How to Guide

Configure Alert Suppression in Netsurion Open XDR

Publication Date:

11 September 2023

Table of Contents

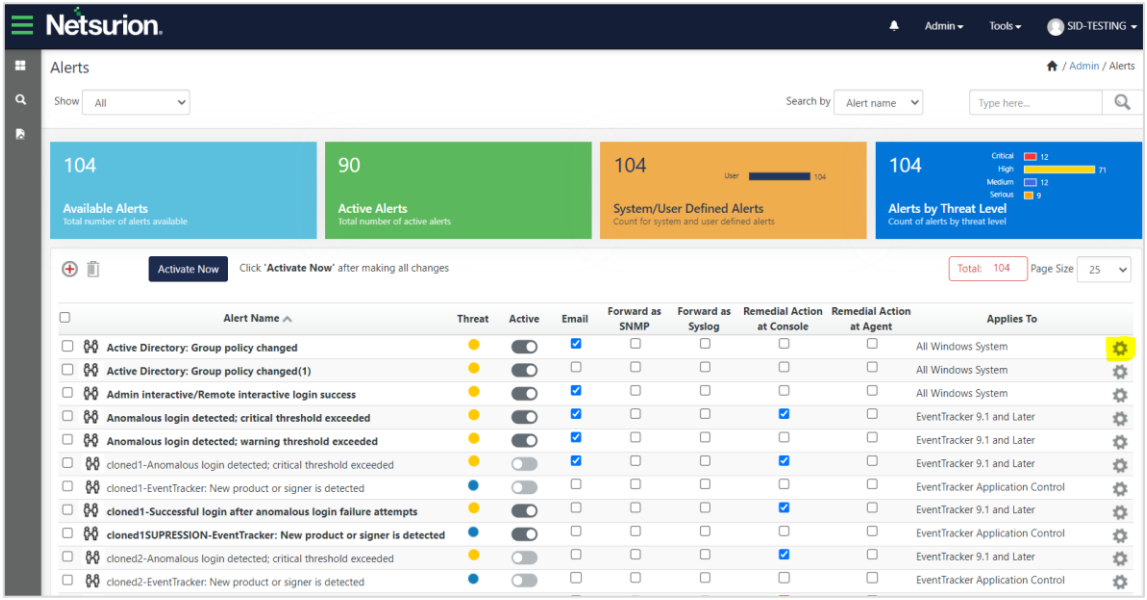
1 Overview

This document describes the function of suppressing the alert based on the specified interval and criteria. This prevents the generation of voluminous alerts and limits the alert generation to the required amount within the specified interval.

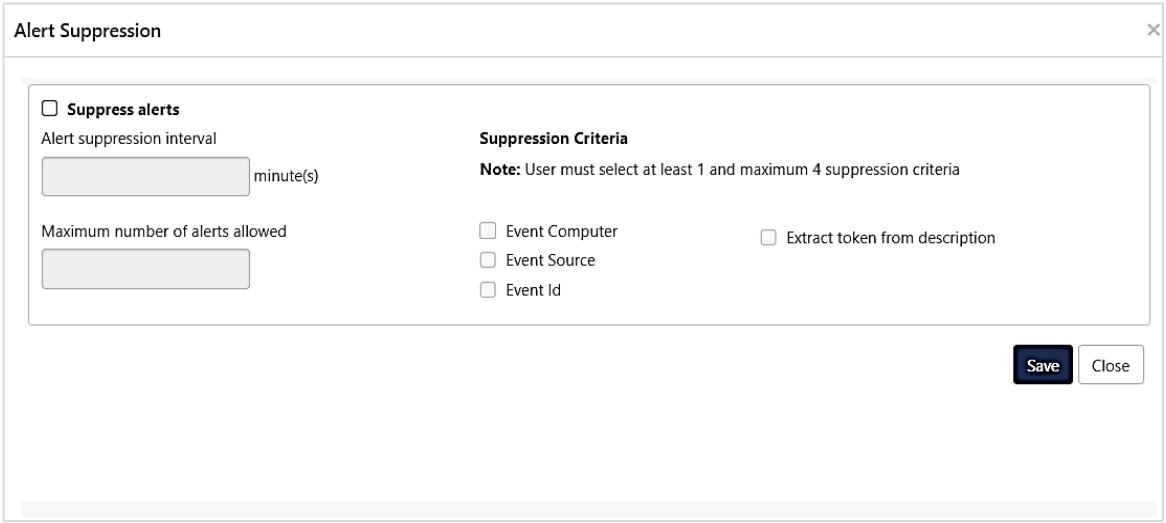
2 Configuring the Alert Suppression

Perform the following procedure to suppress the required alerts.

