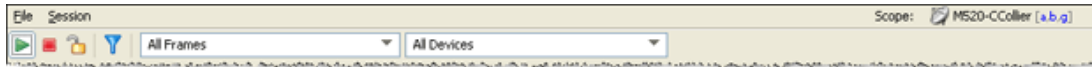
You can either start the monitoring session and suspend the Spectrum Analysis, or cancel the Live View session.

Live View consists of four main categories of information:

- Data
- Connections
- Devices
- Frames.

Common Area

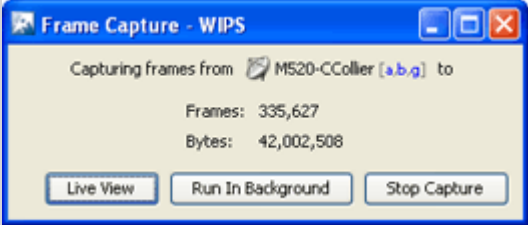
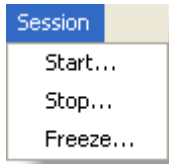
The common area holds the menus and buttons that are common to the Live View window. It is located at the top of the window.





Menus



The following menu items are available:

Menu	Option	Description
File	Open	Opens a captured frame file for viewing. See Frame Capture Analysis on page 390 for more information.
File	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 on page 735 for more information.)
File	Settings	Opens the Live View Settings popup window where you can set options for your Live View sessions. (See Live View Settings on page 723 for more information.)
File	Edit Filters	Opens the Live View Filter popup window where you can set options to filter data. (See Live View Filters on page 724 for more information.)
File	Schedule Frame Capture	Schedule a Frame Capture session using the scheduler. See Automatic Frame Captures on page 736 for more information.

Menu	Option	Description
	Reduced Bandwidth Interface	<p>Shrinks the Frame Capture window and conserves bandwidth while running Live View.</p>  <p>While in the reduced bandwidth state, you can:</p> <ul style="list-style-type: none"> 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.
<p>Session</p> 	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.

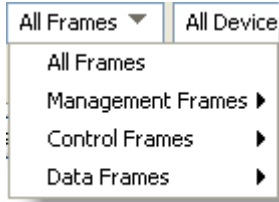
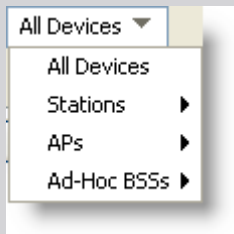
Buttons

Button	Description
	Starts a Live View session.
	Stops a Live View session.

Button	Description
	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 on page 724 for more information.)

Drop-down Menus

The following are the 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.

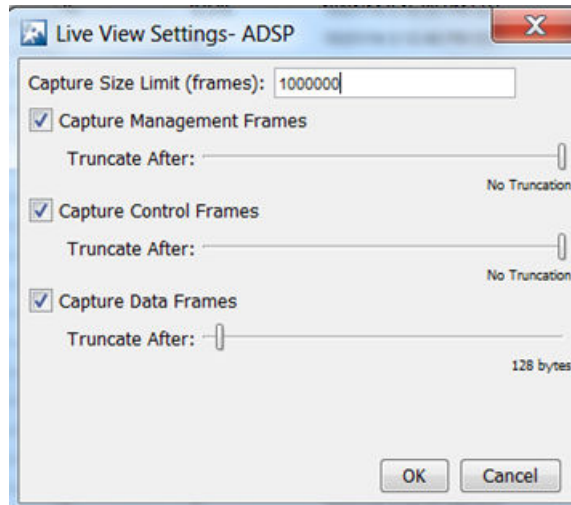
Live View Settings

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.
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:

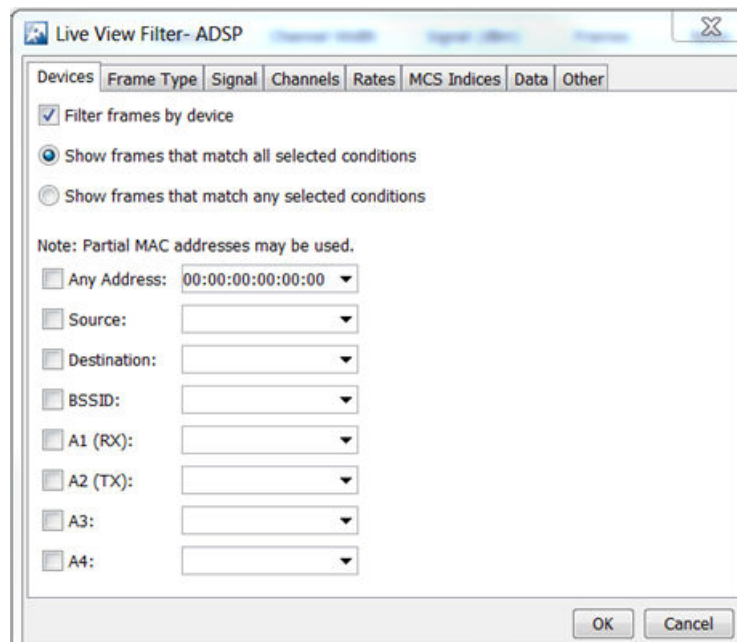
- Select **File > Settings** to display the **Live View Settings** popup window.



- Make your adjustments to the values in this screen.
- 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** pop-up window.



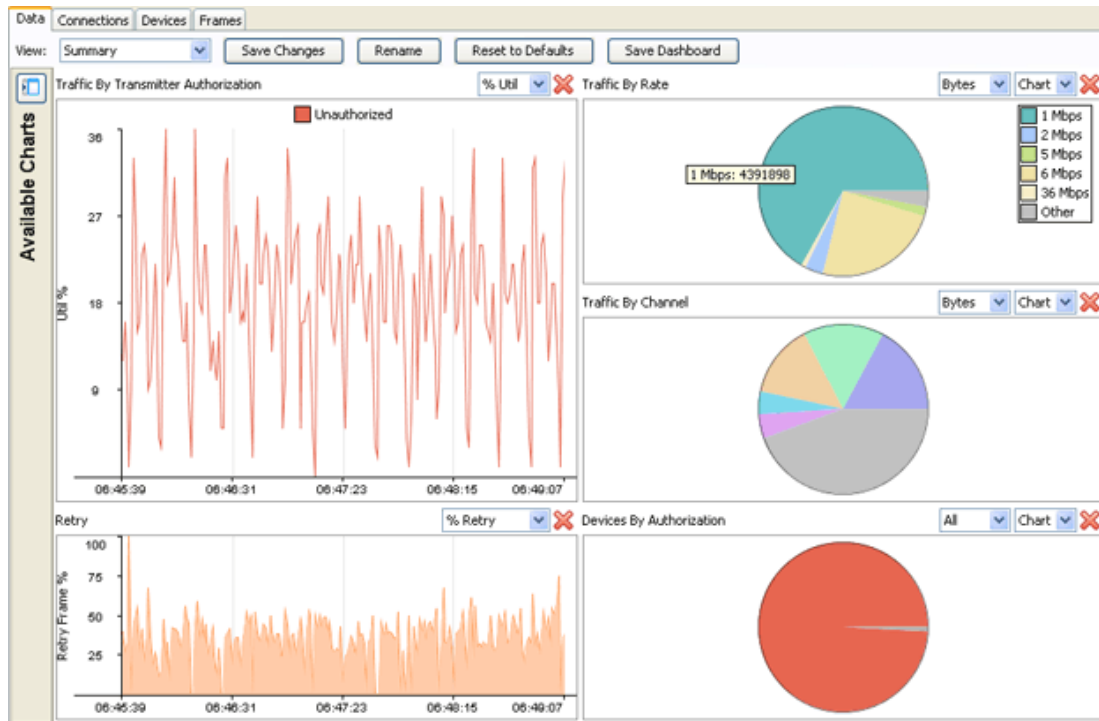
Frames may be filtered by any of the following methods:

Method	Description
Devices	<p>To filter Live View frames by devices, go to the Devices tab and check Filter frames by device. Select any of the following conditions:</p> <ul style="list-style-type: none"> • Any Address • Source • Destination • BSSID • A1 (RX) • A2 (TX) • A3 • A4 <p>For every condition that you select, you must specify a MAC address. You have the option of displaying frames that match all of the selected conditions or displaying frames that match any of the selected conditions.</p>
Frame Type	<p>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.</p>
Signal Filters	<p>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.</p>
Channel Filters	<p>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.</p>
Rates Filters	<p>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.</p>
MCS Indices	<p>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.</p>
Data Filters	<p>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.</p>
Other	<p>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.</p>

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.

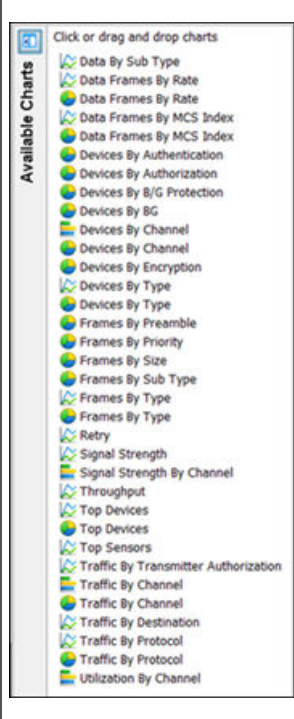



The **Data** tab focus can be changed by changing the view. Depending on the view that is selected different charts are displayed. There are four available views:


View	Description
Summary	Provides a summary of frame data using the following charts: <ul style="list-style-type: none"> • 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.

	<p>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.</p> <p>To hide Available Charts, click the Hide Available Charts button  button.</p>
--	--

To rearrange a view, you can drag and drop charts to another location.

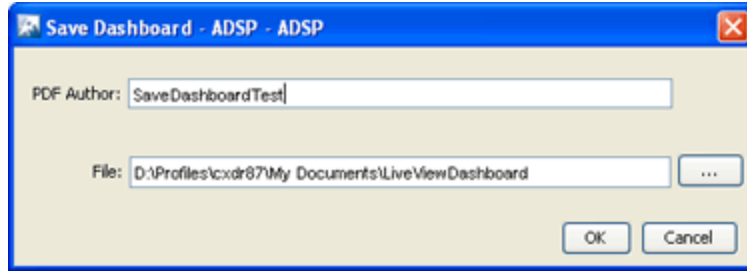
To remove a chart, click the **Remove** button  associated with the chart.

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.

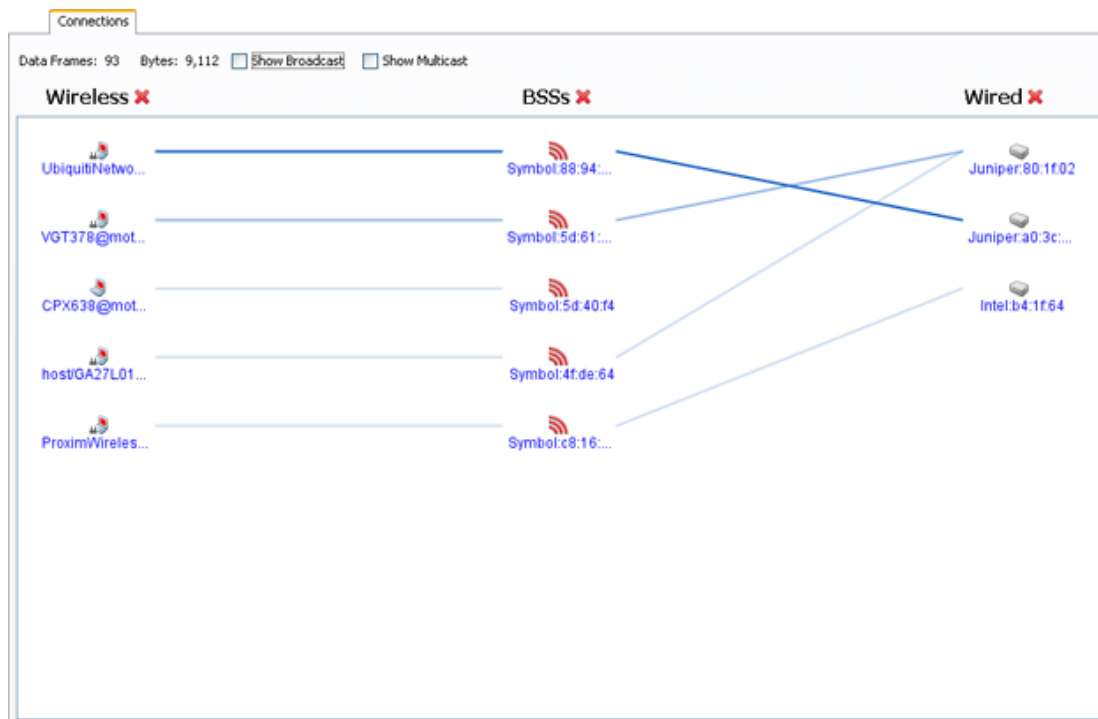
You can save a PDF file with a snapshot of the data charts by clicking the **Dashboard** button. A dialog window opens where you can name the PDF file and specify an author's name.



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.

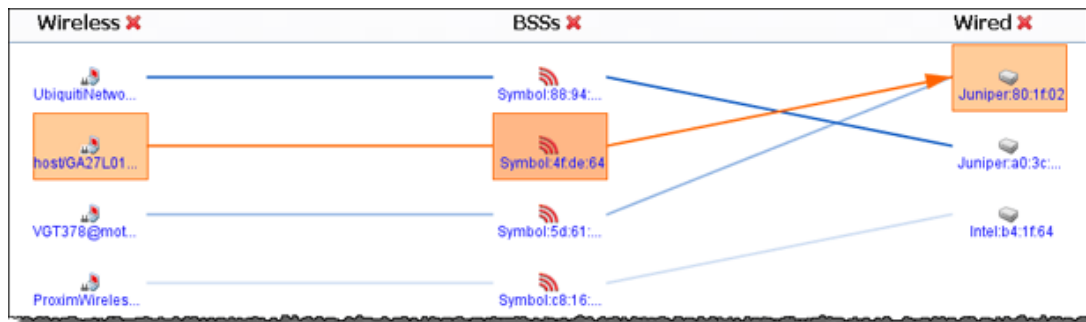
If more than 50,000 frames have been captured during the Live View session, only the most recent 50,000 frames are displayed.

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.

Showing connection 1 of 2 including Cisco:35:37:a0  

The **Data Frames** and **Bytes** fields will only show the data corresponding to the selected connection.

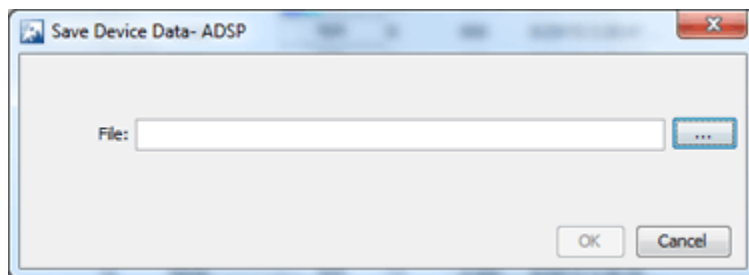
Devices Tab

The **Devices** tab displays the devices that have been seen during a Live Monitoring session in tabular 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_	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 ...		
Motorola:4e:fe:56	DevMgmt_107	149	Upper	-60	80	15,768	5/29/13 2:46:03 ...		

Options are provided to show all devices, only BSSs, Wireless Clients, or Wired Clients. If more than 50,000 frames have been captured during the live monitoring session, only the most recent 50,000 frames are displayed.

The **Export** button can be used to export device data to a CSV file.



Just browse to a folder (directory) to save the file in, type in a name, and click the **Select** button. The name of the file is displayed in the **File** field. Now, click **OK** to save the file in the selected folder (directory).

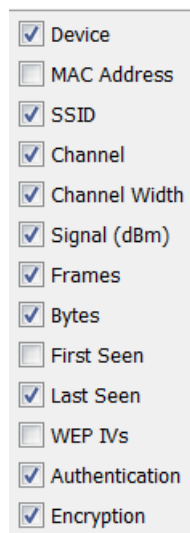
The **Devices** table can be customized to display the following information:

Column	Description
Device	Lists the different devices that have been seen during the Live Monitoring session.
MAC Address	Displays the MAC address of the seen device.

Column	Description
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.

Time	Source	Destination	BSSID	Observe...	Channel...	Rate	Signal (d...)	Size	Protocol
15:51:08.1...	Motorola:48:83:6c	Intel:a1:b3:2c	Motorola:48:83:6c44		None	6 Mbps	-67	213	Probe response
15:51:08.1...	Symbol:c8:46:30	Broadcast	Symbol:c8:46:30 44		None	6 Mbps	-70	230	Beacon
15:51:08.1...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f0 44		None	6 Mbps	-83	160	Beacon
15:51:08.1...	Symbol:c8:46:31	Broadcast	Symbol:c8:46:31 44		None	6 Mbps	-70	196	Beacon
15:51:08.1...	Symbol:e4:ea:70	Broadcast	Symbol:e4:ea:70 44		None	6 Mbps	-76	97	Beacon
15:51:08.1...	Motorola:48:83:6c	Broadcast	Motorola:48:83:6c44		None	6 Mbps	-67	202	Beacon
15:51:08.1...	Symbol:c8:46:32	Broadcast	Symbol:c8:46:32 44		None	6 Mbps	-71	205	Beacon
15:51:08.1...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f0 44		None	6 Mbps	-83	160	Beacon
15:51:08.2...	Symbol:c8:46:30	Broadcast	Symbol:c8:46:30 44		None	6 Mbps	-70	230	Beacon
15:51:08.2...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f0 44		None	6 Mbps	-83	160	Beacon
15:51:08.2...	Motorola:43:cb:3c	Broadcast	Motorola:43:cb:3c13		None	1 Mbps	-74	212	Beacon
15:51:08.2...	Symbol:c8:46:31	Broadcast	Symbol:c8:46:31 44		None	6 Mbps	-70	196	Beacon
15:51:08.2...	Symbol:e4:ea:70	Broadcast	Symbol:e4:ea:70 44		None	6 Mbps	-76	97	Beacon
15:51:08.2...	Motorola:48:83:6c	Broadcast	Motorola:48:83:6c44		None	6 Mbps	-67	202	Beacon
15:51:08.2...	Motorola:43:cb:31	Broadcast	Motorola:43:cb:3113		None	1 Mbps	-75	232	Beacon
15:51:08.2...	Symbol:c8:46:32	Broadcast	Symbol:c8:46:32 44		None	6 Mbps	-70	205	Beacon
15:51:08.2...	Motorola:20:ba:f0	Broadcast	Motorola:20:ba:f0 44		None	6 Mbps	-83	160	Beacon
15:51:09.3...	Motorola:43:db:1c	Broadcast	Motorola:43:db:1c1		None	1 Mbps	-72	148	Beacon
15:51:09.3...	Cisco:df:3d:a0	Broadcast	Cisco:df:3d:a0 1		None	1 Mbps	-83	195	Beacon
15:51:09.3...	Symbol:c8:3c:21	Broadcast	Symbol:c8:3c:21 1		None	1 Mbps	-82	207	Beacon
15:51:09.3...	Cisco:0c:fc:8e	Broadcast	Cisco:0c:fc:8e 1		None	1 Mbps	-80	148	Beacon

0000	80000000	fffffff	ffff5c0e	8b20bafo					
0010	5c0e8b20	bafo30b2	36783d99	10000000					
0020	32000100	000b4465	764d676d	745f3130					
0030	3201088c	129824b0	48606c05	04000100					
0040	00071255	5349240d	11340d18	64111888					
0050	05189511	1e0b0500	0000093d	a40f00a0					
0060	f8000000	00010000	003139af	4dd40700					
0070	50f20200	0180dd16	00a0f801	01010000					
0080	00000000	00000000	00000000	0000dd10					

