



Extreme AirDefense Essentials v25.4.0 User Guide

Configuration, Management, and Alarm Monitoring

9039380-00 Rev AA
July 2025



Copyright © 2025 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: <https://www.extremenetworks.com/about-extreme-networks/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/>

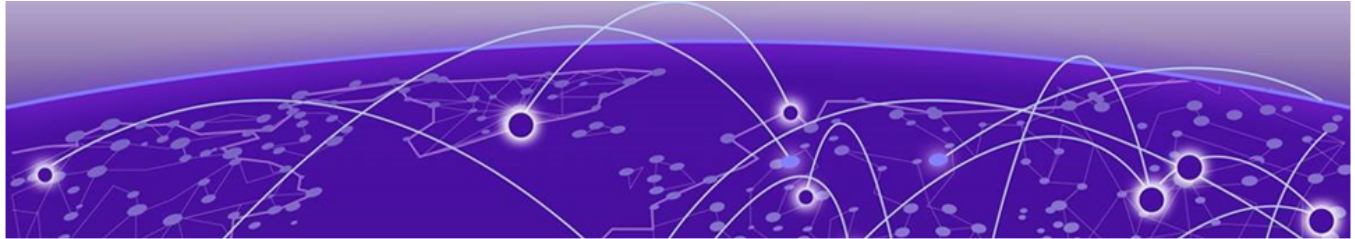


Table of Contents

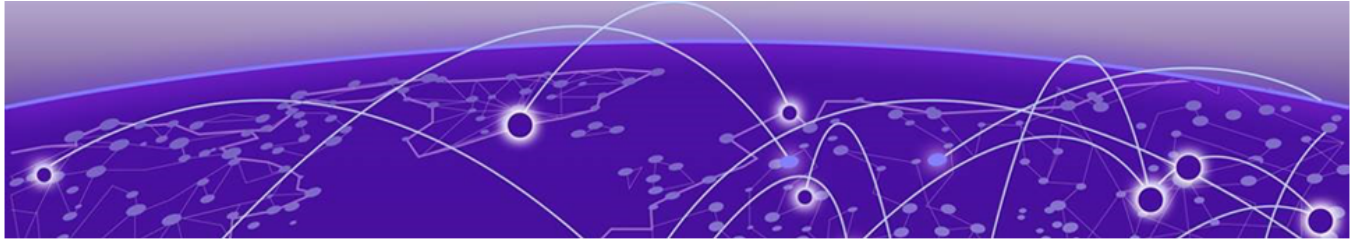
Abstract.....	V
Preface.....	6
Conventions.....	6
Text Conventions.....	6
Terminology.....	8
Send Feedback.....	8
Help and Support.....	8
Subscribe to Product Announcements.....	9
Documentation and Training.....	9
Open Source Declarations.....	9
Training.....	10
Scope of Documentation.....	11
Prerequisites and Limitations.....	12
Extreme AirDefense Essentials in ExtremeCloud IQ	13
WIPS Policies for Extreme AirDefense Essentials.....	16
Summary.....	17
Widget - Alarms Overview.....	19
Widget - Alarm Count by Severity.....	19
Impact Percentile Map.....	20
Widget - Alarms By Device Types.....	21
Widget - Frequently Seen Alarms.....	22
Widget - Alarm Count By Location.....	22
Widget - Alarms Distribution Per Category.....	23
Alarms.....	24
Alarms Cycle	25
Alarm Details.....	27
Live Alarms View.....	28
Live Alarms Widgets.....	30
Live Alarms Raised Table.....	31
Expired Alarms View.....	32
Expired Alarms Activity Line Graph.....	34
Expired Alarms Widgets.....	35
Expired Alarms Raised Table.....	35
Rogue Device Detection.....	36
Locate Rogue Devices.....	37
Terminate Rogue Devices.....	38
Manual Rogue Classification.....	39
Sync Rogue Sanctioned Alarm.....	40

Viewing Data by Sensor.....	42
------------------------------------	-----------

Alarm Management Settings.....	46
---------------------------------------	-----------

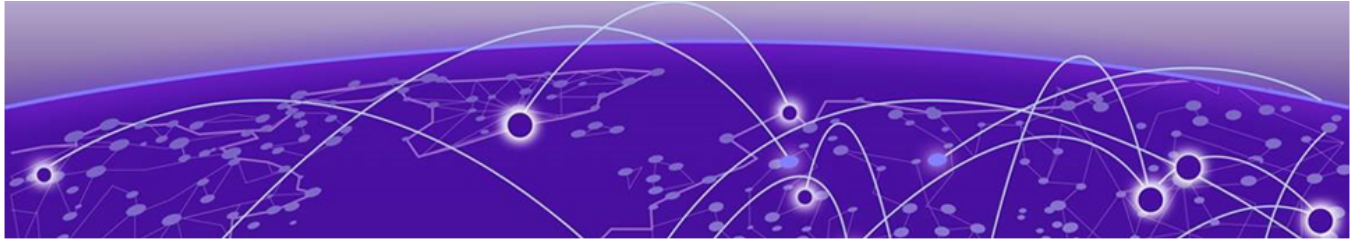
Alarm Notifications Webhook Configurations.....	47
---	----

Classified Devices Management Settings.....	49
---	----



Abstract

The Extreme AirDefense Essentials User Guide for version 25.4.0 by Extreme Networks, serves as a comprehensive manual for utilizing the Extreme AirDefense Essentials platform within ExtremeCloud IQ. This guide outlines configuration and operational procedures for implementing security protocols, managing alarms, and monitoring network threats. Version 25.4.0 adds support for AP4020. Key features include descriptions of alarm management settings, rogue device detection and termination, and viewing data by sensor. The document also provides information on configuring WIPS policies, using widgets for monitoring alarm activity, and leveraging the platform's tools for threat detection and response. It is intended for network administrators seeking to enhance network security and visibility.



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 Extreme Networks switches or 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 User Enablement 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, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and 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 2800. 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](#)

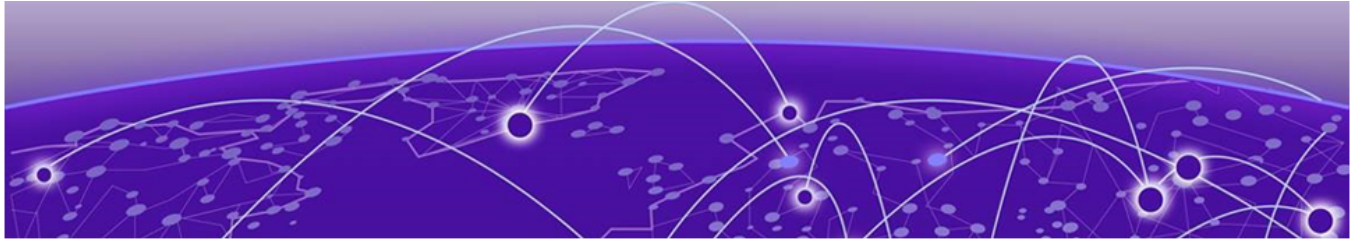
[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

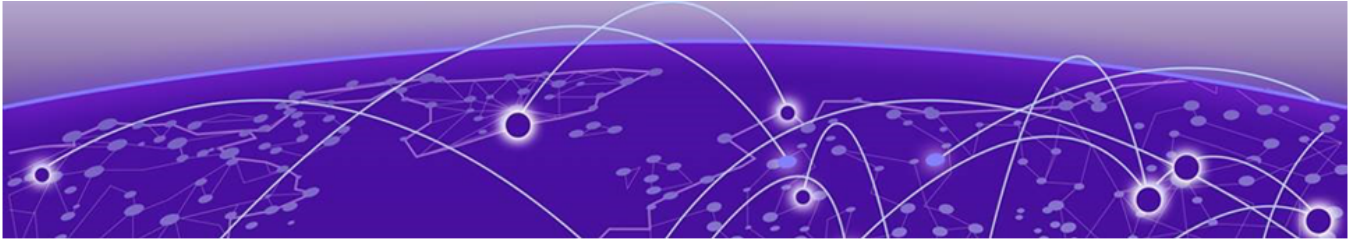
Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.



Scope of Documentation

The Extreme AirDefense Essentials guide includes the following:

- Extreme AirDefense Essentials in ExtremeCloud IQ
- Extreme AirDefense Essentials [Summary](#)
- Extreme AirDefense Essentials [Alarms](#)
- Extreme AirDefense Essentials [Sensors](#)
- Extreme AirDefense Essentials [Settings](#)



Prerequisites and Limitations

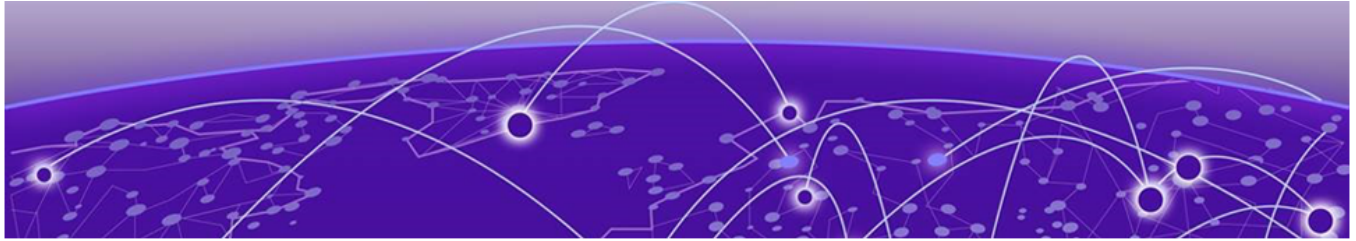
This document provides the information required to perform an Extreme AirDefense Essentials AP sensor configuration.

You must be familiar with accessing and performing basic functions in ExtremeCloud IQ and Extreme AirDefense Essentials. For more information, see the following product documentation:

- [ExtremeCloud IQ](#)
- [Extreme AirDefense Essentials](#)

You need the following before you begin:

- An ExtremeCloud IQ account with Pilot license for access to Extreme AirDefense Essentials services
- An ExtremeCloud IQ supported AP model that is connected to the cloud and assigned a working network policy.



Extreme AirDefense Essentials in ExtremeCloud IQ

Extreme AirDefense Essentials is a cloud-based management tool you can use to configure, implement and review security protocols that evaluate and monitor threat detection for devices in your network.

To get started, go to the ExtremeCloud IQ Dashboard and select the Essentials  > icon from the list. Then select Extreme AirDefense Essentials. The Extreme AirDefense Essentials Overview launches in ExtremeCloud IQ.

The Extreme AirDefense Essentials Overview launches in ExtremeCloud IQ.

