Extreme AirDefense Essentials User Guide

Version 23R3

9037817-00 Rev AA
May 2023

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/

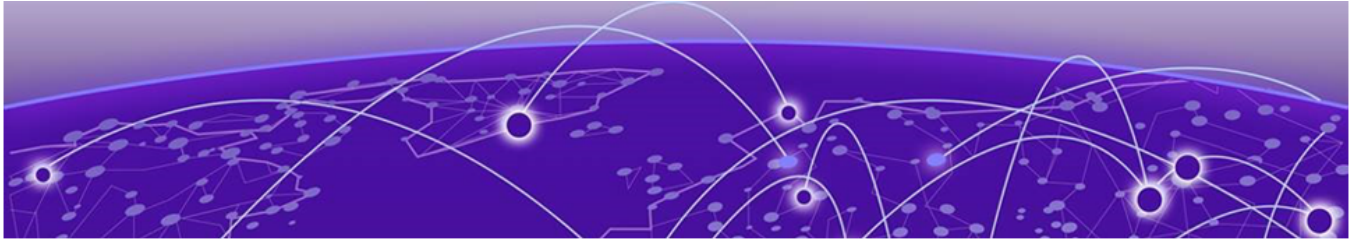


Table of Contents

Preface

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 *enter* and *type*	When you see the word *enter* 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 *type*.
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**
Words in italicized type	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.
italic text	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, *member*[*member*...].
\	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

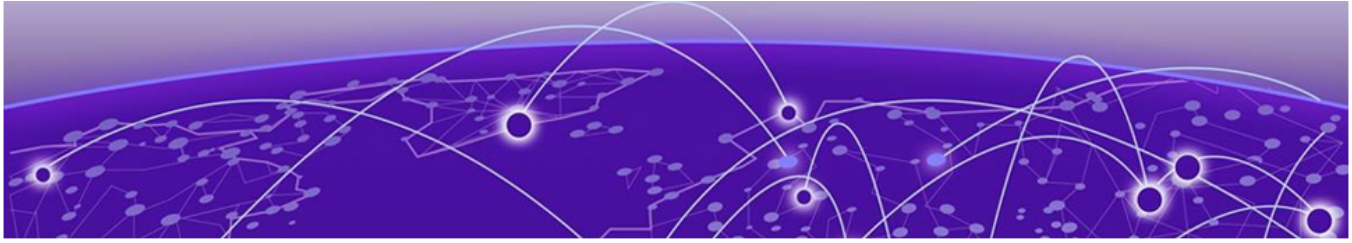
Release Notes

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/.



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

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.

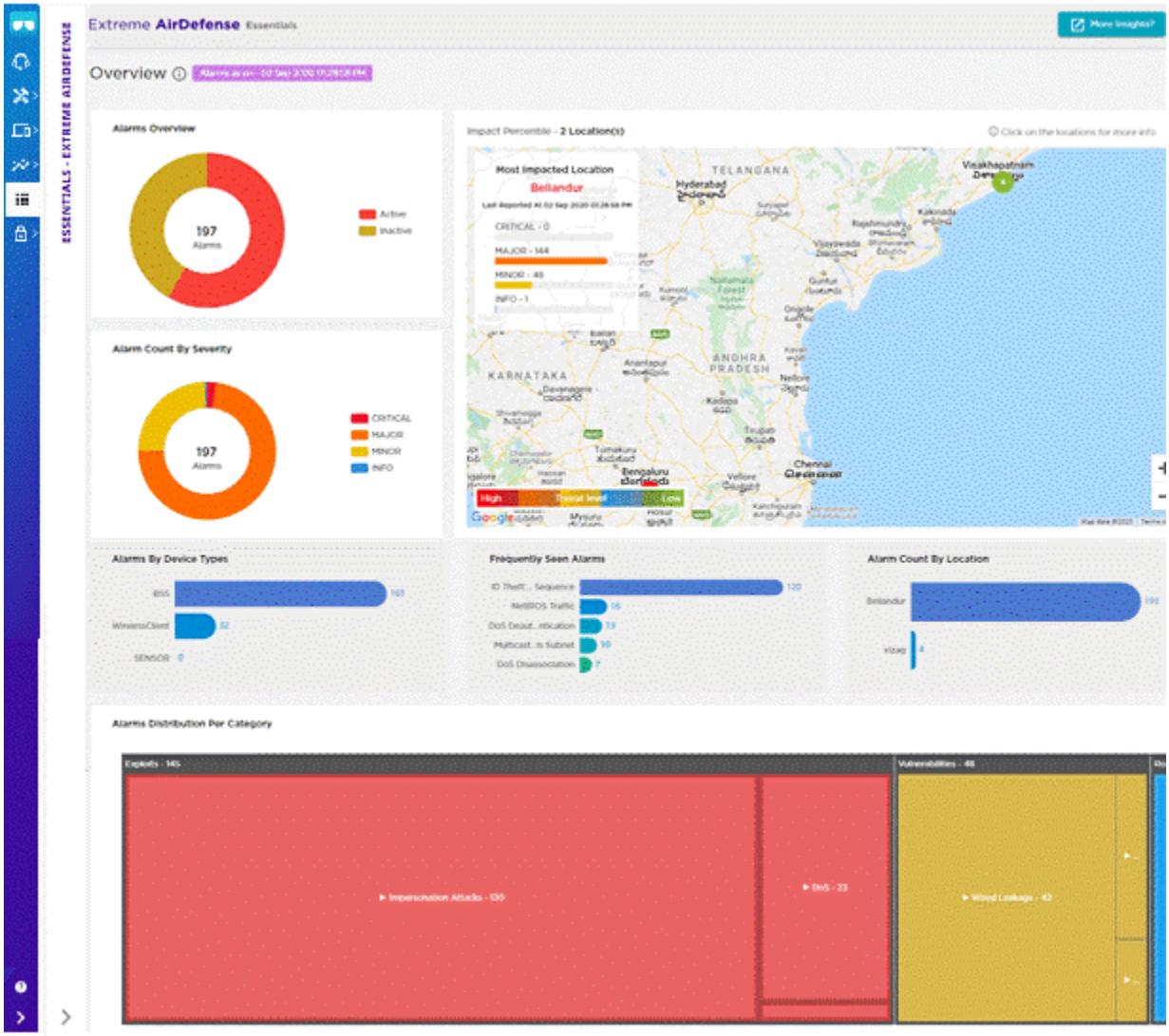


Figure 1: Extreme AirDefense Essentials Overview View in ExtremeCloud IQ

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

- Widget - Alarms Overview on page 15
- Widget - Alarm Count by Severity on page 15
- Impact Percentile Map on page 16
- Widget - Alarms By Device Types on page 17
- Widget - Frequently Seen Alarms on page 18
- Widget - Alarm Count By Location on page 18
- Widget - Alarms Distribution Per Category on page 19

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 40.

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
- AP5010
- 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.

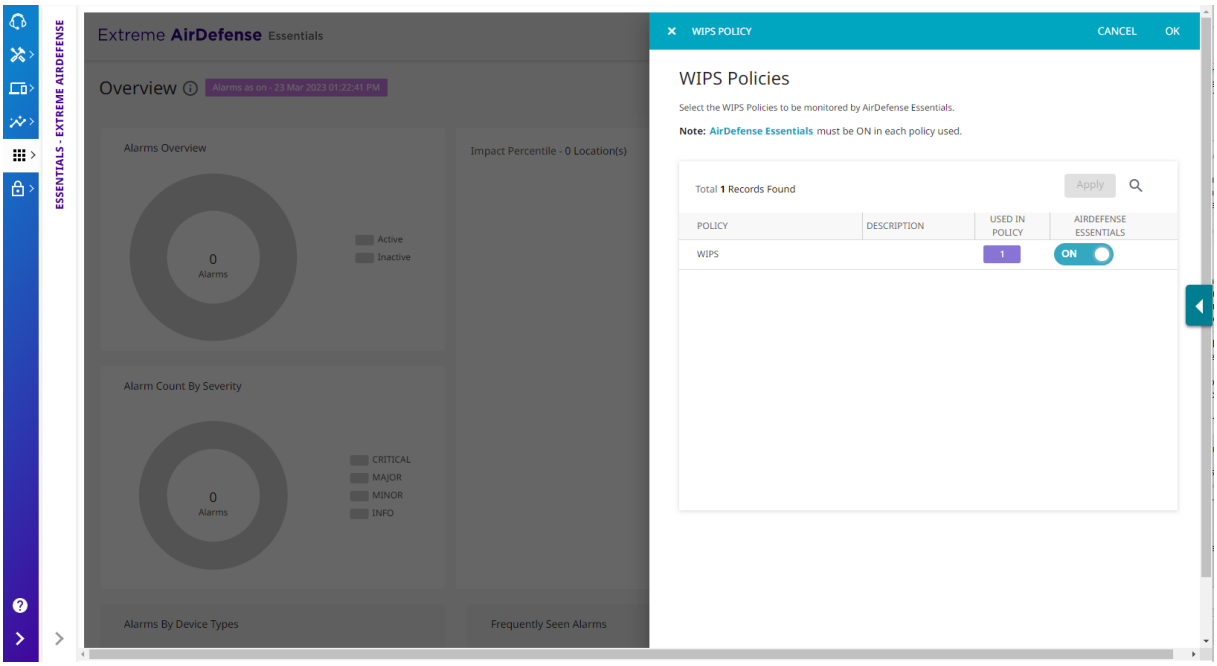
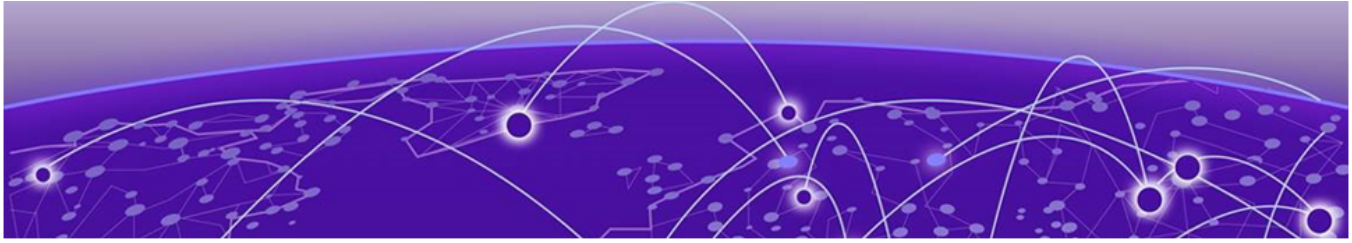


