

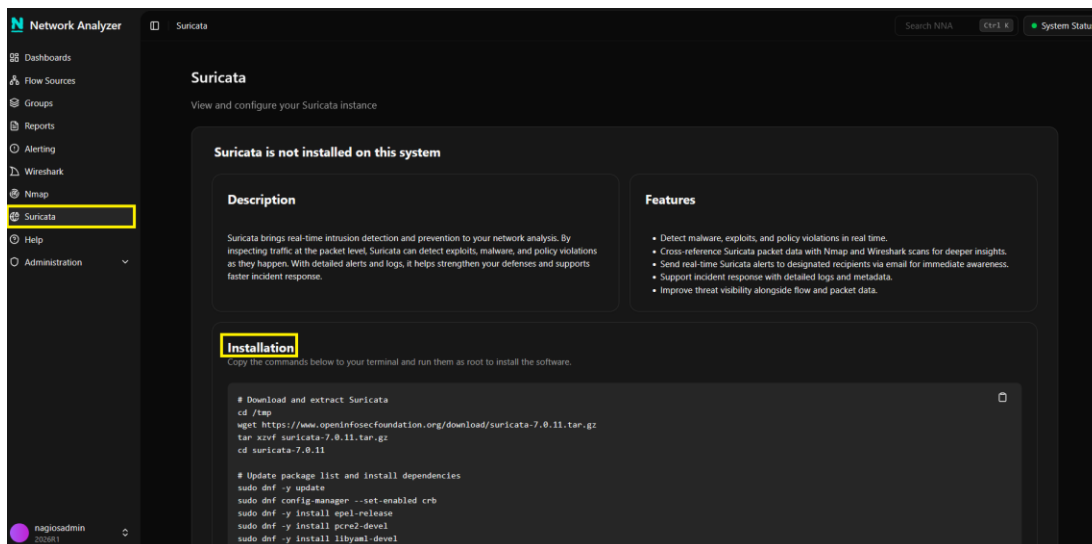
# How To Use Suricata With Nagios Network Analyzer 2026

## Purpose

This document describes how to install Suricata alongside Nagios Network Analyzer 2026, and how to use the integrated network interface and pcap file scanning, alert viewing, and ruleset management capabilities.

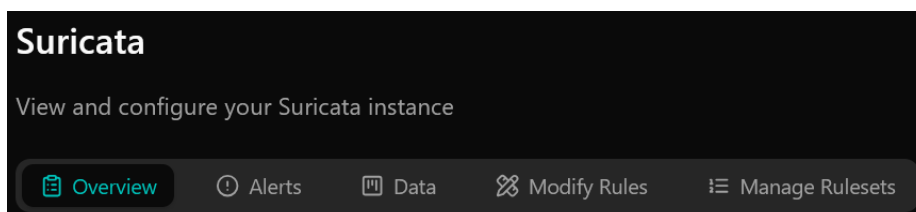
## Initial Setup

To begin, navigate to the **Suricata** section of the UI, and run the commands in the **Installation** section from the command line of your Network Analyzer server. You can use the **Copy** button to copy all of the commands, then paste them into the command prompt and hit **Enter** to run the entire install process.



The installation will take a few minutes to complete once started.

Once the installation completes, refresh the Suricata page. You will now see several tabs of options.



**Note:** after installation, you click the **View Install Instructions** button on the upper right of the Suricata menu to review the instructions.

# How To Use Suricata With Nagios Network Analyzer 2026

## Overview Tab

This tab provides a way to view Suricata Status, start a Suricata scan of the primary Network Analyzer server network interface, view the start time of the current scan if one is running, view Total Weekly Alerts, view a treemap of Suricata Alert Categories, view a pie chart of alert Severity Distribution, and view Top Suricata Alerts From This Week.

Note that you can hover over any section of the Suricata Alert Categories treemap panel to see the number of matching alerts, and click them to drill down to a pre-filtered list of alerts in the category.

**Suricata** View Install Instructions

View and configure your Suricata instance

Overview Alerts Data Modify Rules Manage Rulesets

**Suricata Status** Inactive ▶

**Scan Start Time** ----/--/-- --:--:--

**Total Weekly Alerts** 135

**Interface** None

**Suricata Alert Categories From The Week**

- Generic Protocol Command Decode
- Web Application Attack
- Not Suspicious Traffic

**Severity Distribution From The Week**

- Severity 3
- Severity 2
- Severity 1

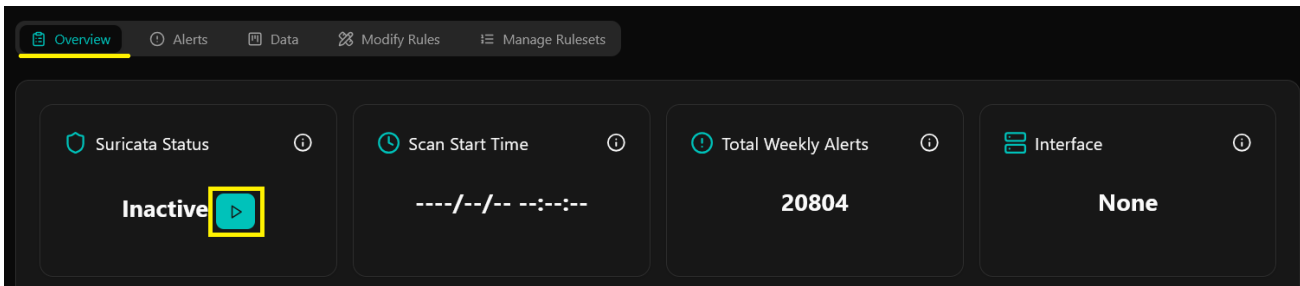
**Top Suricata Alerts From This Week**

Alert Signature	Count
SURICATA Ethertype unknown	52
ET SCAN Possible Nmap User-...	28
SURICATA HTTP Response exce...	19
SURICATA ICMPv4 unknown co...	16
ET INFO Spotify P2P Client	13
ET INFO Server Responded wit...	2
SURICATA HTTP request field ...	1
SURICATA Applayer Detect pro...	1