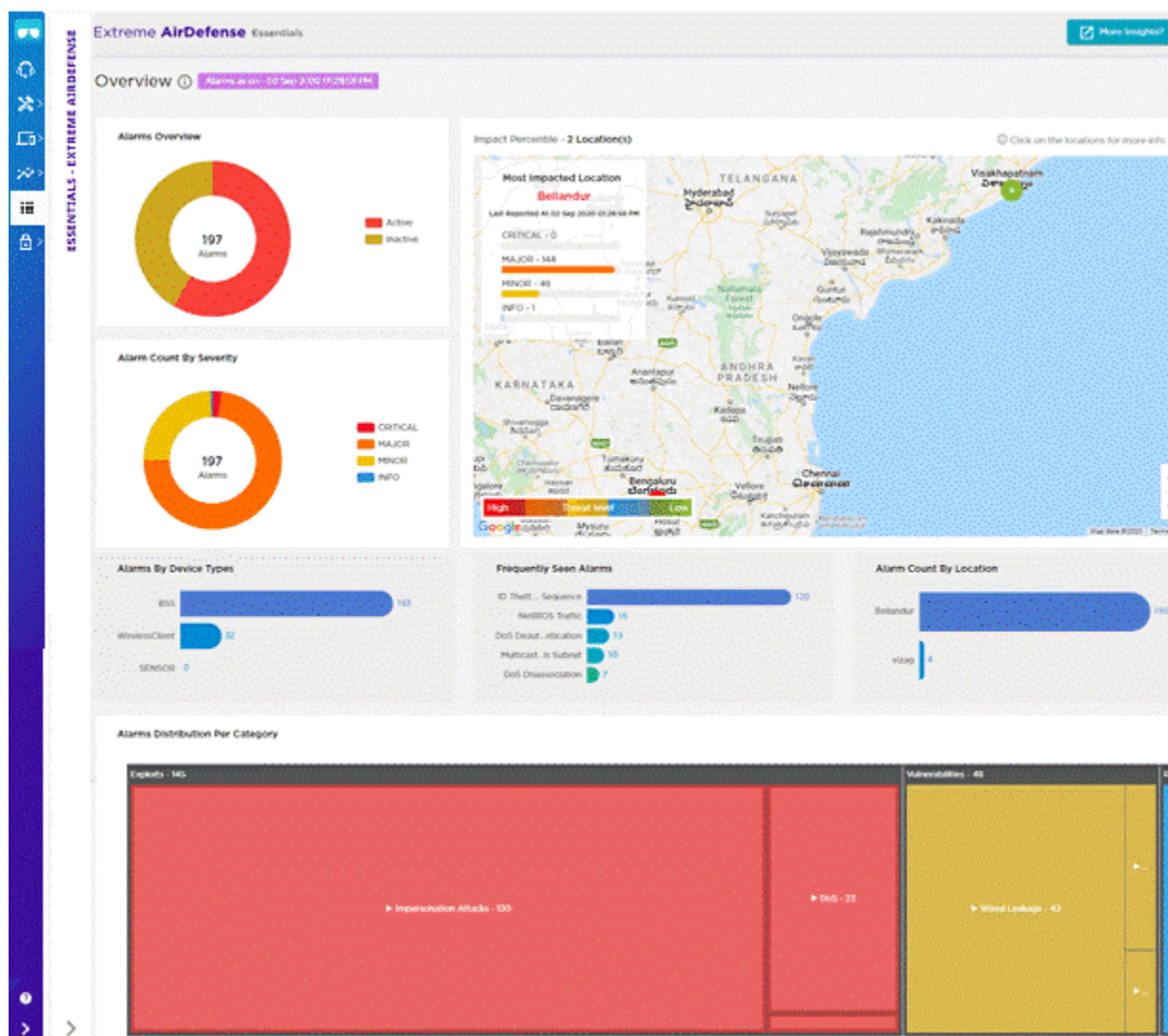


Figure 1: Extreme AirDefense Essentials Overview View in ExtremeCloud IQ

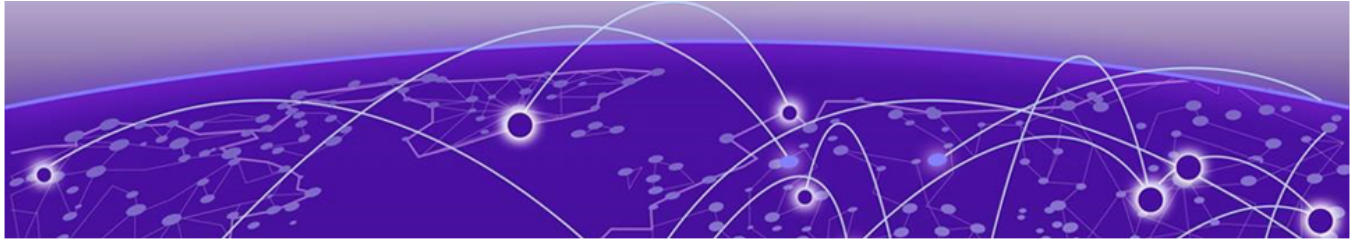
The Extreme AirDefense Essentials Overview in ExtremeCloud IQ includes the following widgets:

- [Widget - Alarms Overview](#) on page 19
- [Widget - Alarm Count by Severity](#) on page 19
- [Impact Percentile Map](#) on page 20
- [Widget - Alarms By Device Types](#) on page 21
- [Widget - Frequently Seen Alarms](#) on page 22
- [Widget - Alarm Count By Location](#) on page 22
- [Widget - Alarms Distribution Per Category](#) on page 23

Select the **More Insights** button at the top right corner of the Overview to launch Extreme AirDefense Essentials and open the Extreme AirDefense Essentials [Alarm Management Settings](#) on page 46.

The following access point models are supported:

- AP302W
- AP305C/CX
- AP305C-1
- AP410C/CX
- AP410C-1
- AP460C
- AP460S6C
- AP460S12C
- AP510C
- AP650
- AP3000
- AP3000X
- AP4000
- AP4000-1
- AP4020
- AP5010
- AP5020
- AP5050D
- AP5050U



WIPS Policies for Extreme AirDefense Essentials

To access Extreme AirDefense Essentials, the WIPS Policy must be enabled for Extreme AirDefense Essentials in ExtremeCloud IQ.

1. From the Extreme AirDefense Essentials overview view, select the **Settings** icon located beside the **More Insights?** button.

The **WIPS Policies** window opens, where you can select the policies for Wireless Threat Detection.

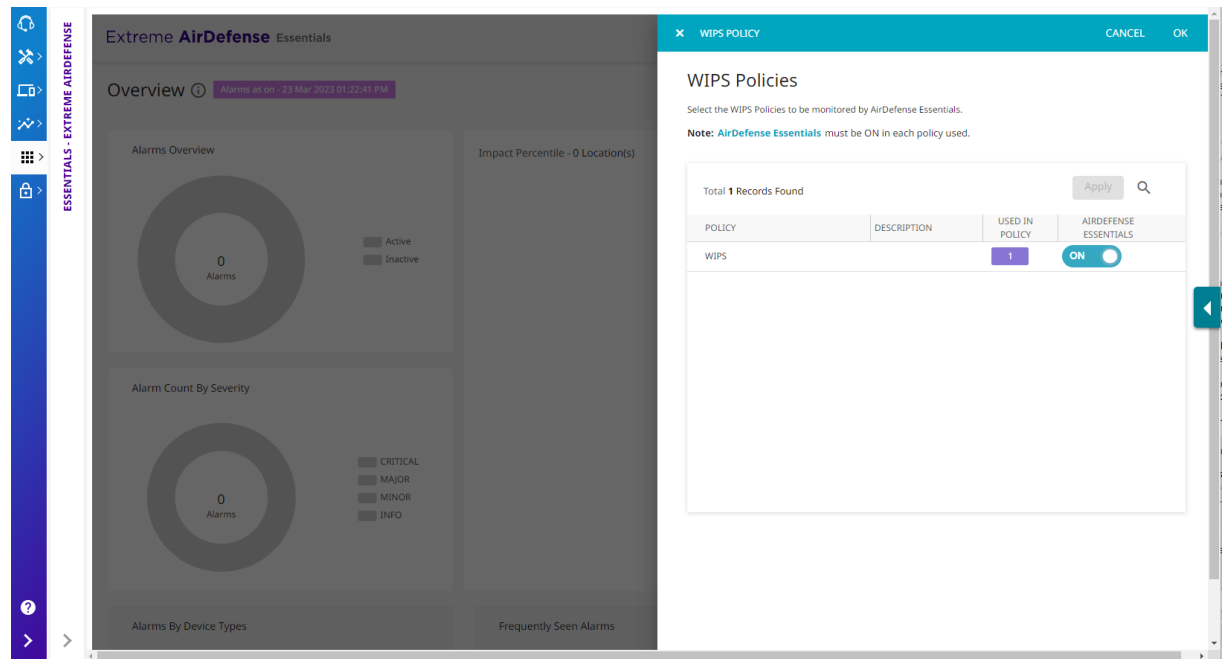
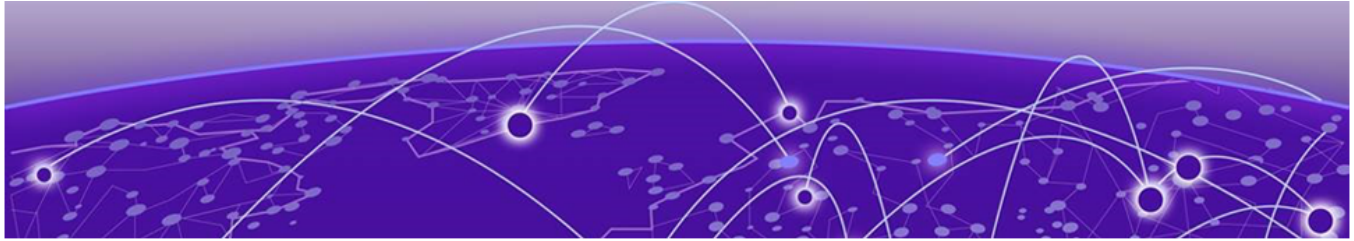


Figure 2: Extreme AirDefense Essentials WIPS Policies

2. Select the WIPS Policies that are used in Extreme AirDefense Essentials and select **Apply** then **Ok**.



Summary

- [Widget - Alarms Overview](#) on page 19
- [Widget - Alarm Count by Severity](#) on page 19
- [Impact Percentile Map](#) on page 20
- [Widget - Alarms By Device Types](#) on page 21
- [Widget - Frequently Seen Alarms](#) on page 22
- [Widget - Alarm Count By Location](#) on page 22
- [Widget - Alarms Distribution Per Category](#) on page 23

The Extreme AirDefense Essentials Summary displays various data and statistics for the locations managed in your network.

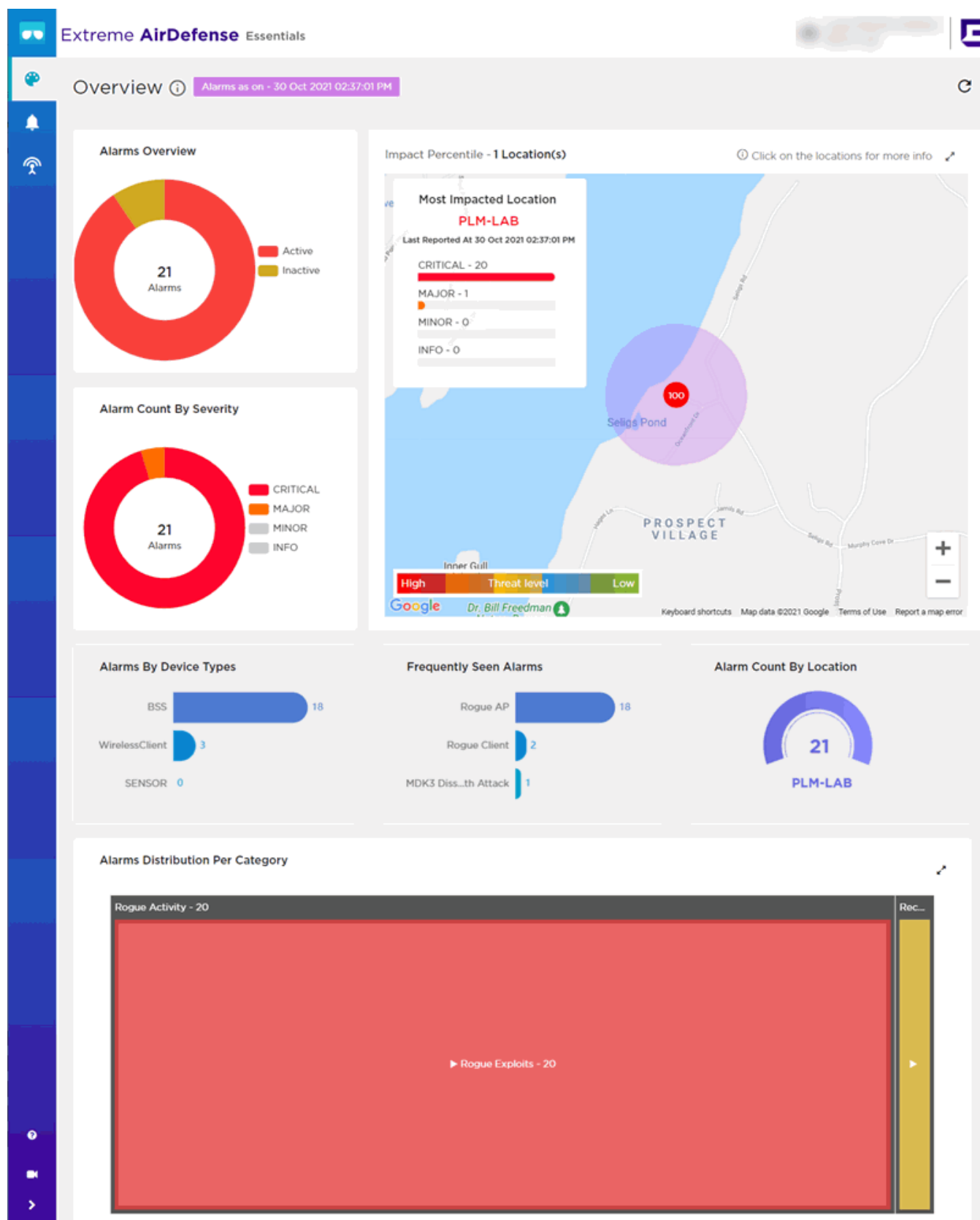


Figure 3: Summary Overview

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

**Note**

Summary widgets do not refresh automatically. You need to manually refresh the screen.

