Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Extreme Network Access Control (NAC) to Forward Logs to EventTracker

EventTracker v9.x and above

Publication Date:

July 23, 2021

Abstract

This guide provides instructions to configure Extreme Network Access Control to forward Extreme Network Access Control logs via syslog.

Scope

The configurations detailed in this guide are consistent with EventTracker version v 9.x or above and Extreme Management Center version 7.1.

Audience

Administrators who are assigned the task to monitor Extreme Network Access Control events using EventTracker.

Table of Contents

1. Overview

Extreme Networks Network Access Control (NAC) is a complete standard-based, multi-vendor, interoperable, pre-connect, and post-connect Network Access Control solution for wired and wireless LAN and VPN users. The Extreme Control engine is monitored by Extreme Management Center which provides the analytics for the network.

Log configuration can be achieved via syslog. It will send events like authentication events, user logon events, ethernet connectivity events. With this events EventTracker generate detail reports for user logon activities, ethernet connectivity status, and user authentication activities. Its graphical representation shows login success by username, authentication success by username, ethernet link status, etc.

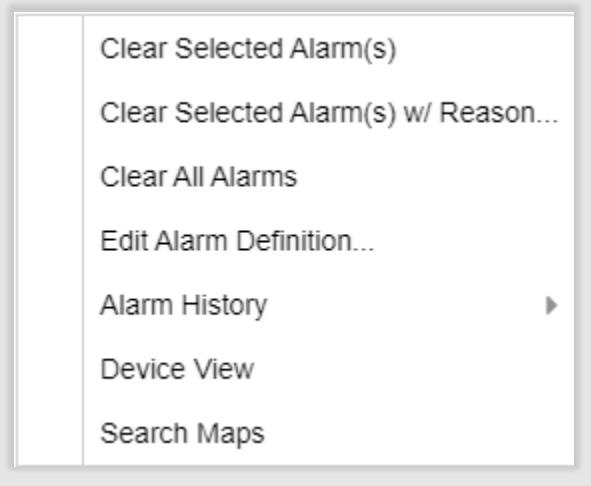
2. Prerequisites

- Admin access to Extreme Network Access Control(NAC).

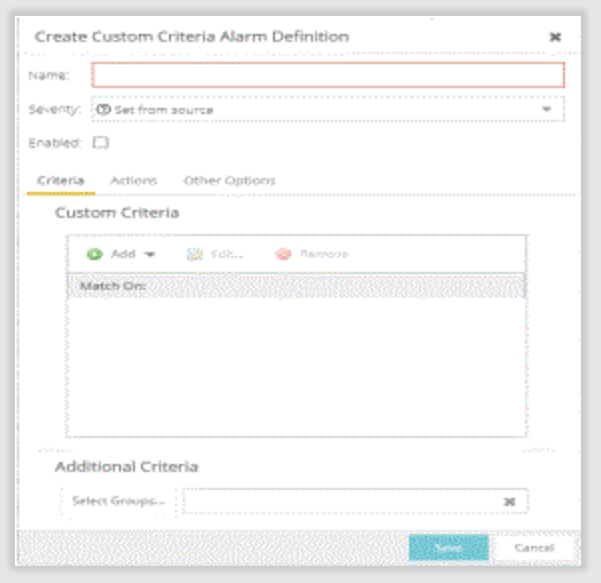
3. Configuring Extreme Network Access Control

3.1 Enable syslog/ Remote Logging.

1. Log in to the Extreme Network Access Control (NAC) web interface with Admin privileges.
2. Navigate to **Alarms tab,** right-click on the alarm or select the **Menu** icon (☰) to display several additional functions.
3. Click on **Edit Alarm Definition**.



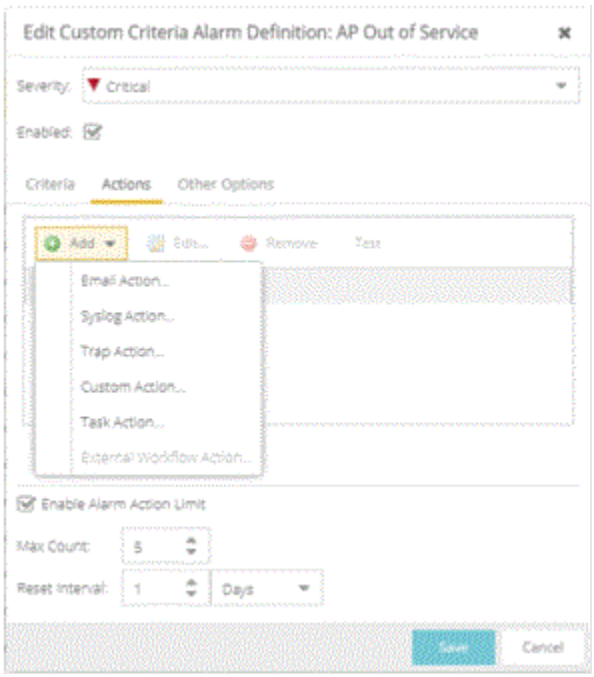
4. Select to open the alarm in the Alarm Configuration window, from which you can edit the criteria which triggers the alarm. The **Create Custom Criteria Alarm Definition** window opens.



5. The severity of the alarm displays in the Severity field. Use the drop-down list to change the alarm severity. The Enabled check box indicates if the custom criteria has been enabled.

   - Select the **Criteria** tab to open the **Custom Criteria** window, where you can Add, Edit or Remove specific criteria details the alarm.

     Use the Additional Criteria field to add new criteria. Select the **Select Groups** button to open the Alarm Group Section window.
   - Select the **Actions** tab to Add, Edit, Remove actions to the alarm definition. Select the Add button to open the Action drop-down list:



6. Select **Syslog action** from the drop-down list.
    - Syslog Server: Enter EventTracker IP address.
    - Port: Enter syslog server port number 514.
    - Click **Enable** to provide custom log format.

    Time $time Device $device: alarmName="$alarmName", alarmSource="$alarmSource", alarmSourceName="$alarmSourceName", alarmSubcomponent="$alarmSubcomponent", severity="$severity", type="$type", trigger="$trigger", server="$server", Time="$time", message="$message", eventType="$eventType", eventSeverity="$eventSeverity", eventCategory="$eventCategory", eventTitle="$eventTitle", eventUser="$eventUser", eventClient="$eventClient", deviceIP="$deviceIP", deviceIpCtx="$deviceIpCtx", deviceNickName="$deviceNickName", deviceBootProm="$deviceBootProm", deviceStatus="$deviceStatus", snmp="$snmp", sysName="$sysName", sysLocation="$sysLocation", sysUpTime="$sysUpTime", chassisId="$chassisId", chassisType="$chassisType", trapName="$trapName", trapEnterprise="$trapEnterprise", trapOid="$trapOid", trapArgs="$trapArgs"

    Note: We can receive all type of Extreme NAC event logs to EventTracker with above format.

7. Click **Save** changes.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.
Netsurion's EventTracker cyber threat protection platform provides SIEM, end protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.
Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters
Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers
EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support