How To Use Suricata With Nagios Network Analyzer 2026

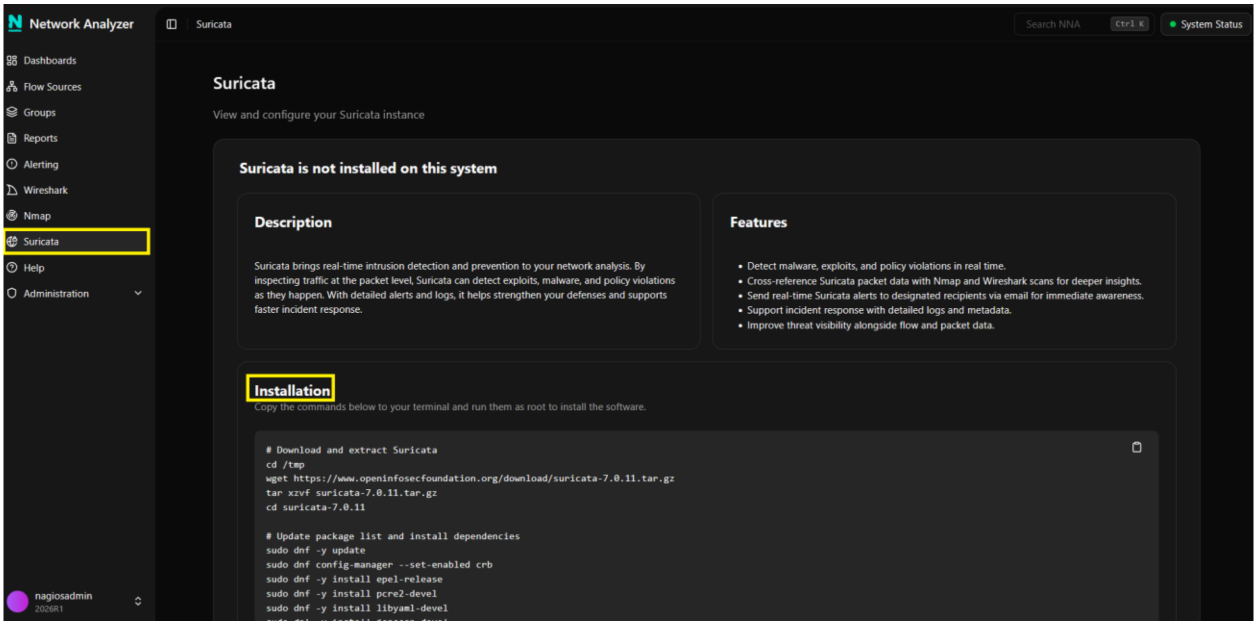
Purpose

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.

You can also find the commands in the Installation Commands section of this guide.



Suricata

View and configure your Suricata instance

Suricata is not installed on this system

Description

Suricata brings real-time intrusion detection and prevention to your network analysis. By inspecting traffic at the packet level, Suricata can detect exploits, malware, and policy violations as they happen. With detailed alerts and logs, it helps strengthen your defenses and supports faster incident response.

Features

- Detect malware, exploits, and policy violations in real time.
- Cross-reference Suricata packet data with Nmap and Wireshark scans for deeper insights.
- Send real-time Suricata alerts to designated recipients via email for immediate awareness.
- Support incident response with detailed logs and metadata.
- Improve threat visibility alongside flow and packet data.

Installation

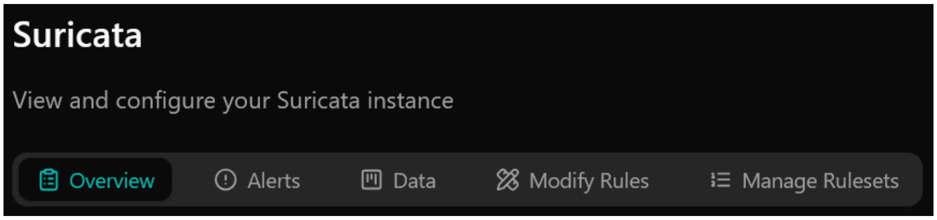
Copy the commands below to your terminal and run them as root to install the software.

```
# Download and extract Suricata
cd /tmp
wget https://www.openinfosecfoundation.org/download/suricata-7.0.11.tar.gz
tar xzvf suricata-7.0.11.tar.gz
cd suricata-7.0.11

# Update package list and install dependencies
sudo dnf -y update
sudo dnf config-manager --set-enabled crb
sudo dnf -y install epel-release
sudo dnf -y install pcre2-devel
sudo dnf -y install libyaml-devel
```

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

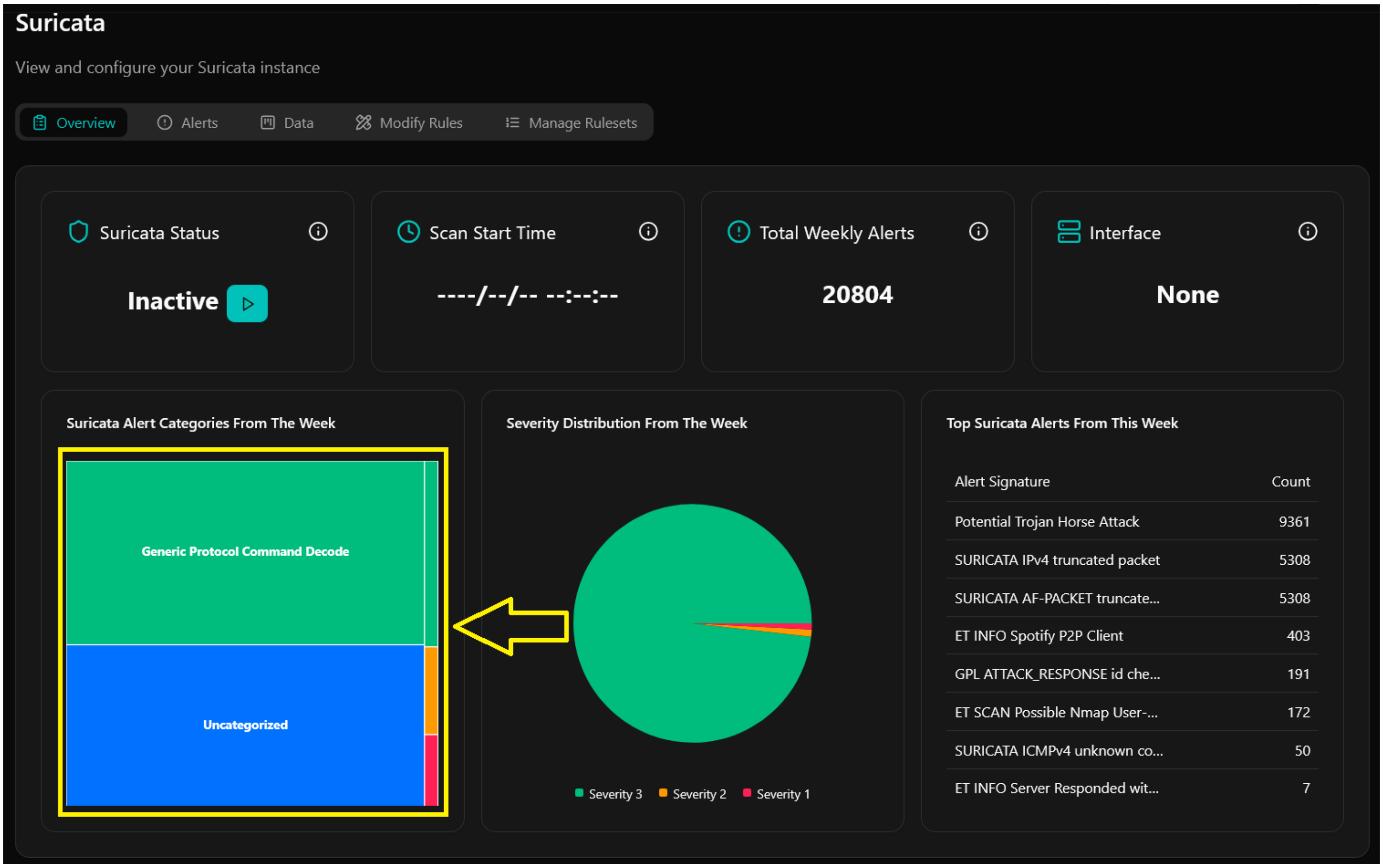
Once the installation completes, refresh the Suricata page. You will now see several tabs of options.