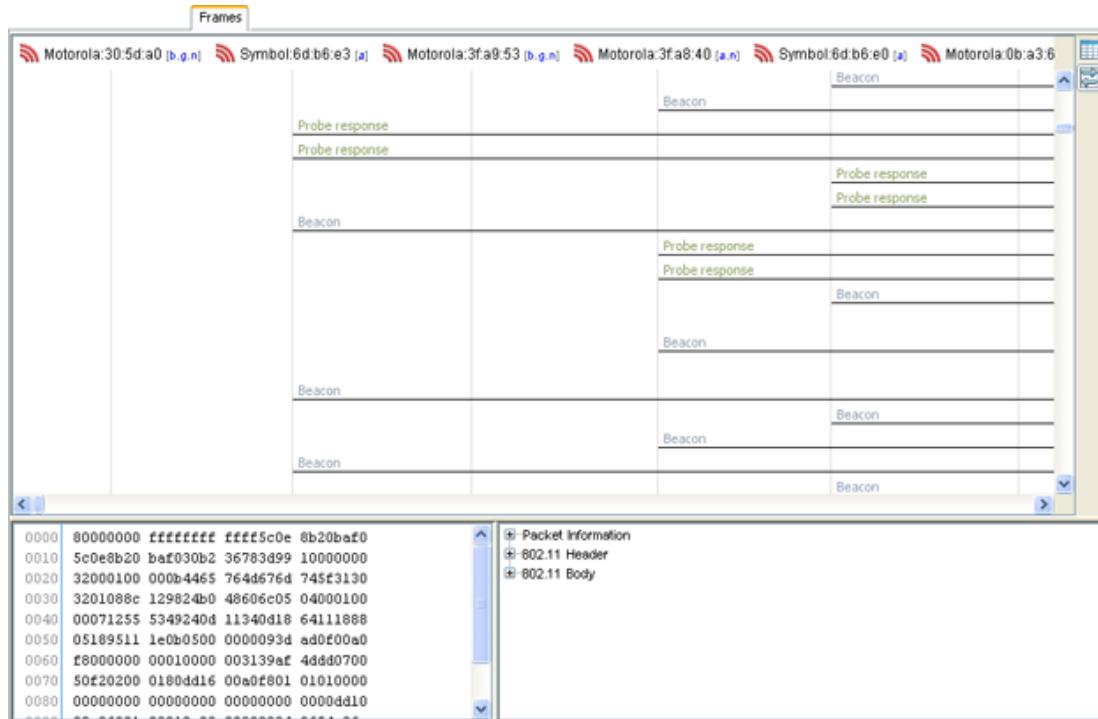
The captured file is stored in either/or, at times, both of the following directories:


```
/usr/local/smx/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

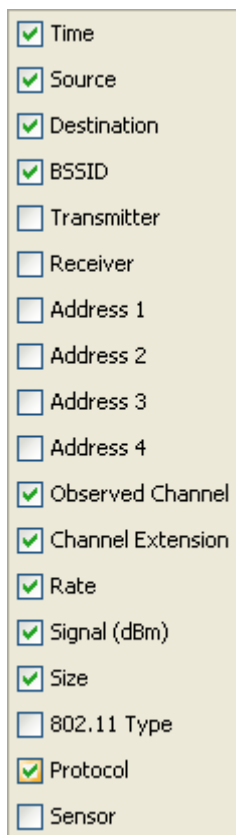
The frame table can be customized to display the following information:

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.

Column	Description
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.

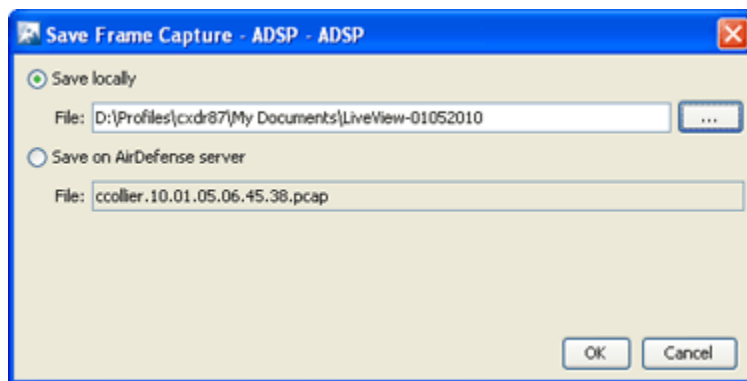
Frame Capture

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**.

Save Frame Capture to the Extreme AirDefense Server

To save the file on your AirDefense server:

1. Select the **Save on AirDefense** server radio button.



Note

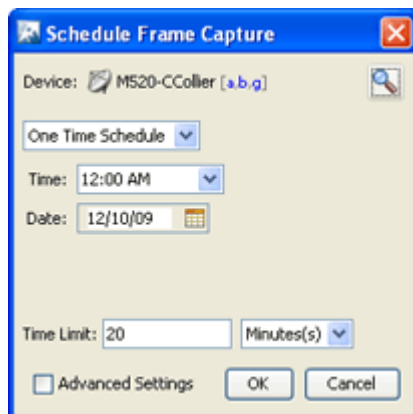
The file name is selected automatically. You cannot change it.

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:

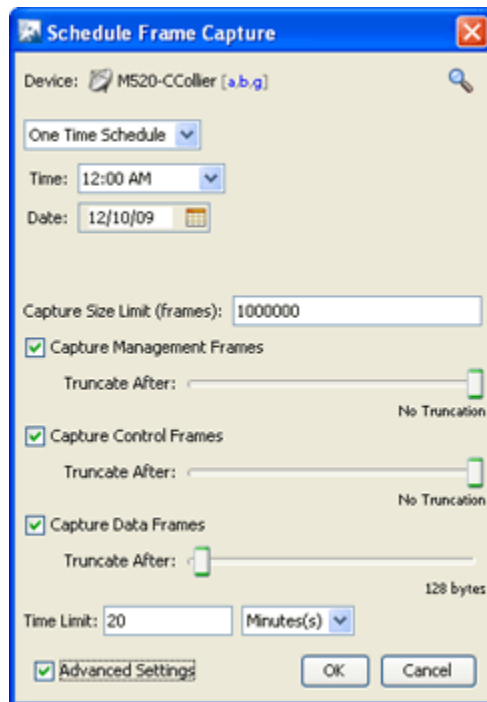
Interval	Action
One Time Schedule	Choose a time for the backup by selecting a time from the Time drop-down menu. Then, select a day for the frame capture by clicking the Calendar button in the Date field and selecting a date.
Intra-Day Schedule	Select a time to begin the frame capture. Then, select a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

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 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.

- Place a time limit on the frame capture by entering the time in the **Time Limit** field; then, select **Minute(s)** or **Hour(s)**.
- Click **OK** to set the automatic frame capture schedule.

Advanced Settings

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) AirDefense appliance.
 - Three (minimum) AirDefense 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

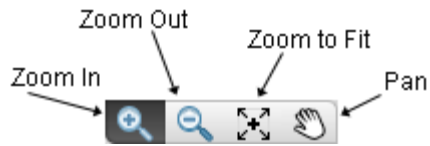
A map can only be linked to sensors on the same floor. In a multi floor building, sensors should be grouped by floors and each floor associated with its own map. At least 3 sensors per floor plan are required for location triangulation.

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 near the top-ride side of the windows 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 closer.
	Click this tool to zoom out (reduce the size) a floor plan image. Each click will zoom out further.
	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.

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.




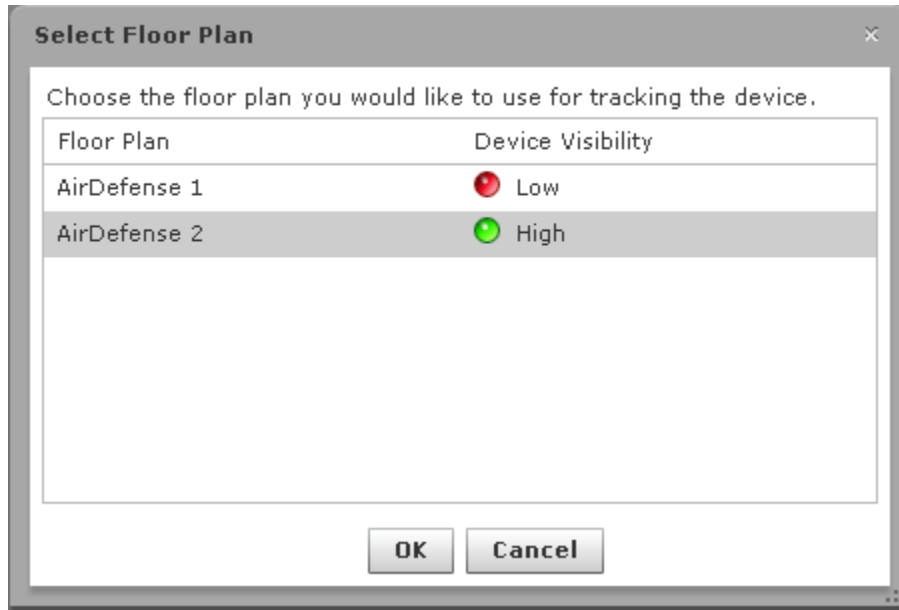
Important

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.

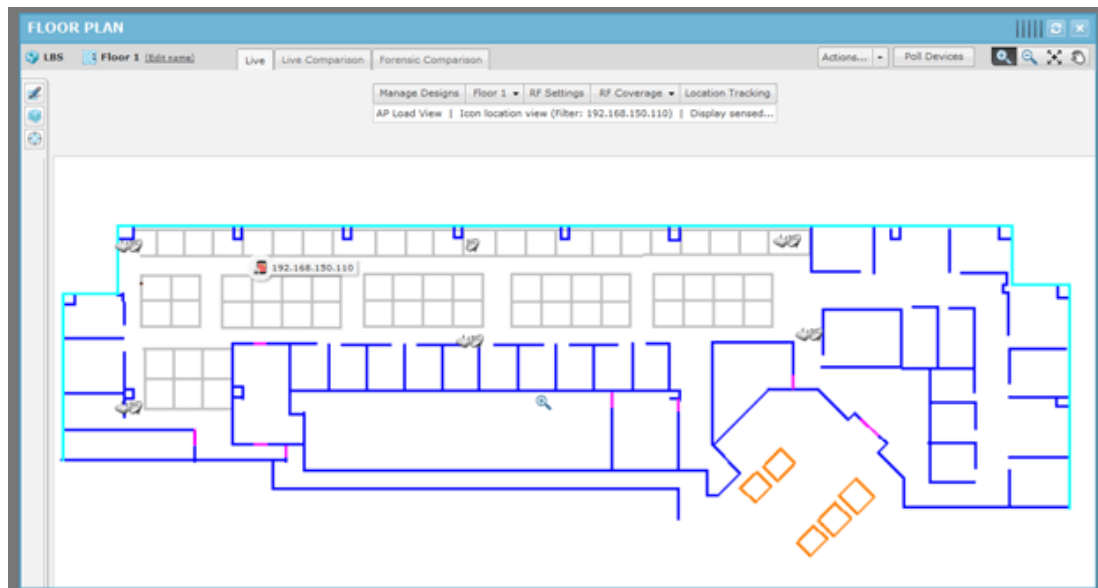
One or more maps or floor plans of the tracking coverage area are needed for this to work. You can obtain floor plans from any source, including producing your own by using drawing tools. Most applications will require multiple maps, for example, if you are setting up multiple buildings. You must supply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

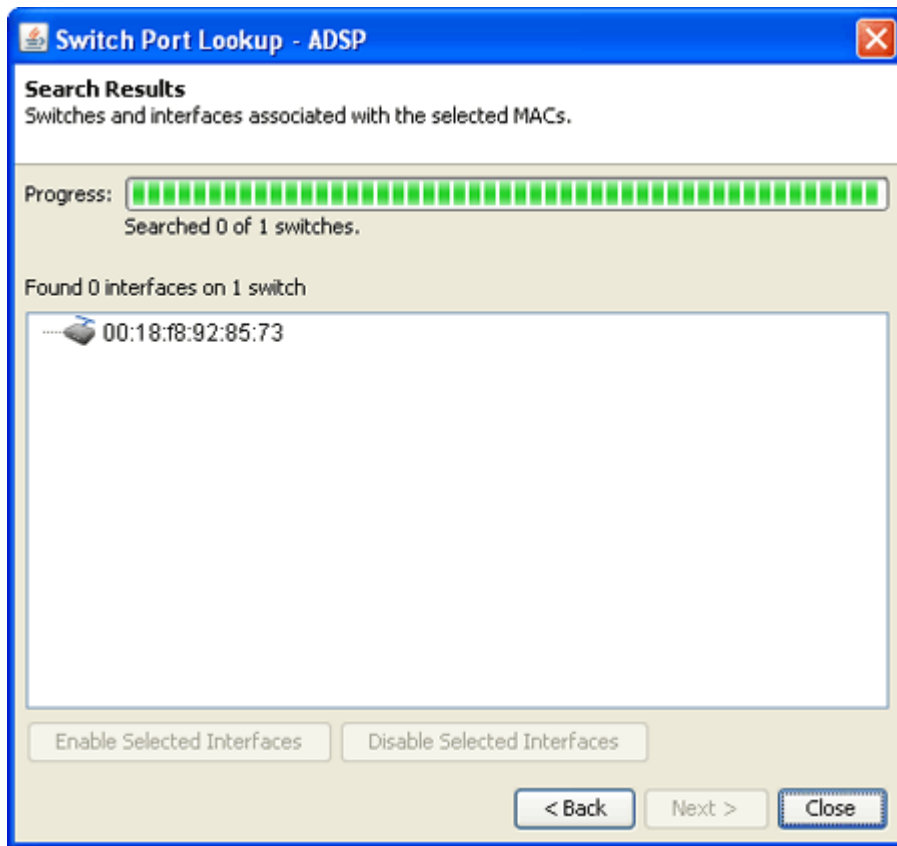
Function/Feature	Description
Search Scope	A drop-down menu that allows you to limit the scope of your search.
Selected Device	A read-only field that displays the MAC address of the selected device.
Similar MACs offset by	This function appears only if selected device is a BSS. If checked, the search includes 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

To perform Port Lookup

1. Click the  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.



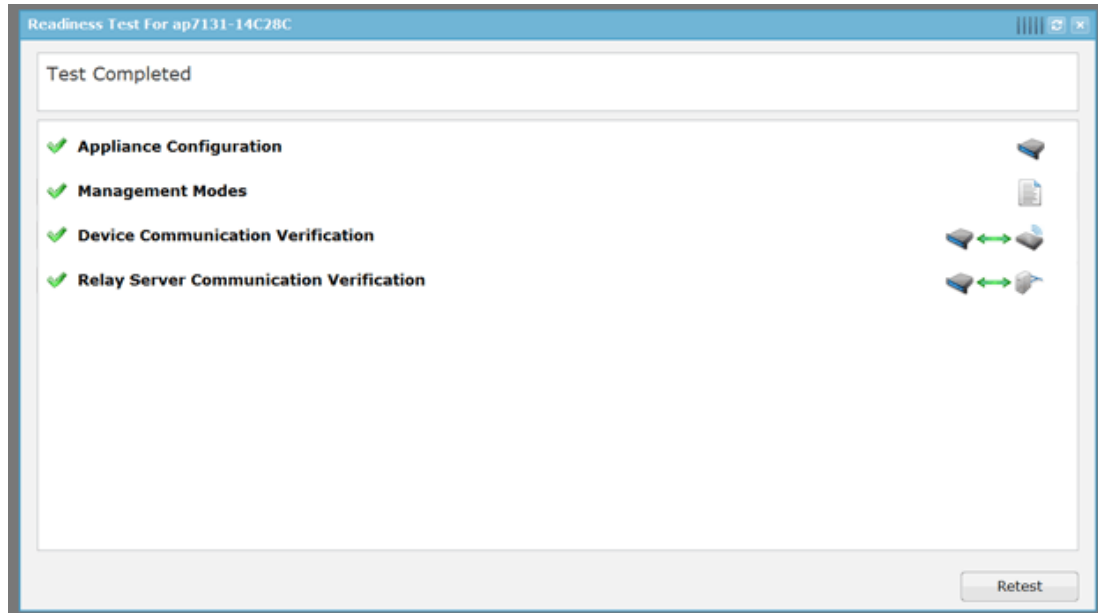
From this window, you can disable or enable a selected (highlighted) interface by clicking the appropriate button.

6. Click **Close** to exit.




Readiness Test

The **Readiness Test** checks the connections and the communication settings between AirDefense and devices in your network. The devices may be an AP, 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.

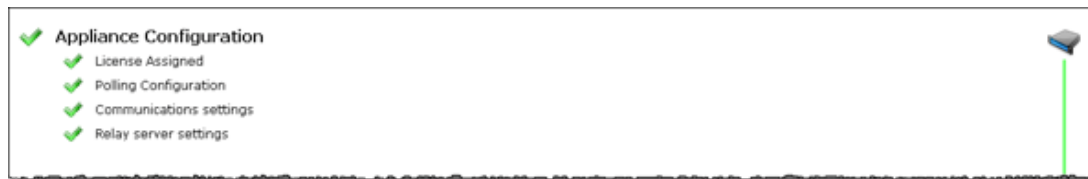
To access the Readiness Test, click **Readiness Test** from the drop-down menu of an AP, a Sensor, a Switch, or a network folder (level). A series of test are run and displayed in a **Readiness Test** overlay.



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.
- 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 AirDefense can communicate with the selected device via the CLI.
- HTTP Connection—validates that AirDefense 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.

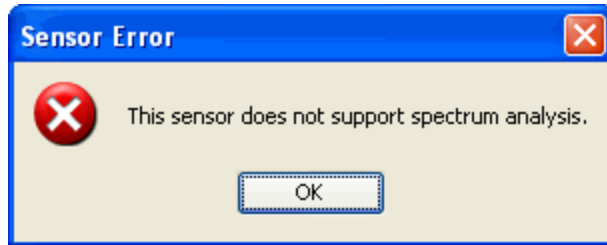
There are two ways to turn on background analysis:

- 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.

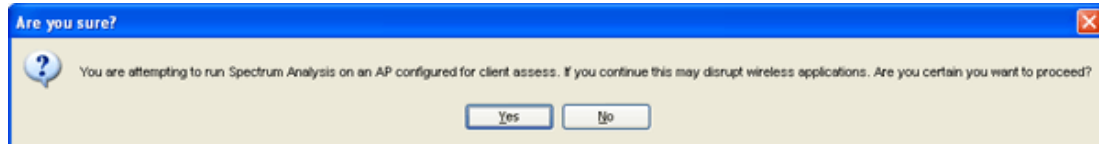
Dedicated Analysis

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:

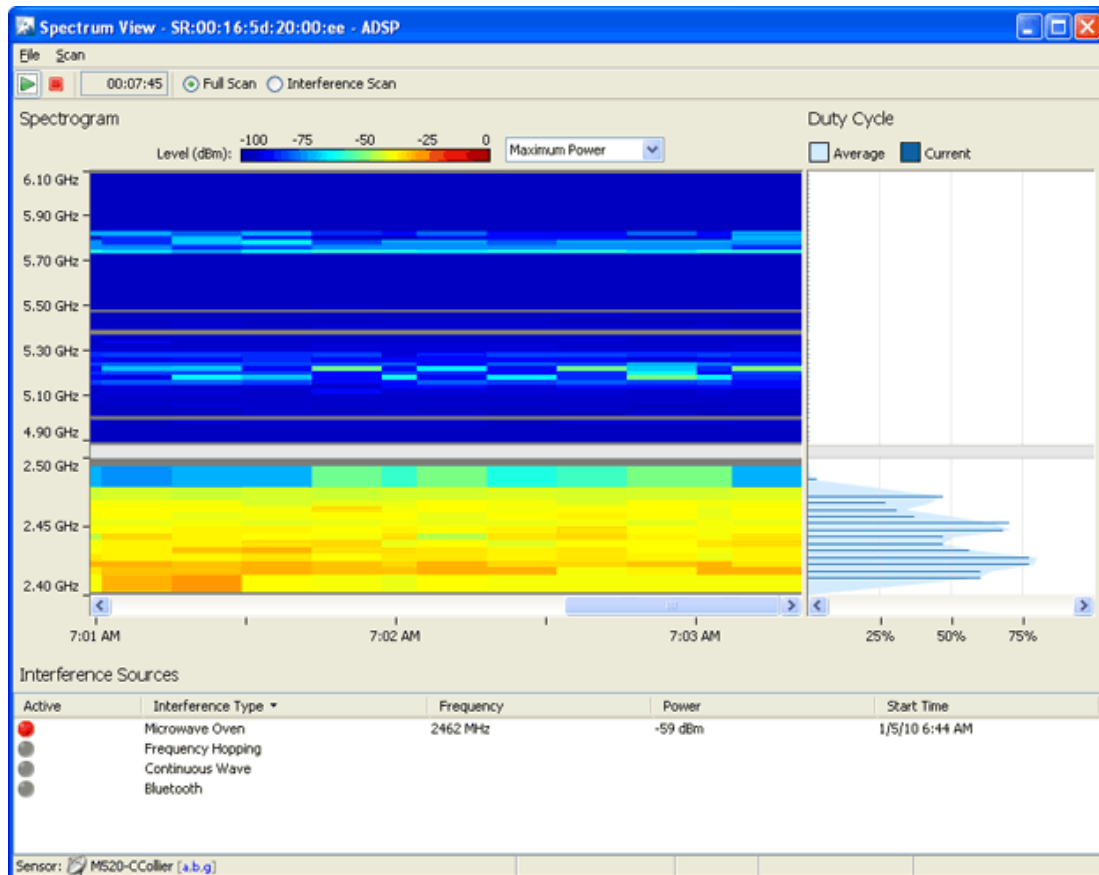


In addition, if you attempt to run Spectrum Analysis on an AP configured for client access (device configured as AP and Sensor), the following error popup may display:



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.

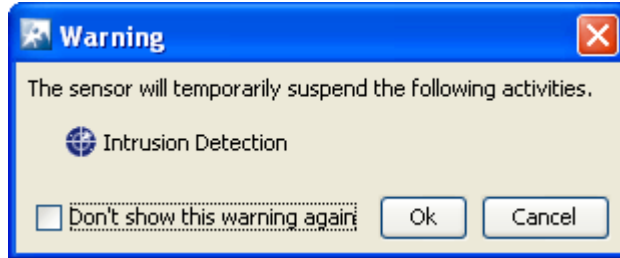
To access the **Spectrum View** window, click the drop-down menu button  for a Sensor and then select **Spectrum Analysis** from the drop-down menu.



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 temporarily suspend Intrusion Detection.



You must click **OK** to continue. You can turn the warning off by selecting the checkbox next to **Don't show this warning again**.

There are three conditions that may prevent a scan from starting. They are:

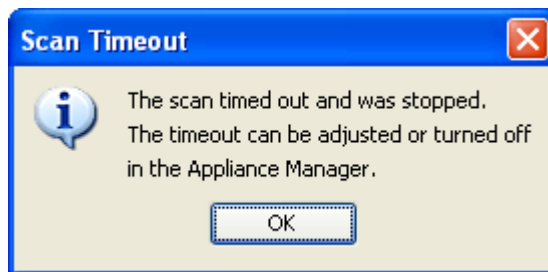
- The Sensor is already running a dedicated RF scan for any user
- Another user is running Live View on the Sensor
- Ten scans are already running (maximum supported).

You can stop a scan by clicking the Stop Scan  button or selecting **Scan > Stop Scan**.

A scan can be restarted by clicking the Start Scan  button or selecting **Scan > Start Scan**.

A counter is displayed next to the **Stop Scan** button to show how long the scan has been running.

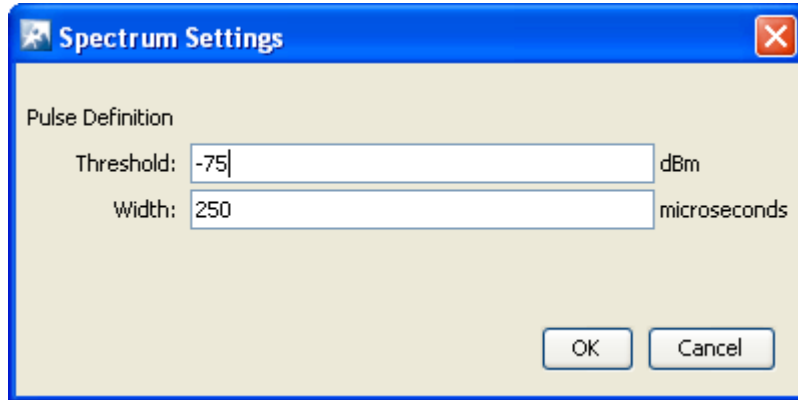
The default scanning time is 10 minutes. Scanning time can be adjusted by selecting **Configuration > Appliance Management > Appliance Settings**. If a timeout occurs, the following **Scan Timeout** popup is displayed:



Click **OK** to close the popup.

Spectrum Settings

Spectrum View lets you adjust the pulse definition via the Spectrum Settings window. To access the Spectrum Settings, select **File > Settings**.



As you can see, there are two fields for pulse definition: **Threshold** and **Width**. You can adjust the pulse threshold by typing in a new value in dBm. You can adjust the pulse width by typing in a new value in microseconds. Click **OK** to set the new values and close the window.

Scanning Modes

There are two scanning modes:

- Full Scan
- Interference Scan

Full Scan scans the entire 2.4GHz bandwidth (in 5MHz steps) and 5GHz bandwidth (in 20MHz steps) with a short dwell time (around 50 ms). It supports limited classification of interference sources.

Interference Scan scans three frequencies in the 2.4GHz band and three frequencies in the 5GHz band with a longer dwell time (around 500 ms). It supports classification for all interference sources. To select a mode, select the appropriate radio button or select a mode from the Scan menu.

Spectrogram

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 scroll bar 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.

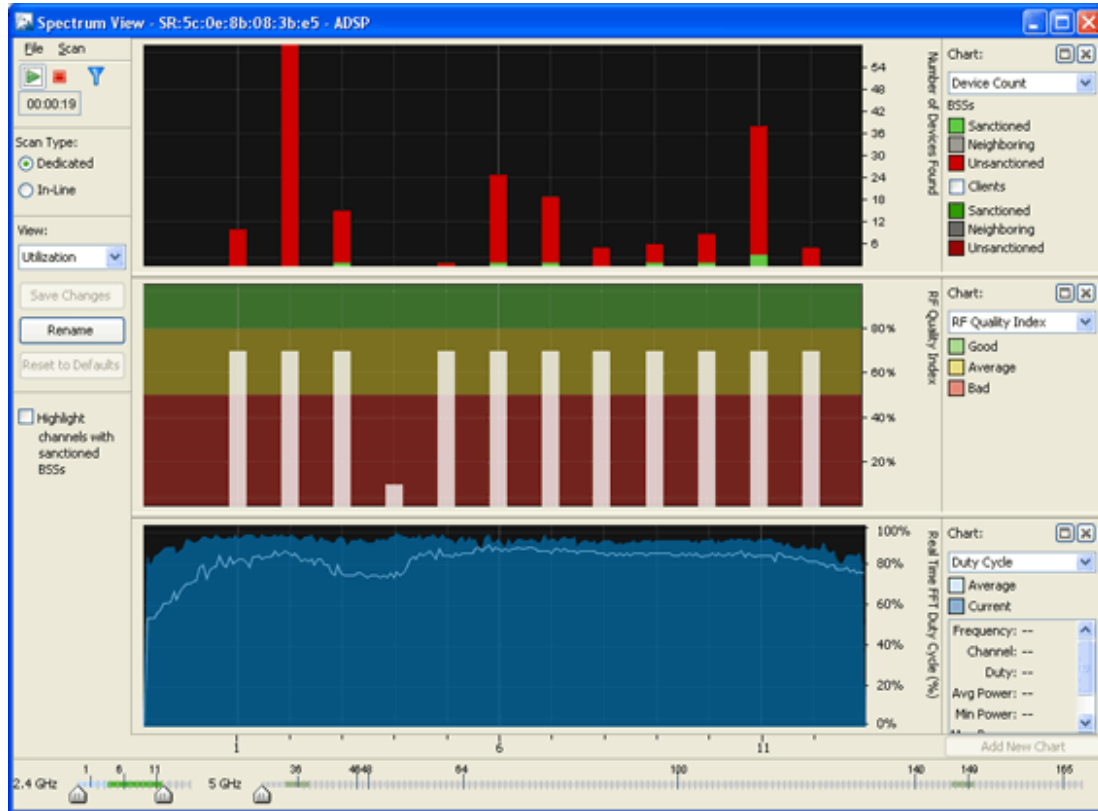
Advanced Spectrum Analysis is the next generation of Spectrum Analysis. Advanced Spectrum Analysis will only run on devices with the MB92 or newer chipsets. Currently, only the models AP621, AP622, AP6511, AP6521, AP6522, and AP8132 can run this enhanced version of Spectrum Analysis.



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.



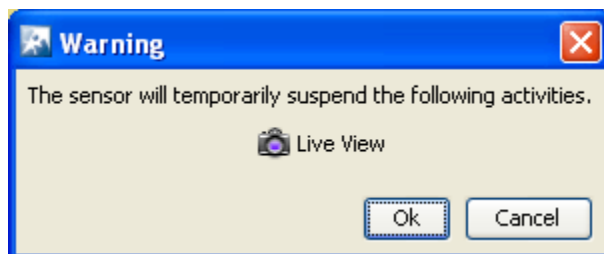
Select **File > Close** to exit the **Spectrum View** window. You will be prompted to save the scan to an AirDefense file. An AirDefense file can be opened by navigating to **Menu > Open > Spectrum Analysis**.

Scanning



A dedicated scan starts automatically when the Spectrum View window is opened. There are three conditions that may prevent a scan from starting. They are:

- The Sensor is already running a dedicated RF scan for any user
- Another user is running Live View on the Sensor
- Ten scans are already running (maximum supported).

If one of these conditions exists, a warning similar to this is displayed:

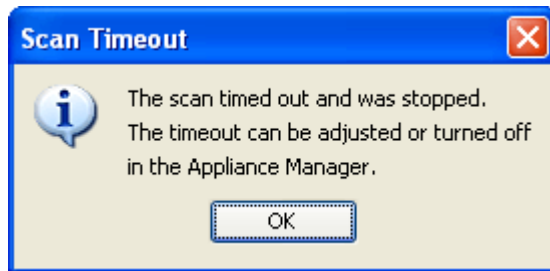


To continue, you will have to click **OK** to suspend the activity. Clicking **Cancel** will stop Advanced Spectrum Analysis from running.