Widget - Alarms Overview

The Alarms Overview widget displays alarms activity for the alarms monitored in Extreme AirDefense Essentials.

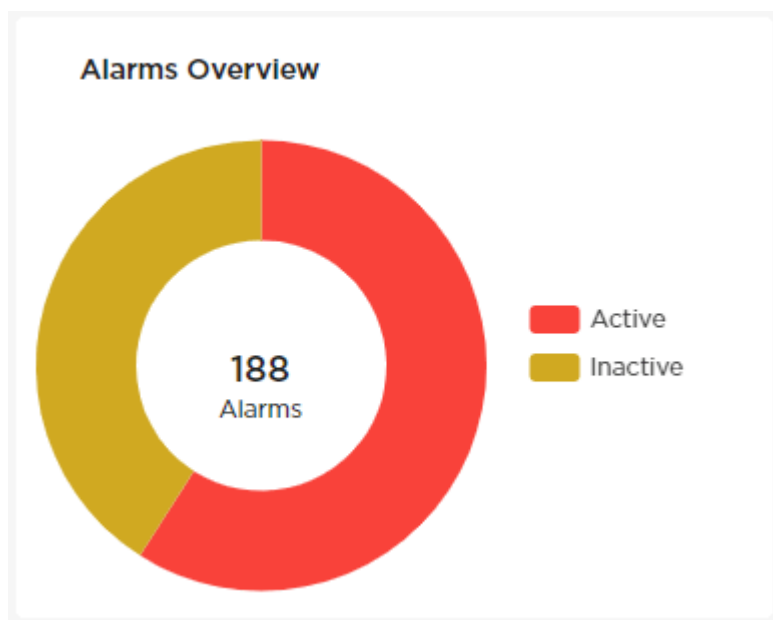


Figure 4: Alarms Overview Widget

The widget represents the total number of alarms detected in Extreme AirDefense Essentials. The colors identify the number of alarms that are currently active or inactive.

Place your cursor over a color to display the number of alarms in that category, and the percentage of the total alarms that the category represents.

Widget - Alarm Count by Severity

This widget displays the severity index for the alarms in Extreme AirDefense Essentials..

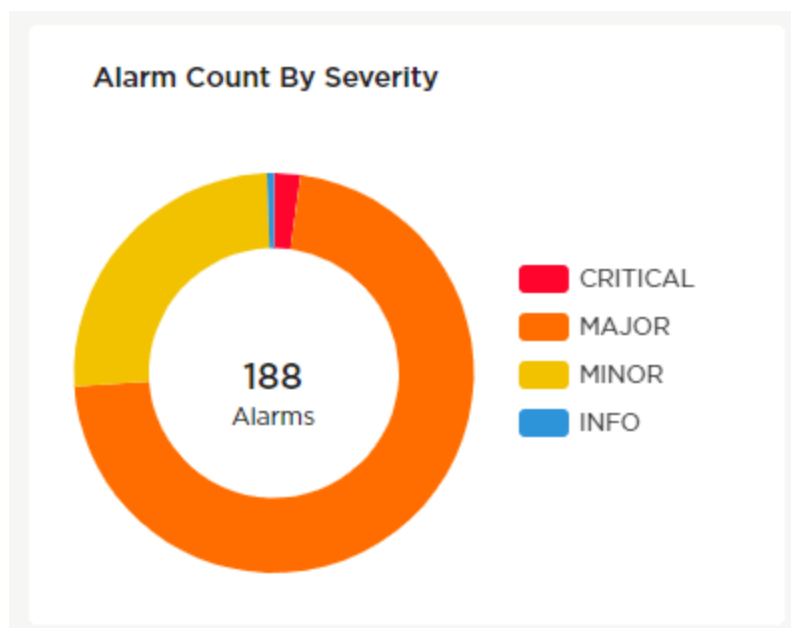


Figure 5: Alarm Count by Severity Widget

The widget represents the total number of alarms in Extreme AirDefense Essentials. The colors identify the severity of the alarms that are currently active.

Place your cursor over a color to display the number of alarms in that category, and the percentage of the total alarms that the category represents.

Impact Percentile Map

The Impact Percentile Map displays locations with alarm activity in your network as detected by Extreme AirDefense Essentials.

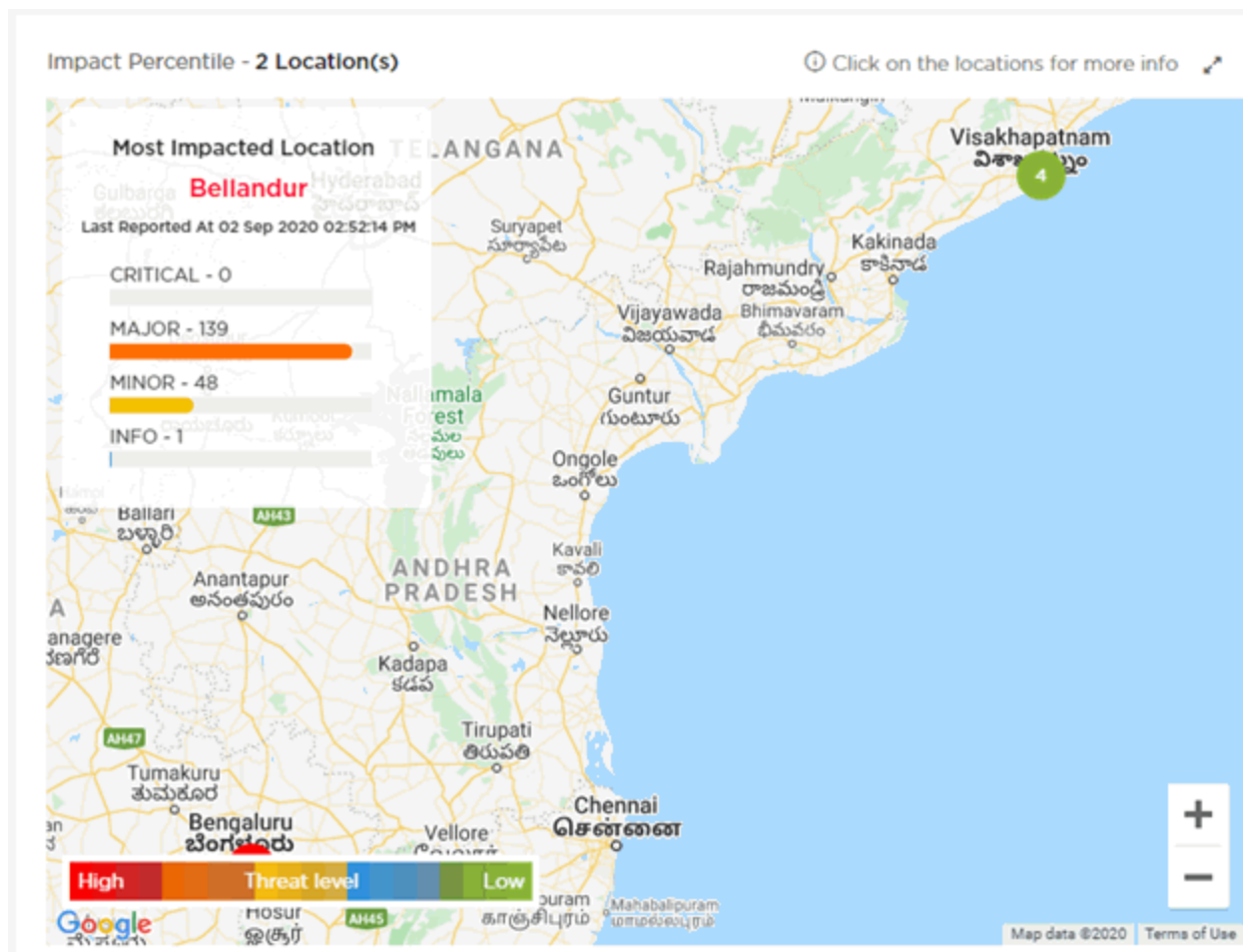


Figure 6: Impact Percentile Map

Select a location in the map to display details about the alarms at the site, including the threat score and percentile, the total number of alarms, and a break-down of the alarms by alarm severity: **Critical**, **Major**, **Minor**, and **Info**.

The map also includes an inset graphic that identifies the most impacted location in your network and the total number of alarms at that location categorized by severity: **Critical**, **Major**, **Minor**, and **Info**.

Use the zoom tools in the bottom right corner of the map to zoom in and out of the map view.

Widget - Alarms By Device Types

This widget displays the top alarms by device type.

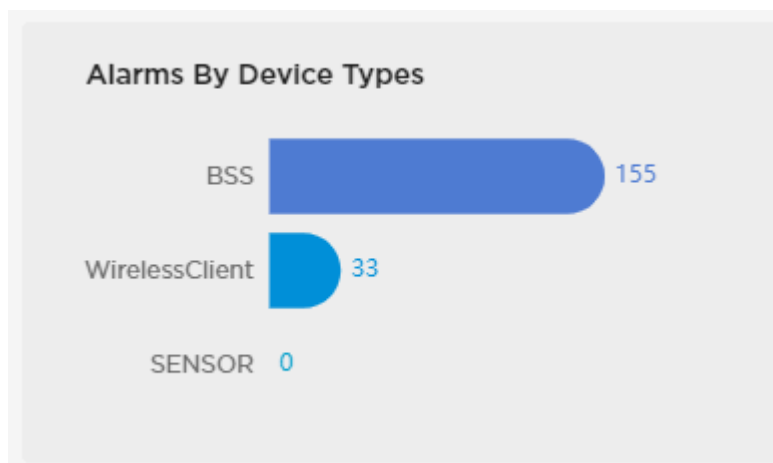


Figure 7: Alarms By Device Types Widget

Place your cursor over a device type in the widget to display more details about the alarms for that device type.

Widget - Frequently Seen Alarms

This widget displays the top five types of alarms seen most frequently by Extreme AirDefense Essentials.

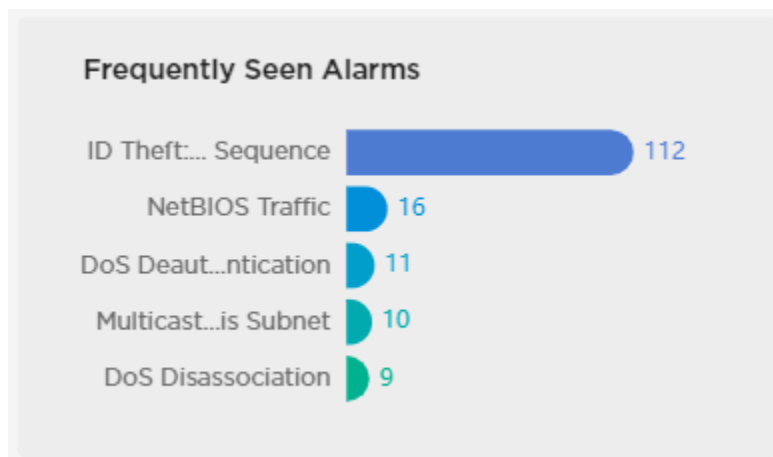


Figure 8: Frequently Seen Alarms Widget

To display more details about the detected alarms, place your cursor over an alarm type in the widget.

Widget - Alarm Count By Location

This widget displays the locations with the most alarms in Extreme AirDefense Essentials.

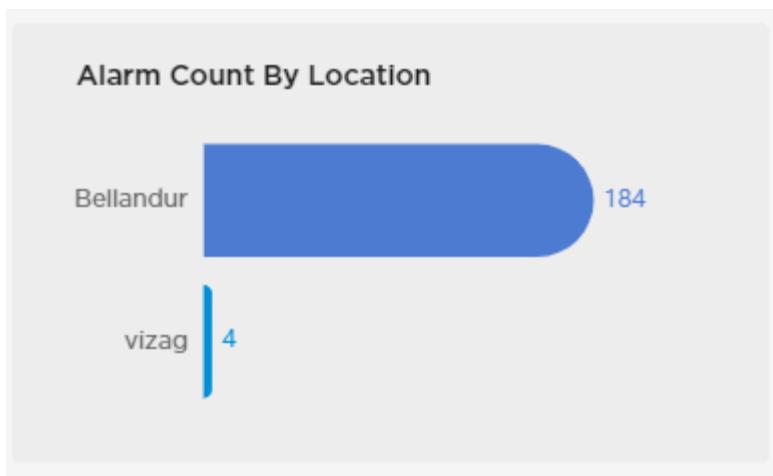


Figure 9: Alarm Count By Location

Place your cursor over location in the widget to display more details about the alarms at that location.