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 and configure your Suricata instance

Suricata Status: Inactive

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

Total Weekly Alerts: 20804

Interface: None

Suricata Alert Categories From The Week

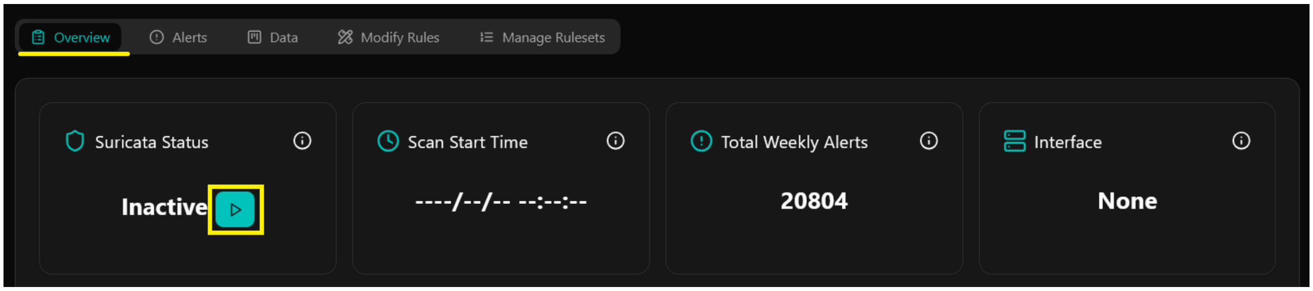
Severity Distribution From The Week

Top Suricata Alerts From This Week

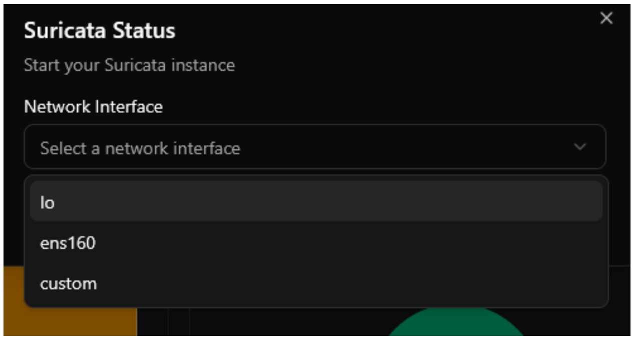
Alert Signature	Count
Potential Trojan Horse Attack	9361
SURICATA IPv4 truncated packet	5308
SURICATA AF-PACKET truncate...	5308
ET INFO Spotify P2P Client	403
GPL ATTACK_RESPONSE id che...	191
ET SCAN Possible Nmap User-...	172
SURICATA ICMPv4 unknown co...	50
ET INFO Server Responded wit...	7

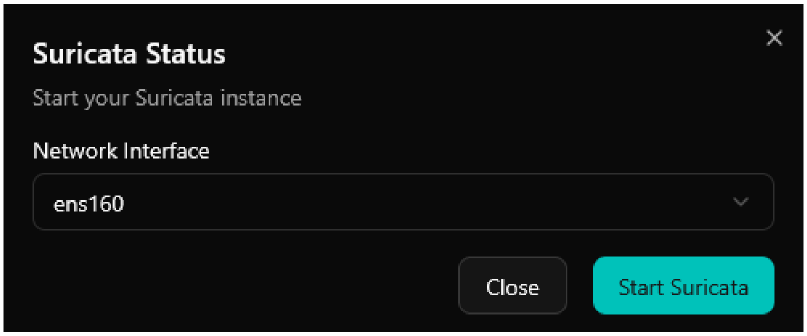
Starting and Stopping a Scan

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

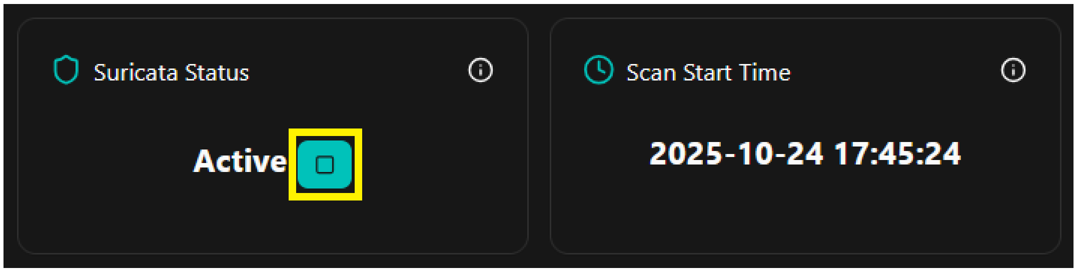


Choose the interface you'd like to scan, then click **Start Suricata**:





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



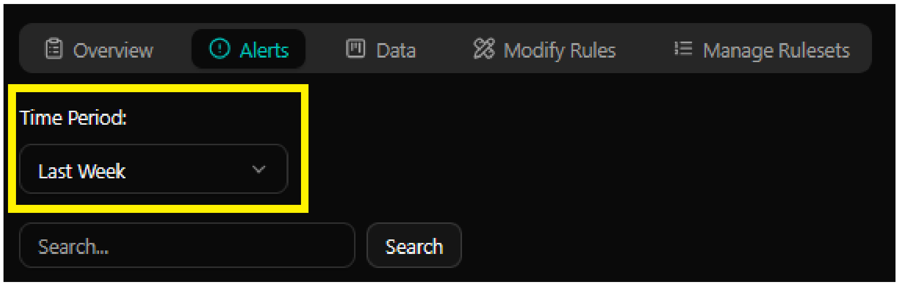
Any alerts resulting from the scan will appear in the **Alerts** tab.