You can stop a scan by clicking the Stop Scan  button or selecting **Scan > Stop Scan**. A new scan can be started by clicking the Start Scan  button or selecting **Scan > Start Scan**.

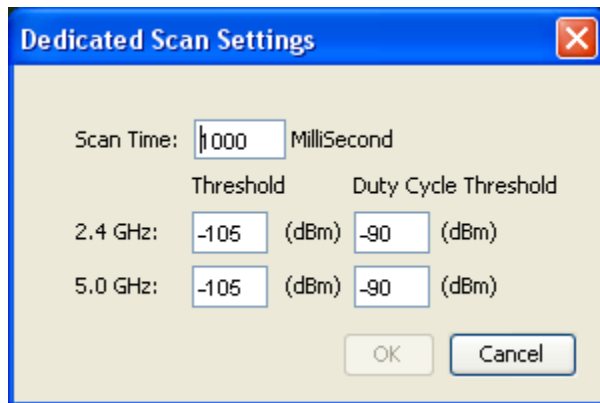
A counter is displayed next to the **Stop Scan** button to show how long the scan has been running.

The default scanning time is 10 minutes. Scanning time can be adjusted by selecting **Configuration > Appliance Management > Appliance Settings**. If a timeout occurs, the following **Scan Timeout** popup is displayed:



Click **OK** to close the popup.

You can change the scan time, threshold, or duty cycle for dedicated scans by navigating to **File > Dedicated Scan Settings**.



The scan time (default 1000) should be entered in milliseconds. The threshold (default -105 for 2.4 and 5 GHz) and duty cycle (default -90 for 2.4 and 5 GHz) should be entered in dBm. After making changes, click OK to confirm the changes or click Cancel to discard any changes.

Scan Type

Advanced Spectrum Analysis supports two types of scans:

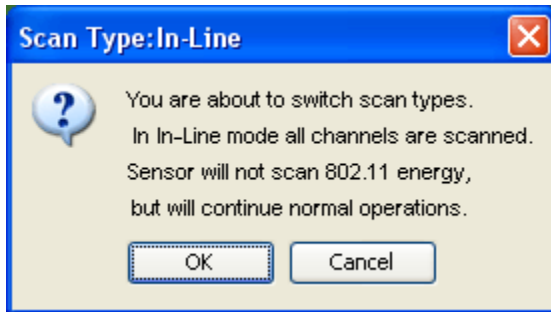
- Dedicated Scan—Conducts a full detailed spectrum scan (default).

- In-Line Scan—Conducts a spectrum scan of all channels minus 802.11 details.

**Note**

To conduct an In-Line Scan, you must enable location tracking RSSI scan under **Configuration > Operational Management > Sensor Operation** and set the refresh rate to 1 second.

You can change the scan type by selecting the appropriate radio button. When the scan type is changed, a warning is displayed.



Click **OK** to confirm the scan type change.

Views

Advanced Spectrum Analysis has the following four views that display default charts for each view:

- Utilization—Displays charts that show how your network is being utilized. The default charts are:
 - Device Count
 - RF Quality Index
 - Duty Cycle.
- Physical Layer—Displays charts that highlight the physical layer of your network. The default charts are:
 - Spectrogram
 - Duty Cycle.
- Interference—Displays charts that show interference sources in your network. The default charts are:
 - Interference
 - Spectral Density.
- Spectrum Detail—Displays charts that show the spectrum details of your network. The default charts are:
 - Spectrogram
 - Real Time FFT (Fast Fourier Transform)
 - Spectral Density.




You can change which charts are displayed for each view using the **Charts** drop-down menu. Once you have changed charts and you want to save the changes, click the **Save Changes** button.

You can change the name of a view by clicking the **Rename** button. This allows you to name the views according to your needs. If for any reason you want to retrieve the default views, you can do so by clicking the **Reset to Defaults** button.

Selecting the **Highlight channels with sanctioned BSSs** checkbox highlights the channels with sanction BSSs in all the charts.

Chart Manipulation

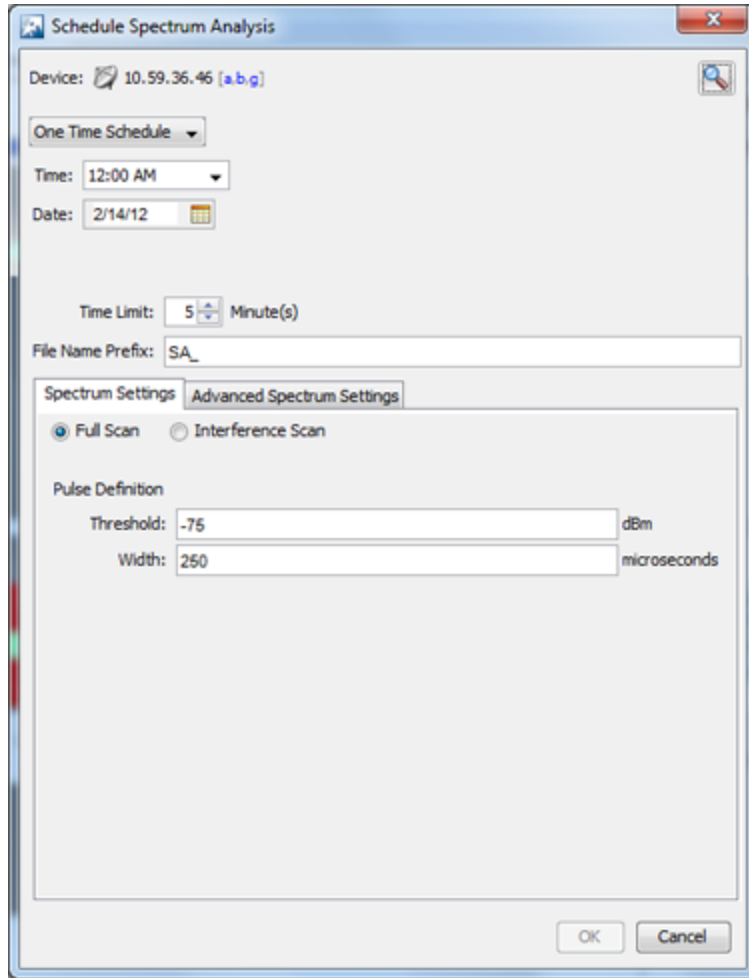
The following chart manipulations are available:

- 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	<p>There are five options to schedule an assessment. Depending on the option you select, you must fill in the related fields as follows:</p> <ul style="list-style-type: none"> • 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 In the Sensor Operation settings of the Sensor Monitoring category under the Configuration tab, there is an option to enable background scanning..
Advanced Spectrum Settings	Only used in Advanced Spectrum Analysis. These are the Dedicated Scan Settings described under Each time a scan is started, the table clears and is updated when data becomes available..

You can switch devices by clicking **Search** button.

Device Search- ADSP

Scope: ADSP

Search Now

Criteria

MAC Address: [dropdown]

Name: [text box]

IP Address: [text box]

802.1x Username: [text box]

Vendor: [text box]

DNS Name: [text box]

SSID: [text box]

New Search

Supports 802.11a: Yes No Either

Supports 802.11b: Yes No Either

Supports 802.11g: Yes No Either

Supports 802.11n: Yes No Either

Results:

Close

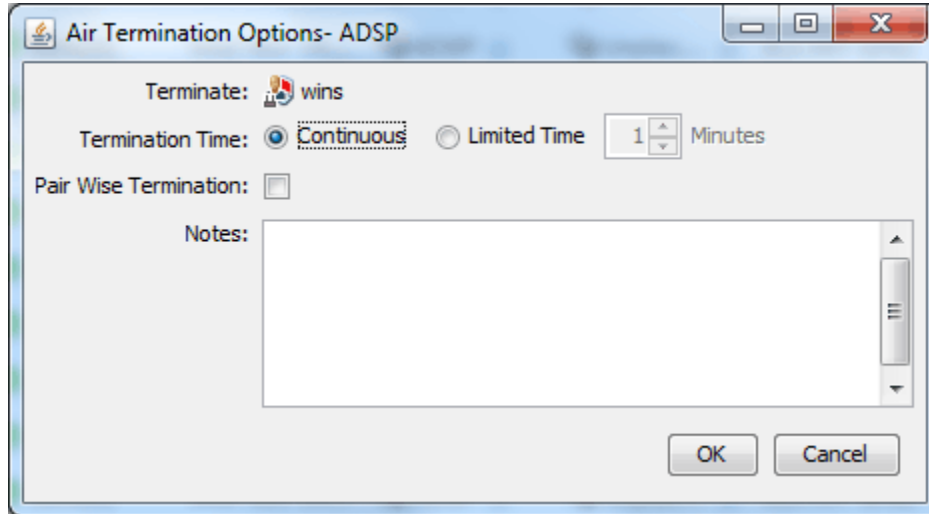
When searching, you can supply additional information such as:

- Select the scope from the network tree
- The MAC address of the device
- The name of the device
- The IP address of the device
- The 802.1x username used for authentication
- The vendor name of the device
- The DNS name used by the device
- The SSID of the device
- Select whether or not the device supports the 802.11a, b, g, or n protocols.

Once you have entered the search criteria, click the **Search Now** button. The results are displayed in the Results area. Select the device that you want to run Spectrum Analysis on and then click **Close**.

Terminate

AirDefense 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.




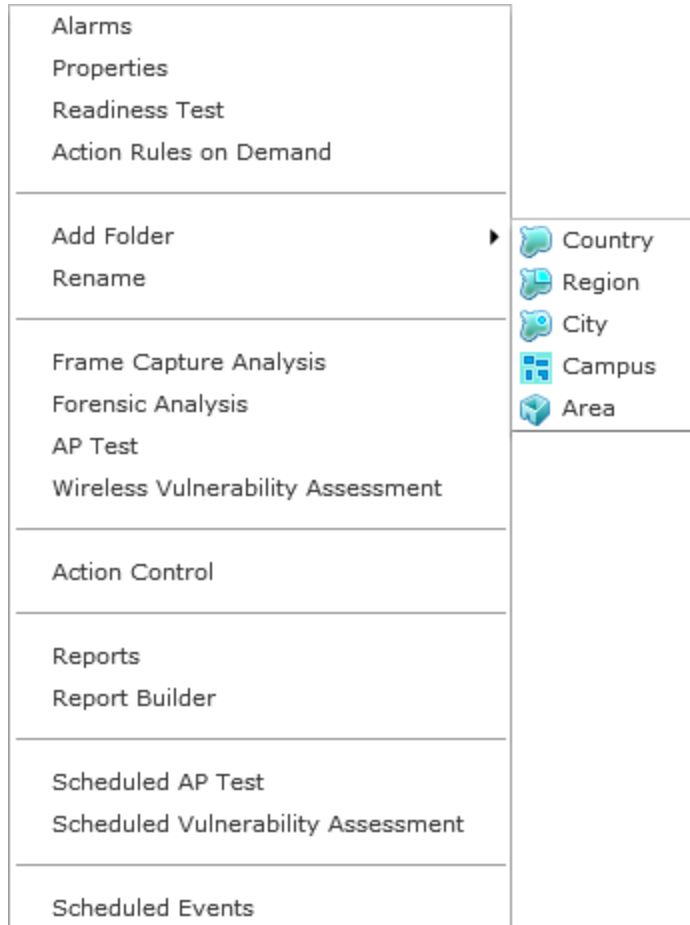
Network Level Drop-down Menus

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.

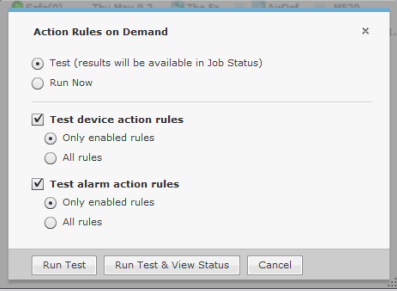
Appliance Level Drop-down Menu

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.




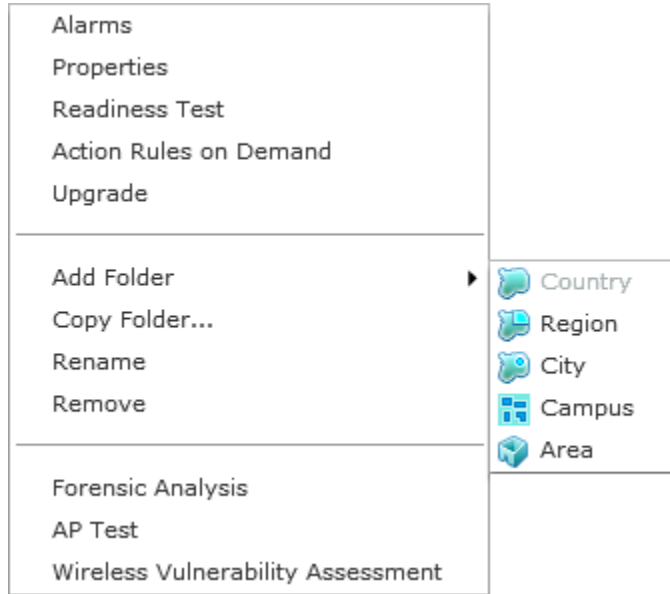
The drop-down menu for appliances contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Appliance. See Alarms on page 480 for more information.
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 managed through ASDP). You are alerted of problem areas. (See Readiness Test on page 743 for more information.)

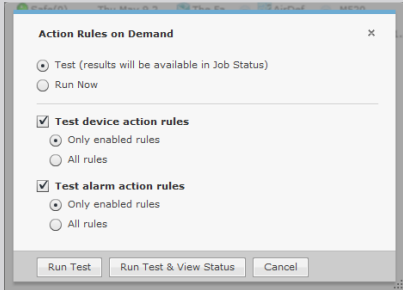
Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in Job Status on page 612, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> • 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 window. See Frame Capture Analysis on page 390 for more information.
Forensic Analysis	Accesses Forensic AnalysisBasic. See Forensic Analysis-Basic on page 391 for more information.
AP Test	Accesses Scheduled AP Tests. See Scheduled AP Tests on page 409 for more information.
Wireless Vulnerability Assessment	Accesses Scheduled Vulnerability Assessment. See Scheduled Vulnerability Assessment on page 811 for more information.
Action Control	Accesses Advanced vs. Basic Forensic Analysis.
Reports	Accesses Reports (Web Reporting Interface).
Report Builder	Accesses the Report Builder (Report Builder).
Scheduled AP Test	Accesses Scheduled AP Tests.
Scheduled Vulnerability Assessment	Accesses Scheduled Vulnerability Assessment.
Scheduled Events	Accesses Scheduled Events.

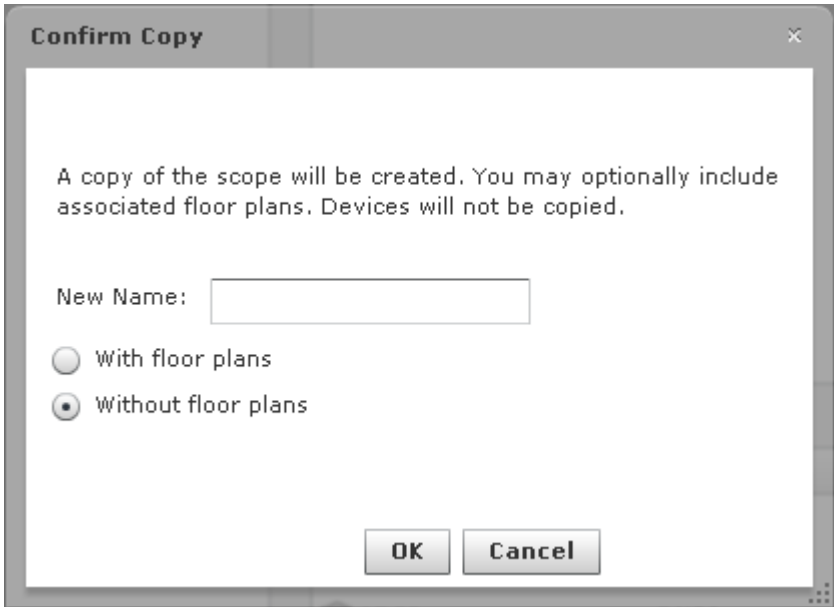
Country Level Drop-down Menu

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.




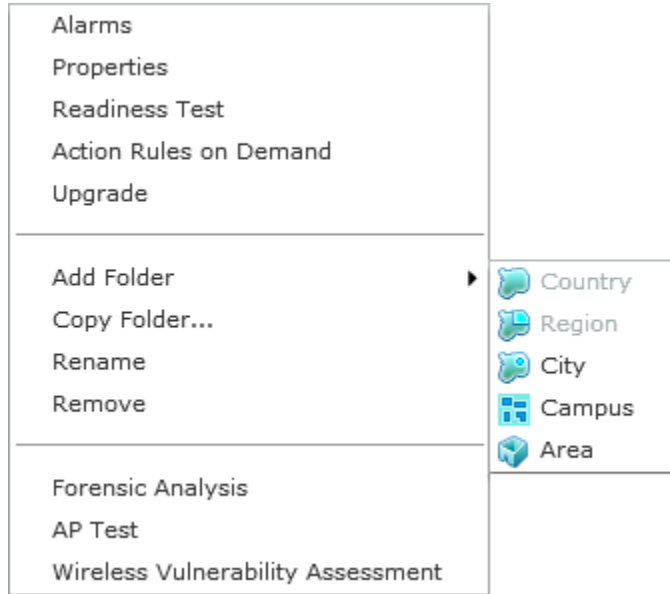
The drop-down menu for countries contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Country. See Frame Capture Analysis on page 390 for more information.
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 on page 743 for more information.)
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in Job Status on page 612, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> • 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.

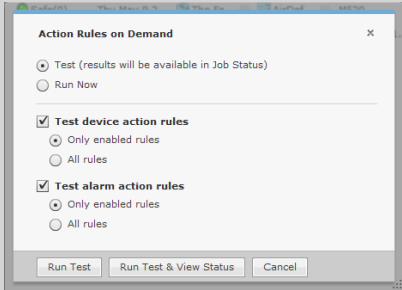
Function	Description
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	<p>Copies the network scope of a Country.</p>  <p>Enter a name for the country, select if you want the to include the floor plans or not, and click OK.</p>
Rename	Opens a dialog window to rename the selected Country.
Remove	Removes the selected Country from your network.
Forensic Analysis	Accesses Forensic Analysis-Basic for this country. See Forensic Analysis-Basic on page 391 for more information.
AP Test	Accesses AP Tests (Scheduled AP Tests). See Scheduled AP Tests on page 409 for more information.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment. (Scheduled Vulnerability Assessment). See On-Demand Vulnerability Assessment on page 810 for more information.

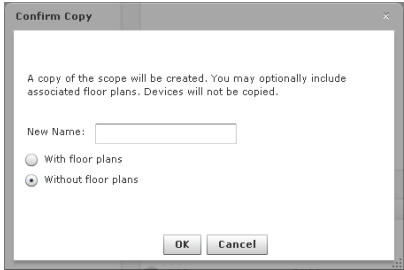
Region Level Drop-down Menu

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.




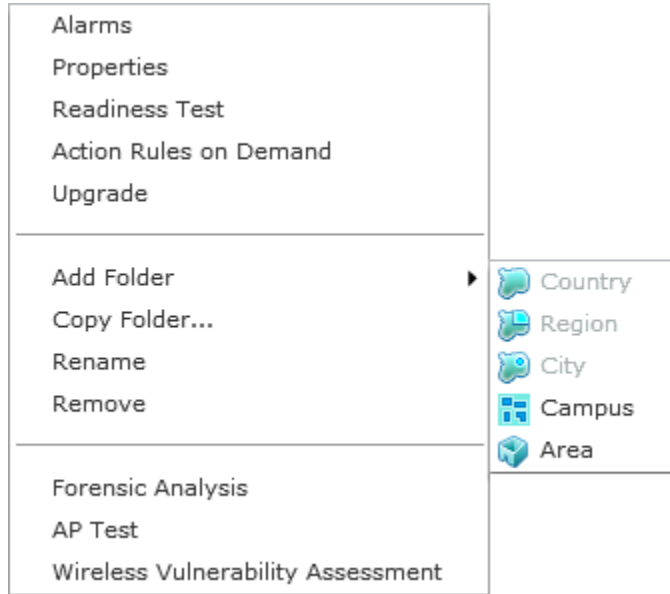
The drop-down menu for regions contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Region. See Alarms on page 480 for more information.
Properties	Opens the Properties overlay for the selected Region.
Readiness Test	Validates that devices in the region scope are management ready of problem areas. You are alerted of problem areas. (See Readiness Test on page 743 for more information.)
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in Job Status on page 612, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> • 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.