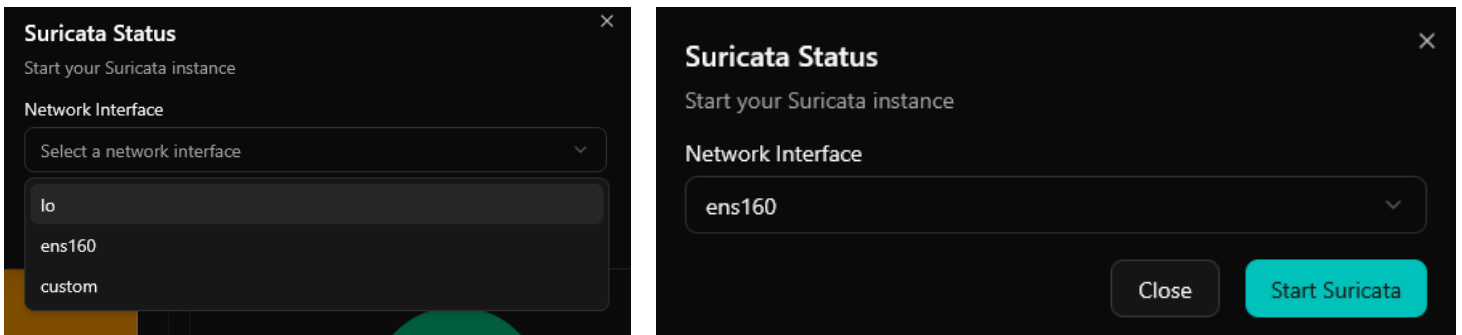
# How To Use Suricata With Nagios Network Analyzer 2026

## Starting and Stopping a Scan

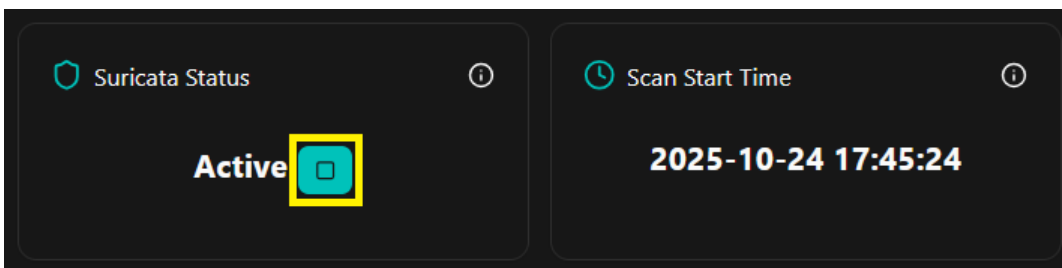
To start a Suricata scan, go to the **Overview** tab, then click the **start** button in the **Suricata Status** panel:



Choose the interface you'd like to scan, then click **Start Suricata**:



When you're ready to stop the scan, click the **stop** button:



Any alerts resulting from the scan will appear in the **Alerts** tab.

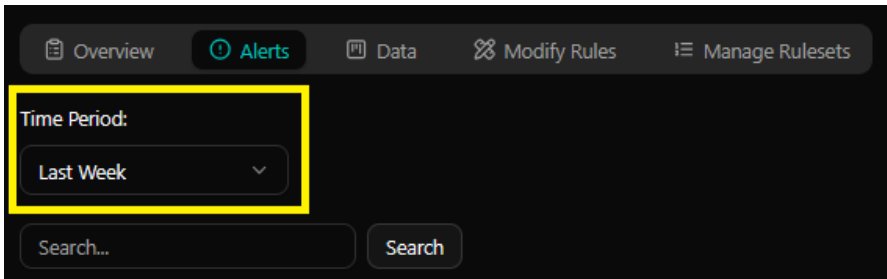
# How To Use Suricata With Nagios Network Analyzer 2026

## Alerts Tab

Alerts generated based on your [Rules](#), found by scans run from the **Overview** tab, can be found here.

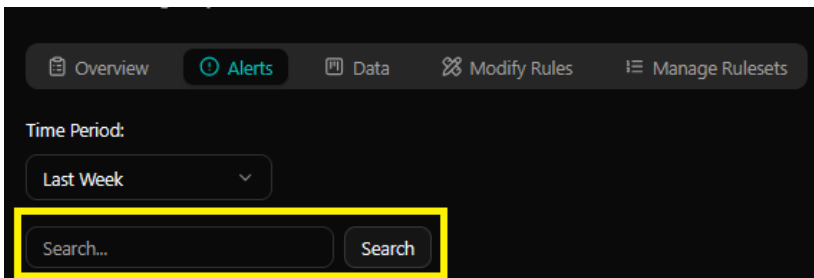
## Adjusting the Time Period

Use the **Time Period** dropdown to view alerts from the last hour, day, week, month, or year.