Figure 2: Extreme AirDefense Essentials WIPS Policies

2. Select the WIPS Policies that are used in Extreme AirDefense Essentials and select **Apply** then **Ok**.
3. Visit the Summary on page 13 page for more information.



Summary

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

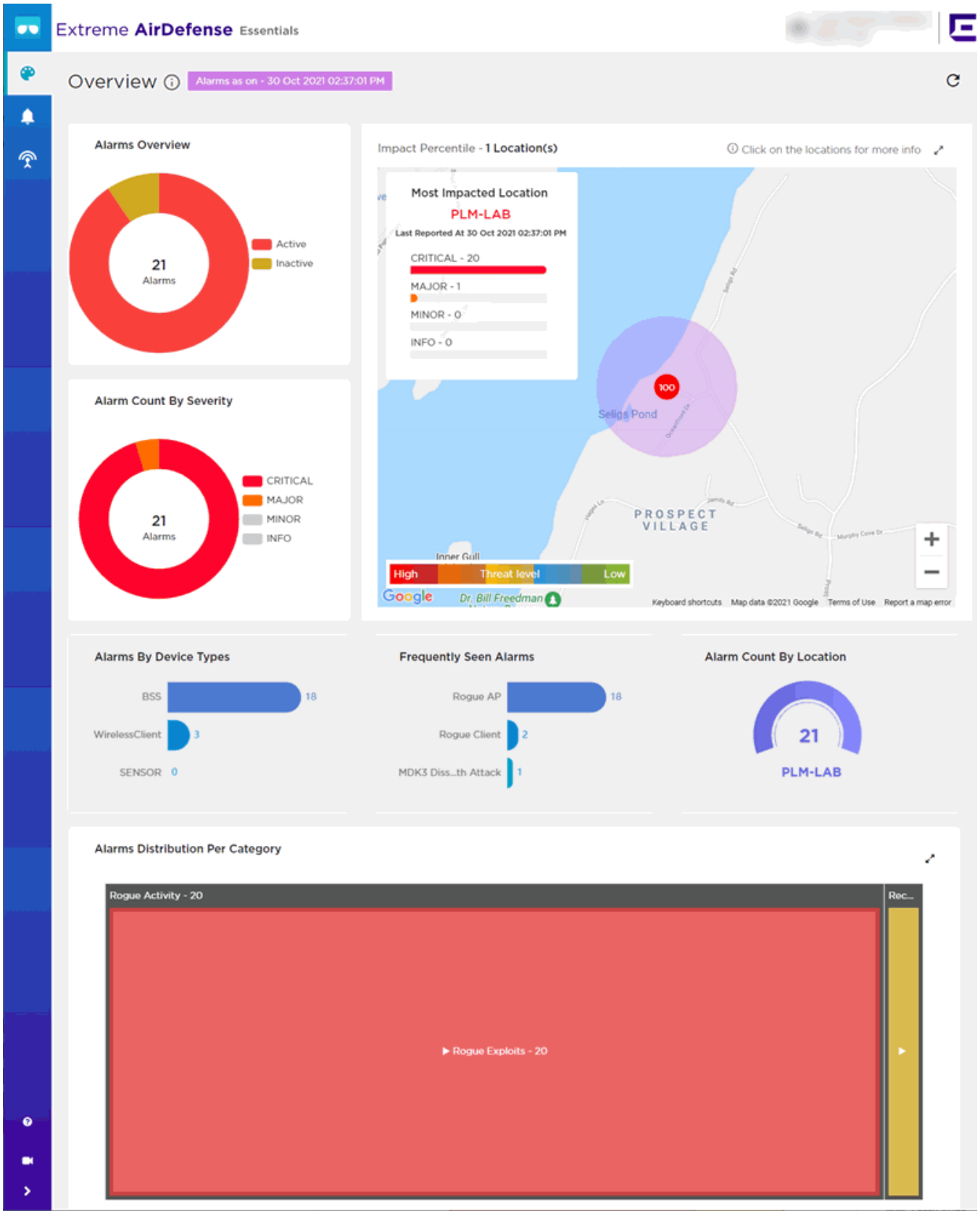


Figure 3: Summary Overview

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.

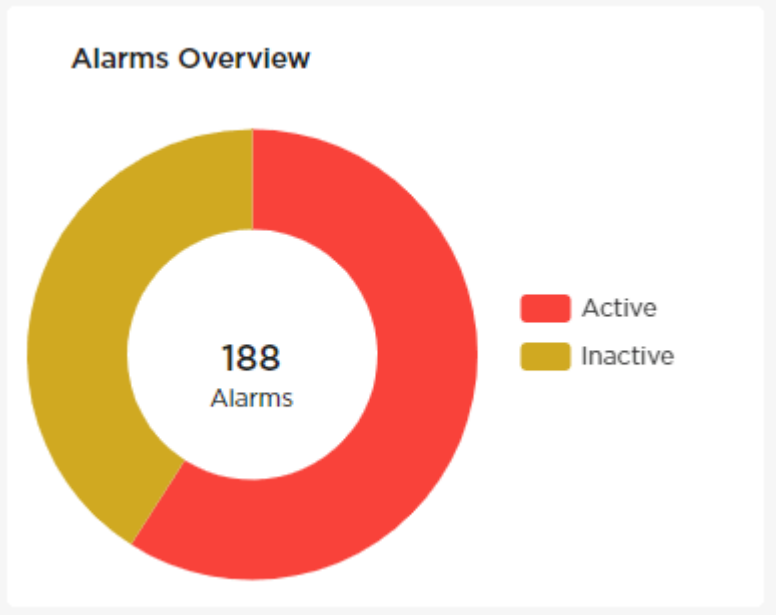


Figure 4: Alarms Overview Widget

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..

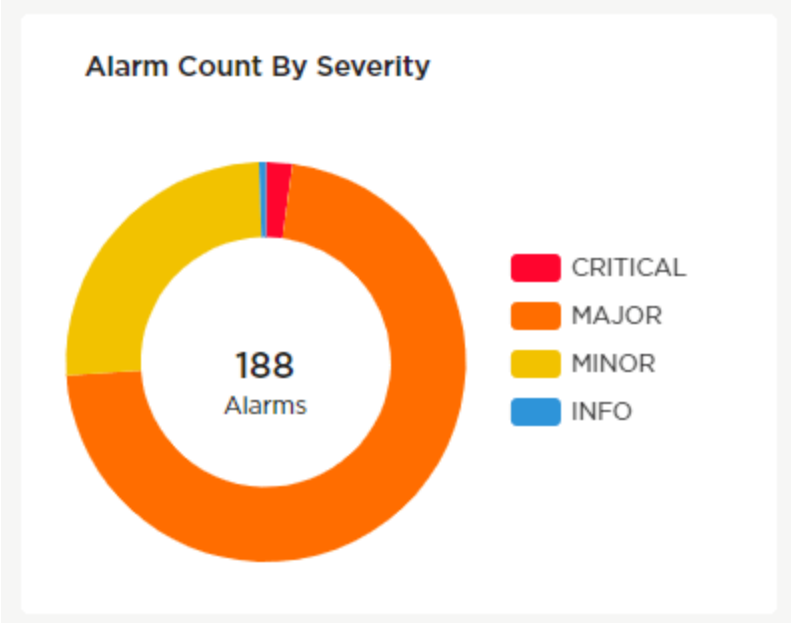


Figure 5: Alarm Count by Severity Widget

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.