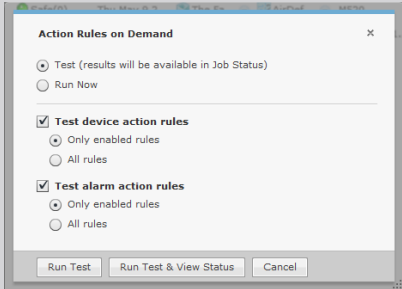
Function	Description
Upgrade	Upgrades the firmware for devices in the selected Region.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	<p>Copies the network scope of a Region.</p>  <p>Enter a name for the region, select if you want the to include the floor plans or not, and click OK.</p>
Rename	Opens a dialog window to rename the selected Region.
Remove	Removes the selected Region from your network. See Remove Devices on page 473 for more information.
Forensic Analysis	Accesses Forensic Analysis—Basic. See Forensic Analysis-Basic on page 391 for more information.
AP Test	Accesses AP Test (Scheduled AP Tests). See Scheduled AP Test for more information.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (Scheduled Vulnerability Assessment). See Wireless Vulnerability Assessment for more information.

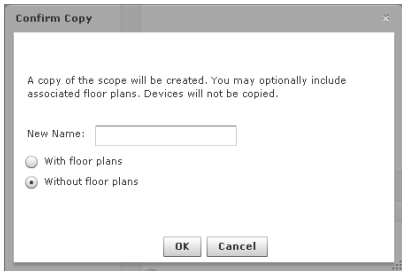
City Level Drop-down Menu

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.




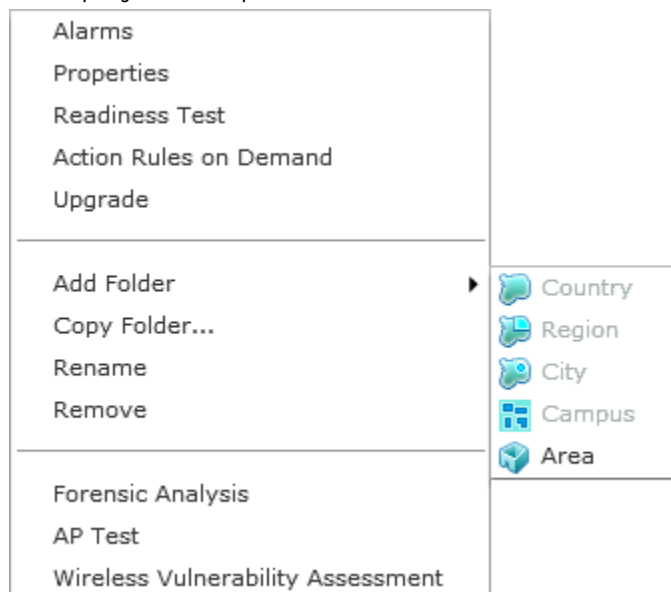
The drop-down menu for cities contains the following functions:

Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected City. See Alarms on page 480 for more information.
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 on page 743 for more information.)
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in Job Status on page 612, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> • 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.

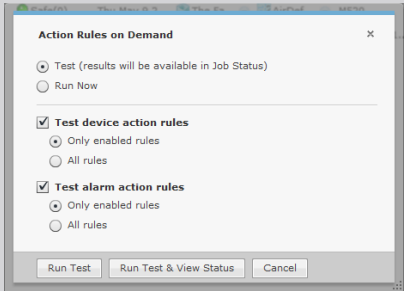
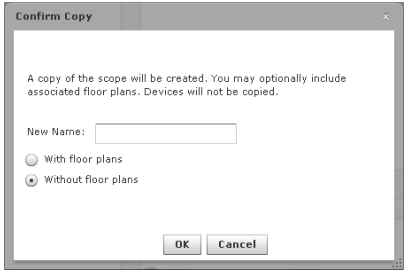
Function	Description
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	<p>Copies the network scope of a City.</p>  <p>Enter a name for the city, select if you want the to include the floor plans or not, and click OK.</p>
Rename	Opens a dialog window to rename the selected City.
Remove	Removes the selected City from your network.
Forensic Analysis	Accesses Forensic Analysis—Basic. See Forensic Analysis-Basic on page 391 for more information.
AP Test	Accesses AP Test (Scheduled AP Tests). See Scheduled AP Test for more information.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment. See Scheduled Vulnerability Assessment on page 811 for more information.

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. See Alarms on page 480 for more information.
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 managed through ASDP). You are alerted of problem areas. (See Readiness Test on page 743 for more information.)
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in Job Status on page 612, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> • 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.
Add Folder	Adds a new folder to the network tree by selecting one of the available network levels. The added folder is given a generic name. You should rename the new folder.
Copy Folder	<p>Copies the network scope of a Campus.</p>  <p>Enter a name for the campus, select if you want the to include the floor plans or not, and click OK.</p>
Rename	Opens a dialog window to rename the selected Campus.

Function	Description
Remove	Removes the selected Campus from your network.
Forensic Analysis	Accesses Forensic Analysis—Basic. See Forensic Analysis-Basic on page 391 for more information.
AP Test	Accesses AP Test (Scheduled AP Tests). See Scheduled AP Test for more information.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (Scheduled Vulnerability Assessment). See Scheduled Vulnerability Assessment on page 811 for more information.

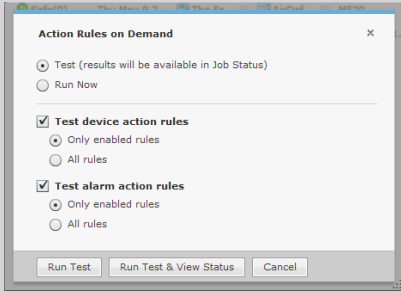
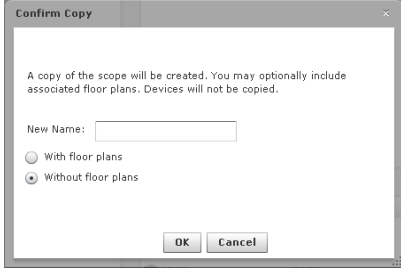
Area (Building) Level Drop-down Menu

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.


Alarms	
Properties	
Readiness Test	
Action Rules on Demand	
Live RF / Floor Plan	
Upgrade	
<hr/>	
Copy Folder...	
Rename	
Remove	
<hr/>	
Forensic Analysis	
AP Test	
Wireless Vulnerability Assessment	

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. See Alarms on page 480 for more information.
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 on page 743 for more information.)

Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in Job Status on page 612, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> • 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.
Copy Folder	<p>Copies the network scope of a Area.</p>  <p>Enter a name for the building, select if you want the to include the floor plans or not, and click OK.</p>
Rename	Opens a dialog window to rename the selected Area.
Remove	Removes the selected Area from your network.
Forensic Analysis	Accesses Forensic Analysis—Basic. See Forensic Analysis-Basic on page 391 for more information.
AP Test	Accesses AP Test (Scheduled AP Tests). See Scheduled AP Test for more information.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (Scheduled Vulnerability Assessment). See Scheduled Vulnerability Assessment on page 811 for more information.

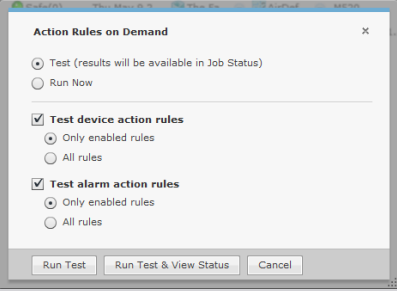
Live RF/Floor Plan Level Drop-down Menu

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.

Alarms
Properties
Readiness Test
Action Rules on Demand
Live RF / Floor Plan
Upgrade
<hr/>
Rename
<hr/>
Forensic Analysis
AP Test
Wireless Vulnerability Assessment
Add Device

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. See Alarms on page 480 for more information.
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 on page 743 for more information.)

Function	Description
Action Rules on Demand	<p>Runs an on demand test on your alarm action rules and/or device action rules.</p>  <p>You can run the test and view the results later in Job Status on page 612, or you can run the test now and view the results now. There are two options for each type of test:</p> <ul style="list-style-type: none"> • 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.
Rename	Opens a dialog window to rename the selected Floor.
Forensic Analysis	Accesses Forensic Analysis-Basic. See Forensic Analysis-Basic on page 391 for more information.
AP Test	Accesses AP Test (Scheduled AP Tests). See Scheduled AP Test for more information.
Wireless Vulnerability Assessment	Accesses Wireless Vulnerability Assessment (Scheduled Vulnerability Assessment). See Scheduled Vulnerability Assessment on page 811 for more information.
Add Device	Adds devices to the AirDefense Services Platform. Add devices to AirDefense. See Add Devices for more information.

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.

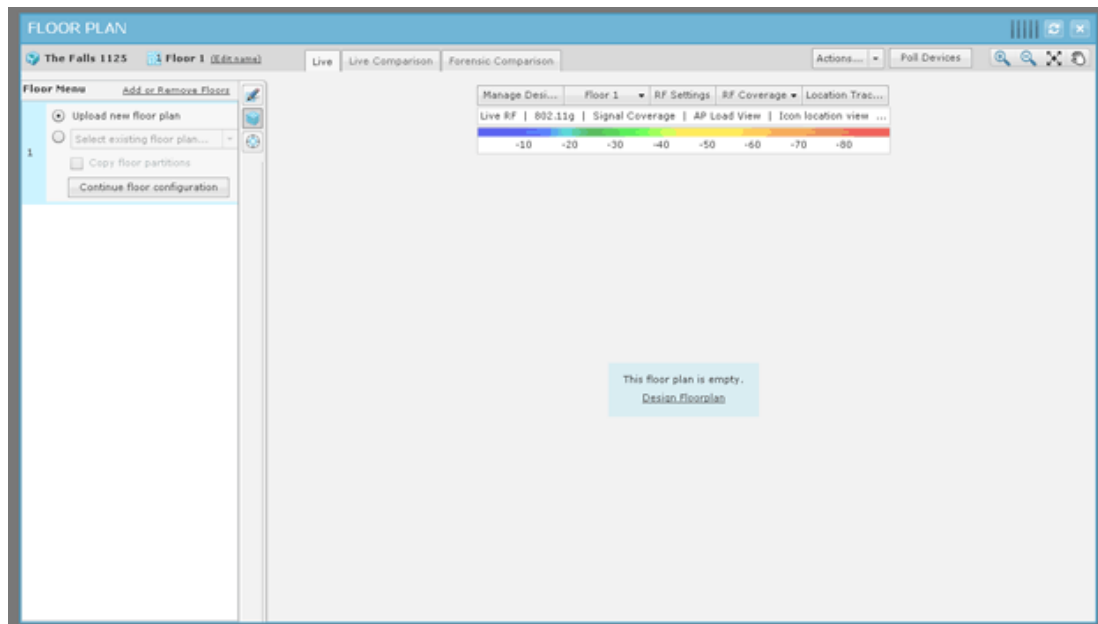


Note

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.



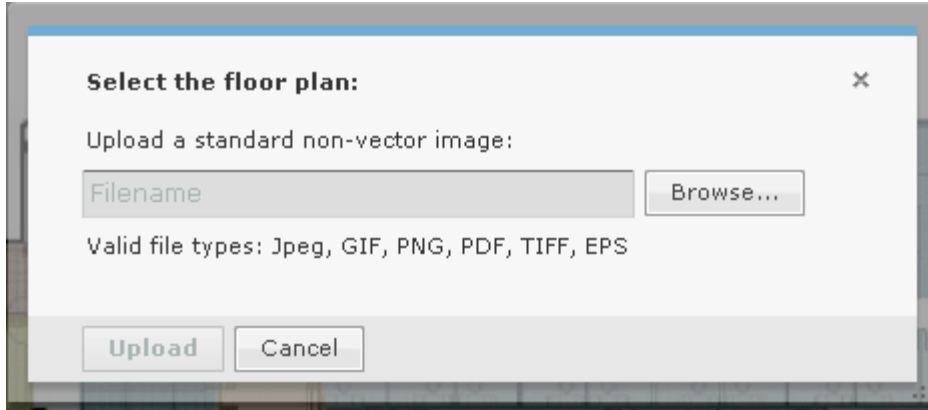
When the floor plan is complete, you will need to click the **Close** button X to save and close. The Floor Plan can then be viewed throughout AirDefense, and can be used to locate devices in your network and display Live RF data.

To upload a background image, click the **Continue floor configuration** button or the **Design Floorplan** link to get started.

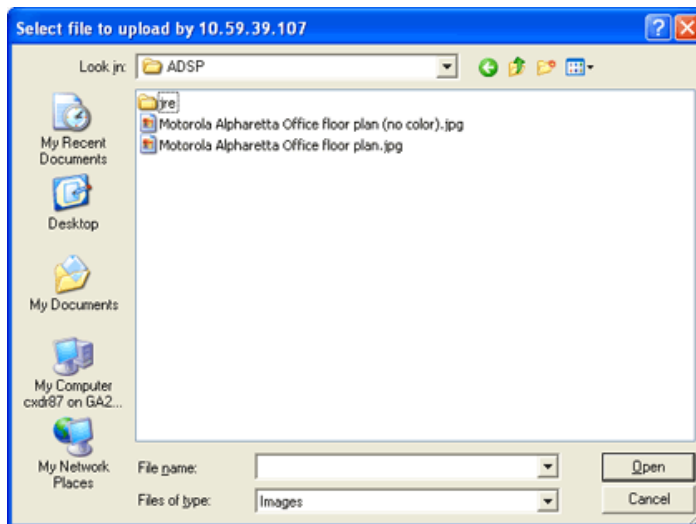


Note

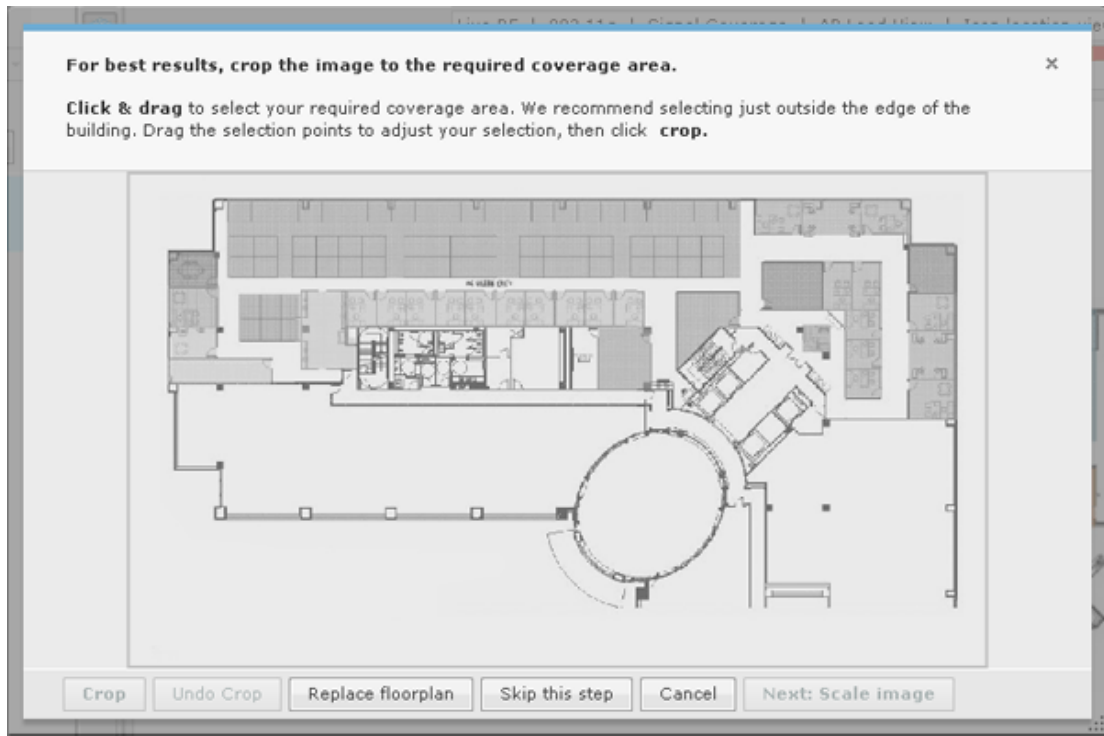
The Floor Plan single dimension limit (width or height) is 8192 pixels while the total pixel count (width x height) limit is 8,000,000 pixels. If the appliance has at least 2GB of memory, the total pixel count may be as high as 16,777,215 pixels but the single dimension limit is still 8192 pixels.



1. Click the **Browse** button.



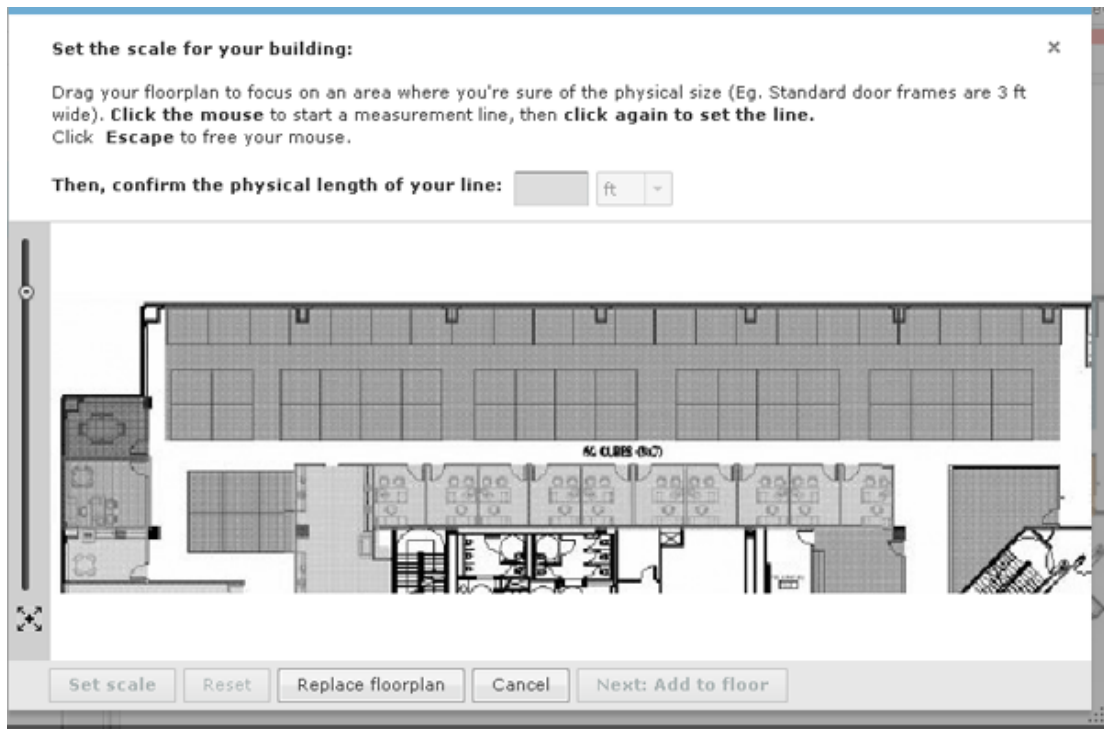
2. Browse to the location of the image, select it (usually a BMP, GIF, or JPG file), and then click **Open**. The **Upload** button is now active. Click it.



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 points 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.

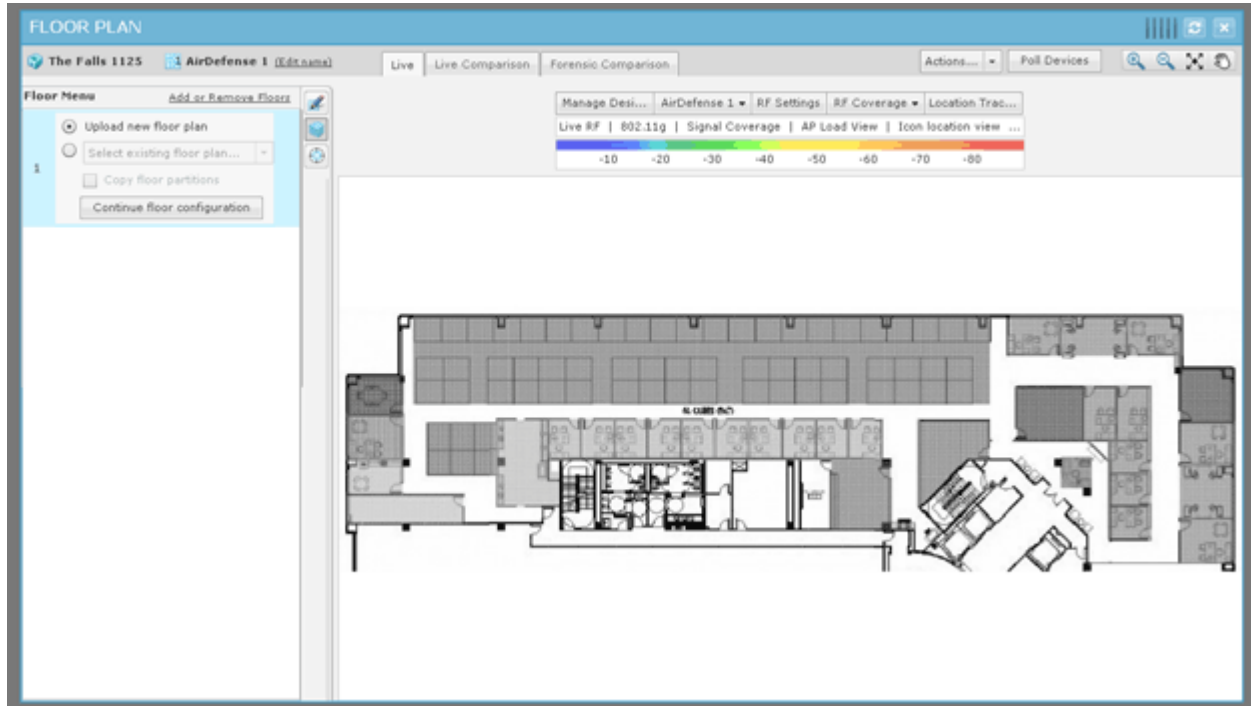
- The **Next: Add to floor** button is activated. Click it to add the floor to your floor plan.



Note

You can undo any changes by clicking the **Cancel** button. You can remove an image by clicking the **Replace floor plan** 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 AirDefense does calculations to locate devices and/or to display Live RF data.

Add Additional Floors

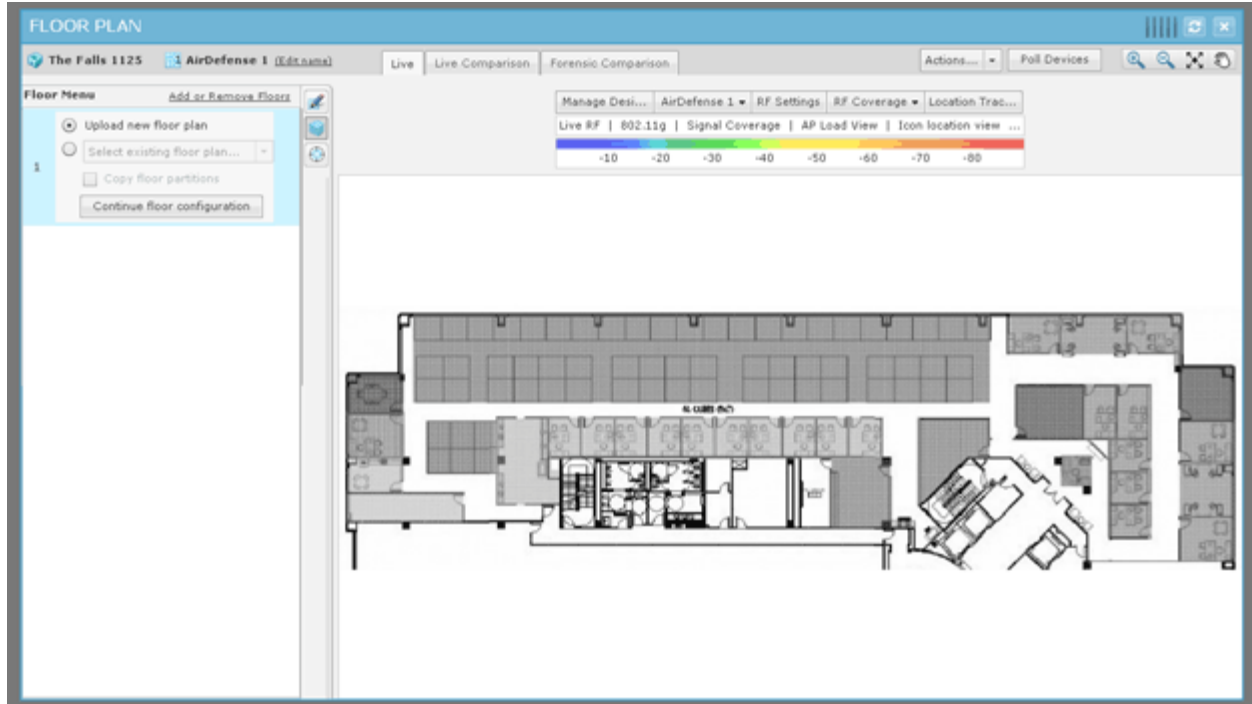
To add an additional floor to your building:

- Reveal the existing floors by clicking anywhere on the **Floor Plan Toolbar**.

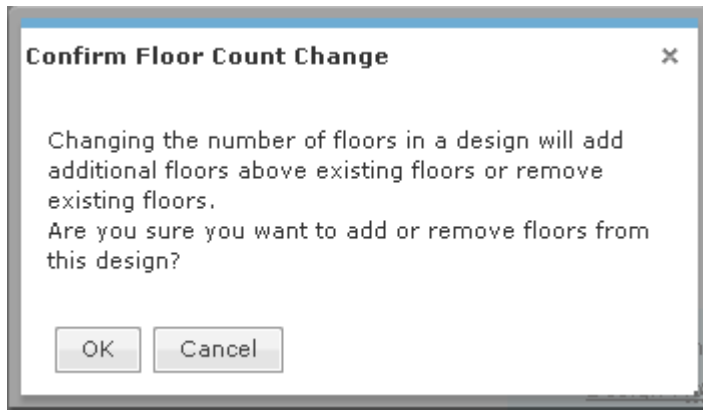


Note

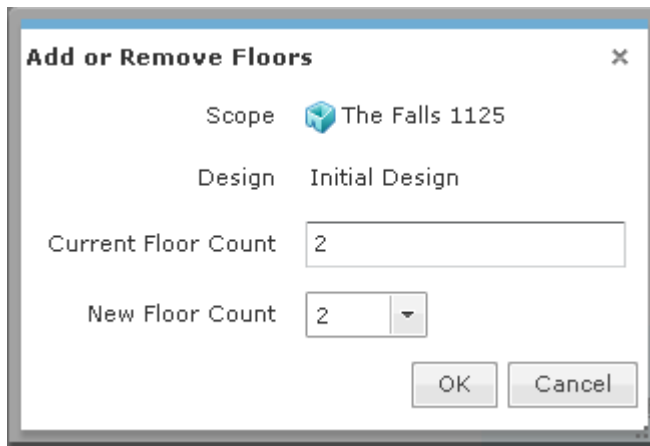
Clicking the **Floor Plan Toolbar** also removes floor selection from view.



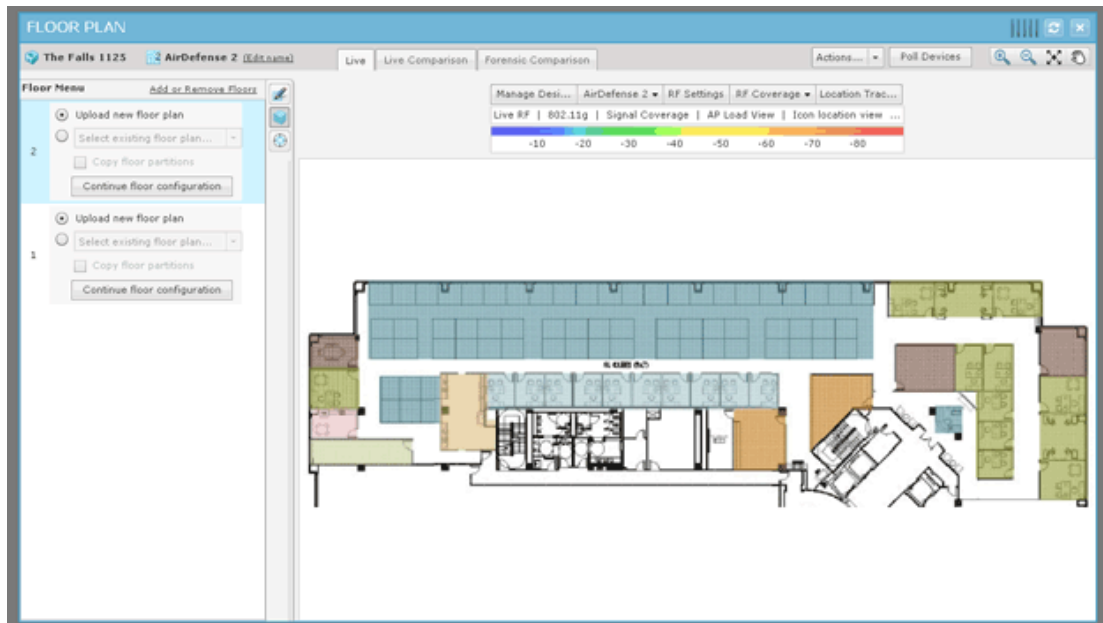