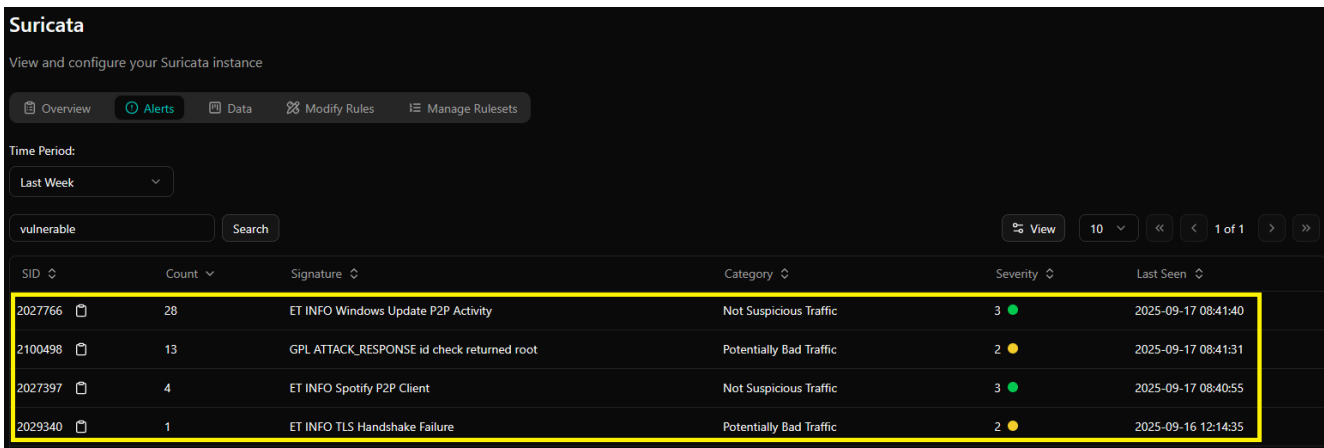
## Searching Alerts

Use the **Search** bar to find specific alerts:



## Reviewing Alert Details

To drill down to the individual entries that generated alerts, simply click an entry in the alerts table:

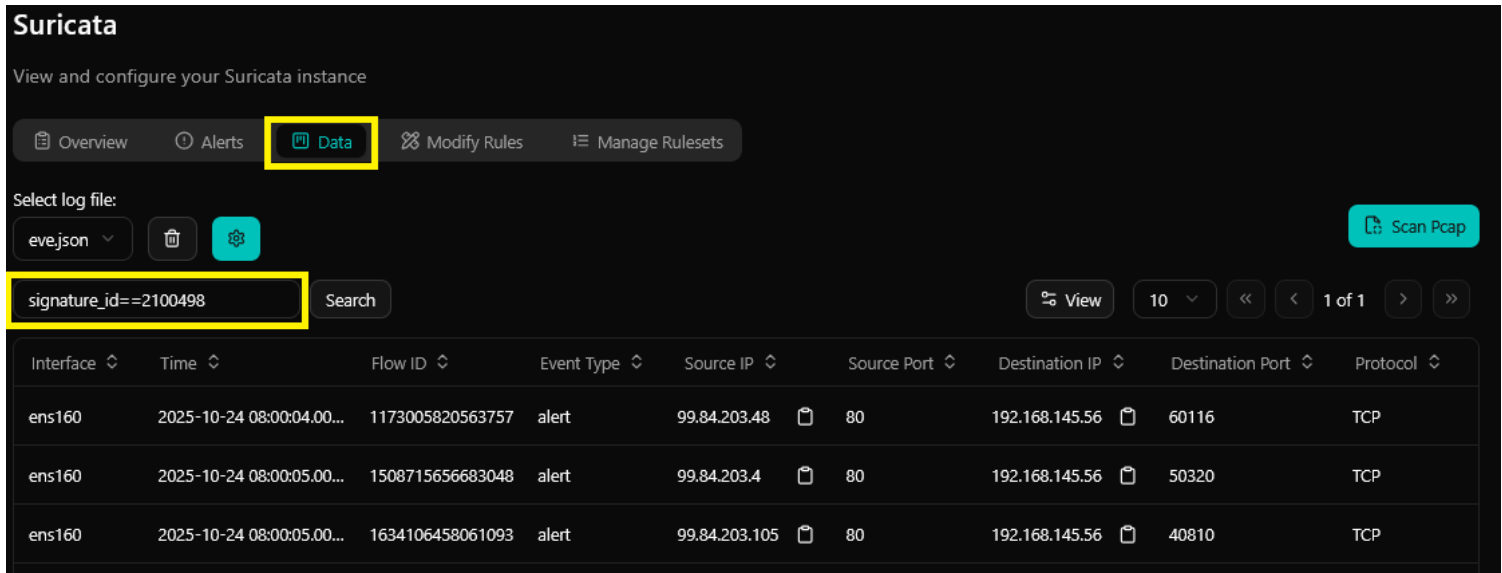


The screenshot shows the Suricata Alerts table. The table is highlighted with a yellow box. The table has the following columns: SID, Count, Signature, Category, Severity, and Last Seen. The table contains the following data:

SID	Count	Signature	Category	Severity	Last Seen
2027766	28	ET INFO Windows Update P2P Activity	Not Suspicious Traffic	3	2025-09-17 08:41:40
2100498	13	GPL ATTACK_RESPONSE id check returned root	Potentially Bad Traffic	2	2025-09-17 08:41:31
2027397	4	ET INFO Spotify P2P Client	Not Suspicious Traffic	3	2025-09-17 08:40:55
2029340	1	ET INFO TLS Handshake Failure	Potentially Bad Traffic	2	2025-09-16 12:14:35

# How To Use Suricata With Nagios Network Analyzer 2026



This will switch you to a list of matching alert events in the **Data** tab, filtered by the SID (Signature ID) of the chosen alert:




Suricata

View and configure your Suricata instance

Overview Alerts **Data** Modify Rules Manage Rulesets

Select log file: eve.json  

**signature\_id==2100498** Search  View 10 << < 1 of 1 > >>

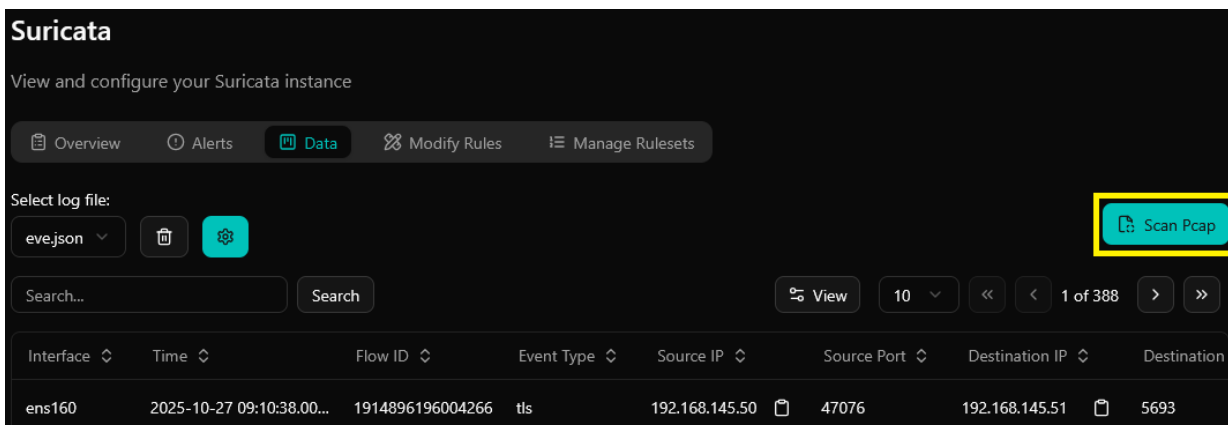
Interface	Time	Flow ID	Event Type	Source IP	Source Port	Destination IP	Destination Port	Protocol
ens160	2025-10-24 08:00:04.00...	1173005820563757	alert	99.84.203.48	80	192.168.145.56	60116	TCP
ens160	2025-10-24 08:00:05.00...	1508715656683048	alert	99.84.203.4	80	192.168.145.56	50320	TCP
ens160	2025-10-24 08:00:05.00...	1634106458061093	alert	99.84.203.105	80	192.168.145.56	40810	TCP

## Data Tab

Here you can scan Pcap files, and review the raw data from Pcap scans you have run, either directly with the **Scan Pcap** button found here, or that you chose to scan with Suricata via the **Wireshark > Capture History** tab (you can learn more about integrating Wireshark [here](#)).

## Scanning a PCAP File



To scan a pcap file with Suricata, first click the **Scan Pcap** button:




Suricata

View and configure your Suricata instance

Overview Alerts **Data** Modify Rules Manage Rulesets

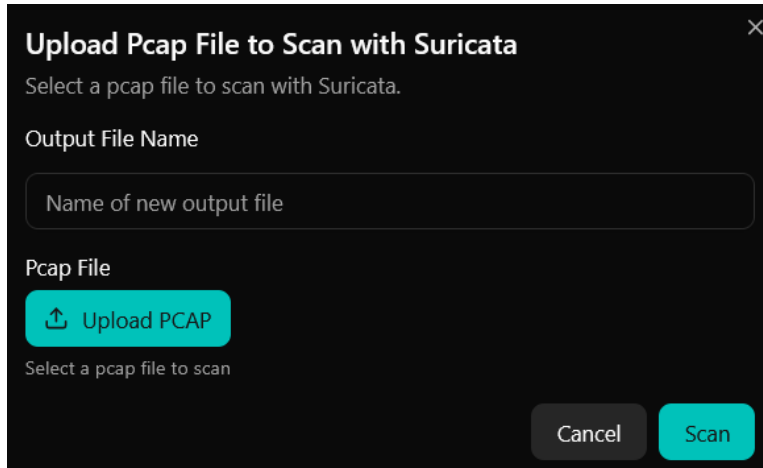
Select log file: eve.json  

Search... Search  View 10 << < 1 of 388 > >>

Interface	Time	Flow ID	Event Type	Source IP	Source Port	Destination IP	Destination
ens160	2025-10-27 09:10:38.00...	1914896196004266	tls	192.168.145.50	47076	192.168.145.51	5693

# How To Use Suricata With Nagios Network Analyzer 2026

Next, define the **Output File Name** (which is what it will show as in the **Select Log File** dropdown), click **Upload PCAP** to select a file, then click **Scan**:

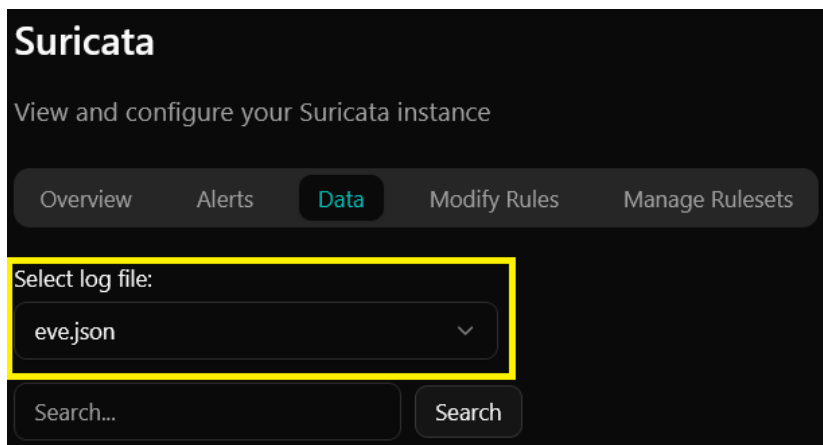


The screenshot shows a dark-themed dialog box titled "Upload Pcap File to Scan with Suricata". It contains a close button (X) in the top right corner. Below the title is the instruction "Select a pcap file to scan with Suricata." There are two main sections: "Output File Name" with a text input field containing "Name of new output file", and "Pcap File" with a blue "Upload PCAP" button. At the bottom, there are "Cancel" and "Scan" buttons.