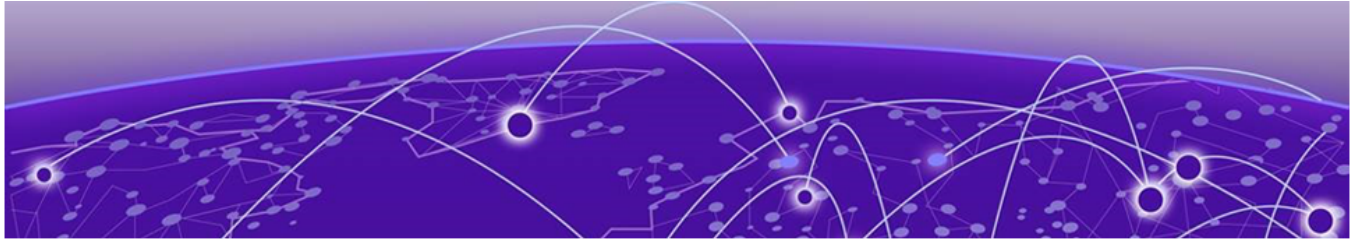
Widget - Alarms Distribution Per Category

This widget displays the alarm categories for alarms in Extreme AirDefense Essentials. The widget also includes the total number of alarms for each category.



Select a category to display more details about the alarms in that category and subcategory (if applicable).

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



Alarms

[Alarms Cycle](#) on page 25

[Alarm Details](#) on page 27

[Live Alarms View](#) on page 28

[Expired Alarms View](#) on page 32

[Rogue Device Detection](#) on page 36

Extreme AirDefense Essentials offers many types of alarms to help you monitor the network. You can view both live and expired alarms. View alarm counts in any of the following ways:

- Location
- Severity
- Category
- Frequently Seen Alarms
- Total Alarm Count

In the **Alarms** window, select the **Information** icon beside the Alarms heading to view a diagram of the Alarm Cycle.

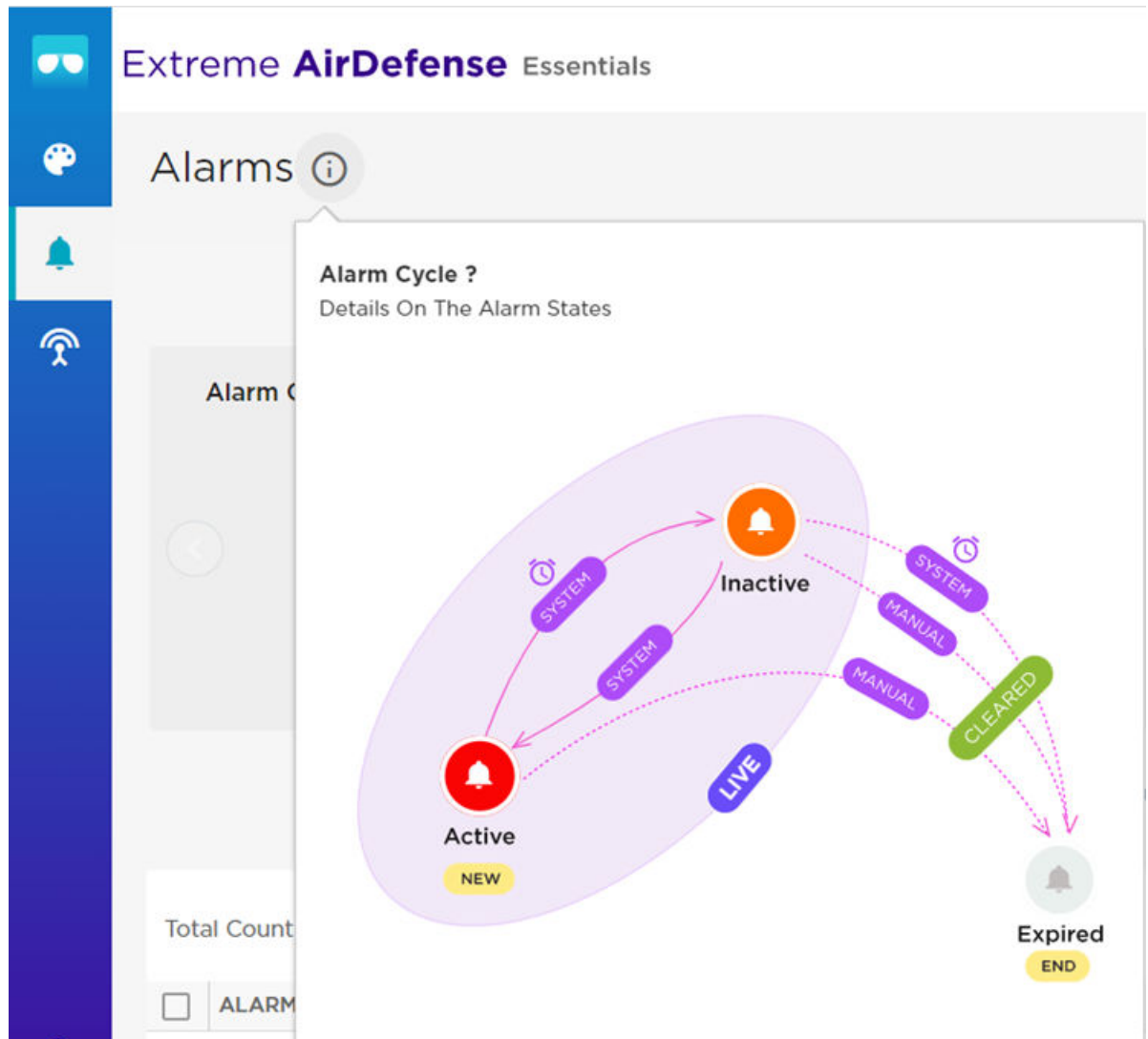


Figure 10: Alarms Life Cycle diagram

Related Links

- [Alarms Cycle](#) on page 25
- [Alarm Details](#) on page 27
- [Live Alarms View](#) on page 28
- [Expired Alarms View](#) on page 32

Alarms Cycle

Extreme AirDefense Essentials tracks alarms detected as an alarm cycle, documenting details at the various alarm states. The following graphic depicts the typical alarm cycle:

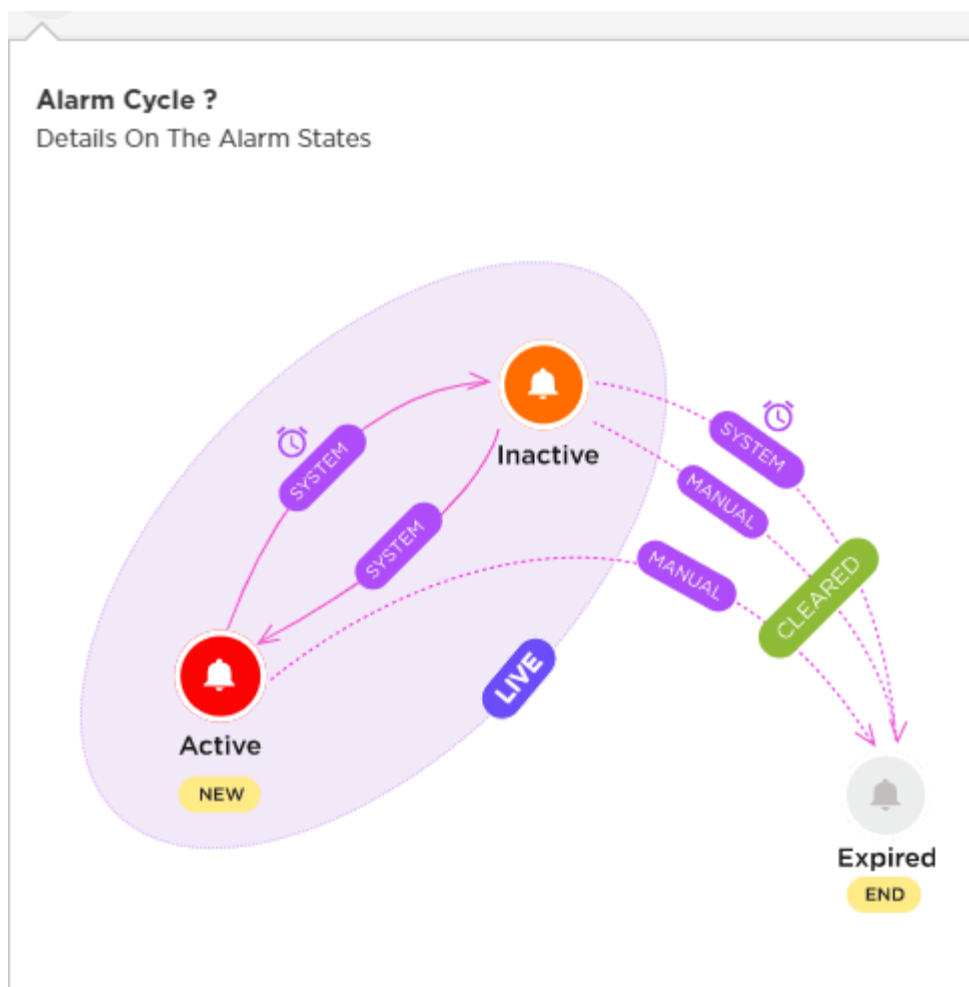


Figure 11: Alarm Cycle

Active

An alarm is in the Active state at the start of the alarm cycle. When a threat is detected, an alarm is created and Extreme AirDefense Essentials begins monitoring the activity. An alarm will be considered active until the issue is resolved and the threat or event has been cleared. This activity is displayed in Extreme AirDefense Essentials on the [Live Alarms View](#).

Inactive

An alarm is considered Inactive if it is no longer active, but has not yet been cleared. This activity is displayed in Extreme AirDefense Essentials on the [Live Alarms View](#).

Cleared

When the issue is resolved and the threat has been resolved, the alarm is considered cleared.

Expired

An alarm is considered expired after it has been cleared. This is the end of the Alarm Cycle. This activity is displayed in Extreme AirDefense Essentials as Expired Activity on the **Alarms** page.

Alarm Details

The **Alarm Details** window provides additional data to analyze the selected alarm.

To open the **Alarm Details** window, select an alarm in the Alarms table.

The screenshot displays the 'ALARM DETAILS' window. The top bar is blue with a close button (X), the title 'ALARM DETAILS', and navigation buttons (back, forward, OK). The main content area is divided into two sections. The top section, titled 'Alarm Name', shows 'Rogue AP' with a red 'ACTIVE' status. Below this, it lists 'Raised On 01 Oct 2021 08:43:46 AM', 'Location - xiqextremeqapps+Preeti-g8r2-rogu>>argentina>>argentinaa>>floor2-arg', 'Raised Against BSS - 548D5A693D18', 'Reported By SENSOR - BCF3102A99C0', 'Category -Rogue Activity', and 'Subcategory -Rogue Exploits'. To the right, under 'ALARM ACTIONS', are four icons: 'Clear Alarm' (orange bell with X), 'Expert Help' (blue document), 'Rogue Terminate' (red circle with slash), and 'Rogue Locate' (blue location pin). The bottom section, titled 'Alarm State And Time', shows a timeline of the alarm's state: 'Active' (red bell icon, 01 Oct 2021 08:43:46 AM) transitions to 'Inactive' (grey bell icon) via a 'Cleared' action, which then transitions to 'Expired' (grey bell icon with slash) via another 'Cleared' action.

ALARM DETAILS

Alarm Name

Rogue AP **ACTIVE**

Raised On 01 Oct 2021 08:43:46 AM

Location - xiqextremeqapps+Preeti-g8r2-rogu>>argentina>>argentinaa>>floor2-arg

Raised Against BSS - 548D5A693D18

Reported By SENSOR - BCF3102A99C0

Category -Rogue Activity

Subcategory -Rogue Exploits

ALARM ACTIONS

Clear Alarm Expert Help

Rogue Terminate Rogue Locate

Alarm State And Time

Active 01 Oct 2021 08:43:46 AM

Inactive

Expired

Cleared

Cleared

Figure 12: Alarms Details Window

The following actions are available in the **Alarm Details** window:

	Field	Description
	Alarm Details	View several details regarding the selected alarm, including: • Alarm type, severity, and status • Location of the device • Type of device against the alarm was raised • Sensor that reported the alarm • Alarm category • Alarm subcategory
	Rogue Terminate	Manually terminate alarms for rogue APs and rogue clients. Extreme AirDefense Essentials consolidates all termination requests triggered in the last 10 minutes. Extreme AirDefense Essentials maintains the list of MAC addresses until the next reboot. The list of MAC addresses is overwritten with each subsequent rogue termination request.
	Rogue Locate	Locate the rogue AP that is detected by Extreme AirDefense Essentials on a floor map within ExtremeLocation™ Essentials. For more information, see Rogue Device Detection on page 36.
	Expert Help	Select the Expert Help icon to display additional industry information about the alarm type.
	Alarm State and Time	View the time duration and activity states over the life cycle of the selected alarm.