2. Click the **Add or Remove Floors** link. The following dialog box is displayed:



3. Click **OK** to continue to the following dialog box:



4. 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.
5. 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:



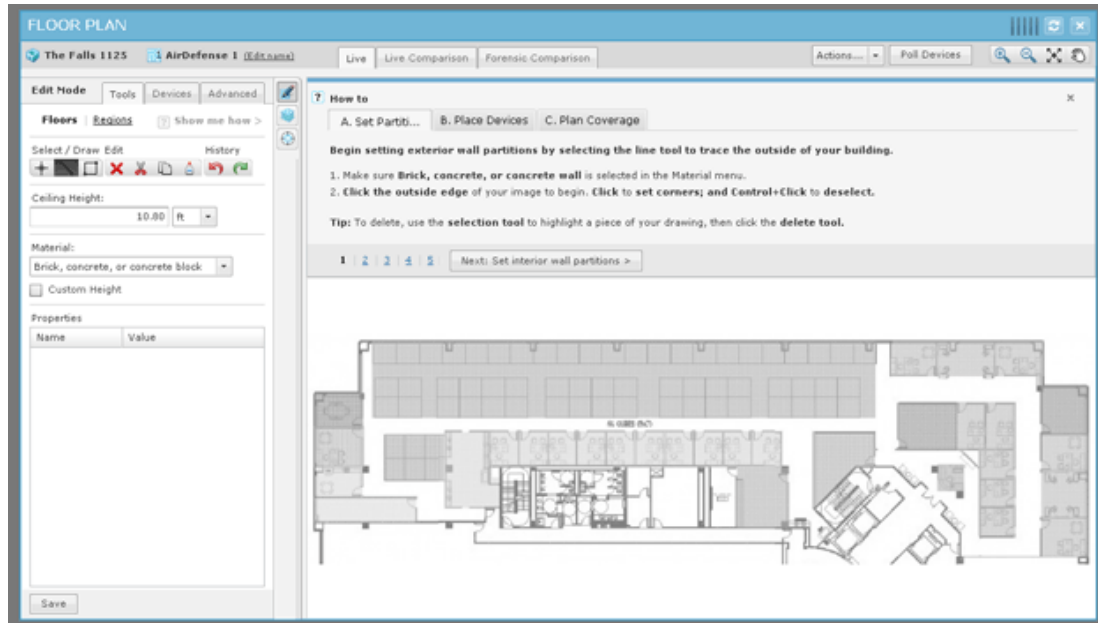
6. To access the different floors within a building, click the thumbnail image for the floor located in the left pane.

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 [Floor Plan Actions](#) on page 784 and the [Context Label](#) on page 780.



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.

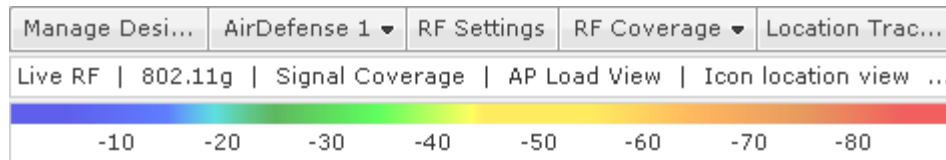
Global Tools

Global tools are tools that are available on all Floor Plan pages. They are:

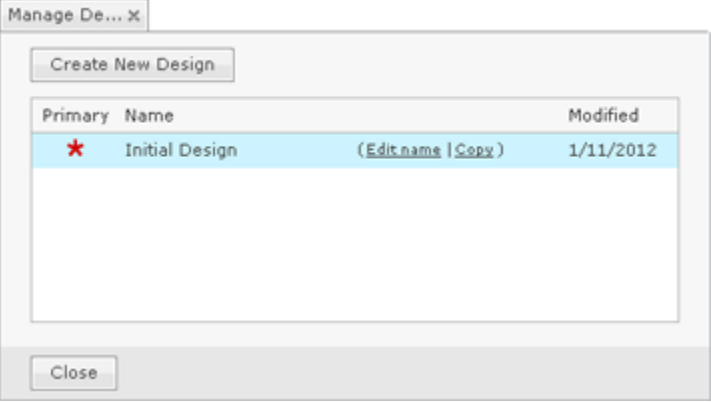
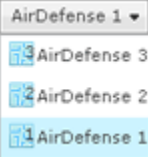
- Context Label
- Actions
- Floor manipulation.

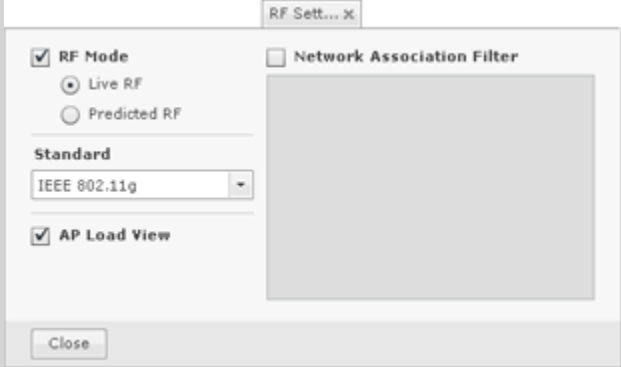
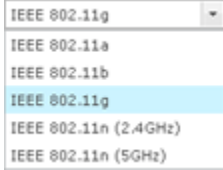


Context Label

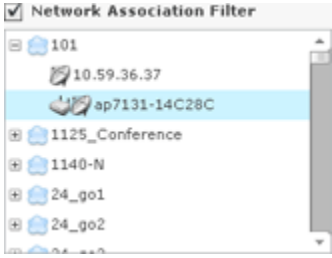
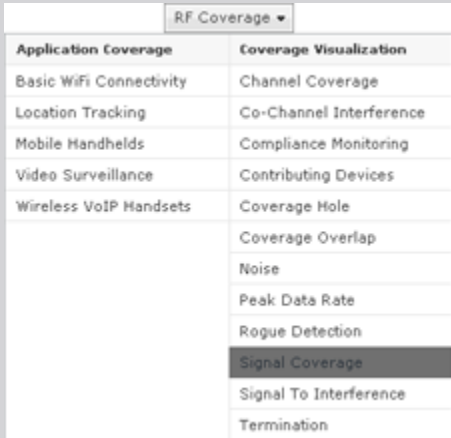
The Context Label, located near the top-center of the Floor Plan, controls the context of the Floor Plan.

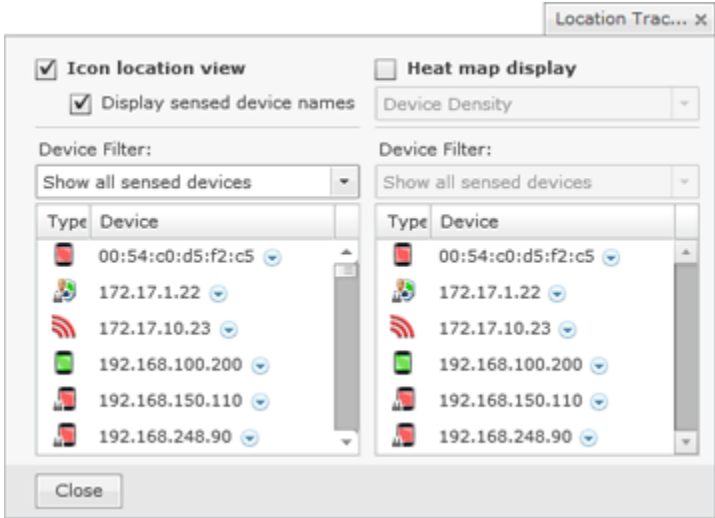
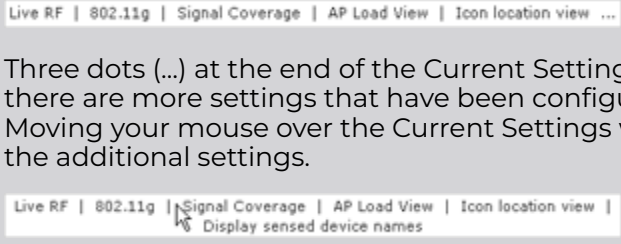



The Context Label shows you the following information:

Field	Description
Manage Designs	<p>When this field is clicked, a list of existing designs is displayed:</p>  <p>You can edit or add to the list using the following actions:</p> <ul style="list-style-type: none"> • 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. <p>Click Close to exit the design manager.</p>
Floor Selection	<p>This field shows the selected floor. If you click the field, you can select another floor to view.</p> 
RF Settings	<p>RF Settings includes:</p> <ul style="list-style-type: none"> • RF Mode setting • Protocol setting • AP Load View setting • Network Association Filter.

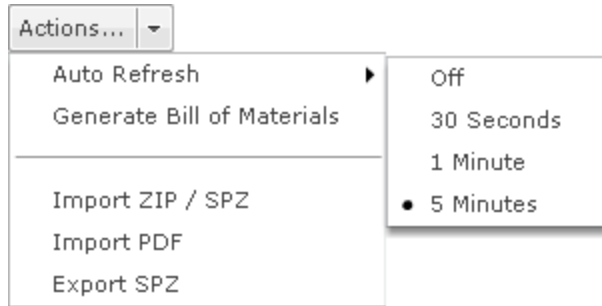
Field	Description
<p>RF Mode Setting</p>	<p>The RF Mode setting determines if your heat maps display no RF data (deselected), Live RF data (selected), or Predicted RF data (selected).</p> 
<p>Protocol Setting</p>	<p>The Protocol setting allows you to filter RF data according to the selected protocol.</p> 
<p>AP Load View Setting</p>	<p>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.</p>  <p>Click on the smaller circle to display all the associated Wireless Clients in a table.</p> 

Field	Description
<p>Network Association Filter Setting</p>	<p>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.</p> 
<p>RF Coverage</p>	<p>This field lets you select the coverage visualization or application coverage for your heat maps. If you click the field, you can select another visualization or application.</p>  <p>Visualizations and applications are configured in Configuration > Network Assurance > Live RF Settings.</p>

Field	Description
<p>Location Tracking</p>	<p>This field displays a list of devices being tracked grouped by device type.</p>  <p>If a device in the list is selected (highlighted) it is highlighted in the floor plan map. Location Tracking has two views: 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.</p>
<p>Current Settings</p>	<p>This field gives you a quick view of the settings that have been set via the Context Label.</p>  <p>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.</p>
<p>Color Chart</p>	<p>The color chart is a legend representing the signals displayed as RF data in the Floor Plan. Each color represents a signal strength (in dBm).</p> 

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.



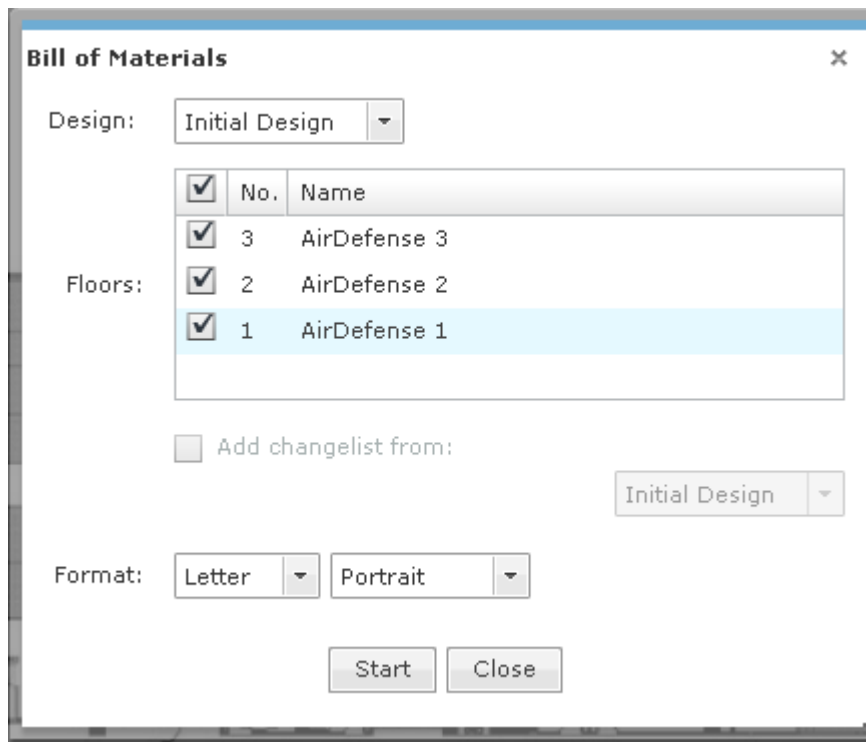
Auto Refresh

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.) AirDefense 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.

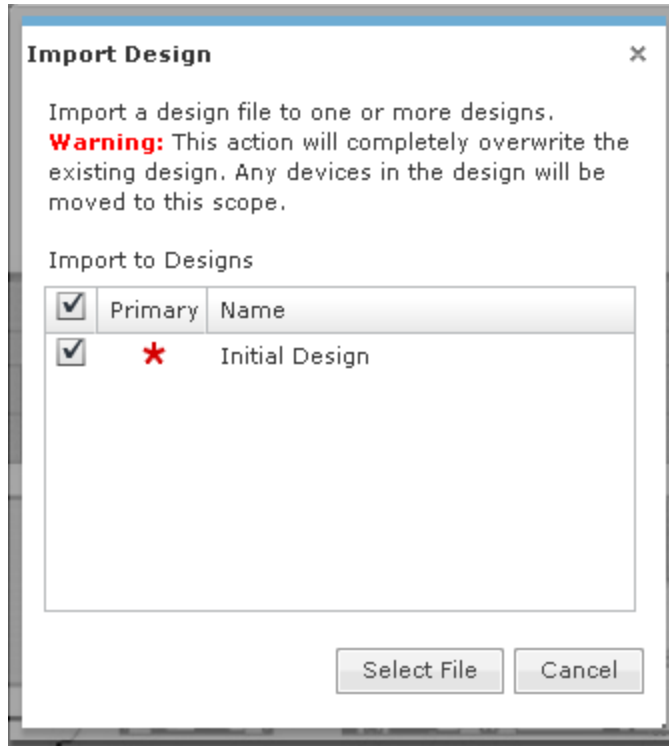
Click **Start** to begin the process. A checklist is generated to indicate success or not. Click the link, **Click to choose where to save the PDF file.**, to specify where to place the generated PDF file and then click **Save** to save the file. If an error occurs, an error message is generated.

Import ZIP / SPZ

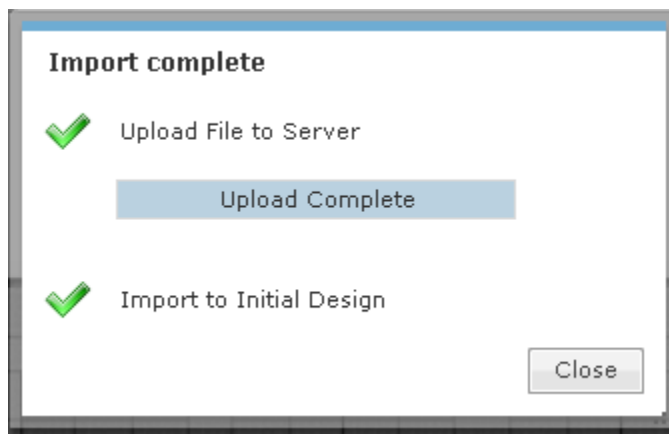
This section describes the different ways you can import and export floor plans.

LAN Planner

You can import a LAN Planner (or Outdoor Planner) design that has been exported to a ZIP file or 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**.

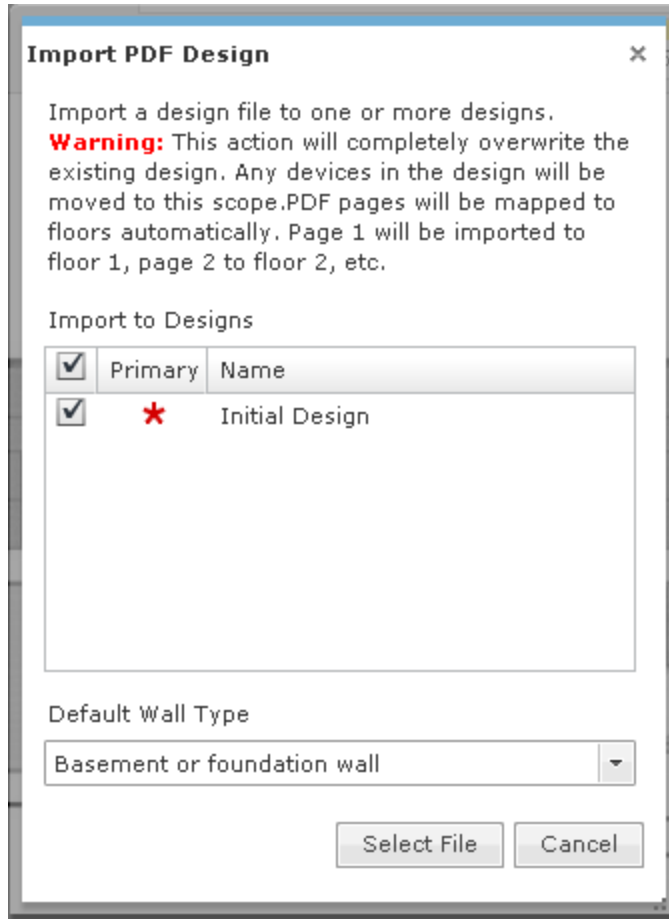


Note

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.

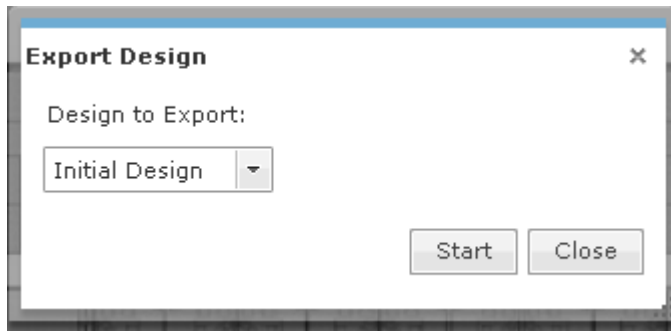
Imported PDF pages are automatically mapped to existing floors. Page 1 is imported to floor 1, page 2 is imported to floor2, and so on.

Export Floor Plan to ZIP File

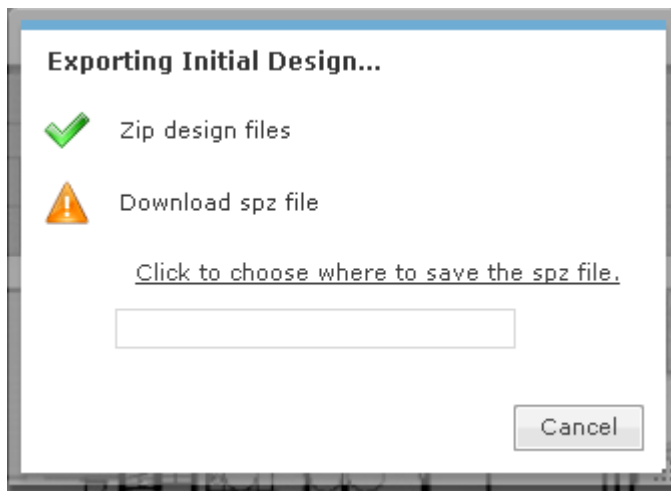
**Note**

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.

1. Select **Export ZIP** to export the selected floor plan design to a ZIP file that can be imported into LAN Planner.



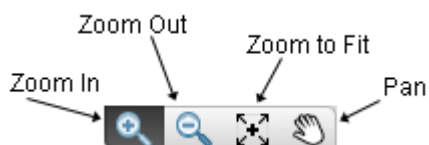
2. To begin, select a design from the drop-down menu and then click **Start**. A checklist is generated to indicate success or not.







3. 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 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.



The following tools are available:

Function	Description
	Enlarges the size (zoom in) a floor plan image. Clicking the image area will zoom into another level.
	Reduces the size (zoom out) a floor plan image. Clicking the image area will zoom out to another level.
	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.
	Moves/re-positions the floor plan image. A hand is used to move/re-position the image.

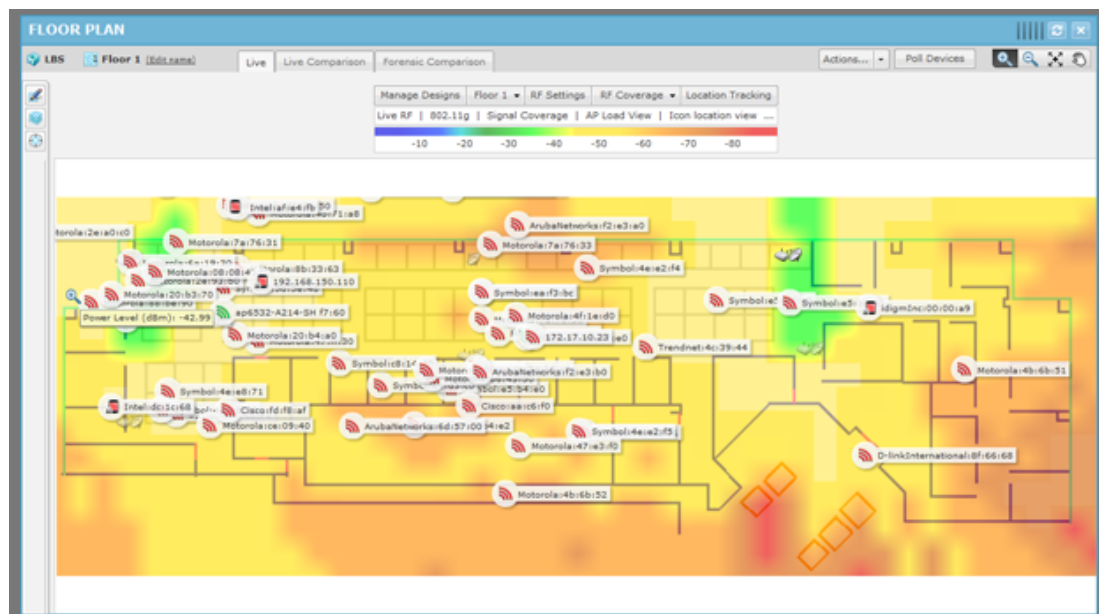
Live Tab



Note

A Live RF license is required to access this feature.

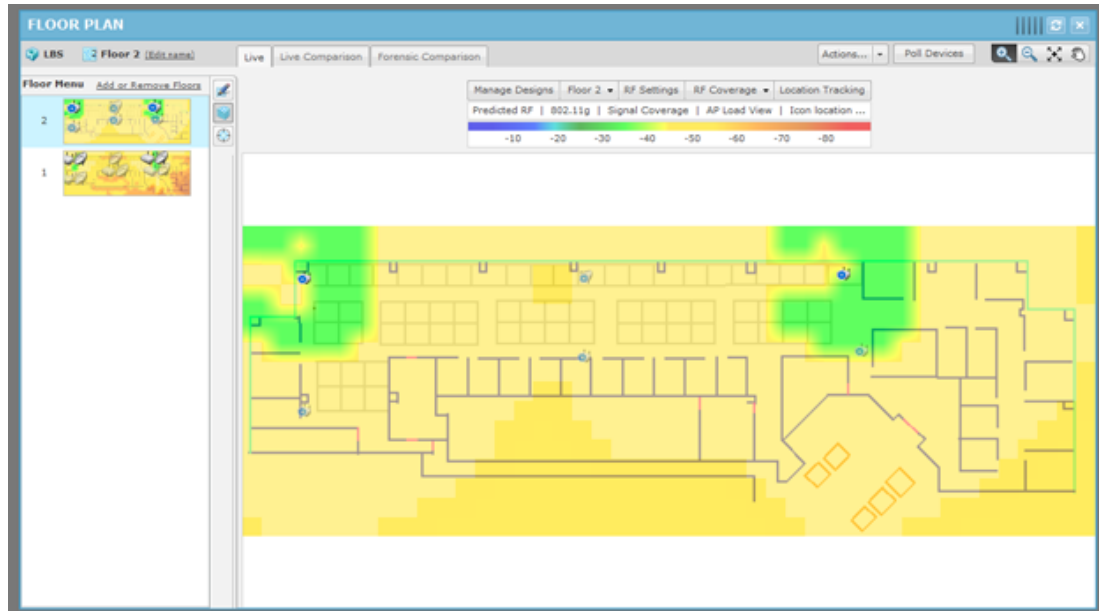
The **Live** tab displays a heat map that represents signal coverage for APs placed on a **Floor Plan**. When the **Floor Plan** is accessed, if devices are in place, **Live RF** starts and a heat map is displayed.



Live RF data is available on all **Floor Plan** pages. When the **Floor Plan** is refreshed either 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.



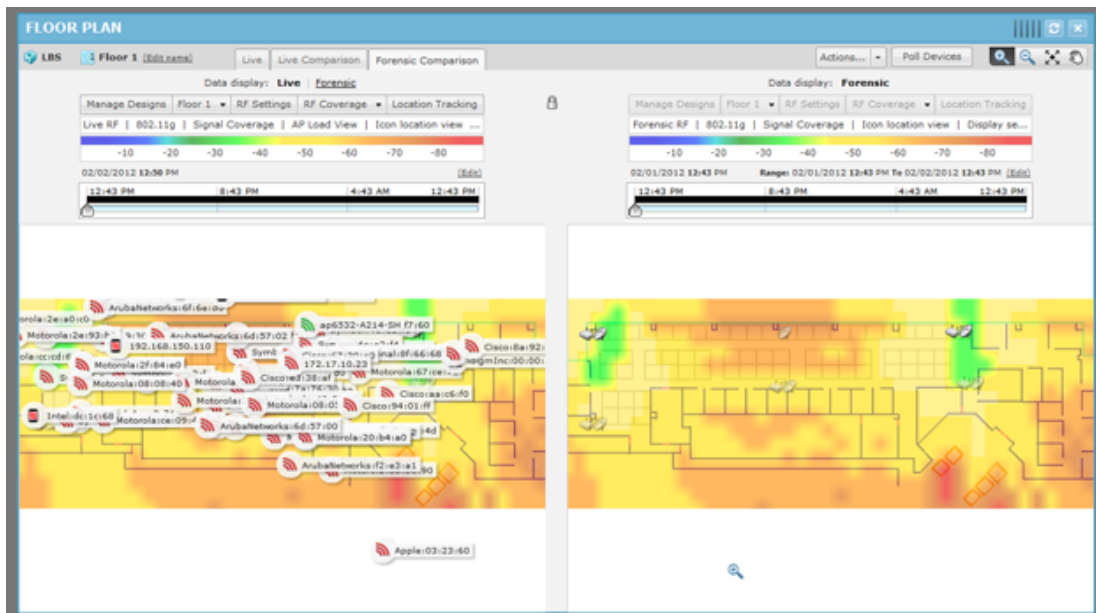
You have access to the **Context Label** where you can manipulate one or both of the images.

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

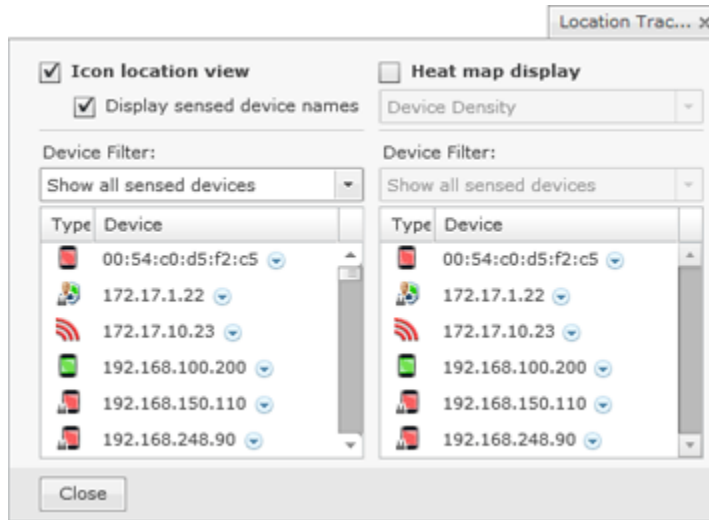
Tracking enables you to locate and track rogue devices that may be threatening your wireless LAN. In order for **Tracking** to open and function properly, you must have at least three sensors for each floor map that is loaded.



Note

Tracking is not intended to be used on devices that are being terminated.

To start tracking a device, click the **Location Tracking** button in the **Context Label**.

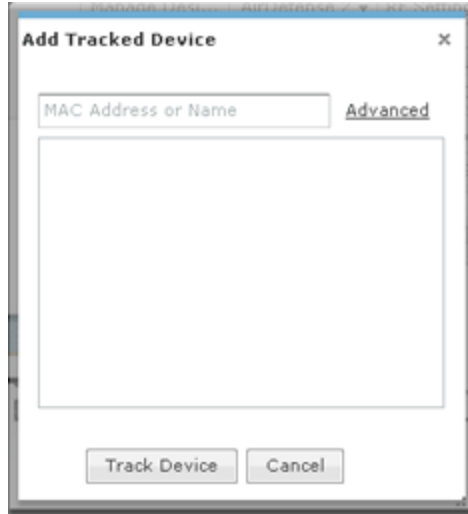


All sensed devices are displayed when Location Tracking (in the list of devices and the floor plan) is first accessed. You can group devices by type by selecting **Filter by device type** from the drop-down menu. You can search for devices by selecting **Search for devices** from the drop-down menu.

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. The **Add Tracked Devices** dialog opens where you can type in a MAC address.



You can enter the complete MAC address or a part of it.



Note

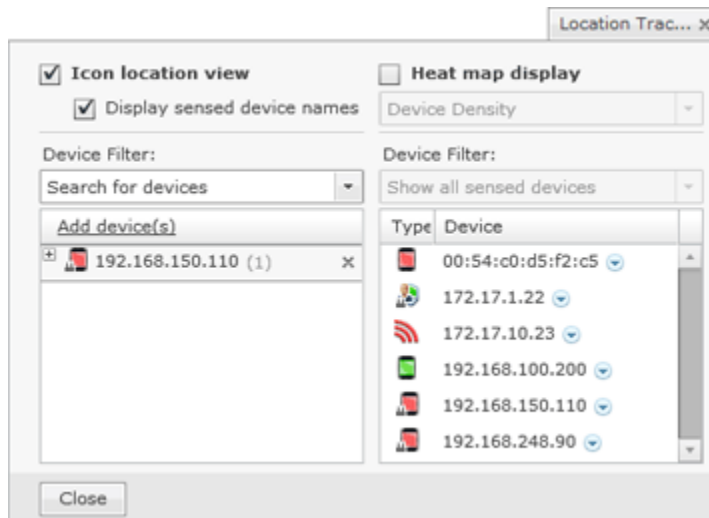
The **Advanced** link is used to open a search dialog that gives you more options to find devices.

When you see the device listed, click on it and then click **Track Device**. The device is displayed in the tracked device list.

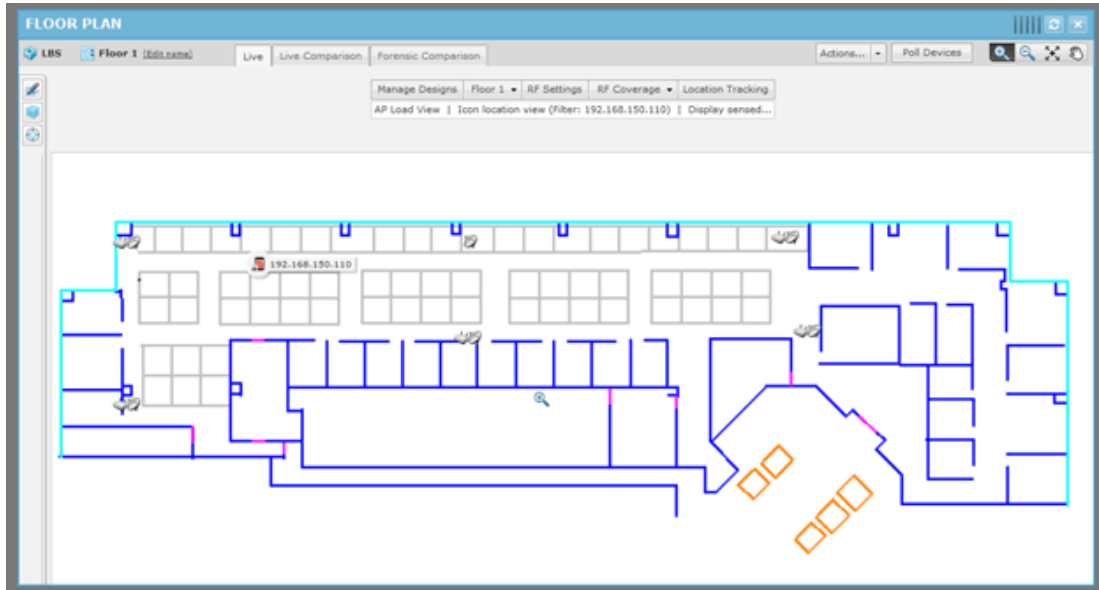


Note

You may select more than one device using the <Shift> key or the <Ctrl> key.

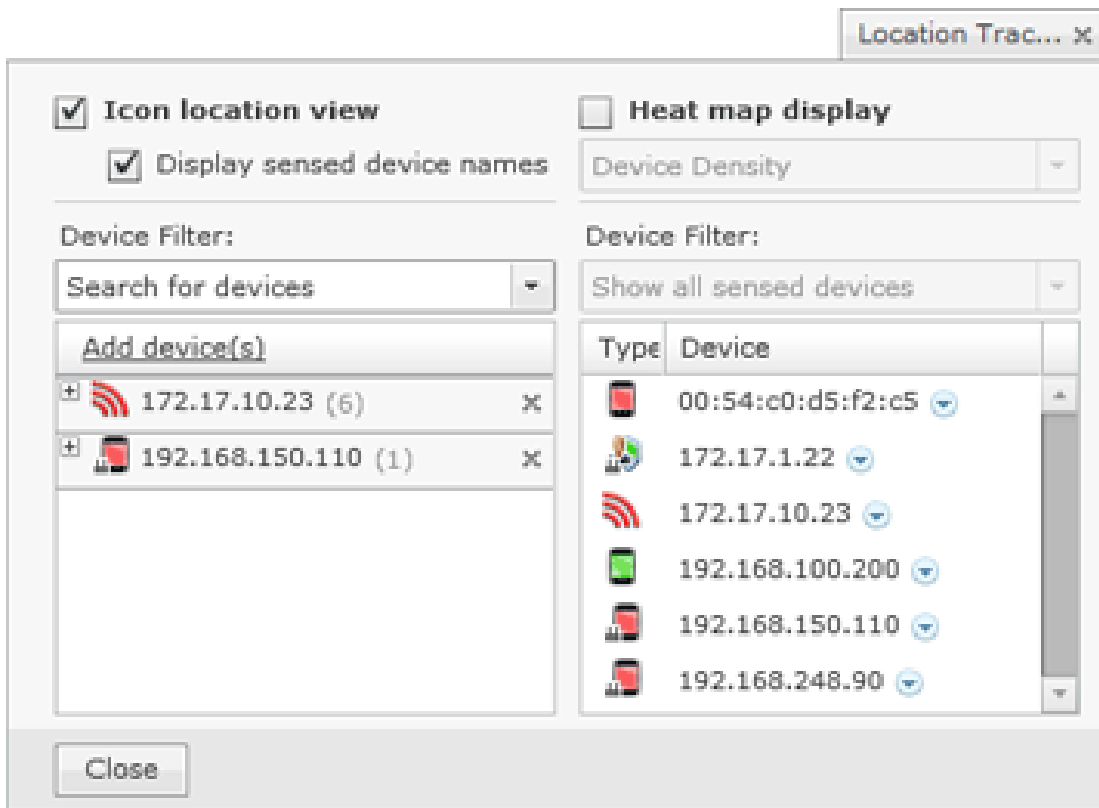


Click the **Close** button or anywhere outside the Location Tracking dialog to display the device in the Floor Plan.

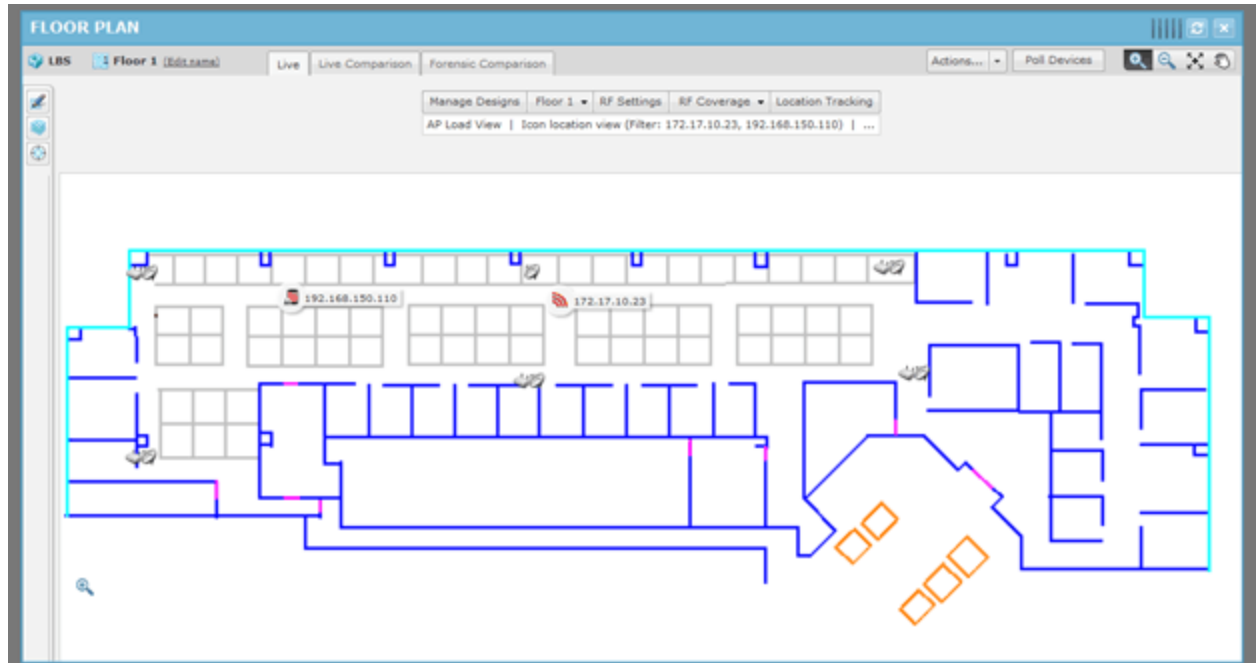


The **Floor Plan** shows the device being tracked. Click the **Refresh** button to refresh the image. If the device has moved, you will see its current position in the floor plan.

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 NX and VX controllers, the WiOS controller must be enabled so that RSSI data can be passed to ADSP. There are procedures for BSSs and Wireless Clients tracking. Refer [BSS Tracking](#) and [Client Tracking](#).



Note

This is only for the controller infrastructure. The 5.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** check box.
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** fields.
