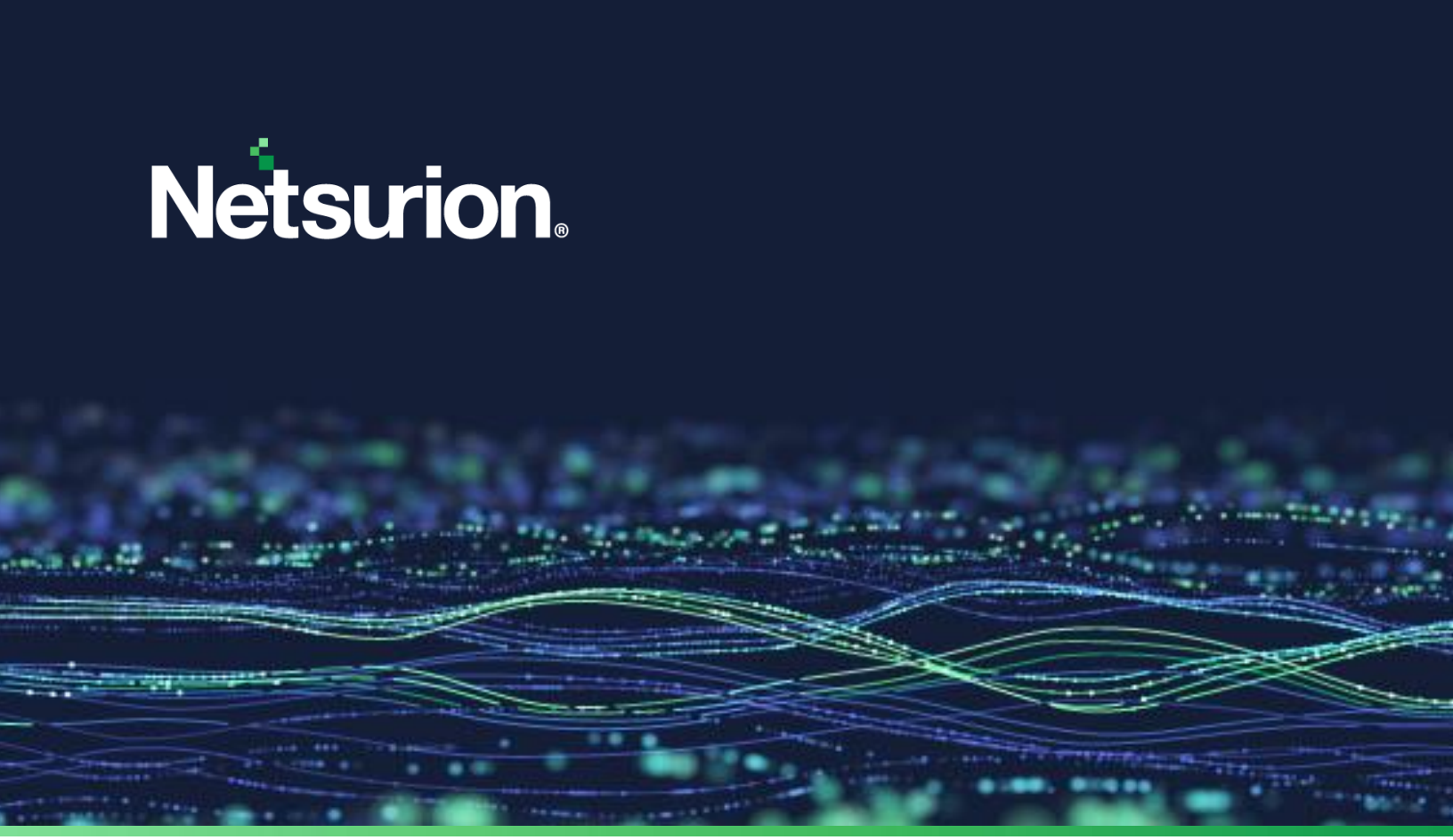


Feature Guide

Remedial Actions in Netsurion Open XDR

Publication Date

March 06, 2024

Abstract

The purpose of this document is to help users understand and execute remedial actions at the Manager Console system and Remote Agent systems.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.x.

Audience

This guide is for the administrators responsible for configuring remedial actions at the Manager Console system and Remote Agent systems.