Alerts Tab

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

Adjusting the Time Period

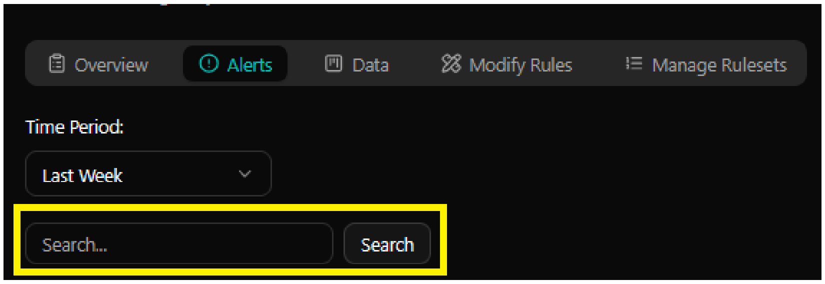
Use the **Time Period** dropdown to view alerts from the last hour, day, week, month, or year.



Time Period: Last Week

Searching Alerts

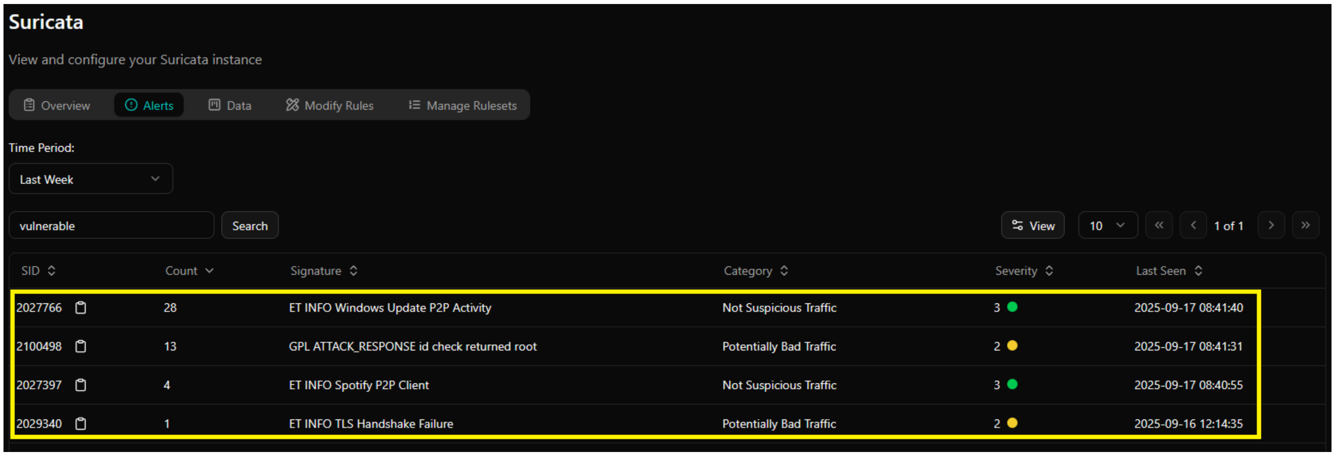
Use the **Search** bar to find specific alerts:



Time Period: Last Week

Reviewing Alert Details

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

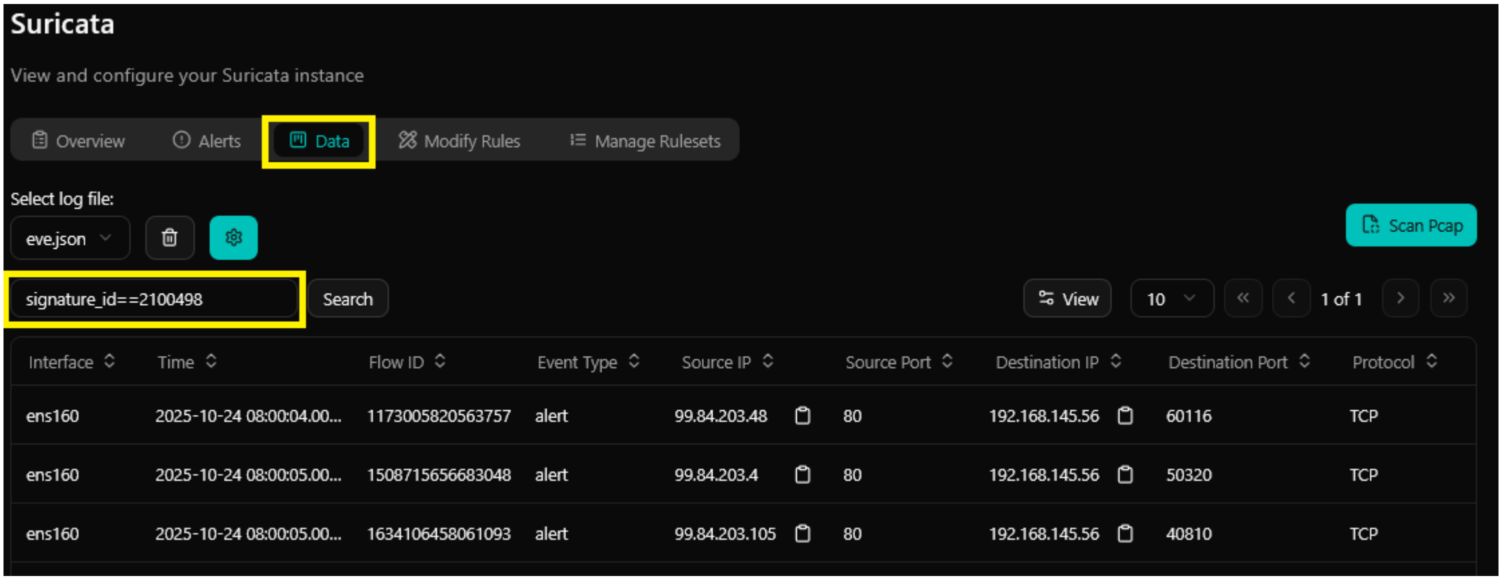


Time Period: Last Week

vulnerable

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

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:



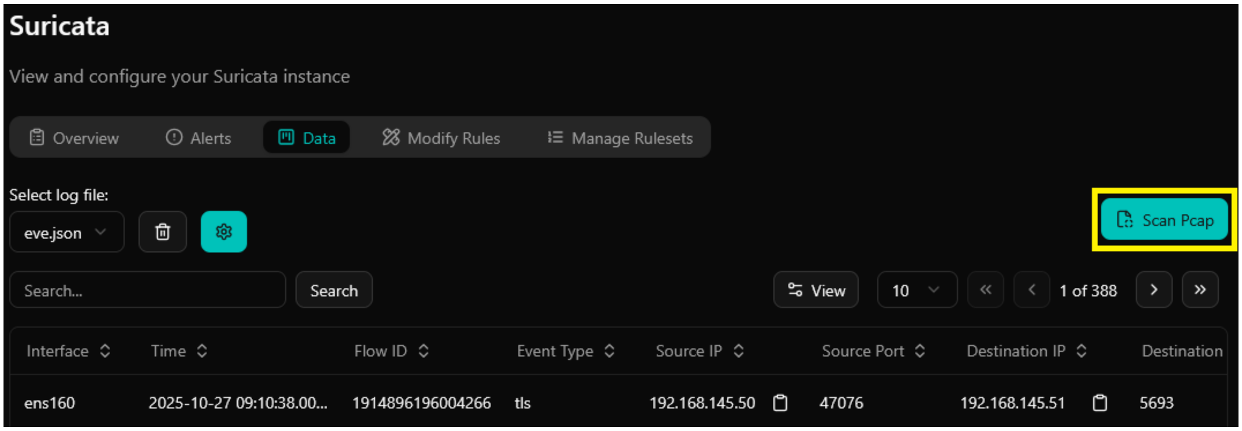
Interface	Time	Flow ID	Event Type	Source IP	Source Port	Destination IP	Destination Port	Protocol
ens160	2025-10-24 08:00:04.00...	1173005820563757	alert	99.84.203.48	80	192.168.145.56	60116	TCP
ens160	2025-10-24 08:00:05.00...	1508715656683048	alert	99.84.203.4	80	192.168.145.56	50320	TCP
ens160	2025-10-24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

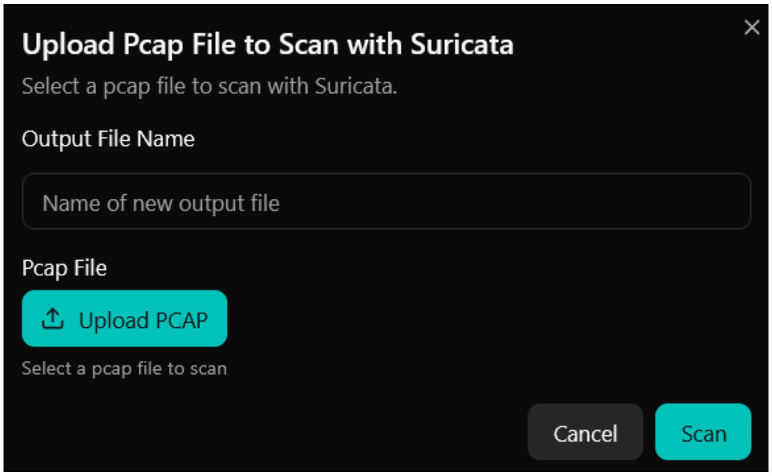
Scanning a PCAP File

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



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

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**:



Upload Pcap File to Scan with Suricata

Select a pcap file to scan with Suricata.

Output File Name

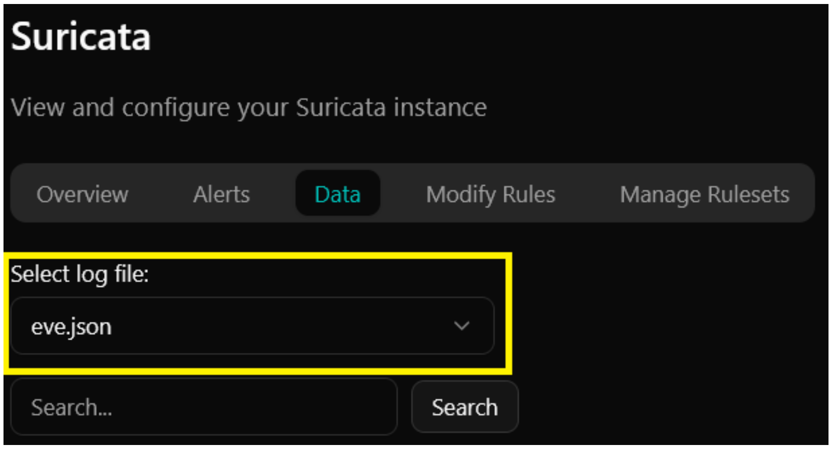
Name of new output file

Pcap File

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:



Suricata

View and configure your Suricata instance

Select log file: eve.json

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

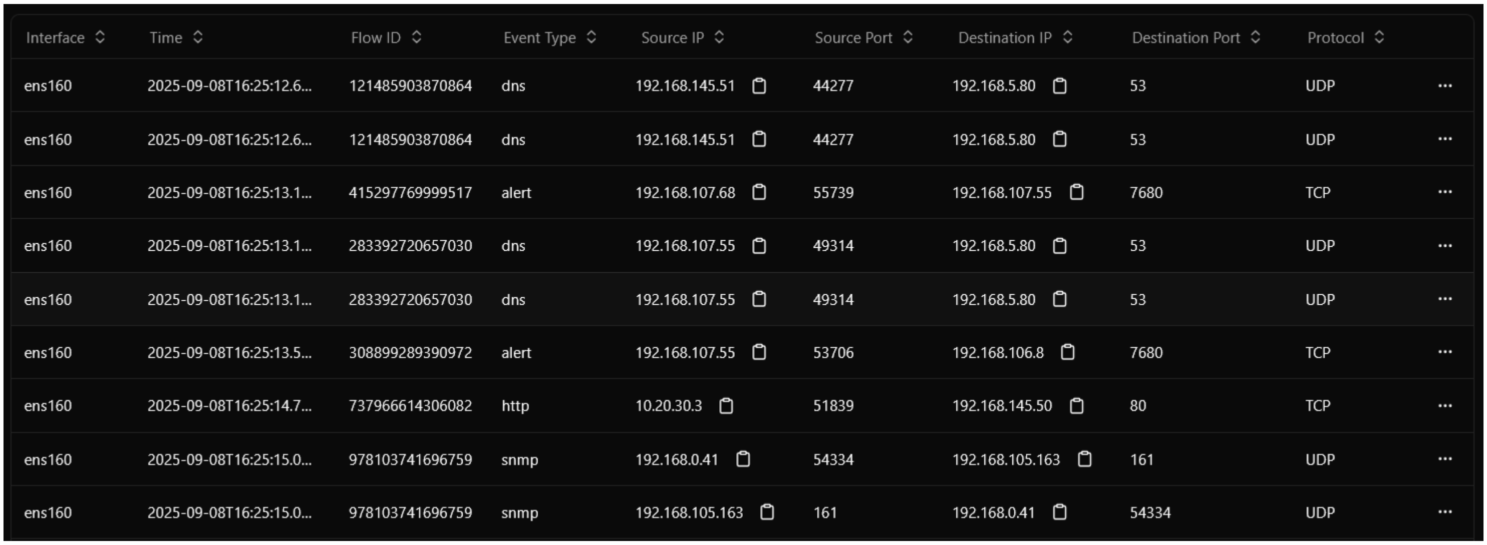
Other files would include either Pcaps that you imported and scanned, or Pcaps generated by Wireshark that you chose to scan with Suricata.

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

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

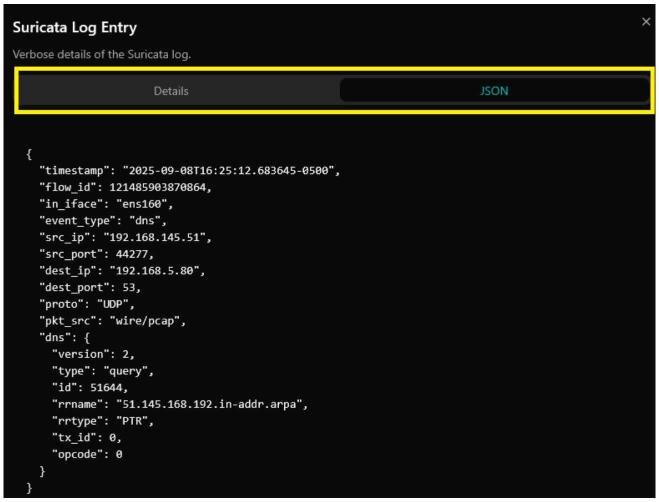
Consider employing methods such as logrotate to ensure the file remains at a reasonable size even if an extended scan is run.

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	···

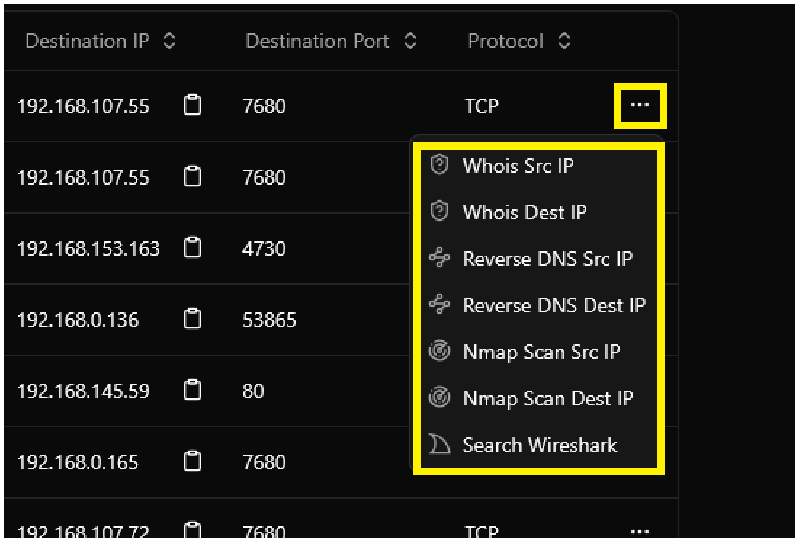
Click on an entry in the table to see complete details, either as text in the **Details** section, or as **JSON**:



```
{
  "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,
    "rrname": "51.145.168.192.in-addr.arpa",
    "rrtype": "PTR",
    "tx_id": 0,
    "opcode": 0
  }
}
```

Further Event Actions

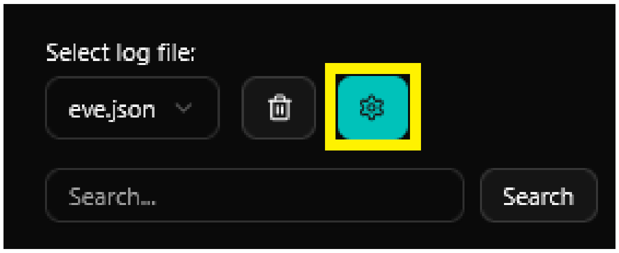
It is also possible to run a Whois, Reverse DNS lookup, Nmap Scan of the Source and Destination IP, or run a Wireshark Search of each entry in the table. Click the **Actions** icon on the far right of any entry to choose one of these options:



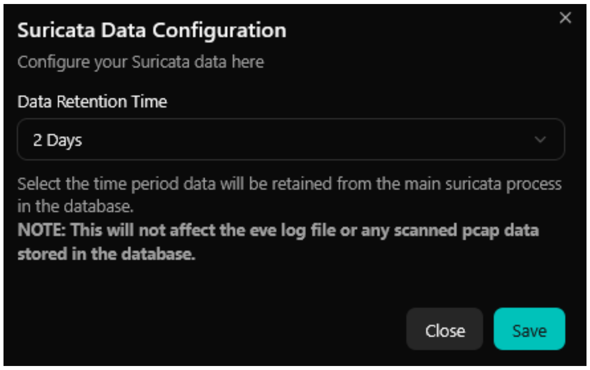
Destination IP	Destination Port	Protocol
192.168.107.55	7680	TCP
192.168.107.55	7680	
192.168.153.163	4730	
192.168.0.136	53865	
192.168.145.59	80	
192.168.0.165	7680	
192.168.107.72	7680	TCP

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**.



Select log file: eve.json



Suricata Data Configuration

Configure your Suricata data here

Data Retention Time: 2 Days

Select the time period data will be retained from the main suricata process in the database.

NOTE: This will not affect the eve log file or any scanned pcap data stored in the database.