Once the scan completes, the raw data will appear in the events table here on the **Data** tab.

## Viewing Scan Data

To view scan data, first select a log file using the **Select log file** dropdown:



The screenshot shows the "Suricata" configuration page with the "Data" tab selected. A yellow box highlights the "Select log file:" dropdown menu, which currently shows "eve.json". Below the dropdown is a "Search..." input field and a "Search" button.

The `eve.json` file is your main suricata file, and contains the results of the most recent Suricata scan run from the **Overview** tab.

Other files would include either Pcaps that you imported and scanned, or Pcaps generated by Wireshark that you chose to scan with Suricata.

# How To Use Suricata With Nagios Network Analyzer 2026

**Note:** it is important to watch the size of your main Suricata file, located at:

`/usr/local/var/log/suricata/eve.json`

Consider employing methods such as logrotate to ensure the file remains at a reasonable size even if an extended scan is run.

Once you've selected a file, the results will appear in the events table:

Interface	Time	Flow ID	Event Type	Source IP	Source Port	Destination IP	Destination Port	Protocol	
ens160	2025-09-08T16:25:12.6...	121485903870864	dns	192.168.145.51	44277	192.168.5.80	53	UDP	...
ens160	2025-09-08T16:25:12.6...	121485903870864	dns	192.168.145.51	44277	192.168.5.80	53	UDP	...
ens160	2025-09-08T16:25:13.1...	415297769999517	alert	192.168.107.68	55739	192.168.107.55	7680	TCP	...
ens160	2025-09-08T16:25:13.1...	283392720657030	dns	192.168.107.55	49314	192.168.5.80	53	UDP	...
ens160	2025-09-08T16:25:13.1...	283392720657030	dns	192.168.107.55	49314	192.168.5.80	53	UDP	...
ens160	2025-09-08T16:25:13.5...	308899289390972	alert	192.168.107.55	53706	192.168.106.8	7680	TCP	...
ens160	2025-09-08T16:25:14.7...	737966614306082	http	10.20.30.3	51839	192.168.145.50	80	TCP	...
ens160	2025-09-08T16:25:15.0...	978103741696759	snmp	192.168.0.41	54334	192.168.105.163	161	UDP	...
ens160	2025-09-08T16:25:15.0...	978103741696759	snmp	192.168.105.163	161	192.168.0.41	54334	UDP	...

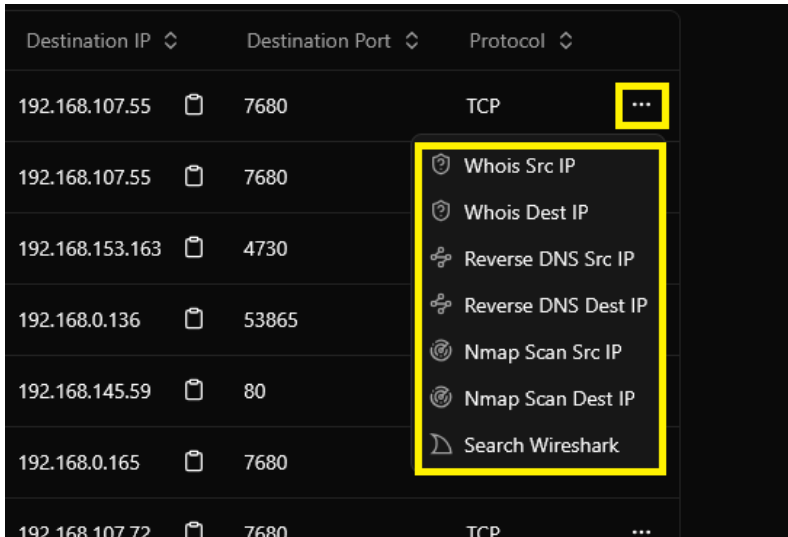
Click on an entry in the table to see complete details, either as text in the **Details** section, or as **JSON**:

```
{
  "timestamp": "2025-09-08T16:25:12.683645-0500",
  "flow_id": 121485903870864,
  "in_iface": "ens160",
  "event_type": "dns",
  "src_ip": "192.168.145.51",
  "src_port": 44277,
  "dest_ip": "192.168.5.80",
  "dest_port": 53,
  "proto": "UDP",
  "pkt_src": "wire/pcap",
  "dns": {
    "version": 2,
    "type": "query",
    "id": 51644,
    "rname": "51.145.168.192.in-addr.arpa",
    "rntype": "PTR",
    "tx_id": 0,
    "opcode": 0
  }
}
```