To close the window and return to the **Alarms** table, select **OK**.

Related Links

[Locate Rogue Devices](#) on page 37

[Terminate Rogue Devices](#) on page 38

Live Alarms View

View alarm data from the **Live Alarms View**. Review data about alarms that have not yet been cleared in your network.

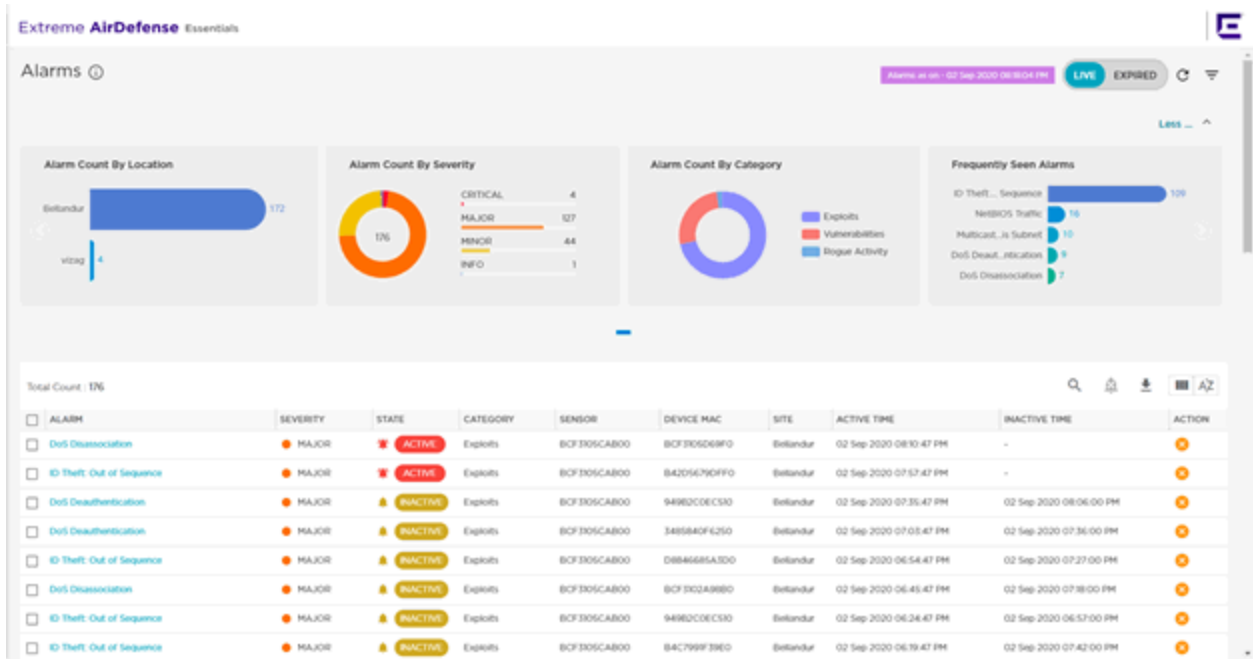


Figure 13: Live Alarms View

Select the **Live** icon to display data about alarms that have not been cleared.

Filter the alarms to more easily find an alarm. To display filter options, select the **Filter** icon.

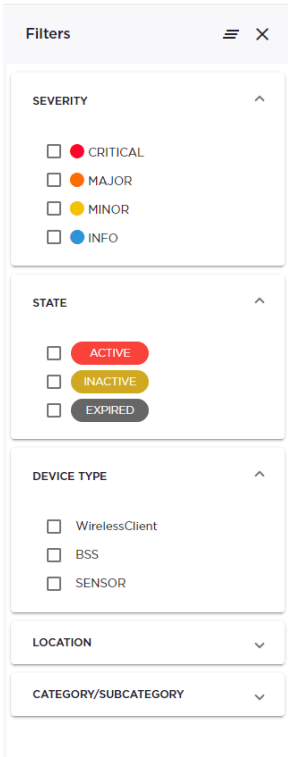


Figure 14: Filter View

Sort alarms by **Severity**, **Alarm State**, **Device Type**, **Location**, and **Category / Subcategory**.



Note

When sites or locations are deleted from the Network Plan in ExtremeCloud IQ, the live alarms that are associated with the site or location are also deleted.

The **Alarms View - Live** is divided into the following panes:

- [Live Alarms Widgets](#) on page 30
- [Live Alarms Raised Table](#) on page 31

Live Alarms Widgets

Extreme AirDefense Essentials offers graphical widget reports that provide comprehensive insight into the alarms generated on your network.

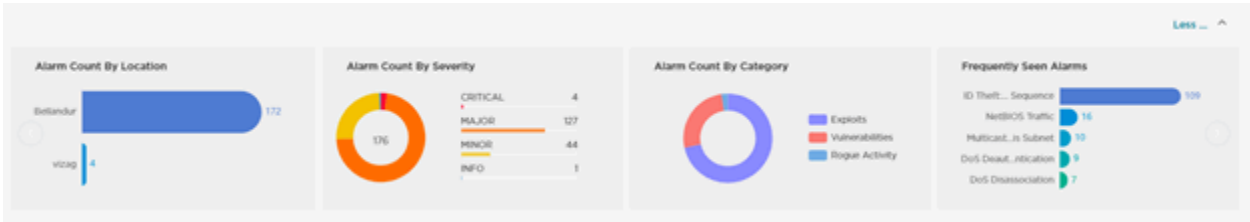


Figure 15: Live Alarms Widgets

The following widgets display live data:

- **Alarm Count By Location** - The locations with the most active and inactive alarms in Extreme AirDefense Essentials
- **Alarm Count By Severity** - The severity index for active and inactive alarms in Extreme AirDefense Essentials
- **Alarm Count By Category** - The types of alarm categories for the active and inactive alarms in Extreme AirDefense Essentials. This widget also includes the total number of active and inactive alarms for each category.
- **Frequently Seen Alarms** - The five types of active and inactive alarms seen most frequently by Extreme AirDefense Essentials

Select the arrow at the top right of the pane to collapse or expand the pane.

Live Alarms Raised Table

The **Live Alarms Raised** table displays details about the active and inactive alarms raised. For definitions of alarm status, see [Alarms Cycle](#) on page 25.

Total Count : 126

ALARM	SEVERITY	STATE	CATEGORY	SENSOR	DEVICE MAC	SITE	ACTIVE TIME	INACTIVE TIME	ACTION
☐ DoS Disassociation	MAJOR	ACTIVE	Exploits	BCF3305CAB00	BCF3305D69F0	Bellandur	02 Sep 2020 08:30:47 PM	-	
☐ ID Theft: Out of Sequence	MAJOR	ACTIVE	Exploits	BCF3305CAB00	842D56790FF0	Bellandur	02 Sep 2020 07:57:47 PM	-	
☐ DoS Deauthentication	MAJOR	INACTIVE	Exploits	BCF3305CAB00	94982C0EC30	Bellandur	02 Sep 2020 07:35:47 PM	02 Sep 2020 08:06:00 PM	
☐ DoS Deauthentication	MAJOR	INACTIVE	Exploits	BCF3305CAB00	3485840F6250	Bellandur	02 Sep 2020 07:03:47 PM	02 Sep 2020 07:36:00 PM	
☐ ID Theft: Out of Sequence	MAJOR	INACTIVE	Exploits	BCF3305CAB00	D8846685A3D0	Bellandur	02 Sep 2020 06:54:47 PM	02 Sep 2020 07:27:00 PM	
☐ DoS Disassociation	MAJOR	INACTIVE	Exploits	BCF3305CAB00	BCF3302A98B0	Bellandur	02 Sep 2020 06:45:47 PM	02 Sep 2020 07:36:00 PM	
☐ ID Theft: Out of Sequence	MAJOR	INACTIVE	Exploits	BCF3305CAB00	94982C0EC30	Bellandur	02 Sep 2020 06:24:47 PM	02 Sep 2020 06:57:00 PM	
☐ ID Theft: Out of Sequence	MAJOR	INACTIVE	Exploits	BCF3305CAB00	84C799F39E0	Bellandur	02 Sep 2020 06:19:47 PM	02 Sep 2020 07:42:00 PM	
☐ ID Theft: Out of Sequence	MAJOR	INACTIVE	Exploits	BCF3305CAB00	168B0DF8A58	Bellandur	02 Sep 2020 05:53:47 PM	02 Sep 2020 06:24:00 PM	
☐ ID Theft: Out of Sequence	MAJOR	INACTIVE	Exploits	BCF3305CAB00	D884667F73D0	Bellandur	02 Sep 2020 05:31:47 PM	02 Sep 2020 06:27:00 PM	
☐ ID Theft: Out of Sequence	MAJOR	INACTIVE	Exploits	BCF3305CAB00	842D5673CB02	Bellandur	02 Sep 2020 05:11:47 PM	02 Sep 2020 05:42:00 PM	

Figure 16: Live Alarms Raised Table

Use the tools at the top of the **Alarms Raised** pane to perform several functions using the data in the table:



- Select the Search tool to search for specific data in the table.
- Select the Download tool to export the table into a .csv report. You can choose to download all rows or selected rows in the table.
- Select the Columns tool to add additional columns to the table. The following columns can be added to the table: **Subcategory**, **Device Type**, and **Floor**.
- Select the Sort tool to sort the data alphabetically (ascending or descending).

The following columns are included in the **Alarms Raised** table:

Column	Description
Alarm	The type of alarm that is raised. Select an alarm type in this column to display the Alarms Details right-panel for additional details about the selected alarm.
Alarm Severity	The severity of the alarm.
State	The status of the alarm.
Category	The category of the alarm.
Sensor	The sensor for which the alarm was raised.
Device MAC	The MAC address for the device for which the alarm was raised.
Site	The site where device for which the alarm was raised is located.
Active Time	The time the alarm first became active.
Inactive Time	The time the alarm first became inactive.
Actions	Select the icon to clear the alarm.

Select an alarm in the **Live Alarms Raised** table to open the **Alarm Details** window and display additional detailed information about the Live alarms in your network.

Related Links

[Alarm Details](#) on page 27

[Alarms Cycle](#) on page 25

Expired Alarms View

View alarm data from the **Expired Alarms View**. Review data about alarms that have been cleared in your network.

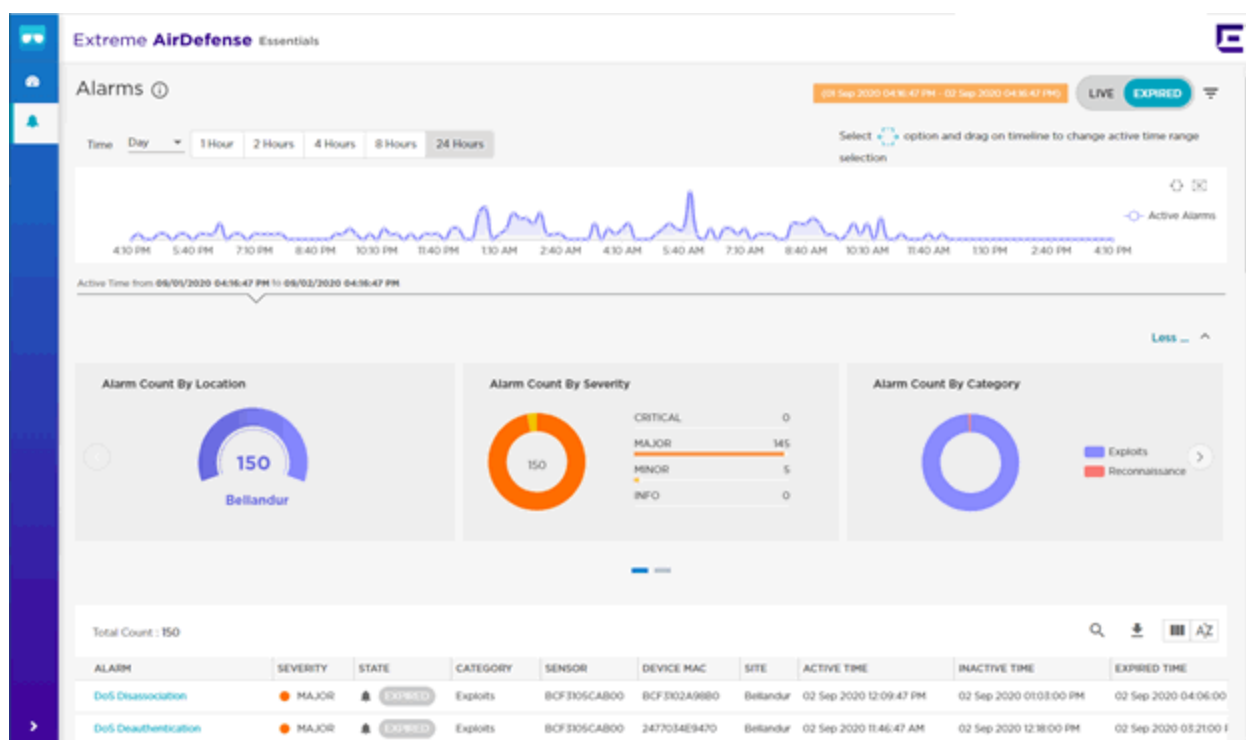


Figure 17: Expired Alarms View

Select the **Expired** icon to display data about alarms that have been cleared.