Table of Contents

1 Overview

Alerting is a reactive mechanism against critical events collected in Netsurion Open XDR. The responsibility lies with the user to configure the required notifications like e-mail, beep, messages, or custom actions. If configured properly, the notification mechanism spontaneously notifies the users about the events that occurred in all monitored systems that include Windows, non-Windows, Agent based and Agent-less systems.

The notifications consist of a summary of the incident that helps users to investigate the root cause and explore efficient ways to take preventive and remedial measures. Upon receiving a notification, the security personnel should act promptly to avert any disastrous consequences. Netsurion Open XDR provides the necessary facilities to automate remedial actions at the Manager Console and remote systems as well, where Agents are deployed.

2 Remedial Actions

Remedial Actions are automated corrective actions taken to mitigate issues that occur at the Manager and Agent systems.

The remedial Actions help users in the following ways:

- Block unauthorized use of PC device access.
- Protect enterprise networks against threats posed by portable storage media.
- Enumerate and kill processes that cause havoc.
- Minimize maintenance effort.
- Maximize uptime.

2.1 Alert Actions

Upon receiving events that require user's attention, Open XDR can be configured to:

- Raise a beep sound from the PC speaker.
- Send an e-mail to one or more recipients.
- Send network messages to specific devices connected to the network.
- Forward events as Traps to specific devices.

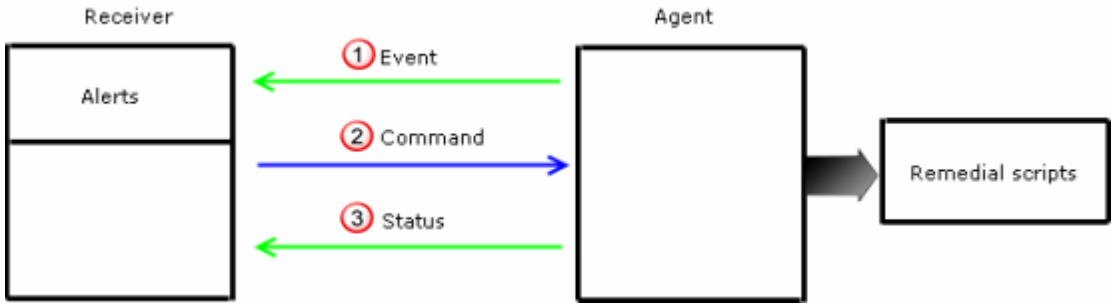
Apart from these traditional notifications to analyze the impact and severity of events, it can also be configured to execute remedial actions at the Manager Console. Through the "Agent side remedial action' feature, custom actions such as blocking USB ports or running scripts are provided.

a. Remote systems must have a Windows Operating system (presently non-Windows OS are not supported).
b. You cannot execute custom actions on Agentless systems.

c. If you execute scripts on multiple systems, the scripts should be present locally in each system in the Open XDR installation directory (…\Program Files\Prism Microsystems\EventTracker\Agent\Script).

d. Following are the custom actions that can be performed on the remote systems.

- Run Custom Script
- Restart Service
- Restart System
- Shutdown System
- Stop Service
- Terminate Process



2.2 Remedial Action Events

Remedial Action Events and Traps
Manager Side: This event is generated and logged at the Manager side.
Event ID = 2035 Event Type = Information Desc = Matched Remedial action request. Initiating Remedial Action Type: <n> on system <system>
Agent side: The Agent forwards these traps to the Manager as an acknowledgement.
Event ID = 3234 Usage = Remedial Events Event Type = Information Desc = Received Remedial action request for <Action Type> action.

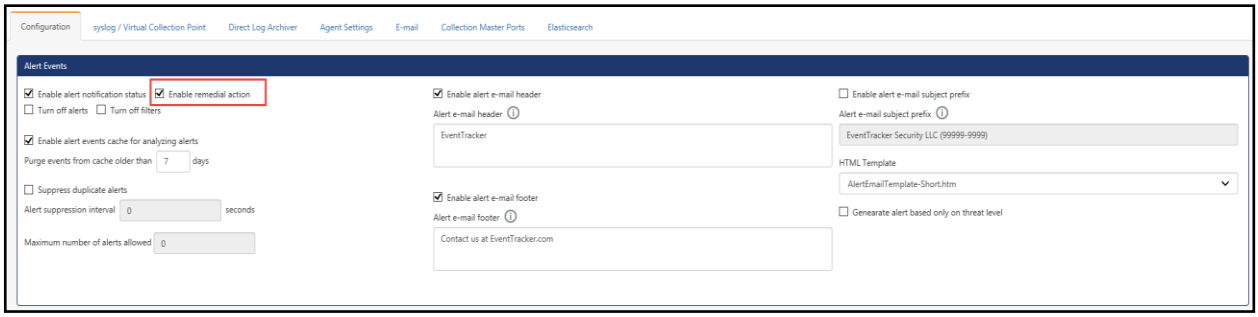
Event ID = 3235 Usage = Remedial Events Event Type = Information Desc = Successfully initiated <Action Type> action.
Event ID = 3236 Usage = Remedial Events Event Type = Error Desc = Failed to initiate <Action Type> Remedial action.