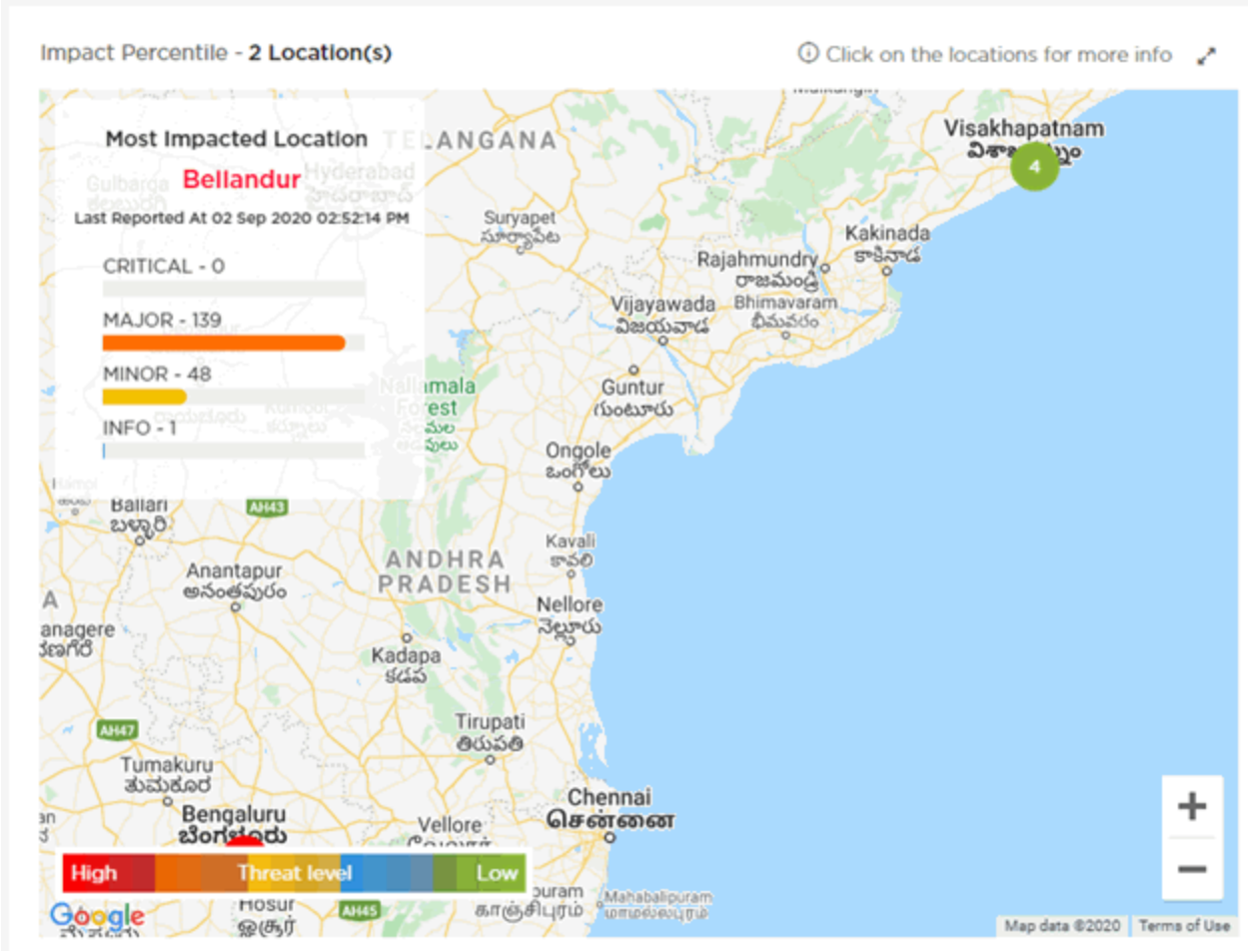


Figure 6: Impact Percentile Map

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.

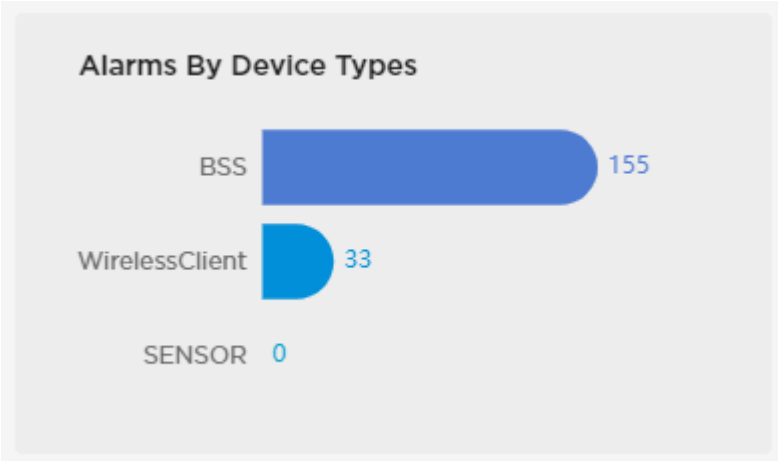


Figure 7: Alarms By Device Types Widget

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.

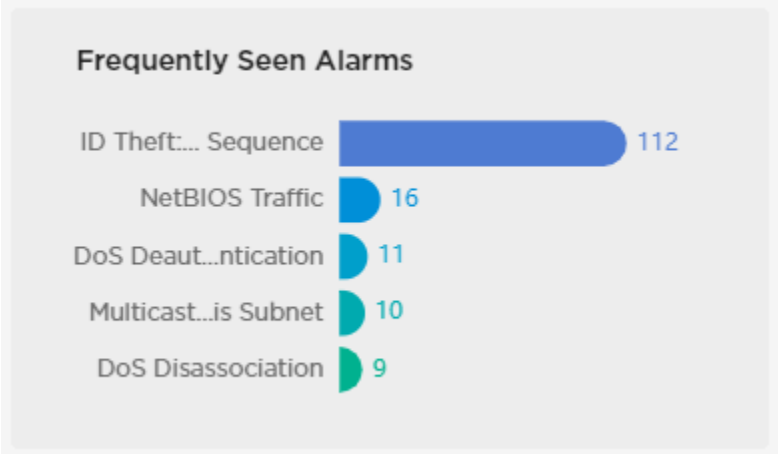


Figure 8: Frequently Seen Alarms Widget

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.

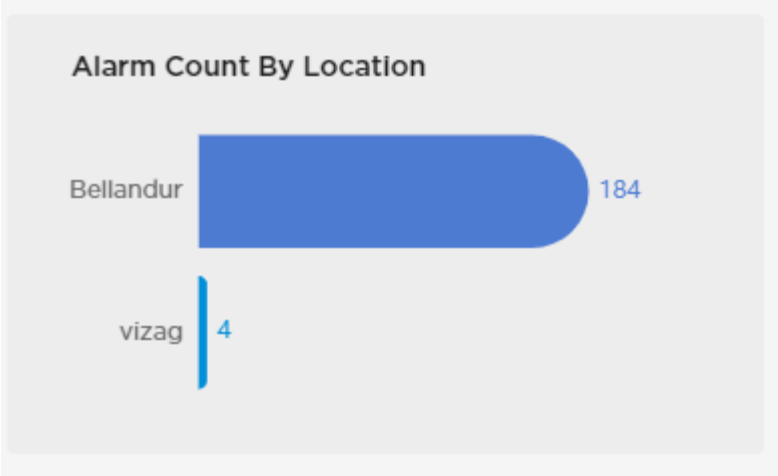


Figure 9: Alarm Count By Location

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

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.