# How To Use Suricata With Nagios Network Analyzer 2026

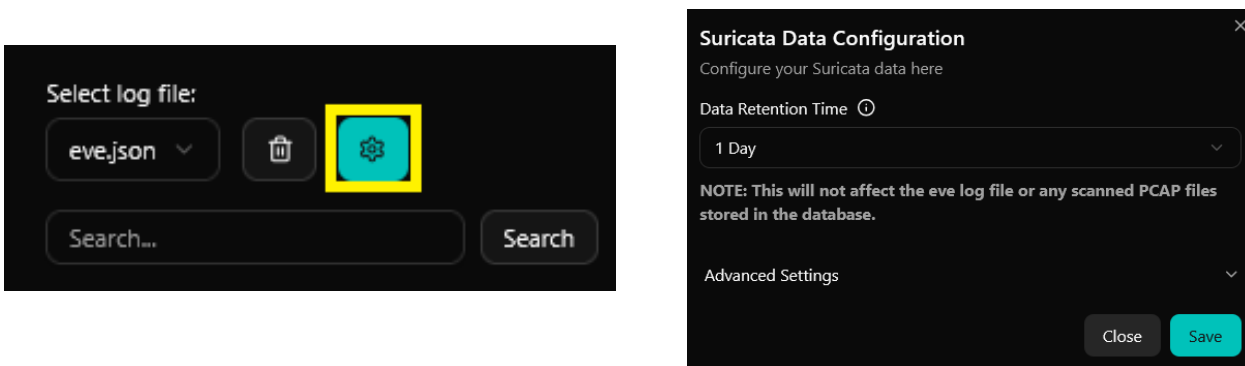
## Further Event Actions

It is also possible to run a Whois, Reverse DNS lookup, [Nmap](#) Scan of the Source and Destination IP, or run a Wireshark Search of each entry in the table. Click the **Actions** icon on the far right of any entry to choose one of these options:



## Suricata Data Configuration

To customize how long data from the main Suricata process will be retained in the database, click the gear icon to the right of the Select log file dropdown, select a Data Retention Time, then click **Save**.

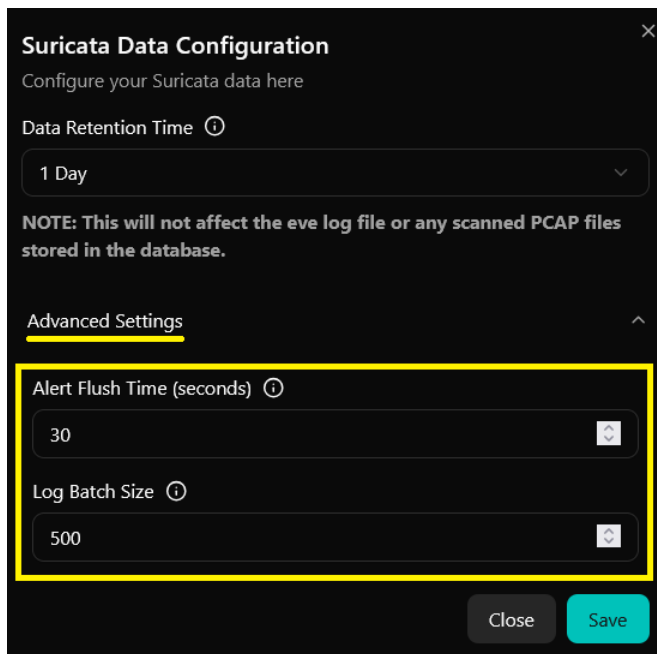


This setting will not affect the `eve.json` log file itself, or any scanned Pcap data stored in the database. It is specifically related to Suricata scan data that is stored in the database, such as the IP addresses and ports in scanned packets.

# How To Use Suricata With Nagios Network Analyzer 2026

## Advanced Settings

The **Advanced Settings** section of the Data Configuration menu enables you to customize the Alert Flush Time and Log Batch Size settings, which determine when the data in the `eve.json` file is moved into the database:



**Suricata Data Configuration** ×  
Configure your Suricata data here

Data Retention Time ⓘ  
1 Day ▼

**NOTE:** This will not affect the eve log file or any scanned PCAP files stored in the database.

Advanced Settings ▲

Alert Flush Time (seconds) ⓘ  
30 ▼

Log Batch Size ⓘ  
500 ▼

Close Save

- **Alert Flush Time:** sets the time in seconds to flush alerts from Suricata to the database.
- **Log Batch Size:** sets how many Suricata logs need to be processed before being pushed to the database.

These advanced settings help maintain system stability in times of extreme activity. Since the Log Batch Size ceiling is for both regular logs and alerts, it can be a valuable safeguard against things like sudden alert floods.

### An example using the default settings:

Due to a network security incident, 500 alerts a second are being generated. If the system waited the full 30 seconds defined by the Alert Flush Time setting before flushing, there would be 15,000 alerts in memory in the final moment before the transfer kicked in, which could overload the system. But, thanks to the Log Batch Size setting, the alerts would be flushed from memory into the database after each set of 500 appeared.

**Important:** increasing these limits can increase load on your Network Analyzer server, so you must ensure that your system has sufficient memory and disk IO to handle the work.

# How To Use Suricata With Nagios Network Analyzer 2026

## Modify Rules Tab

Here you can add ruleset files and view, edit, and delete individual Suricata rules. Rules define specific patterns and behaviors that indicate potential threats, and can be customized to meet your unique requirements and policies.

By default the `suricata.rules` file will be present. After initial Network Analyzer installation it will include the rules from the `et/open` Ruleset, which is automatically enabled. As new rulesets are enabled in **Manage Rulesets**, they will be added to the list in the **Modify Rules** tab. Keep in mind that the rules shown in the **Modify Rules** tab update based on the **Update Frequency** defined for the corresponding rulesets (either defined in the Ruleset files added in **Modify Rules**, or using the setting for Rulesets managed in the **Manage Rulesets** tab). Included Rulesets are set to **1 day** by default.

## Adding Rules

There are three ways to add rules to the list. The first is to enable a ruleset in the [Manage Rulesets](#) tab. Each individual rule in your enabled rulesets will appear in the **Modify Rules** list to be individually customized and enabled/disabled.

The second option is to upload a rules file here in **Modify Rules**, using the **Upload Ruleset** button.