3 Enable Remedial Actions

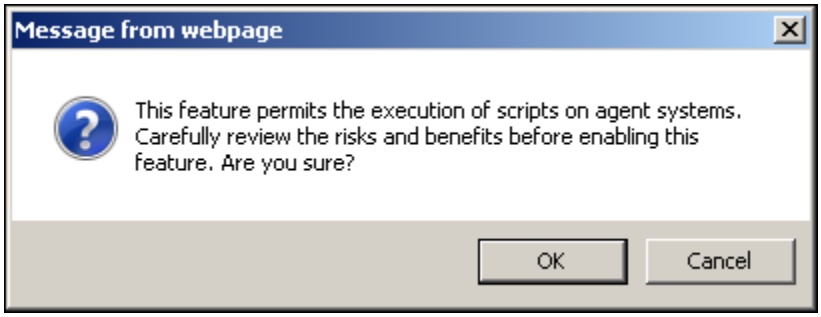
3.1 Manager

It is mandatory to enable remedial action at the Manager Console. Otherwise, you cannot execute the remedial action at the Agent systems.

1. Login to the Netsurion Open XDR web.
2. Click the **Admin** dropdown and then select the **Manager** option. The Manager Configuration window will be displayed.
3. Select the **Enable Remedial Action** checkbox.