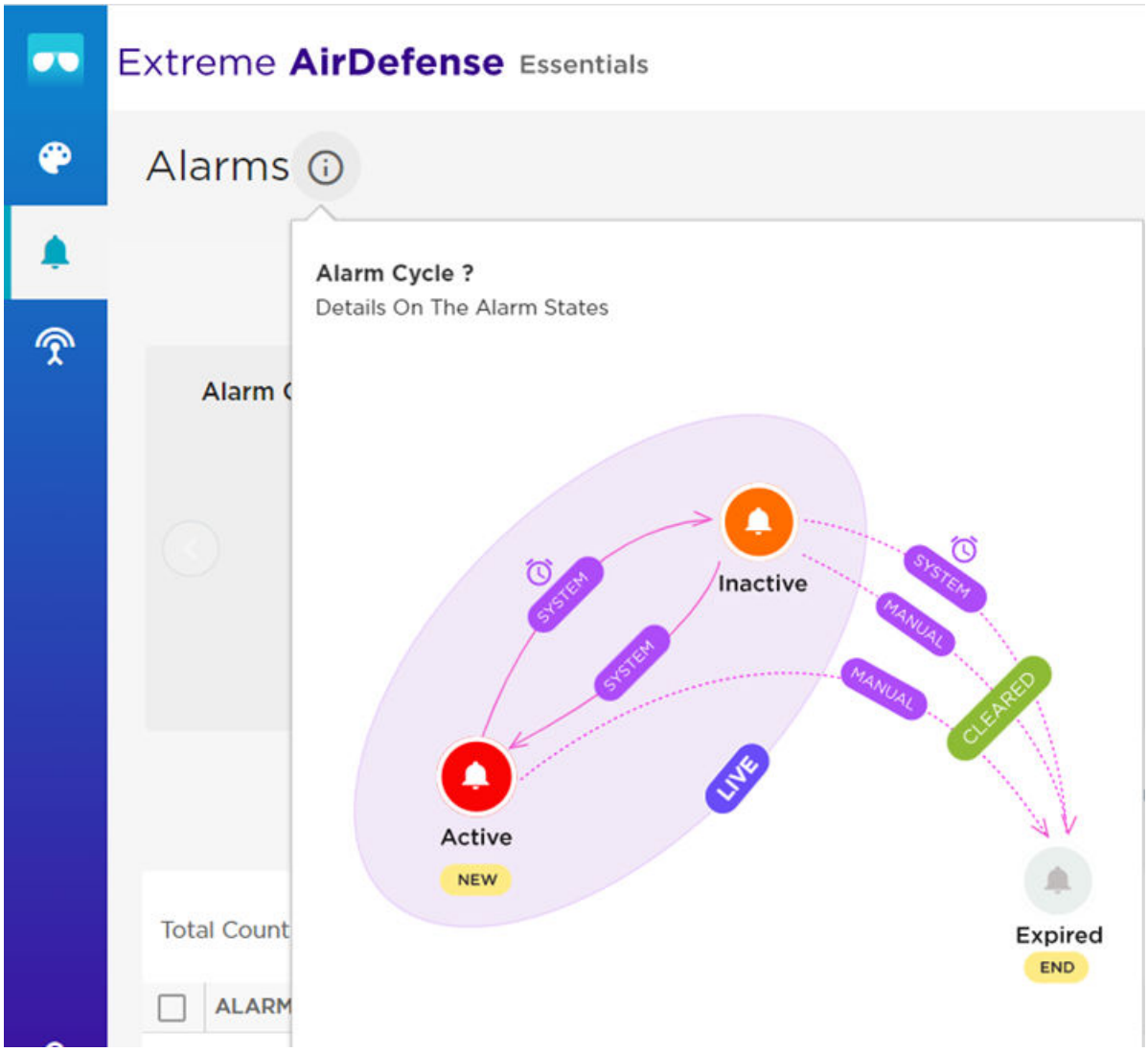


Figure 10: Alarms Life Cycle diagram

Related Topics

Alarms Cycle on page 21
Alarm Details on page 23
Live Alarms View on page 24
Expired Alarms View on page 28

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:

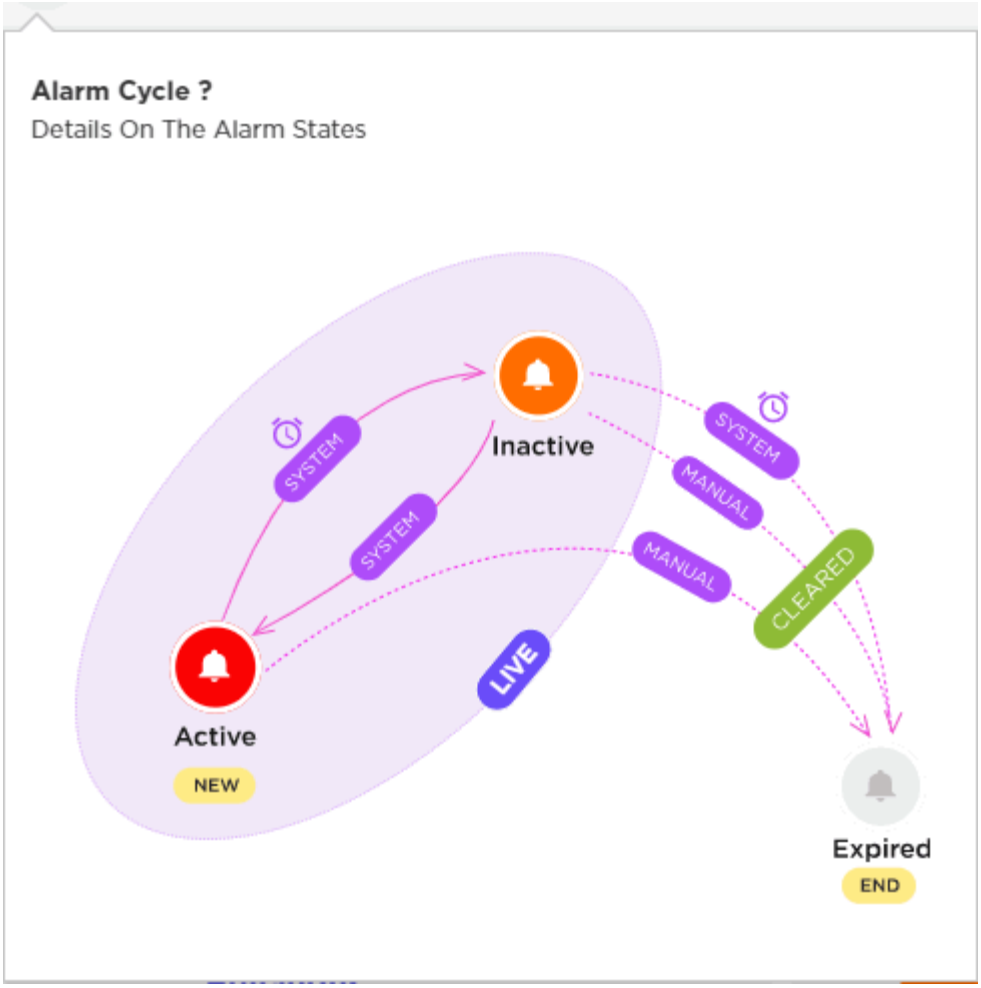


Figure 11: Alarm Cycle

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. The 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.

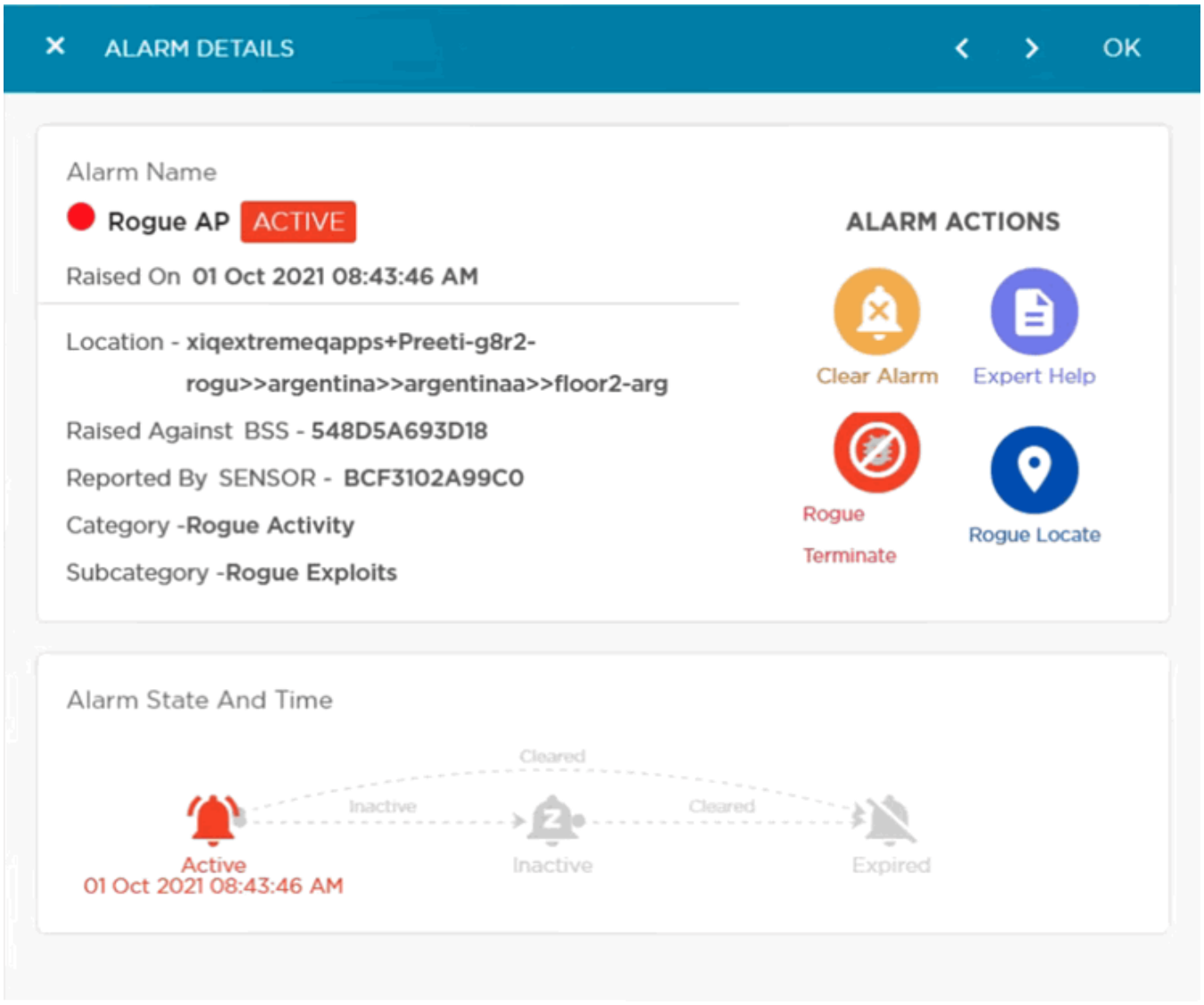


Figure 12: Alarms Details Window

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 32.
	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 Topics