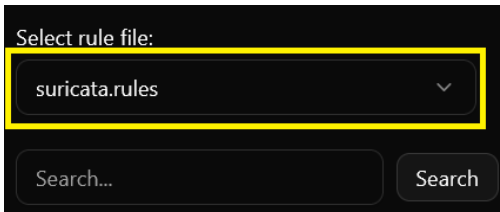
The third is to click the **+ Add Rule** button to the right of the **Upload Ruleset** button. This enables you to define and add single custom rules.

The screenshot displays the 'Suricata' configuration page in Nagios Network Analyzer. The main interface shows a table of rules with columns for SID, Action, and Protocol. A modal window titled 'Add Rule' is open, allowing the user to create a new rule. The modal includes fields for Action, Protocol, Source (IP Address and Port), Destination (IP Address and Port), Direction, and Rule Options (msg, sid). The 'Enabled' checkbox is checked. In the background, the 'Upload Ruleset' and '+ Add Rule' buttons are highlighted with a yellow box.

# How To Use Suricata With Nagios Network Analyzer 2026

## Selecting a Rule File

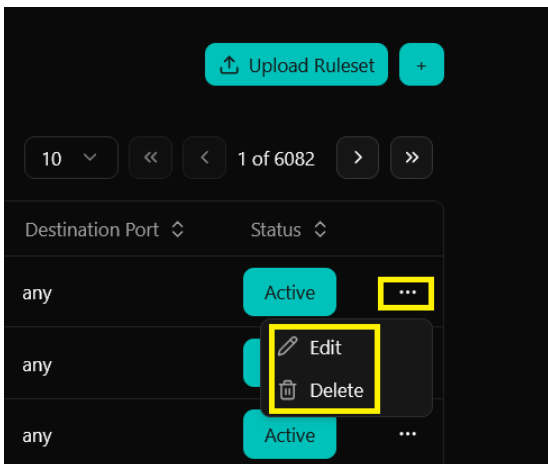
Use the **Select rule file** dropdown to select a different rules file:



## Editing or Deleting a Rule

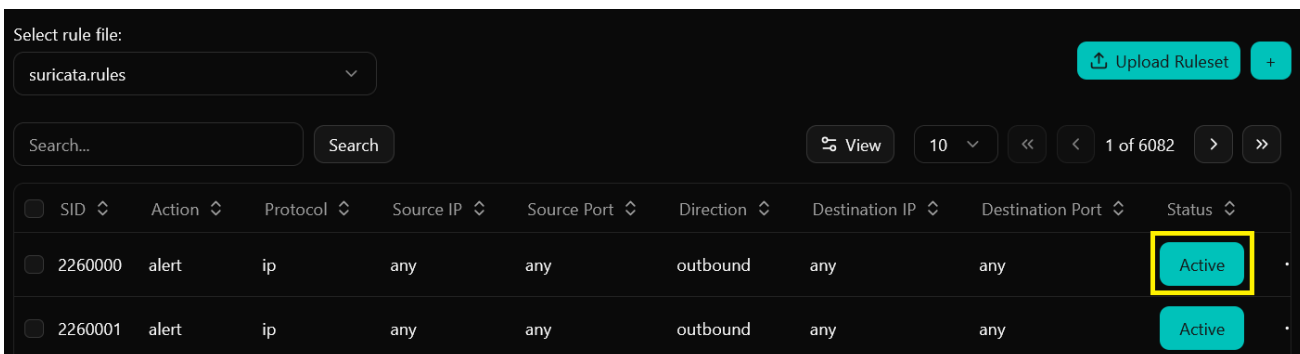
To edit a rule, click the Actions icon to the far right in the table, and select **Edit**.

To delete a rule, click the Actions icon to the far right in the table, and select **Delete**.



## Activating and Deactivating a Rule

To activate or deactivate a rule, use the **Active/Inactive** button in the **Status** column on the right:



# How To Use Suricata With Nagios Network Analyzer 2026

## Adjusting Classtype Severities

The Severity of Suricata alerts is determined by the **classtype** setting for each Rule:



Rule Options	
flow	established
app-layer-event	applayer_mismatch_protocol_both_directions
flowint	applayer.anomaly.count,+1
<b>classtype</b>	<b>protocol-command-decode</b>
rev	1

The Severity codes of each classification type can be changed by modifying the following file:

```
/usr/local/etc/suricata/classification.config
```

Simply modify the trailing number in the target classification type in this file to make the adjustment.

The numbers, meaning, and color used in the user interface for Severity are:

- 1 – Highest/Critical (**red**)
- 2 – Moderate/Minor (**orange**)
- 3 – Low/Informational (**green**)

Changes made to the `classification.config` will be incorporated next time Suricata is run.

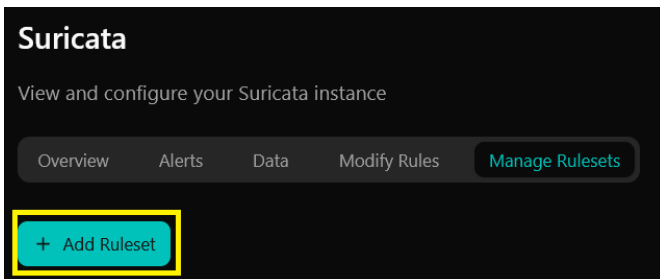
# How To Use Suricata With Nagios Network Analyzer 2026