6. Click **Apply**.
7. Navigate to **Network > Access Point Radios**.
8. Double-click on the B/G radio of the AP650.
9. Select the **Enable Enhanced Beacon Table** check box.
10. Click **Apply**.
11. Repeat [Step 9](#) and [Step 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.)

Verify Location Tracking

To verify Location Tracking with this setup:

1. Navigate to **Security > Enhanced Probe/Beacon Table > Beacon Table**.
2. Click the **Beacon Found** tab.
Verify that this page is being populated with rogue AP and signal strength data.
3. In the **Portal MAC** column, verify that the radio MAC of your AP650 is displayed.
4. The column next to the **Portal MAC** column is the **Rogue AP MAC** detected by the portal.
5. Copy one the Rogue AP MAC addresses detected by the AP650 radio (A or B/G).
6. In AirDefense, drag the AP650 to a floor plan with 2 other sensors.
7. Attempt to track the device that matches the previously recorded MAC address.
If the target device is detected by the other 2 sensors, location tracking should work.


Client Tracking

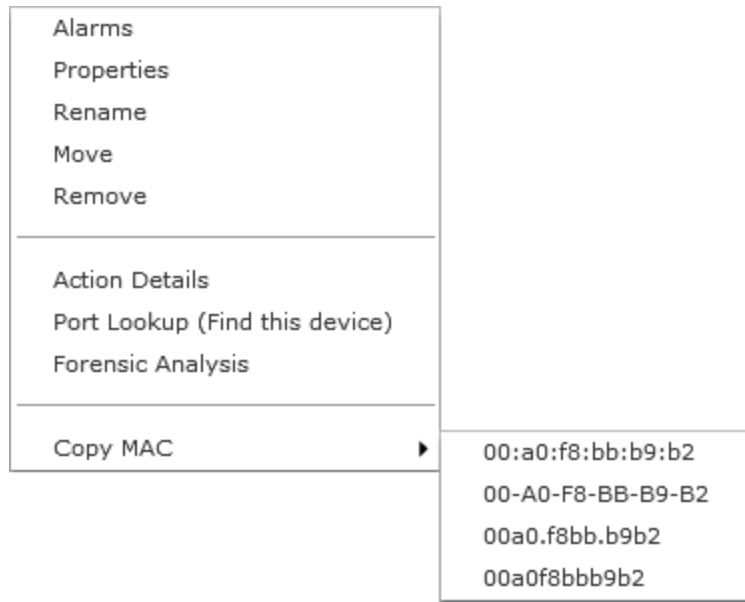
In order to activate Wireless Client tracking, you must enable the Enhanced Probe table on the RFSX000 controller. This allows an AP to forward an MU probe request data to the controller.

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** check box.
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** check box.
11. Click **Apply**.
12. Repeat [Step 9](#), [Step 10](#), and [Step 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:

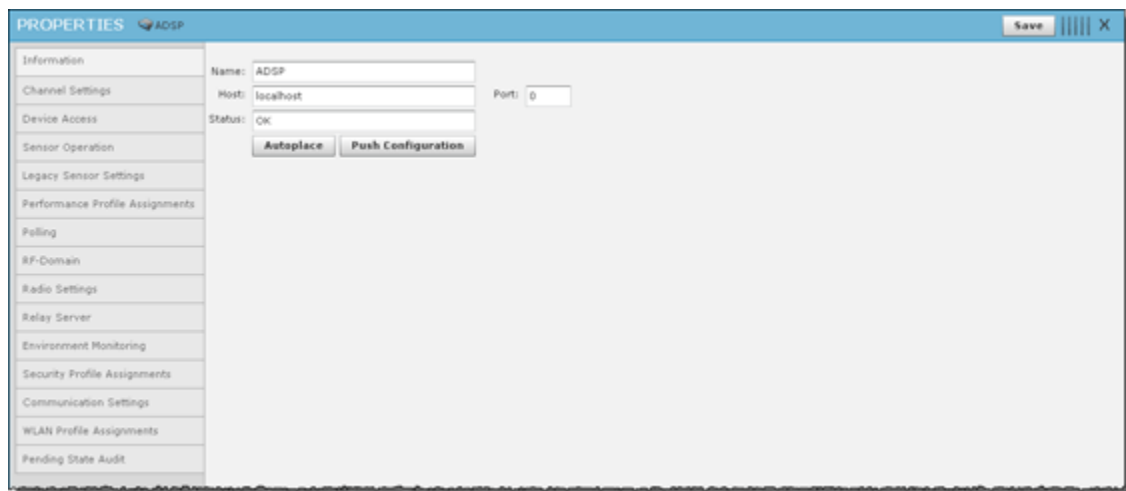
Function	Description
Alarms	Accesses the Alarms tab where you can view the alarms for the selected Unplaced Devices level. See Alarms on page 480 for more information.
Properties	Opens the Properties overlay for the selected Unplaced Devices level.
Rename	Opens a dialog window to rename the selected unplaced device.
Move	Moves the selected unplaced device to another network level (floor). See Move Devices on page 473 for more information.
Remove	Removes the selected unplaced device from your network. See Remove Devices on page 473 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 on page 741 window where you can locate the physical port where the unknown device is accessing your network.
Forensic Analysis	Accesses Forensic Analysis—Basic. See Forensic Analysis-Basic on page 391 for more information.
Copy MAC	Copies the MAC address of the selected unplaced device for later use.

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



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.

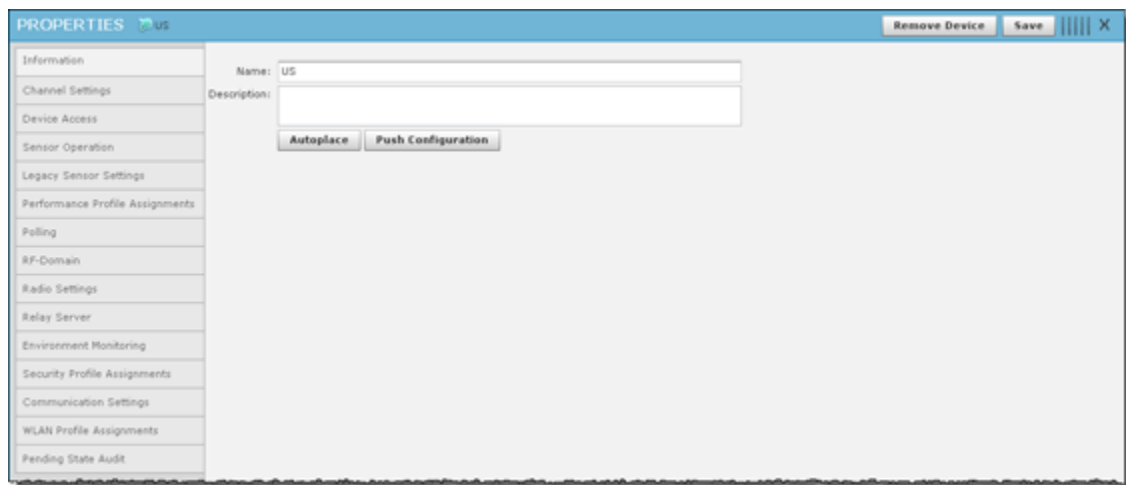
You can view and/or override an appliance's configuration by selecting:

- [Sensor Operation](#) on page 634
- [Sensor Only Settings](#) on page 630
- [Performance Profiles](#) on page 540

- [Polling](#) on page 531
- [Environment Monitoring](#) on page 553
- [Security Profiles](#) on page 511
- [Communication Settings Profile](#) on page 524
- [Location Based Services](#) on page 613
- [Pending State - Audit](#) on page 629

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:

- [Sensor Operation](#) on page 634
- [Sensor Only Settings](#) on page 630
- [Performance Profiles](#) on page 540
- [Polling](#) on page 531
- [Environment Monitoring](#) on page 553
- [Security Profiles](#) on page 511
- [Communication Settings Profile](#) on page 524

- [Location Based Services](#) on page 613
- [Pending State - Audit](#) on page 629

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.

Security

AirDefense has several modules that you can install to provide security for your network. You can enhance AirDefense 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 hackers 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



Note

Each of these modules require a separate license.

WIPS

By installing an AirDefense 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.

AirDefense 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

AirDefense 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 **i** 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. AirDefense 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 AirDefense 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.

Keep the following considerations in mind when deploying your sensors.

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

Keep the following considerations in mind when you place devices:

- Device Density
- Device Requirements per Area
- Desired Monitoring and Intrusion Protection Functionality
- Assets to be Protected
- Sensor Quantity and Placement
- Power and Data Cabling

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

Desired Monitoring and Intrusion Protection Functionality

Your decisions about sensor placement should also take into account what functionality you plan to use. Five important functions that are 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 devices 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—iEven 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 Extreme Networks.

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 sensors 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

This section discusses the planning the placement of sensors.

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 for Sensor Placement

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 (could be a 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 any intrusion. 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 Sensor Placement with WEP Cloaking

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 for Sensor Placement with Location Tracking

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

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

measure unique signal strengths and sensor combinations for each location considered significant.

IDS versus Location Tracking

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



Example 1

You have a small office of 10,000 sq. ft. For Wireless IDS/IPS you would only need 1 sensor; to maximize the coverage it makes sense to place the sensor in the center of the building. When location tracking is 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

AirDefense 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 is 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 is 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 is 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 Profile is 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 is 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.

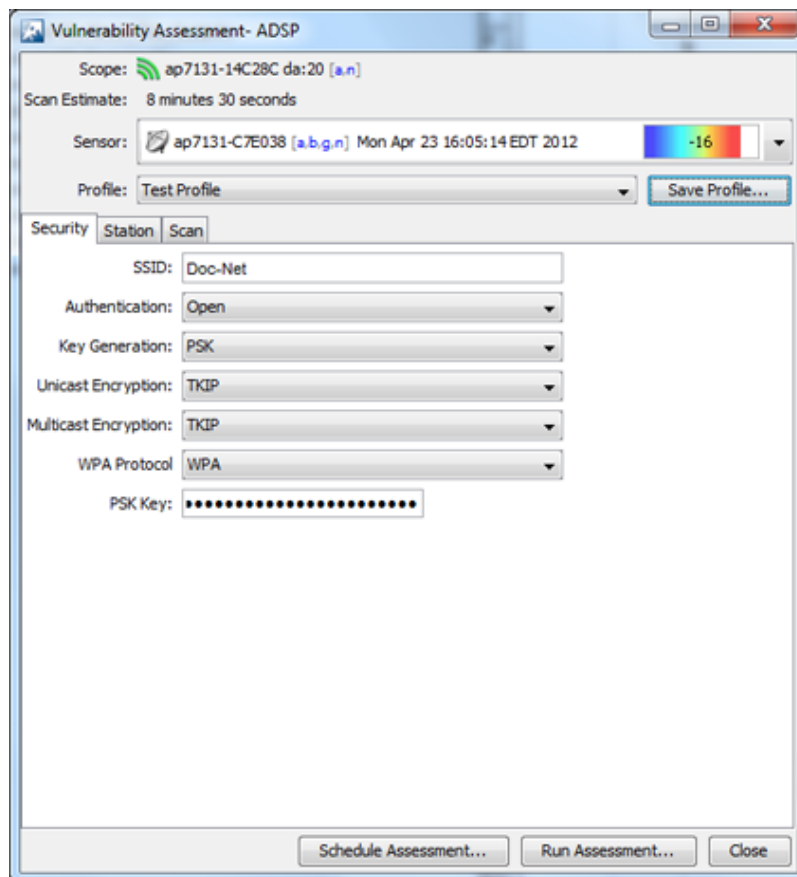
On-Demand Vulnerability Assessment

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

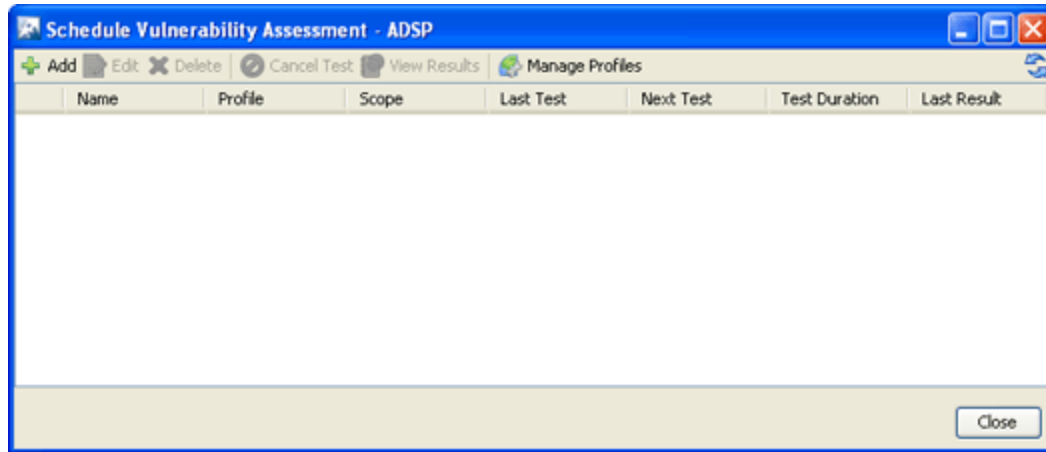
When the scope is network level, all APs in the scope are assessed.



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.

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](#) on page 431.

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

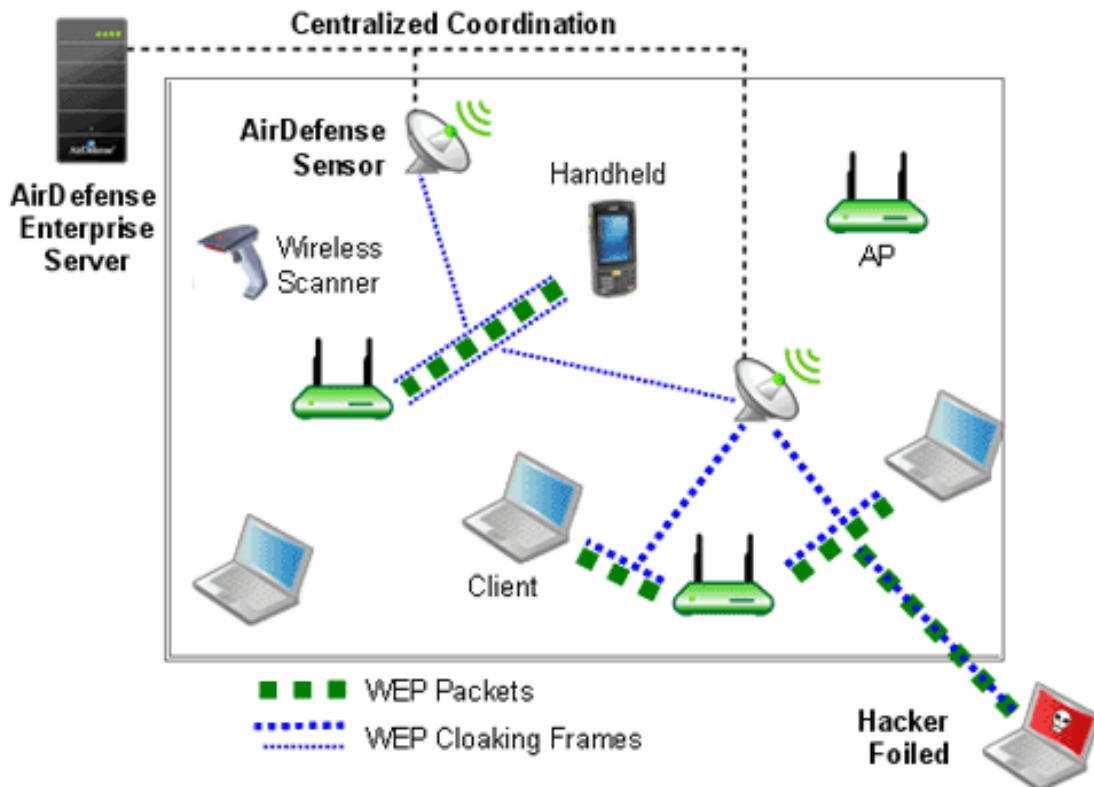
By default, the sensor is a passive wireless monitoring device and does not transmit (provided termination has not been enabled). Enabling the sensors for WEP Cloaking will cause the sensors to actively transmit on the channels of the devices it is protecting.

WEP Cloaking Overview

AirDefense sensors communicate with the AirDefense appliance to coordinate cloaking operation. The server can be configured to instruct a group of sensors to cloak sanctioned devices in a given location. Sensors are designed to intelligently adjust their frequency scanning patterns to maximize cloaking effectiveness while performing

regular Wireless IPS scanning on other channels. More than one sensor can cloak a single wireless device depending on spatial coverage.

Once configured for cloaking, sensors intelligently analyze local traffic and insert carefully timed cloaking frames as shown in the figure below. To attackers, who do not have the secret WEP key, these cloaking frames appear as legitimate WEP traffic between sanctioned devices. Sanctioned devices, configured with the production WEP key, automatically ignore the cloaking frames as their integrity test fails.



An attacker sniffing traffic will not be able to distinguish between cloaking frames and legitimate frames, and therefore, cannot filter out the cloaked frames. When statistical WEP cracking tools are run on the captured data, they simply fail to decode the key. The following figure shows a screenshot of Aircrack-ng with WEP Cloaking enabled.