4. A dialog box will be displayed as shown below:

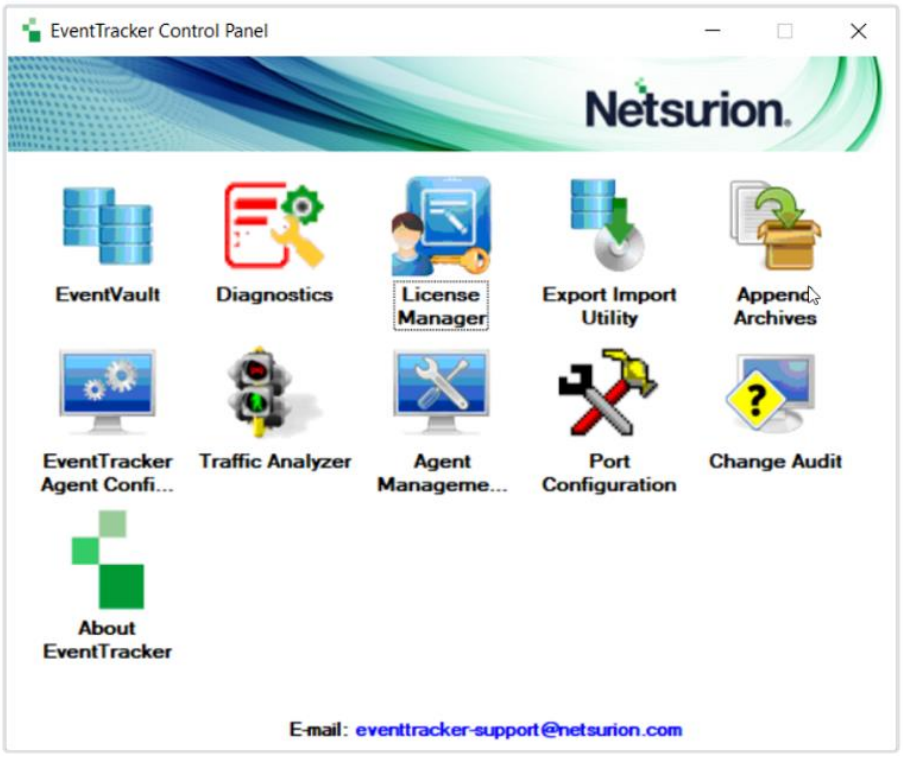


5. Click **OK.** Now click the **Save** button on the Manager Configuration window.

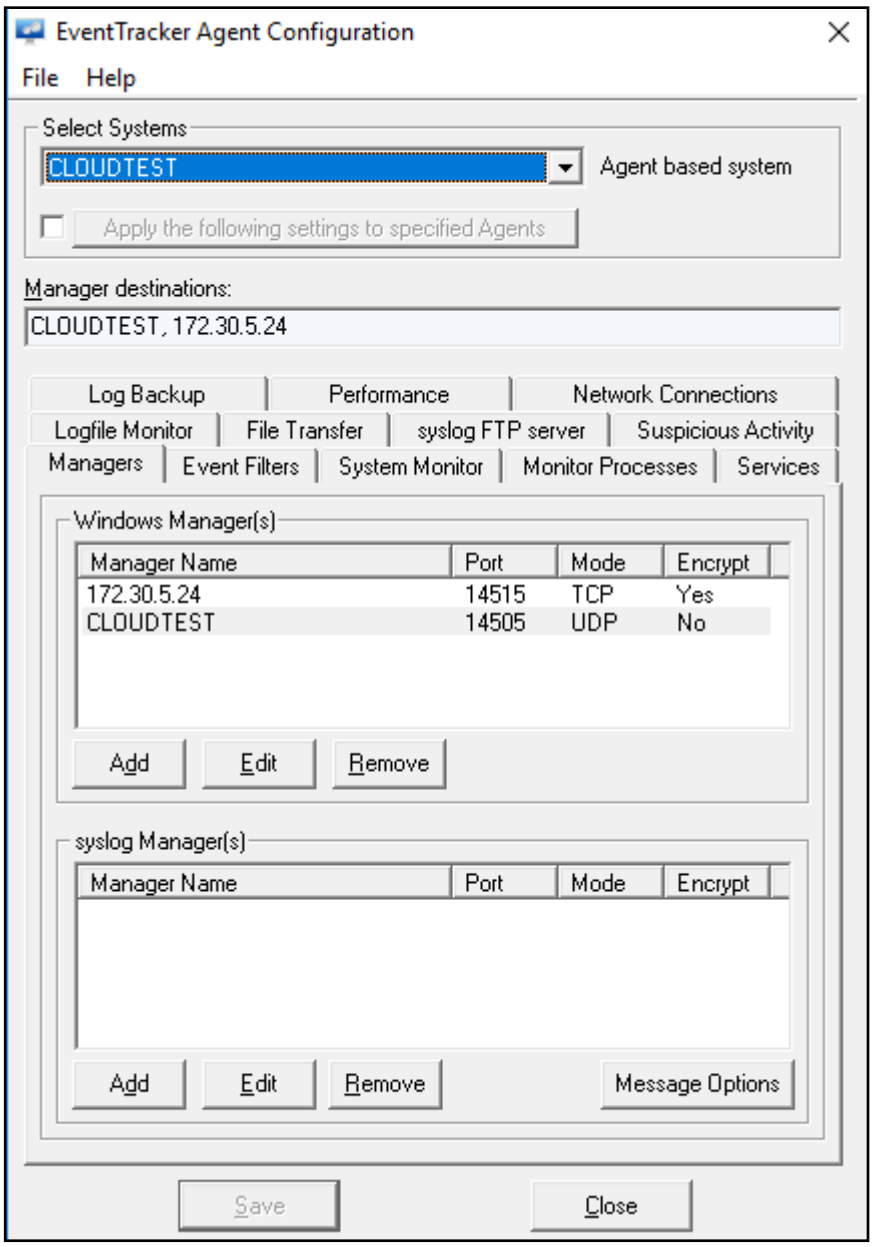
3.2 Agent

After enabling remedial actions at the Manager Console, you must individually enable Remedial Action on all the Agent systems. You can also include or exclude Agents from taking remedial actions.

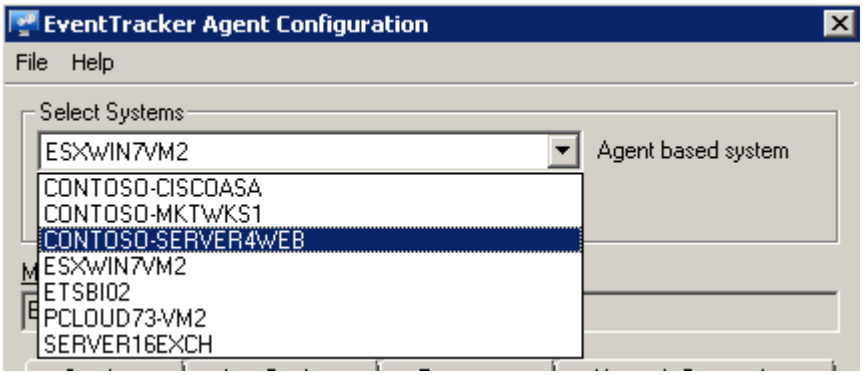
1. Open the Netsurion Open XDR Control Panel.
2. Double-click the Netsurion Open XDR Agent Configuration option.