## Manage Rulesets Tab

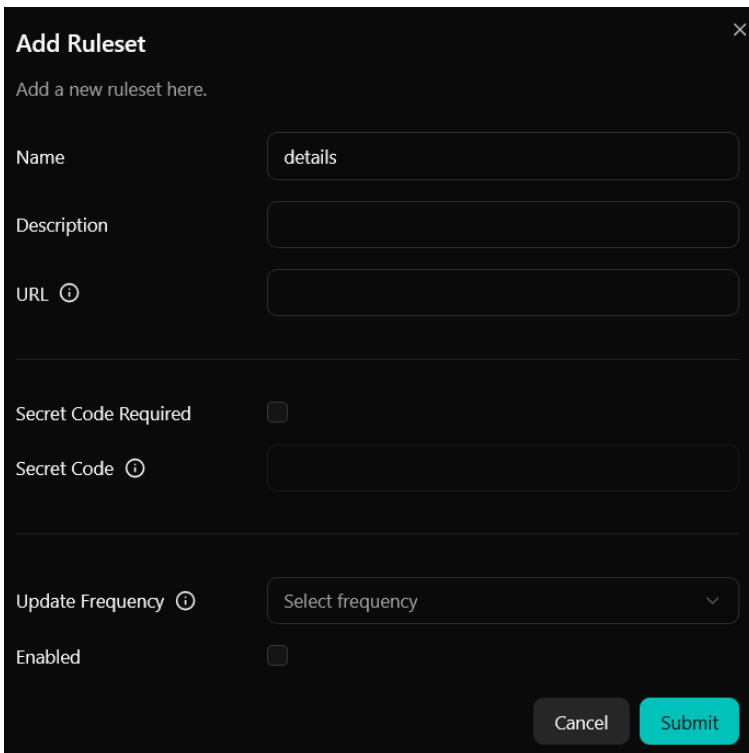
Here you can add, edit, delete, and enable/disable rulesets.

### Adding a Ruleset

To add a ruleset, click the **+ Add Ruleset** button...



...then define the ruleset identification, connection, and authentication details, and click **Submit**.

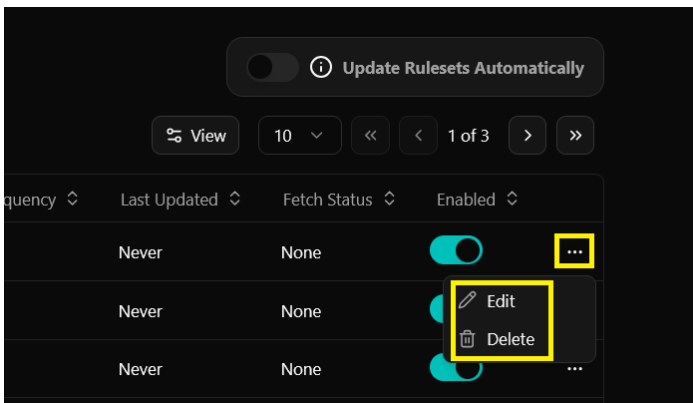
A screenshot of the 'Add Ruleset' form. The title is 'Add Ruleset' with a close button (X) in the top right corner. Below the title is the instruction 'Add a new ruleset here.' The form contains several fields: 'Name' with the value 'details', 'Description', 'URL' with a help icon, 'Secret Code Required' with an unchecked checkbox, 'Secret Code' with a help icon, 'Update Frequency' with a dropdown menu showing 'Select frequency', and 'Enabled' with an unchecked checkbox. At the bottom right, there are two buttons: 'Cancel' and 'Submit'.

# How To Use Suricata With Nagios Network Analyzer 2026

## Editing and Deleting Rulesets

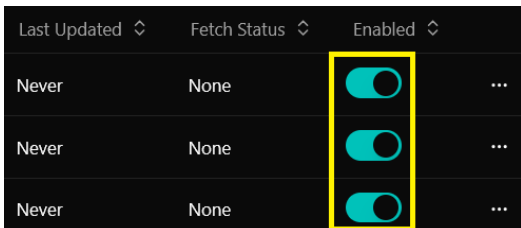
To edit a ruleset, click the Actions icon, and select **Edit**.

To delete a ruleset, click the Actions icon, and select **Delete**.



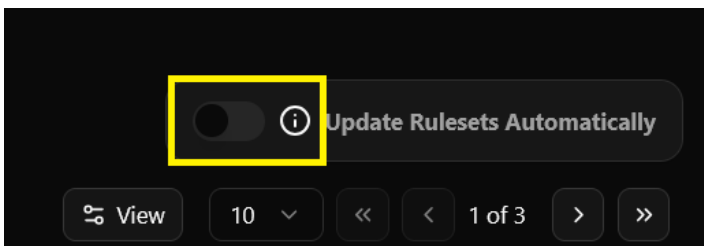
## Enabling and Disabling Rulesets

Use the toggle in the Enabled column on the far right of an entry to enable or disable a ruleset:



## Updating Rulesets Automatically

Use the **Update Rules Automatically** toggle to automatically pull updates for your rulesets.



**Note:** If this is enabled, changes you have made to individual rules in the **Modify Rules** tab (eg editing or deleting them) will be overwritten when their corresponding ruleset is auto-updated.

# How To Use Suricata With Nagios Network Analyzer 2026

## Suricata Upgrade Notes

Some new versions of Nagios Network Analyzer will upgrade your Suricata version. The Network Analyzer upgrader will handle the update for you, so no additional steps are absolutely required.

Although major Suricata updates could add new options to key files in `/usr/local/etc/suricata` such as the `suricata.yaml`, `classification.conf`, `reference.config`, and `threshold.config`, the Suricata update run by Network Analyzer will not overwrite your current files.

Instead, your current files will be retained as the active files Suricata uses, and the latest version will be saved as **.new** in `/usr/local/etc/suricata`:

- `suricata.yaml.new`
- `classification.conf.new`
- `reference.config.new`
- `threshold.config.new`

These **.new** files can be referenced to view changes and incorporate them into the working files at your discretion.

## Finishing Up

This completes the documentation on Using Suricata with NNA 2026. If you have additional questions or other support-related questions, please visit the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Documentation Hub](#)

[Visit Nagios Library](#)