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.

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.

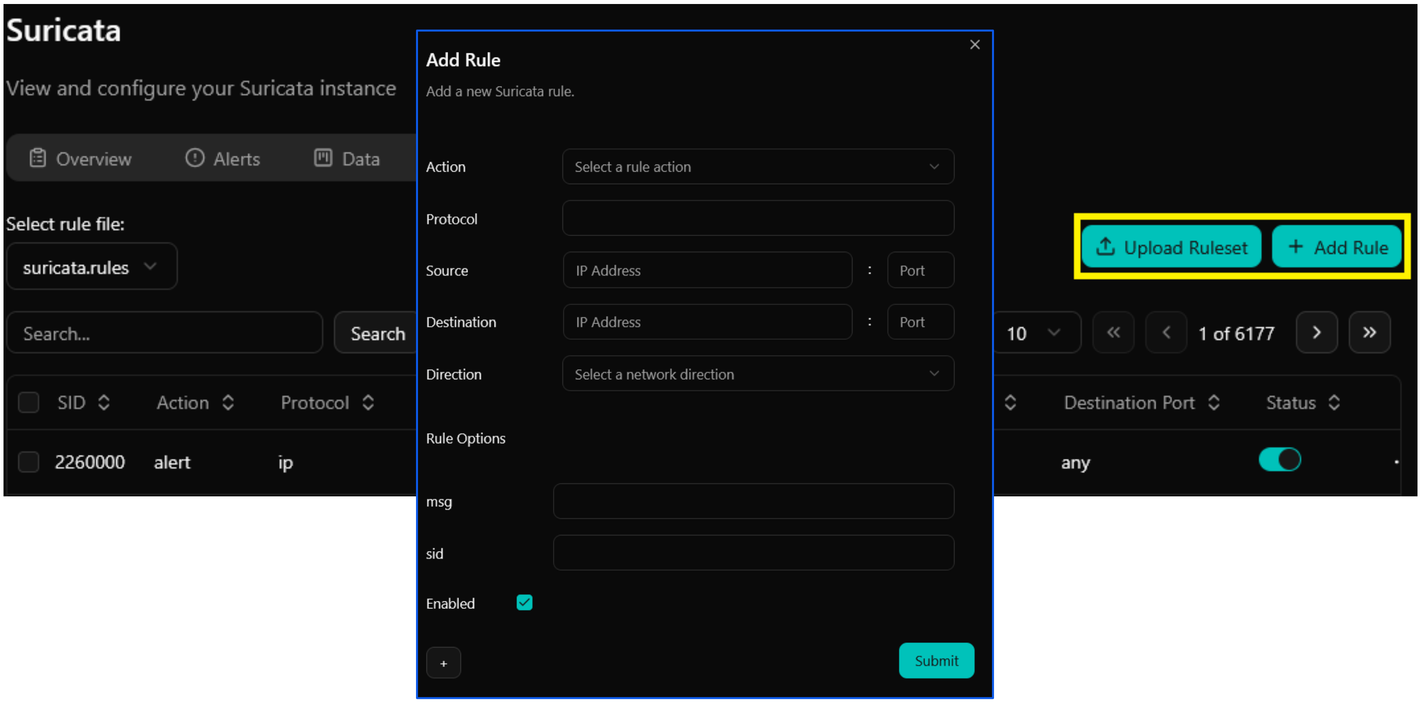
By default the `suricata.rules` file will be present. After initial Network Analyzer installation it will include the rules from the `et/open` Ruleset, which is automatically enabled. As new rulesets are enabled in **Manage Rulesets**, they will be added to the list in the **Modify Rules** tab. Keep 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.

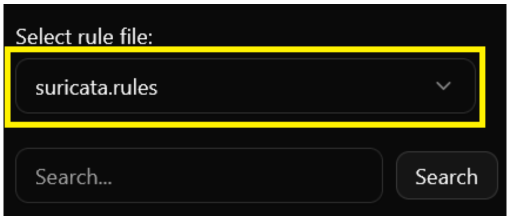
The second option is to upload a rules file here in **Modify Rules**, using the **Upload Ruleset** button.

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.



Selecting a Rule File

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

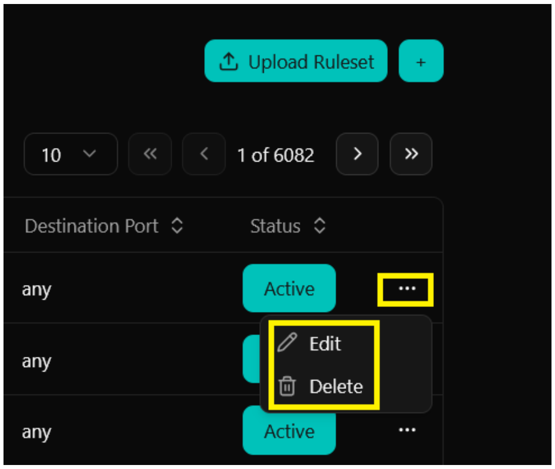


Select rule file: suricata.rules

Editing or Deleting a Rule

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

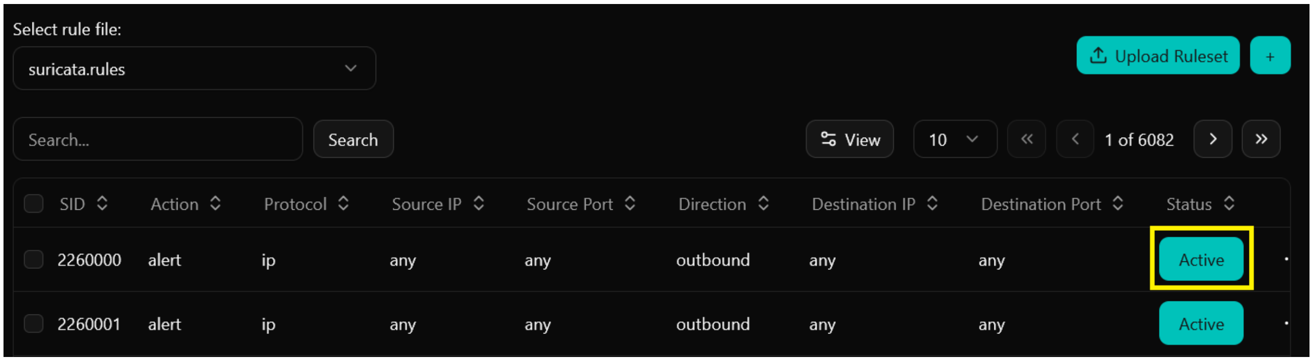
To delete a rule, click the Actions icon to the far right in the table, and select **Delete**.