Locate Rogue Devices on page 33
Terminate Rogue Devices on page 34

Live Alarms View

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

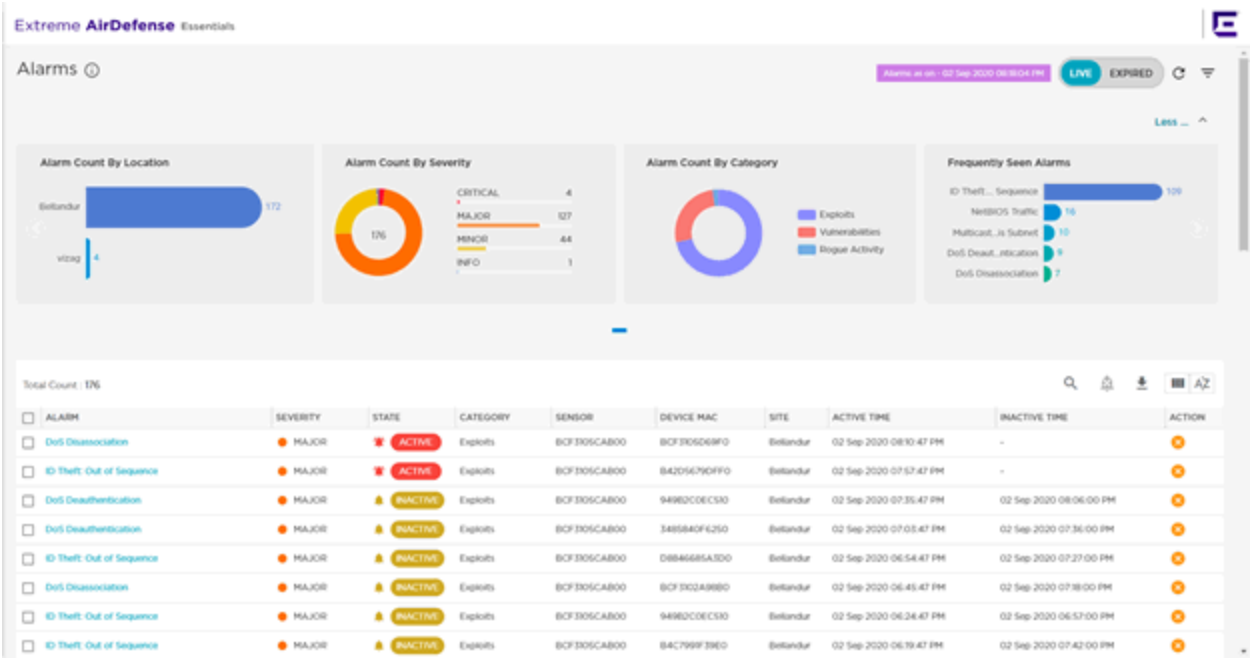
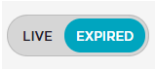


Figure 13: Live Alarms View

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.

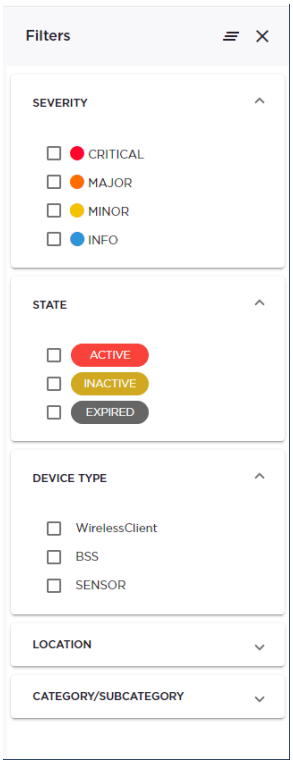


Figure 14: Filter View

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 26
- Live Alarms Raised Table on page 27

Live Alarms Widgets

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

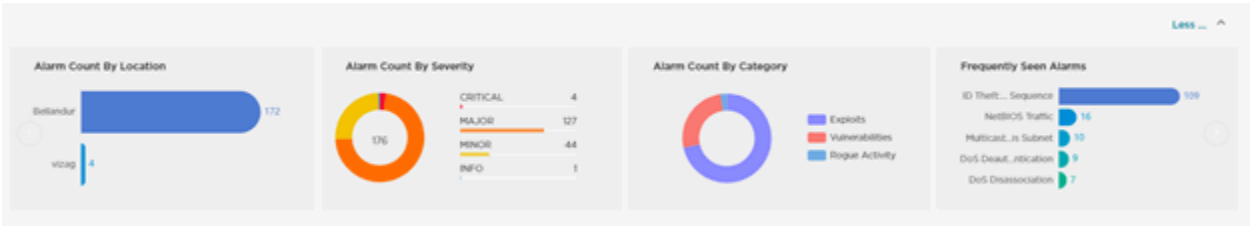


Figure 15: Live Alarms Widgets

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 21.