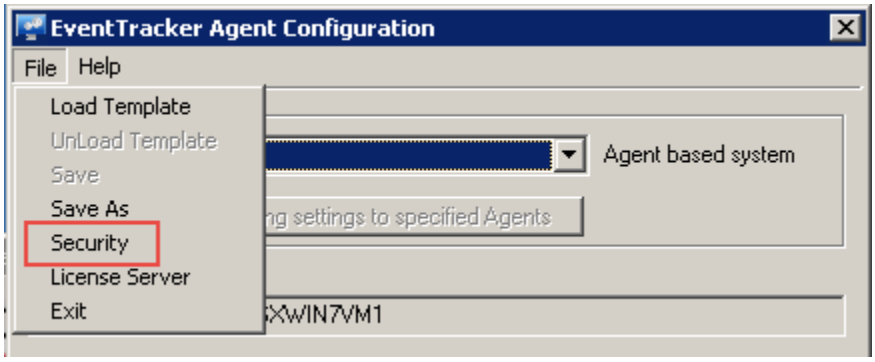
3. The Agent Configuration Window will be displayed as shown below:



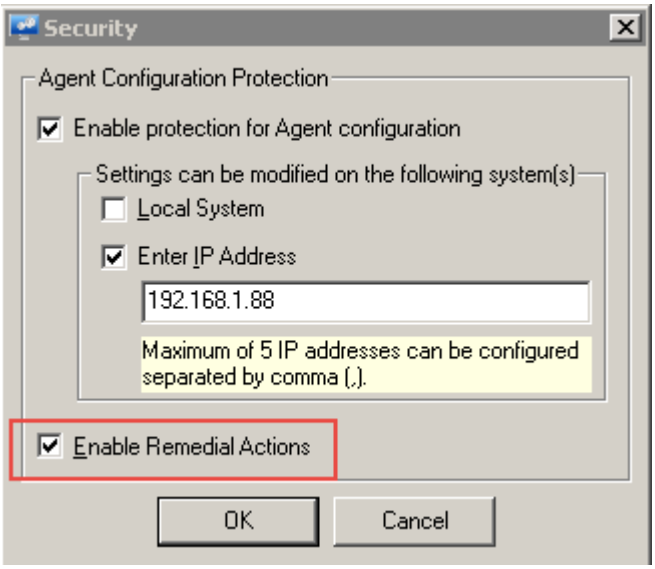
4. Select a system where you want to execute remedial actions from the **Select Systems** dropdown list.



5. Click the **File** menu and then select the **Security** option.



6. The Security window will be displayed as shown below:



7. Select the **Remedial Action** checkbox.
8. Click **OK**.
9. Click **Save,** and then click **Close** in the **Netsurion Open XDR Agent Configuration** window.