Destination Port	Status	
any	Active	···
any		
any	Active	···

Activating and Deactivating a Rule

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



Select rule file: suricata.rules

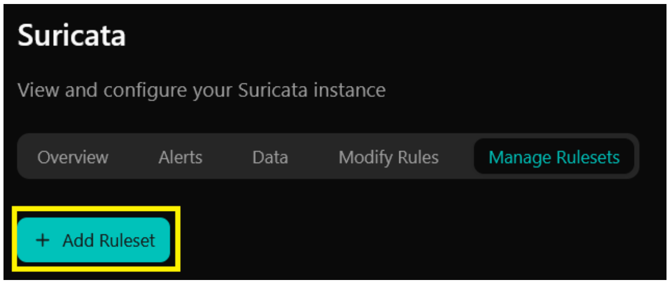
□	SID	Action	Protocol	Source IP	Source Port	Direction	Destination IP	Destination Port	Status
□	2260000	alert	ip	any	any	outbound	any	any	Active
□	2260001	alert	ip	any	any	outbound	any	any	Active

Manage Rulesets Tab

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

Adding a Ruleset

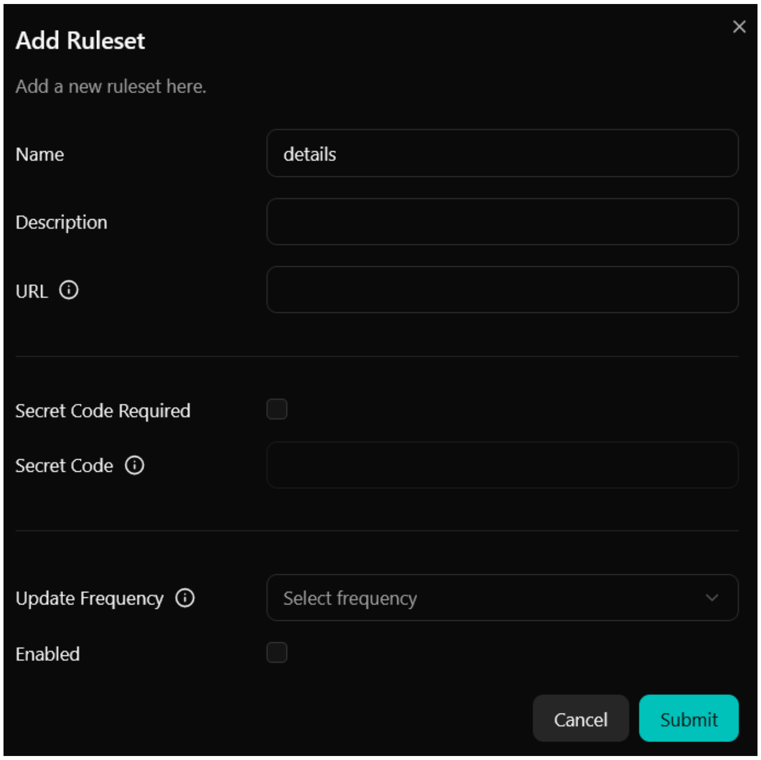
To add a ruleset, click the **+ Add Ruleset** button…



Suricata

View and configure your Suricata instance

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



Add Ruleset

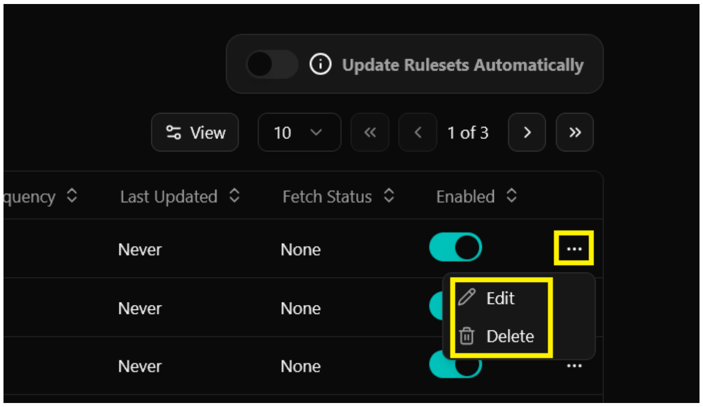
Add a new ruleset here.

Name	details
Description	
URL ⓘ	
Secret Code Required	□
Secret Code ⓘ	
Update Frequency ⓘ	Select frequency
Enabled	□

Editing and Deleting Rulesets

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

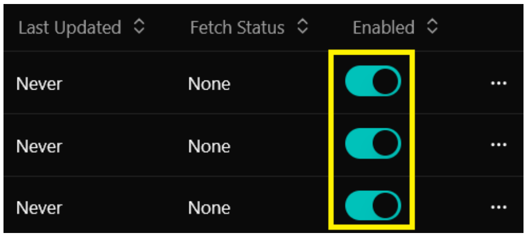
To delete a ruleset, click the Actions icon, and select **Delete**.



quency	Last Updated	Fetch Status	Enabled	
	Never	None		···
	Never	None		
	Never	None		···

Enabling and Disabling Rulesets

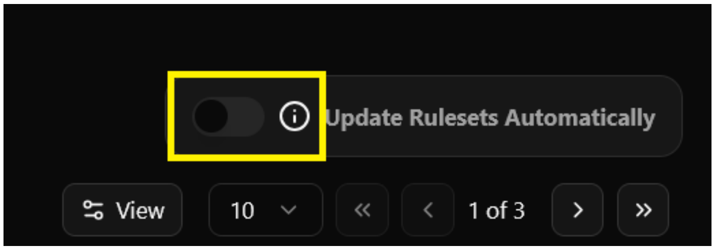
Use the toggle in the Enabled column on the far right of an entry to enable or disable a ruleset:



Last Updated	Fetch Status	Enabled	
Never	None		···
Never	None		···
Never	None		···

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.

Installation Commands

On the following pages, you will find the installation commands initially shown in the user interface.

Be sure to use the commands that match your Network Analyzer server OS (in the UI, the commands shown are automatically based on your OS).

Note that some commands span multiple lines, and include a `\ ` (line continuation character). For best results, copy and paste the entire batch of commands at once into your terminal.