1. In the Netsurion Open XDR console, go to **Alerts** and click the **Alert Suppression settings** icon located adjacent to each alert to set the alert suppression for the required alert.

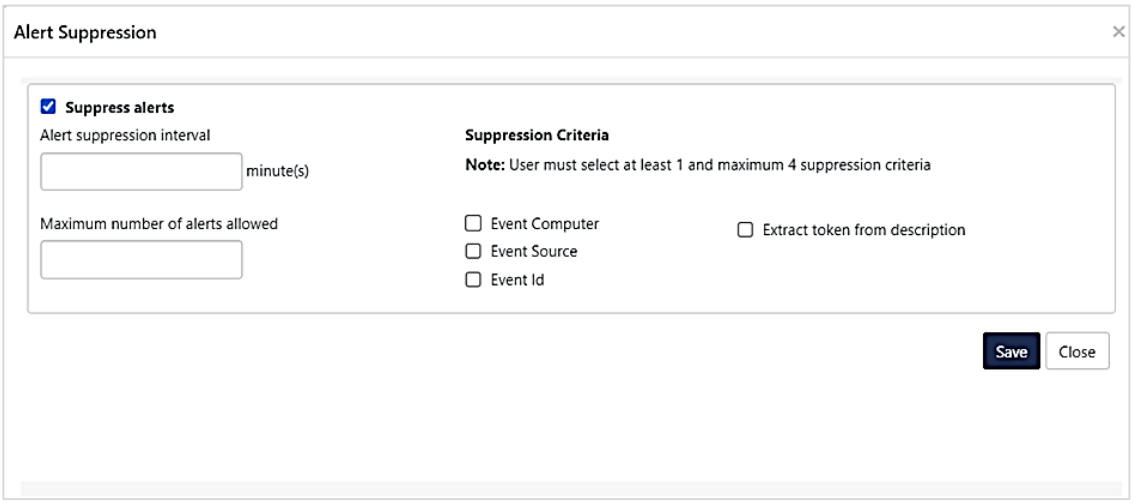


The following Alert Suppression configuration window pops up.



2. In the **Alert Suppression** window, select the **Suppress alerts** check box to enable the settings.

   This enables to configure the Alert suppression interval, maximum number of alerts allowed and Suppression Criteria.



3. Provide the necessary details and click **Save** to update the appropriate alert suppression configuration.

   - **Alert suppression interval:** Specify the required suppression interval in minutes.
   - **Maximum number of alerts allowed:** Specify the number alerts that must be generated within the specified suppression interval.

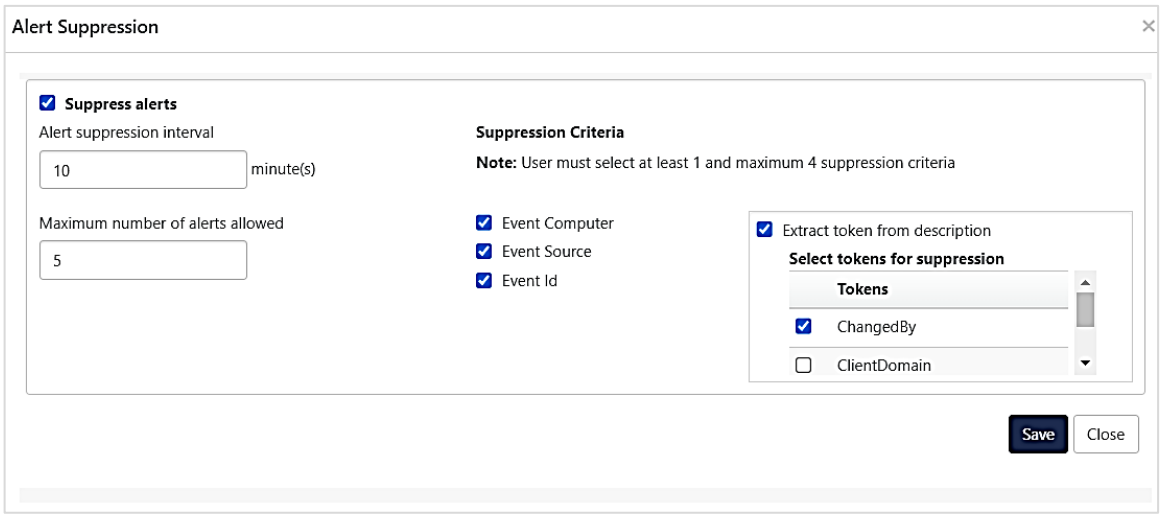
   > **Note**:
   >
   > The fields, **Alert suppression interval** and **Maximum number of alerts allowed** are mandatory.