```

AirCrack-ng

[00:10:45] Tested 1894657 keys (got 711357 IVs)

KB    depth  byte(vote)
0     0/ 1    01< 74> 99< 22> 95< 7> DA< 3> 2B< 3> 72< 0>
1     0/ 1    23< 107> 94< 40> 26< 18> F2< 16> DA< 15> 6A< 13>
2     0/ 1    45< 122> CA< 21> 6C< 3> 70< 1> 42< 0> AD< 0>
3     0/ 1    67< 124> 21< 15> 80< 10> 81< 5> 62< 3> B3< 3>
4     0/ 1    89< 45> B3< 9> 2A< 8> DD< 8> F4< 8> 45< 5>
5     1/ 2    AC< 10> 82< 7> B4< 5> 66< 1> 81< 0> F5< 0>
6     5/ 6    F6< 10> CB< 9> 6D< 9> FF< 7> 3C< 5> D2< 5>
7     0/ 1    97< 35> F4< 13> FF< 13> 3C< 12> F6< 11> E4< 11>
8     1/ 2    CB< 30> 4B< 10> 5D< 5> 28< 5> 08< 5> 2A< 5>
9     6/ 7    59< 15> 32< 13> 6B< 12> 1E< 11> 73< 11> 52< 9>
10    0/ 1    72< 61> 05< 30> EC< 20> 17< 16> CD< 15> EF< 14>
11    0/ 9    46< 43> 18< 32> 71< 31> 0C< 30> 4B< 26> 98< 25>

Attack failed. Possible reasons:

* Out of luck: you must capture more IVs. Usually, 104-bit WEP
  can be cracked with about one million IVs, sometimes more.

* If all votes seen equal, or if there are many negative votes,
  then the capture file is corrupted, or the key is not static.

* A false positive prevented the key from being found. Try to
  disable each Korek attack (-k 1 .. 17), raise the fudge factor
  (-f)

```

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 devices 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.

ADSPAdmin

When performing initial AirDefense configuration, you have to use AirDefense's ADSPAdmin utility from the command line interface (CLI).

Once AirDefense is set up, use the Graphical User Interface (GUI) for ongoing configuration. The following functions are provided in ADSPAdmin:

- Manage
- Dbase
- Software
- Config

Accessing the ADSPAdmin Console

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> key combination.

2. Type `c`, then press <Enter> at the command prompt. The **Config** screen displays.

```

*** ADSPAdmin ***

(C) Config

(IDS) Airids config
(IP) IP address config
(IPv6) IPv6 address config
(NETPORT) Network port speed/duplex config
(DNS) Define DNS servers
(BONDING) High Availability Ethernet config
(HNAME) Set hostname
(DNAME) Set domain name
(TIME) Time/Date config
(TZ) Set timezone
(NTP) Enable/disable NTP
(PING) Enable/disable ICMP Echo Request (ping) responses
(SNMPPA) Enable/disable reception Snmp agent requests
(SNMPC) Configure Snmp agent community string.
(SNMPT) Enable/disable SNMP trap reception
(HTTP) Enable/disable unencrypted sensor connections
(PANIC) Enable/disable reboot on system error
(UIPORT) Display network port for dashboard access