4 Configure Remedial Actions

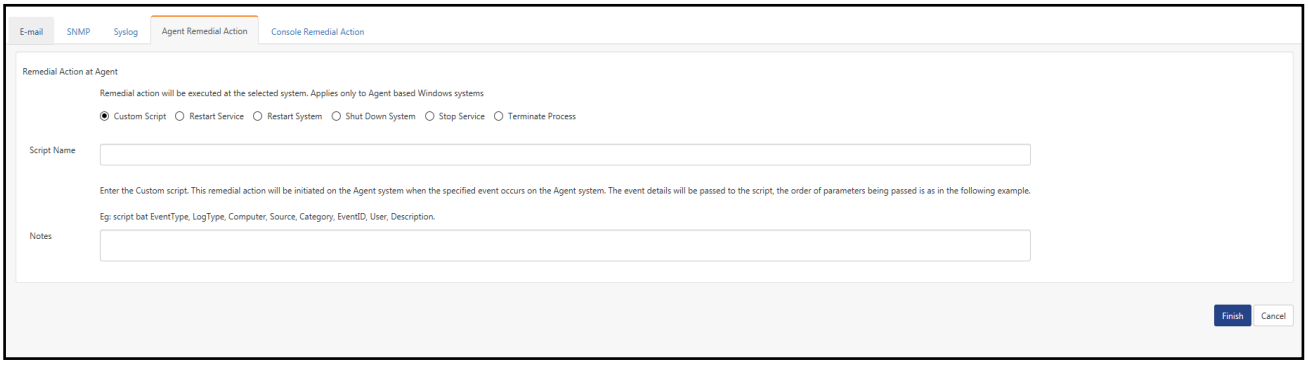
Though Netsurion Open XDR is equipped with predefined alerts that are applicable to all monitored systems irrespective of Operating system and mode of monitoring (Agent based or Agent less), to get the alert notification messages, you need to explicitly configure the alert actions. While configuring alert actions, it is user's choice to include/exclude systems. The same rule applies to user-defined alerts. Note that remedial actions can be executed only on systems where the Netsurion Open XDR Agent has been deployed.

Excluding systems for alert actions doesn't mean that they are excluded from monitoring.

4.1 Agent Remedial Actions

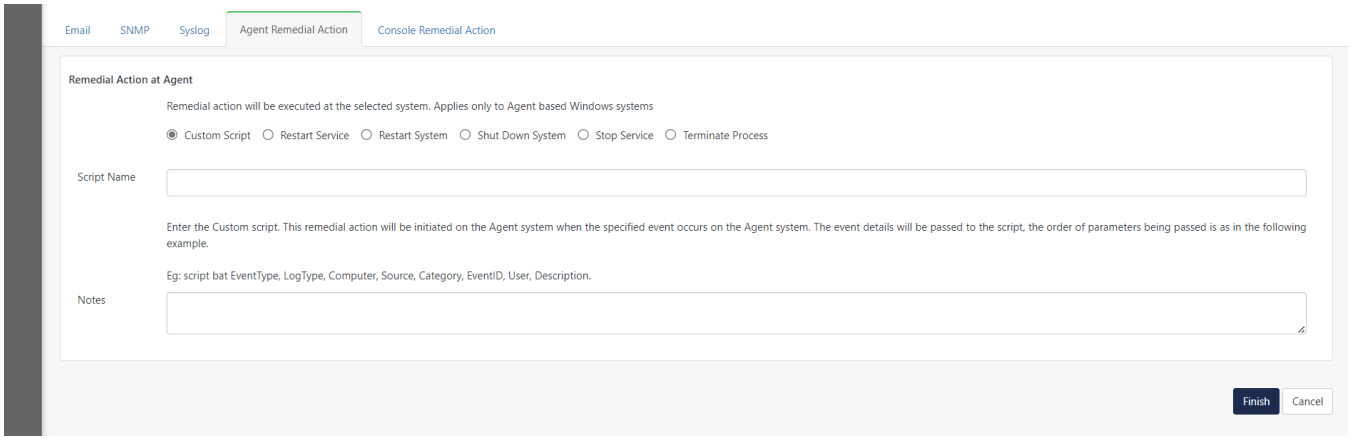
In the Netsurion Open XDR web console, click the **Admin** dropdown and then select the **Alerts** option. The **Alert Management** page will be displayed.

- Select an Alert.
- Select the checkbox against the selected Alert under **Remedial action at Agent**.
  (OR)
- Double-click an Alert. The Alert Configuration page will be displayed.
- Click the **Action** option on the right side, and select the **Agent Remedial action** tab. The Agent dialog box will be displayed as shown below:

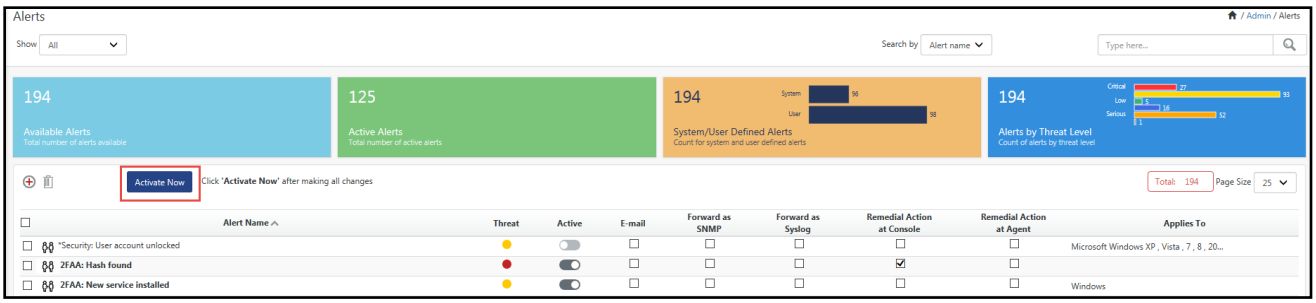


Field	Description
Custom Script	Type the name of the script in the **Script Name** field. Script files are stored in the default Netsurion Open XDR Agent installation path typically …\Program Files\Prism Microsystems\EventTracker\Agent
Restart Service	Type the name of the service that you want to restart in the **Service Name** field.
Restart System	Netsurion Open XDR disables the **Script Name** field.
Shut Down	Netsurion Open XDR disables the **Script Name** field.
Stop Service	Type the name of the service that you want to stop in **the Service Name** field.
Terminate Process	Netsurion Open XDR enables this option only when you set an alert for Events 3217, 3218, 3221, 3223, and 3226.

Note:
Provide the appropriate description in the Notes field for future reference.



1. Select an appropriate option and then click **OK**.
2. Now, click the **Activate Now** button on the Alert Management page.



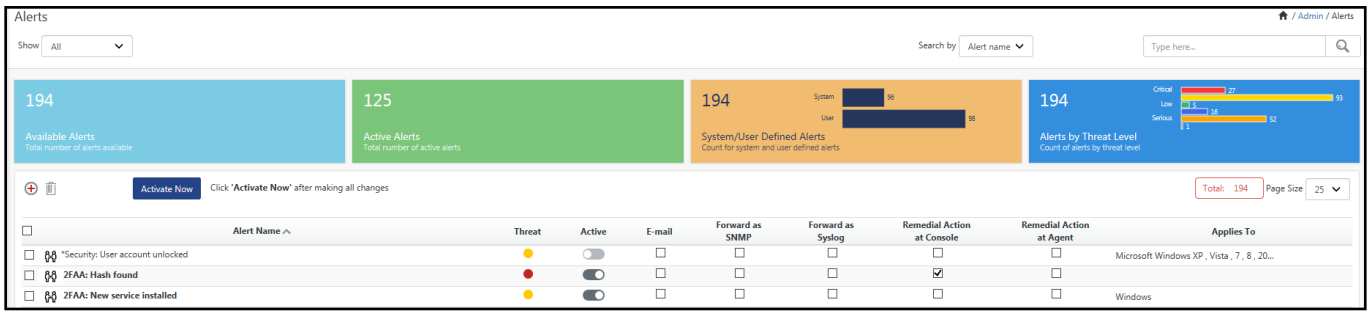
3. Remedial actions will be initiated only on systems where Remedial Action is enabled. You can also exclude systems where remedial actions have been enabled.

4.2 Console Remedial Actions

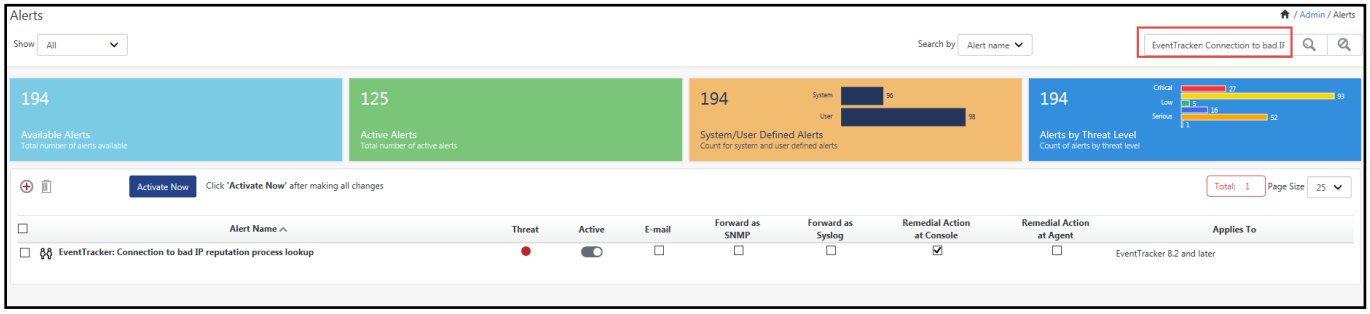
This option enables you to configure custom actions to be executed on receipt of an event at the Manager system.

For example, if you want to execute the Console remedial Action to the **Bad Ip reputation-process lookup** alert:

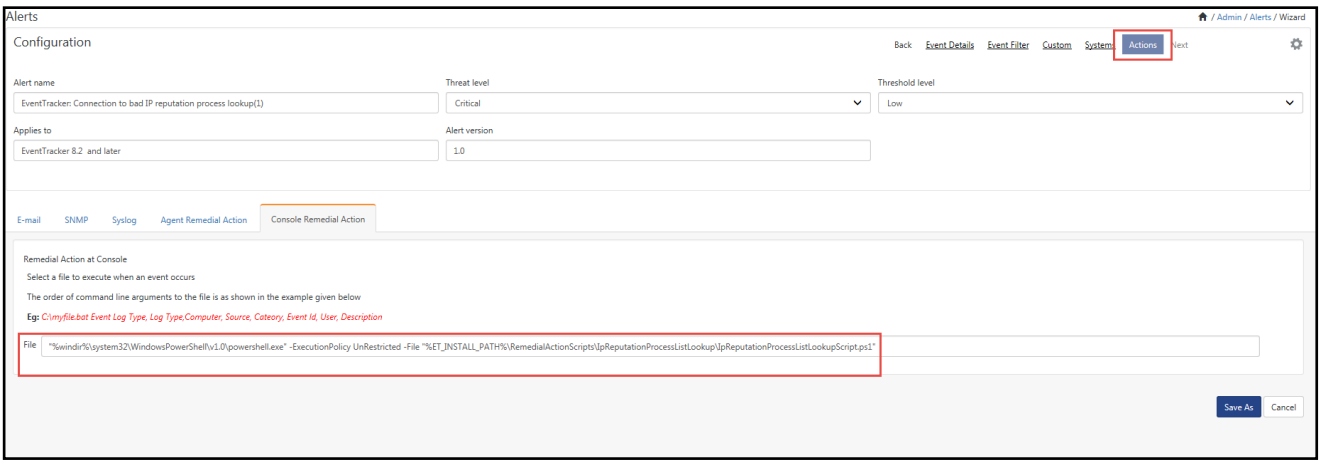
1. Click the **Admin** dropdown and then select the **Alerts** option. The Alert Management page will be displayed.



2. Search the Alert in the search box at the right-side of the interface.



3. Select the Alert (**Connection to bad IP reputation process lookup**), and then select the checkbox against the selected Alert under **Remedial action at Console**.
   (OR)
   Double-click the alert and click the **Action** option in the Alert configuration page. Now select the **Console Remedial Action** tab.
4. The Remedial Action Console window will be displayed as shown below:

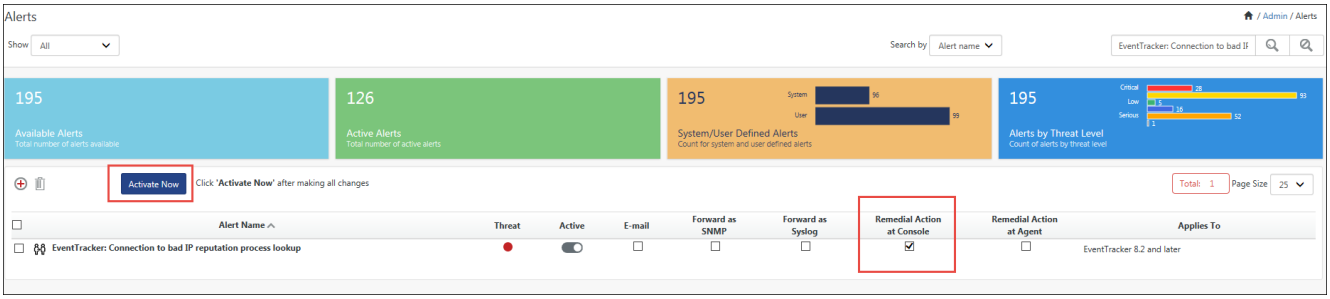


5. Enter the file name with the mentioned path and verify the appropriate script path to execute when an event occurs.

Note:
If you have stored the script in a different path, replace it with the path where you have stored the script.

6. Check the appropriate script path to execute when an event occurs.
7. Click **Finish**.

8. Now, click the **Activate Now** button after confirming all the changes made and activate the alert.



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