Filter the alarms to more easily find an alarm. To display filter options, select the **Filter** icon.

The Filter View interface is a sidebar on the left side of the screen. It has a title 'Filters' with a menu icon and a close 'X' button. Below the title, there are five filter sections, each with a title and a list of options:

- SEVERITY**: Includes checkboxes for CRITICAL (red dot), MAJOR (orange dot), MINOR (yellow dot), and INFO (blue dot).
- STATE**: Includes checkboxes for ACTIVE (red pill), INACTIVE (yellow pill), and EXPIRED (grey pill).
- DEVICE TYPE**: Includes checkboxes for WirelessClient, BSS, and SENSOR.
- LOCATION**: A dropdown menu.
- CATEGORY/SUBCATEGORY**: A dropdown menu.

Figure 18: Filter View

Sort alarms by **Severity**, **Alarm State**, **Device Type**, **Location**, and **Category / Subcategory**.

The **Alarms View - Expired** is divided into the following panes:

- [Expired Alarms Activity Line Graph](#) on page 34
- [Expired Alarms Widgets](#) on page 35
- [Expired Alarms Raised Table](#) on page 35

Expired Alarms Activity Line Graph

The **Activity Line Graph** of the [Expired Alarms View](#) displays activity details during the time duration you specify.



Figure 19: Expired Alarms Activity Line Graph

Expand the **Day** drop-down list to select the date for which the time duration displays. Select the time duration (**1 Hour**, **2 Hours**, **4 Hours**, **8 Hours**, **24 Hours**) for which you want to display alarm activity.

Select the  button and drag on the timeline to define a range of time for which you want to display the alarm activity.

Expired Alarms Widgets

The **Alarms Widgets** pane of the **Expired Alarms View** displays widgets that provide comprehensive insight into the alarms generated on your network.

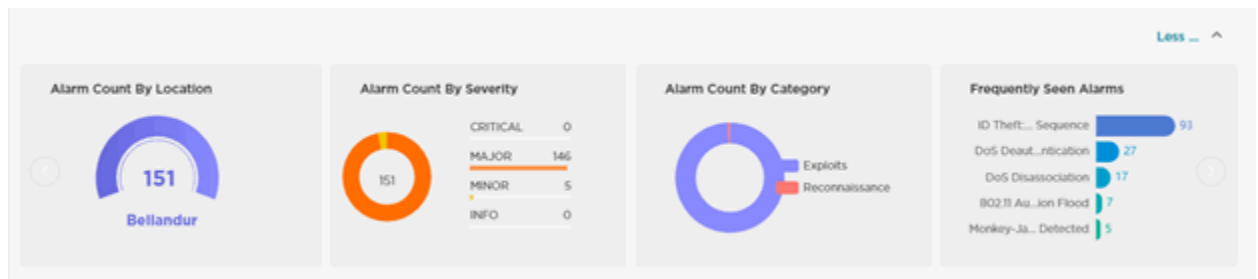


Figure 20: Expired Alarms Widgets

These widgets are:

- **Alarm Count By Location** - The locations with the most active alarms in Extreme AirDefense Essentials.
- **Alarm Count By Severity** - The severity index for active alarms in Extreme AirDefense Essentials.
- **Alarm Count By Category** - The types of alarm categories for the active alarms in Extreme AirDefense Essentials. The widget also includes the total number of alarms for each category.
- **Frequently Seen Alarms** - The five types of active alarms seen most frequently by Extreme AirDefense Essentials.

To collapse or expand the pane, select the arrow at the top right of the pane.

Expired Alarms Raised Table

The Expired Alarms Raised table in the **Expired Alarms Raised View** displays details about the alarms raised that have been cleared.

Total Count : 151									
ALARM	SEVERITY	STATE	CATEGORY	SENSOR	DEVICE MAC	SITE	ACTIVE TIME	INACTIVE TIME	EXPIRED TIME
ID Theft: Out of Sequence	MAJOR	EXPIRED	Exploits	BCF3105CAB00	D88466C2E750	Bellandur	02 Sep 2020 03:04:47 PM	02 Sep 2020 03:36:00 PM	02 Sep 2020 07:39:00 PM
DoS Deauthentication	MAJOR	EXPIRED	Exploits	BCF3105CAB00	380025295815	Bellandur	02 Sep 2020 02:40:46 PM	02 Sep 2020 03:12:00 PM	02 Sep 2020 06:15:00 PM
DoS Deauthentication	MAJOR	EXPIRED	Exploits	BCF3105CAB00	949B2C0EC510	Bellandur	02 Sep 2020 02:22:47 PM	02 Sep 2020 03:24:00 PM	02 Sep 2020 06:27:00 PM
DoS Deauthentication	MAJOR	EXPIRED	Exploits	BCF3105CAB00	4C49E371FE43	Bellandur	02 Sep 2020 02:22:47 PM	02 Sep 2020 02:54:00 PM	02 Sep 2020 05:57:00 PM
DoS Deauthentication	MAJOR	EXPIRED	Exploits	BCF3105CAB00	3485841594A0	Bellandur	02 Sep 2020 01:41:47 PM	02 Sep 2020 02:12:00 PM	02 Sep 2020 05:15:00 PM
DoS Disassociation	MAJOR	EXPIRED	Exploits	BCF3105CAB00	BCF3105D7AF0	Bellandur	02 Sep 2020 01:39:47 PM	02 Sep 2020 02:12:00 PM	02 Sep 2020 05:15:00 PM
DoS Disassociation	MAJOR	EXPIRED	Exploits	BCF3105CAB00	BCF3107062F0	Bellandur	02 Sep 2020 01:39:47 PM	02 Sep 2020 02:12:00 PM	02 Sep 2020 05:15:00 PM
ID Theft: Out of Sequence	MAJOR	EXPIRED	Exploits	BCF3105CAB00	7467F77C0430	Bellandur	02 Sep 2020 01:12:47 PM	02 Sep 2020 01:45:00 PM	02 Sep 2020 05:48:00 PM
802.11 Authentication Flood	MAJOR	EXPIRED	Exploits	BCF3105CAB00	2477034EAC6C	Bellandur	02 Sep 2020 12:38:47 PM	02 Sep 2020 01:15:00 PM	02 Sep 2020 04:18:00 PM
ID Theft: Out of Sequence	MAJOR	EXPIRED	Exploits	BCF3105CAB00	184B0DB1BA58	Bellandur	02 Sep 2020 12:37:47 PM	02 Sep 2020 01:09:00 PM	02 Sep 2020 05:12:00 PM

Figure 21: Expired Alarms Raised Table

Use the tools at the top of the **Alarms Raised** pane to perform several functions using the data in the table:



- Select the Search tool to search for specific data in the table.
- Select the Download tool to export the table into a .csv report. You can choose to download all rows or selected rows in the table.
- Select the Columns tool to add additional columns to the table. The following columns can be added to the table: **Subcategory**, **Device Type**, and **Floor**.
- Select the Sort tool to sort the data alphabetically (ascending or descending).

The following columns are included in the **Alarms Raised** table:

Column	Description
Alarm	The type of alarm that is raised. Select an alarm type in this column to display the Alarms Details right-panel for additional details about the selected alarm.
Alarm Severity	The severity of the alarm: Active or Cleared .
State	The state of the alarm: Expired .
Category	The category of the alarm.
Sensor	The sensor for which the alarm was raised.
Device MAC	The MAC address for the device for which the alarm was raised.
Site	The site where the device alarm raised is located.
Time Raised	The time that the alarm was first raised.
Time Cleared	The time that the alarm was cleared, if appropriate.
Cleared By	The name of the user that cleared the alarm.
Actions	Select the Actions drop-down list to display several Action functions.

Rogue Device Detection

A rogue AP is defined as an unsanctioned BSS (Basic Service Set) that is attached to your sanctioned wired infrastructure. The Rogue AP alarms and the alarms of their associated rogue clients are listed in the Alarms table.

You can locate rogue APs and their clients on a floor map, and you can terminate the rogue AP.



Note

Before locating a rogue AP or client, you must enable ExtremeLocation Essentials and configure a floor map for each location.

To determine wireless rogue devices, Extreme AirDefense Essentials considers the MAC address of a wired AP and calculates the BSS MAC address range for that wired AP. If the BSS of another AP is within the range of that calculation — between the wired

MAC address and the calculated BSS — that intruding AP is considered rogue. Clients associated with the rogue AP are considered rogue clients.

Related Links

[Locate Rogue Devices](#) on page 37

[Terminate Rogue Devices](#) on page 38

Locate Rogue Devices

Before locating a rogue AP or client, you must enable ExtremeLocation Essentials and configure a floor map for each location.

Take the following steps to locate a rogue device on an ExtremeLocation Essentials floor map:

1. From Extreme AirDefense Essentials, select  to display the **Alarms** page.
2. From the Alarms table, select a **Rogue AP** or **Rogue Client** alarm from the list.

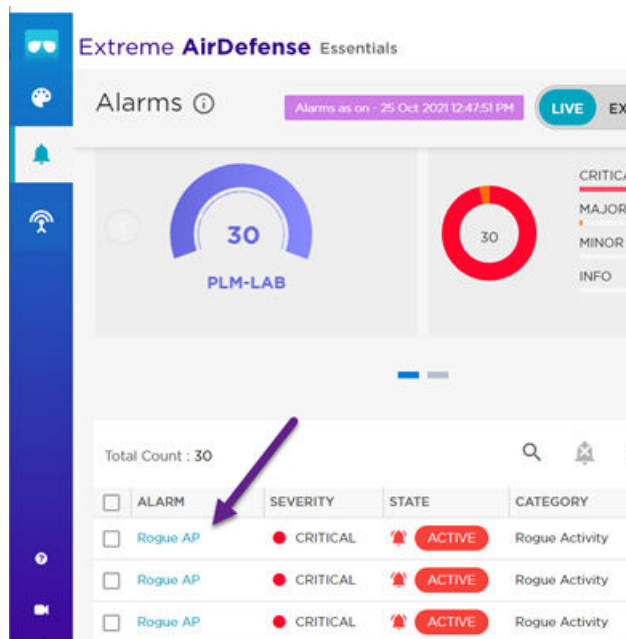


Figure 22: Rogue AP in Alarms List

The **Alarm Details** dialog displays.