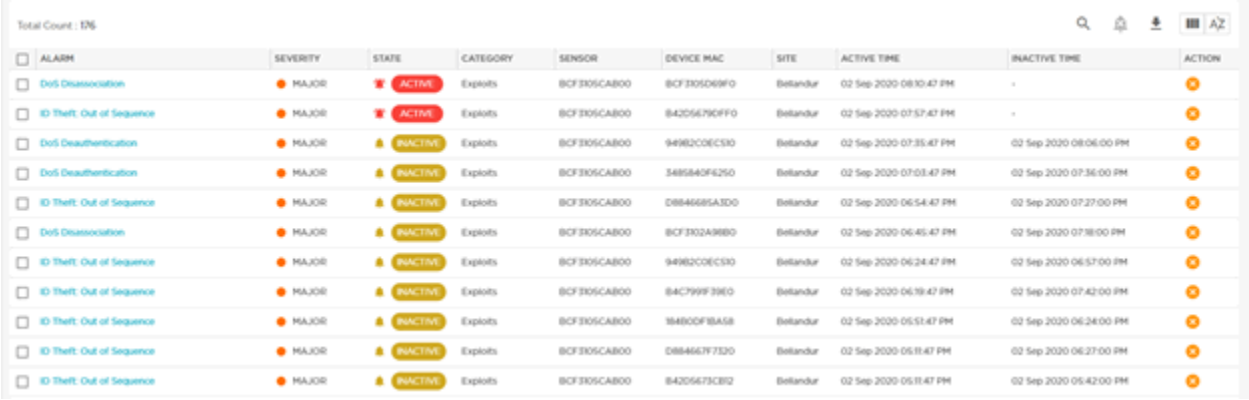


Figure 16: Live Alarms Raised Table

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 Topics

Alarm Details on page 23
Alarms Cycle on page 21

Expired Alarms View

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

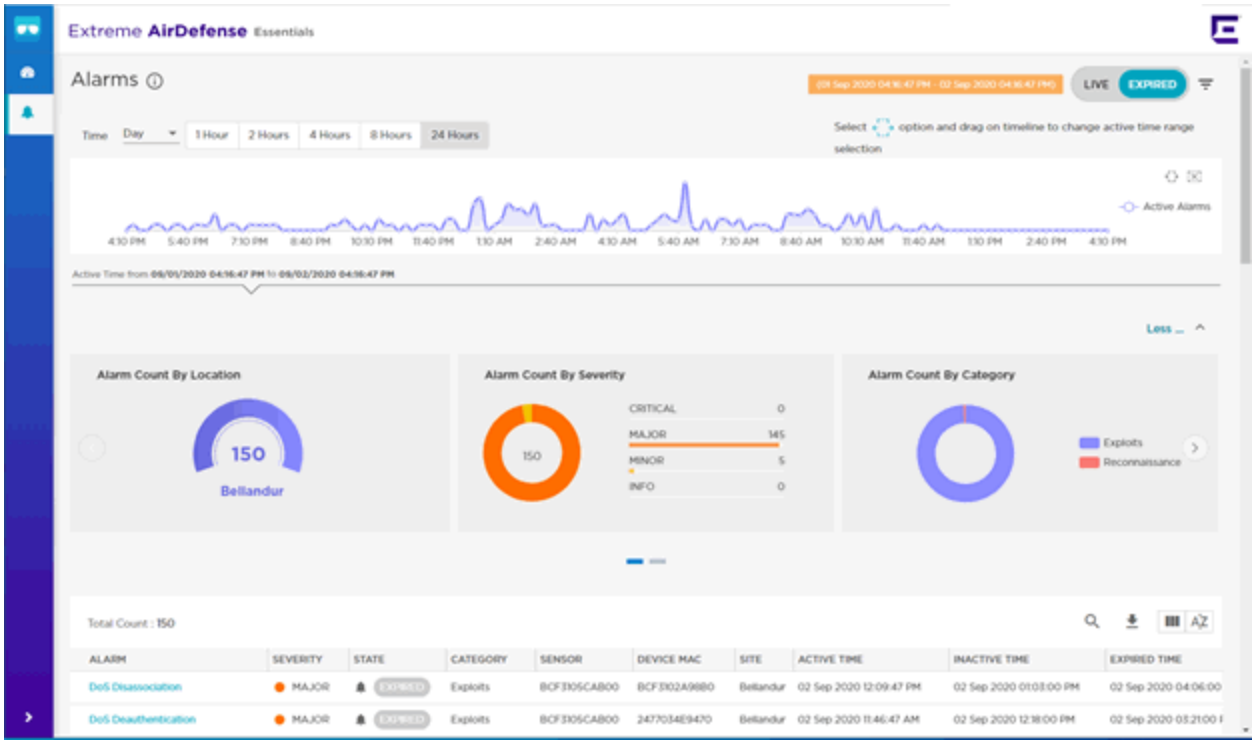
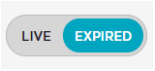


Figure 17: Expired Alarms View

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.

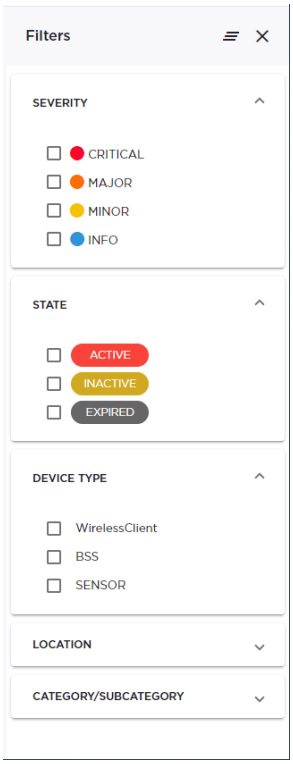


Figure 18: Filter View

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 30
- Expired Alarms Widgets on page 31
- Expired Alarms Raised Table on page 31

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.

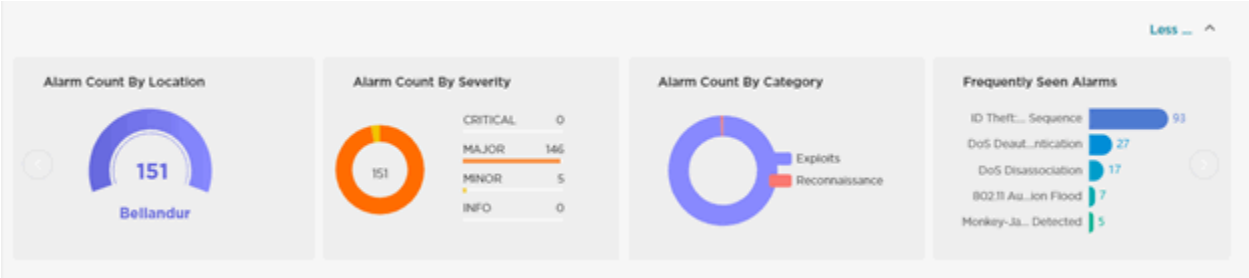


Figure 20: Expired Alarms Widgets

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.

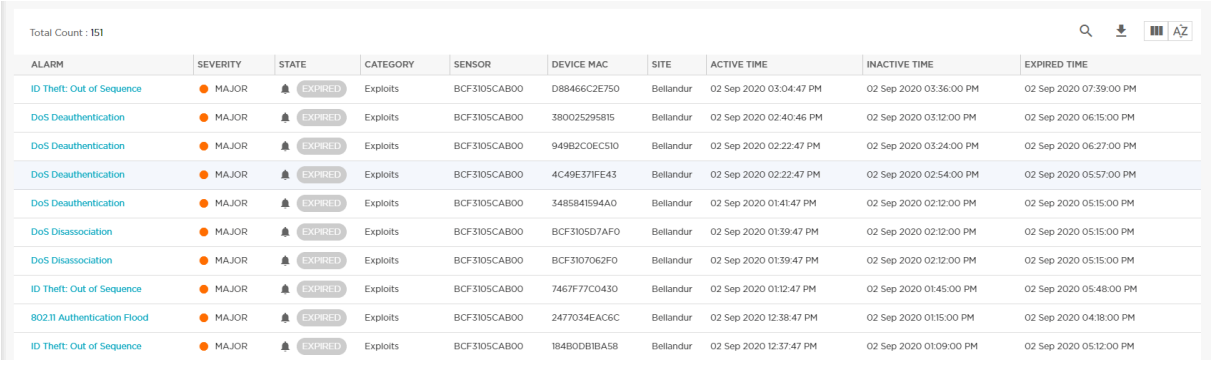


Figure 21: Expired Alarms Raised Table

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 Topics

Locate Rogue Devices on page 33
Terminate Rogue Devices on page 34

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.

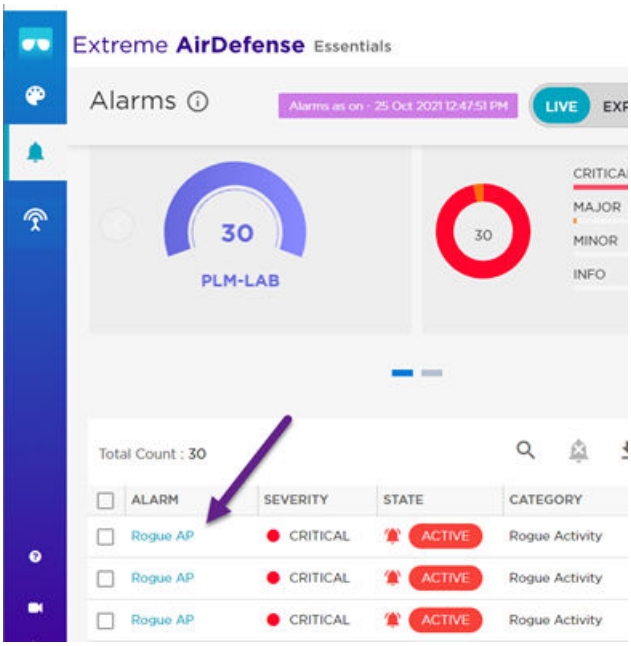


Figure 22: Rogue AP in Alarms List

The **Alarm Details** dialog displays.

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

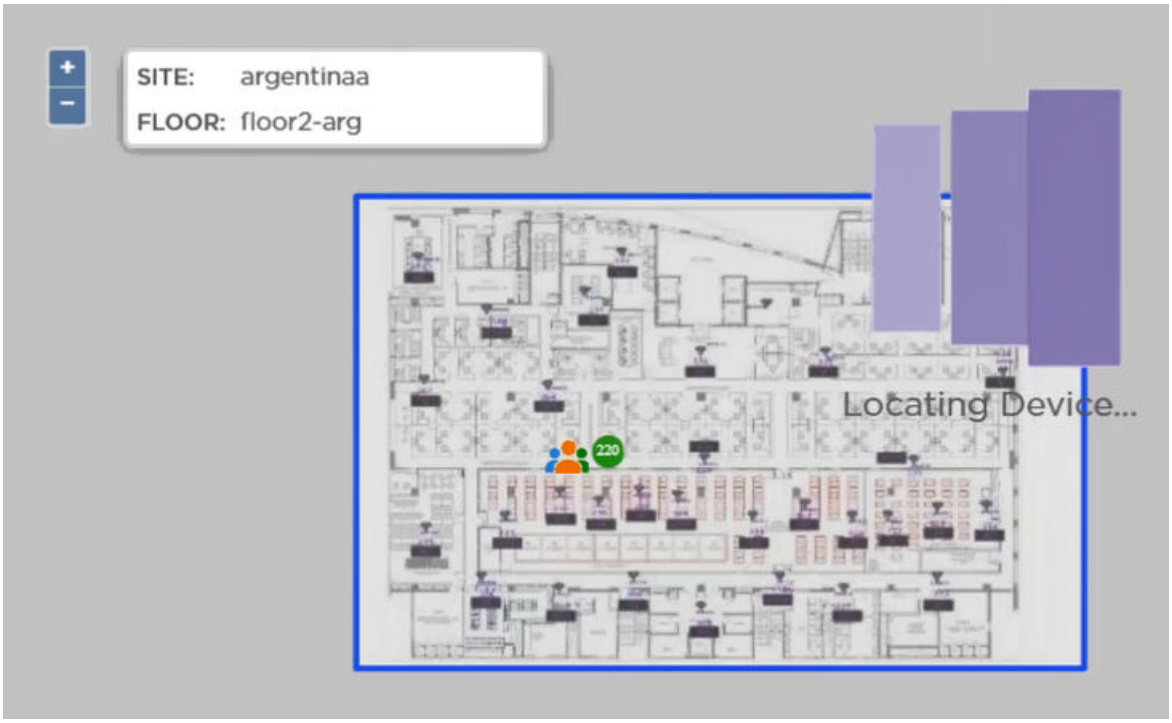


Figure 23: Locating Rogue Device in ExtremeLocation Essentials

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 Topics

Rogue Device Detection on page 32

Terminate Rogue Devices

Take the following steps to terminate a rogue device:

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.