Click your OS to access the commands:

| RHEL |

| CentOS |

| Oracle |

| Debian/Ubuntu |

RHEL

```
cd /tmp
wget https://www.openinfosecfoundation.org/download/suricata-7.0.11.tar.gz
tar xzvf suricata-7.0.11.tar.gz
cd suricata-7.0.11

# Update package list and install dependencies
sudo dnf -y update
sudo dnf -y install ${rhelRPM:-\
https://dl.fedoraproject.org/pub/epel/epel-release-latest-$(rpm -E %{rhel}).noarch.rpm}
sudo dnf -y install pcre2-devel
sudo dnf -y install libyaml-devel
sudo dnf -y install jansson-devel
sudo dnf -y install libpcap-devel
sudo dnf -y install rustc cargo
sudo dnf -y install libcap-ng-devel
sudo dnf -y install libunwind-devel
sudo dnf -y install file-devel
sudo dnf -y install lz4-devel

# Configure, build, and install Suricata
./configure
sudo make
sudo make install-full
sudo ldconfig
sudo /usr/local/bin/suricata-update update-sources

# Permissions for NNA to use Suricata
sudo chown -R nna:nnacmd /usr/local/var/log/suricata
sudo chmod -R 770 /usr/local/var/log/suricata

sudo chmod 644 /usr/local/etc/suricata/suricata.yaml

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata
sudo chmod -R 775 /usr/local/var/lib/suricata

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata/rules
sudo chmod -R 2775 /usr/local/var/lib/suricata/rules

sudo chown -R root:nnacmd /usr/local/etc/suricata
sudo chmod -R 770 /usr/local/etc/suricata/suricata.yaml
sudo chmod -R 770 /usr/local/etc/suricata
sudo chmod 640 /usr/local/etc/suricata/*.config

sudo setcap cap_net_admin,cap_net_raw=eip /usr/local/bin/suricata
```

CentOS

```
cd /tmp
wget https://www.openinfosecfoundation.org/download/suricata-7.0.11.tar.gz
tar xzvf suricata-7.0.11.tar.gz
cd suricata-7.0.11

# Update package list and install dependencies
sudo dnf -y update
sudo dnf config-manager --set-enabled crb
sudo dnf -y install epel-release
sudo dnf -y install pcre2-devel
sudo dnf -y install libyaml-devel
sudo dnf -y install jansson-devel
sudo dnf -y install libpcap-devel
sudo dnf -y install rustc cargo
sudo dnf -y install libcap-ng-devel
sudo dnf -y install libunwind-devel
sudo dnf -y install file-devel
sudo dnf -y install lz4-devel
sudo dnf -y install zlib-devel
sudo pip install pyyaml

# Configure, build, and install Suricata
./configure
sudo make
sudo make install-full
sudo ldconfig
sudo /usr/local/bin/suricata-update update-sources

# Permissions for NNA to use Suricata
sudo chown -R nna:nnacmd /usr/local/var/log/suricata
sudo chmod -R 770 /usr/local/var/log/suricata

sudo chmod 644 /usr/local/etc/suricata/suricata.yaml

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata
sudo chmod -R 775 /usr/local/var/lib/suricata

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata/rules
sudo chmod -R 2775 /usr/local/var/lib/suricata/rules

sudo chown -R root:nnacmd /usr/local/etc/suricata
sudo chmod -R 770 /usr/local/etc/suricata/suricata.yaml
sudo chmod -R 770 /usr/local/etc/suricata
sudo chmod 640 /usr/local/etc/suricata/*.config

sudo setcap cap_net_admin,cap_net_raw=eip /usr/local/bin/suricata
```

Oracle

```
cd /tmp
wget https://www.openinfosecfoundation.org/download/suricata-7.0.11.tar.gz
tar xzvf suricata-7.0.11.tar.gz
cd suricata-7.0.11

# Update package list and install dependencies
sudo dnf -y update
sudo dnf -y install epel-release
sudo dnf -y install pcre2-devel
sudo dnf -y install libyaml-devel
sudo dnf -y install jansson-devel
sudo dnf -y install libpcap-devel
sudo dnf -y install rustc cargo
sudo dnf -y install libcap-ng-devel
sudo dnf -y install libunwind-devel
sudo dnf -y install file-devel
sudo dnf -y install lz4-devel
sudo pip install pyyaml


# Configure, build, and install Suricata
./configure
sudo make
sudo make install-full
sudo ldconfig
sudo /usr/local/bin/suricata-update update-sources

# Permissions for NNA to use Suricata
sudo chown -R nna:nnacmd /usr/local/var/log/suricata
sudo chmod -R 770 /usr/local/var/log/suricata

sudo chmod 644 /usr/local/etc/suricata/suricata.yaml

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata
sudo chmod -R 775 /usr/local/var/lib/suricata

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata/rules
sudo chmod -R 2775 /usr/local/var/lib/suricata/rules

sudo chown -R root:nnacmd /usr/local/etc/suricata
sudo chmod -R 770 /usr/local/etc/suricata/suricata.yaml
sudo chmod -R 770 /usr/local/etc/suricata
sudo chmod 640 /usr/local/etc/suricata/*.config

sudo setcap cap_net_admin,cap_net_raw=eip /usr/local/bin/suricata
```

Debian | Ubuntu

```
cd /tmp
wget https://www.openinfosecfoundation.org/download/suricata-7.0.11.tar.gz
tar xzvf suricata-7.0.11.tar.gz
cd suricata-7.0.11

# Update package list and install dependencies
sudo apt -y update
sudo apt -y install autoconf automake build-essential cargo \
cbindgen libjansson-dev libpcap-dev libpcre2-dev libtool \
libyaml-dev make pkg-config rustc zlib1g-dev
sudo apt -y install libcap-ng-dev
sudo apt -y install libunwind-dev
sudo apt -y install libmagic-dev
sudo apt -y install liblz4-dev

# Configure, build, and install Suricata
./configure
sudo make
sudo make install-full
sudo ldconfig
sudo /usr/local/bin/suricata-update update-sources

# Permissions for NNA to use Suricata
sudo chown -R nna:nnacmd /usr/local/var/log/suricata
sudo chmod -R 770 /usr/local/var/log/suricata

sudo chmod 644 /usr/local/etc/suricata/suricata.yaml

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata
sudo chmod -R 775 /usr/local/var/lib/suricata

sudo chown -R nna:nnacmd /usr/local/var/lib/suricata/rules
sudo chmod -R 2775 /usr/local/var/lib/suricata/rules

sudo chown -R root:nnacmd /usr/local/etc/suricata
sudo chmod -R 770 /usr/local/etc/suricata/suricata.yaml
sudo chmod -R 770 /usr/local/etc/suricata
sudo chmod 640 /usr/local/etc/suricata/*.config

sudo setcap cap_net_admin,cap_net_raw=eip /usr/local/bin/suricata
```

Finishing Up

This completes the documentation on how to use Suricata with 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