3. Select  to Locate the rogue device.
ExtremeLocation Essentials opens to the floor map and displays the rogue device.

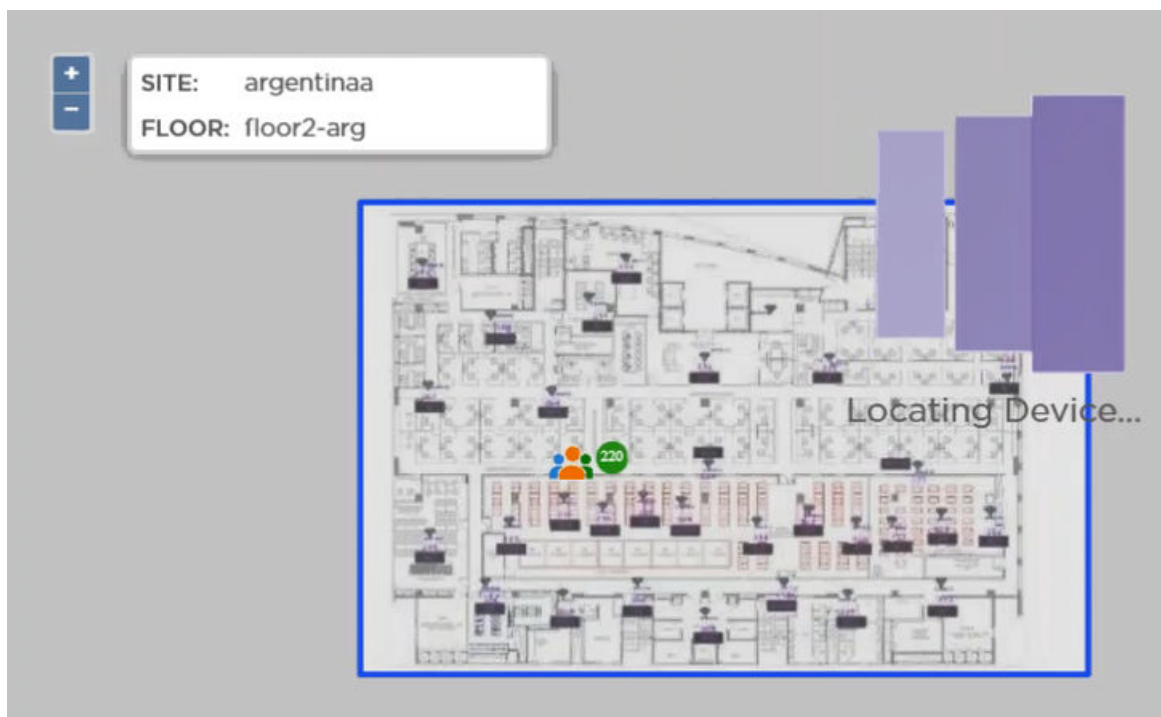


Figure 23: Locating Rogue Device in ExtremeLocation Essentials



Note

Devices that were visible within the last minute display on the floor map. If the device does not display, select the **Historical** view.

Related Links

[Rogue Device Detection](#) on page 36

Terminate Rogue Devices

Take the following steps to terminate a rogue device:

1. From Extreme AirDefense Essentials, select  to display the **Alarms** page.

- From the Alarms table, select a **Rogue AP** or **Rogue Client** alarm from the list.

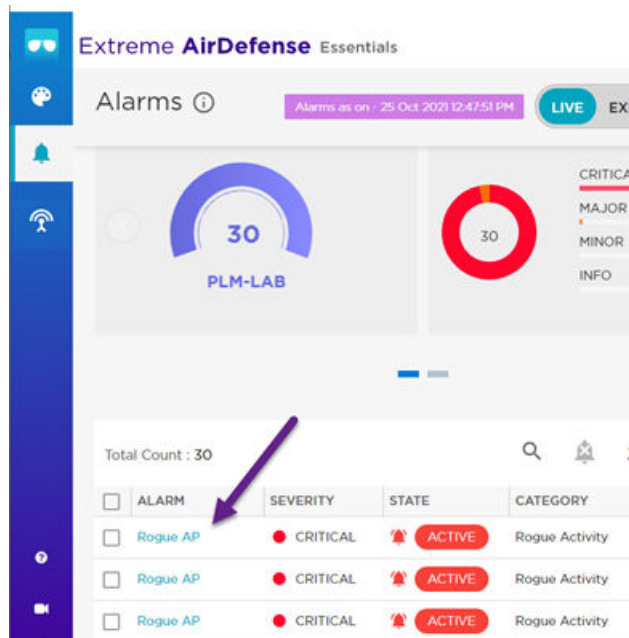


Figure 24: Rogue AP in Alarms List

The **Alarm Details** dialog displays.

- Select  to terminate the rogue device.
Extreme AirDefense Essentials prompts you to confirm that you want to terminate the rogue device. Select **Yes**.

Manual Rogue Classification

Take the following steps to manually classify rogue devices in the alarms list, and then clear the selected alarms:

- From Extreme AirDefense Essentials, select  to display the **Alarms** page.
- From the Alarms table, select the checkboxes for the **Rogue AP** or **Rogue Client** devices you want to manually classify.
- Select  to classify the selected device alarms.

- From the **Add Classified Device** confirmation prompt, select **Yes, Sanction** to classify the selected devices.

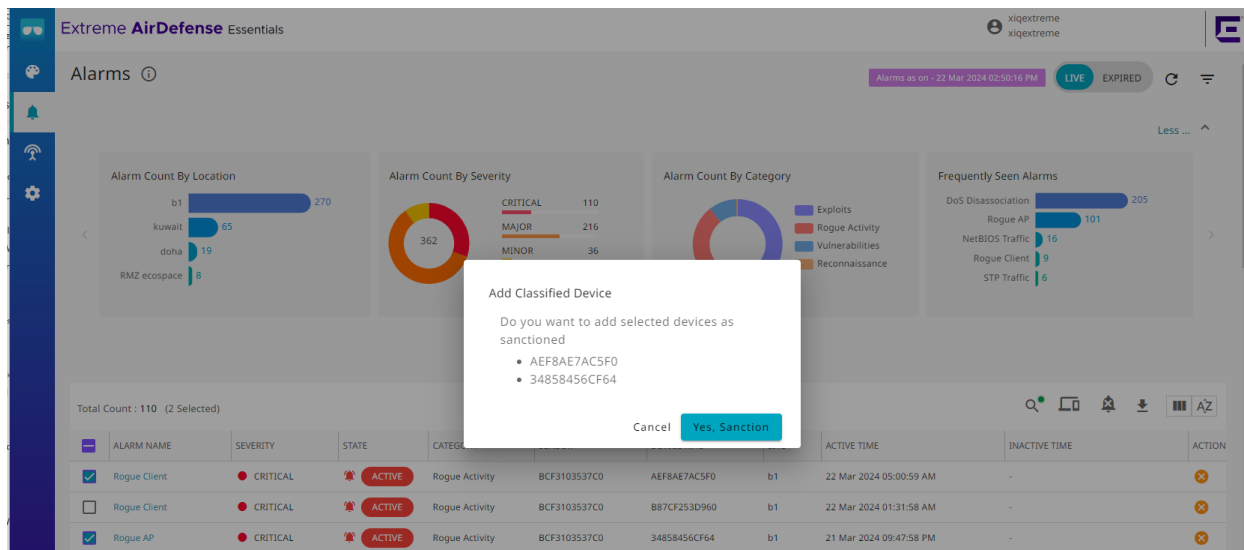


Figure 25: Manually Classify Rogue Devices Confirmation Prompt

- Select  to clear the selected device alarms from the alarms list.

The manually sanctioned devices no longer appear as rogue devices on the network.

Related Links

[Classified Devices Management Settings](#) on page 49

[Rogue Device Detection](#) on page 36

NEW! Sync Rogue Sanctioned Alarm

After a rogue alarm is generated, the rogue device is added to a sanctioned list and the alarm state for that sanctioned rogue device remains active without updates. The **Sync Rogue Sanctioned Alarm** button changes all sanctioned device rogue alarm states to inactive. Take the following steps to sync multiple sanctioned device rogue alarms in the Alarms Raised table, changing the alarm state to inactive:

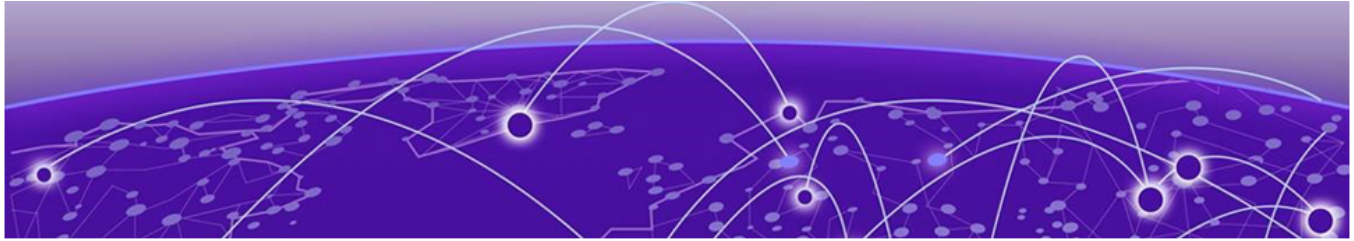
- From Extreme AirDefense Essentials, select  to display the **Alarms** page.
- Verify you have **Rogue AP** or **Rogue Client** devices with active alarms in the **Alarms Raised** table.
- Select  to sync all sanctioned device rogue alarms and change the alarm state to INACTIVE.

The **Alarms Raised** table refreshes, and any sanctioned device rogue alarms change state from ACTIVE to INACTIVE.

Related Links

[Classified Devices Management Settings](#) on page 49

[Rogue Device Detection](#) on page 36



Viewing Data by Sensor

The Extreme AirDefense Essentials **Sensors** view provides network insight from the perspective of each AP radio sensor. Filter sensors by model type, impact level, or location. The following data is available for each sensor on the **Sensors** view:

- Information that identifies the sensor
- Sensor connectivity status
- Alarm activity per sensor

1. From Extreme AirDefense Essentials, select  to display the **Sensors** screen.

The following information is available for each sensor:

- Connectivity status
- Host Name
- AP MAC address
- AP Serial Number
- AP Model Number
- Location
- Number of alarms
- Date and time the sensor was last seen

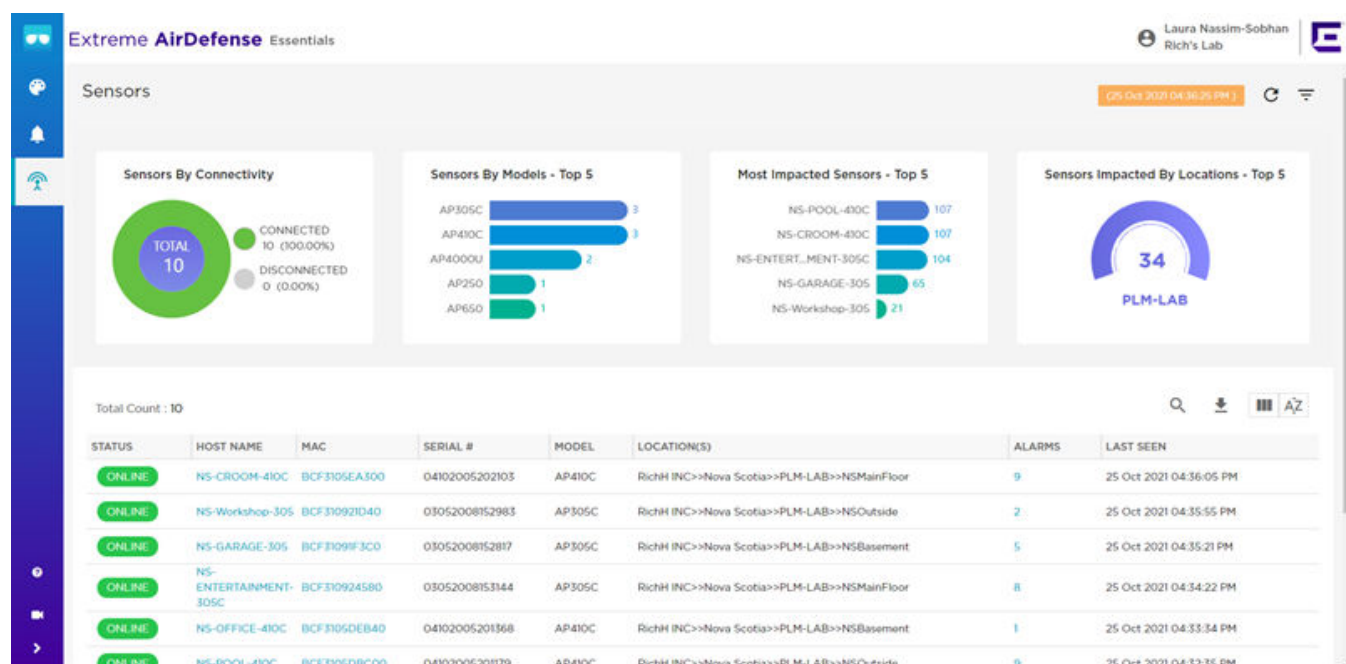


Figure 26: Sensors View

- To display additional sensor details, select a sensor from the **Sensors** view.
The **Sensors Details** window displays. The alarms associated with the sensor are organized by alarm severity.