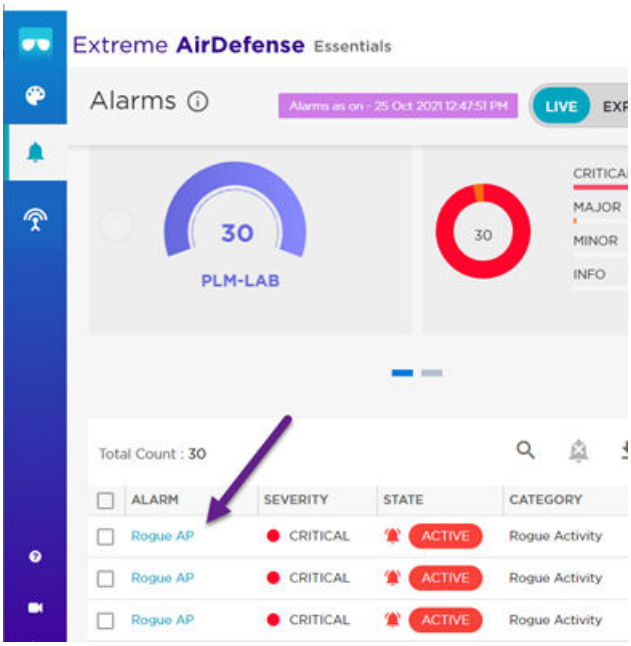


Figure 24: Rogue AP in Alarms List

The **Alarm Details** dialog displays.

3. Select to terminate the rogue device.

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

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

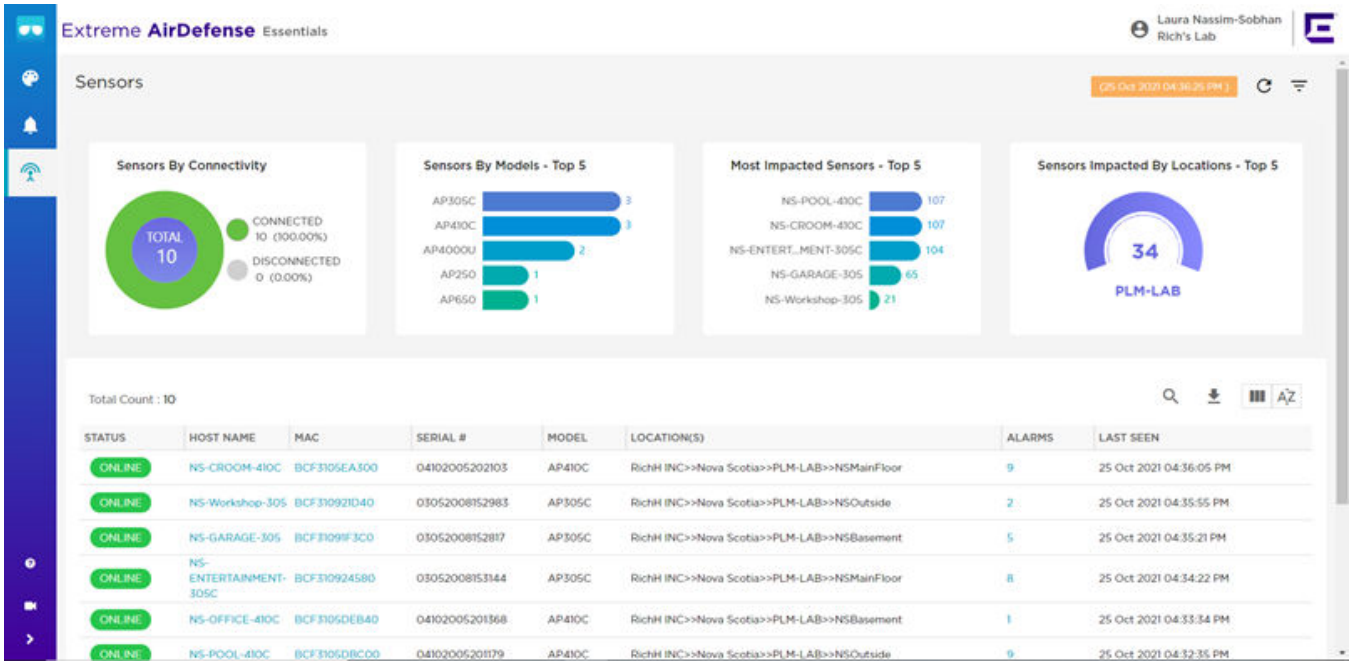


Figure 25: Sensors View

2. 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.