   - **Suppression Criteria**: Select the appropriate alert suppression criteria to suppress the alert.

   > **Note**:
   >
   > An alert will be suppressed only if it matches the configured suppression criteria. You must select at least **1** suppression criteria (Event Computer, Event Source, Event ID, Extract token from description) from the list.

   > **Note**:
   >
   > In the case of the suppression criteria for **Extract token from description**, you can select the tokens for suppression, only if there are common tokens available in the configured rules for the alerts.

The following configuration for alert suppression restricts the number of alerts that can be generated within a 10-minute period to 5, with the remaining alerts being muted or suppressed when alert matches the Suppression Criteria.



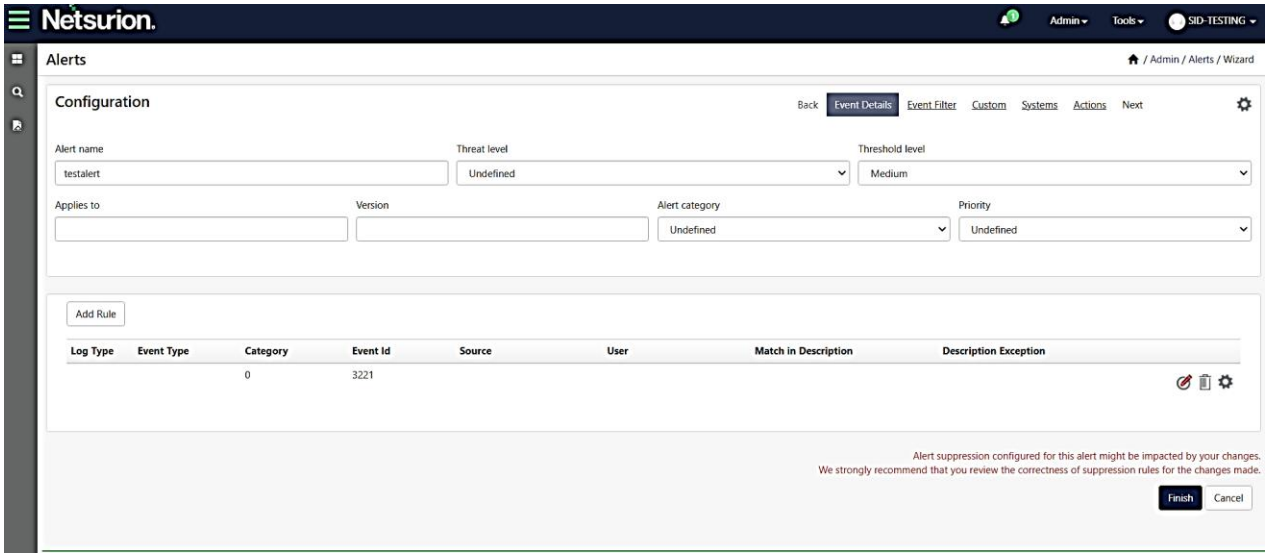
IMPORTANT:

- Alert Suppression supports Regular expressions or key-value pair token types, so that user can define them in advance alert configuration for events.
- If a common token type is found among the multiple alerts, then it displays the token details (as shown in the above image) to select the tokens for the suppression criteria. If no common tokens found, appropriate message will be displayed to configure the tokens.
- If the rule for an alert does not have a common token type, but is included for Alert Suppression, then that alert will not be suppressed.