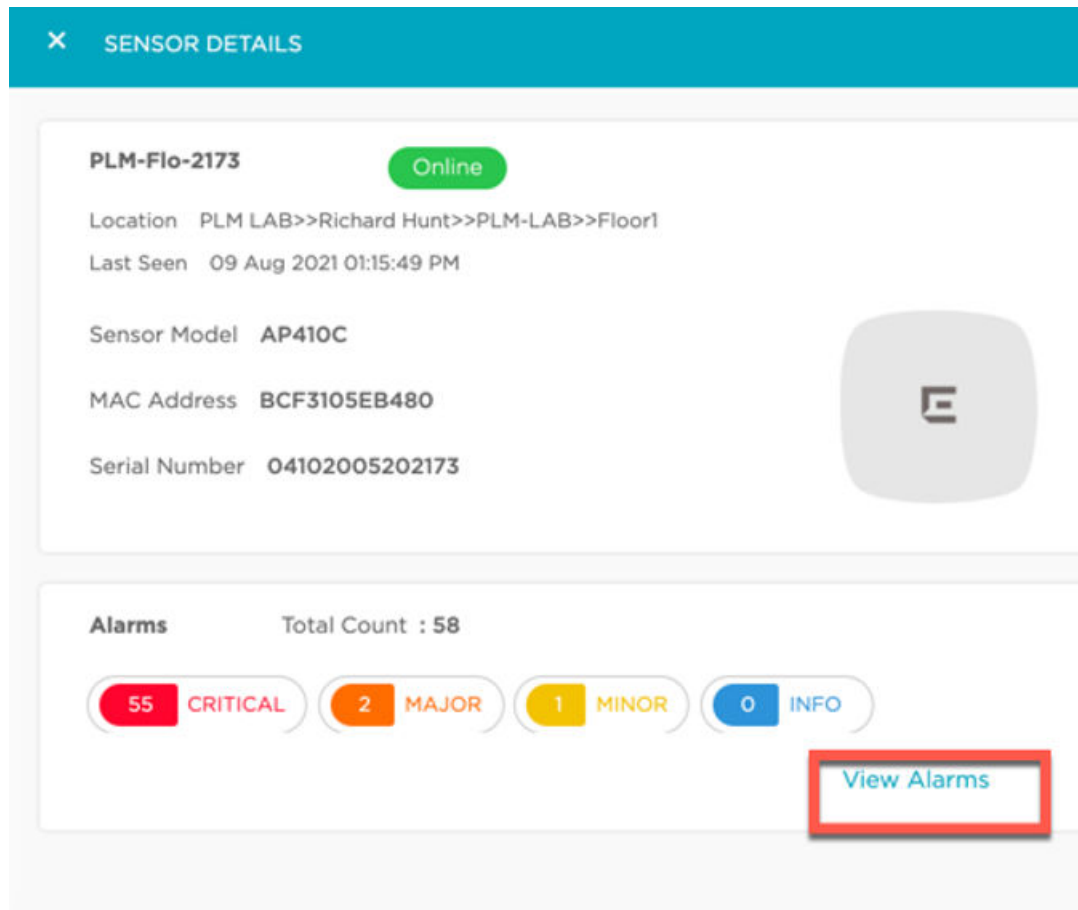


Figure 27: Sensor Details Window

3. To view alarms associated with the selected sensor, select **View Alarms**.
The **Alarms** view displays with the filter set to the selected sensor.

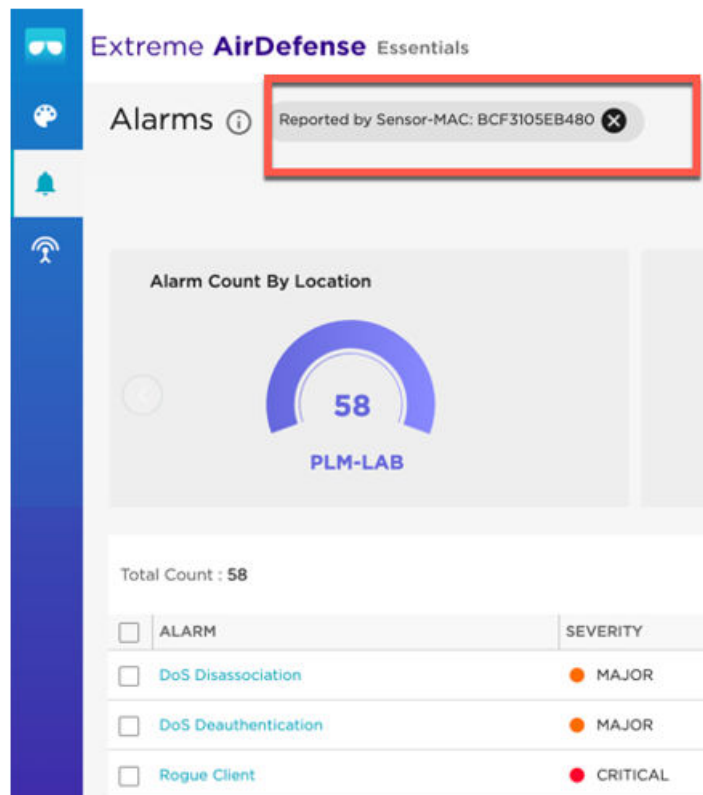
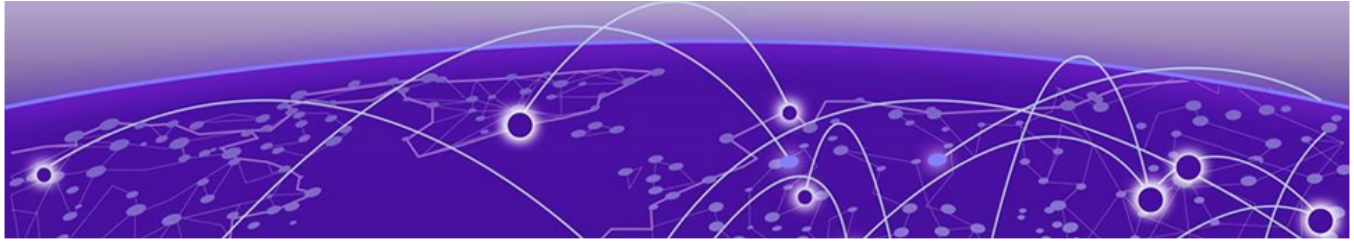


Figure 28: Alarms per Sensor



Alarm Management Settings

[Alarm Notifications Webhook Configurations](#) on page 47

[Classified Devices Management Settings](#) on page 49

The Extreme AirDefense Essentials **Settings** view provides you with Alarm Management settings to enable or disable a group of alarms, or individual alarms. The following alarm groups are available to manage from the **Settings** view:

- Exploits
- Reconnaissance
- Rogue Activity
- Vulnerabilities

1. From Extreme AirDefense Essentials, select  to display the **Settings** screen.

- To display individual alarm settings within a group, select an alarm name to expand from the **Settings** view.

ALARM NAME	SEVERITY	SUBCATEGORY	ACTIONS
Exploits Enabled Alarms = 11 and Disabled Alarms = 1			
EAP Failure Injection	Major	DoS	Enabled
ID Theft: Out of Sequence	Major	Impersonation Attacks	Disabled
ID Theft: EAP Spoofed Success	Major	Impersonation Attacks	Enabled
Airsnarf Attack	Major	Active Attacks	Enabled
Fata-jack Tool Detected	Major	DoS	Enabled
Fake-DHCP Server Detected	Major	Active Attacks	Enabled
DoS Deauthentication	Major	DoS	Enabled
802.11 Authentication Flood	Major	DoS	Enabled
DoS Disassociation	Major	DoS	Enabled
Hunter-Killer Tool Detected	Major	DoS	Enabled
Monkey-jack Tool Detected	Minor	Active Attacks	Enabled
TKIP ICV Attack	Major	Active Attacks	Enabled
Reconnaissance Enabled Alarms = 9			
Rogue Activity Enabled Alarms = 2			
Vulnerabilities Enabled Alarms = 19			

Figure 29: Settings View

- To enable or disable alarms, select the action button for a group of alarms, or select the action toggle for an individual alarm.

The **Settings** view automatically refreshes. Go to the [Alarms](#) view to display and filter alarm messages for enabled alarms.

Alarm Notifications Webhook Configurations

The Extreme AirDefense Essentials **Settings, Alarm Notifications** button provides a **Webhook Configurations** settings pane to configure push notifications for enabled alarms.

A web server or service must be configured to receive the data. This web server can then pass on the received data to third-party application data processors for further action, or store the data locally.

- From Extreme AirDefense Essentials, select  to display the **Settings** screen.
- Select the **Alarm Notifications** button to display the **Webhook Configurations** settings pane.

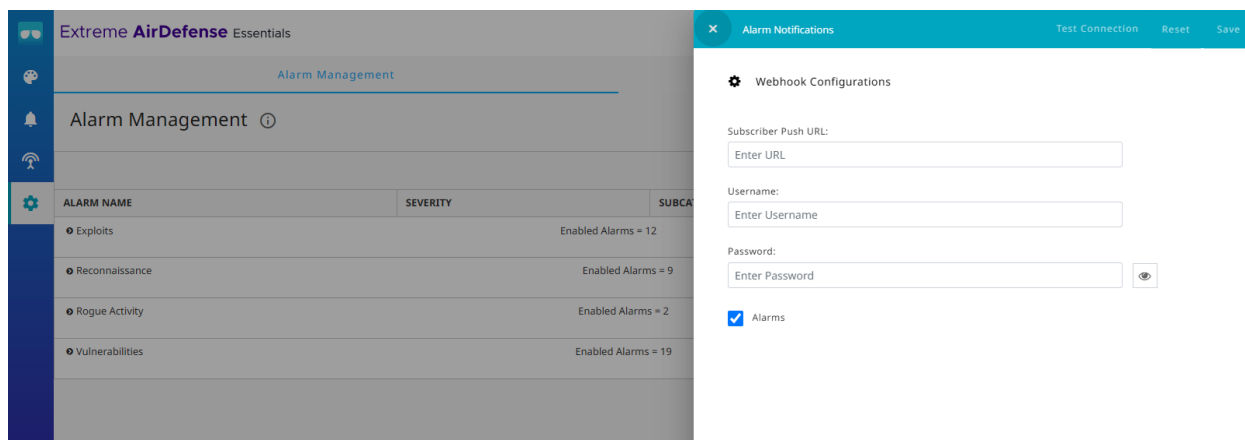


Figure 30: Alarm Notifications Webhook Configurations Settings Pane

- Provide the following values to configure the Alarm Notifications Webhook Configurations settings:

Subscriber Push URL

Configure the remote web server URL where alarms notifications are transferred in real-time.



Note

The web server must listen on one of the standard ports, 443 (https) or 80 (http). Extreme AirDefense Essentials does not support web servers listening on ports other than these two ports.

Username

Set the user name valid for accessing the remote web server.

Password

Set the password for the above user name.

Alarms

Select to push enabled alarms to the remote web server in real-time.

- Select **Save** to save the changes made to the **Subscriber Settings** parameters.

At any time, select the **Reset** button to revert the changes made to the subscriber settings parameters.

- Test the connection.

Select **Test Connection** to test the web server connection. The test also detects and mitigates a blocked tenant. If connection status is successful, blocked tenants are released and Extreme AirDefense Essentials begins sending notifications.

Classified Devices Management Settings

The Extreme AirDefense Essentials **Settings, Classified Devices Management** view provides you with the list of sanctioned devices and delete options. Manually sanctioned devices do not appear as rogue devices on the network.

- 1. From Extreme AirDefense Essentials, select  to display the **Settings** screen.
- 2. Select the **Classified Devices Management** tab to display all the sanctioned devices.

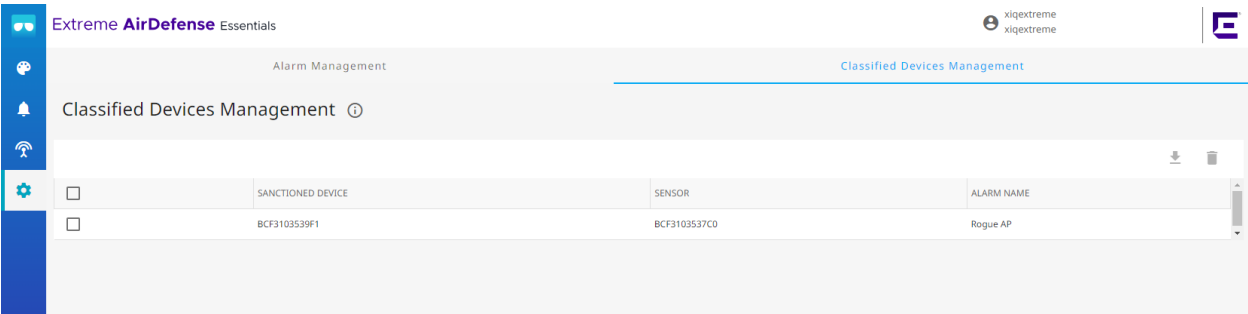


Figure 31: Classified Devices Management Settings

- 3. To delete sanctioned devices, select the checkbox for the sanctioned devices to you want to remove, and select .

The **Settings** view automatically refreshes. Go to the [Alarms](#) view to display and filter alarm messages for enabled alarms.