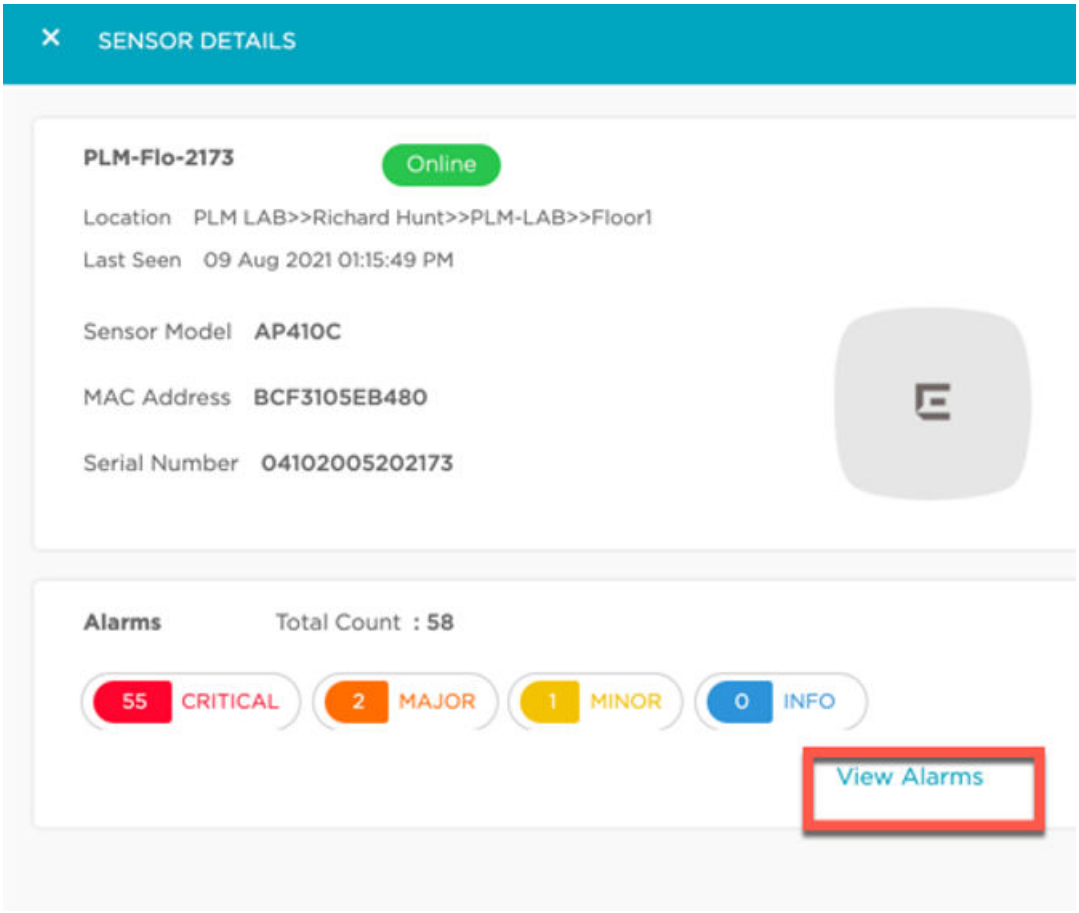


Figure 26: Sensor Details Window

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

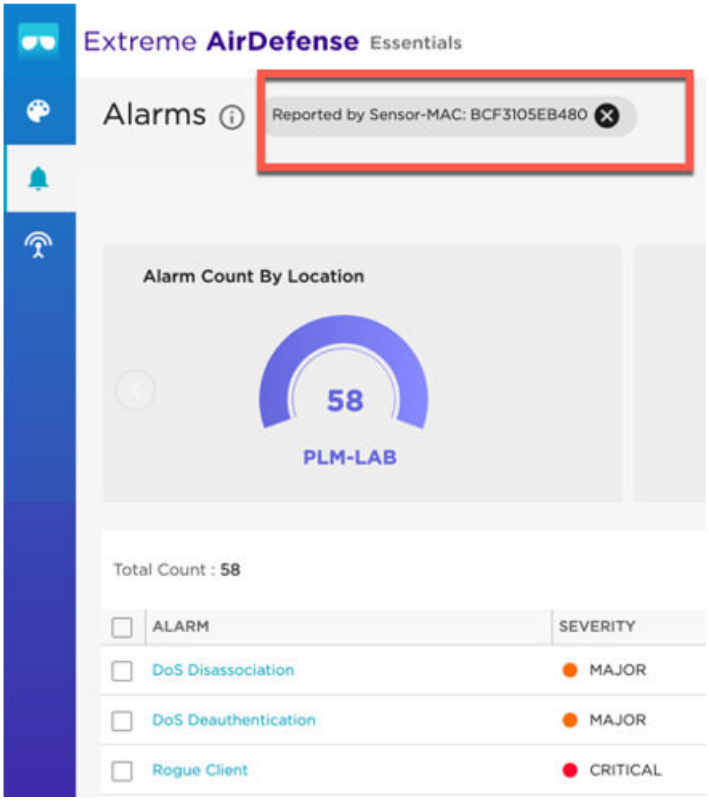


Figure 27: Alarms per Sensor

NEW!

Alarm Management Settings

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.

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

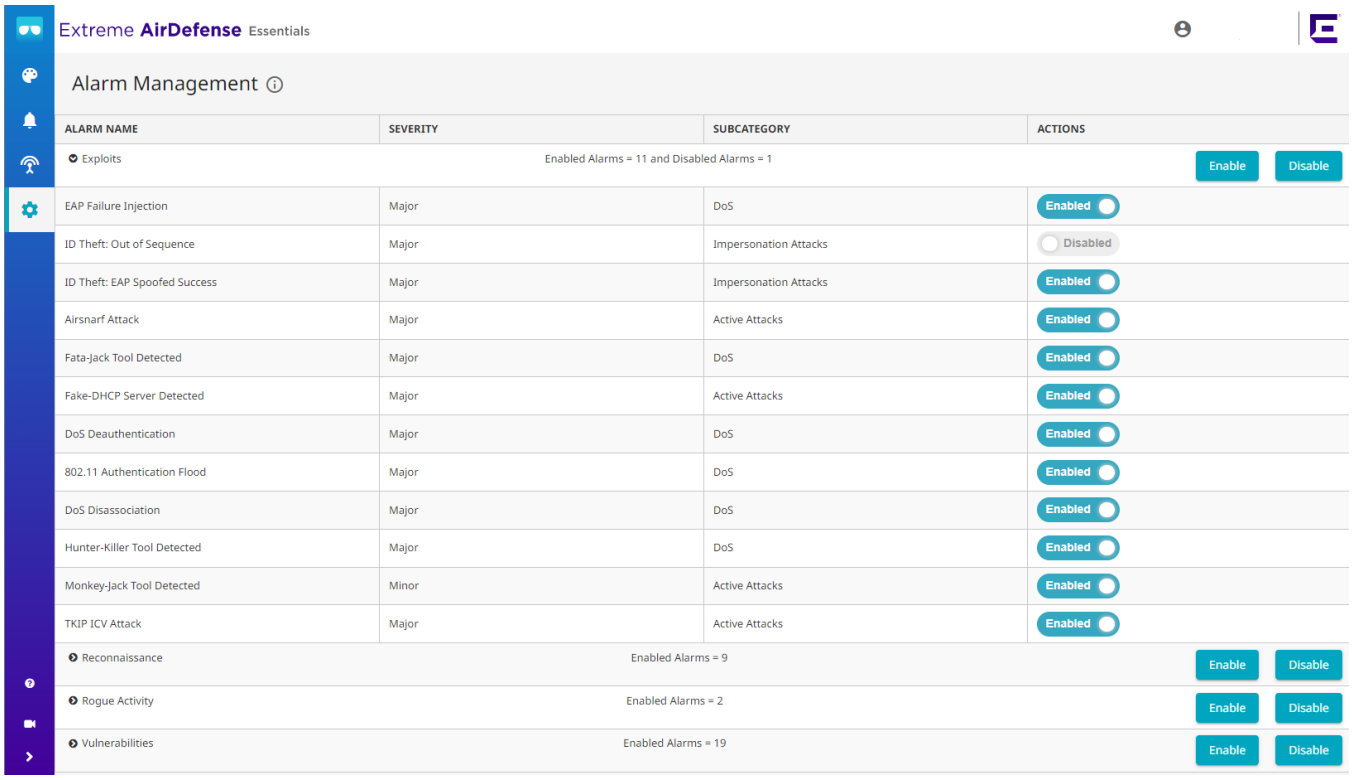
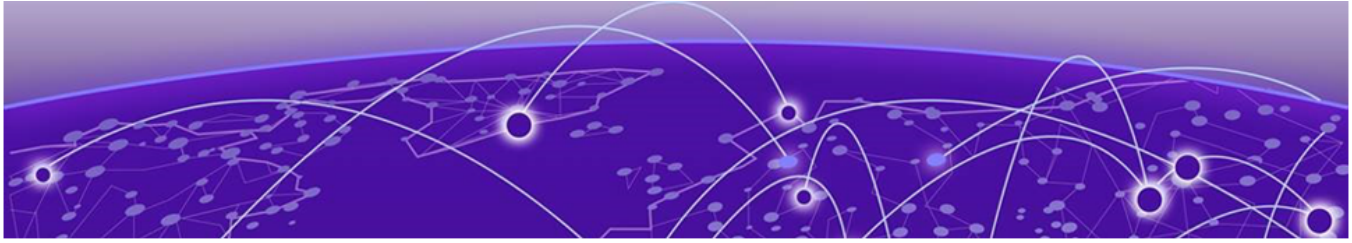


Figure 28: Settings View

3. 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.



Glossary

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Extreme Defender for IoT

Extreme Defender for IoT provides unique in-line security for mission critical and/or vulnerable IoT devices. Placed between the IoT device and the network, the Defender for IoT solution helps secure and isolate IoT devices protecting them from internal and external hacking attempts, viruses, malware and ransomware, DDoS attacks, and more. Designed to be simple and flexible, Defender for IoT can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

The solution is comprised of the Extreme Defender Application Software and the Defender Adapter (SA201) or AP3912i access point. ExtremeCloud IQ Controller is the supported platform for the Extreme Defender Application.

For more information, see https://www.extremenetworks.com/product/extreme-defender-for-iot/.

ExtremeAnalytics for ExtremeCloud IQ - Site Engine

ExtremeAnalytics™ for ExtremeCloud™ IQ - Site Engine, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. ExtremeAnalytics for ExtremeCloud IQ - Site Engine provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more at https://www.extremenetworks.com/product/extremeanalytics-for-extremecloud-iq-site-engine/.

ExtremeCloud IQ Controller

Extreme Campus Controller has been rebranded to ExtremeCloud IQ Controller. The new ExtremeCloud IQ Controller supports Campus/Centralized sites only.

The ExtremeCloud IQ Controller is a next generation orchestration application offering all the mobility services required for modern unified access deployments offering simplified integration with ExtremeCloud IQ to take advantage of Cloud Visibility into the network. The ExtremeCloud IQ Controller extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud IQ Controller includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge.

ExtremeCloud IQ - Site Engine

ExtremeCloud™ IQ - Site Engine (formerly known as Extreme Management Center and Netsight), is a web-based control interface that provides centralized visibility into your network. ExtremeCloud IQ - Site Engine reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, ExtremeCloud IQ - Site Engine becomes the central location for monitoring and managing all the components in the infrastructure. Learn more at https://www.extremenetworks.com/product/extremecloud-iq-site-engine/.

ExtremeCloud™ IQ

ExtremeCloud™ IQ is an industry-leading and visionary approach to cloud-managed networking, built from the ground up to take full advantage of the Extreme Networks end-to-end networking solutions. ExtremeCloud IQ delivers unified, full-stack management of wireless access points, switches, and routers and enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and deliver new levels of network automation and intelligence. Learn more about ExtremeCloud IQ at https://www.extremenetworks.com/support/documentation/extremecloud-iq/.

ExtremeControl for ExtremeCloud IQ - Site Engine

ExtremeControl for ExtremeCloud™ IQ - Site Engine, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more at https://www.extremenetworks.com/product/extremecontrol-for-extremecloud-iq-site-engine/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800,

and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density Wi-Fi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy.