

# How Alerting Works in Nagios Network Analyzer 2026

## Purpose

This document will help you understand how alerting works in Nagios Network Analyzer 2026, and how to set alerts up.

## Prerequisites

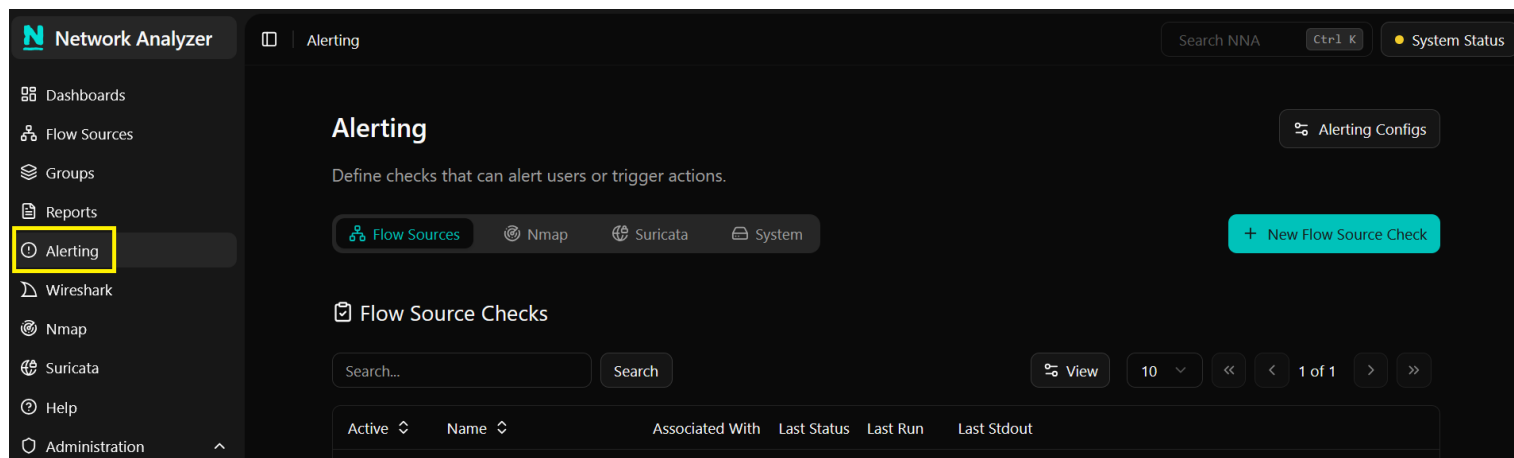
You will need an existing Source to be able to create checks in Nagios Network Analyzer. Information about this can be found in the following documentation:

[Understanding Sources And Sourcegroups In Network Analyzer](#)

## Alerting In Nagios Network Analyzer

In Nagios Network Analyzer, select **Alerting** from the side navigation bar.

This is the central location to manage and create alerts.



There are multiple alert methods available in Nagios Network Analyzer.

- **Nagios / NRDP** - Send an alert to your Nagios XI or Nagios Core server using NRDP
- **SNMP Receivers** - SNMP Traps can be sent to other applications using the Nagios MIB
- **Commands** - Run a custom command and pass variables to the command
- **Email Users** - Email Nagios Log Server users

# How Alerting Works in Nagios Network Analyzer 2026

For detailed guidance on Nagios / NRDP and the Network Analyzer Wizard, refer to the following comprehensive documentation:

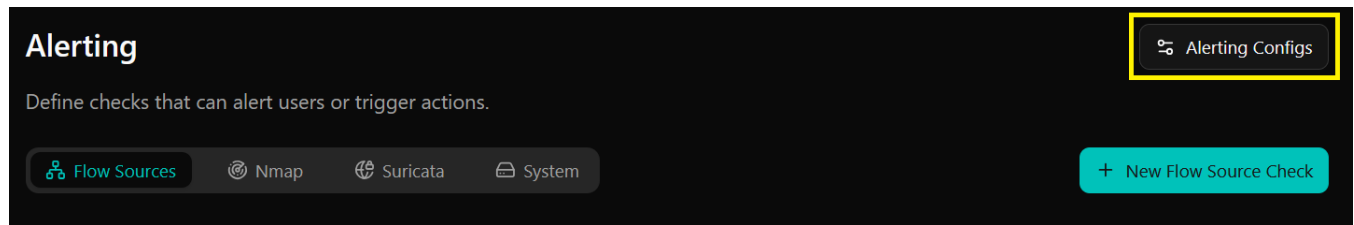
[Integrating Nagios Network Analyzer With Nagios XI](#)

The remainder of this documentation will focus on the **Commands**, **SNMP Receivers**, and **Email Users** functionality. The **Commands** and **SNMP Receivers** alert methods require you to define the settings before you can create an alert. These settings are explained first.

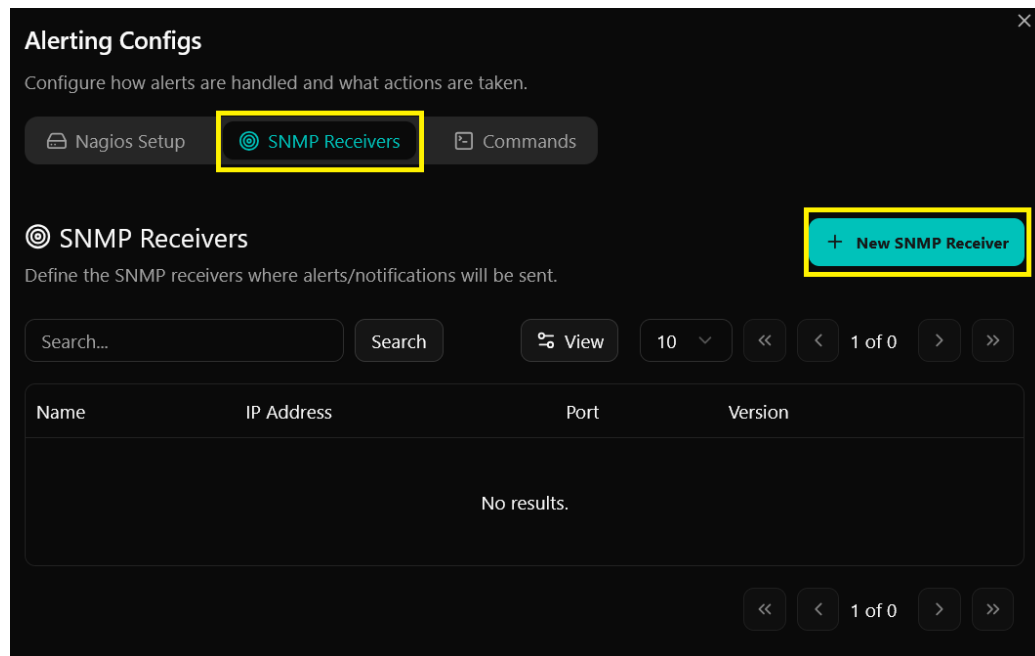
## SNMP Receivers

To be able to send alerts to a SNMP Receiver you need to define the details of the receiver.

1. On the Alerting page, click **Alerting Configs** button to the right:



2. Click the middle tab “SNMP Receivers”, then click the blue + **New SNMP Receiver** button:

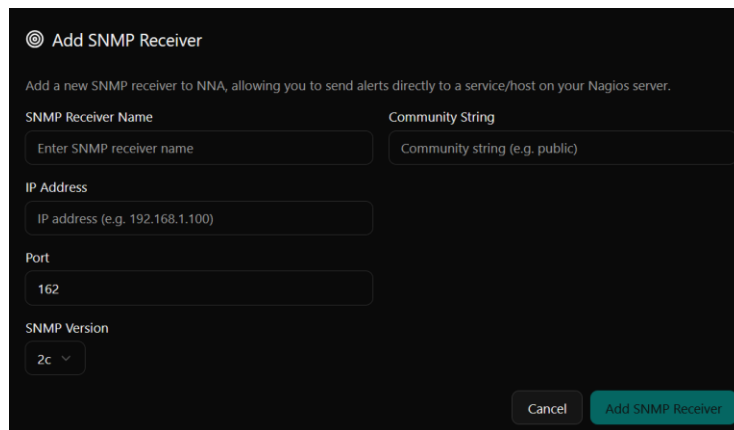


# How Alerting Works in Nagios Network Analyzer 2026

3. You will need to provide the following information:

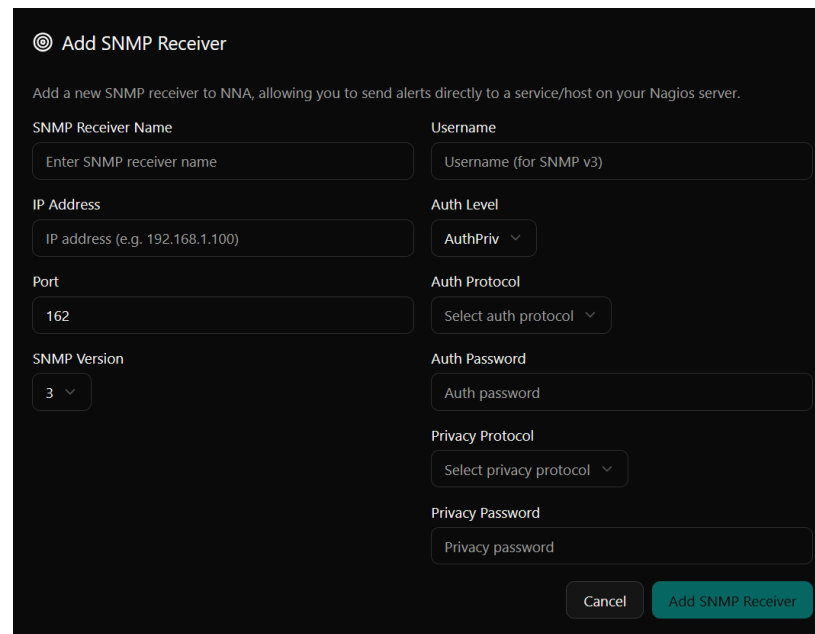
- **SNMP Receiver Name:** a friendly name for the SNMP Trap receiver.
- **IP Address and Port:** The IP address that is receiving traps. Could be an NSTI server or a Nagios XI server that is listening for incoming traps. You also need to define the **Port** the traps can be sent on (162 is the standard default).
- **SNMP Version:** The version of SNMP you are using; changing the version will change the trap security options available.

## ▪ Version 2c



The screenshot shows the 'Add SNMP Receiver' form for Version 2c. The form has a title 'Add SNMP Receiver' with a target icon. Below the title is a description: 'Add a new SNMP receiver to NNA, allowing you to send alerts directly to a service/host on your Nagios server.' The form contains the following fields: 'SNMP Receiver Name' (text input with placeholder 'Enter SNMP receiver name'), 'Community String' (text input with placeholder 'Community string (e.g. public)'), 'IP Address' (text input with placeholder 'IP address (e.g. 192.168.1.100)'), 'Port' (text input with value '162'), and 'SNMP Version' (dropdown menu with value '2c'). At the bottom right are 'Cancel' and 'Add SNMP Receiver' buttons.

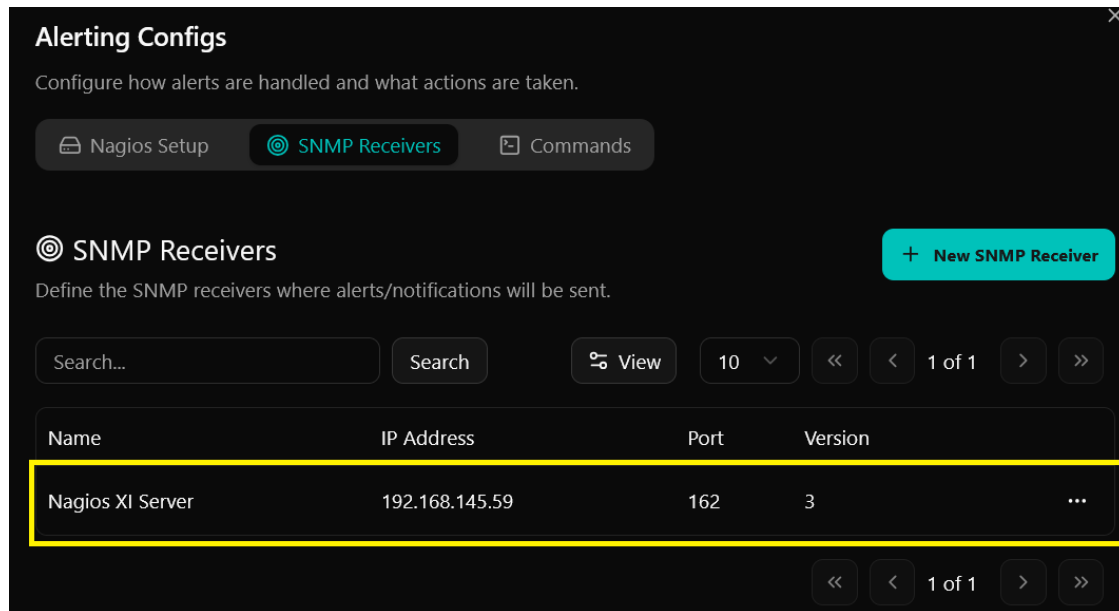
## ▪ Version 3



The screenshot shows the 'Add SNMP Receiver' form for Version 3. The form has a title 'Add SNMP Receiver' with a target icon. Below the title is a description: 'Add a new SNMP receiver to NNA, allowing you to send alerts directly to a service/host on your Nagios server.' The form contains the following fields: 'SNMP Receiver Name' (text input with placeholder 'Enter SNMP receiver name'), 'Username' (text input with placeholder 'Username (for SNMP v3)'), 'IP Address' (text input with placeholder 'IP address (e.g. 192.168.1.100)'), 'Auth Level' (dropdown menu with value 'AuthPriv'), 'Port' (text input with value '162'), 'Auth Protocol' (dropdown menu with value 'Select auth protocol'), 'SNMP Version' (dropdown menu with value '3'), 'Auth Password' (text input with placeholder 'Auth password'), 'Privacy Protocol' (dropdown menu with value 'Select privacy protocol'), and 'Privacy Password' (text input with placeholder 'Privacy password'). At the bottom right are 'Cancel' and 'Add SNMP Receiver' buttons.

# How Alerting Works in Nagios Network Analyzer 2026

4. Once you have filled in the information, Click **Add SNMP Receiver** button to define the SNMP Receiver. The new command will appear in the list under SNMP Receivers.



Proceed to the [Creating A Check](#) section in this document to define a check that uses the SNMP Receiver.

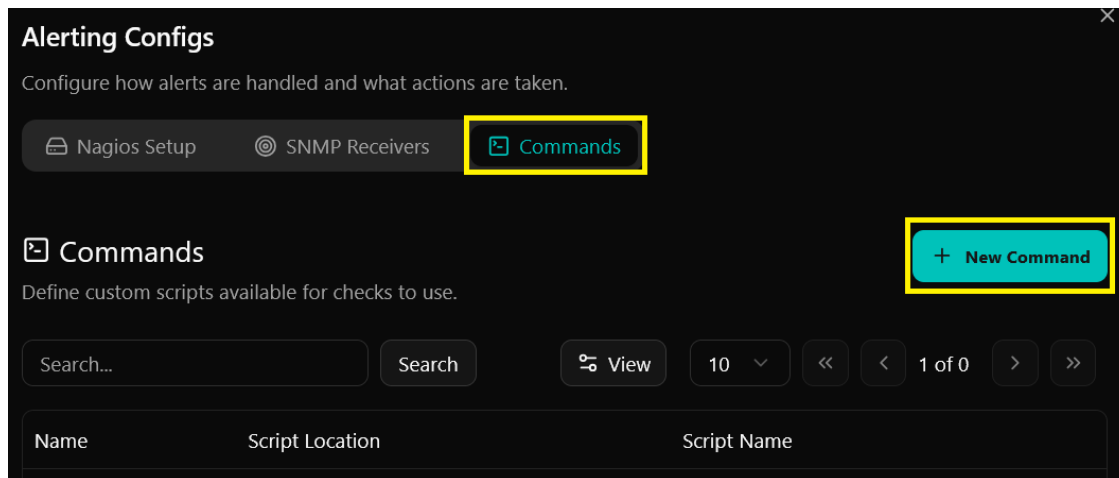
## Commands

Nagios Network Analyzer allows you to execute a command as an alerting method. This could be a binary command such as `/usr/sbin/sendmail` or your own custom script. If you use your own script you will need to place it somewhere on the system, such as `/usr/local/nagiosna/scripts/`.

Once you've decided on the location of the command you need to define how Nagios Network Analyzer will use it.

1. On the **Alerting Configs** page, click the **Commands** tab and then click the **+New Command** button.

# How Alerting Works in Nagios Network Analyzer 2026



2. The **Add Command** box will appear.

- Provide a friendly **Command Name**.
- Define the **Script Location** and **Script Name**.
- Define the **Passed Arguments**. This is how you send data to the command, there are Nagios Network Analyzer macros available, and they are explained at the bottom of the modal.
- Once you've populated all the fields, click the **Add Command** button.

**Add Command**

Add a new command to NNA, allowing you to send alerts directly to a service/host on your Nagios server.

Command Name  
Execute Automation Chain

Script Location  
/usr/local/nagios/scripts

Script Name  
execute\_automation.sh

Passed Arguments  
"%sourcename%" "%state%"

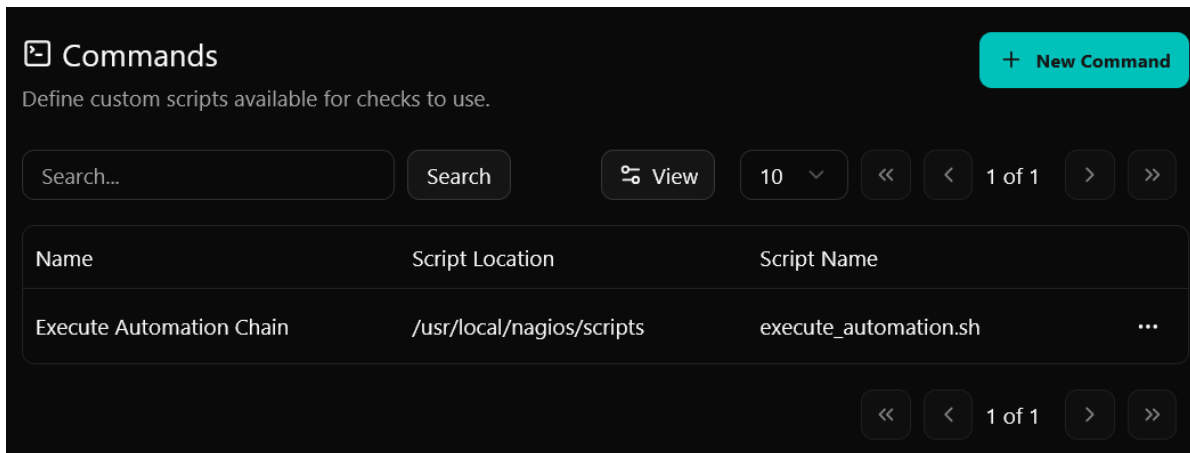
You can pass some basic macros to the script via arguments that will be auto-populated when the script is executed.

- %sourcename% - the name of the source that is being alerted on
- %sourcegroupname% - the name of the source group that is being alerted on
- %state% - the state of the check
- %returncode% - the return code of the check
- %output% - the output of the check

Cancel Add Command

# How Alerting Works in Nagios Network Analyzer 2026

3. The new command will appear in the list on the **Commands** tab.



You can now proceed to the [Creating A Check](#) section in this document to define a check that executes the command.

## Email Users

To be able to send email alerts in Nagios Network Analyzer you will need to create Nagios Network Analyzer user accounts with their email addresses correctly defined. The following guides provide further details on this part of the setup:

[Understanding Email Sending in Nagios Network Analyzer](#)

[Managing Users in Nagios Network Analyzer](#)

Once you have done this proceed to the [Creating A Check](#) section in this document to define a check that sends emails.

# How Alerting Works in Nagios Network Analyzer 2026

## Creating A Check

Checks are how alerts are triggered. The following example creates a check that will notify if a source has no flow data received on the port that the flow data is being received on. After the example, we'll also cover the [Nmap](#) and [Suricata](#) alert options.

On the **Alerting** page, click the **Flow Sources** tab and then click the **+New Flow Source Check** button.



### Step 1 – Select Source

Enter a friendly name for the check for management and organizational purposes. The name can only contain whitespaces and alphanumeric characters.

Select **Flow Source** or **Flow Source Group**. This defines the source/sources the check will get values from.

Click the **Next** button to proceed.

A screenshot of the "Add Flow Source Check" form, specifically Step 1 - Select Source. The form has a dark background. At the top left, there is a checkbox labeled "Add Flow Source Check" which is checked. At the top right, the text "Step 1 - Select Source" is displayed. Below the checkbox, a subtitle reads "Select the flow source for the check. You can select a flow source group, or a single flow source." The form contains a "Name" field with the text "Flow Data 9914" entered. Below this is a "Check Association" section with two radio buttons: "Flow Source" (which is selected) and "Flow Source Group". Below the radio buttons is a dropdown menu showing "SP Firewall". At the bottom right of the form, there are two buttons: "Cancel" and "Next".

# How Alerting Works in Nagios Network Analyzer 2026

## Step 2 – Select Criteria

☒ Add Flow Source Check Step 2 - Select Criteria

Select the criteria you would like to check for. You can configure things like a single port, IP, or network.

Metric  
Bytes ▾

Force Check on Creation ☐

Warning Threshold  
1:

Critical Threshold  
1:

Queries

Destination ▾ Port ▾ ☒ is ☐ is not 9914

and

Cancel Previous Next

**Metric:** Choose the metric to check against. If you want a packet count, choose **Packets**. If you want total bytes, choose **Bytes**. There are multiple traffic dimensions available, and this setting specifies which one will be checked.

**Warning threshold is / Critical threshold is:** After extracting a value from the selected metric, Network Analyzer evaluates it against these thresholds to determine if the state is **WARNING**, **CRITICAL**, or **OK**. In this example, setting both thresholds to 1 : means that if less than 1 is received, the check will enter a **CRITICAL** state, indicating that no flows were received.

More detailed information on thresholds is explained in the [Nagios Threshold Values](#) section of this document.

The bottom half of **this Step** is how you filter what data the check is looking at, as this allows granularity.

In this example, **Flows** is the type of traffic being analyzed. The filter criteria used is:

- **Destination:** Specifies the direction of the flow traffic being examined.
- **Port:** This check is testing to make sure flow data is actually being received, seeing as the flow data is received on a port then this makes it easy to check.
- **is:** Defines the operation; in this case, verify that the **destination port is 9914**.
- **9914:** The specific port number being monitored.



# How Alerting Works in Nagios Network Analyzer 2026

Based on those selections, if no flow data is received it will be in a **CRITICAL** state, otherwise it will be **OK**.

You can specify as many of these filters as you would like by clicking the **and** button. This will add a new box where you can specify additional filters. Please note that it is a Boolean AND, where the traffic must meet all specifications that are chosen for the check to be used.

Click the **Next** button to proceed.

## Step 3 – Select Alerting Methods

Here, you choose the alerting method. The following screenshots display the available options. You can select multiple methods across different tabs, for example, sending Emails, and sending an SNMP trap, and executing a Command simultaneously.

Click the **Create** button to create the alert.

**Add Flow Source Check** Step 3 - Select Alerting


Select how you would like to be notified of this check. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

**User** Nagios Snmp Receiver Command

- ☒ nagiosadmin
- ☒ docadmins

Cancel Previous Create

# How Alerting Works in Nagios Network Analyzer 2026

 Add Flow Source Check

Step 3 - Select Alerting

Select how you would like to be notified of this check. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

User

Nagios

Snmp Receiver


Command

☒ SNMP Receiver Example

Cancel

Previous

Create

 Add Flow Source Check

Step 3 - Select Alerting

Select how you would like to be notified of this check. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

User

Nagios

SNMP Receiver

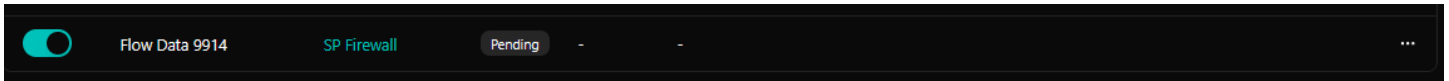
Command

Select/Unselect All

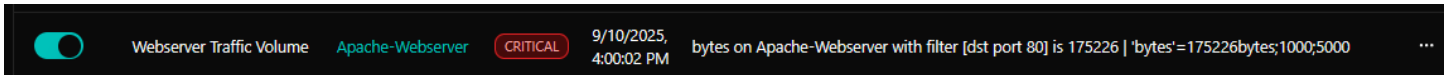
☒ Execute Automation Chain

# How Alerting Works in Nagios Network Analyzer 2026

The check will be created and will appear on the screen in a pending state:



Here is an example of a check in a **CRITICAL** state:



The checks run **every five** minutes, and it's important to understand that each time the check runs, it will send a notification to your alerting method.

## Check Actions

There are some actions available for the checks you have defined. On the **Alerting** page, click the **Actions** icon (three horizontal dots) on the line of the alert:

### Run Check

Run the check immediately.

### View / Edit

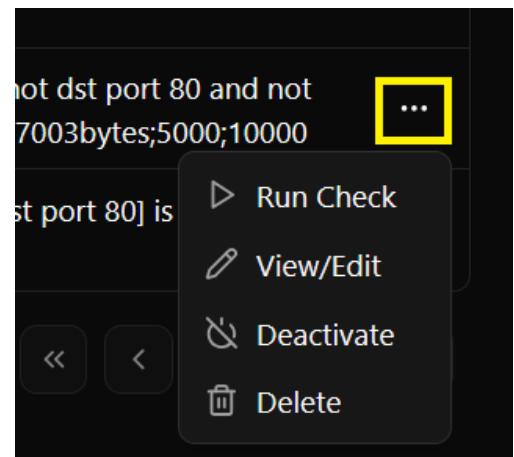
Review an existing check and make any changes required.

### Deactivate

Deactivate the check without deleting it for future checks.

### Delete

Delete the check, no more alerts will be sent.



## Nagios Threshold Values

Nagios Thresholds can be complicated to initially understand, but once you grasp them, they can be very powerful. Documentation on Nagios thresholds is available here:

<https://nagios-plugins.org/doc/guidelines.html#THRESHOLDFORMAT>

The Nagios Threshold standards were designed with many different use cases, including those where negative numbers are valid values. However, in the case of Nagios Network Analyzer, the alert value being tested will always be 0 or greater (no negative numbers are involved).

# How Alerting Works in Nagios Network Analyzer 2026

## Nmap Alerts

Nmap alerts enable you to monitor the number of open or closed ports found by a Scheduled scan. You can learn more about installing and using Nmap in Network Analyzer 2026 here:

[Using Nmap with Network Analyzer 2026](#)

To begin, select the Nmap tab in **Alerting**, then click **+ New Nmap Check**.

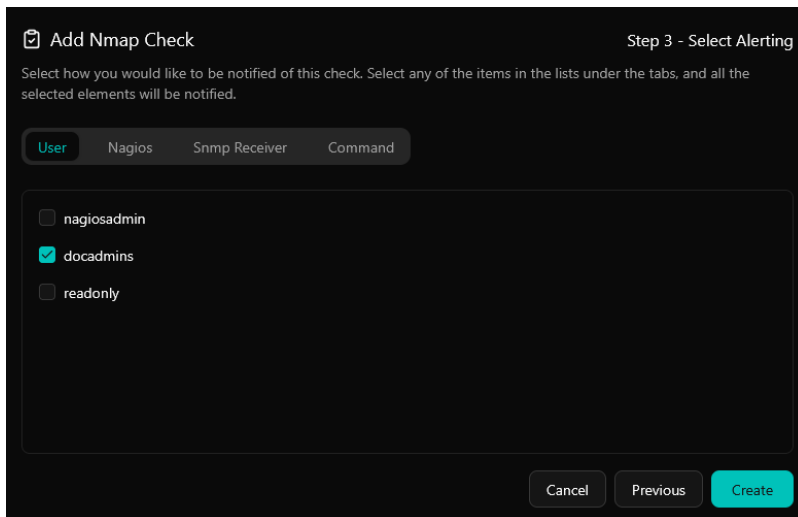


Next, input a friendly **Name** for the alert, and choose a Scheduled Scan from the dropdown, then click **Next**.

Now choose either Ports Open or Ports Closed from the **Metric** dropdown, and enter your Warning and Critical Threshold values, then click **Next**.

# How Alerting Works in Nagios Network Analyzer 2026

Finally, choose your notification options, and click **Create**.



**Add Nmap Check** Step 3 - Select Alerting

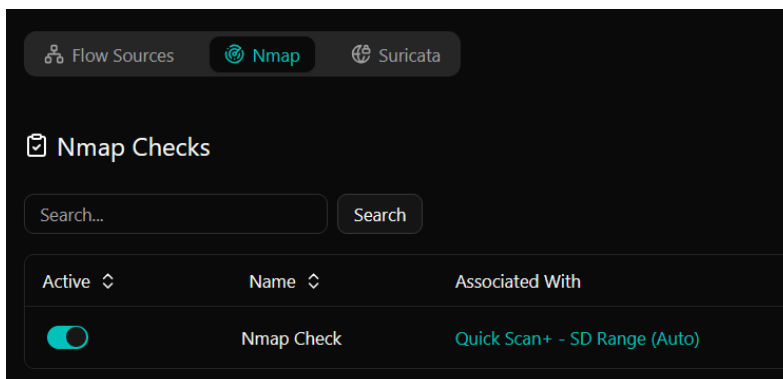
Select how you would like to be notified of this check. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

**User** Nagios Snmp Receiver Command

- ☐ nagiosadmin
- ☒ docadmins
- ☐ readonly

Cancel Previous Create

Your Nmap check will now appear in the **Nmap** tab of the **Alerting** menu.



Flow Sources **Nmap** Suricata

**Nmap Checks**

Search... Search

Active	Name	Associated With
<input checked="" type="checkbox"/>	Nmap Check	Quick Scan+ - SD Range (Auto)

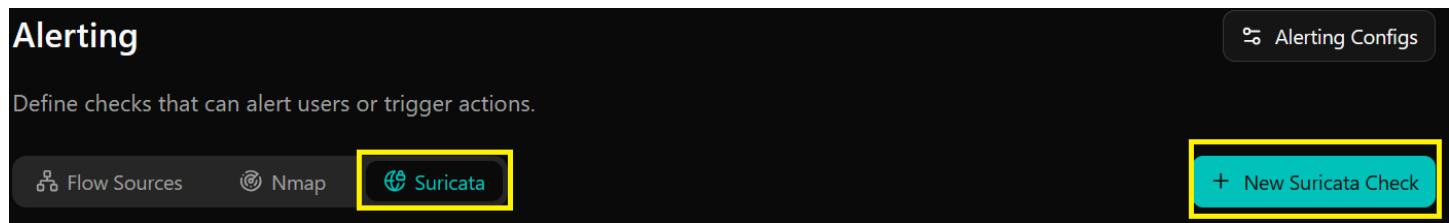
## Suricata Alerts

Suricata alerts enable you check for the presence of certain Signature IDs in your Suricata Alerts. You can learn more about installing and using Suricata in Network Analyzer 2026 here:

[Using Suricata with Network Analyzer 2026](#)

To begin, select the Suricata tab in **Alerting**, then click **+ New Suricata Check**.

# How Alerting Works in Nagios Network Analyzer 2026

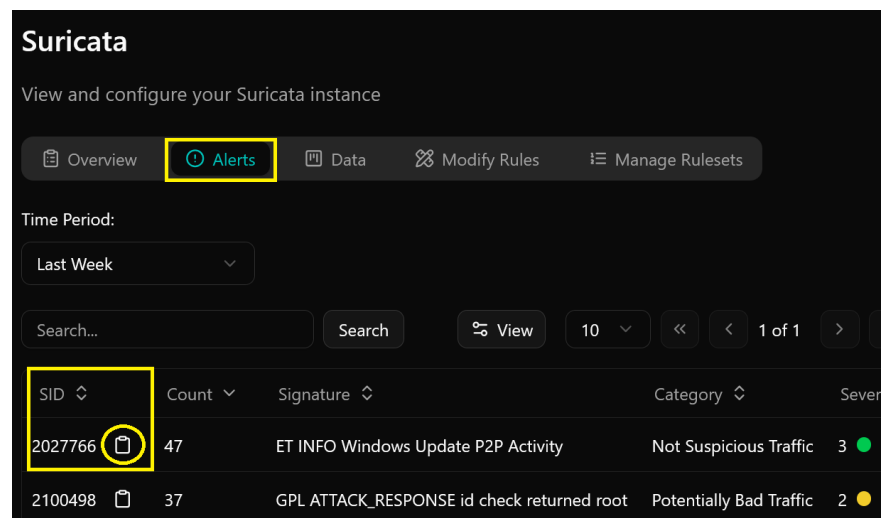


In the first page of the **Add Suricata Check** dialog, you'll define a friendly **Name** for the alert, choose the **Signature ID** (SID, see note below) to check for, and define your **Threshold** values, **Check Frequency**, and **Lookback Period** (how far to look back in your Suricata data for matching results).

The screenshot shows the 'Add Suricata Check' dialog, Step 1 - Select Criteria. The dialog has a title bar with a checkmark icon and the text 'Add Suricata Check'. Below the title bar, it says 'Step 1 - Select Criteria' and 'Select the criteria you would like to check for.' The form contains several fields: 'Name' (SID 2100498 - root events), 'Check On' (Signature ID), 'Metric' (Alert Count), 'Check Frequency' (Every 5 Minutes), 'Signature ID' (2100498), 'Warning Threshold' (1), 'Critical Threshold' (3), and 'Lookback Period' (1 Day). At the bottom right, there are 'Cancel' and 'Next' buttons.

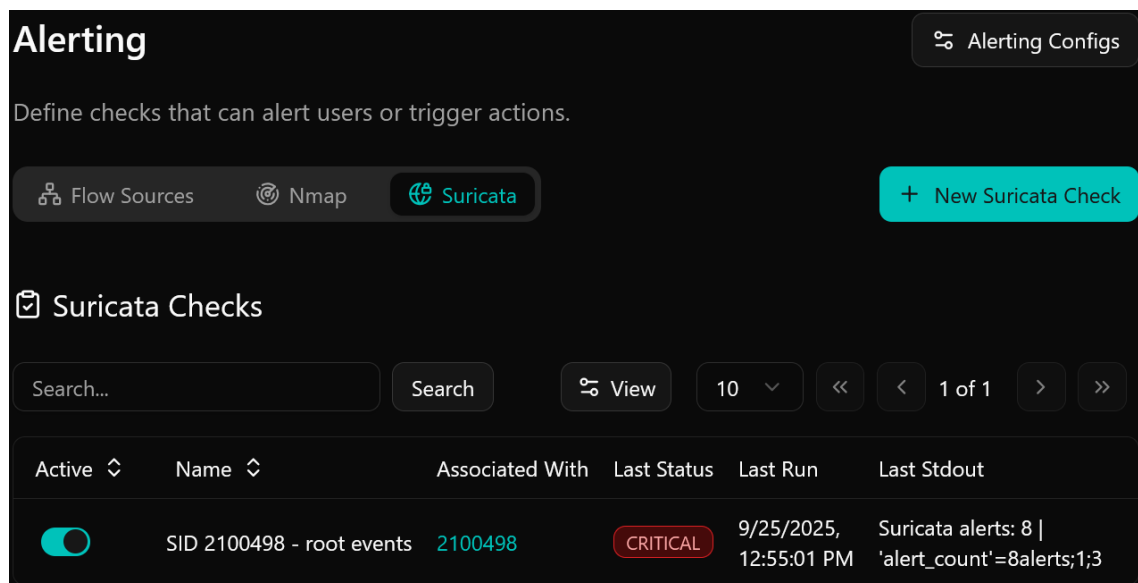
## Finding Alert SIDs

You can easily find the SID of your Suricata Alerts in the **Alerts** tab of the Suricata menu. Click the clipboard icon to copy the SID.



# How Alerting Works in Nagios Network Analyzer 2026

Finalize your Suricata alert by choosing your notification methods, then click **Create**. Your new Suricata check will now appear in the Suricata tab of the Alerting menu.



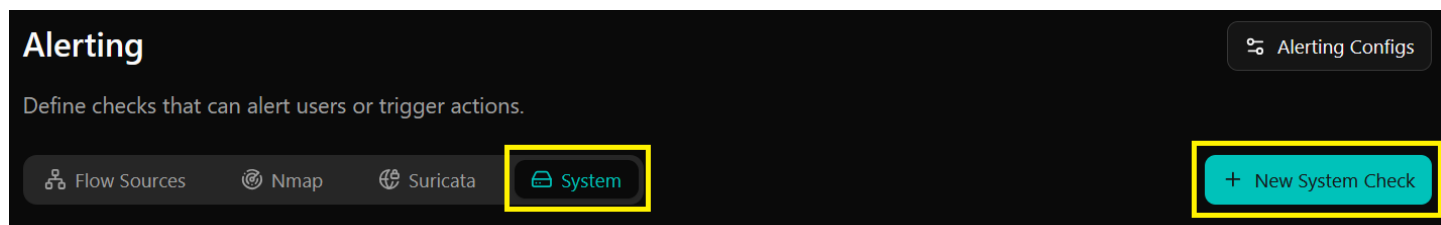
The screenshot shows the 'Alerting' section of the Nagios Network Analyzer interface. At the top, there's a header 'Alerting' with a sub-header 'Alerting Configs'. Below this, a description states 'Define checks that can alert users or trigger actions.' A navigation bar contains tabs for 'Flow Sources', 'Nmap', and 'Suricata', with a '+ New Suricata Check' button. The 'Suricata Checks' section features a search bar, a 'Search' button, a 'View' button, and pagination controls showing '10' items and '1 of 1' pages. A table lists the checks with columns: Active, Name, Associated With, Last Status, Last Run, and Last Stdout. One check is listed: 'SID 2100498 - root events' with ID '2100498', status 'CRITICAL', last run '9/25/2025, 12:55:01 PM', and last stdout 'Suricata alerts: 8 | 'alert\_count'=8alerts;1;3'.

Active	Name	Associated With	Last Status	Last Run	Last Stdout
<input checked="" type="checkbox"/>	SID 2100498 - root events	2100498	CRITICAL	9/25/2025, 12:55:01 PM	Suricata alerts: 8   'alert_count'=8alerts;1;3

## System Alerts

System alerts enable you to run basic checks of resource utilization on your Network Analyzer server, including CPU, Memory, and Root Drive usage.

To begin, select the **System** tab in **Alerting**, then click **+ New System Check**:



The screenshot shows the 'Alerting' section of the Nagios Network Analyzer interface, similar to the previous one but with the 'System' tab selected. The 'System' tab is highlighted with a yellow box, and the '+ New System Check' button is also highlighted with a yellow box. The table is currently empty.

# How Alerting Works in Nagios Network Analyzer 2026

Next, enter a **Name** for the check, and select the **Check Association**, in **Step 1**:

The screenshot shows the 'Add System Check' dialog in Step 1. The title is 'Add System Check' with a checkmark icon. The subtitle is 'Step 1 - Select Resource and Metric'. Below the title, it says 'Select the resource for the check.' There is a text input field for 'Name' containing 'NNA Memory Used'. Below that, there is a section for 'Check Association' with three radio buttons: 'CPU', 'Memory' (which is selected), and 'Root Drive'. Below the radio buttons, there are two dropdown menus. The first dropdown is labeled 'Memory Used (%)' and has a downward arrow. The second dropdown is also labeled 'Memory Used (%)' and has a checkmark icon. Below the second dropdown, there is a third option 'Memory Swap (%)'. At the bottom right, there are two buttons: 'Cancel' and 'Next'.

In **Step 2**, define your Warning and Critical thresholds, and choose whether the check should be run immediately after creation with the **Force Check on Creation** toggle (if left off, the check will run for the first time the next time checks are normally scheduled to execute).

The screenshot shows the 'Add System Check' dialog in Step 2. The title is 'Add System Check' with a checkmark icon. The subtitle is 'Step 2 - Select Thresholds'. Below the title, it says 'Select the thresholds for the check.' There are two text input fields: 'Warning Threshold' with the value '70' and 'Critical Threshold' with the value '90'. To the right of these fields is a toggle switch labeled 'Force Check on Creation', which is currently turned off. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.



# How Alerting Works in Nagios Network Analyzer 2026

Finalize your System check by choosing your notification options in **Step 3**, then click **Create**.

Your new System check will appear in the Alerting menu list:

## Alerting

Alerting Configs

Define checks that can alert users or trigger actions.

Flow Sources

Nmap

Suricata

System

New System Check

System Checks

Search... Search

View 10 1 of 1

Active	Name	Check Metric	Last Status	Last Run	Last Stdout
<input checked="" type="checkbox"/>	NNA Memory Used	Memory Used (%)	WARNING	12/9/2025, 11:36:25 AM	Memory status: 82.01   'used_percent'=82.01%;70;90

1 of 1

## Finishing Up

This completes the documentation on Understanding Alerting in Nagios Network Analyzer 2026. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Nagios Knowledge Base](#)

[Visit Nagios Library](#)