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

```

Manage System

Use the following included utilities to perform system management tasks:

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 (<i>syslogdata.txt</i>).
TRIMLOG	Truncate system log files when they become too large.
ADMU	Resets the administrator password back to the system default.
WHITELIST	Manages a list of IP addresses/address ranges that are allowed access to the AirDefense server.
PASSWD	Change the password of a Command Line User (<i>smxmgr</i> and <i>smxarchive</i>).
RESTART	Restart AirDefense processes Warning: This is not a full system reboot!

ADSPadmin Utility	Use this utility to...
REBOOT	Reboot AirDefense appliance Warning: This is a full system reboot!
HALT	Halt AirDefense (stop processes.)

Manage the Database

Use the following included utilities to manage AirDefense database.

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

Use this utility to check and upgrade the AirDefense software.

ADSPadmin Utility	Use this utility to...
SERVMOD	Update the current version of AirDefense software with feature enhancements or improvements.

Configure AirDefense

The ADSPadmin Config program area provides the following utilities for configuring AirDefense:

- **IDS**—Use this item to enable or disable SSLv3 support, Fast Termination, and MAC Spoof detection settings on the AirDefense appliance. These settings are required for AirDefense to work properly with some legacy systems.
- **IP**—use this to change the IP address, subnet mask, and default gateway of the AirDefense appliance.
- **IPv6**—use this to change the IPv6 address of the AirDefense appliance.
- **NETPORT**—use this to change network interface settings, and to toggle Auto-negotiation on and off.
- **DNS**—use this to add or delete a DNS name server (Domain Name Server).
- **BONDING**—use this to enable the High Availability Ethernet.
- **HNAME**—use this to change the name of the AirDefense appliance.
- **DNAME**—use this to change the domain to which the AirDefense appliance belongs.

- TIME—use this to configure the AirDefense appliances operating time and date.
- TZ—use this to configure the time zone in which the AirDefense 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.
- SSLv3—use this to configure SSL version 3 support.

Configure IDS

Use the switches under IDS to enable AirDefense to work with some specific features. The following configurations are available under IDS:

- SSLv3—Use this switch to enable/disable support for *SSLv3*, *TLSv1.0* and *TLSv1.1* protocols. Recently these protocols were found vulnerable and we recommend that you do not use them. However, if your deployment has access points and sensors that support these protocols, we recommend that you enable this switch. Otherwise, you should evaluate the devices in your network and consider disabling support for *SSLv3*, *TLSv1.0* and *TLSv1.1* protocols using this switch.
- FTMODE—Use this switch to enable/disable Fast Termination. When enabled, AirDefense internally adjusts various operating parameters and configurations to support Fast Termination.
- SPOOF—Use this switch to enable/disable AirDefense's new *MAC Spoof Detection* algorithm. This algorithm uses Forensic data and forensic queries to raise the new "MAC Spoof Detected" alarm. If you are not interested in this new alarm, we recommend you disable this alarm using this switch. By default, this switch is enabled.

IP Address Configuration

To configure the IP address of your AirDefense server:

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

To configure the IPv6 address of your AirDefense server:

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 Auto-negotiation on and off. The Auto-negotiation feature enables the AirDefense 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 Configuration

To configure the DNS servers of your AirDefense server:

1. Type `dns`, then press `[Enter]` at the prompt to define DNS servers. This adds or deletes a DNS name server (Domain Name Server). This is the name of the server you give to your DNS server. The **NameServer** screen opens, displaying your current DNS servers IP address in bold text.
 - 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 index number of the name server 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.)
2. At the prompt, type `a` to add a new DNS server. To delete a server, type `d`.



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 and 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 Configuration

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 Configuration



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 AirDefense.

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 AirDefense appliance, then press `[Enter]`. You are prompted to save your changes.
3. Type `yes`, then press `[Enter]`.

dname Configuration

To configure the DNAME value of your AirDefense server:



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 AirDefense appliance, then press `[Enter]`. You are prompted to save your changes.
3. Type `yes`, then press `[Enter]`.

Time Configuration



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. You can also 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 AirDefense appliances 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 any other delimiters.)
3. Press `[Enter]`. You are prompted to enter a time in 24-hour HHMM or HHMMSS format. (Do not use colon (:), or any other delimiters.)
4. Press `[Enter]`. You are prompted to save your changes.
5. Type `yes`, then press `[Enter]`.

Time Zone Configuration

To configure a valid time zone (TZ) for your AirDefense server:



Important

Any change will cause a system reboot on exit from ADSPAdmin.

1. Type `tz`, then press `[Enter]` at the prompt to change the AirDefense appliances time zone. The **Time Zone** screen displays a list of global, continental regions. AirDefense prompts you to choose a global area in which your AirDefense 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 AirDefense appliance resides. Press `[Enter]`. A list of nationalities appears.

4. Enter the number of the region within your nationality in which the AirDefense 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 Configuration

Instead of setting the AirDefense Time (TIME) and Timezone (TZ), you can enable automatic time synchronization with an NTP.

For example, if you change the AirDefense time such as when you move the AirDefense appliances 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.



Note

Entering an invalid time server generates an error and logs you out of ADSPadmin. Also, changing the time configurations after your AirDefense Appliance has accumulated data can have an adverse affect on the integral state, time, and event associations that are essential to accurate data reporting.

PING Config

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.

SNMP Agent Configuration

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.

SNMP Community String Configuration

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] again.



Note

The default community string is *public*.

3. Type `yes` and press [Enter] to save your change (or `no` to disregard your change).

SNMP Trap Configuration

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 SNMP are displayed indicating if the status is OK or not.
5. Press [Enter] to display the Config menu.

The SNMP daemons are stopped and then restarted. The Config menu is displayed.

HTTP Configuration

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 Configuration

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 Configuration

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.

Troubleshooting

AirDefense provides modules and solution packages to assist you in troubleshooting your network. The individual modules are:

- [AP Testing](#)
- [Connection Troubleshooting](#)
- [Live RF](#)
- [Forensic RF](#)
- [Spectrum Analysis](#)

The available solution packages are:

- [Advanced Spectrum Analysis](#)
- [Advanced Troubleshooting](#)
- [Assurance Suite \(Network Assurance\)](#)
- [Radio Share 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.

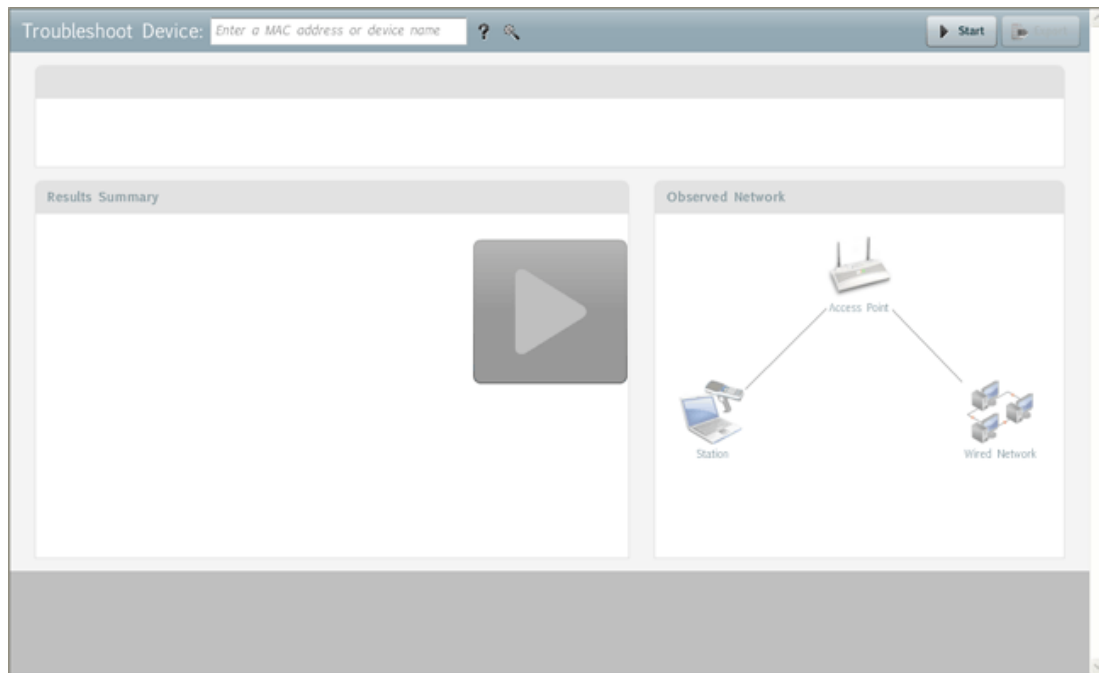
See the [AP Testing](#) for details on how to schedule both automated and on-demand tests for APs.

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

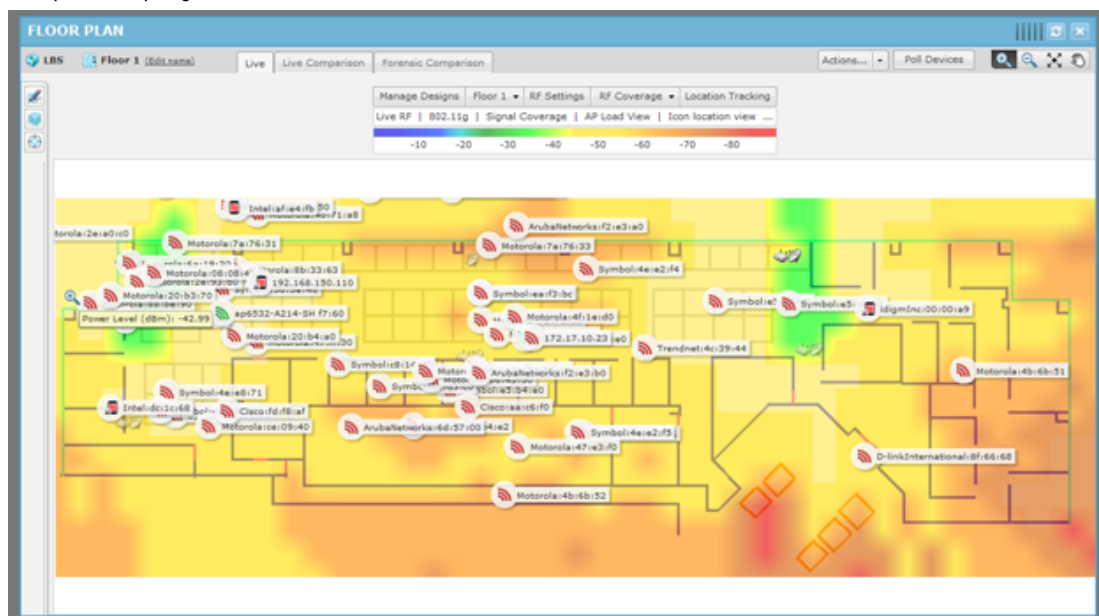
the status of a Wireless Client within your wireless network and display results summarizing the status.

The Troubleshooting tool is accessed through the ADSP GUI.



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 refreshed (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 AirDefense 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.

Forensic RF

The Forensic RF feature, included with the Live RF license, visualizes forensic data to display coverage over a specific time range.



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 AirDefense software; no extra hardware is required.



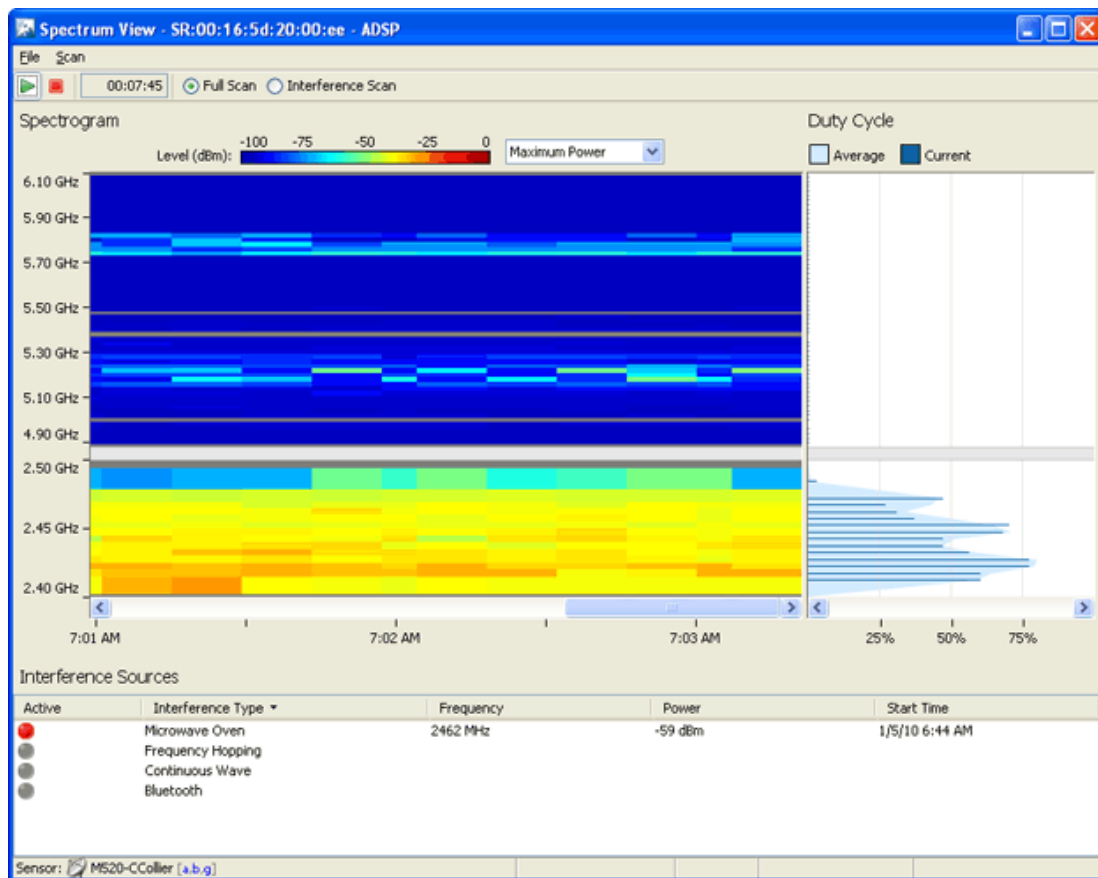
Note

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).

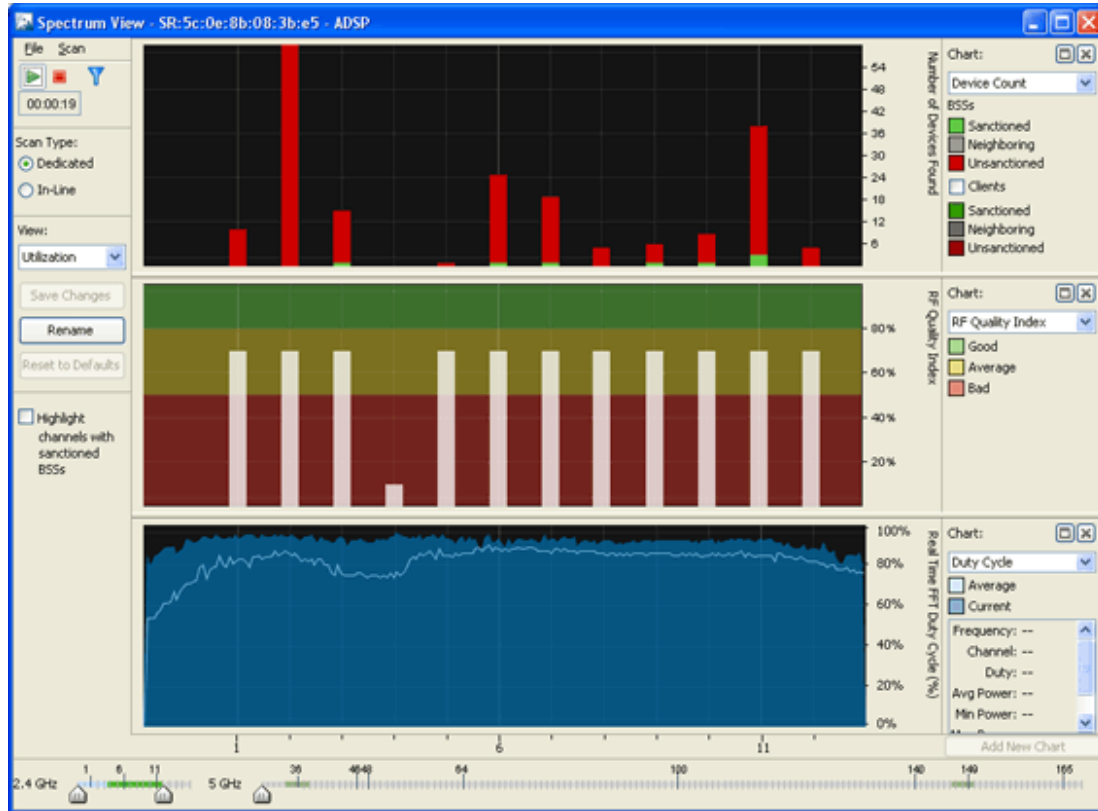
- Generate 'RF Spectrum Analysis' alerts (Bluetooth, Microwave, Frequency Hopper, Continuous Wave)
- Dedicated Spectrum View
 - Sensor temporarily dedicated to Spectrum Analysis
 - While in Spectrum View the sensor provides no protocol analysis (after user-configured time period, sensor defaults back 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 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.

The [Advanced Spectrum Analysis](#) topic in Configuration chapter fully explains how to configure and use the Advanced Spectrum Analysis tool.

Advanced Troubleshooting

An Advanced Troubleshooting license gives you access to two modules: AP Test and Connection Troubleshooting. AP Test provides a way to remotely test connectivity to APs 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 as a part of the license.

Assurance Suite (Network Assurance)

The Network Assurance solution includes several modules that assist 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

AirDefense 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

For more information on customer support see [Getting Help](#) section in this document.

AirDefense Icons

AirDefense uses a large number of icons to represent the different states of devices managed by it. AirDefense icons can be broadly classified as:

- [AirDefense Application Icons](#)—Describes the various icons used to depict AirDefense's state.
- [Wireless Client Icons](#)—Describes the various icons used to depict the state of wireless clients identified in the AirDefense managed network.










AirDefense Application Icons

The following Icons are used in the AirDefense application. They are organized into the following categories:

- [Overlay Icons](#)—Describes the icons used as overlay to convey additional meaning to other icons
- [Dashboard Icons](#)—Describes the icons used on the AirDefense dashboard
- [Tree Icons](#)—Describes the various icons used to represent AirDefense tree hierarchy
- [Alarm Icons](#)—Describes the various icons used to represent the various alarms generated by AirDefense
- [Appliance Icons](#)—Describes the icons used to represent the state of the AirDefense Appliance
- [Switch Icons](#)—Describes the various icons used to represent the switches managed by the AirDefense Appliance
- [Sensor Icons](#)—Describes the various icons used to represent the state of sensors managed by the AirDefense Appliance
- [Access Point Icons](#)—Describes the various icons used to represent the state of access point managed by the AirDefense Appliance
- [BSS Icons](#)—Describes the various icons used to represent the different BSSs identified by AirDefense
- [Unknown Device Icons](#)—Describes the icons used to represent unknown devices identified by AirDefense
- [Manager Icons](#)—Describes the icons used to represent device managers identified by AirDefense
- [SSID Icons](#)—Describes the icon that indicates the SSID of a BSS






Overlay Icons

The following symbols are used in conjunction (as overlay) with the device icons to help identify them:

Symbol	Description
	Offline device
	Unlicensed device
	Device on wired network
	Device on wireless network
	Unmanaged device
	Part of a bridged network
	Associated to a network
	Participating in an Ad-Hoc network
	Wi-Fi Direct device










Dashboard Icons

The following icons represent the dashboard graphs and charts:

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






The following icons describe the device in the tree view window:

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.
	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



The following are the 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.

Icon	Description
	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



The following icons indicate the state of the AirDefense appliance.

Icon	Description
	Online AirDefense appliance.
	Offline AirDefense appliance.

Switch Icons








These icons indicate the state of the switches managed by AirDefense.

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.

Icon	Description
	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

These icons indicate the state of a sensor:

Icon	Description
	A Sensor that is functioning normally and is communicating with the AirDefense Server. To be online, the Sensor must be connected to the AirDefense Server.
	A Sensor that is not communicating with the AirDefense 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 AirDefense 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 AirDefense appliance.
	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 AirDefense Server. If you did not intentionally take the Sensor off-line, check the Sensor's configuration settings.










Icons



These icons indicate an APs state and capabilities:

Icon	Description
	An online AP that is managed by AirDefense.
	An online AP that is not managed by AirDefense.
	An offline AP that is managed by AirDefense.
	A planned as related to adding planned devices to a floor plan.
	An AP that has a Sensor in radio share mode.

BSS Icons



These icons indicate the state of the BSS:

Icon	Description
	Sanction BSS—BSS that has been sanctioned by AirDefense.
	Unsanctioned BSS—BSS that has not been sanctioned by AirDefense.
	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 AirDefense.
	Bridge Unsanctioned BSS—Two or more BSSs that have been bridged and are not sanctioned by AirDefense.
	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 AirDefense.

Icon	Description
	Wi-Fi Direct Unsanctioned BSS—Wi-Fi Direct BSS that has not been sanctioned by AirDefense.
	Wi-Fi Direct Neighboring BSS—Wi-Fi Direct BSS that is on a neighboring network.



Unknown Device Icons

These icons depict the status of unknown devices in the network:

Icon	Description
	Unknown device detected in your wireless traffic.
	Non-wireless device marked as a wired resource.


Manager Icons

These icons depict managers in the AirDefense network:

Icon	Description
	Wired Manager
	Wireless Manager

SSID Icon

This icon depicts the SSID information:

Icon	Description
	This is the Service Set Identifier to which the BSSs belong.

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 AirDefense GUI. The different types are:






- [Default or Un-categorized Devices](#)—Default (used to identify Wireless Clients that have not been associated with a specific type)
- [MCDs](#)—Describes the various icons used to represent the state of mobile computing devices carried by employees

- [VoIP Phones](#)—Describes the various icons used to represent the state of Voice Over Internet Protocol (VoIP) devices in the network
- [Laptops](#)—Describes the various icons used to represent the state of Laptops identified by AirDefense
- [Employee Laptops](#)—Describes the various icons used to represent the state of laptops assigned to employees as identified by AirDefense
- [Employee Phones](#)—Describes the various icons used to represent the state of mobile phones assigned to employees as identified by AirDefense
- [Employee Devices](#)—Describes the various icons used to represent the state of devices other than Laptops, MCDs, and Mobile Phones assigned to employees as identified by AirDefense
- [High Priority Visitor Devices](#)—Describes the various icons used to represent the state of devices identified as High Priority Visitor devices
- [Visitor Devices](#)—Describes the various icons used to represent the state of visitor devices
- [Low Priority Visitor Devices](#)—Describes the various icons used to represent the state of devices identified as belonging to Low Priority Visitors

Default or Uncategorized Devices











The following icons describe devices that are identified by AirDefense but are yet to be classified:




Icon	Description
	A Wireless Client that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	A Wireless Client that is not sanctioned by AirDefense 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.
	A Wireless Client that is sanctioned by AirDefense and is currently probing and is associated to a BSS.
	A Wireless Client that is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.

Icon	Description
	One or more Wireless Clients that are not sanctioned by AirDefense 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 AirDefense.
	A Wi-Fi Direct Wireless Client that is not sanctioned by AirDefense.
	A Wi-Fi Direct Wireless Client on a neighboring network.

MCDs










These icons display MCD status:





Icon	Description
	A MCD that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	A MCD that is not sanctioned by AirDefense 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 AirDefense and is currently probing and is associated to a BSS.
	A MCD that is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more MCDs that are not sanctioned by AirDefense forming an Ad-Hoc network.
	One or more MCDs on a neighboring network forming an Ad-Hoc network.

Icon	Description
	A Wi-Fi Direct MCD that is sanctioned by AirDefense.
	A Wi-Fi Direct MCD that is not sanctioned by AirDefense.
	A Wi-Fi Direct MCD on a neighboring network.

VoIP Phones












These icons display VOIP phone status:



Icon	Description
	A VoIP Phone that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	A VoIP Phone that is not sanctioned by AirDefense 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 AirDefense and is currently probing and is associated to a BSS.
	A VoIP Phone is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more VoIP Phones that are not sanctioned by AirDefense forming an Ad-Hoc network.

Icon	Description
	One or more VoIP Phones on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct VoIP Phone that is sanctioned by AirDefense.
	A Wi-Fi Direct VoIP Phone that is not sanctioned by AirDefense.
	A Wi-Fi Direct VoIP Phone on a neighboring network.

Laptops














These icons display the status of laptops in your network:

Icon	Description
	A Laptop that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	A Laptop that is not sanctioned by AirDefense 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 AirDefense and is currently probing and is associated to a BSS.
	A Laptop is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more Laptops that are not sanctioned by AirDefense 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 AirDefense.

Icon	Description
	A Wi-Fi Direct Laptop that is not sanctioned by AirDefense.
	A Wi-Fi Direct Laptop on a neighboring network.














Employee Laptops

These icons display the status of laptops assigned to employees:

Icon	Description
	An Employee Laptop that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	An Employee Laptop that is not sanctioned by AirDefense 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.
	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 AirDefense and is currently probing and is associated to a BSS.
	An Employee Laptop is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more Employee Laptops that are not sanctioned by AirDefense 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 AirDefense.
	A Wi-Fi Direct Employee Laptop that is sanctioned by AirDefense.
	A Wi-Fi Direct Employee Laptop on a neighboring network.














Employee Phones

These icons display the status of mobile phones assigned to employees:

Icon	Description
	An Employee Phone that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	An Employee Phone that is not sanctioned by AirDefense 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 AirDefense and is currently probing and is associated to a BSS.
	An Employee Phone is not sanctioned by AirDefense 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.
	One or more Employee Phones that are sanctioned by AirDefense forming an Ad-Hoc network.
	One or more Employee Phones that are not sanctioned by AirDefense 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 AirDefense.
	A Wi-Fi Direct Employee Phone that is not sanctioned by AirDefense.
	A Wi-Fi Direct Employee Phone on a neighboring network.














Employee Devices

These icons display the status of other devices (other than laptops and mobile phones) assigned to employees:

Icon	Description
	An Employee Device that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	An Employee Device that is not sanctioned by AirDefense 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 AirDefense and is currently probing and is associated to a BSS.
	An Employee Device is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more Employee Devices that are not sanctioned by AirDefense forming an Ad-Hoc network.
	One or more Employee Devices on a neighboring network forming an Ad-Hoc network.
	A Wi-Fi Direct Employee Device that is sanctioned by AirDefense.
	A Wi-Fi Direct Employee Device that is not sanctioned by AirDefense.
	A Wi-Fi Direct Employee Device on a neighboring network.














High Priority Visitor Devices

These icons display the status of high priority visitor devices in your network.

Icon	Description
	A High Priority Visitor Device that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	A High Priority Visitor Device that is not sanctioned by AirDefense 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 AirDefense and is currently probing and is associated to a BSS.
	A High Priority Visitor Device is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more High Priority Visitor Devices that are not sanctioned by AirDefense 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 AirDefense.
	A Wi-Fi Direct High Priority Visitor Device that is not sanctioned by AirDefense.
	A Wi-Fi Direct High Priority Visitor Device on a neighboring network.














Visitor Devices

These icons display the status of visitor devices in your network.

Icon	Description
	A Visitor Device that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	A Visitor Device that is not sanctioned by AirDefense 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 AirDefense and is currently probing and is associated to a BSS.
	A Visitor Device is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more Visitor Devices that are not sanctioned by AirDefense 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 AirDefense.
	A Wi-Fi Direct Visitor Device that is not sanctioned by AirDefense.
	A Wi-Fi Direct Visitor Device on a neighboring network.

Low Priority Visitor Devices

These icons display the status of low priority visitor devices in your network.

Icon	Description
	A Low Priority Visitor Device that is sanctioned by AirDefense and is currently probing but is not associated to a BSS.
	A Low Priority Visitor Device that is not sanctioned by AirDefense 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.
	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 AirDefense and is currently probing and is associated to a BSS.
	A Low Priority Visitor Device is not sanctioned by AirDefense 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 AirDefense forming an Ad-Hoc network.
	One or more Low Priority Visitor Devices that are not sanctioned by AirDefense 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 AirDefense.
	A Wi-Fi Direct Low Priority Visitor Device that is not sanctioned by AirDefense.
	A Wi-Fi Direct Low Priority Visitor Device on a neighboring network.