Note:

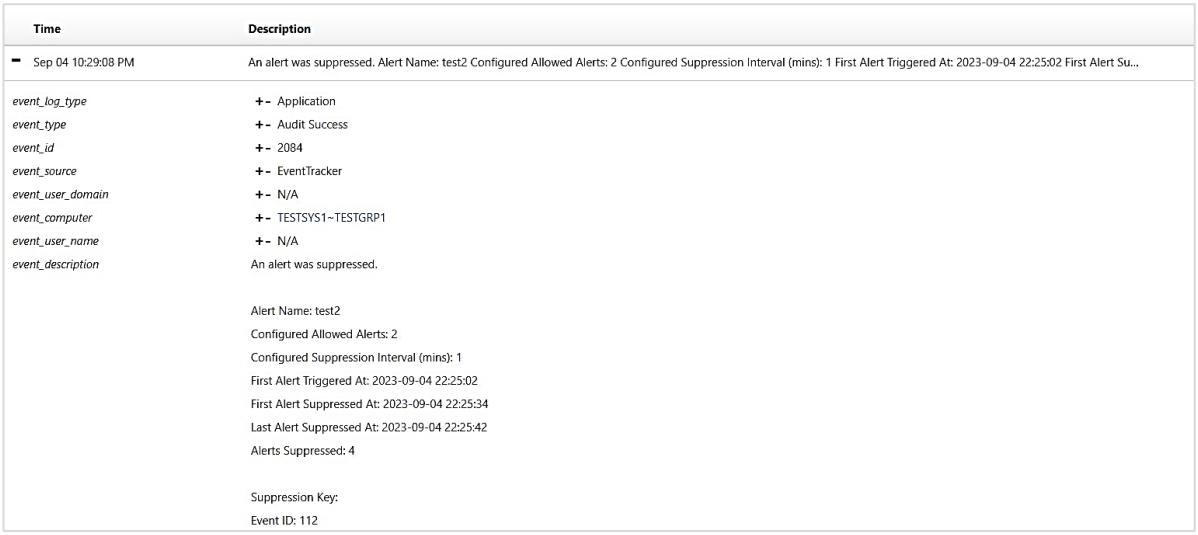
Editing the alert configuration may have an impact on the alert suppression if configured.

An information message stating '***Alert suppression configured for this alert might be impacted by your changes. We strongly recommend that you review the correctness of suppression rules for the changes made***.' will be displayed if the Alert suppression is enabled for a particular alert.



3 Audit Event, Alert, and Report

- Audit Event is generated for the supressed alerts which includes the details of the suppression.



Time	Description
− Sep 04 10:29:08 PM	An alert was suppressed. Alert Name: test2 Configured Allowed Alerts: 2 Configured Suppression Interval (mins): 1 First Alert Triggered At: 2023-09-04 22:25:02 First Alert Su...
event_log_type	+ - Application
event_type	+ - Audit Success
event_id	+ - 2084
event_source	+ - EventTracker
event_user_domain	+ - N/A
event_computer	+ - TESTSYS1~TESTGRP1
event_user_name	+ - N/A
event_description	An alert was suppressed. Alert Name: test2 Configured Allowed Alerts: 2 Configured Suppression Interval (mins): 1 First Alert Triggered At: 2023-09-04 22:25:02 First Alert Suppressed At: 2023-09-04 22:25:34 Last Alert Suppressed At: 2023-09-04 22:25:42 Alerts Suppressed: 4 Suppression Key: Event ID: 112

- An alert (inactive by default) and pre-defined report is added to the platform to notify the SOC when the alert suppression is done.
    - **Alert Name**: EventTracker: Alert(s) suppressed
    - **Report Name**: EventTracker - Alert suppressed events

Note:

Deprecated the global configuration for Alert suppression in the **Netsurion Open XDR** > **Manager** > **Configuration** page and the Alert based count in the **Alert Configuration**.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

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

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support